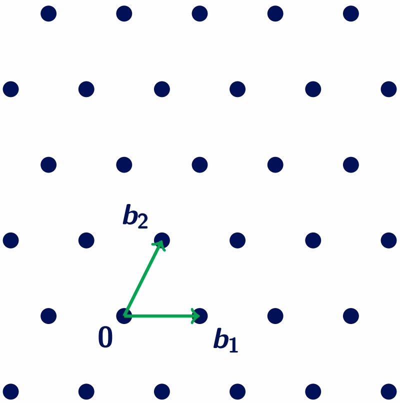
On the existence of good lattice packings and smoothing within a fixed genus

Wessel van Woerden (Université de Bordeaux, IMB, Inria).

université de BORDEAUX

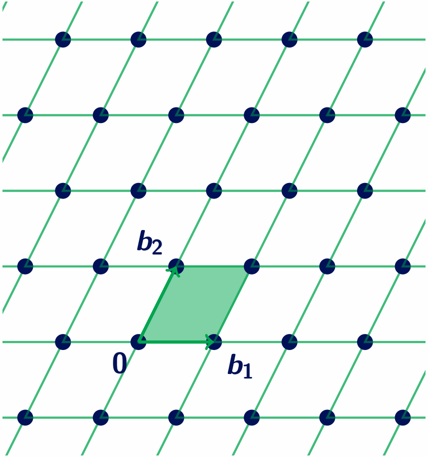


Lattice

$\mathbb{R}$-linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$

$$\mathcal{L}(B) := \{\sum_i x_i b_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n,$$

basis B, gram matrix $G := B^\top B$



Lattice

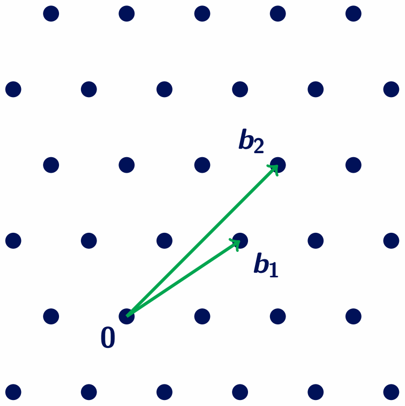
$\mathbb{R}$-linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$

$$\mathcal{L}(B) := \{\textstyle\sum_i x_i b_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n,$$

basis B, gram matrix $G := B^\top B$

Lattice volume

$$\det(\mathcal{L}) := \mathrm{vol}(\mathbb{R}^n/\mathcal{L}) = |\det(B)|$$



Lattice

$\mathbb{R}$-linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$

$$\mathcal{L}(B) := \{\sum_i x_i b_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n,$$

basis B, gram matrix $G := B^\top B$

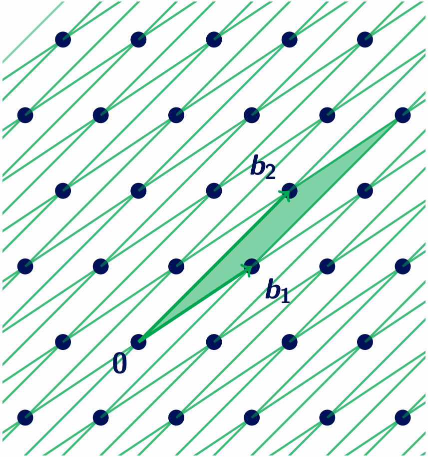
Lattice volume

$$\det(\mathcal{L}) := \mathrm{vol}(\mathbb{R}^n/\mathcal{L}) = |\det(B)|$$

Infinitely many distinct bases

$$B' = B \cdot U, \quad G' = U^\top G U,$$

for $U \in \mathcal{GL}_n(\mathbb{Z})$.



Lattice

$\mathbb{R}$-linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$

$$\mathcal{L}(B) := \{\textstyle\sum_i x_i b_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n,$$

basis B, gram matrix $G := B^\top B$

Lattice volume

$$\det(\mathcal{L}) := \mathrm{vol}(\mathbb{R}^n/\mathcal{L}) = |\det(B)|$$

Infinitely many distinct bases

$$B' = B \cdot U, \quad G' = U^\top G U,$$

for $U \in \mathcal{GL}_n(\mathbb{Z})$.

Random lattices

- Random lattices are useful in cryptography

Random lattices

- Random lattices are useful in cryptography
- But there are many different notions of randomness

Random lattices

- Random lattices are useful in cryptography
- But there are many different notions of randomness

Random lattices

- Random lattices are useful in cryptography
- But there are many different notions of randomness

Definition: random q-ary lattices

$q \geq 2, 0 < n < m$, let $A \leftarrow \mathcal{U}(\mathbb{Z}^{m\times n})$ and consider $\mathcal{L} = A\mathbb{Z}^n + q\mathbb{Z}^m \subset \mathbb{Z}^m$.

Random lattices

- Random lattices are useful in cryptography
- But there are many different notions of randomness

Definition: random q-ary lattices

$q \geq 2, 0 < n < m$, let $A \leftarrow \mathcal{U}(\mathbb{Z}^{m \times n})$ and consider $\mathcal{L} = A\mathbb{Z}^n + q\mathbb{Z}^m \subset \mathbb{Z}^m$.

- LWE, SIS
- allows for worst-case to average-case reduction

Random lattices

- Random lattices are useful in cryptography
- But there are many different notions of randomness

Definition: random q-ary lattices

$q \geq 2, 0 < n < m$, let $A \leftarrow \mathcal{U}(\mathbb{Z}^{m\times n})$ and consider $\mathcal{L} = A\mathbb{Z}^n + q\mathbb{Z}^m \subset \mathbb{Z}^m$.

- LWE, SIS
- allows for worst-case to average-case reduction

Definition (Siegel 1945): Haar measure

The Haar measure on $\mathcal{SL}_n(\mathbb{R})$ has finite mass on the quotient space of unit volume lattices $\mathcal{SL}_n(\mathbb{R})/\mathcal{SL}_n(\mathbb{Z})$.

- Random lattices are useful in cryptography
- But there are many different notions of randomness

Definition: random q-ary lattices

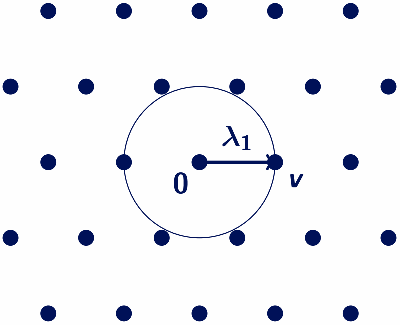
$q \geq 2, 0 < n < m$, let $A \leftarrow \mathcal{U}(\mathbb{Z}^{m\times n})$ and consider $\mathcal{L} = A\mathbb{Z}^n + q\mathbb{Z}^m \subset \mathbb{Z}^m$.

- LWE, SIS
- allows for worst-case to average-case reduction

Definition (Siegel 1945): Haar measure

The Haar measure on $\mathcal{SL}_n(\mathbb{R})$ has finite mass on the quotient space of unit volume lattices $\mathcal{SL}_n(\mathbb{R})/\mathcal{SL}_n(\mathbb{Z})$.

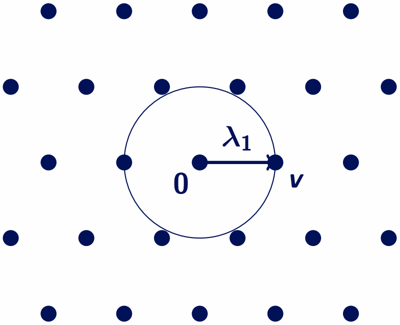
- Mathematically elegant and useful for certain proofs



First minimum & theta series

$$\lambda_1(\mathcal{L}) := \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|_2$$

$$\theta_{\mathcal{L}}(q) := \sum_{x \in \mathcal{L}} q^{\|x\|^2} = 1 + N_{\lambda_1} q^{\lambda_1^2} + \dots$$



First minimum & theta series

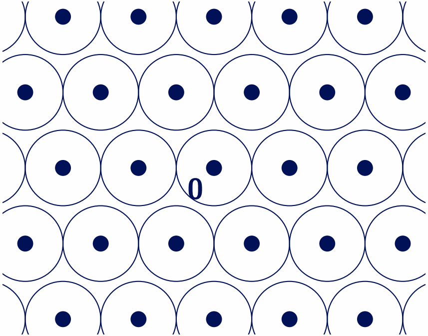
$$\lambda_1(\mathcal{L}) := \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|_2$$

$$\theta_{\mathcal{L}}(q) := \sum_{x \in \mathcal{L}} q^{\|x\|^2} = 1 + N_{\lambda_1} q^{\lambda_1^2} + \dots$$

Minkowski's Theorem

$$\lambda_1(\mathcal{L}) \leq \underbrace{2 \frac{\det(\mathcal{L})^{1/n}}{\mathtt{vol}(\mathcal{B}^n)^{1/n}}}_{\mathsf{Mk}(\mathcal{L})} \approx \sqrt{2n/\pi e}\, \det(\mathcal{L})^{1/n}$$

First minimum



First minimum & theta series

$$\lambda_1(\mathcal{L}) := \min_{x \in \mathcal{L}\setminus\{0\}} \|x\|_2$$

$$\theta_{\mathcal{L}}(q) := \sum_{x\in\mathcal{L}} q^{\|x\|^2} = 1 + N_{\lambda_1} q^{\lambda_1^2} + \dots$$

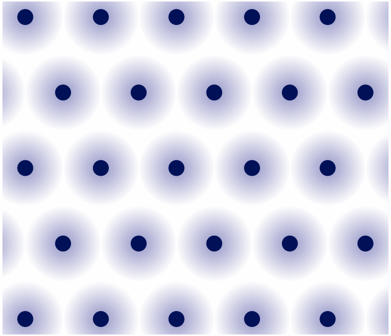
Minkowski's Theorem

$$\lambda_1(\mathcal{L}) \le \underbrace{2\frac{\det(\mathcal{L})^{1/n}}{\mathrm{vol}(\mathcal{B}^n)^{1/n}}}_{\mathsf{Mk}(\mathcal{L})} \approx \sqrt{2n/\pi e}\,\det(\mathcal{L})^{1/n}$$

Minkowski-Hlawka Theorem:

For random lattices $\mathbb{E}[\lambda_1(\mathcal{L})] = \mathsf{gh}(\mathcal{L}) := \frac{1}{2}\mathsf{Mk}(\mathcal{L}) \approx \sqrt{n/2\pi e}\cdot\det(\mathcal{L})^{1/n}$.

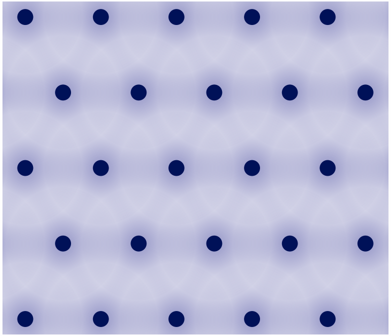
$\Rightarrow$ there exists a lattice with $\lambda_1(\mathcal{L}) \ge \mathsf{gh}(\mathcal{L})$ ($\exists$ good lattice packing)



Smoothing parameter

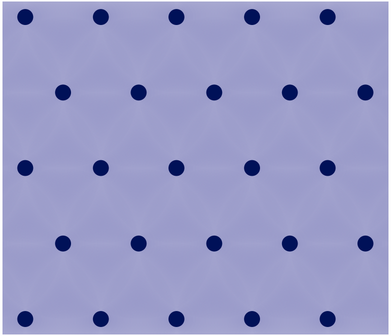
'minimum $s > 0$ such that centered Gaussian with width s is ϵ-close to uniform over $\mathbb{R}^n/\mathcal{L}$'

Smoothing parameter



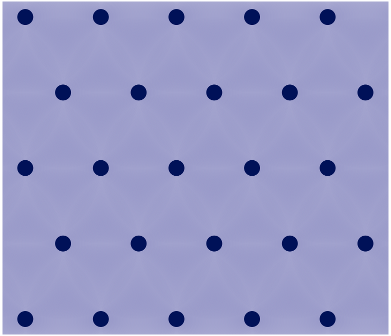
Smoothing parameter

'minimum $s > 0$ such that centered Gaussian with width s is ϵ-close to uniform over $\mathbb{R}^n/\mathcal{L}$'



Smoothing parameter

'minimum $s > 0$ such that centered Gaussian with width s is ϵ-close to uniform over $\mathbb{R}^n/\mathcal{L}$'



Smoothing parameter

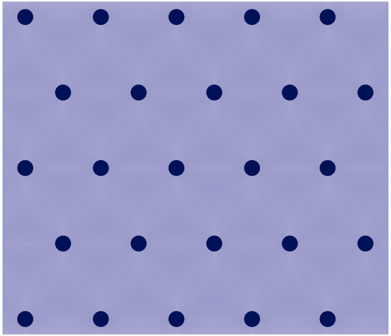
'minimum $s > 0$ such that centered Gaussian with width s is ϵ-close to uniform over $\mathbb{R}^n/\mathcal{L}$'

$$\eta_\varepsilon(\mathcal{L}) = \min\{s > 0 : \theta_{\mathcal{L}^*}(\exp(-\pi s^2)) \leq 1 + \varepsilon\}$$

Dual lattice

$$\mathcal{L}^* := \{y \in \mathbb{R}^n : \forall x \in \mathcal{L}, \langle x, y \rangle \in \mathbb{Z}\}$$

$$\eta_{2^{-n}}(\mathcal{L}) \leq \sqrt{n}/\lambda_1(\mathcal{L}^*)$$



Smoothing parameter

'minimum $s > 0$ such that centered Gaussian with width s is ϵ-close to uniform over $\mathbb{R}^n/\mathcal{L}$'

$$\eta_\varepsilon(\mathcal{L}) = \min\{s > 0 : \theta_{\mathcal{L}^*}(\exp(-\pi s^2)) \leq 1 + \varepsilon\}$$

Dual lattice

$$\mathcal{L}^* := \{y \in \mathbb{R}^n : \forall x \in \mathcal{L}, \langle x, y\rangle \in \mathbb{Z}\}$$

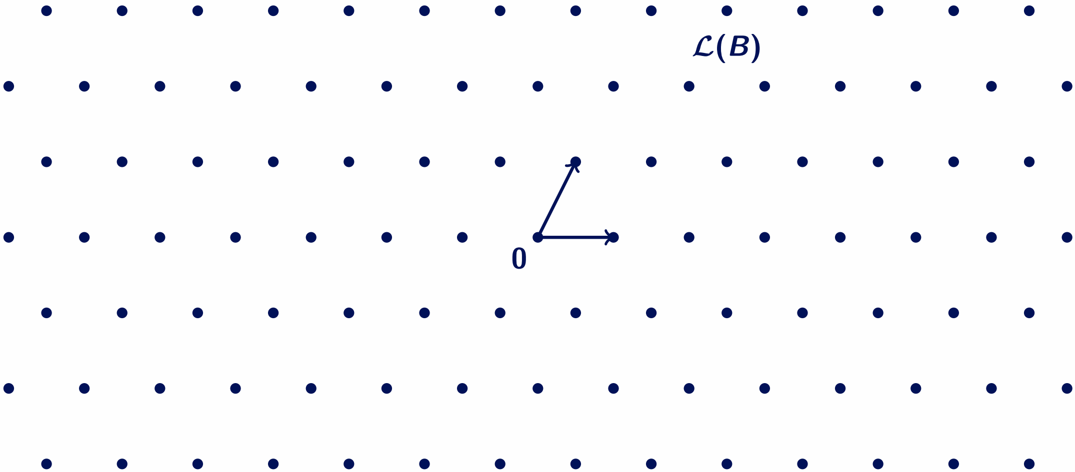
$$\eta_{2^{-n}}(\mathcal{L}) \leq \sqrt{n}/\lambda_1(\mathcal{L}^*)$$

Good smoothing: $\epsilon \in (e^{-n}, 1]$

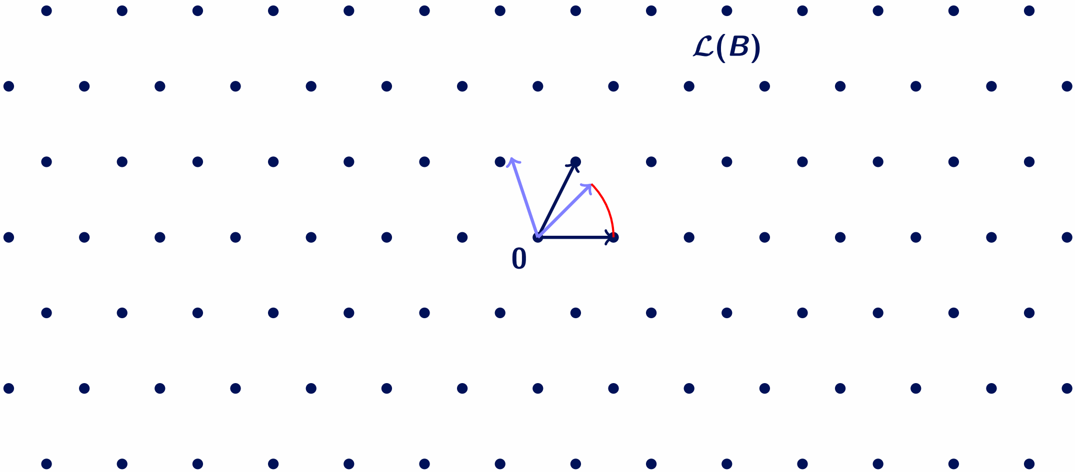
For a random lattice $\mathcal{L}^*$, $\theta_{\mathcal{L}^*}(\exp(-\pi s^2)) \leq 1 + O(ns^{-n}\det(\mathcal{L}))$

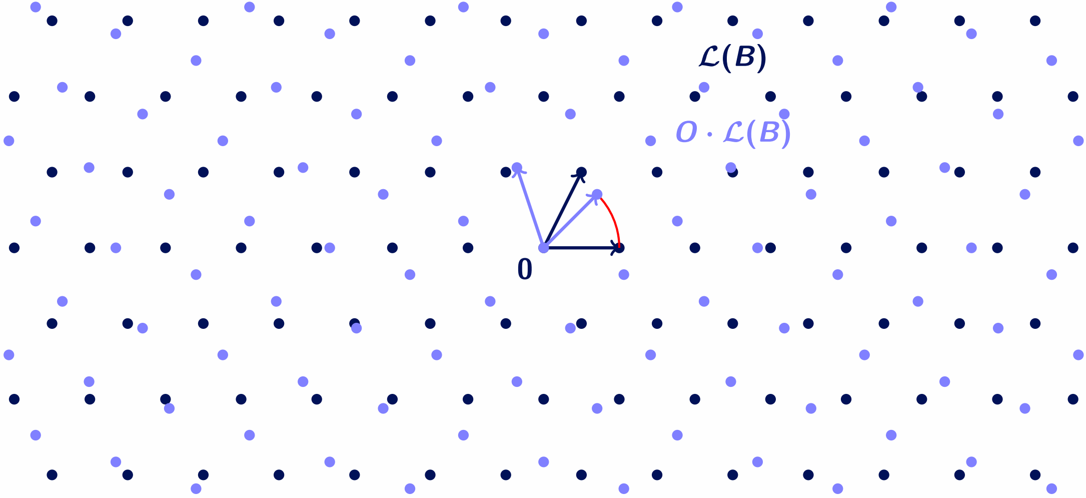
$\Rightarrow$ there exists a lattice with $\eta_\varepsilon(\mathcal{L}) \leq \theta(n\det(\mathcal{L})/\varepsilon)^{1/n}$.

Lattice Isomorphism Problem (LIP)

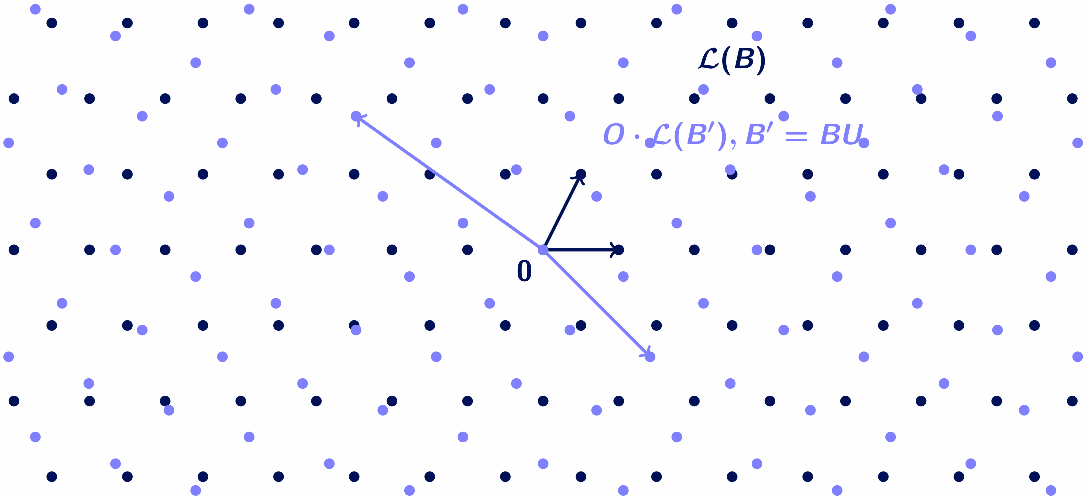


Lattice Isomorphism Problem (LIP)




$\mathcal{L}(B)$
$O \cdot \mathcal{L}(B)$
$\mathbf{0}$

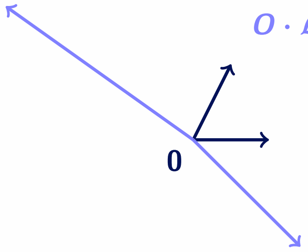
Lattice Isomorphism Problem (LIP)



Lattice Isomorphism Problem (LIP)

$\mathcal{L}(B)$

$O \cdot \mathcal{L}(B'), B' = BU$



$$\mathcal{L}(B_1) \cong \mathcal{L}(B_2)$$

$$\iff$$

$$O \cdot \mathcal{L}(B_1) = \mathcal{L}(B_2) \qquad \text{for some } O \in O_d(\mathbb{R})$$

$$\iff$$

$$O \cdot B_1 \cdot U = B_2 \qquad \text{for some } O \in O_d(\mathbb{R}), U \in \mathrm{GL}_d(\mathbb{Z})$$

Lattice Isomorphism Problem

$$\mathcal{L}(B_1) \cong \mathcal{L}(B_2)$$

$$\iff$$

$$O \cdot \mathcal{L}(B_1) = \mathcal{L}(B_2) \qquad \text{for some } O \in O_d(\mathbb{R})$$

$$\iff$$

$$O \cdot B_1 \cdot U = B_2 \qquad \text{for some } O \in O_d(\mathbb{R}), U \in \mathrm{GL}_d(\mathbb{Z})$$

- If either O or U is trivial: linear algebra.

Lattice Isomorphism Problem

$$\mathcal{L}(B_1) \cong \mathcal{L}(B_2)$$

$$\iff$$

$$O \cdot \mathcal{L}(B_1) = \mathcal{L}(B_2) \qquad \text{for some } O \in O_d(\mathbb{R})$$

$$\iff$$

$$O \cdot B_1 \cdot U = B_2 \qquad \text{for some } O \in O_d(\mathbb{R}), U \in \mathrm{GL}_d(\mathbb{Z})$$

$$\iff$$

$$U^t B_1^t B_1 U = B_2^t B_2 \qquad \text{for some } U \in \mathrm{GL}_d(\mathbb{Z})$$

- If either O or U is trivial: linear algebra.
- Use $O^t O = I$ to remove the orthonormal transformation.

Lattice Isomorphism Problem

$$\mathcal{L}(B_1) \cong \mathcal{L}(B_2)$$

$$\iff$$

$$O \cdot \mathcal{L}(B_1) = \mathcal{L}(B_2) \qquad \text{for some } O \in O_d(\mathbb{R})$$

$$\iff$$

$$O \cdot B_1 \cdot U = B_2 \qquad \text{for some } O \in O_d(\mathbb{R}), U \in \mathrm{GL}_d(\mathbb{Z})$$

$$\iff$$

$$U^t B_1^t B_1 U = B_2^t B_2 \qquad \text{for some } U \in \mathrm{GL}_d(\mathbb{Z})$$

- If either O or U is trivial: linear algebra.
- Use $O^t O = I$ to remove the orthonormal transformation.
- Restrict to integral or rational gram matrices

Cryptography from LIP

- LIP as a new hardness assumption

Cryptography from LIP

- LIP as a new hardness assumption

Ducas & vW: On LIP, QFs, Remarkable Lattices, and Cryptography

Use LIP to hide a remarkable lattice:

- Identification, Encryption and Signature scheme

Cryptography from LIP

- LIP as a new hardness assumption

Ducas & vW: On LIP, QFs, Remarkable Lattices, and Cryptography

Use LIP to hide a remarkable lattice:

- Identification, Encryption and Signature scheme

Bennett et al.: Just how hard are rotations of $\mathbb{Z}^n$?

- Encryption scheme based on LIP on $\mathbb{Z}^n$,

Cryptography from LIP

- LIP as a new hardness assumption

Ducas & vW: On LIP, QFs, Remarkable Lattices, and Cryptography

Use LIP to hide a remarkable lattice:

- Identification, Encryption and Signature scheme

Bennett et al.: Just how hard are rotations of $\mathbb{Z}^n$?

- Encryption scheme based on LIP on $\mathbb{Z}^n$,

Ducas et al.: HAWK scheme

Efficient signature scheme based on module-LIP on $\mathbb{Z}^n$

- submitted to NIST call for additional signatures

- Several others works using LIP appeared recently

Distinghuish LIP

Definition: distinguish LIP ($\boldsymbol{\Delta}$-LIP)

Let $\mathcal{L}_1, \mathcal{L}_2$ be two non-isomorphic lattices and let $\boldsymbol{b} \leftarrow \{1, 2\}$ uniform.
Given $\mathcal{L} \in [\mathcal{L}_{\boldsymbol{b}}]$, recover $\boldsymbol{b}$.

Distinghuish LIP

Definition: distinguish LIP ($\mathbf{\Delta}$-LIP)

Let $\mathcal{L}_1, \mathcal{L}_2$ be two non-isomorphic lattices and let $b \leftarrow \{1, 2\}$ uniform.
Given $\mathcal{L} \in [\mathcal{L}_b]$, recover b.

- $\mathcal{L}_1, \mathcal{L}_2$ can be represented by any (good) gram matrix G_1, G_2.
- $\mathcal{L}$ is represented by a random $U^\top G_b U \leftarrow \mathcal{D}([G_b])$ (worst-case)

Distinghuish LIP

Definition: distinguish LIP (Δ-LIP)

Let $\mathcal{L}_1, \mathcal{L}_2$ be two non-isomorphic lattices and let $b \leftarrow \{1, 2\}$ uniform.
Given $\mathcal{L} \in [\mathcal{L}_b]$, recover b.

- $\mathcal{L}_1, \mathcal{L}_2$ can be represented by any (good) gram matrix G_1, G_2.
- $\mathcal{L}$ is represented by a random $U^\top G_b U \leftarrow \mathcal{D}([G_b])$ (worst-case)

Usual security assumption:

Given:

1. some remarkable lattice $\mathcal{L}_1$
2. an auxiliary lattice $\mathcal{L}_2$ with certain (good) geometric properties

Then: cryptographic scheme is secure if Δ-LIP on $\mathcal{L}_1, \mathcal{L}_2$ is hard.

Distinghuish LIP

Definition: distinguish LIP (Δ-LIP)

Let $\mathcal{L}_1, \mathcal{L}_2$ be two non-isomorphic lattices and let $b \leftarrow \{1, 2\}$ uniform.
Given $\mathcal{L} \in [\mathcal{L}_b]$, recover b.

- $\mathcal{L}_1, \mathcal{L}_2$ can be represented by any (good) gram matrix G_1, G_2.
- $\mathcal{L}$ is represented by a random $U^\top G_b U \leftarrow \mathcal{D}([G_b])$ (worst-case)

Usual security assumption:

Given:

1. some remarkable lattice $\mathcal{L}_1$
2. an auxiliary lattice $\mathcal{L}_2$ with certain (good) geometric properties

Then: cryptographic scheme is secure if Δ-LIP on $\mathcal{L}_1, \mathcal{L}_2$ is hard.

Goal: find an auxiliary lattice with the right properties

Arithmetic Invariants ($\mathbf{ari}(\mathcal{L})$)

- $\mathbf{det}(\mathcal{L}) = \mathbf{det}(\mathcal{L}_b)$.
- $\mathbf{gcd}(\mathcal{L}) := \mathbf{gcd}\{\langle x, y\rangle : x, y \in \mathcal{L}\}$
- parity $\mathbf{par}(\mathcal{L}) = \mathbf{gcd}\{\|x\|^2 : x \in \mathcal{L}\} / \mathbf{gcd}(\mathcal{L})$

Invariants

Arithmetic Invariants ($\mathbf{ari}(\mathcal{L})$)

- $\mathbf{det}(\mathcal{L}) = \mathbf{det}(\mathcal{L}_b)$.
- $\mathbf{gcd}(\mathcal{L}) := \mathbf{gcd}\{\langle x, y\rangle : x, y \in \mathcal{L}\}$
- parity $\mathbf{par}(\mathcal{L}) = \mathbf{gcd}\{\|x\|^2 : x \in \mathcal{L}\} / \mathbf{gcd}(\mathcal{L})$
- Equivalence over $R \supset \mathbb{Z}$, $U \in \mathrm{GL}_n(R)$, $R \in \{\mathbb{R}, \mathbb{Q}, \forall p\ \mathbb{Q}_p, \underbrace{\forall p\ \mathbb{Z}_p}_{\text{Genus}}\}$

Invariants

Arithmetic Invariants ($\mathsf{ari}(\mathcal{L})$)

- $\det(\mathcal{L}) = \det(\mathcal{L}_b)$.
- $\gcd(\mathcal{L}) := \gcd\{\langle x, y\rangle : x, y \in \mathcal{L}\}$
- parity $\mathsf{par}(\mathcal{L}) = \gcd\{\|x\|^2 : x \in \mathcal{L}\} / \gcd(\mathcal{L})$
- Equivalence over $R \supset \mathbb{Z}$, $U \in \mathrm{GL}_n(R)$, $R \in \{\mathbb{R}, \mathbb{Q}, \underbrace{\forall p\ \mathbb{Q}_p, \forall p\ \mathbb{Z}_p}_{\text{Genus}}\}$

Lemma:

If $\mathsf{ari}(Q_0) \neq \mathsf{ari}(Q_1)$, then $\Delta\,\mathsf{LIP}^{Q_0,Q_1}$ can be solved efficiently.

Arithmetic Invariants ($\mathrm{ari}(\mathcal{L})$)

- $\det(\mathcal{L}) = \det(\mathcal{L}_b)$.
- $\gcd(\mathcal{L}) := \gcd\{\langle x, y\rangle : x, y \in \mathcal{L}\}$
- parity $\mathrm{par}(\mathcal{L}) = \gcd\{\|x\|^2 : x \in \mathcal{L}\} / \gcd(\mathcal{L})$
- Equivalence over $R \supset \mathbb{Z}$, $U \in \mathrm{GL}_n(R)$, $R \in \{\mathbb{R}, \mathbb{Q}, \forall p\ \mathbb{Q}_p, \underbrace{\forall p\ \mathbb{Z}_p}_{\text{Genus}}\}$

Lemma:

If $\mathrm{ari}(Q_0) \neq \mathrm{ari}(Q_1)$, then $\Delta\,\mathrm{LIP}^{Q_0, Q_1}$ can be solved efficiently.

$\Rightarrow$ auxiliary lattice must have same invariants

Genus

p-adic integers:

For a prime p the p-adic integers $\mathbb{Z}_p$ are given by formal series, i.e.,

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i, \quad \text{with } 0 \leq a_i < p \right\}$$

Genus

p-adic integers:

For a prime p the p-adic integers $\mathbb{Z}_p$ are given by formal series, i.e.,

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i, \quad \text{with } 0 \leq a_i < p \right\}$$

Genus:

The genus $\mathbf{gen}(\mathcal{L})$ of a lattice $\mathcal{L}$ consists of all lattices that are equivalent over $\mathbb{R}$ and over $\mathbb{Z}_p$ for all primes p

Genus

p-adic integers:

For a prime p the p-adic integers $\mathbb{Z}_p$ are given by formal series, i.e.,

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i, \quad \text{with } 0 \leq a_i < p \right\}$$

Genus:

The genus $\mathbf{gen}(\mathcal{L})$ of a lattice $\mathcal{L}$ consists of all lattices that are equivalent over $\mathbb{R}$ and over $\mathbb{Z}_p$ for all primes p

- Equivalent over $\mathbb{R}$ $\Leftrightarrow$ same rank

Genus

p-adic integers:

For a prime p the p-adic integers $\mathbb{Z}_p$ are given by formal series, i.e.,

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i, \quad \text{with } 0 \leq a_i < p \right\}$$

Genus:

The genus $\mathrm{gen}(\mathcal{L})$ of a lattice $\mathcal{L}$ consists of all lattices that are equivalent over $\mathbb{R}$ and over $\mathbb{Z}_p$ for all primes p

- Equivalent over $\mathbb{R}$ $\Leftrightarrow$ same rank
- Equivalent over $\mathbb{Z}_p$ $\Leftrightarrow \mathbb{Z}_p \otimes \mathcal{L}_1 \cong \mathbb{Z}_p \otimes \mathcal{L}_2$
  $\Leftrightarrow U^\top G_1 U = G_2$ for $U \in \mathcal{GL}_n(\mathbb{Z}_p)$.

Genus

p-adic integers:

For a prime p the p-adic integers $\mathbb{Z}_p$ are given by formal series, i.e.,

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i, \quad \text{with } 0 \leq a_i < p \right\}$$

Genus:

The genus $\mathbf{gen}(\mathcal{L})$ of a lattice $\mathcal{L}$ consists of all lattices that are equivalent over $\mathbb{R}$ and over $\mathbb{Z}_p$ for all primes p

- Equivalent over $\mathbb{R}$ $\Leftrightarrow$ same rank
- Equivalent over $\mathbb{Z}_p$ $\Leftrightarrow \mathbb{Z}_p \otimes \mathcal{L}_1 \cong \mathbb{Z}_p \otimes \mathcal{L}_2$
  $\Leftrightarrow U^\top G_1 U = G_2$ for $U \in \mathcal{GL}_n(\mathbb{Z}_p)$.
- Covers all the other known arithmetic invariants

Motivation

Ducas & vW: On LIP, QFs, Remarkable Lattices, and Cryptography

Instantiation blows up geometric gaps from f to $O(f^2)$ or $O(f^3)$. If there exists a lattice $\mathcal{L}_2 \in \mathbf{gen}(\mathcal{L}_1)$ with geometric gaps of $O(1)$ then this reduces to $O(f)$. $(\mathrm{gh}(\mathcal{L})/\lambda_1(\mathcal{L}) = O(1)$ for $\mathcal{L} = \mathcal{L}_2, \mathcal{L}_2^*)$

Ducas & vW: On LIP, QFs, Remarkable Lattices, and Cryptography

Instantiation blows up geometric gaps from f to $O(f^2)$ or $O(f^3)$. If there exists a lattice $\mathcal{L}_2 \in \mathsf{gen}(\mathcal{L}_1)$ with geometric gaps of $O(1)$ then this reduces to $O(f)$. $(\mathrm{gh}(\mathcal{L})/\lambda_1(\mathcal{L}) = O(1)$ for $\mathcal{L} = \mathcal{L}_2, \mathcal{L}_2^*)$

Bennett et al.: Just how hard are rotations of $\mathbb{Z}^n$?

Do there exist lattices in $\mathsf{gen}(\mathbb{Z}^n)$ with $\lambda_1(\mathcal{L}) \geq \Omega(\sqrt{n/\log(n)})$ or with $\eta_\varepsilon(\mathcal{L}) \leq \eta_\varepsilon(\mathbb{Z}^n)/\sqrt{\log(n)} \approx \sqrt{\log(1/\varepsilon)/\log(n)}$ for $\varepsilon < n^{-\omega(1)}$?

Ducas & vW: On LIP, QFs, Remarkable Lattices, and Cryptography

Instantiation blows up geometric gaps from f to $O(f^2)$ or $O(f^3)$. If there exists a lattice $\mathcal{L}_2 \in \mathrm{gen}(\mathcal{L}_1)$ with geometric gaps of $O(1)$ then this reduces to $O(f)$. ($\mathrm{gh}(\mathcal{L})/\lambda_1(\mathcal{L}) = O(1)$ for $\mathcal{L} = \mathcal{L}_2, \mathcal{L}_2^*$)

Bennett et al.: Just how hard are rotations of $\mathbb{Z}^n$?

Do there exist lattices in $\mathrm{gen}(\mathbb{Z}^n)$ with $\lambda_1(\mathcal{L}) \geq \Omega(\sqrt{n/\log(n)})$ or with $\eta_\varepsilon(\mathcal{L}) \leq \eta_\varepsilon(\mathbb{Z}^n)/\sqrt{\log(n)} \approx \sqrt{\log(1/\varepsilon)/\log(n)}$ for $\varepsilon < n^{-\omega(1)}$?

Ackermann, Wallet, et al.: to appear

Conjecture: for $n \geq 85$ there exists at least one $\mathcal{L} \in \mathrm{gen}(\mathbb{Z}^n)$ such that $\lambda_1(\mathcal{L}) \geq \sqrt[4]{72n}$. (needed to instantiate their PKE security proof)

Results (1) - Good (dual) packing

Theorem (good packing): Minkowski-Hlawka theorem for fixed genus

Let $\mathcal{G}$ be any genus of dimension $n \geq 6$ such that $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p. Then there exists a lattice $\mathcal{L}^* \in \mathcal{G}$ with $\lambda_1(\mathcal{L})^2 \geq \lceil \Theta(\omega_n / \det(\mathcal{L}))^{-2/n} \rfloor \approx n/2\pi e \cdot \det(\mathcal{L})^{2/n} = \mathrm{gh}(\mathcal{L})^2$.

Results (1) - Good (dual) packing

Theorem (good packing): Minkowski-Hlawka theorem for fixed genus

Let $\mathcal{G}$ be any genus of dimension $n \geq 6$ such that $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p. Then there exists a lattice $\mathcal{L}^* \in \mathcal{G}$ with $\lambda_1(\mathcal{L})^2 \geq \lceil \Theta(\omega_n / \det(\mathcal{L}))^{-2/n} \rfloor \approx n/2\pi e \cdot \det(\mathcal{L})^{2/n} = \mathrm{gh}(\mathcal{L})^2$.

- Θ can be replaced by a small universal constant
- Essentially matches packing density of a random lattice

Results (1) - Good (dual) packing

Theorem (good packing): Minkowski-Hlawka theorem for fixed genus

Let $\mathcal{G}$ be any genus of dimension $n \geq 6$ such that $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p. Then there exists a lattice $\mathcal{L}^* \in \mathcal{G}$ with $\lambda_1(\mathcal{L})^2 \geq \lceil \Theta(\omega_n / \det(\mathcal{L}))^{-2/n} \rfloor \approx n/2\pi e \cdot \det(\mathcal{L})^{2/n} = \mathrm{gh}(\mathcal{L})^2$.

- Θ can be replaced by a small universal constant
- Essentially matches packing density of a random lattice
- Similar result for simultaneous good primal and dual packing.

Results (1) - Good (dual) packing

Theorem (good packing): Minkowski-Hlawka theorem for fixed genus

Let $\mathcal{G}$ be any genus of dimension $n \geq 6$ such that $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p. Then there exists a lattice $\mathcal{L}^* \in \mathcal{G}$ with $\lambda_1(\mathcal{L})^2 \geq \lceil \Theta(\omega_n / \det(\mathcal{L}))^{-2/n} \rfloor \approx n/2\pi e \cdot \det(\mathcal{L})^{2/n} = \mathrm{gh}(\mathcal{L})^2$.

- Θ can be replaced by a small universal constant
- Essentially matches packing density of a random lattice
- Similar result for simultaneous good primal and dual packing.
- Requirement that $p^{n-5} \nmid \det(\mathcal{G})^2$ can be replaced by a milder but more technical condition. (or removed at a small loss)

Results (2) - Good smoothing

Theorem (good smoothing):

'...' Let $\varepsilon \in [e^{-n}, 1)$, then there exists a lattice $\mathcal{L} \in \mathcal{G}$ with $\eta_\varepsilon(\mathcal{L}^*) \leq \theta(n \det(\mathcal{L}^*)/\varepsilon)^{\frac{1}{n}}$.

Results (2) - Good smoothing

Theorem (good smoothing):

'...' Let $\varepsilon \in [e^{-n}, 1)$, then there exists a lattice $\mathcal{L} \in \mathcal{G}$ with $\eta_\varepsilon(\mathcal{L}^*) \leq \theta(n \det(\mathcal{L}^*)/\varepsilon)^{\frac{1}{n}}$.

- Same conditions as previous result

Results (2) - Good smoothing

Theorem (good smoothing):

'...' Let $\varepsilon \in [e^{-n}, 1)$, then there exists a lattice $\mathcal{L} \in \mathcal{G}$ with $\eta_\varepsilon(\mathcal{L}^*) \leq \theta(n \det(\mathcal{L}^*)/\varepsilon)^{\frac{1}{n}}$.

- Same conditions as previous result
- Essentially matches smoothing of random lattice

Results (2) - Good smoothing

Theorem (good smoothing):

'...' Let $\varepsilon \in [e^{-n}, 1)$, then there exists a lattice $\mathcal{L} \in \mathcal{G}$ with $\eta_\varepsilon(\mathcal{L}^*) \leq \theta(n \det(\mathcal{L}^*)/\varepsilon)^{\frac{1}{n}}$.

- Same conditions as previous result
- Essentially matches smoothing of random lattice
- Works even for constant ε

Results (2) - Good smoothing

Theorem (good smoothing):

'...' Let $\varepsilon \in [e^{-n}, 1)$, then there exists a lattice $\mathcal{L} \in \mathcal{G}$ with $\eta_\varepsilon(\mathcal{L}^*) \leq \theta(n \det(\mathcal{L}^*)/\varepsilon)^{\frac{1}{n}}$.

- Same conditions as previous result
- Essentially matches smoothing of random lattice
- Works even for constant ε
- Also works for $\varepsilon < e^{-n}$ but smoothing for such cases is essentially determined by $\lambda_1(\mathcal{L}^*)$.

The tool: mass formulas (1)

Definition: distribution over Genus

Consider the mass function w given by $w(\mathcal{L}) = 1/|\mathrm{Aut}(\mathcal{L})|$. For a genus $\mathcal{G}$ let $\mathcal{D}(\mathcal{G})$ be the distribution where each isomorphism class $[\mathcal{L}]$ is sampled with relative weight $w(\mathcal{L})$.

The tool: mass formulas (1)

Definition: distribution over Genus

Consider the mass function w given by $w(\mathcal{L}) = 1/|\mathrm{Aut}(\mathcal{L})|$. For a genus $\mathcal{G}$ let $\mathcal{D}(\mathcal{G})$ be the distribution where each isomorphism class $[\mathcal{L}]$ is sampled with relative weight $w(\mathcal{L})$.

Theorem: Smith-Minkowski-Siegel mass formula

Any genus $\mathcal{G}$ contains a finite number of isom. classes and its mass

$$M(\mathcal{G}) := \sum_{[\mathcal{L}] \in \mathcal{G}} w(G),$$

is efficiently computable given the prime factorization of $\det(\mathcal{G})^2$.

Definition: distribution over Genus

Consider the mass function w given by $w(\mathcal{L}) = 1/|\mathrm{Aut}(\mathcal{L})|$. For a genus $\mathcal{G}$ let $\mathcal{D}(\mathcal{G})$ be the distribution where each isomorphism class $[\mathcal{L}]$ is sampled with relative weight $w(\mathcal{L})$.

Theorem: Smith-Minkowski-Siegel mass formula

Any genus $\mathcal{G}$ contains a finite number of isom. classes and its mass

$$M(\mathcal{G}) := \sum_{[\mathcal{L}] \in \mathcal{G}} w(G),$$

is efficiently computable given the prime factorization of $\det(\mathcal{G})^2$.

- $[\mathcal{L}] \in \mathcal{G}$ is sampled from $\mathcal{D}(\mathcal{G})$ with probability $w(\mathcal{L})/M(\mathcal{L})$.

Definition: distribution over Genus

Consider the mass function w given by $w(\mathcal{L}) = 1/|\mathrm{Aut}(\mathcal{L})|$. For a genus $\mathcal{G}$ let $\mathcal{D}(\mathcal{G})$ be the distribution where each isomorphism class $[\mathcal{L}]$ is sampled with relative weight $w(\mathcal{L})$.

Theorem: Smith-Minkowski-Siegel mass formula

Any genus $\mathcal{G}$ contains a finite number of isom. classes and its mass

$$M(\mathcal{G}) := \sum_{[\mathcal{L}]\in\mathcal{G}} w(G),$$

is efficiently computable given the prime factorization of $\det(\mathcal{G})^2$.

- $[\mathcal{L}] \in \mathcal{G}$ is sampled from $\mathcal{D}(\mathcal{G})$ with probability $w(\mathcal{L})/M(\mathcal{L})$.
- Lemma: $|\mathcal{G}| \geq 2M(\mathcal{G})$.

The tool: mass formulas (2)

Definition: average theta series

For a genus $\mathcal{G}$ its average theta series is given by

$$\Theta_{\mathcal{G}}(q) = \mathbb{E}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})}\left[\theta_{\mathcal{L}}(q)\right] = \frac{\sum_{[\mathcal{L}] \in \mathcal{G}} w(\mathcal{L}) \cdot \theta_{\mathcal{L}}(q)}{M(\mathcal{G})}$$

The tool: mass formulas (2)

Definition: average theta series

For a genus $\mathcal{G}$ its average theta series is given by

$$\Theta_{\mathcal{G}}(q) = \mathbb{E}_{[\mathcal{L}]\leftarrow\mathcal{D}(\mathcal{G})}\left[\theta_{\mathcal{L}}(q)\right] = \frac{\sum_{[\mathcal{L}]\in\mathcal{G}} w(\mathcal{L})\cdot\theta_{\mathcal{L}}(q)}{M(\mathcal{G})}$$

Theorem: Siegel-Weil mass formula

The coefficients of $\Theta_{\mathcal{G}}(q)$ can be efficiently computed given the prime factorization of $\det(\mathcal{G})^2$. (polytime in the input and j for q^j)

The tool: mass formulas (2)

Definition: average theta series

For a genus $\mathcal{G}$ its average theta series is given by

$$\Theta_{\mathcal{G}}(q) = \mathbb{E}_{[\mathcal{L}]\leftarrow\mathcal{D}(\mathcal{G})}\left[\theta_{\mathcal{L}}(q)\right] = \frac{\sum_{[\mathcal{L}]\in\mathcal{G}} w(\mathcal{L})\cdot\theta_{\mathcal{L}}(q)}{M(\mathcal{G})}$$

Theorem: Siegel-Weil mass formula

The coefficients of $\Theta_{\mathcal{G}}(q)$ can be efficiently computed given the prime factorization of $\det(\mathcal{G})^2$. (polytime in the input and j for q^j)

- Recall that computing (coeff. of) $\theta_{\mathcal{L}}(q)$ is usually extremely hard

The tool: mass formulas (2)

Definition: average theta series

For a genus $\mathcal{G}$ its average theta series is given by

$$\Theta_{\mathcal{G}}(q) = \mathbb{E}_{[\mathcal{L}]\leftarrow\mathcal{D}(\mathcal{G})}\left[\theta_{\mathcal{L}}(q)\right] = \frac{\sum_{[\mathcal{L}]\in\mathcal{G}} w(\mathcal{L})\cdot\theta_{\mathcal{L}}(q)}{M(\mathcal{G})}$$

Theorem: Siegel-Weil mass formula

The coefficients of $\Theta_{\mathcal{G}}(q)$ can be efficiently computed given the prime factorization of $\det(\mathcal{G})^2$. (polytime in the input and j for q^j)

- Recall that computing (coeff. of) $\theta_{\mathcal{L}}(q)$ is usually extremely hard
- Surprisingly the average is efficient to compute

The tool: mass formulas (2)

Definition: average theta series

For a genus $\mathcal{G}$ its average theta series is given by

$$\Theta_{\mathcal{G}}(q) = \mathbb{E}_{[\mathcal{L}]\leftarrow\mathcal{D}(\mathcal{G})}\left[\theta_{\mathcal{L}}(q)\right] = \frac{\sum_{[\mathcal{L}]\in\mathcal{G}} w(\mathcal{L})\cdot\theta_{\mathcal{L}}(q)}{M(\mathcal{G})}$$

Theorem: Siegel-Weil mass formula

The coefficients of $\Theta_{\mathcal{G}}(q)$ can be efficiently computed given the prime factorization of $\det(\mathcal{G})^2$. (polytime in the input and j for q^j)

- Recall that computing (coeff. of) $\theta_{\mathcal{L}}(q)$ is usually extremely hard
- Surprisingly the average is efficient to compute
- Old but not well known result (by experimental validation)

Example: even unimodular case (1)

Definition: even unimodular lattices

The genus $\mathcal{G}_{n,e}$ of n-dimensional even unimodular lattices consists of all integral lattices of determinant 1 and even parity.

Definition: even unimodular lattices

The genus $\mathcal{G}_{n,e}$ of n-dimensional even unimodular lattices consists of all integral lattices of determinant 1 and even parity.

Lemma: mass formula

For $n = 8k \geq 8$ we have

$$\Theta_{\mathcal{G}_{8k,e}}(q) = E_{4k}(q^2) = 1 + \frac{-8k}{B_{4k}} \sum_{m=1}^{\infty} \sigma_{4k-1}(m) q^{2m},$$

where B_i is the i-th Bernoulli number, and $\sigma_z(m) = \sum_{d|m} d^z$ is the sum of positive divisors function.

Example: even unimodular case (1)

Definition: even unimodular lattices

The genus $\mathcal{G}_{n,e}$ of n-dimensional even unimodular lattices consists of all integral lattices of determinant 1 and even parity.

Lemma: mass formula

For $n = 8k \geq 8$ we have

$$\Theta_{\mathcal{G}_{8k,e}}(q) = E_{4k}(q^2) = 1 + \frac{-8k}{B_{4k}} \sum_{m=1}^{\infty} \sigma_{4k-1}(m) q^{2m},$$

where B_i is the i-th Bernoulli number, and $\sigma_z(m) = \sum_{d|m} d^z$ is the sum of positive divisors function.

- $\mathcal{G}_{8k,e} = \{[E_8]\}$, $\Theta_{\mathcal{G}_{8,e}}(q) = 1 + 240q^2 + 2160q^4 + 6720q^6 + O(q^8)$

Example: even unimodular case (1)

Definition: even unimodular lattices

The genus $\mathcal{G}_{n,e}$ of n-dimensional even unimodular lattices consists of all integral lattices of determinant 1 and even parity.

Lemma: mass formula

For $n = 8k \geq 8$ we have

$$\Theta_{\mathcal{G}_{8k,e}}(q) = E_{4k}(q^2) = 1 + \frac{-8k}{B_{4k}} \sum_{m=1}^{\infty} \sigma_{4k-1}(m) q^{2m},$$

where B_i is the i-th Bernoulli number, and $\sigma_z(m) = \sum_{d|m} d^z$ is the sum of positive divisors function.

- $\mathcal{G}_{8k,e} = \{[E_8]\}$, $\Theta_{\mathcal{G}_{8,e}}(q) = 1 + 240q^2 + 2160q^4 + 6720q^6 + O(q^8)$
- $\Theta_{\mathcal{G}_{128,e}}(q) = 1 + 6.11 \cdot 10^{-37} q^2 + 5.64 \cdot 10^{-18} q^4 + 7.00 \cdot 10^{-7} q^6 + 52.01 q^8 + 6.63 \cdot 10^7 q^{10} + O(q^{12})$

Good packing

- Idea: recall that:

$$\Theta_{\mathcal{G}_{128,e}}(q) = 1 + 6.11 \cdot 10^{-37} q^2 + 5.64 \cdot 10^{-18} q^4 + 7.00 \cdot 10^{-7} q^6 + 52.01 q^8 + O(q^{10})$$

- Idea: recall that:

$$\Theta_{\mathcal{G}_{128,e}}(q) = 1 + 6.11 \cdot 10^{-37} q^2 + 5.64 \cdot 10^{-18} q^4 + 7.00 \cdot 10^{-7} q^6 + 52.01 q^8 + O(q^{10})$$

$\Rightarrow$ on expectation there are only

$$6.11 \cdot 10^{-37} + 5.64 \cdot 10^{-18} + 7.00 \cdot 10^{-7} = 7.00 \cdot 10^{-7}$$

non-zero vectors of squared norm < 8.

Good packing

- Idea: recall that:

$$\Theta_{\mathcal{G}_{128,e}}(q) = 1 + 6.11 \cdot 10^{-37} q^2 + 5.64 \cdot 10^{-18} q^4 + 7.00 \cdot 10^{-7} q^6 + 52.01 q^8 + O(q^{10})$$

$\Rightarrow$ on expectation there are only

$$6.11 \cdot 10^{-37} + 5.64 \cdot 10^{-18} + 7.00 \cdot 10^{-7} = 7.00 \cdot 10^{-7}$$

non-zero vectors of squared norm < 8.

$\Rightarrow$ there exists a lattice $\mathcal{L} \in \mathcal{G}_{128,e}$ with $\leq 7.00 \cdot 10^{-7} < 2$ non-zero vectors of squared norm < 8, $\Rightarrow \lambda_1(\mathcal{L})^2 \geq 8$.

- Idea: recall that:

$$\Theta_{\mathcal{G}_{128,e}}(q) = 1 + 6.11 \cdot 10^{-37} q^2 + 5.64 \cdot 10^{-18} q^4 + 7.00 \cdot 10^{-7} q^6 + 52.01 q^8 + O(q^{10})$$

$\Rightarrow$ on expectation there are only

$$6.11 \cdot 10^{-37} + 5.64 \cdot 10^{-18} + 7.00 \cdot 10^{-7} = 7.00 \cdot 10^{-7}$$

non-zero vectors of squared norm < 8.

$\Rightarrow$ there exists a lattice $\mathcal{L} \in \mathcal{G}_{128,e}$ with $\leq 7.00 \cdot 10^{-7} < 2$ non-zero vectors of squared norm < 8, $\Rightarrow \lambda_1(\mathcal{L})^2 \geq 8$.

Lemma: existence of good packing

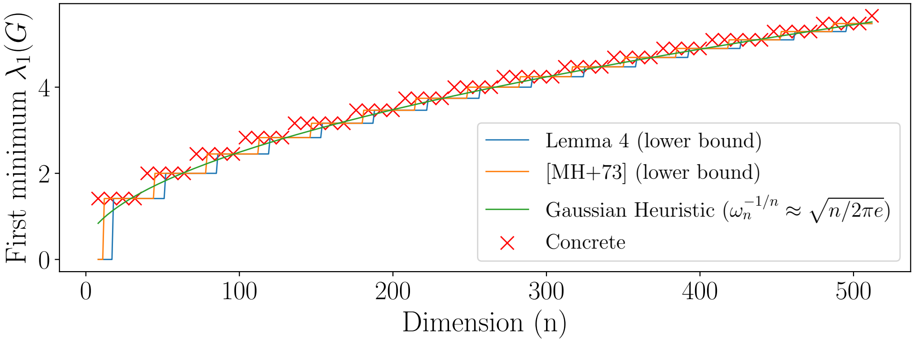
Let $\mathcal{G}$ be a genus with average theta series $\Theta_{\mathcal{G}}(q) = 1 + \sum_{m=1}^{\infty} N_m q^m$.
If $\sum_{m=1}^{\lambda} N_m < 2$, then there exists a lattice $\mathcal{L} \in \mathcal{G}$ s.t. $\lambda_1(\mathcal{L})^2 > \lambda$.

Lemma: even packing (Serre)

Let $n = 8k \geq 8$ with $k \in \mathbb{N}$, then there exists an n-dimensional even unimodular lattice $\mathcal{L}$ with $\lambda_1(\mathcal{L})^2 \geq 2 \cdot \left\lceil \frac{1}{2}(\frac{3}{5}\omega_n)^{-2/n} \right\rceil \approx n/2\pi e$.

Lemma: even packing (Serre)

Let $n = 8k \geq 8$ with $k \in \mathbb{N}$, then there exists an n-dimensional even unimodular lattice $\mathcal{L}$ with $\lambda_1(\mathcal{L})^2 \geq 2 \cdot \left\lceil \frac{1}{2}\left(\frac{3}{5}\omega_n\right)^{-2/n} \right\rceil \approx n/2\pi e$.



Example: even unimodular case (2)

Lemma: even packing (Serre)

Let $n = 8k \geq 8$ with $k \in \mathbb{N}$, then there exists an n-dimensional even unimodular lattice $\mathcal{L}$ with $\lambda_1(\mathcal{L})^2 \geq 2 \cdot \left\lceil \frac{1}{2}\left(\frac{3}{5}\omega_n\right)^{-2/n} \right\rceil \approx n/2\pi e$.

- Essentially same result for odd case (by Conway & Thompson)

Example: even unimodular case (2)

Lemma: even packing (Serre)

Let $n = 8k \geq 8$ with $k \in \mathbb{N}$, then there exists an n-dimensional even unimodular lattice $\mathcal{L}$ with $\lambda_1(\mathcal{L})^2 \geq 2 \cdot \left\lceil \frac{1}{2}(\frac{3}{5}\omega_n)^{-2/n} \right\rceil \approx n/2\pi e$.

- Essentially same result for odd case (by Conway & Thompson)
- Self-dual so also good dual packing

Example: even unimodular case (2)

Lemma: even packing (Serre)

Let $n = 8k \geq 8$ with $k \in \mathbb{N}$, then there exists an n-dimensional even unimodular lattice $\mathcal{L}$ with $\lambda_1(\mathcal{L})^2 \geq 2 \cdot \left\lceil \frac{1}{2}(\frac{3}{5}\omega_n)^{-2/n} \right\rceil \approx n/2\pi e$.

- Essentially same result for odd case (by Conway & Thompson)
- Self-dual so also good dual packing
- More generally: sum over primal and dual theta series to lower bound $\lambda_1(\mathcal{L})$ and $\lambda_1(\mathcal{L}^*)$ simultaneously.

Example: even unimodular case (2)

Lemma: even packing (Serre)

Let $n = 8k \geq 8$ with $k \in \mathbb{N}$, then there exists an n-dimensional even unimodular lattice $\mathcal{L}$ with $\lambda_1(\mathcal{L})^2 \geq 2 \cdot \left\lceil \frac{1}{2}(\frac{3}{5}\omega_n)^{-2/n} \right\rceil \approx n/2\pi e$.

- Essentially same result for odd case (by Conway & Thompson)
- Self-dual so also good dual packing
- More generally: sum over primal and dual theta series to lower bound $\lambda_1(\mathcal{L})$ and $\lambda_1(\mathcal{L}^*)$ simultaneously.
- Not aware of similar results for other genera

- Recall: for the smoothing parameter $\eta_\varepsilon(\mathcal{L}^*)$ we need to bound $\theta_{\mathcal{L}}(\exp(-\pi s^2)) \leq 1 + \varepsilon$.
- Note that for any $s > 0$ we have

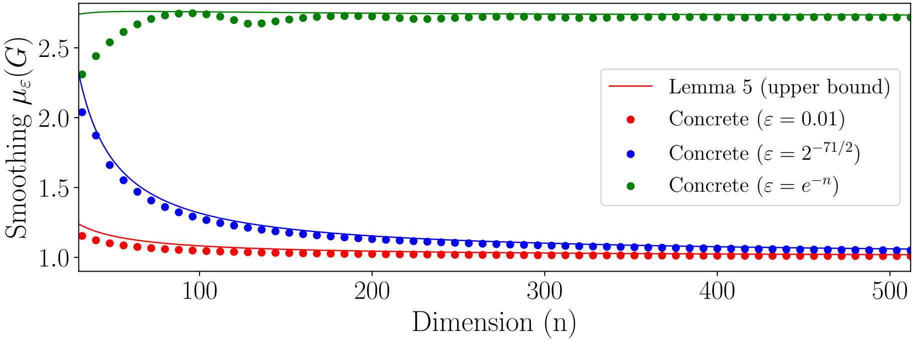
$$\theta_{\mathcal{G}}(\exp(-\pi s^2)) = \mathbb{E}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})} \left[\theta_{\mathcal{L}}(\exp(-\pi s^2))\right]$$

Lemma: existence of good smoothing

For any genus $\mathcal{G}$, let $\varepsilon > 0$ and let $s > 0$ be such that $\Theta_{\mathcal{G}}(\exp(-\pi s^2)) \leq 1 + \varepsilon$, then there exists a lattice $\mathcal{L} \in \mathcal{G}$ such that $\eta_\varepsilon(\mathcal{L}^*) \leq s$.

Lemma: even smoothing

Let $n = 8k \geq 8$ with $k \in \mathbb{N}$, and $\varepsilon \in [e^{-n}, 1)$, then there exists an n-dimensional even unimodular lattice $\mathcal{L}$ with $\eta_\varepsilon(\mathcal{L}) \leq (\pi\varepsilon/n)^{-\frac{1}{n+2}}$.



General case: compute mass formula

- Note that we want to count the average number of solutions N_y to $f(x) := x^\top G_{\mathcal{L}} x = y$ with $x \in \mathbb{Z}^n$ over the randomness of $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.

General case: compute mass formula

- Note that we want to count the average number of solutions N_y to $f(x) := x^\top G_{\mathcal{L}} x = y$ with $x \in \mathbb{Z}^n$ over the randomness of $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(y)$ of solutions over $\mathbb{Z}_p$ and $\mathbb{R} = \mathbb{Z}_\infty$.

General case: compute mass formula

- Note that we want to count the average number of solutions N_y to $f(x) := x^\top G_{\mathcal{L}} x = y$ with $x \in \mathbb{Z}^n$ over the randomness of $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(y)$ of solutions over $\mathbb{Z}_p$ and $\mathbb{R} = \mathbb{Z}_\infty$.

Theorem: Siegel-Weil mass formula

For any genus $\mathcal{G}$ of dimension ≥ 2 and average theta series $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_y q^m$ we have

$$N_y = \prod_{p=2,3,\ldots,\infty} \delta_{\mathcal{G},p}(y)$$

General case: compute mass formula

- Note that we want to count the average number of solutions N_y to $f(x) := x^\top G_{\mathcal{L}} x = y$ with $x \in \mathbb{Z}^n$ over the randomness of $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(y)$ of solutions over $\mathbb{Z}_p$ and $\mathbb{R} = \mathbb{Z}_\infty$.

Theorem: Siegel-Weil mass formula

For any genus $\mathcal{G}$ of dimension ≥ 2 and average theta series $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_y q^m$ we have

$$N_y = \prod_{p=2,3,\ldots,\infty} \delta_{\mathcal{G},p}(y)$$

- Local-global principle

General case: compute mass formula

- Note that we want to count the average number of solutions N_y to $f(x) := x^\top G_{\mathcal{L}} x = y$ with $x \in \mathbb{Z}^n$ over the randomness of $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(y)$ of solutions over $\mathbb{Z}_p$ and $\mathbb{R} = \mathbb{Z}_\infty$.

Theorem: Siegel-Weil mass formula

For any genus $\mathcal{G}$ of dimension ≥ 2 and average theta series $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_y q^m$ we have

$$N_y = \prod_{p=2,3,\ldots,\infty} \delta_{\mathcal{G},p}(y)$$

- Local-global principle
- Only primes $p | 2y \det(\mathcal{G})^2$ have to be considered

General case: compute mass formula

- Note that we want to count the average number of solutions N_y to $f(x) := x^\top G_{\mathcal{L}} x = y$ with $x \in \mathbb{Z}^n$ over the randomness of $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(y)$ of solutions over $\mathbb{Z}_p$ and $\mathbb{R} = \mathbb{Z}_\infty$.

Theorem: Siegel-Weil mass formula

For any genus $\mathcal{G}$ of dimension ≥ 2 and average theta series $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_y q^m$ we have

$$N_y = \prod_{p=2,3,\ldots,\infty} \delta_{\mathcal{G},p}(y)$$

- Local-global principle
- Only primes $p | 2y \det(\mathcal{G})^2$ have to be considered
- Can even be generalized to matrix equations!

  (mass formula from $M(\mathcal{G})$ follows from equation $U^\top G U = G$)

Local density over reals

- For $f(x) = x^\top x = x_1^2 + \ldots + x_n^2 \in \mathbb{R}$ the density of solutions for $f(x) = y$ is essentially the volume of the sphere of radius $\sqrt{y}$.

Local density over reals

- For $f(x) = x^\top x = x_1^2 + \ldots + x_n^2 \in \mathbb{R}$ the density of solutions for $f(x) = y$ is essentially the volume of the sphere of radius $\sqrt{y}$.
- More precisely we get $\delta_{I_n,\infty}(y) = \frac{1}{2} n\omega_n y^{n/2-1} = \frac{d}{dy}(\omega_n y^{n/2})$

Local density over reals

- For $f(x) = x^\top x = x_1^2 + \ldots + x_n^2 \in \mathbb{R}$ the density of solutions for $f(x) = y$ is essentially the volume of the sphere of radius $\sqrt{y}$.
- More precisely we get $\delta_{I_n,\infty}(y) = \frac{1}{2} n\omega_n y^{n/2-1} = \frac{d}{dy}(\omega_n y^{n/2})$

Local density over reals

- For $f(x) = x^\top x = x_1^2 + \ldots + x_n^2 \in \mathbb{R}$ the density of solutions for $f(x) = y$ is essentially the volume of the sphere of radius $\sqrt{y}$.
- More precisely we get $\delta_{I_n,\infty}(y) = \frac{1}{2} n \omega_n y^{n/2-1} = \frac{d}{dy}(\omega_n y^{n/2})$

Lemma: local density at $\mathbb{R}$ ($p = \infty$)

We have $\delta_{\mathcal{G},\infty}(y) = \frac{1}{2} n \omega_n y^{n/2-1} \cdot \det(\mathcal{G})^{-1}$

Local density over reals

- For $f(x) = x^\top x = x_1^2 + \ldots + x_n^2 \in \mathbb{R}$ the density of solutions for $f(x) = y$ is essentially the volume of the sphere of radius $\sqrt{y}$.
- More precisely we get $\delta_{I_n,\infty}(y) = \frac{1}{2} n\omega_n y^{n/2-1} = \frac{d}{dy}(\omega_n y^{n/2})$

Lemma: local density at $\mathbb{R}$ ($p = \infty$)

We have $\delta_{\mathcal{G},\infty}(y) = \frac{1}{2} n\omega_n y^{n/2-1} \cdot \det(\mathcal{G})^{-1}$

- Behaves as expected:

  sparser lattice $\Rightarrow$ larger $\det(\mathcal{G})$ $\Rightarrow$ smaller coefficients.

Local density over $\mathbb{Z}_p$

- This is where things get complicated, count solutions mod p^k

Local density over $\mathbb{Z}_p$

- This is where things get complicated, count solutions mod p^k
- Ratio between #solutions $x^\top G x = y \bmod p^k$ and $p^{(n-1)k}$ for $k \to \infty$

Local density over $\mathbb{Z}_p$

- This is where things get complicated, count solutions mod p^k
- Ratio between #solutions $x^\top G x = y \bmod p^k$ and $p^{(n-1)k}$ for $k \to \infty$
- Has only small contribution, e.g.

Local density over $\mathbb{Z}_p$

- This is where things get complicated, count solutions mod p^k
- Ratio between #solutions $x^\top G x = y \bmod p^k$ and $p^{(n-1)k}$ for $k \to \infty$
- Has only small contribution, e.g.

Local density over $\mathbb{Z}_p$

- This is where things get complicated, count solutions mod p^k
- Ratio between #solutions $x^\top G x = y \bmod p^k$ and $p^{(n-1)k}$ for $k \to \infty$
- Has only small contribution, e.g.

Lemma: Local densities at $\mathbb{Z}_p$ are bounded

Let $\mathcal{G}$ be a genus with $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p, then for all $y \geq 0$ we have

$$\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(y) \leq \frac{18\zeta(2)}{7\zeta(3)} < 3.52$$

Local density over $\mathbb{Z}_p$

- This is where things get complicated, count solutions mod p^k
- Ratio between #solutions $x^\top G x = y \bmod p^k$ and $p^{(n-1)k}$ for $k \to \infty$
- Has only small contribution, e.g.

Lemma: Local densities at $\mathbb{Z}_p$ are bounded

Let $\mathcal{G}$ be a genus with $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p, then for all $y \geq 0$ we have

$$\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(y) \leq \frac{18\zeta(2)}{7\zeta(3)} < 3.52$$

Rough idea:

$G \sim_{\mathbb{Z}_p} G_0 + p \cdot G_1 + p^2 \cdot G_2 + \ldots$ with $\det(G_i) \neq 0 \bmod p$, $\dim(G_0) \geq 6$
If $\delta_{G_0,p}(y) \leq c$ for all $y \geq 0$, then $\delta_{G,p}(y) \leq c$ for all $y \geq 0$.

Theorem:

Let $\mathcal{G}$ be any genus with $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p. Let $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_y q^y$ be its average theta series, then for $y \geq 1$ we have

$$N_y \leq 3.52 \cdot \delta_{\mathcal{G},\infty}(y) \leq 1.76 \cdot n\omega_n y^{n/2-1} \cdot \det(\mathcal{G})^{-1}$$

Finalizing

Theorem:

Let $\mathcal{G}$ be any genus with $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p. Let $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_y q^y$ be its average theta series, then for $y \geq 1$ we have

$$N_y \leq 3.52 \cdot \delta_{\mathcal{G},\infty}(y) \leq 1.76 \cdot n\omega_n y^{n/2-1} \cdot \det(\mathcal{G})^{-1}$$

- Tight up to a constant factor

Theorem:

Let $\mathcal{G}$ be any genus with $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p. Let $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_y q^y$ be its average theta series, then for $y \geq 1$ we have

$$N_y \leq 3.52 \cdot \delta_{\mathcal{G},\infty}(y) \leq 1.76 \cdot n\omega_n y^{n/2-1} \cdot \det(\mathcal{G})^{-1}$$

- Tight up to a constant factor
- Sufficient to prove the main results

Finalizing

Theorem:

Let $\mathcal{G}$ be any genus with $p^{n-5} \nmid \det(\mathcal{G})^2$ for all primes p. Let $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_y q^y$ be its average theta series, then for $y \geq 1$ we have

$$N_y \leq 3.52 \cdot \delta_{\mathcal{G},\infty}(y) \leq 1.76 \cdot n\omega_n y^{n/2-1} \cdot \det(\mathcal{G})^{-1}$$

- Tight up to a constant factor
- Sufficient to prove the main results
- Conjecture: remove conditions $\implies$ extra factor $\mathrm{poly}(y)$
  (but rather tedious to work out)

Conclusion

For any genus $\mathcal{G}$ we can show

- the existence of a good and dual packing (simultaneously)

Conclusion

For any genus $\mathcal{G}$ we can show

- the existence of a good and dual packing (simultaneously)
- the existence of a good smoothing even for large $\varepsilon > 0$

Conclusion

For any genus $\mathcal{G}$ we can show

- the existence of a good and dual packing (simultaneously)
- the existence of a good smoothing even for large $\varepsilon > 0$
- by Markov inequality: many good packings/smoothings

Conclusion

For any genus $\mathcal{G}$ we can show

- the existence of a good and dual packing (simultaneously)
- the existence of a good smoothing even for large $\varepsilon > 0$
- by Markov inequality: many good packings/smoothings

We achieve this by

- The quite unknown but beautiful Siegel-Weil mass formula

Conclusion

For any genus $\mathcal{G}$ we can show

- the existence of a good and dual packing (simultaneously)
- the existence of a good smoothing even for large $\varepsilon > 0$
- by Markov inequality: many good packings/smoothings

We achieve this by

- The quite unknown but beautiful Siegel-Weil mass formula
- Counting solutions in $\mathbb{Z}_p$

Conclusion

For any genus $\mathcal{G}$ we can show

- the existence of a good and dual packing (simultaneously)
- the existence of a good smoothing even for large $\varepsilon > 0$
- by Markov inequality: many good packings/smoothings

We achieve this by

- The quite unknown but beautiful Siegel-Weil mass formula
- Counting solutions in $\mathbb{Z}_p$

Open questions:

- What about other geometric properties?
- What else can we do with these mass formulas?

Thank you! :)

Questions?

Thank you! :)

Questions?