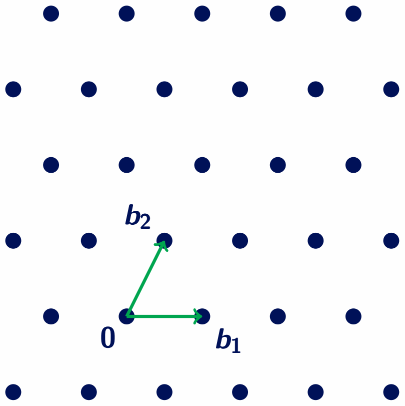
Dense (and smooth) lattices in any genus

Wessel van Woerden (PQShield).

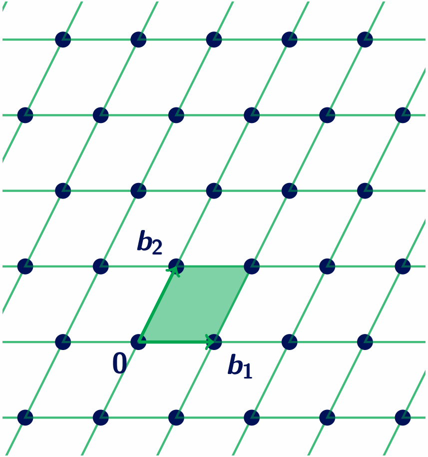


Lattice

$\mathbb{R}$-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 $G := B^t B$



Lattice

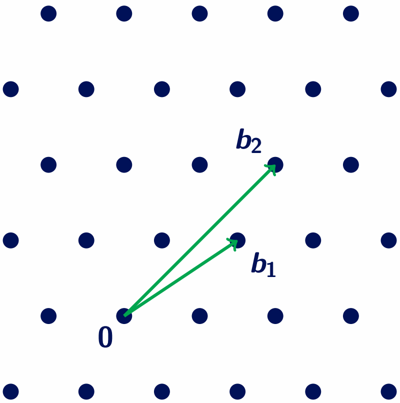
$\mathbb{R}$-linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$

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

basis B, gram matrix $G := B^t B$

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, gram matrix $G := B^t B$

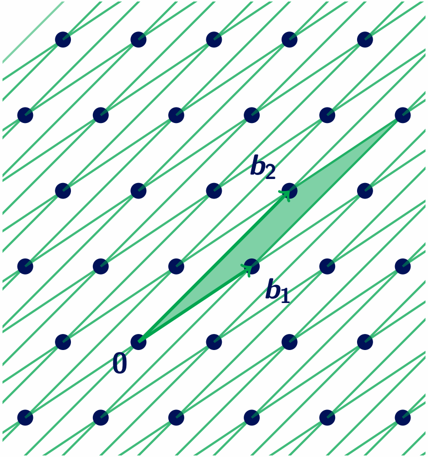
Lattice (co)volume

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

Infinitely many distinct bases

$$B' = B \cdot U, \quad G' = U^t G U,$$

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



Lattice

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

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

basis B, gram matrix $G := B^t B$

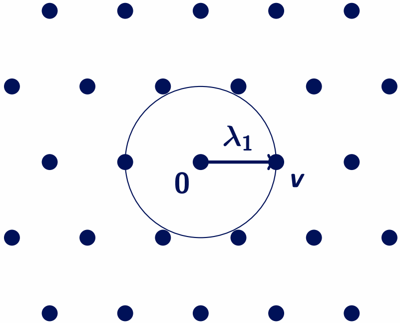
Lattice (co)volume

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

Infinitely many distinct bases

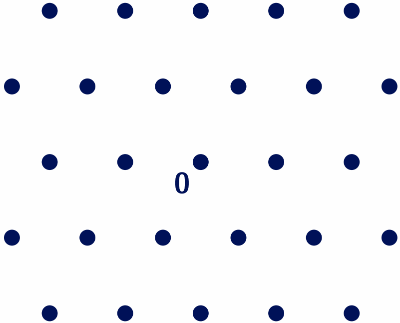
$$B' = B \cdot U, \quad G' = U^t G U,$$

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



First minimum & theta series

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

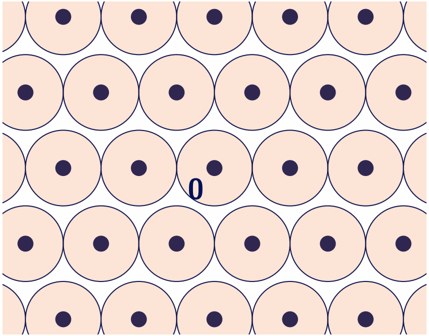


First minimum & theta series

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

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

Lattice packings



First minimum & theta series

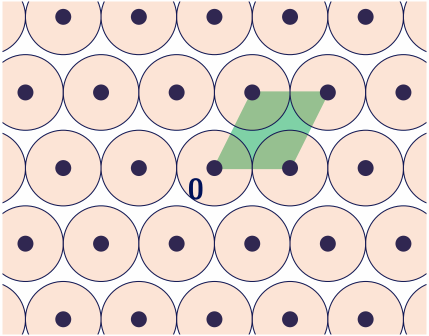
$$\lambda_1(\mathcal{L}) := \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|_2$$

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

Packing density

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

Lattice packings



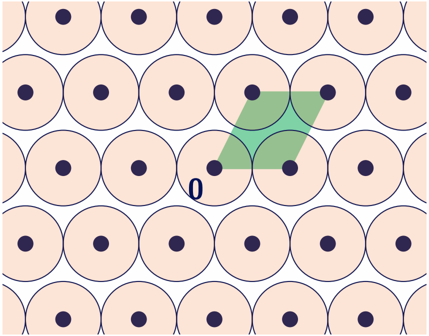
First minimum & theta series

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

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

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 & theta series

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

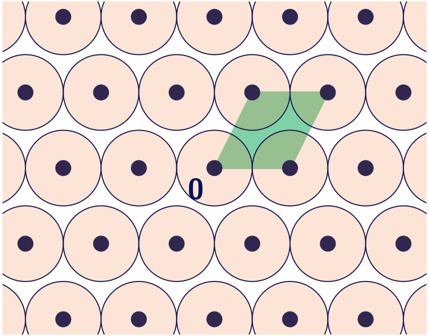
$$\theta_{\mathcal{L}}(q) := \sum_{x \in \mathcal{L}} q^{\|x\|^2} = 1 + N_{\lambda_1} q^{\lambda_1^2} + \ldots$$

Packing density

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

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

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



First minimum & theta series

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

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

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-Hlawka Theorem

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

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

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

Good packings from random lattices

- Observation: ‘random’ lattices are good packings

Good packings from random lattices

- Observation: ‘random’ lattices are good packings
  - Gaussian Heuristic: $\lambda_1(\mathcal{L}) \approx \mathrm{gh}(\mathcal{L})$

Good packings from random lattices

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

Good packings from random lattices

- Observation: ‘random’ lattices are good packings
  - Gaussian Heuristic: $\lambda_1(\mathcal{L}) \approx \mathbf{gh}(\mathcal{L})$
- Seen as the hardest instances for lattice problems

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

Good packings from random lattices

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

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

$\uparrow$

Seems harder?
Actually easier!

- Crypto: random q-ary lattices (LWE, SIS, NTRU) (WC to AC reductions)

Good packings from random lattices

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

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

↑ Seems harder? Actually easier!

- Crypto: random q-ary lattices (LWE, SIS, NTRU) (WC to AC reductions)

Definition (Siegel 1945): Haar measure

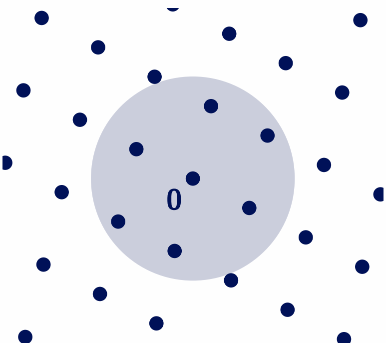
The Haar measure on $\mathcal{SL}_n(\mathbb{R})$ has finite mass on the quotient space of unit volume lattices $\mathcal{L}_{[n]} = \mathcal{SL}_n(\mathbb{R})/\mathcal{SL}_n(\mathbb{Z})$.

Average number of lattice points: Hlawka43, Siegel45

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

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

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



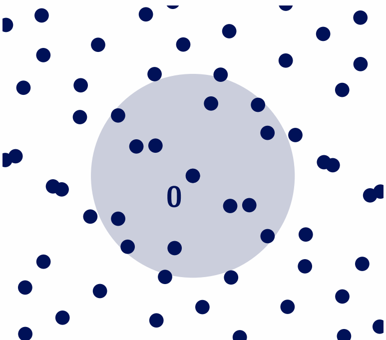
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

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

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

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

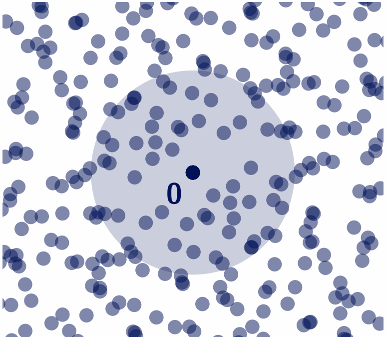


Average number of lattice points: Hlawka43, Siegel45

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

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

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



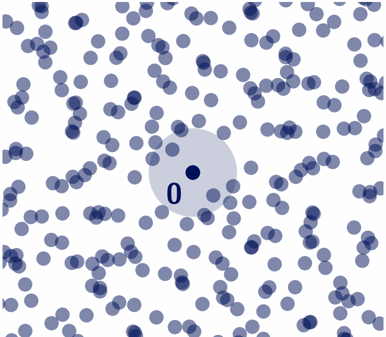
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

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

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

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



Proof: Minkowski-Hlawka Theorem

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

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

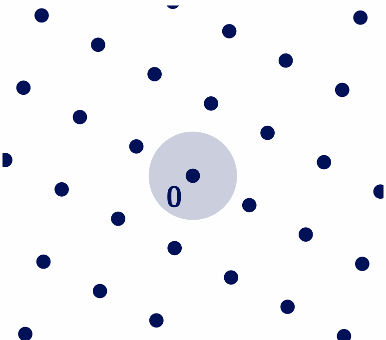
Averaging formula and the Minkowski-Hlawka Theorem

Average number of lattice points: Hlawka43, Siegel45

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

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

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



Proof: Minkowski-Hlawka Theorem

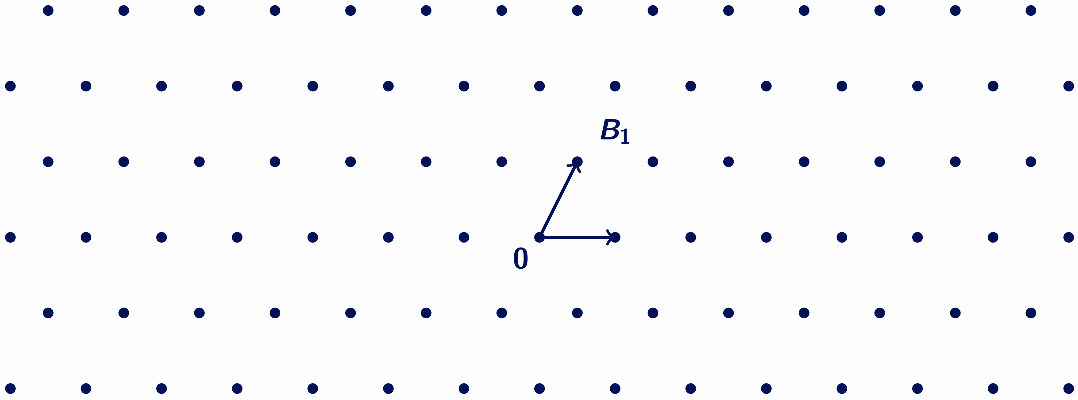
Pick $\lambda = \frac{1}{2}\mathrm{Mk}(n)$,

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

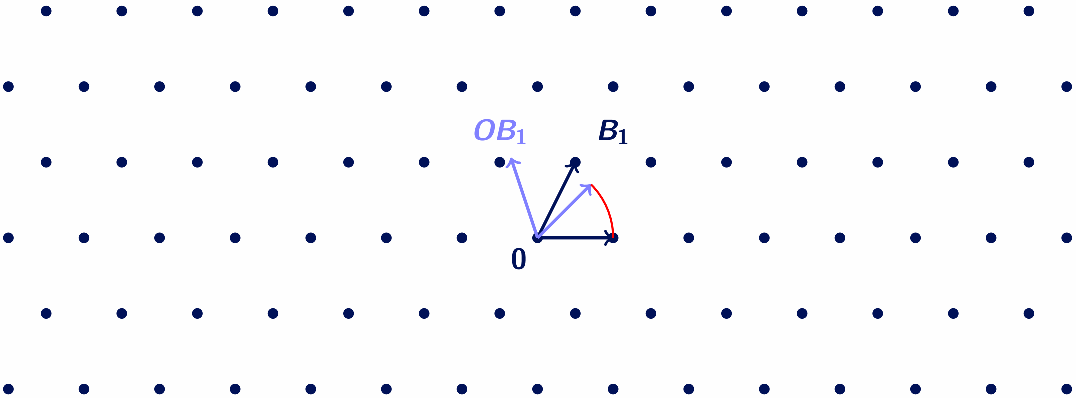
$\Rightarrow \exists \mathcal{L} \in \mathcal{L}_{[n]}$ with $|\mathcal{L} \cap \lambda \cdot \mathcal{B}^n| \leq 2$,

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

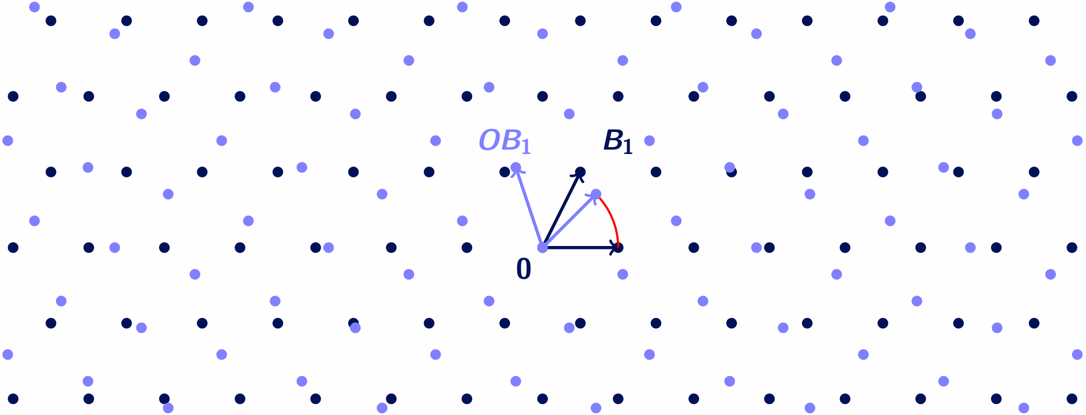
LIP and the genus of a lattice



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

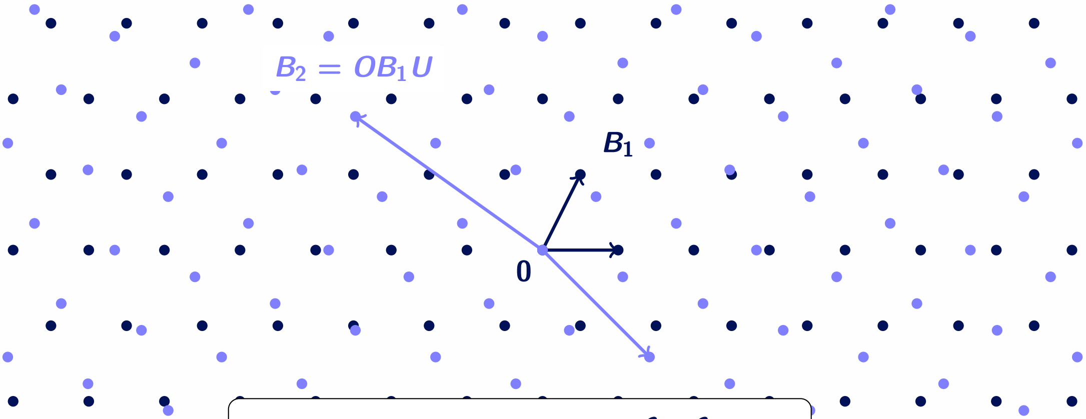


$$\mathcal{L}_1 = \mathcal{L}(B_1)$$



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

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

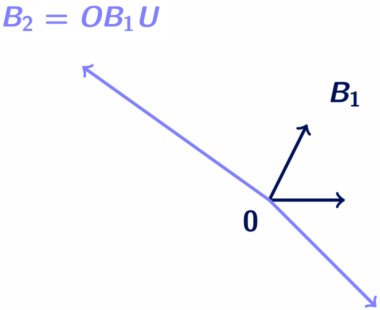


$\mathcal{L}_1 = \mathcal{L}(B_1)$

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

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

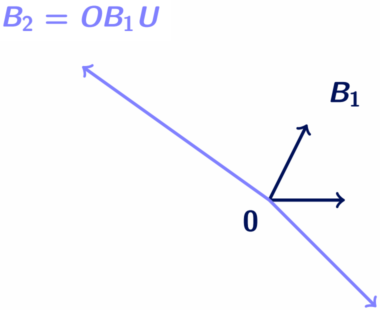
Lattice Isomorphism Problem (LIP)



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

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

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



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

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

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

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

Lattice Isomorphism Problem

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

$$\Longleftrightarrow$$

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

$$\Longleftrightarrow$$

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

Lattice Isomorphism Problem

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

$$\iff$$

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

$$\iff$$

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

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

Lattice Isomorphism Problem

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

$$\iff$$

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

$$\iff$$

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

$$\iff$$

$$U^t B_1^t B_1 U = \underbrace{B_2^t B_2}_{\text{gram matrix}} \qquad \text{for some } U \in \mathrm{GL}_n(\mathbb{Z})$$

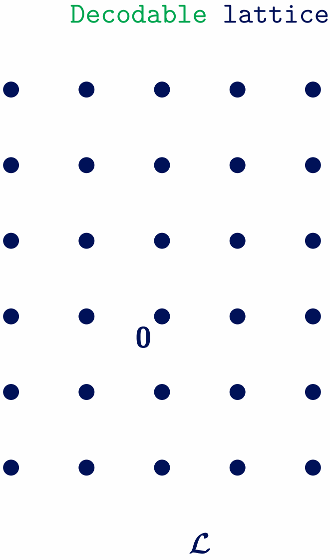
- If either O or U is known or trivial: linear algebra.
- Use gram matrix formulation to only consider U.

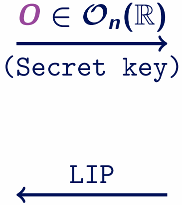
Lattice Isomorphism Problem

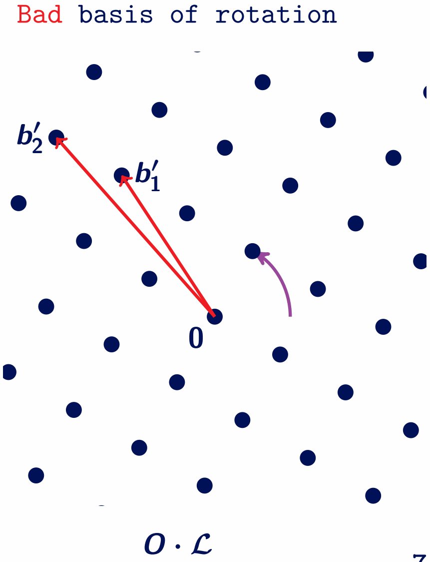
$$\mathcal{L}(B_1) \cong \mathcal{L}(B_2)$$
$$\Longleftrightarrow$$
$$O \cdot \mathcal{L}(B_1) = \mathcal{L}(B_2) \quad \text{for some } O \in O_n(\mathbb{R})$$
$$\Longleftrightarrow$$
$$O \cdot B_1 \cdot U = B_2 \quad \text{for some } O \in O_n(\mathbb{R}), U \in \mathrm{GL}_n(\mathbb{Z})$$
$$\Longleftrightarrow$$
$$U^t B_1^t B_1 U = \underbrace{B_2^t B_2}_{\text{gram matrix}} \quad \text{for some } U \in \mathrm{GL}_n(\mathbb{Z})$$

- If either O or U is known or trivial: linear algebra.
- Use gram matrix formulation to only consider U.
- We restrict to integer gram matrices $G := B^t B$.

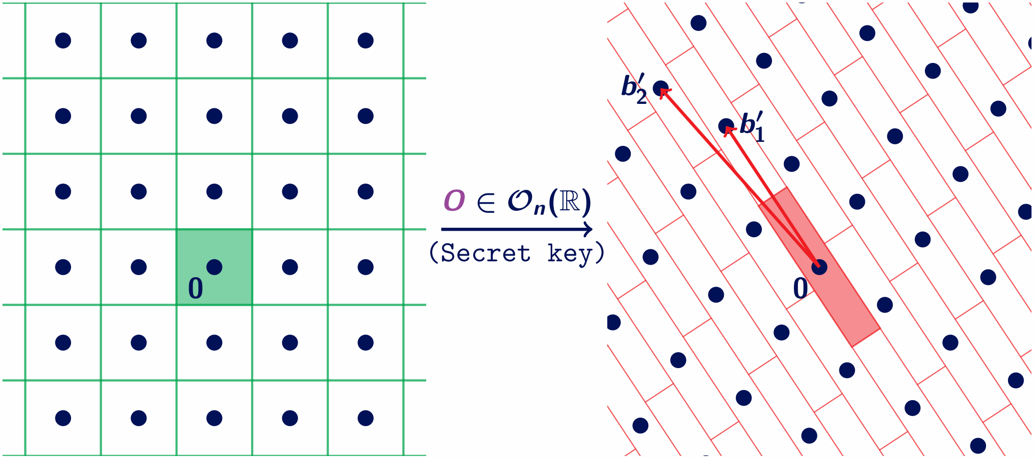
Encryption scheme from LIP (informal)





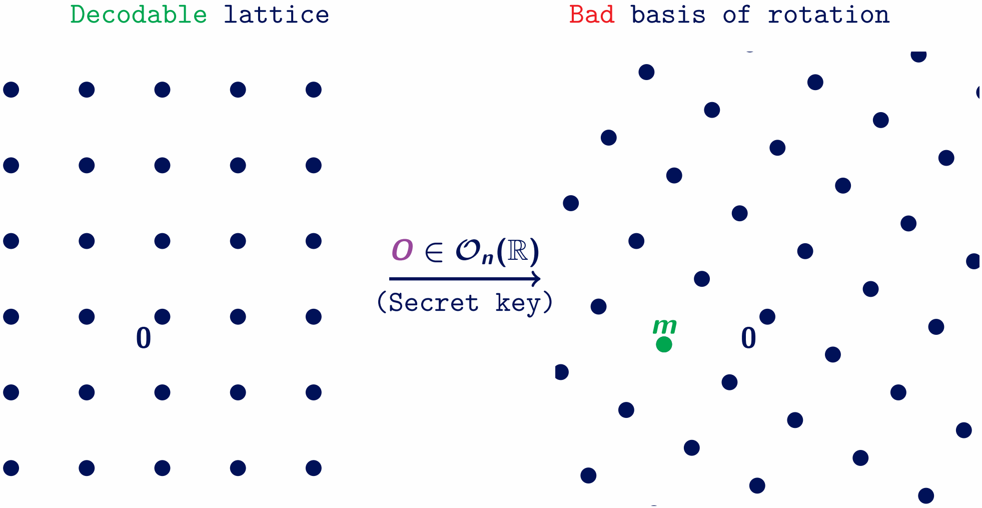


Decodable lattice | Bad basis of rotation



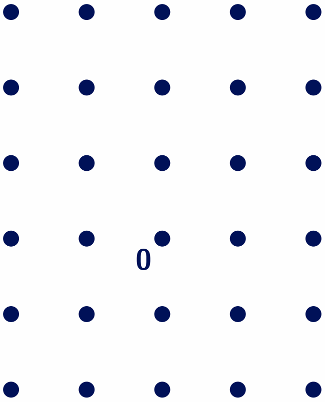
Hides (decoding) structure of $\mathcal{L}$

Encryption scheme from LIP (informal)



Encryption scheme from LIP (informal)

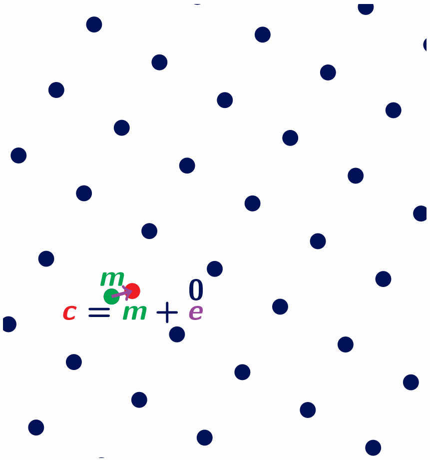
Decodable lattice



$\boldsymbol{O} \in \mathcal{O}_n(\mathbb{R})$

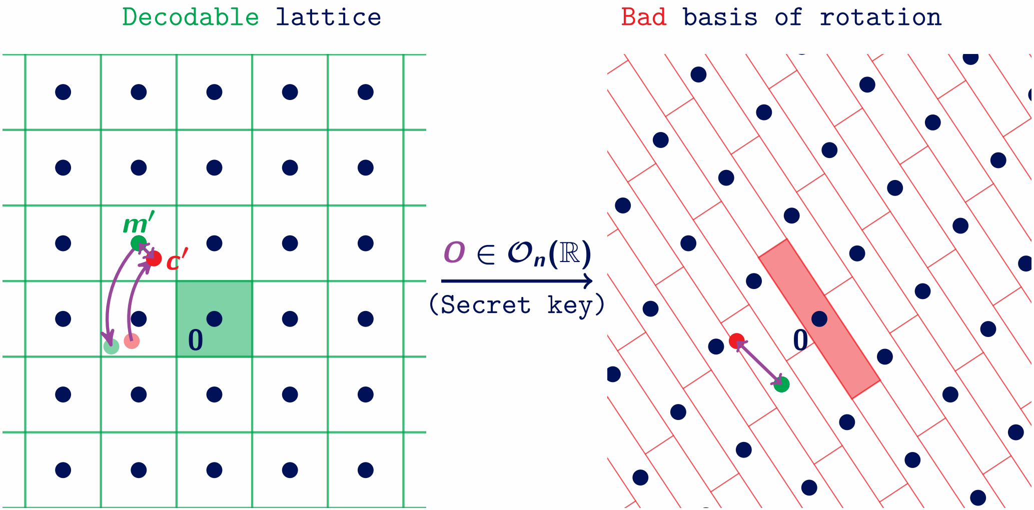
(Secret key)

Bad basis of rotation



Encrypt by adding a small error

Encryption scheme from LIP (informal)



Decrypt using decoding algorithm

Cryptography from LIP

- 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

- 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 $\mathbb{Z}^n$

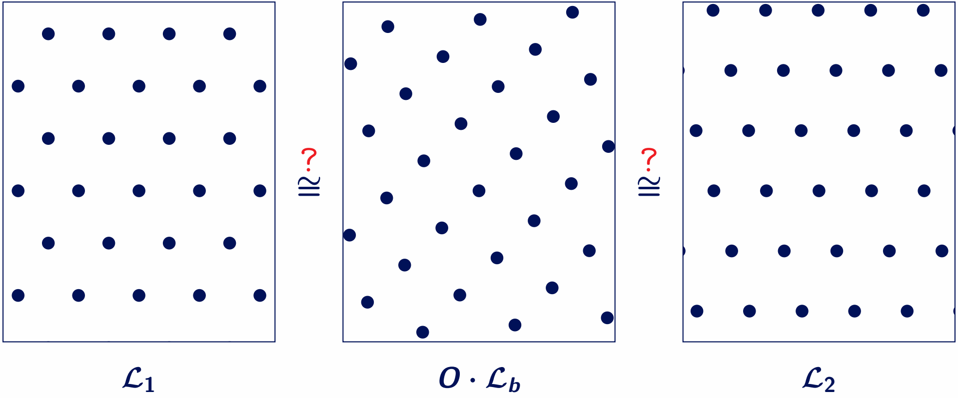
- now in round 2 of NIST call for additional signatures

- 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.



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 $\boldsymbol{b} \leftarrow \{1, 2\}$ uniform.
Given $\mathcal{L} \in [\mathcal{L}_b]$, recover $\boldsymbol{b}$.

Usual security assumption:

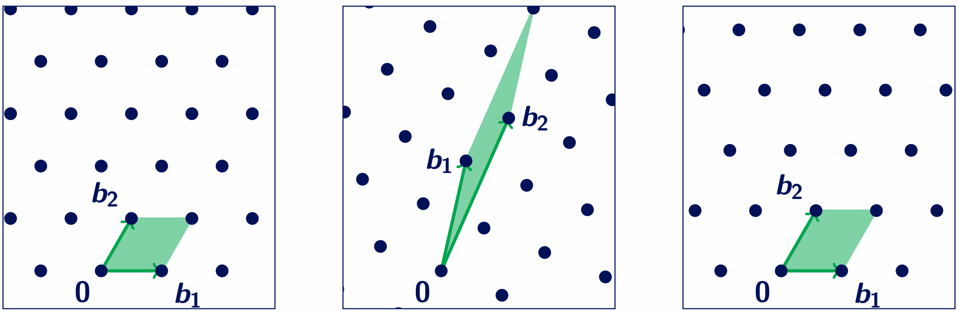
Given:

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.

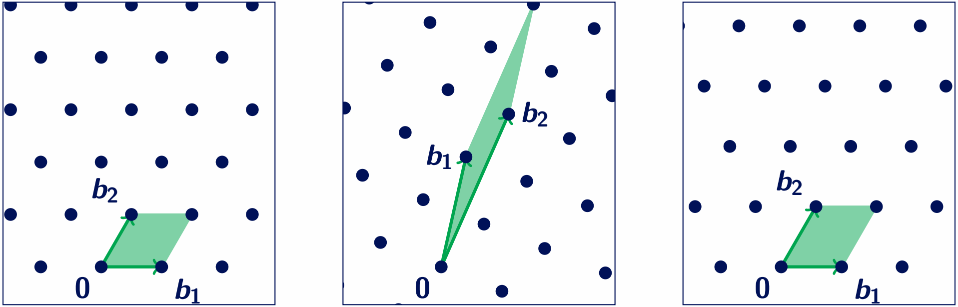
Goal: find an auxiliary lattice with the right geometric properties

Example: good packing, smoothing, covering..



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

Invariants

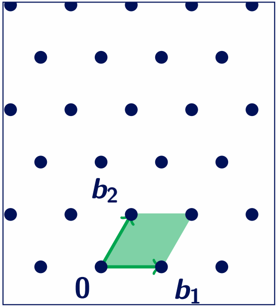


$$\det(\mathcal{L}_1) \stackrel{?}{=} \det(O \cdot \mathcal{L}_b) \stackrel{?}{=} \det(\mathcal{L}_2)$$

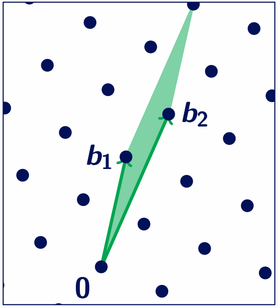
Lemma:

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

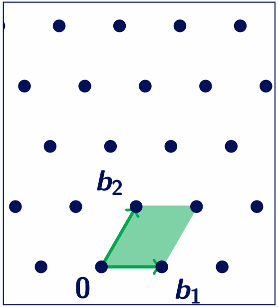
Invariants



$\det(\mathcal{L}_1) \overset{?}{=}$



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



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

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

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. ($\Leftrightarrow$ $U^t G_1 U = G_2$ for some $U \in \mathcal{GL}_n(\mathbb{Z}_p)$)

- 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. ($\Leftrightarrow U^t G_1 U = G_2$ for some $U \in \mathcal{GL}_n(\mathbb{Z}_p)$)

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. ($\Leftrightarrow U^t G_1 U = G_2$ for some $U \in \mathcal{GL}_n(\mathbb{Z}_p)$)

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: $\langle x, y \rangle \in \mathbb{Z}$ 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. ($\Leftrightarrow$ $U^t G_1 U = G_2$ for some $U \in \mathcal{GL}_n(\mathbb{Z}_p)$)

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*

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. ($\Leftrightarrow$ $U^t G_1 U = G_2$ for some $U \in \mathcal{GL}_n(\mathbb{Z}_p)$)

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*

How restricting is the genus invariant?

Dense lattices in any genus

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 $\varepsilon < n^{-\omega(1)}$?

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

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

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

Mass formula and the size of 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 $\det(\mathcal{G})^2$.

Mass formula and the size of 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 $\det(\mathcal{G})^2$.

- **Lemma:** $|\mathcal{G}| \geq 2M(\mathcal{G})$. Proof: $|\mathrm{Aut}(\mathcal{L})| \geq 2$. □

Mass formula and the size of 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 $\det(\mathcal{G})^2$.

- Lemma: $|\mathcal{G}| \geq 2M(\mathcal{G})$. Proof: $|\mathrm{Aut}(\mathcal{L})| \geq 2$. □
- Example: $M(\mathrm{Gen}(\mathbb{Z}^{32})) \approx 4.33 \cdot 10^{16}$
  $M(\mathrm{Gen}(\mathbb{Z}^{40})) \approx 1.21 \cdot 10^{63}$

Mass formula and the size of 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 $\det(\mathcal{G})^2$.

- Lemma: $|\mathcal{G}| \geq 2M(\mathcal{G})$. Proof: $|\mathrm{Aut}(\mathcal{L})| \geq 2$. □
- Example: $M(\mathrm{Gen}(\mathbb{Z}^{32})) \approx 4.33 \cdot 10^{16}$

  $M(\mathrm{Gen}(\mathbb{Z}^{40})) \approx 1.21 \cdot 10^{63}$
- Grows fast: $M(\mathcal{G}) \geq n^{\Omega(n^2)}$ as $n \to \infty$

Mass formula and the size of 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 $\det(\mathcal{G})^2$.

- Lemma: $|\mathcal{G}| \geq 2M(\mathcal{G})$. Proof: $|\mathrm{Aut}(\mathcal{L})| \geq 2$. $\square$
- Example: $M(\mathrm{Gen}(\mathbb{Z}^{32})) \approx 4.33 \cdot 10^{16}$

  $M(\mathrm{Gen}(\mathbb{Z}^{40})) \approx 1.21 \cdot 10^{63}$
- Grows fast: $M(\mathcal{G}) \geq n^{\Omega(n^2)}$ as $n \to \infty$
- Enormous number of isomorphism classes in same genus

Mass formula and the size of 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 $\det(\mathcal{G})^2$.

- Lemma: $|\mathcal{G}| \geq 2M(\mathcal{G})$. Proof: $|\mathrm{Aut}(\mathcal{L})| \geq 2$. □
- Example: $M(\mathrm{Gen}(\mathbb{Z}^{32})) \approx 4.33 \cdot 10^{16}$

  $M(\mathrm{Gen}(\mathbb{Z}^{40})) \approx 1.21 \cdot 10^{63}$
- Grows fast: $M(\mathcal{G}) \geq n^{\Omega(n^2)}$ as $n \to \infty$
- Enormous number of isomorphism classes in same genus
- Question: do these behave like random lattices?

Random distribution over genus

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 $\frac{w(\mathcal{L})}{M(\mathcal{G})}$.

Random distribution over genus

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 $\frac{w(\mathcal{L})}{M(\mathcal{G})}$.

- Coincides with the distribution of random lattices (Haar measure) restricted to a single genus.

Random distribution over genus

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 $\frac{w(\mathcal{L})}{M(\mathcal{G})}$.

- Coincides with the distribution of random lattices (Haar measure) restricted to a single genus.
- Can be sampled from efficiently.

  (limit distribution of randomized Kneser's p-neighbouring method)

Random distribution over genus

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 $\frac{w(\mathcal{L})}{M(\mathcal{G})}$.

- Coincides with the distribution of random lattices (Haar measure) restricted to a single genus.
- Can be sampled from efficiently.
  (limit distribution of randomized Kneser's p-neighbouring method)
- Comes with similar average point counting results!
  ($\implies$ Minkowski-Hlawka like theorem?)

Kneser p-neighbouring (1957) and sampling

- Two integral lattices $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours $\mathcal{L}_1 \sim_p \mathcal{L}_2$ if

$$[\mathcal{L}_1 : \mathcal{L}_1 \cap \mathcal{L}_2] = [\mathcal{L}_2 : \mathcal{L}_1 \cap \mathcal{L}_2] = p.$$

Kneser p-neighbouring (1957) and sampling

- Two integral lattices $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours $\mathcal{L}_1 \sim_p \mathcal{L}_2$ if

$$[\mathcal{L}_1 : \mathcal{L}_1 \cap \mathcal{L}_2] = [\mathcal{L}_2 : \mathcal{L}_1 \cap \mathcal{L}_2] = p.$$

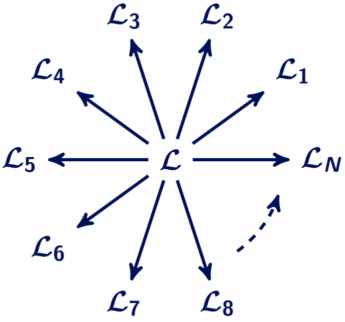
- If $\mathcal{L}_1 \sim_p \mathcal{L}_2$ then $\mathbf{Gen}(\mathcal{L}_1) = \mathbf{Gen}(\mathcal{L}_2)$.

Kneser p-neighbouring (1957) and sampling

- Two integral lattices $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours $\mathcal{L}_1 \sim_p \mathcal{L}_2$ if

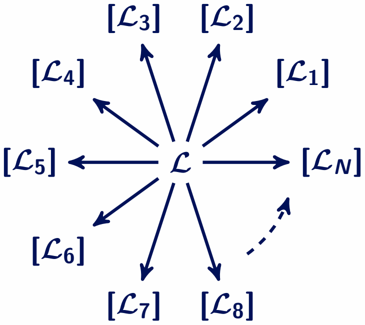
$$[\mathcal{L}_1 : \mathcal{L}_1 \cap \mathcal{L}_2] = [\mathcal{L}_2 : \mathcal{L}_1 \cap \mathcal{L}_2] = p.$$

- If $\mathcal{L}_1 \sim_p \mathcal{L}_2$ then $\mathbf{Gen}(\mathcal{L}_1) = \mathbf{Gen}(\mathcal{L}_2)$.
- A lattice has $\sim p^{n-2}$ p-neighours ($\leftrightarrow$ isotropic lines in $\mathcal{L}/p\mathcal{L}$).



Kneser p-neighbouring (1957) and sampling

- Two integral lattices $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours $\mathcal{L}_1 \sim_p \mathcal{L}_2$ if
$$[\mathcal{L}_1 : \mathcal{L}_1 \cap \mathcal{L}_2] = [\mathcal{L}_2 : \mathcal{L}_1 \cap \mathcal{L}_2] = p.$$
- If $\mathcal{L}_1 \sim_p \mathcal{L}_2$ then $\mathbf{Gen}(\mathcal{L}_1) = \mathbf{Gen}(\mathcal{L}_2)$.
- A lattice has $\sim p^{n-2}$ p-neighours ($\leftrightarrow$ isotropic lines in $\mathcal{L}/p\mathcal{L}$).

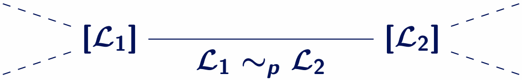


Kneser p-neighbouring (1957) and sampling

- Two integral lattices $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours $\mathcal{L}_1 \sim_p \mathcal{L}_2$ if

$$[\mathcal{L}_1 : \mathcal{L}_1 \cap \mathcal{L}_2] = [\mathcal{L}_2 : \mathcal{L}_1 \cap \mathcal{L}_2] = p.$$

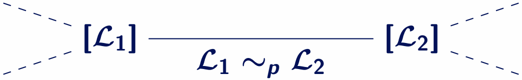
- If $\mathcal{L}_1 \sim_p \mathcal{L}_2$ then $\mathbf{Gen}(\mathcal{L}_1) = \mathbf{Gen}(\mathcal{L}_2)$.
- A lattice has $\sim p^{n-2}$ p-neighours ($\leftrightarrow$ isotropic lines in $\mathcal{L}/p\mathcal{L}$).
- Turns any genus into a graph with nodes $[\mathcal{L}_1], \ldots, [\mathcal{L}_N]$ and an edge $([\mathcal{L}_i], [\mathcal{L}_j])$ if $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours up to isometry.



- Two integral lattices $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours $\mathcal{L}_1 \sim_p \mathcal{L}_2$ if

$$[\mathcal{L}_1 : \mathcal{L}_1 \cap \mathcal{L}_2] = [\mathcal{L}_2 : \mathcal{L}_1 \cap \mathcal{L}_2] = p.$$

- If $\mathcal{L}_1 \sim_p \mathcal{L}_2$ then $\mathbf{Gen}(\mathcal{L}_1) = \mathbf{Gen}(\mathcal{L}_2)$.
- A lattice has $\sim p^{n-2}$ p-neighours ($\leftrightarrow$ isotropic lines in $\mathcal{L}/p\mathcal{L}$).
- Turns any genus into a graph with nodes $[\mathcal{L}_1], \ldots, [\mathcal{L}_N]$ and an edge $([\mathcal{L}_i], [\mathcal{L}_j])$ if $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours up to isometry.



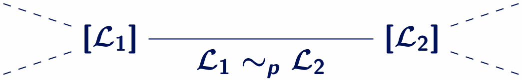
- Random walk: $\mathcal{L}_1 \sim_p \mathcal{L}_2 \sim_p \ldots \sim_p \mathcal{L}_k$ where $\mathcal{L}_{i+1}$ is a uniformly random p-neighbour of $\mathcal{L}_i$.

Kneser p-neighbouring (1957) and sampling

- Two integral lattices $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours $\mathcal{L}_1 \sim_p \mathcal{L}_2$ if

$$[\mathcal{L}_1 : \mathcal{L}_1 \cap \mathcal{L}_2] = [\mathcal{L}_2 : \mathcal{L}_1 \cap \mathcal{L}_2] = p.$$

- If $\mathcal{L}_1 \sim_p \mathcal{L}_2$ then $\mathbf{Gen}(\mathcal{L}_1) = \mathbf{Gen}(\mathcal{L}_2)$.
- A lattice has $\sim p^{n-2}$ p-neighours ($\leftrightarrow$ isotropic lines in $\mathcal{L}/p\mathcal{L}$).
- Turns any genus into a graph with nodes $[\mathcal{L}_1], \ldots, [\mathcal{L}_N]$ and an edge $([\mathcal{L}_i], [\mathcal{L}_j])$ if $\mathcal{L}_1, \mathcal{L}_2$ are p-neighbours up to isometry.



- Random walk: $\mathcal{L}_1 \sim_p \mathcal{L}_2 \sim_p \ldots \sim_p \mathcal{L}_k$ where $\mathcal{L}_{i+1}$ is a uniformly random p-neighbour of $\mathcal{L}_i$.
- For large enough p, a random walk has limit distribution $\mathcal{D}(\mathcal{G})$.
  $\implies$ efficient sampling algorithm for $\mathcal{D}(\mathcal{G})$.

Results - 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 $\mathrm{rk}_{\mathbb{F}_p}(\mathcal{G}) \geq 6$ 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

$$\lambda_1(\mathcal{L})^2 \geq \left\lceil (C \cdot \det(\mathcal{L})/\omega_n)^{2/n} \right\rceil \approx n/2\pi e \cdot \det(\mathcal{L})^{2/n} = \mathrm{gh}(\mathcal{L})^2.$$

Results - 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 $\mathrm{rk}_{\mathbb{F}_p}(\mathcal{G}) \geq 6$ 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

$$\lambda_1(\mathcal{L})^2 \geq \left\lceil (C \cdot \det(\mathcal{L})/\omega_n)^{2/n} \right\rceil \approx n/2\pi e \cdot \det(\mathcal{L})^{2/n} = \mathrm{gh}(\mathcal{L})^2.$$

- Essentially matches packing density of a random lattice.

Results - 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 $\mathrm{rk}_{\mathbb{F}_p}(\mathcal{G}) \geq 6$ 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

$$\lambda_1(\mathcal{L})^2 \geq \left\lceil (C \cdot \det(\mathcal{L})/\omega_n)^{2/n} \right\rceil \approx n/2\pi e \cdot \det(\mathcal{L})^{2/n} = \mathrm{gh}(\mathcal{L})^2.$$

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

Results - 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 $\mathrm{rk}_{\mathbb{F}_p}(\mathcal{G}) \geq 6$ 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

$$\lambda_1(\mathcal{L})^2 \geq \left\lceil (C \cdot \det(\mathcal{L})/\omega_n)^{2/n} \right\rceil \approx n/2\pi e \cdot \det(\mathcal{L})^{2/n} = \mathrm{gh}(\mathcal{L})^2.$$

- 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

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

- Similar result for smoothing parameter and covering radius.

The hammer: 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 hammer: 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 hammer: 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 (this work)

Let $\mathcal{G}$ be any genus such that $\mathrm{rk}_{\mathbb{F}_p}(\mathcal{G}) \geq 6$ 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 hammer: 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 (this work)

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

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

- Sufficient to prove main results with MH-like argument

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.

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 $n = 8k \geq 8$, B_i the i-th Bernoulli number, and $\sigma_z(m) = \sum_{d|m} d^z$ is the sum of positive divisors function, we have

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

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 $n = 8k \geq 8$, B_i the i-th Bernoulli number, and $\sigma_z(m) = \sum_{d|m} d^z$ is the sum of positive divisors function, we have

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

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

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 $n = 8k \geq 8$, B_i the i-th Bernoulli number, and $\sigma_z(m) = \sum_{d|m} d^z$ is the sum of positive divisors function, we have

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

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

Example: even unimodular case (2)

- Idea: recall that:

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

Example: even unimodular case (2)

- 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.

Example: even unimodular case (2)

- 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, $\Rightarrow \lambda_1(\mathcal{L})^2 \geq 8$.

Example: even unimodular case (2)

- 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. $\lambda_1(\mathcal{L})^2 > \lambda$.

Example: even unimodular case (3)

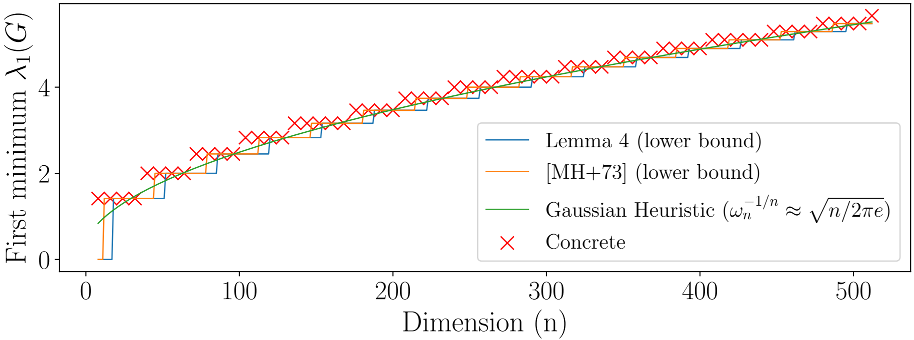
Lemma: even packing (Milnor, Serre, 73)

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

Example: even unimodular case (3)

Lemma: even packing (Milnor, Serre, 73)

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



General case: compute mass formula

- We want to count the average number of solutions N_m to $f(x) := x^t G_{\mathcal{L}} x = m$ with $x \in \mathbb{Z}^n$ when $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.

General case: compute mass formula

- We want to count the average number of solutions N_m to $f(x) := x^t G_{\mathcal{L}} x = m$ with $x \in \mathbb{Z}^n$ when $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(m)$ of solutions over $\mathbb{Z}_p$ and $\mathbb{R} = \mathbb{Z}_\infty$.

General case: compute mass formula

- We want to count the average number of solutions N_m to $f(x) := x^t G_{\mathcal{L}} x = m$ with $x \in \mathbb{Z}^n$ when $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(m)$ 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 $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_m q^m$ we have

$$N_m = \mathbb{E}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})} \left| \{x \in \mathcal{L} : \|x\|^2 = m\} \right| = \prod_{p=2,3,\dots,\infty} \delta_{\mathcal{G},p}(m)$$

General case: compute mass formula

- We want to count the average number of solutions N_m to $f(x) := x^t G_{\mathcal{L}} x = m$ with $x \in \mathbb{Z}^n$ when $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(m)$ 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 $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_m q^m$ we have

$$N_m = \mathop{\mathbb{E}}_{[\mathcal{L}]\leftarrow\mathcal{D}(\mathcal{G})} \left|\{x \in \mathcal{L} : \|x\|^2 = m\}\right| = \prod_{p=2,3,\ldots,\infty} \delta_{\mathcal{G},p}(m)$$

- Local-global principle

General case: compute mass formula

- We want to count the average number of solutions N_m to $f(x) := x^t G_{\mathcal{L}} x = m$ with $x \in \mathbb{Z}^n$ when $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(m)$ 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 $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_m q^m$ we have

$$N_m = \mathop{\mathbb{E}}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})} \left| \{x \in \mathcal{L} : \|x\|^2 = m\} \right| = \prod_{p=2,3,\ldots,\infty} \delta_{\mathcal{G},p}(m)$$

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

General case: compute mass formula

- We want to count the average number of solutions N_m to $f(x) := x^t G_{\mathcal{L}} x = m$ with $x \in \mathbb{Z}^n$ when $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$.
- Idea: compute density $\delta_{\mathcal{G},p}(m)$ 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 $\Theta_{\mathcal{G}}(q) = 1 + \sum_{y=1}^{\infty} N_m q^m$ we have

$$N_m = \mathop{\mathbb{E}}_{[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})} \left| \{x \in \mathcal{L} : \|x\|^2 = m\} \right| = \prod_{p=2,3,\ldots,\infty} \delta_{\mathcal{G},p}(m)$$

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

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

- Need: upper bound on expected number N_m of solutions.

$$N_m = \underbrace{\delta_{\mathcal{G},\infty}(m)} \cdot \underbrace{\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(m)}$$

Bounding densities

- Need: upper bound on expected number N_m of solutions.

$$N_m = \underbrace{\delta_{\mathcal{G},\infty}(m)}_{\text{main contribution}} \cdot \underbrace{\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(m)}_{\text{typically } \theta(1)}$$

Bounding densities

- Need: upper bound on expected number N_m of solutions.

$$N_m = \underbrace{\delta_{\mathcal{G},\infty}(m)}_{\sim \mathrm{vol}(\sqrt{m}\mathcal{S}^{n-1})} \cdot \underbrace{\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(m)}_{\text{typically } \theta(1)}$$

Bounding densities

- Need: upper bound on expected number N_m of solutions.

$$N_m = \underbrace{\delta_{\mathcal{G},\infty}(m)}_{\substack{\sim \text{vol}(\sqrt{m}\mathcal{S}^{n-1}) \\ \frac{1}{2} n\omega_n m^{n/2-1} \cdot \det(\mathcal{G})^{-1}}} \cdot \underbrace{\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(m)}_{\text{typically } \theta(1)}$$

- Need: upper bound on expected number N_m of solutions.

$$N_m = \underbrace{\delta_{\mathcal{G},\infty}(m)}_{\substack{\sim \mathrm{vol}(\sqrt{m}\mathcal{S}^{n-1}) \\ \frac{1}{2} n\omega_n m^{n/2-1} \cdot \det(\mathcal{G})^{-1}}} \cdot \underbrace{\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(m)}_{\substack{\leq \frac{18\zeta(2)}{7\zeta(3)} \approx 3.52 \\ \text{if } \mathrm{rk}_{\mathbb{F}_p}(\mathcal{G}) \geq 6 \ \forall p}}$$

Bounding densities

- Need: upper bound on expected number N_m of solutions.

$$N_m = \underbrace{\delta_{\mathcal{G},\infty}(m)}_{\substack{\sim \mathrm{vol}(\sqrt{m}\mathcal{S}^{n-1}) \\ \frac{1}{2} n\omega_n m^{n/2-1} \cdot \det(\mathcal{G})^{-1}}} \cdot \underbrace{\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(m)}_{\substack{\leq \frac{18\zeta(2)}{7\zeta(3)} \approx 3.52 \\ \text{if } \mathrm{rk}_{\mathbb{F}_p}(\mathcal{G}) \geq 6 \ \forall p}}$$

- Relies on classification of p-adic normal forms by Conway.

Bounding densities

- Need: upper bound on expected number N_m of solutions.

$$N_m = \underbrace{\delta_{\mathcal{G},\infty}(m)}_{\substack{\sim\mathrm{vol}(\sqrt{m}\mathcal{S}^{n-1}) \\ \frac{1}{2}n\omega_n m^{n/2-1}\cdot\det(\mathcal{G})^{-1}}} \cdot \underbrace{\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(m)}_{\substack{\leq \frac{18\zeta(2)}{7\zeta(3)}\approx 3.52 \\ \text{if } \mathrm{rk}_{\mathbb{F}_p}(\mathcal{G})\geq 6\ \forall p}}$$

- Relies on classification of p-adic normal forms by Conway.
- Sufficient to prove the main results

Bounding densities

- Need: upper bound on expected number N_m of solutions.

$$N_m = \underbrace{\delta_{\mathcal{G},\infty}(m)}_{\substack{\sim \mathrm{vol}(\sqrt{m}\mathcal{S}^{n-1}) \\ \frac{1}{2} n\omega_n m^{n/2-1} \cdot \det(\mathcal{G})^{-1}}} \cdot \underbrace{\prod_{p=2,3,\ldots} \delta_{\mathcal{G},p}(m)}_{\substack{\leq \frac{18\zeta(2)}{7\zeta(3)} \approx 3.52 \\ \text{if } \mathrm{rk}_{\mathbb{F}_p}(\mathcal{G}) \geq 6 \ \forall p}}$$

- Relies on classification of p-adic normal forms by Conway.
- Sufficient to prove the main results
- Conjecture: remove conditions $\Longrightarrow$ extra factor $\mathbf{poly}(m)$

  (but rather tedious to work out)

Open Questions

Better invariants:

Can we construct stronger efficiently computable invariants?

Open Questions

Better invariants:

Can we construct stronger efficiently computable invariants?

Structured case:

What about module lattices? (e.g. Hermitian forms over CM fields)

Open Questions

Better invariants:

Can we construct stronger efficiently computable invariants?

Structured case:

What about module lattices? (e.g. Hermitian forms over CM fields)

WC-AC reductions:

- the random case $[\mathcal{L}] \leftarrow \mathcal{D}(\mathcal{G})$ is heuristically the hardest.
- from any class $[\mathcal{L}] \in \mathcal{G}$ we can efficiently step to a random class.

Can we make a worst-case to average-case reduction within a genus?

Example: SVP, SIVP, LIP

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 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 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 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

- Lots of other deep theory behind it: randomness, Kneser p-neighbouring, modular forms, more general mass formula's, ...

Conclusion

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

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

- Lots of other deep theory behind it: randomness, Kneser $\boldsymbol{p}$-neighbouring, modular forms, more general mass formula's, ...

  '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 Siegel-Weil mass formula we can show for any genus:

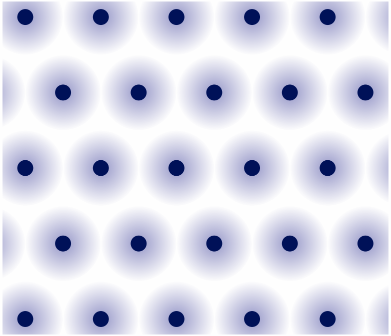
- $\exists$ good primal and dual packings
- $\exists$ good smoothing
- $\exists$ good coverings

$\Longrightarrow$ usefull for instantiating LIP-based cryptography

- Lots of other deep theory behind it: randomness, Kneser p-neighbouring, modular forms, more general mass formula's, ...

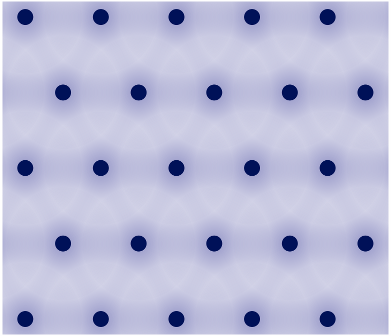
‘Random lattices in a genus behave like fully random lattices’

Thanks!



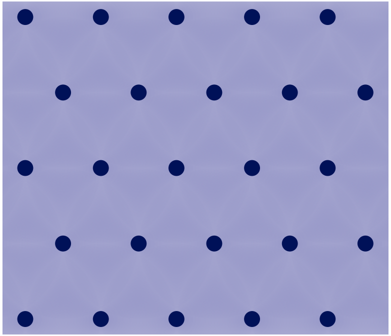
Smoothing parameter

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



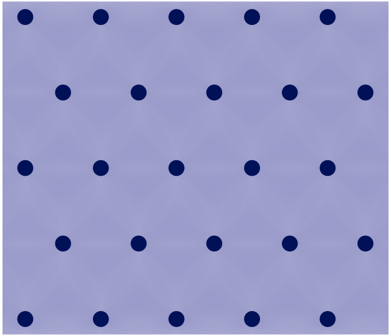
<u>Smoothing parameter</u>

'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

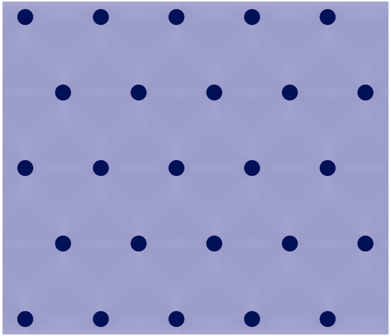
'minimum $s > 0$ such that centered Gaussian with width s is ϵ-close to uniform over $\mathbb{R}^n/\mathcal{L}$'

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

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 $\eta_\varepsilon(\mathcal{L}) \leq (\det(\mathcal{L})/\varepsilon)^{1/n}$.