Institut Mines-Telecom

Lattice Codes: A theta series perspective

Jean-Claude Belfiore
Based on joint works with C. Ling (ICL), F. Oggier (NTU) and A. Campello Jr.

MCM 2015, München

Outline

Outline

Theta series in Communications: the Past

Definition

Let Λ be a lattice, its theta series is a function of the complex variable τ (holomorphic in the upper half plane),

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

with $q = e^{\imath\pi\tau}$ (we will also use $y = \imath\tau$ and $\tau \in \imath\mathbb{R}$)

Theta series in Communications: the Past

Definition

Let Λ be a lattice, its theta series is a function of the complex variable τ (holomorphic in the upper half plane),

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

with $q = e^{\imath\pi\tau}$ (we will also use $y = \imath\tau$ and $\tau \in \imath\mathbb{R}$)

Error probability

Error probability of a lattice used on a Gaussian channel via union bound and exponential bound of the error function,

$$P_e \leq \frac{1}{2}\left(\Theta_\Lambda(\tau) - 1\right)$$

evaluated at $\tau = \frac{\imath}{8\pi\sigma^2}$.

Approximation

First non trivial term of theta series gives,

$$P_e \lessapprox \frac{\kappa}{2} e^{-\frac{d^2}{8\sigma^2}}$$

where d is the minimum distance of the lattice Λ and κ is its so-called kissing number.

Theta series in Communications: the Past

Definition

Let Λ be a lattice, its theta series is a function of the complex variable τ (holomorphic in the upper half plane),

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

with $q = e^{\imath\pi\tau}$ (we will also use $y = \imath\tau$ and $\tau \in \imath\mathbb{R}$)

Computation of theta series

New problems need the computation of the *full theta series*. Hopefully, theta series of many interesting lattices can be computed by using Jacobi theta functions,

$$\begin{cases} \vartheta_3(\tau) & = \sum_{k\in\mathbb{Z}} q^{k^2} \\ \vartheta_2(\tau) & = \sum_{k\in\mathbb{Z}} q^{\left(k+\frac{1}{2}\right)^2} \end{cases}$$

Error probability

Error probability of a lattice used on a Gaussian channel via union bound and exponential bound of the error function,

$$P_e \leq \frac{1}{2}\left(\Theta_\Lambda(\tau) - 1\right)$$

evaluated at $\tau = \frac{\imath}{8\pi\sigma^2}$.

Approximation

First non trivial term of theta series gives,

$$P_e \lessapprox \frac{\kappa}{2} e^{-\frac{d^2}{8\sigma^2}}$$

where d is the minimum distance of the lattice Λ and κ is its so-called kissing number.

Theta series in Communications: The Present

The Lattice

Let Γ_{72} be the extremal $72-$dimensional lattice found in [Nebe, 2010]. Its Hermite constant is

$$\gamma\left(\Gamma_{72}\right)=\frac{d_{\min}^{2}\left(\Gamma_{72}\right)}{\mathrm{Vol}\left(\Gamma_{72}\right)^{\frac{1}{36}}}=8$$

or approximately 9 dB. One important invariant of a lattice is its flatness factor (to be discussed) which mainly depends on the theta series of the lattice.

Theta series in Communications: The Present

The Lattice

Let Γ_{72} be the extremal 72−dimensional lattice found in [Nebe, 2010]. Its Hermite constant is

$$\gamma\left(\Gamma_{72}\right)=\frac{d_{\min}^{2}\left(\Gamma_{72}\right)}{\mathrm{Vol}\left(\Gamma_{72}\right)^{\frac{1}{36}}}=8$$

or approximately 9 dB. One important invariant of a lattice is its flatness factor (to be discussed) which mainly depends on the theta series of the lattice.

Approximate theta series

$$\begin{aligned}\Theta_{\Gamma_{72}}(\tau)=&1+6218175600q^{8}\\&+152817883545 60q^{10}\\&+9026867482214400q^{12}\\&+198917945081856 0000q^{14}\\&+2130061597599908700 00q^{16}\\&+1314408751763141099520 0q^{18}\\&+5251007186902874957414 40q^{20}\\&+O\left(q^{20}\right)\end{aligned}$$

Theta series in Communications: The Present

The Lattice

Let Γ_{72} be the extremal 72−dimensional lattice found in [Nebe, 2010]. Its Hermite constant is

$$\gamma(\Gamma_{72}) = \frac{d^2_{\min}(\Gamma_{72})}{\mathrm{Vol}(\Gamma_{72})^{\frac{1}{36}}} = 8$$

or approximately 9 dB. One important invariant of a lattice is its flatness factor (to be discussed) which mainly depends on the theta series of the lattice.

Flatness factor

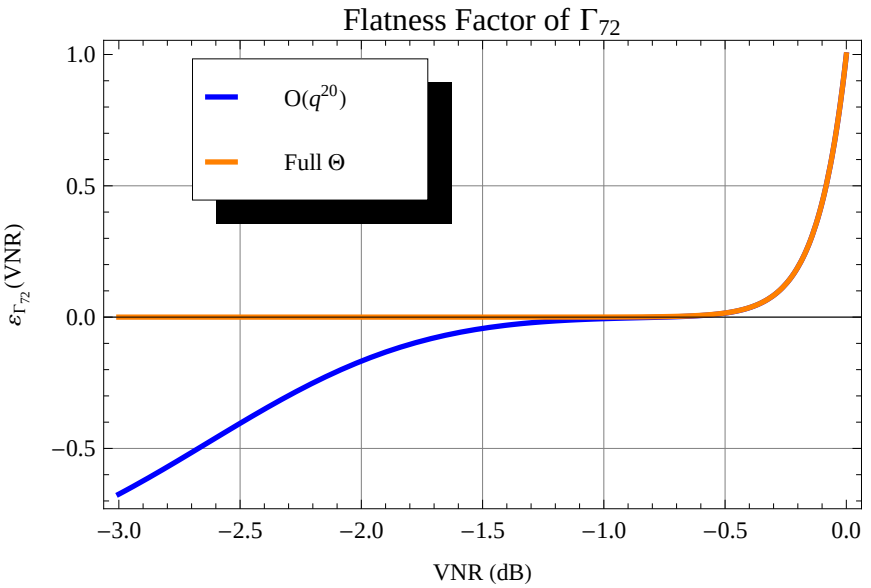

Figure : Flatness factor of Γ_{72} and approximation

Outline

Coset Encoding on $\mathbb{Z}$

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

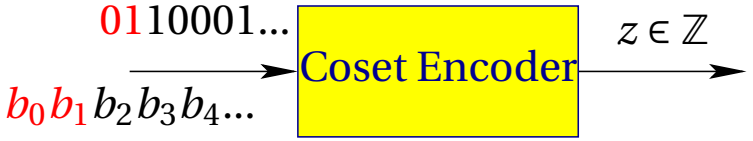

Figure : Special attention to bits b_0 and b_1

Coset Encoding on $\mathbb{Z}$

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

Figure : Special attention to bits b_0 and b_1

Coset Encoding on $\mathbb{Z}$

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

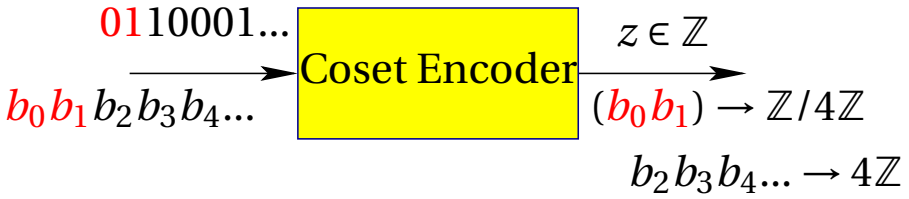

Figure : Special attention to bits b_0 and b_1

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

Coset Encoding on $\mathbb{Z}$

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

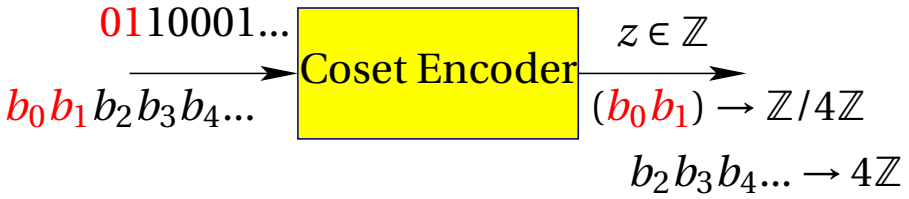

Figure : Special attention to bits b_0 and b_1

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

Decoding $(b_0 b_1)$

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

Coset Encoding on $\mathbb{Z}$

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

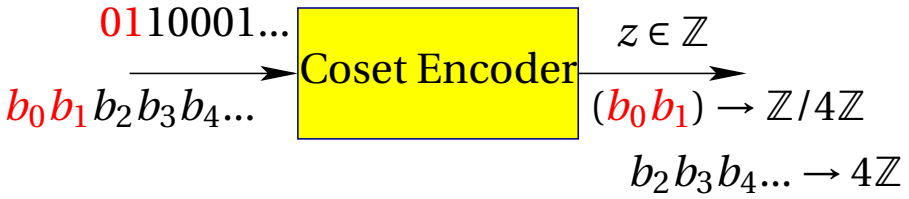

Figure : Special attention to bits b_0 and b_1

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

Decoding $(b_0 b_1)$

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

And with noise..?

What happens if instead of z, we observe $z +$ noise ?

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z \in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z \in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

Suppose $t = 0$, then likelihood is

$$p_{y|t=0}(x) \propto \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}}, \quad x \in [0,4)$$

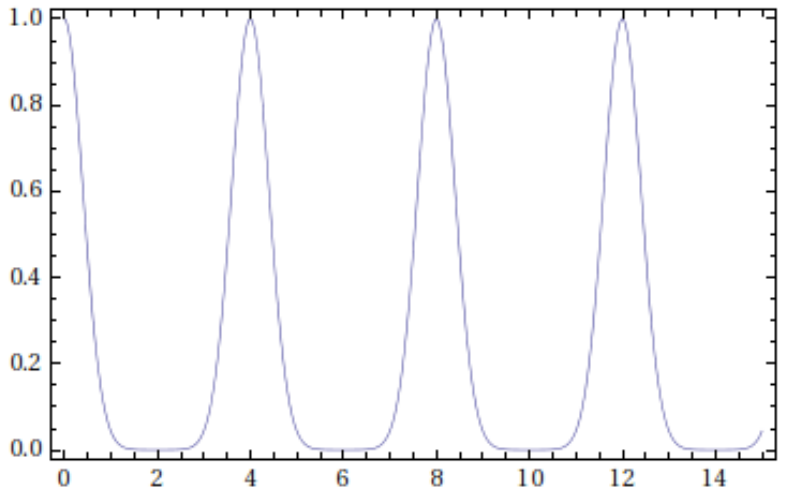

Figure : Sum of Gaussian measures, $\sigma = 0.4$

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z \in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

Suppose $t = 0$, then likelihood is

$$p_{y|t=0}(x) \propto \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}}, \quad x \in [0,4)$$

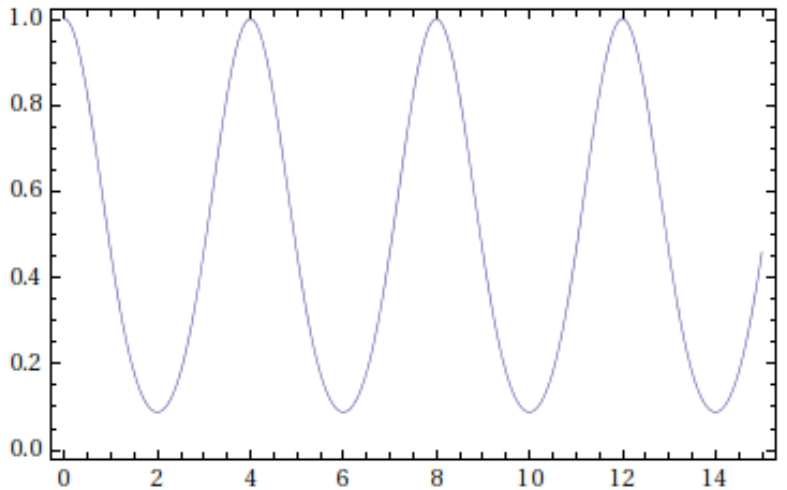

Figure : Sum of Gaussian measures, $\sigma = 0.8$

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z \in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

Suppose $t = 0$, then likelihood is

$$p_{y|t=0}(x) \propto \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}}, \quad x \in [0,4)$$

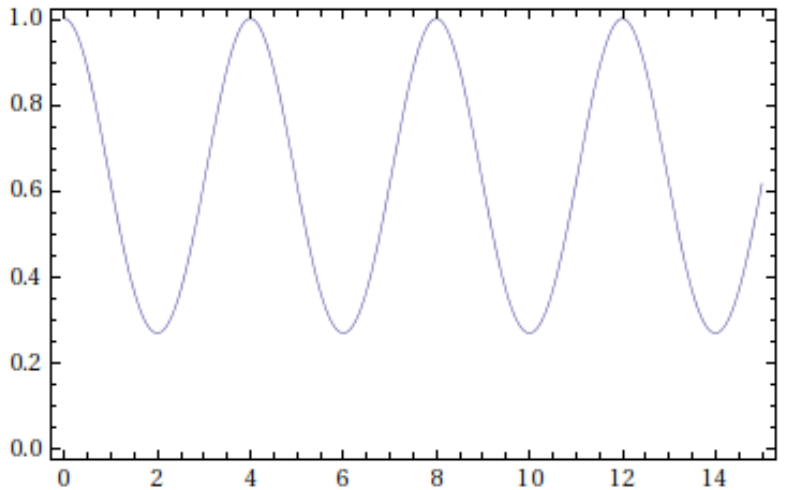

Figure : Sum of Gaussian measures, $\sigma = 1$

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z \in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

Suppose $t = 0$, then likelihood is

$$p_{y|t=0}(x) \propto \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}}, \quad x \in [0,4)$$

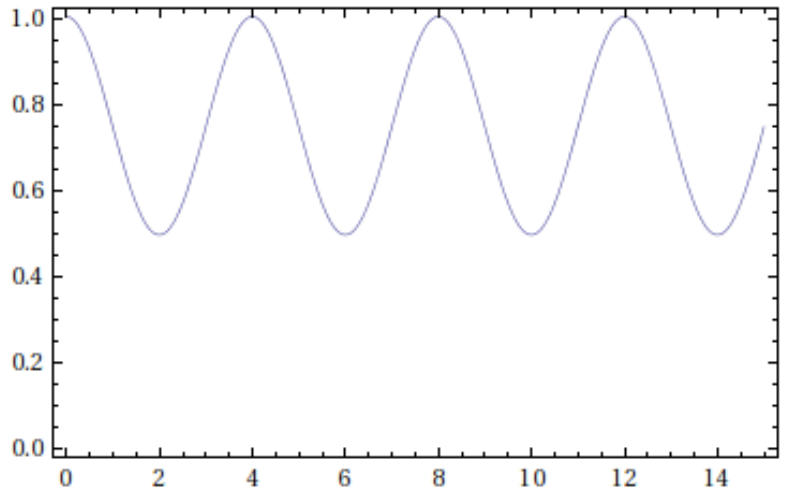

Figure : Sum of Gaussian measures, $\sigma = 1.2$

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z \in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

Suppose $t = 0$, then likelihood is

$$p_{y|t=0}(x) \propto \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}}, \quad x \in [0,4)$$

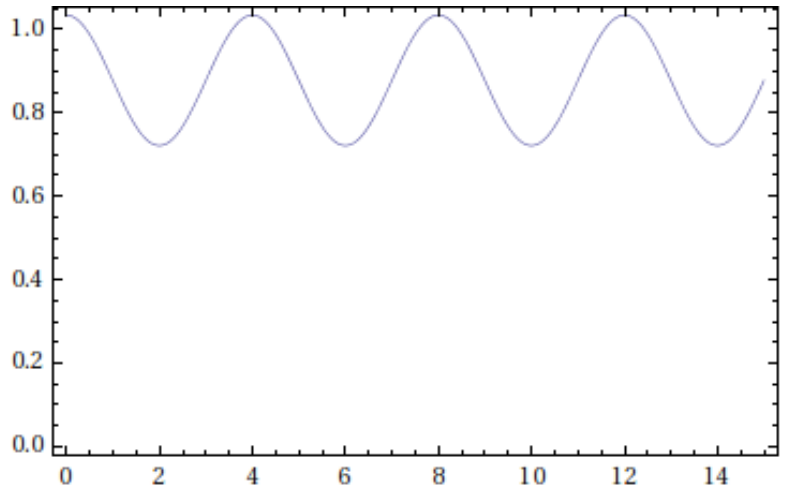

Figure : Sum of Gaussian measures, $\sigma = 1.4$

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z \in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

Suppose $t = 0$, then likelihood is

$$p_{y|t=0}(x) \propto \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}}, \quad x \in [0,4)$$

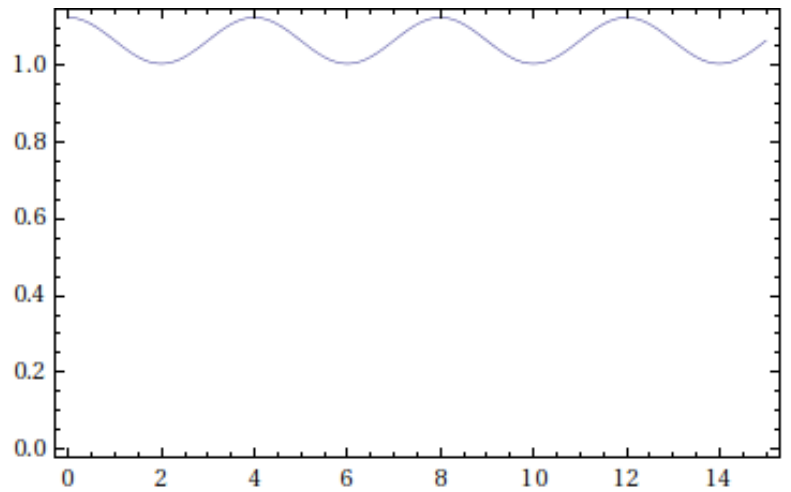

Figure : Sum of Gaussian measures, $\sigma = 1.7$

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z\in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

Suppose $t = 0$, then likelihood is

$$p_{y|t=0}(x) \propto \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}}, \quad x \in [0,4)$$

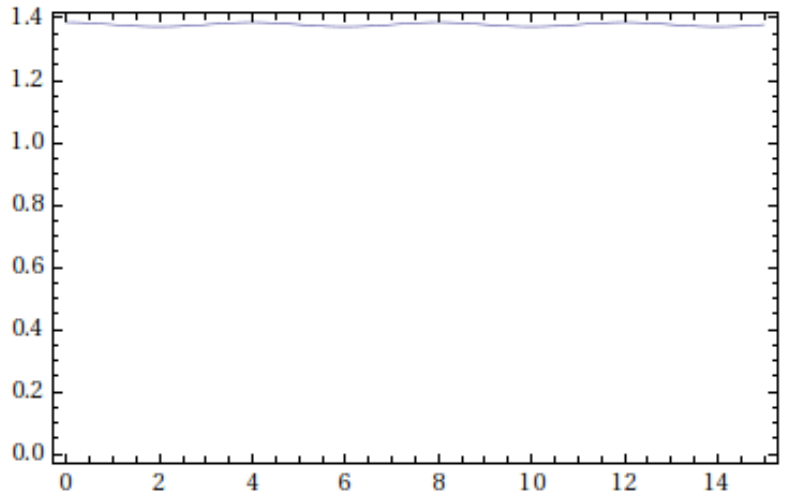

Figure : Sum of Gaussian measures, $\sigma = 2.2$

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

Likelihood

Suppose $y = z + \nu$ where

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

Likelihood is

$$p_{y|b_1,b_2}(x) \propto \sum_{z \in 4\mathbb{Z}} e^{-\frac{(x-t-z)^2}{2\sigma^2}}$$

where $t \in \{0,1,2,3\}$ is labelled by (b_0, b_1).

Same in dimension n with a lattice Λ_b and a sublattice $\Lambda_e \subset \Lambda_b$.

Suppose $t = 0$, then likelihood is

$$p_{y|t=0}(x) \propto \sum_{k=-\infty}^{+\infty} e^{-\frac{(x-4k)^2}{2\sigma^2}}, \quad x \in [0,4)$$

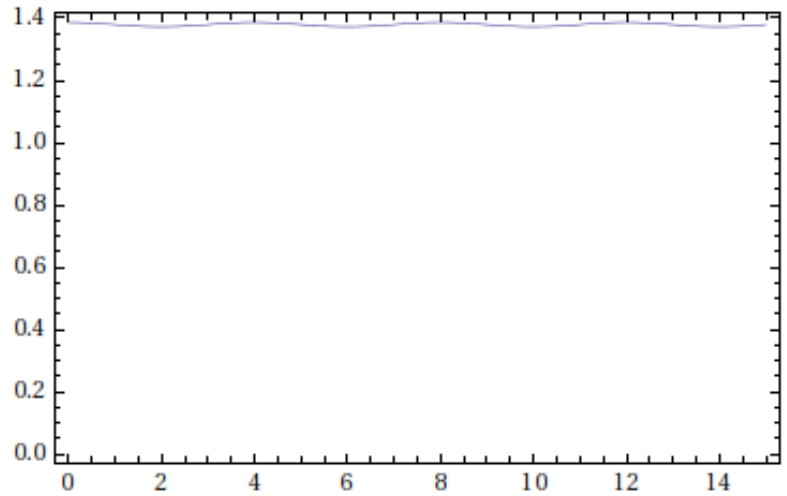

Figure : Sum of Gaussian measures, $\sigma = 2.2$

How flat the sum of Gaussian measures is ?

Sum of Gaussian measures

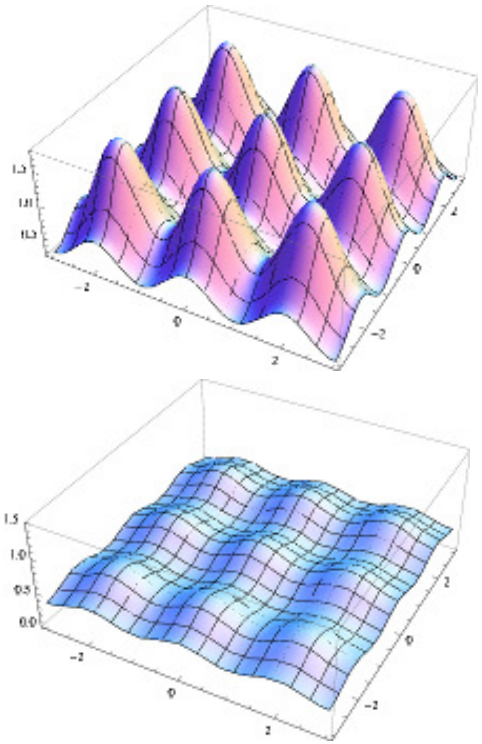

Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

How flat the sum of Gaussian measures is ?

Sum of Gaussian measures

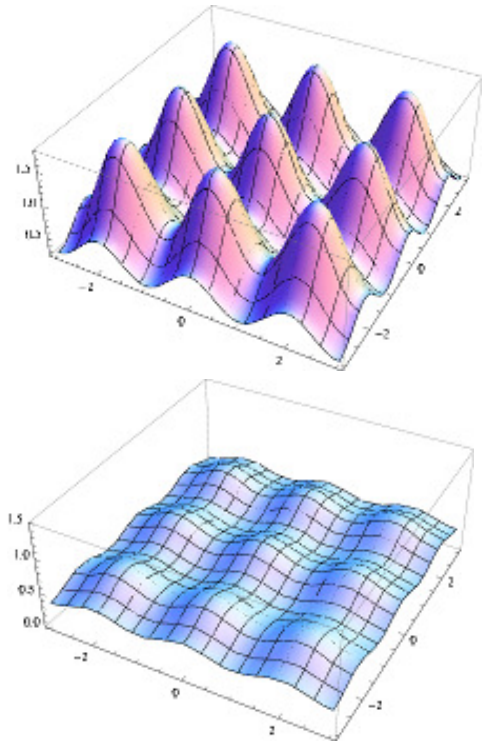

Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

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

How flat the sum of Gaussian measures is ?

Sum of Gaussian measures

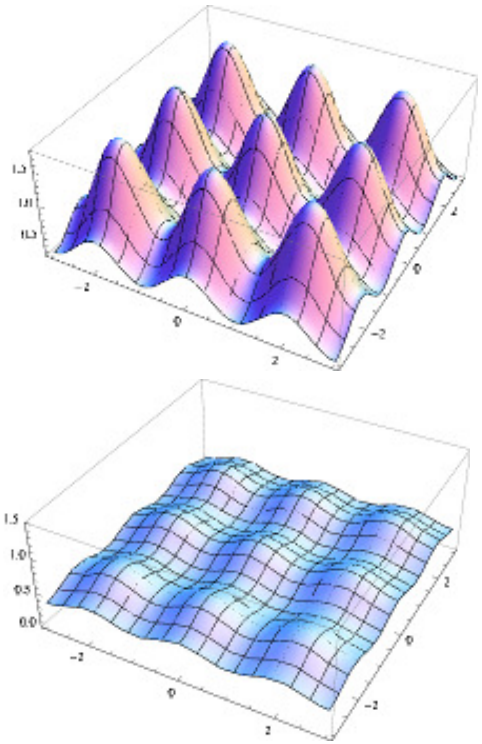

Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

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

Flatness factor ($L_\infty-$distance w.r.t. uniform)

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

How flat the sum of Gaussian measures is ?

Sum of Gaussian measures

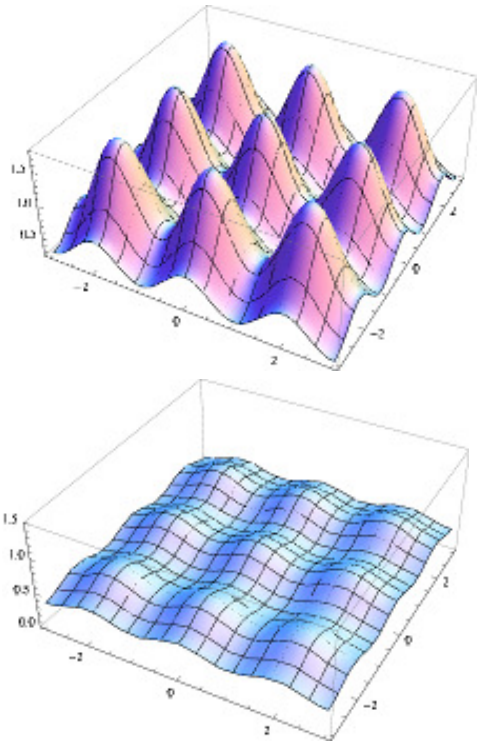

Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

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

Flatness factor ($L_\infty-$distance w.r.t. uniform)

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

The flatness factor can be computed

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

Theta Series again

Definition

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

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

Theta Series again

Definition

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

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

Union Bound

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*.

Theta Series again

Definition

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

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

Union Bound

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*.

Full Theta series needed

For ...

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

Outline

Gaussian Wiretap Channel

Flatness Factor

Information Leakage [Ling & al., 14]

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

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

where

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

is the *flatness factor* of the lattice Λ_e.

Gaussian Wiretap Channel — Flatness Factor

Information Leakage [Ling & al., 14]

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

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

where

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

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,

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

Discrete Gaussian Sampling on Λ

Illustration

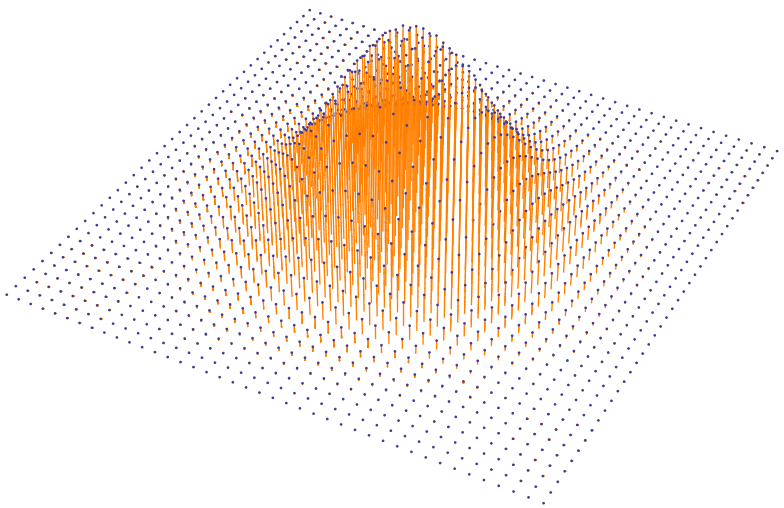

Figure : Discrete Gaussian Sampling on $\Lambda = \mathbb{Z}^2$

Discrete Gaussian Sampling on Λ

Illustration

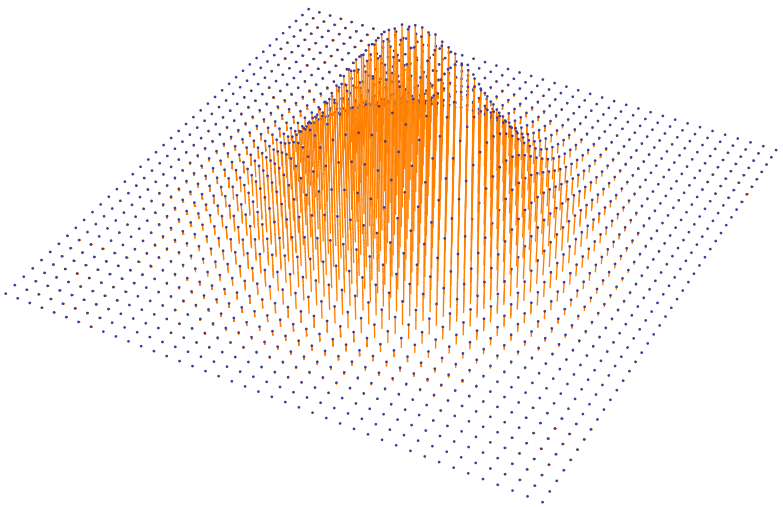

Figure : Discrete Gaussian Sampling on $\Lambda = \mathbb{Z}^2$

Lattice sampling

Sample a lattice point $\mathbf{x}$ with probability

$$\frac{e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}}}{\sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\boldsymbol{\lambda}\|^2}{2\sigma^2}}}$$

Discrete Gaussian Sampling on Λ

Illustration

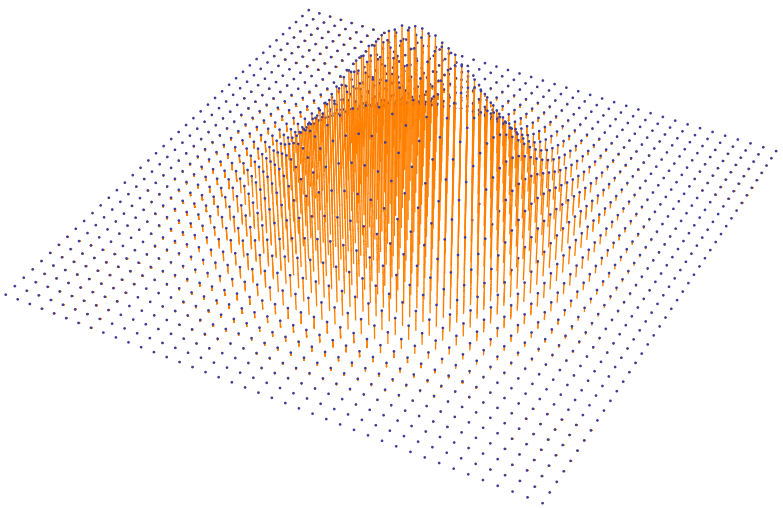

Figure : Discrete Gaussian Sampling on $\Lambda = \mathbb{Z}^2$

Lattice sampling

Sample a lattice point $\mathbf{x}$ with probability

$$\frac{e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}}}{\sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\boldsymbol{\lambda}\|^2}{2\sigma^2}}}$$

Universal algorithms

Universal algorithms (e.g. the Metropolis-Hastings-Klein algorithm) are very slow. Necessity of deriving more specialized ones.

Discrete Gaussian Sampling on Λ

Illustration

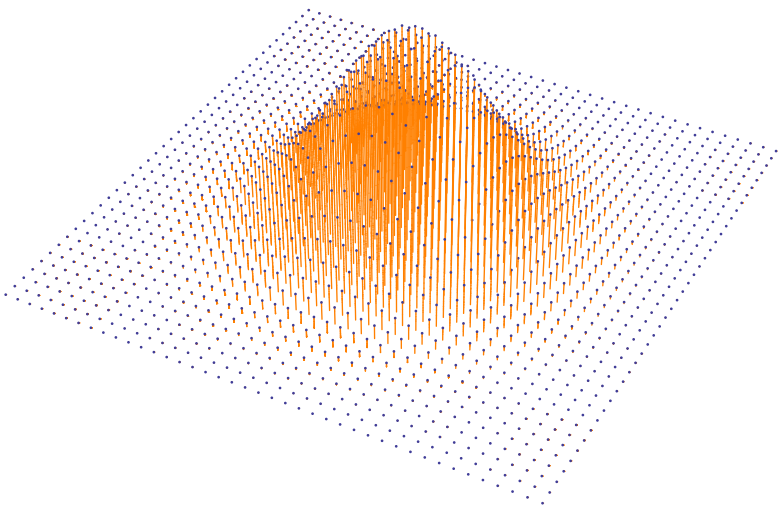

Figure : Discrete Gaussian Sampling on $\Lambda = \mathbb{Z}^2$

Lattice sampling

Sample a lattice point $\mathbf{x}$ with probability

$$\frac{e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}}}{\sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\boldsymbol{\lambda}\|^2}{2\sigma^2}}}$$

Universal algorithms

Universal algorithms (e.g. the Metropolis-Hastings-Klein algorithm) are very slow. Necessity of deriving more specialized ones.

Applications

- Towards discrete Gaussian shaping
- Lattice decoding
- Lattice crypto

Sampling A_2

Sampling of $\mathbb{Z}$

Use method of [Brakerski & al., 13].
Probabilistic sampler for $\alpha\mathbb{Z} + a$ by using a sampler over the real Gaussian distribution and a rejection algorithm : $\mathcal{S}_{\alpha\mathbb{Z}+a}$

Construction of A_2

We use construction,

$$A_2 = \left(\mathbb{Z} \oplus \sqrt{3}\mathbb{Z}\right) \cup \left(\left(\mathbb{Z} + \frac{1}{2}\right) \oplus \sqrt{3}\left(\mathbb{Z} + \frac{1}{2}\right)\right)$$

Sampling A_2

Sampling of $\mathbb{Z}$

Use method of [Brakerski & al., 13].
Probabilistic sampler for $\alpha\mathbb{Z} + a$ by using a sampler over the real Gaussian distribution and a rejection algorithm : $\mathcal{S}_{\alpha\mathbb{Z}+a}$

Construction of A_2

We use construction,

$$A_2 = \left(\mathbb{Z} \oplus \sqrt{3}\mathbb{Z}\right) \cup \left(\left(\mathbb{Z} + \frac{1}{2}\right) \oplus \sqrt{3}\left(\mathbb{Z} + \frac{1}{2}\right)\right)$$

Probabilities of cosets

Coset $C_0 = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z}$ has probability,

$$p_0 = \frac{\Theta_{C_0}(q)}{\Theta_{A_2}(q)} = \frac{\vartheta_3(q)\,\vartheta_3(q^3)}{\vartheta_3(q)\,\vartheta_3(q^3) + \vartheta_2(q)\,\vartheta_2(q^3)}$$

while coset $C_1 = \left(\left(\mathbb{Z} + \frac{1}{2}\right) \oplus \left(\sqrt{3}\mathbb{Z} + \frac{1}{2}\right)\right)$ has probability

$$p_1 = \frac{\vartheta_2(q)\,\vartheta_2(q^3)}{\vartheta_3(q)\,\vartheta_3(q^3) + \vartheta_2(q)\,\vartheta_2(q^3)}$$

evaluated at $q = e^{-\frac{1}{2\pi\sigma^2}}$.

Sampling A_2

Sampling of $\mathbb{Z}$

Use method of [Brakerski & al., 13].
Probabilistic sampler for $\alpha\mathbb{Z}+a$ by using a sampler over the real Gaussian distribution and a rejection algorithm : $\mathcal{S}_{\alpha\mathbb{Z}+a}$

Construction of A_2

We use construction,

$$A_2 = \left(\mathbb{Z} \oplus \sqrt{3}\mathbb{Z}\right) \cup \left(\left(\mathbb{Z}+\frac{1}{2}\right) \oplus \sqrt{3}\left(\mathbb{Z}+\frac{1}{2}\right)\right)$$

Probabilities of cosets

Coset $C_0 = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z}$ has probability,

$$p_0 = \frac{\Theta_{C_0}(q)}{\Theta_{A_2}(q)} = \frac{\vartheta_3(q)\,\vartheta_3(q^3)}{\vartheta_3(q)\,\vartheta_3(q^3) + \vartheta_2(q)\,\vartheta_2(q^3)}$$

while coset $C_1 = \left(\left(\mathbb{Z}+\frac{1}{2}\right) \oplus \left(\sqrt{3}\mathbb{Z}+\frac{1}{2}\right)\right)$ has probability

$$p_1 = \frac{\vartheta_2(q)\,\vartheta_2(q^3)}{\vartheta_3(q)\,\vartheta_3(q^3) + \vartheta_2(q)\,\vartheta_2(q^3)}$$

evaluated at $q = e^{-\frac{1}{2\pi\sigma^2}}$.

Algorithm

1. Choose C_0 or C_1 with probability p_0 or p_1.
2. Use sampler $\mathcal{S}_{\mathbb{Z}}$ if C_0 or $\mathcal{S}_{\mathbb{Z}+\frac{1}{2}}$ if C_1.
3. Use sampler $\mathcal{S}_{\sqrt{3}\mathbb{Z}}$ if C_0 or $\mathcal{S}_{\sqrt{3}\mathbb{Z}+\frac{\sqrt{3}}{2}}$ if C_1.

Discrete Gaussian Shaping

Rate and Power

Lattice Code

Instead of using two nested lattices (coding + shaping), use only one lattice. Each point is sampled according to Gaussian discrete probability.

Discrete Gaussian Shaping

Rate and Power

Lattice Code

Instead of using two nested lattices (coding + shaping), use only one lattice. Each point is sampled according to Gaussian discrete probability.

Lattice Gaussian Coding achieves the capacity of the Gaussian Channel

Mutual information when using a Lattice Gaussian Code is [Ling & B., 13]

$$I_D \geq \frac{1}{2}\log\left(1+SNR\right) - \frac{6\varepsilon}{n}$$

where ε is related to the flatness factor of the lattice.

Discrete Gaussian Shaping

Rate and Power

Lattice Code

Instead of using two nested lattices (coding + shaping), use only one lattice. Each point is sampled according to Gaussian discrete probability.

Power

The power of the lattice code is

$$P = \frac{1}{n\pi} \frac{\Theta'_\Lambda(y)}{\Theta_\Lambda(y)}$$

evaluated at $y = \frac{1}{2\pi\sigma^2}$.

Lattice Gaussian Coding achieves the capacity of the Gaussian Channel

Mutual information when using a Lattice Gaussian Code is [Ling & B., 13]

$$I_D \geq \frac{1}{2}\log(1+SNR) - \frac{6\varepsilon}{n}$$

where ε is related to the flatness factor of the lattice.

Discrete Gaussian Shaping

Rate and Power

Lattice Code

Instead of using two nested lattices (coding + shaping), use only one lattice. Each point is sampled according to Gaussian discrete probability.

Power

The power of the lattice code is

$$P = \frac{1}{n\pi} \frac{\Theta'_\Lambda(y)}{\Theta_\Lambda(y)}$$

evaluated at $y = \frac{1}{2\pi\sigma^2}$.

Lattice Gaussian Coding achieves the capacity of the Gaussian Channel

Mutual information when using a Lattice Gaussian Code is [Ling & B., 13]

$$I_D \geq \frac{1}{2}\log(1+SNR) - \frac{6\varepsilon}{n}$$

where ε is related to the flatness factor of the lattice.

Rate of the code

The rate (entropy) is,

$$R = \frac{1}{n}\left(\frac{1}{\pi}\frac{\Theta'_\Lambda(y)}{\Theta_\Lambda(y)} + \log\Theta_\Lambda(y)\right)$$

evaluated at $y = \frac{1}{2\pi\sigma^2}$.

Outline

Unimodular lattices

Definition

A lattice Λ of rank n is *unimodular* if

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

Unimodular lattices

Definition

A lattice Λ of rank n is *unimodular* if

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

Examples

$\mathbb{Z}^n$ is unimodular, E_8 and Λ_{24} (Leech lattice) 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*,

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

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*,

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

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, $M_k\left(SL_2\left(\mathbb{Z}\right)\right)$ 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, $M_k\left(SL_2\left(\mathbb{Z}\right)\right)$ 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

Jacobi theta functions

Define

$$\vartheta_3(q) = \sum_{k=-\infty}^{+\infty} q^{k^2} = \Theta_{\mathbb{Z}}(q)$$

$$\vartheta_2(q) = \sum_{k=-\infty}^{+\infty} q^{(k+\frac{1}{2})^2} = \Theta_{\mathbb{Z}+\frac{1}{2}}(q)$$

and consider construction A,

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

We get

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

Theta series of E_8: A Coding approach

Jacobi theta functions

Define

$$\vartheta_3(q) = \sum_{k=-\infty}^{+\infty} q^{k^2} = \Theta_{\mathbb{Z}}(q)$$

$$\vartheta_2(q) = \sum_{k=-\infty}^{+\infty} q^{(k+\frac{1}{2})^2} = \Theta_{\mathbb{Z}+\frac{1}{2}}(q)$$

and consider construction A,

$$\Lambda = 2\mathbb{Z}^8 + \mathcal{C}(8,4)_{\mathbb{F}_2} = \bigcup_{\mathbf{x}\in\mathcal{C}} (2\mathbb{Z}^8 + \mathbf{x})$$

We get

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

Cosets

We have

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

and more generally,

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

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

Theta series of E_8: A Coding approach

Jacobi theta functions

Define

$$\vartheta_3(q) = \sum_{k=-\infty}^{+\infty} q^{k^2} = \Theta_{\mathbb{Z}}(q)$$

$$\vartheta_2(q) = \sum_{k=-\infty}^{+\infty} q^{(k+\frac{1}{2})^2} = \Theta_{\mathbb{Z}+\frac{1}{2}}(q)$$

and consider construction A,

$$\Lambda = 2\mathbb{Z}^8 + \mathcal{C}(8,4)_{\mathbb{F}_2} = \bigcup_{\mathbf{x}\in\mathcal{C}} (2\mathbb{Z}^8 + \mathbf{x})$$

We get

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

Cosets

We have

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

and more generally,

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

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

E_8 again

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

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

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

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

is the Ramanujan form (of weight 12).

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

$$\Theta_\Lambda = E_4^{3m+k}+\sum_{j=1}^{m}a_jE_4^{3(m-j)+k}\Delta_{24}^j$$

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

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

is the Ramanujan form (of weight 12).

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

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

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

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

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).

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

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

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.

$\ell-$modular lattices

Definition

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

- Λ is integral, i.e. its *Gram* matrix $\mathbf{B} = \mathbf{A}^\top \cdot \mathbf{A} \in GL_n(\mathbb{Z})$.
- There exists a similarity φ (isometry + scaling) of similarity factor equal to ℓ such that
$$\varphi(\Lambda^\star) = \Lambda \text{ and } \langle \varphi(\mathbf{x}), \varphi(\mathbf{x}) \rangle = \ell \langle \mathbf{x}, \mathbf{y} \rangle, \ \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n.$$
- 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 $\mathbf{B} = \mathbf{A}^\top \cdot \mathbf{A} \in GL_n(\mathbb{Z})$.
- There exists a similarity φ (isometry + scaling) of similarity factor equal to ℓ such that
$$\varphi(\Lambda^\star) = \Lambda \text{ and } \langle \varphi(\mathbf{x}), \varphi(\mathbf{x}) \rangle = \ell \langle \mathbf{x}, \mathbf{y} \rangle, \ \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n.$$
- 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

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

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

$\eta(q) = q^{\frac{1}{24}} \prod_{j=1}^{\infty}(1-q^j)$ 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

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

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

$\eta(q) = q^{\frac{1}{24}} \prod_{j=1}^{\infty}(1-q^j)$ 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

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

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

$\eta(q) = q^{\frac{1}{24}} \prod_{j=1}^{\infty}(1-q^j)$ 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)

$\ell-$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

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

Example: $\ell = 3$

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

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

$\ell-$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

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

Example: $\ell = 3$

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

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

Coxeter Todd K_{12}

We get

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

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

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

Example: $\ell = 3$

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

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

Coxeter Todd K_{12}

We get

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

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,

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

Modular lattices $\ell = 3$

Construction A

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

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

gives an Hermitian $\mathbb{Z}[\zeta]-$lattice. Its trace lattice is a $\mathbb{Z}-$lattice which is $3-$modular when $\mathcal{C}$ 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.

$\mathbb{F}_4$	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

Modular lattices $\ell = 3$

Construction A

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

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

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

Construction of K_{12}

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

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

is equivalent to K_{12}.

Mapping

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

$\mathbb{F}_4$	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

Modular lattices $\ell = 3$

Construction A

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

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

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

Construction of K_{12}

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

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

is equivalent to K_{12}.

Mapping

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

$\mathbb{F}_4$	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

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

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

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 enumerator is

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

Cosets theta series

- Coset 0 has theta series

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

- Other cosets have theta series

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

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 enumerator is

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

Cosets theta series

- Coset 0 has theta series

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

- Other cosets have theta series

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

Theta series

We get

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

$\ell-$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

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

Example: $\ell = 7$

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

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

$\ell-$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 $k \in \{0, 1, 2\}$;

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

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 $k \in \{0, 1, 2\}$;

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

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,

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

Modular lattices $\ell = 7$

Construction A

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

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

gives an Hermitian $\mathbb{Z}[\alpha]-$lattice. Its trace lattice is a $\mathbb{Z}-$lattice which is $7-$modular when $\mathcal{C}$ 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 A

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

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

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

Construction of P_6

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

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

is equivalent to P_6.

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

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.

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

Conclusion

- The importance of theta series in Communications is increasing.
- Need of better understanding of theta series.