

Dense and smooth lattices in any genus

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

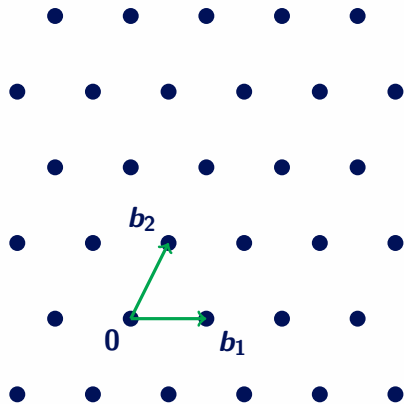
Lattices

Lattice

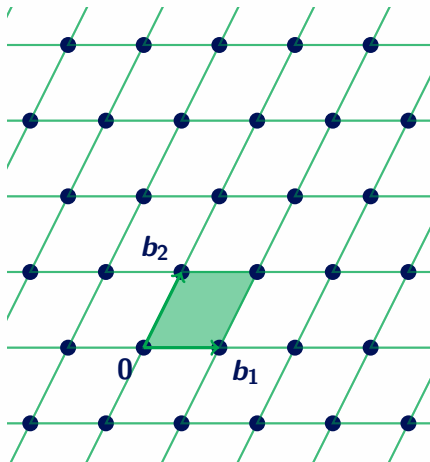
$\mathbb{R}$ -linearly independent $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^n$

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

basis $\mathbf{B}$.



Lattices



Lattice

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

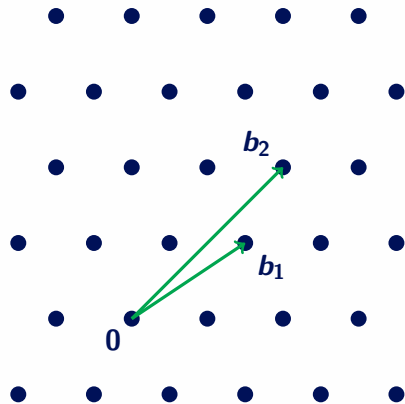
$$\mathcal{L}(B) := \{\sum_i x_i \mathbf{b}_i : x \in \mathbb{Z}^n\} \subset \mathbb{R}^n,$$

basis B .

Lattice (co)volume

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

Lattices



Lattice

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

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

basis B .

Lattice (co)volume

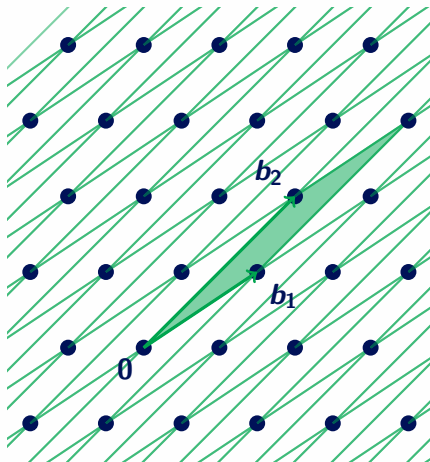
$$\det(\mathcal{L}) := \text{vol}(\mathbb{R}^n / \mathcal{L}) = |\det(B)|$$

Infinitely many distinct bases

$$B' = B \cdot U,$$

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

Lattices



Lattice

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

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

basis B .

Lattice (co)volume

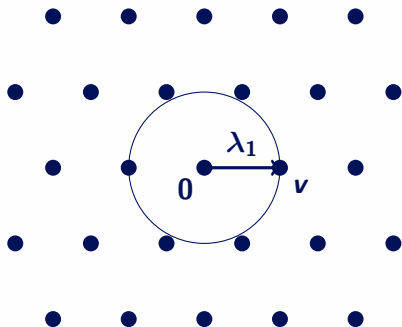
$$\det(\mathcal{L}) := \text{vol}(\mathbb{R}^n / \mathcal{L}) = |\det(B)|$$

Infinitely many distinct bases

$$B' = B \cdot U,$$

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

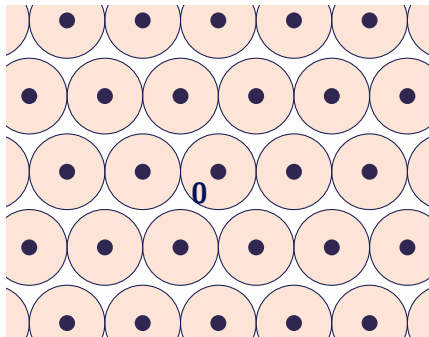
Lattice packings



First minimum & theta series

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

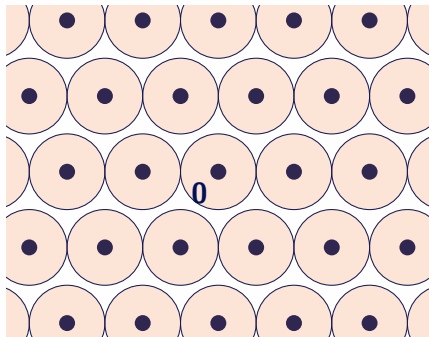
Lattice packings



First minimum & theta series

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

Lattice packings



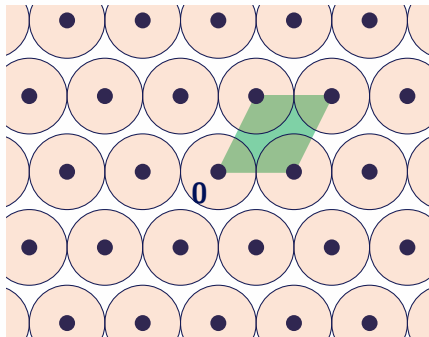
First minimum & theta series

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

Packing density

$$\delta(\mathcal{L}) = \frac{\text{vol}(\mathcal{B}_R^n)}{\text{det}(\mathcal{L})}, \text{ where } R = \frac{1}{2}\lambda_1(\mathcal{L})$$

Lattice packings



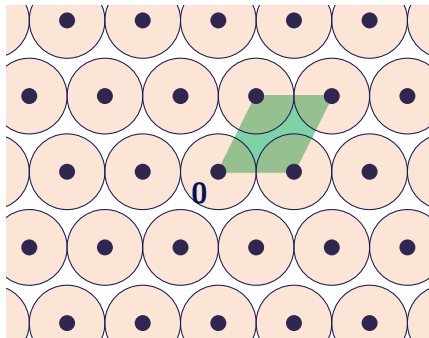
First minimum & theta series

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

Packing density

$$\delta(\mathcal{L}) = \frac{\text{vol}(\mathcal{B}_R^n)}{\text{det}(\mathcal{L})}, \text{ where } R = \frac{1}{2}\lambda_1(\mathcal{L})$$

Lattice packings



First minimum & theta series

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

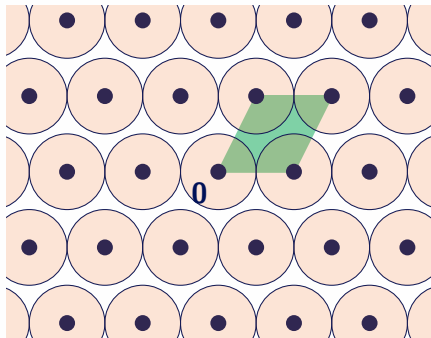
Packing density

$$\delta(\mathcal{L}) = \frac{\text{vol}(\mathcal{B}_R^n)}{\text{det}(\mathcal{L})}, \text{ where } R = \frac{1}{2}\lambda_1(\mathcal{L})$$

Minkowski's Theorem ($\delta(\mathcal{L}) \leq 1$)

$$\lambda_1(\mathcal{L}) \leq 2 \cdot \underbrace{\frac{\text{det}(\mathcal{L})^{1/n}}{\text{vol}(\mathcal{B}_1^n)^{1/n}}}_{\text{Mk}(\mathcal{L})}$$

Lattice packings



Minkowski-Hlawka Theorem

There exists a lattice $\mathcal{L} \subset \mathbb{R}^n$
with $\lambda_1(\mathcal{L}) > \frac{1}{2} \text{Mk}(\mathcal{L})$.

First minimum & theta series

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

Packing density

$$\delta(\mathcal{L}) = \frac{\text{vol}(\mathcal{B}_R^n)}{\text{det}(\mathcal{L})}, \text{ where } R = \frac{1}{2}\lambda_1(\mathcal{L})$$

Minkowski's Theorem ($\delta(\mathcal{L}) \leq 1$)

$$\lambda_1(\mathcal{L}) \leq 2 \cdot \underbrace{\frac{\text{det}(\mathcal{L})^{1/n}}{\text{vol}(\mathcal{B}_1^n)^{1/n}}}_{\text{Mk}(\mathcal{L})}$$

Good packings from random lattices

- **Observation:** 'random' lattices are good packings

Good packings from random lattices

- ▶ **Observation:** ‘random’ lattices are good packings
 - ▶ Gaussian Heuristic: $\lambda_1(\mathcal{L}) \approx \frac{1}{2} \text{Mk}(\mathcal{L})$

Good packings from random lattices

- ▶ **Observation:** ‘random’ lattices are good packings
 - ▶ Gaussian Heuristic: $\lambda_1(\mathcal{L}) \approx \frac{1}{2} \text{Mk}(\mathcal{L})$
- ▶ Seen as the hardest instances for lattice problems

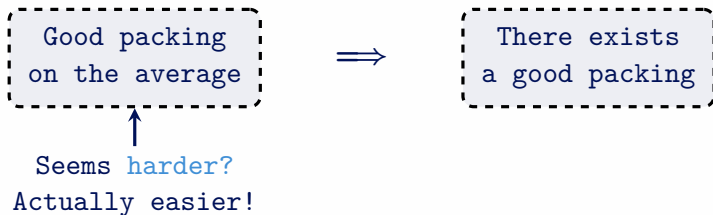
Good packings from random lattices

- **Observation:** ‘random’ lattices are good packings
 - Gaussian Heuristic: $\lambda_1(\mathcal{L}) \approx \frac{1}{2} \text{Mk}(\mathcal{L})$
- Seen as the hardest instances for lattice problems



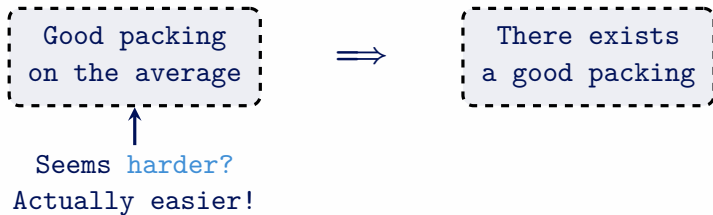
Good packings from random lattices

- **Observation:** ‘random’ lattices are good packings
 - Gaussian Heuristic: $\lambda_1(\mathcal{L}) \approx \frac{1}{2} \text{Mk}(\mathcal{L})$
- Seen as the hardest instances for lattice problems



Good packings from random lattices

- **Observation:** ‘random’ lattices are good packings
 - Gaussian Heuristic: $\lambda_1(\mathcal{L}) \approx \frac{1}{2} \text{Mk}(\mathcal{L})$
- Seen as the hardest instances for lattice problems



- **Random?** Invariant Haar measure over space of all lattices with fixed dimension and volume. (details not so important for this talk)

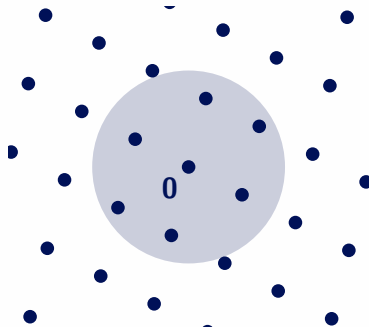
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

Let $\mathcal{L}_{[n]}$ be the space all lattices of dimension n and volume 1, then

$$\mathbb{E}_{\mathcal{L} \in \mathcal{L}_{[n]}} |\mathcal{L} \cap \mathcal{B}_\lambda^n| = 1 + \text{vol}(\mathcal{B}_\lambda^n).$$

‘Average of one non-zero point per unit volume’



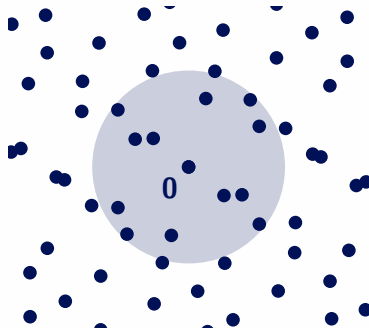
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

Let $\mathcal{L}_{[n]}$ be the space all lattices of dimension n and volume 1, then

$$\mathbb{E}_{\mathcal{L} \in \mathcal{L}_{[n]}} |\mathcal{L} \cap \mathcal{B}_\lambda^n| = 1 + \text{vol}(\mathcal{B}_\lambda^n).$$

‘Average of one non-zero point per unit volume’



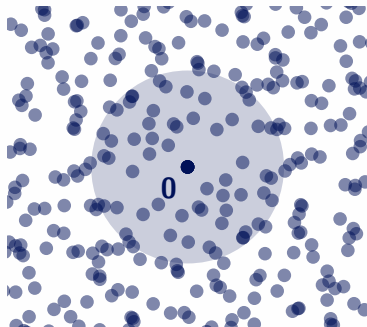
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

Let $\mathcal{L}_{[n]}$ be the space all lattices of dimension n and volume 1, then

$$\mathbb{E}_{\mathcal{L} \in \mathcal{L}_{[n]}} |\mathcal{L} \cap \mathcal{B}_\lambda^n| = 1 + \text{vol}(\mathcal{B}_\lambda^n).$$

‘Average of one non-zero point per unit volume’



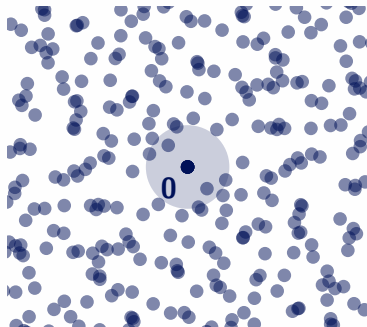
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

Let $\mathcal{L}_{[n]}$ be the space all lattices of dimension n and volume 1, then

$$\mathbb{E}_{\mathcal{L} \in \mathcal{L}_{[n]}} |\mathcal{L} \cap \mathcal{B}_{\lambda}^n| = 1 + \text{vol}(\mathcal{B}_{\lambda}^n).$$

‘Average of one non-zero point per unit volume’



Proof: Minkowski-Hlawka Theorem

Pick $\lambda = \frac{1}{2} \text{Mk}(n)$,

then $\mathbb{E}_{\mathcal{L} \in \mathcal{L}_{[n]}} |\mathcal{L} \cap \mathcal{B}_{\lambda}^n| = 2$.

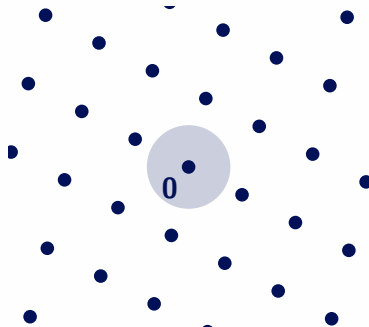
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

Let $\mathcal{L}_{[n]}$ be the space all lattices of dimension n and volume 1, then

$$\mathbb{E}_{\mathcal{L} \in \mathcal{L}_{[n]}} |\mathcal{L} \cap \mathcal{B}_\lambda^n| = 1 + \text{vol}(\mathcal{B}_\lambda^n).$$

‘Average of one non-zero point per unit volume’



Proof: Minkowski-Hlawka Theorem

Pick $\lambda = \frac{1}{2} \text{Mk}(n)$,

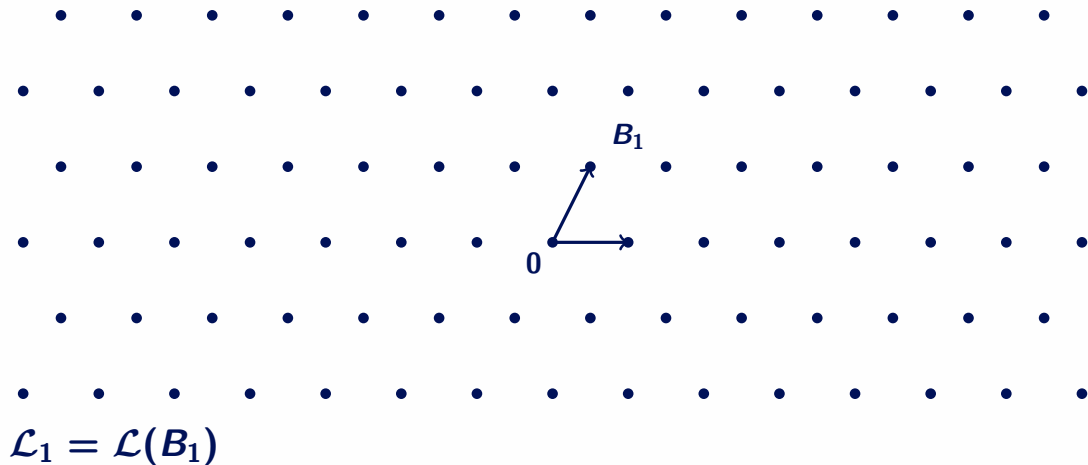
then $\mathbb{E}_{\mathcal{L} \in \mathcal{L}_{[n]}} |\mathcal{L} \cap \mathcal{B}_\lambda^n| = 2$.

$\Rightarrow \exists \mathcal{L} \in \mathcal{L}_{[n]}$ with $|\mathcal{L} \cap \mathcal{B}_\lambda^n| \leq 2$,

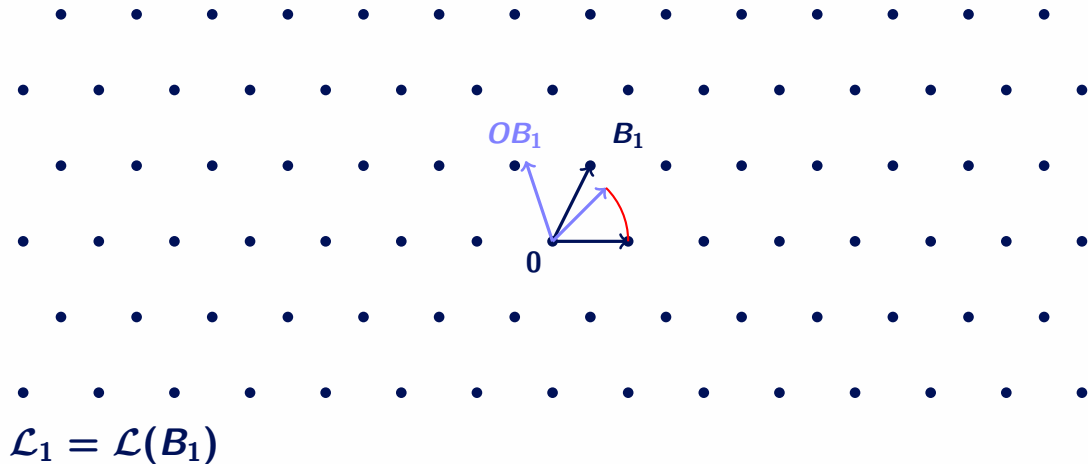
$\Rightarrow \exists \mathcal{L} \in \mathcal{L}_{[n]}$ with $\lambda_1(\mathcal{L}) > \lambda = \frac{1}{2} \text{Mk}(\mathcal{L})$

LIP and the genus of a lattice

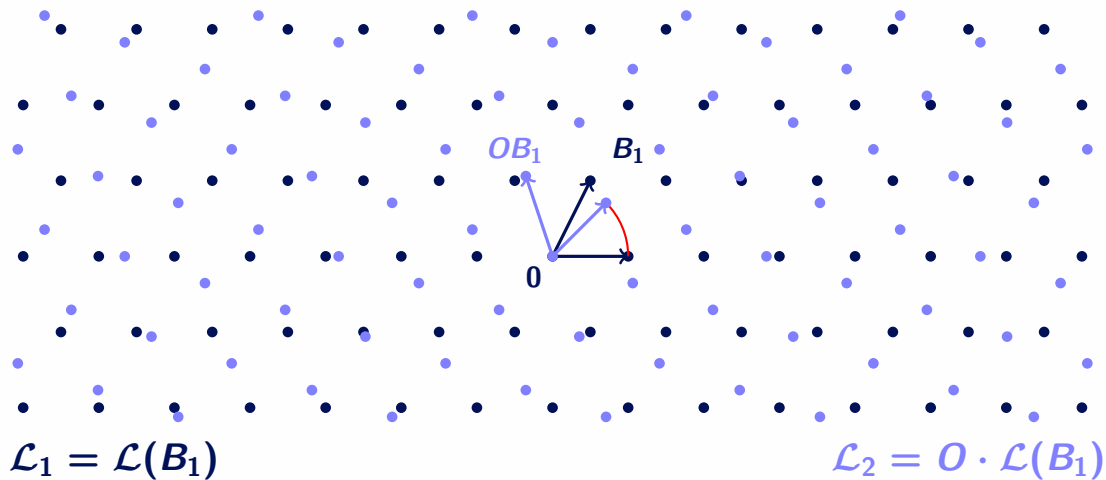
Lattice Isomorphism Problem (LIP)



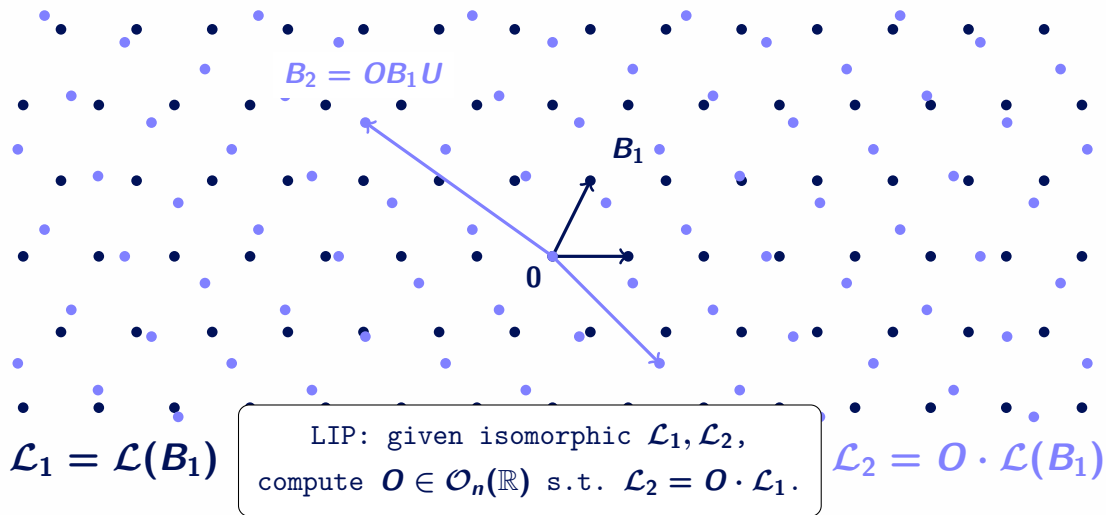
Lattice Isomorphism Problem (LIP)



Lattice Isomorphism Problem (LIP)

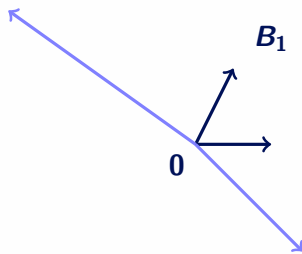


Lattice Isomorphism Problem (LIP)



Lattice Isomorphism Problem (LIP)

$$B_2 = OB_1U$$



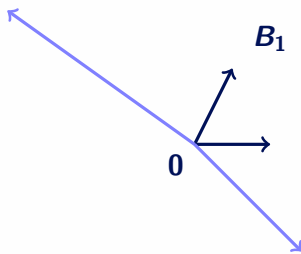
$$\mathcal{L}_1 = \mathcal{L}(B_1)$$

LIP: given isomorphic $\mathcal{L}_1, \mathcal{L}_2$,
compute $O \in \mathcal{O}_n(\mathbb{R})$ s.t. $\mathcal{L}_2 = O \cdot \mathcal{L}_1$.

$$\mathcal{L}_2 = O \cdot \mathcal{L}(B_1)$$

Lattice Isomorphism Problem (LIP)

$$B_2 = OB_1U$$



$$\mathcal{L}_1 = \mathcal{L}(B_1)$$

LIP: given isomorphic $\mathcal{L}_1, \mathcal{L}_2$,
compute $O \in \mathcal{O}_n(\mathbb{R})$ s.t. $\mathcal{L}_2 = O \cdot \mathcal{L}_1$.

$$\mathcal{L}_2 = O \cdot \mathcal{L}(B_1)$$

(unique up to $\text{Aut}(\mathcal{L}) := \{O \in \mathcal{O}_n(\mathbb{R}) : O \cdot \mathcal{L} = \mathcal{L}\}$)

- ▶ LIP as a new hardness assumption

Cryptography from LIP

- ▶ LIP as a new hardness assumption

DvW, EC 2022: 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

DvW, EC 2022: On LIP, QFs, Remarkable Lattices, and Cryptography

Use LIP to hide a remarkable lattice:

- ▶ Identification, Encryption and Signature scheme

BGPSD, EC 2023: 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

DvW, EC 2022: On LIP, QFs, Remarkable Lattices, and Cryptography

Use LIP to hide a remarkable lattice:

- Identification, Encryption and Signature scheme

BGPSD, EC 2023: Just how hard are rotations of $\mathbb{Z}^n$?

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

DPPvW, AC 2022: HAWK scheme

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

- now in round 2 of NIST call for additional signatures

Cryptography from LIP

- ▶ LIP as a new hardness assumption

DvW, EC 2022: On LIP, QFs, Remarkable Lattices, and Cryptography

Use LIP to hide a remarkable lattice:

- ▶ Identification, Encryption and Signature scheme

BGPSD, EC 2023: Just how hard are rotations of $\mathbb{Z}^n$?

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

DPPvW, AC 2022: HAWK scheme

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

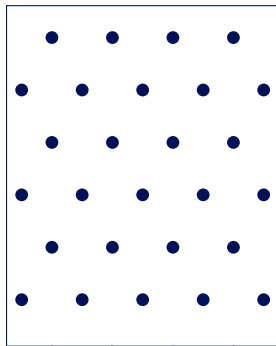
- ▶ now in round 2 of NIST call for additional signatures

- ▶ Many other works using LIP appeared recently

Distinguish LIP

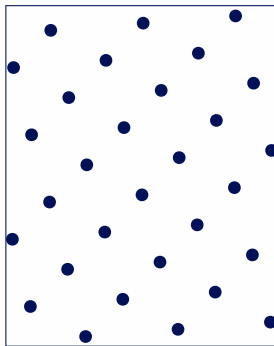
Definition: distinguish LIP (Δ -LIP)

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 .



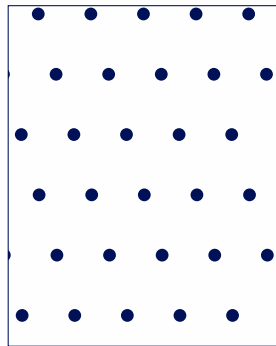
$\mathcal{L}_1$

$\| \cdot \|_2$



$O \cdot \mathcal{L}_b$

$\| \cdot \|_2$



$\mathcal{L}_2$

Distinguish 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 .

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.

Distinguish 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 .

Usual security assumption:

Given:

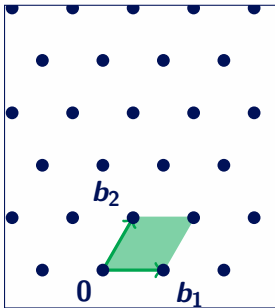
1. some remarkable lattice $\mathcal{L}_1$
2. an auxiliary lattice $\mathcal{L}_2$ with certain (good) geometric properties

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 geometric properties

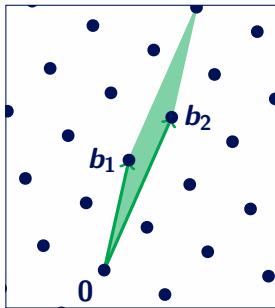
Example: good packing, smoothing, covering..

Invariants



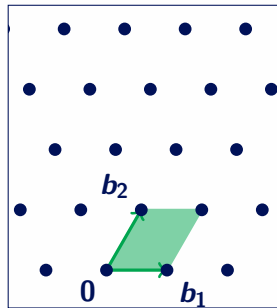
$\det(\mathcal{L}_1)$

$\stackrel{?}{=}$



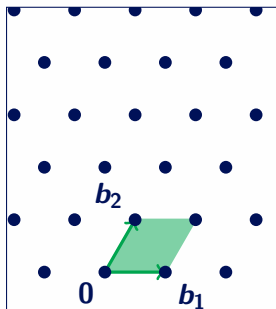
$\det(O \cdot \mathcal{L}_b)$

$\stackrel{?}{=}$



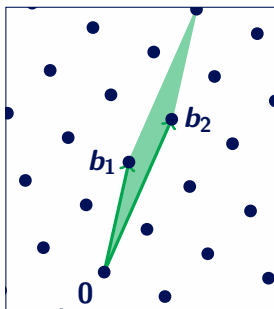
$\det(\mathcal{L}_2)$

Invariants



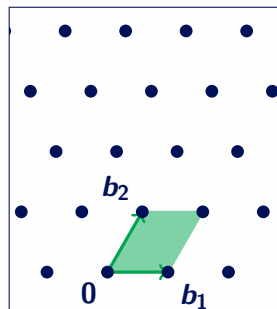
$\det(\mathcal{L}_1)$

$\stackrel{?}{=}$



$\det(O \cdot \mathcal{L}_b)$

$\stackrel{?}{=}$

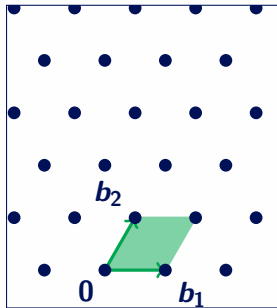


$\det(\mathcal{L}_2)$

Lemma:

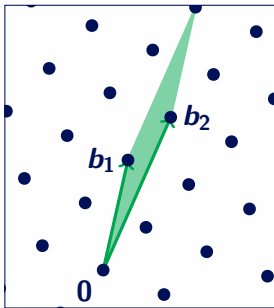
If $\det(\mathcal{L}_1) \neq \det(\mathcal{L}_2)$, then ΔLIP can be solved efficiently.

Invariants



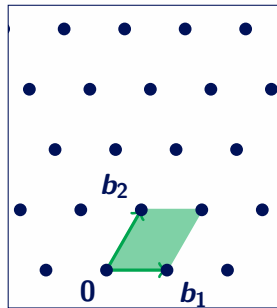
$\det(\mathcal{L}_1)$

$\stackrel{?}{=}$



$\det(O \cdot \mathcal{L}_b)$

$\stackrel{?}{=}$



$\det(\mathcal{L}_2)$

Lemma:

If $\det(\mathcal{L}_1) \neq \det(\mathcal{L}_2)$, then ΔLIP can be solved efficiently.

$\Rightarrow$ auxiliary lattice must have same (polytime-computable) invariants

Genus

- We consider *integral* lattices: $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{L}$

Genus:

Two integral lattices $\mathcal{L}_1, \mathcal{L}_2 \subset \mathbb{R}^n$ are in the same *genus* if

$$\mathcal{L}_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathcal{L}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \text{for all primes } p,$$

where $\mathbb{Z}_p$ are the p -adic integers.

Genus

- We consider **integral** lattices: $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{L}$

Genus:

Two integral lattices $\mathcal{L}_1, \mathcal{L}_2 \subset \mathbb{R}^n$ are in the same **genus** if

$$\mathcal{L}_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathcal{L}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \text{for all primes } p,$$

where $\mathbb{Z}_p$ are the p -adic integers.

Some facts:

- The genus $\mathbf{Gen}(\mathcal{L})$ contains a **finite number** of isomorphism classes

Genus

- We consider **integral** lattices: $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{L}$

Genus:

Two integral lattices $\mathcal{L}_1, \mathcal{L}_2 \subset \mathbb{R}^n$ are in the same **genus** if

$$\mathcal{L}_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathcal{L}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \text{for all primes } p,$$

where $\mathbb{Z}_p$ are the p -adic integers.

Some facts:

- The genus $\mathbf{Gen}(\mathcal{L})$ contains a **finite number** of isomorphism classes
- Genus equivalence is **efficiently computable**
(if factorization $\det(\mathcal{L})^2$ is known.)

Genus

- We consider **integral** lattices: $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{L}$

Genus:

Two integral lattices $\mathcal{L}_1, \mathcal{L}_2 \subset \mathbb{R}^n$ are in the same **genus** if

$$\mathcal{L}_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathcal{L}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \text{for all primes } p,$$

where $\mathbb{Z}_p$ are the p -adic integers.

Some facts:

- The genus $\mathbf{Gen}(\mathcal{L})$ contains a **finite number** of isomorphism classes
- Genus equivalence is **efficiently computable**
(if factorization $\det(\mathcal{L})^2$ is known.)
- **Covers all** the other known efficiently computable invariants*

Good packings in any genus

Motivation

BGPSD, EC 2023: Just how hard are rotations of $\mathbb{Z}^n$?

Do there exist lattices $\mathcal{L} \in \text{gen}(\mathbb{Z}^n)$ with

- ▶ $\lambda_1(\mathcal{L}) \geq \Omega(\text{Mk}(\mathcal{L})/\sqrt{\log(n)})$, or
- ▶ $\eta_\epsilon(\mathcal{L}) \leq \eta_\epsilon(\mathbb{Z}^n)/\sqrt{\log(n)} \approx \sqrt{\log(1/\epsilon)/\log(n)}$ for $\epsilon < n^{-\omega(1)}$?

Motivation

BGPSD, EC 2023: Just how hard are rotations of $\mathbb{Z}^n$?

Do there exist lattices $\mathcal{L} \in \text{gen}(\mathbb{Z}^n)$ with

- ▶ $\lambda_1(\mathcal{L}) \geq \Omega(\text{Mk}(\mathcal{L})/\sqrt{\log(n)})$, or
- ▶ $\eta_\epsilon(\mathcal{L}) \leq \eta_\epsilon(\mathbb{Z}^n)/\sqrt{\log(n)} \approx \sqrt{\log(1/\epsilon)/\log(n)}$ for $\epsilon < n^{-\omega(1)}$?

ARLW, WCC 2024: PKE from LIP

Conjecture: for $n \geq 85$ there exists a lattice $\mathcal{L} \in \text{gen}(\mathbb{Z}^n)$ with

- ▶ $\lambda_1(\mathcal{L}) \geq \sqrt[4]{72n} = \theta(\text{Mk}(\mathcal{L})/\sqrt[4]{n})$.

Motivation

BGPSD, EC 2023: Just how hard are rotations of $\mathbb{Z}^n$?

Do there exist lattices $\mathcal{L} \in \text{gen}(\mathbb{Z}^n)$ with

- ▶ $\lambda_1(\mathcal{L}) \geq \Omega(\text{Mk}(\mathcal{L})/\sqrt{\log(n)})$, or
- ▶ $\eta_\varepsilon(\mathcal{L}) \leq \eta_\varepsilon(\mathbb{Z}^n)/\sqrt{\log(n)} \approx \sqrt{\log(1/\varepsilon)/\log(n)}$ for $\varepsilon < n^{-\omega(1)}$?

ARLW, WCC 2024: PKE from LIP

Conjecture: for $n \geq 85$ there exists a lattice $\mathcal{L} \in \text{gen}(\mathbb{Z}^n)$ with

- ▶ $\lambda_1(\mathcal{L}) \geq \sqrt[4]{72n} = \theta(\text{Mk}(\mathcal{L})/\sqrt[4]{n})$.

DvW, EC 2022: On LIP, QFs, Remarkable Lattices, and Cryptography

For any lattice $\mathcal{L}_1$, does there exist a lattice $\mathcal{L}_2 \in \text{Gen}(\mathcal{L}_1)$ such that

- ▶ $\lambda_1(\mathcal{L}) = \text{Mk}(\mathcal{L})/\theta(1)$ for $\mathcal{L} = \mathcal{L}_2, \mathcal{L}_2^*$?

Motivation

BGPSD, EC 2023: Just how hard are rotations of $\mathbb{Z}^n$?

Do there exist lattices $\mathcal{L} \in \text{gen}(\mathbb{Z}^n)$ with

- ▶ $\lambda_1(\mathcal{L}) \geq \Omega(\text{Mk}(\mathcal{L})/\sqrt{\log(n)})$, or
- ▶ $\eta_\varepsilon(\mathcal{L}) \leq \eta_\varepsilon(\mathbb{Z}^n)/\sqrt{\log(n)} \approx \sqrt{\log(1/\varepsilon)/\log(n)}$ for $\varepsilon < n^{-\omega(1)}$?

ARLW, WCC 2024: PKE from LIP

Conjecture: for $n \geq 85$ there exists a lattice $\mathcal{L} \in \text{gen}(\mathbb{Z}^n)$ with

- ▶ $\lambda_1(\mathcal{L}) \geq \sqrt[4]{72n} = \theta(\text{Mk}(\mathcal{L})/\sqrt[4]{n})$.

DvW, EC 2022: On LIP, QFs, Remarkable Lattices, and Cryptography

For any lattice $\mathcal{L}_1$, does there exist a lattice $\mathcal{L}_2 \in \text{Gen}(\mathcal{L}_1)$ such that

- ▶ $\lambda_1(\mathcal{L}) = \text{Mk}(\mathcal{L})/\theta(1)$ for $\mathcal{L} = \mathcal{L}_2, \mathcal{L}_2^*$?

- ▶ Need: a Minkowski-Hlawka-like Theorem within any fixed genus

Random distribution over a genus

Theorem: Smith-Minkowski-Siegel mass formula (Siegel, 1935)

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

$$M(\mathcal{G}) := \sum_{[\mathcal{L}] \in \mathcal{G}} \frac{1}{|\mathrm{Aut}(\mathcal{L})|},$$

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

Random distribution over a genus

Theorem: Smith-Minkowski-Siegel mass formula (Siegel, 1935)

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

$$M(\mathcal{G}) := \sum_{[\mathcal{L}] \in \mathcal{G}} \frac{1}{|\mathrm{Aut}(\mathcal{L})|},$$

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

► Grows fast: $M(\mathcal{G}) \geq n^{\Omega(n^2)}$ as $n \rightarrow \infty$

Random distribution over a genus

Theorem: Smith-Minkowski-Siegel mass formula (Siegel, 1935)

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

$$M(\mathcal{G}) := \sum_{[\mathcal{L}] \in \mathcal{G}} \frac{1}{|\text{Aut}(\mathcal{L})|},$$

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

► Grows fast: $M(\mathcal{G}) \geq n^{\Omega(n^2)}$ as $n \rightarrow \infty$

Definition: distribution over Genus

Let $w(\mathcal{L}) =: 1/|\text{Aut}(\mathcal{L})|$. For a genus $\mathcal{G}$ let $\mathcal{D}(\mathcal{G})$ be the distribution such that each class $[\mathcal{L}] \in \mathcal{G}$ is sampled with probability $\frac{w(\mathcal{L})}{M(\mathcal{G})}$.

► Question: do these behave like random lattices?

Main result

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

Let $\mathcal{G}$ be any genus of dimension $n \geq 6$ such that $\text{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p . Let $\mathbf{C} = \frac{7\zeta(3)}{9\zeta(2)} \approx 0.57$. Then there exists a $\mathcal{L} \in \mathcal{G}$ with

$$\lambda_1(\mathcal{L})^2 \geq \left\lceil (\mathbf{C} \cdot \det(\mathcal{L}) / \text{vol}(\mathcal{B}_1^n))^{2/n} \right\rceil \approx \left(\frac{1}{2} \text{Mk}(\mathcal{L}) \right)^2.$$

Main result

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

Let $\mathcal{G}$ be any genus of dimension $n \geq 6$ such that $\text{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p . Let $\mathbf{C} = \frac{7\zeta(3)}{9\zeta(2)} \approx 0.57$. Then there exists a $\mathcal{L} \in \mathcal{G}$ with

$$\lambda_1(\mathcal{L})^2 \geq \left\lceil (\mathbf{C} \cdot \det(\mathcal{L}) / \text{vol}(\mathcal{B}_1^n))^{2/n} \right\rceil \approx \left(\frac{1}{2} \text{Mk}(\mathcal{L}) \right)^2.$$

- Essentially matches packing density of a random lattice.

Main result

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

Let $\mathcal{G}$ be any genus of dimension $n \geq 6$ such that $\text{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p . Let $\mathbf{C} = \frac{7\zeta(3)}{9\zeta(2)} \approx 0.57$. Then there exists a $\mathcal{L} \in \mathcal{G}$ with

$$\lambda_1(\mathcal{L})^2 \geq \left\lceil (\mathbf{C} \cdot \det(\mathcal{L}) / \text{vol}(\mathcal{B}_1^n))^{2/n} \right\rceil \approx \left(\frac{1}{2} \text{Mk}(\mathcal{L}) \right)^2.$$

- ▶ Essentially matches packing density of a random lattice.
- ▶ Similar result for simultaneous good **primal** and **dual** packing.

Main result

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

Let $\mathcal{G}$ be any genus of dimension $n \geq 6$ such that $\text{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p . Let $\mathbf{C} = \frac{7\zeta(3)}{9\zeta(2)} \approx 0.57$. Then there exists a $\mathcal{L} \in \mathcal{G}$ with

$$\lambda_1(\mathcal{L})^2 \geq \left\lceil (\mathbf{C} \cdot \det(\mathcal{L}) / \text{vol}(\mathcal{B}_1^n))^{2/n} \right\rceil \approx \left(\frac{1}{2} \text{Mk}(\mathcal{L}) \right)^2.$$

- ▶ Essentially matches packing density of a random lattice.
- ▶ Similar result for simultaneous good **primal** and **dual** packing.
- ▶ For a constant $0 < c \leq 1$ we get that

$$\mathbb{P} \left[\lambda_1(\mathcal{L})^2 \geq \left\lceil c^2 \cdot (\mathbf{C} \cdot \det(\mathcal{L}) / \text{vol}(\mathcal{B}_1^n))^{2/n} \right\rceil \right] > 1 - c^n.$$

- ▶ Similar result for **smoothing parameter** and **covering radius**.

The tool: Siegel-Weil mass formula

Theorem: Siegel-Weil mass formula - average point counting

For any genus $\mathcal{G}$ and integer $m > 0$, the expectation

$$N_m := \mathbb{E}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})} |\{x \in \mathcal{L} : \|x\|^2 = m\}|,$$

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

The tool: Siegel-Weil mass formula

Theorem: Siegel-Weil mass formula - average point counting

For any genus $\mathcal{G}$ and integer $m > 0$, the expectation

$$N_m := \mathbb{E}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})} |\{x \in \mathcal{L} : \|x\|^2 = m\}|,$$

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

- Gives us the average-case counting we need!

The tool: Siegel-Weil mass formula

Theorem: Siegel-Weil mass formula - average point counting

For any genus $\mathcal{G}$ and integer $m > 0$, the expectation

$$N_m := \mathbb{E}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})} |\{x \in \mathcal{L} : \|x\|^2 = m\}|,$$

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

- Gives us the average-case counting we need!

Theorem: Upper bound

Let $\mathcal{G}$ be any genus such that $\text{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p . Then

$$N_m \leq \frac{9\zeta(2)}{7\zeta(3)} n \text{vol}(\mathcal{B}_1^n) \cdot m^{n/2-1} / \det(\mathcal{G}) \quad \text{for all } m > 0.$$

The tool: Siegel-Weil mass formula

Theorem: Siegel-Weil mass formula - average point counting

For any genus $\mathcal{G}$ and integer $m > 0$, the expectation

$$N_m := \mathbb{E}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})} |\{x \in \mathcal{L} : \|x\|^2 = m\}|,$$

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

- Gives us the average-case counting we need!

Theorem: Upper bound

Let $\mathcal{G}$ be any genus such that $\text{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p . Then

$$N_m \leq \frac{9\zeta(2)}{7\zeta(3)} n \text{vol}(\mathcal{B}_1^n) \cdot m^{n/2-1} / \det(\mathcal{G}) \quad \text{for all } m > 0.$$

- Sufficient to prove main results with MH-like argument

Conclusion

- ▶ The genus is the strongest known efficient invariant for LIP

Conclusion

- ▶ The genus is the strongest known efficient invariant for LIP
- ▶ Well studied from a mathematical perspective (long ago!).

Conclusion

- ▶ The genus is the strongest known efficient invariant for LIP
- ▶ Well studied from a mathematical perspective (long ago!).

Thanks to the [Smith-Minkowski-Siegel](#) mass formula any genus

- ▶ contains a finite but typically large number of isom. classes.
- ▶ has a natural randomness distribution

Conclusion

- ▶ The genus is the strongest known efficient invariant for LIP
- ▶ Well studied from a mathematical perspective (long ago!).

Thanks to the [Smith-Minkowski-Siegel](#) mass formula any genus

- ▶ contains a finite but typically large number of isom. classes.
- ▶ has a natural randomness distribution

Thanks to the [Siegel-Weil](#) mass formula we can show for any genus:

- ▶ $\exists$ good primal and dual packings
- ▶ $\exists$ good smoothing
- ▶ $\exists$ good coverings

Conclusion

- ▶ The genus is the strongest known efficient invariant for LIP
- ▶ Well studied from a mathematical perspective (long ago!).

Thanks to the [Smith-Minkowski-Siegel](#) mass formula any genus

- ▶ contains a finite but typically large number of isom. classes.
- ▶ has a natural randomness distribution

Thanks to the [Siegel-Weil](#) mass formula we can show for any genus:

- ▶ $\exists$ good primal and dual packings
- ▶ $\exists$ good smoothing
- ▶ $\exists$ good coverings

$\Rightarrow$ usefull for instantiating LIP-based cryptography

Conclusion

- ▶ The genus is the strongest known efficient invariant for LIP
- ▶ Well studied from a mathematical perspective (long ago!).

Thanks to the [Smith-Minkowski-Siegel](#) mass formula any genus

- ▶ contains a finite but typically large number of isom. classes.
- ▶ has a natural randomness distribution

Thanks to the [Siegel-Weil](#) mass formula we can show for any genus:

- ▶ $\exists$ good primal and dual packings
- ▶ $\exists$ good smoothing
- ▶ $\exists$ good coverings

$\Rightarrow$ usefull for instantiating LIP-based cryptography

‘Random lattices in a genus behave like fully random lattices’

Conclusion

- ▶ The genus is the strongest known efficient invariant for LIP
- ▶ Well studied from a mathematical perspective (long ago!).

Thanks to the Smith-Minkowski-Siegel mass formula any genus

- ▶ contains a finite but typically large number of isom. classes.
- ▶ has a natural randomness distribution

Thanks to the Siegel-Weil mass formula we can show for any genus:

- ▶ $\exists$ good primal and dual packings
- ▶ $\exists$ good smoothing
- ▶ $\exists$ good coverings

$\Rightarrow$ usefull for instantiating LIP-based cryptography

‘Random lattices in a genus behave like fully random lattices’

Thanks!