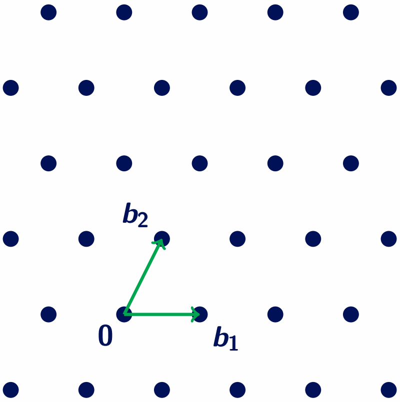
Dense and smooth lattices in any genus

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

université de BORDEAUX

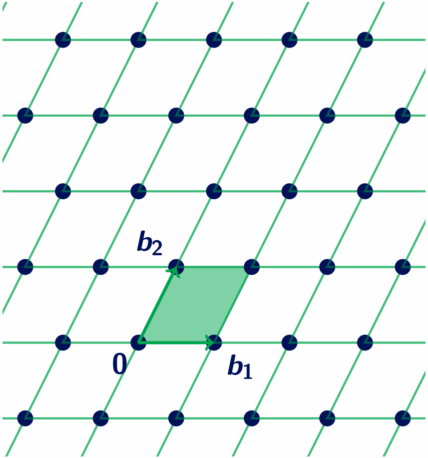


Lattice

$\mathbb{R}$-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.



Lattice

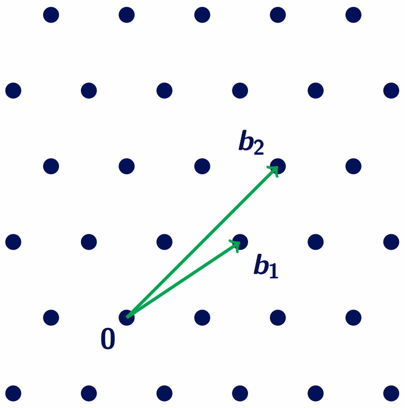
$\mathbb{R}$-linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$

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

basis B.

Lattice (co)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.

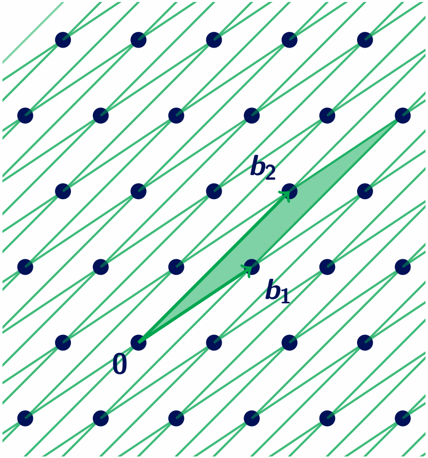
Lattice (co)volume

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

Infinitely many distinct bases

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

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



Lattice

$\mathbb{R}$-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.

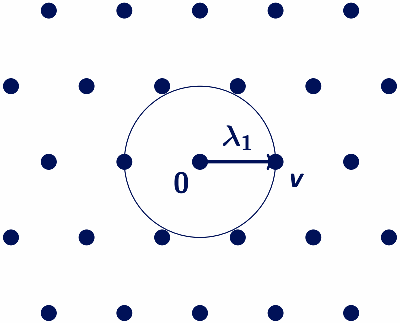
Lattice (co)volume

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

Infinitely many distinct bases

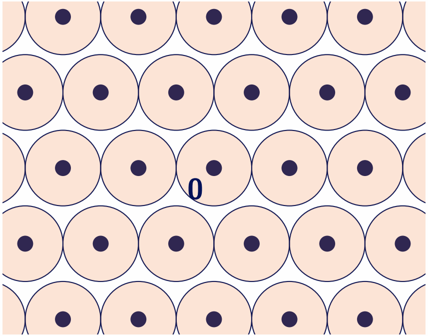
$B' = B \cdot U$,

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



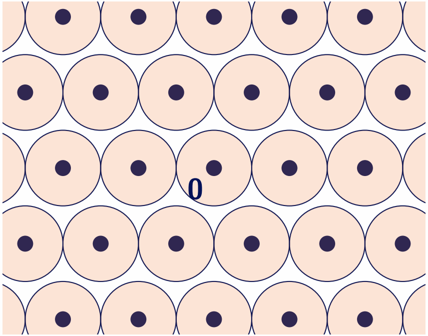
First minimum

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



First minimum

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

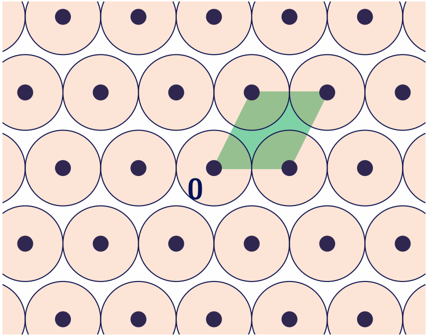


First minimum

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

Packing density

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

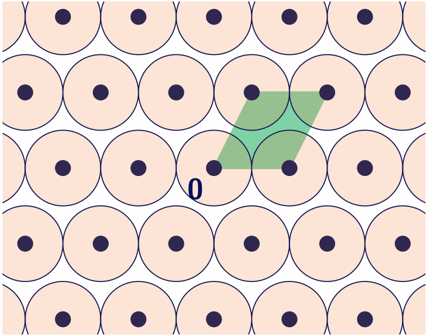


First minimum

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

Packing density

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



First minimum

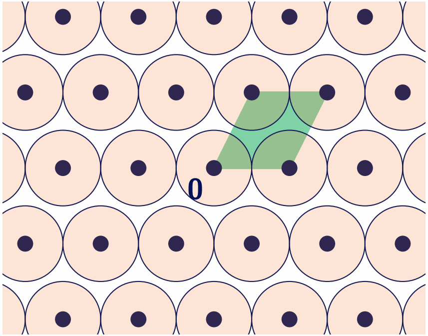
$$\lambda_1(\mathcal{L}) := \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|_2$$

Packing density

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

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

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



Minkowski-Hlawka Theorem

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

First minimum

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

Packing density

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

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

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

Good packings from random lattices

- Observation: 'random' lattices are good packings

Good packings from random lattices

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

Good packings from random lattices

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

Good packings from random lattices

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

$$\boxed{\text{Good packing on the average}} \implies \boxed{\text{There exists a good packing}}$$

Good packings from random lattices

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

Good packing on the average $\Longrightarrow$ There exists a good packing

Seems harder?
Actually easier!

Good packings from random lattices

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

$$\boxed{\text{Good packing on the average}} \implies \boxed{\text{There exists a good packing}}$$

Seems harder?
Actually easier!

- Random? (projection of) invariant Haar measure over space of all lattices with fixed dimension and determinant.

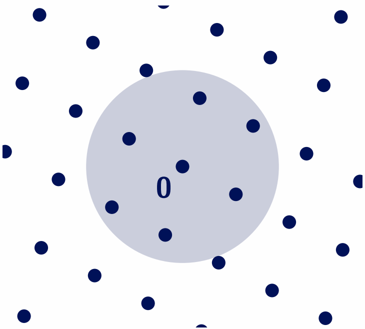
(details not important for this talk)

Average number of lattice points: Hlawka43, Siegel45

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

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

'Average of one non-zero point per unit volume'



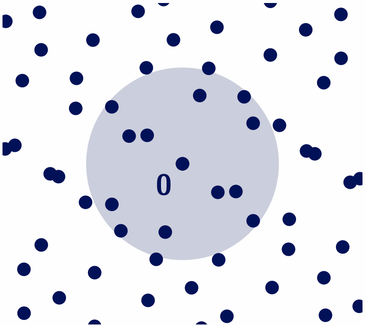
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

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

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

'Average of one non-zero point per unit volume'

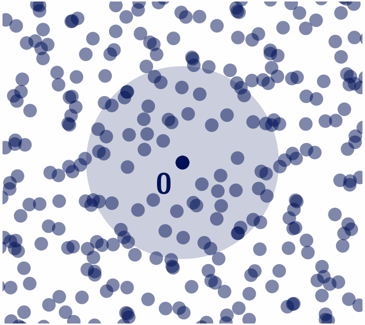


Average number of lattice points: Hlawka43, Siegel45

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

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

'Average of one non-zero point per unit volume'

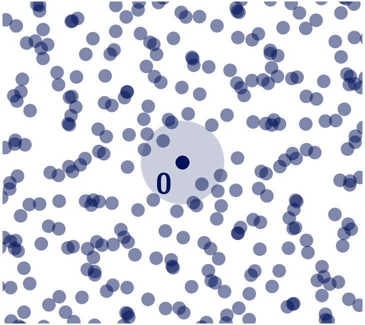


Average number of lattice points: Hlawka43, Siegel45

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

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

'Average of one non-zero point per unit volume'



Proof: Minkowski-Hlawka Theorem

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

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

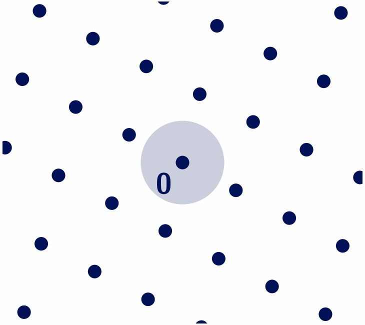
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

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

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

'Average of one non-zero point per unit volume'



Proof: Minkowski-Hlawka Theorem

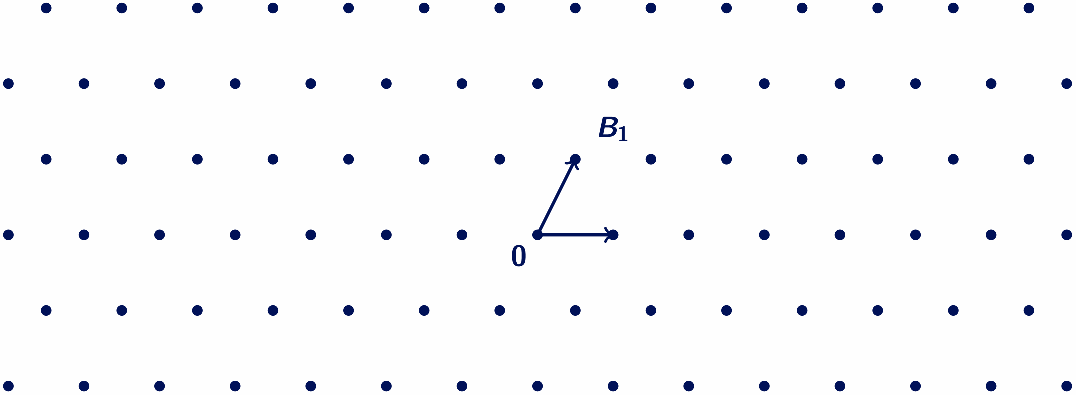
Pick $\lambda = \frac{1}{2}\,\mathrm{Mk}(n)$,

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

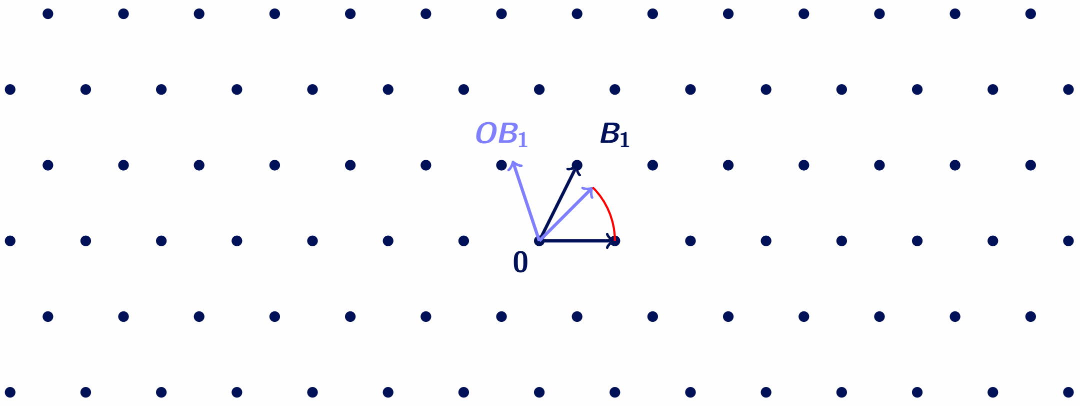
$\Rightarrow \exists \mathcal{L} \in \mathcal{L}_{[n]}$ with $\left|\mathcal{L} \cap \mathcal{B}^n_\lambda\right| \leq 2$,

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

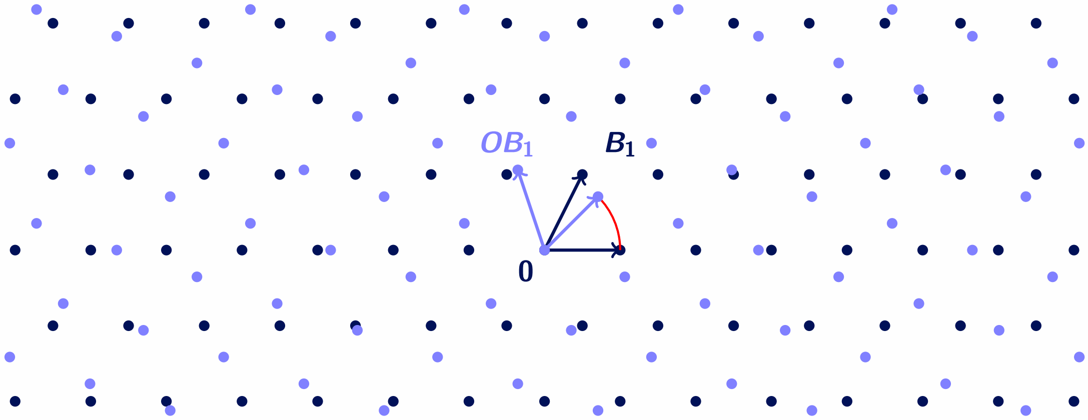
LIP and the genus of a lattice



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

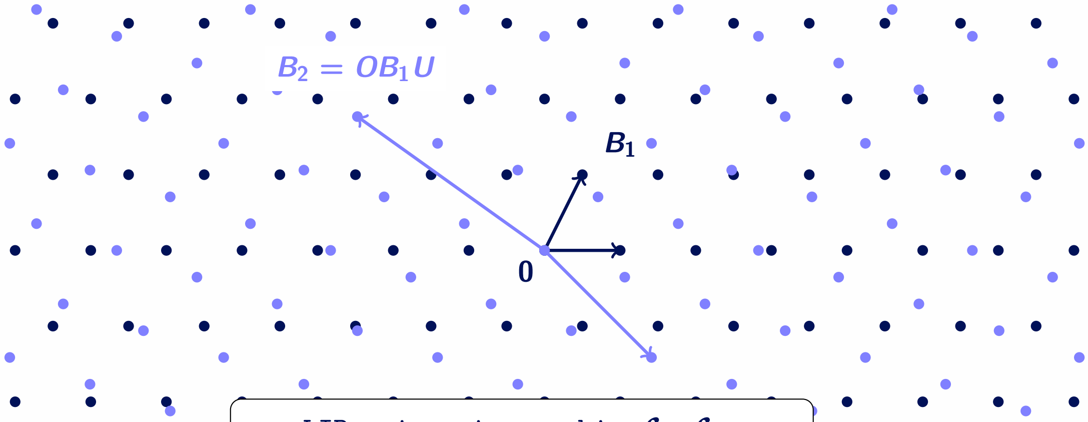


$$\mathcal{L}_1 = \mathcal{L}(B_1)$$



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

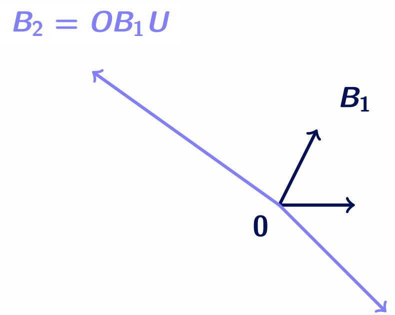
$\mathcal{L}_2 = O \cdot \mathcal{L}_1$



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

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

$\mathcal{L}_2 = O \cdot \mathcal{L}_1$

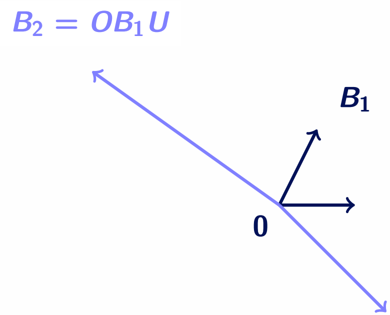


$\mathcal{L}_1 = \mathcal{L}(B_1)$

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

$\mathcal{L}_2 = O \cdot \mathcal{L}_1$

Lattice Isomorphism Problem (LIP)



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

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

$\mathcal{L}_2 = O \cdot \mathcal{L}_1$

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

Cryptography from LIP

- Idea: hide the structure of a ‘remarkable’ lattice by LIP.

Cryptography from LIP

- Idea: hide the structure of a ‘remarkable’ lattice by LIP.

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

- Decodable lattice $\Longrightarrow$ encryption scheme
- Gaussian sampleable lattice $\Longrightarrow$ 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

- Idea: hide the structure of a 'remarkable' lattice by LIP.

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

- Decodable lattice $\implies$ encryption scheme
- Gaussian sampleable lattice $\implies$ 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

- Idea: hide the structure of a 'remarkable' lattice by LIP.

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

- Decodable lattice $\implies$ encryption scheme
- Gaussian sampleable lattice $\implies$ 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 $\mathbb{Z}^n$

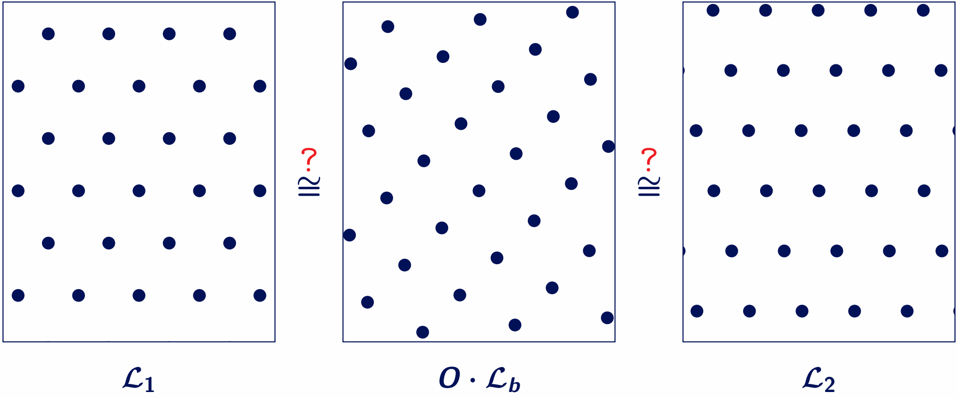
- now in round 2 of NIST call for additional signatures

- Many other works using LIP appeared recently

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.



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.

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.

Usual security assumption:

Given:

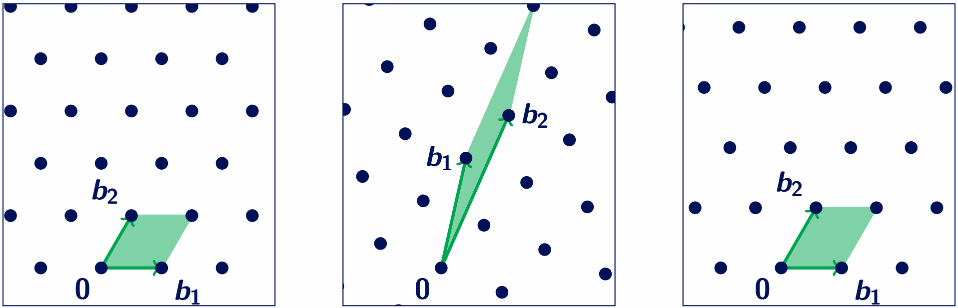
1. some remarkable lattice $\mathcal{L}_1$
2. an auxiliary lattice $\mathcal{L}_2$ with certain (good) geometric properties

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

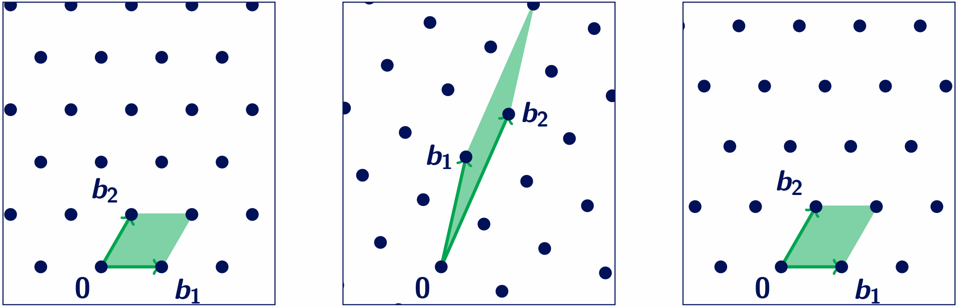
Example: good packing, smoothing, covering..

Invariants



$$\det(\mathcal{L}_1) \stackrel{?}{=} \det(O \cdot \mathcal{L}_b) \stackrel{?}{=} \det(\mathcal{L}_2)$$

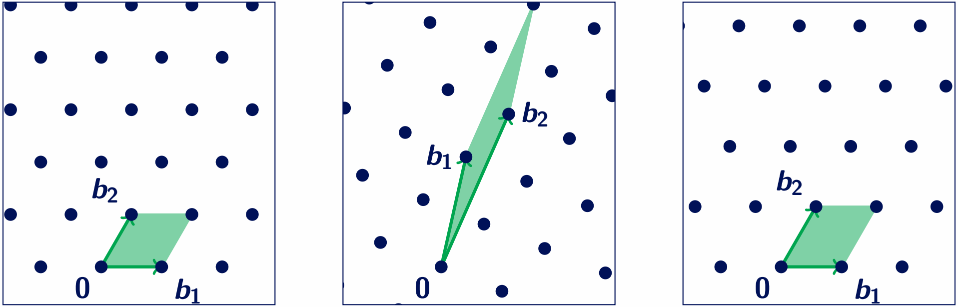
Invariants



$$\det(\mathcal{L}_1) \stackrel{?}{=} \det(O \cdot \mathcal{L}_b) \stackrel{?}{=} \det(\mathcal{L}_2)$$

Lemma:

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



$$\det(\mathcal{L}_1) \stackrel{?}{=} \det(O \cdot \mathcal{L}_b) \stackrel{?}{=} \det(\mathcal{L}_2)$$

Lemma:

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

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

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

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: $\langle x, y \rangle \in \mathbb{Z}$ for all $x, y \in \mathcal{L}$

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

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

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 $\mathbf{det}(\mathcal{L})^2$ is known.)

Genus

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

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 $\mathcal{L} \in \mathsf{gen}(\mathbb{Z}^n)$ with

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

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

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

- $\lambda_1(\mathcal{L}) \geq \Omega(\mathsf{Mk}(\mathcal{L})/\sqrt{\log(n)})$, 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 $\mathcal{L} \in \mathbf{gen}(\mathbb{Z}^n)$ with

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

Motivation

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

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

- $\lambda_1(\mathcal{L}) \geq \Omega(\mathsf{Mk}(\mathcal{L})/\sqrt{\log(n)})$, 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 $\mathcal{L} \in \mathbf{gen}(\mathbb{Z}^n)$ with

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

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

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

- $\lambda_1(\mathcal{L}) = \mathsf{Mk}(\mathcal{L})/\theta(1)$ 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 $\mathcal{L} \in \mathbf{gen}(\mathbb{Z}^n)$ with

- $\lambda_1(\mathcal{L}) \geq \Omega(\mathsf{Mk}(\mathcal{L})/\sqrt{\log(n)})$, 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 $\mathcal{L} \in \mathbf{gen}(\mathbb{Z}^n)$ with

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

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

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

- $\lambda_1(\mathcal{L}) = \mathsf{Mk}(\mathcal{L})/\theta(1)$ 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 $\mathbf{det}(\mathcal{G})^2$)

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 $n \to \infty$

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

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

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

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

Definition: distribution over Genus

Let $w(\mathcal{L}) =: 1/|\mathrm{Aut}(\mathcal{L})|$. 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 $\mathrm{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p. Let $C = \frac{7\zeta(3)}{9\zeta(2)} \approx 0.57$. Then there exists a $\mathcal{L} \in \mathcal{G}$ with

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

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

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

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

- 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 $\mathrm{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p. Let $C = \frac{7\zeta(3)}{9\zeta(2)} \approx 0.57$. Then there exists a $\mathcal{L} \in \mathcal{G}$ with

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

- 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 $\mathrm{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p. Let $C = \frac{7\zeta(3)}{9\zeta(2)} \approx 0.57$. Then there exists a $\mathcal{L} \in \mathcal{G}$ with

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

- 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

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

- 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

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

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

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

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

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

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 $\mathrm{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p. Then

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

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

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

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 $\mathrm{rk}_{\mathcal{F}_p}(\mathcal{G}) \geq 6$ for all primes p. Then

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

- 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

$\implies$ 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

$\Longrightarrow$ 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

$\Longrightarrow$ usefull for instantiating LIP-based cryptography

'Random lattices in a genus behave like fully random lattices'

Thanks!