Exploiting the Symmetry of $\mathbb{Z}^n$: Randomization and the Automorphism Problem

Kaijie Jiang Anyu Wang(✉) Hengyi Luo Guoxiao Liu Yang Yu Xiaoyun Wang

Speaker: Kaijie Jiang

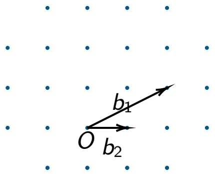
Tsinghua University

December 6, 2023

Lattices

Lattice: $\mathcal{L} = \mathcal{L}(\mathbf{B}) = \{\mathbf{Bz} : \mathbf{z} \in \mathbb{Z}^n\}$. $\mathbf{B} = (\mathbf{b}_1, ..., \mathbf{b}_n)$ is a basis of $\mathcal{L}$.

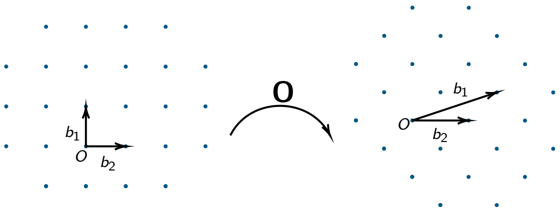
- *Shortest Vector Problem* (SVP): Given $\mathbf{B}$, find a nonzero shortest vector in $\mathcal{L}$.
- *Closest Vector Problem* (CVP): Given $\mathbf{B}$ and a target $\mathbf{t}$, find a vector $\mathbf{v} \in \mathcal{L}$ closest to $\mathbf{t}$.



Lattices Isomorphism Problem

LIP

Given lattices bases $\mathbf{B}_1, \mathbf{B}_2 \in GL_n(\mathbb{R})$ of isomorphic lattices, find $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ and $\mathbf{U} \in GL_n(\mathbb{Z})$ s.t. $\mathbf{B}_1 = \mathbf{O}\mathbf{B}_2\mathbf{U}$.



- Algorithm: [PS97, GS02, Szy03, GS03, SSV09, HR14, JS14, JS17, DSHVvW20, BGPS23, DG23, Duc23].
- Cryptography: [BM21, BGPS23, DPPvW22, DvW22].

Computational Problems related to $\mathbb{Z}^n$

$\mathbb{Z}$SVP and $\mathbb{Z}$LIP

- In SVP, If $\mathcal{L} \cong \mathbb{Z}^n$, we call this problem $\mathbb{Z}$SVP.
- In LIP, If $\mathbf{B}_1 = \mathbf{I}_n$, we call this problem $\mathbb{Z}$LIP.
- Note that $\mathbb{Z}$LIP $=$ $\mathbb{Z}$SVP.

- Algorithm:[GS02, Szy03, GS03, JS14, JS17, BGPS23, Duc23].
- Cryptography:[BM21, BGPS23, DPPvW22].

However, the theoretical complexity of $\mathbb{Z}$LIP is still not well understood.

Key observation of this work: Symmetry of $\mathbb{Z}^n$

$\mathbb{Z}^n$ (and its rotations) possesses a remarkable degree of symmetry.

- For lattice $\mathbb{Z}^n$, $\mathrm{Aut}(\mathbb{Z}^n) = \mathcal{S}_n^{\pm}$. $|\mathcal{S}_n^{\pm}| = 2^n \cdot n!$ **which is known to be the largest possible for any lattice in $\mathbb{R}^n$ when $n > 10$.**

Key observation of this work: Symmetry of $\mathbb{Z}^n$

$\mathbb{Z}^n$ (and its rotations) possesses a remarkable degree of symmetry.

- For lattice $\mathbb{Z}^n$, $\mathrm{Aut}(\mathbb{Z}^n) = \mathcal{S}_n^{\pm}$. $|\mathcal{S}_n^{\pm}| = 2^n \cdot n!$ **which is known to be the largest possible for any lattice in $\mathbb{R}^n$ when $n > 10$.**
- *Q1: Can the symmetry be used to help solve or the reduction of the computational problems related to $\mathbb{Z}^n$?*
- *Q2: Is it feasible to efficiently obtain a nontrivial automorphism for a lattice isomorphic to $\mathbb{Z}^n$?*

Key observation of this work: Symmetry of $\mathbb{Z}^n$

$\mathbb{Z}^n$ (and its rotations) possesses a remarkable degree of symmetry.

- For lattice $\mathbb{Z}^n$, $\text{Aut}(\mathbb{Z}^n) = \mathcal{S}_n^{\pm}$. $|\mathcal{S}_n^{\pm}| = 2^n \cdot n!$ **which is known to be the largest possible for any lattice in $\mathbb{R}^n$ when $n > 10$.**
- *Q1: Can the symmetry be used to help solve or the reduction of the computational problems related to $\mathbb{Z}^n$?*
- *Q2: Is it feasible to efficiently obtain a nontrivial automorphism for a lattice isomorphic to $\mathbb{Z}^n$?*

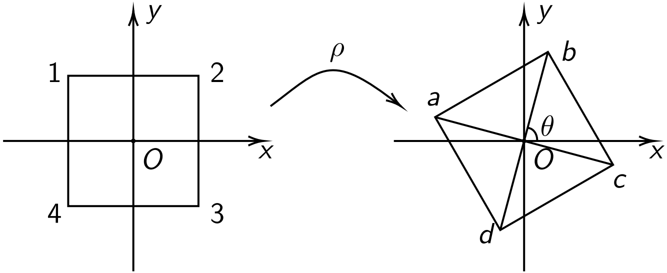
- A1: **Yes!** We provide a *randomization framework*, which can be roughly thought of as 'applying random automorphisms' in $\text{Aut}(\mathcal{L})$ to the output of an oracle, **without knowing the specific elements in Aut$(\mathcal{L})$**.
- A2: **No! It is equivalent to $\mathbb{Z}$LIP**, i.e., $\mathbb{Z}\text{LIP} = \mathbb{Z}\text{LAP}$.

Our Results

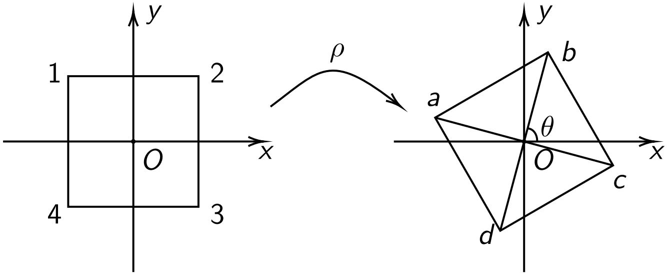
Main Results

- Introduce a randomization framework.
- For any constant γ, $\mathbb{Z}$SVP $=$ γ-$\mathbb{Z}$SVP.
- $\mathbb{Z}$LIP $=$ $\mathbb{Z}$SCVP, which is a special case of CVP.
- $\mathbb{Z}$LIP $=$ $\mathbb{Z}$LAP.

Randomization



Toy example



- $\square_{\frac{\pi}{4}} \to \rho(\square_{\frac{\pi}{4}}) = \square_\theta$, for $\rho \in \mathbb{R}/(2\pi\mathbb{Z})$.
- $\theta \in [0, \frac{\pi}{2})$, $\theta[\rho] = \theta[\rho + \frac{\pi}{2}]$.
- Oracle $\mathcal{O}$ that takes any $\square_\theta$ as input and outputs an arbitrary vertex of $\square_\theta$

Toy example

Randomization

1) generate a $\rho \in \mathbb{R}/(2\pi\mathbb{Z})$ uniformly at random;
2) invoke the oracle $\mathcal{O}$ with input $\rho(\square_{\frac{\pi}{4}}) = \square_\theta$ and obtain an arbitrary vertex of $\square_\theta$;
3) apply ρ^{-1} to the obtained vertex and output a vertex of $\square_{\frac{\pi}{4}}$.

Using the randomness of ρ, it can be shown that the obtained vertex is **uniformly distributed**.

Randomization Framework for lattices

Randomization for Lattices

1) Given a basis $\mathbf{B}$ of lattice $\mathcal{L}$, generate a $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ uniformly at random.
2) invoke the oracle $\mathcal{O}$ with input $\mathbf{B}'$ and obtain an arbitrary response of $\mathcal{L}'$;
3) apply $\mathbf{O}^{-1}$ to the obtained response and output a response in $\mathcal{L}$.

Randomization Framework for lattices

Randomization for Lattices

1) Given a basis $\mathbf{B}$ of lattice $\mathcal{L}$, generate a $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ uniformly at random.
2) invoke the oracle $\mathcal{O}$ with input $\mathbf{B}'$ and obtain an arbitrary response of $\mathcal{L}'$;
3) apply $\mathbf{O}^{-1}$ to the obtained response and output a response in $\mathcal{L}$.

- In Step 2), we randomized the basis $\mathbf{OB}$ in lattice $\mathbf{O}\mathcal{L} = \mathcal{L}'$ to get a $\mathbf{B}'$ by discrete Gaussian sampling. A similar technique was used in [HR14,DvW22,BGPS23].
- The Randomization Framework which can be roughly thought of as 'applying random automorphisms' in Aut($\mathcal{L}$) to the output of an oracle, **without knowing Aut($\mathcal{L}$)**.

Main Reductions

- **For any constant γ, $\mathbb{Z}$SVP $= \gamma$-$\mathbb{Z}$SVP.**
- $\mathbb{Z}$LIP $=$ $\mathbb{Z}$SCVP.
- $\mathbb{Z}$LIP $=$ $\mathbb{Z}$LAP.

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP

Theorem

There is an efficient randomized reduction from $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP for any constant $\gamma = O(1)$.

Proof sketch

Suppose that $\mathcal{L} \cong \mathbb{Z}^n$. Denote $A = \mathcal{L} \cap \gamma\mathcal{B}_2^n$, then by [RS17] it has $|A| = |\mathbb{Z}^n \cap \gamma\mathcal{B}_2^n| \leq n^c$ for some constant c.
The reduction proceeds as follows:

1) Using the randomization framework, we can invoke the γ-$\mathbb{Z}$SVP oracle $m = poly(n)$ times, with $m > n^c$, yielding a vector set $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_m\} \subseteq A$.
2) Then we compute $\mathbf{x}_i - \mathbf{x}_j$ for all $i, j \in [m]$, and check if it is a multiple of the shortest vector.
3) Repeating the above process $O(n^{c+1})$ times.

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP

Proof sketch

Consider the action of $\mathrm{Aut}(\mathcal{L})$ on A. Write $A = \cup_{\mathbf{v} \in \bar{A}} A_{\mathbf{v}}$ to be the disjoint union of distinct orbits, where $A_{\mathbf{v}} = \{\mathbf{O}\mathbf{v} : \mathbf{O} \in \mathrm{Aut}(\mathcal{L})\}$

It can be shown that:

- Each $\mathbf{x}_i \in X$ is independently and uniformly distributed in its own orbit by the randomization.

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP

Proof sketch

Consider the action of $\mathrm{Aut}(\mathcal{L})$ on A. Write $A = \cup_{\mathbf{v}\in\bar{A}} A_{\mathbf{v}}$ to be the disjoint union of distinct orbits, where $A_{\mathbf{v}} = \{\mathbf{O}\mathbf{v} : \mathbf{O} \in \mathrm{Aut}(\mathcal{L})\}$

It can be shown that:

- Each $\mathbf{x}_i \in X$ is independently and uniformly distributed in its own orbit by the randomization.
- Since $m > n^c \geq |\bar{A}|$, there must exist $\mathbf{x}_i$ and $\mathbf{x}_j$ fall in the same orbit

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP

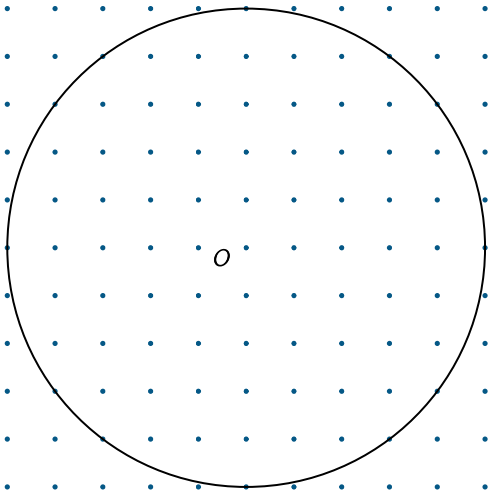
Proof sketch

Consider the action of $\mathrm{Aut}(\mathcal{L})$ on A. Write $A = \cup_{\mathbf{v}\in\bar{A}} A_{\mathbf{v}}$ to be the disjoint union of distinct orbits, where $A_{\mathbf{v}} = \{\mathbf{Ov} : \mathbf{O} \in \mathrm{Aut}(\mathcal{L})\}$

It can be shown that:

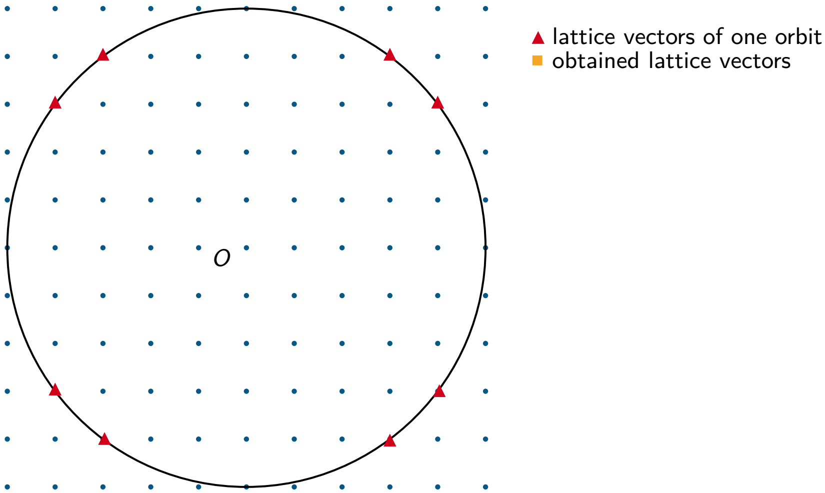
- Each $\mathbf{x}_i \in X$ is independently and uniformly distributed in its own orbit by the randomization.
- Since $m > n^c \geq |\bar{A}|$, there must exist $\mathbf{x}_i$ and $\mathbf{x}_j$ fall in the same orbit
- the probability that $\mathbf{x}_i - \mathbf{x}_j$ is a multiple of a shortest vector of $\mathcal{L}$ is at least $1/|A_{\mathbf{v}}| \geq 1/n^c$.

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration

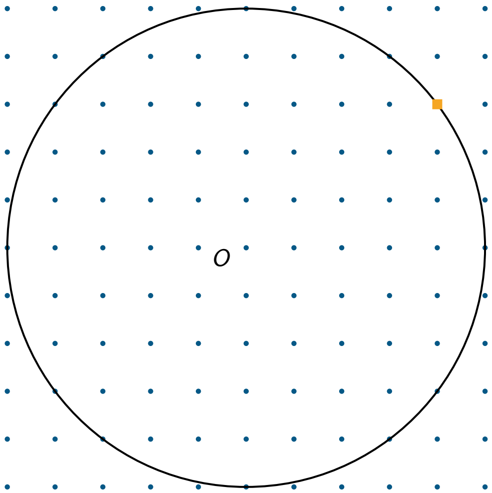


▲ lattice vectors of one orbit
■ obtained lattice vectors

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration

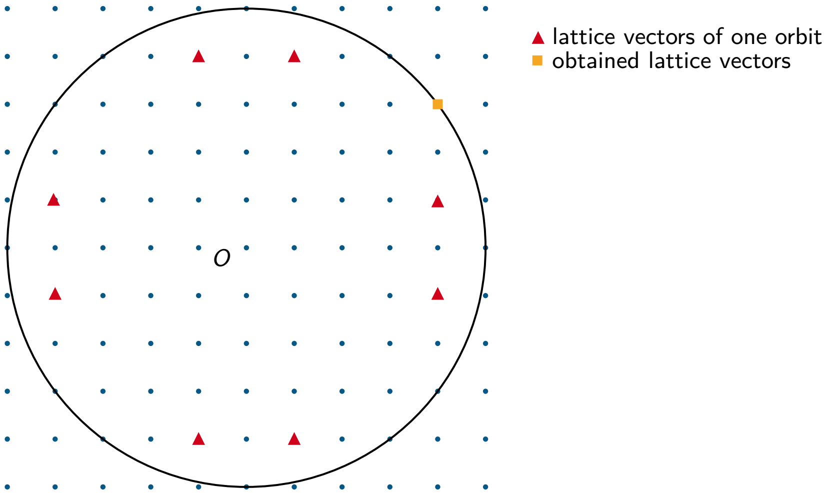


From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration

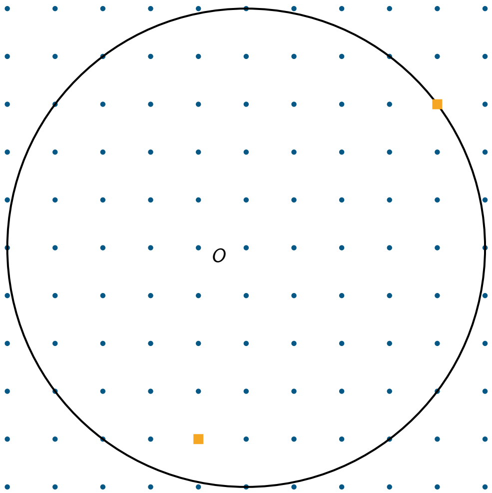


▲ lattice vectors of one orbit
■ obtained lattice vectors

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration

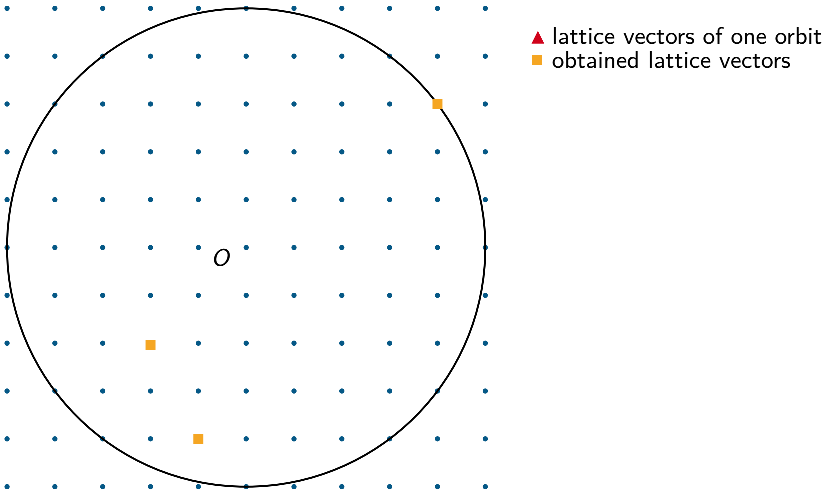


From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration

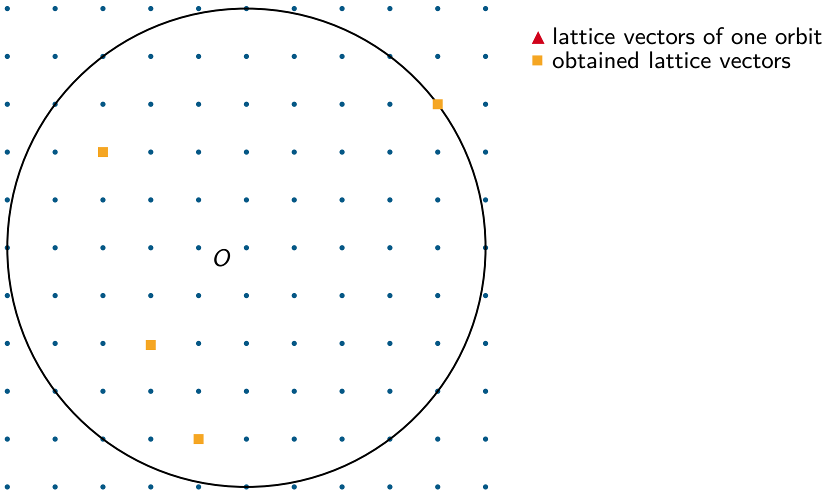


▲ lattice vectors of one orbit
■ obtained lattice vectors

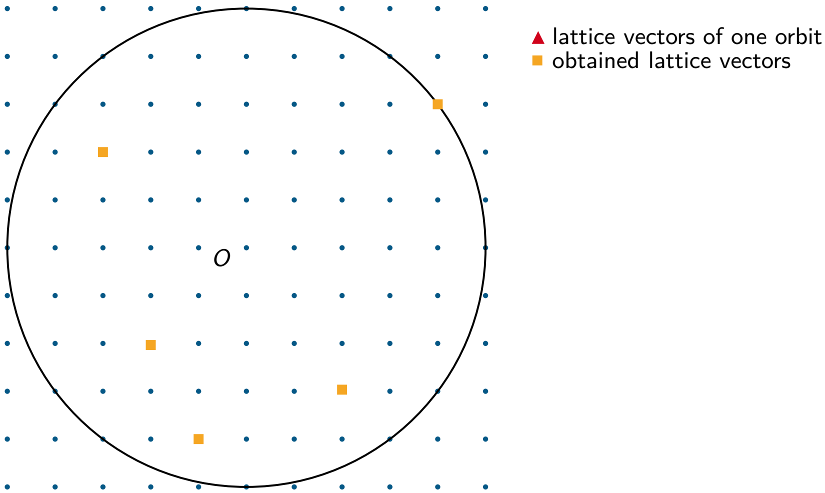
From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration



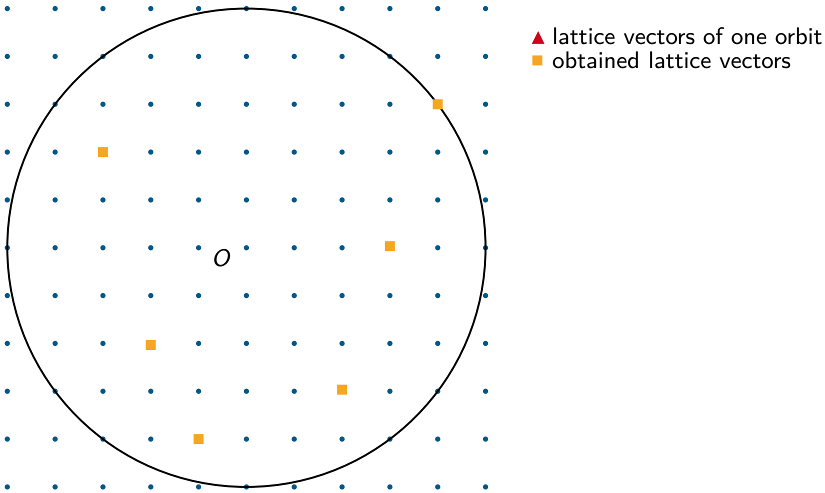
From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration



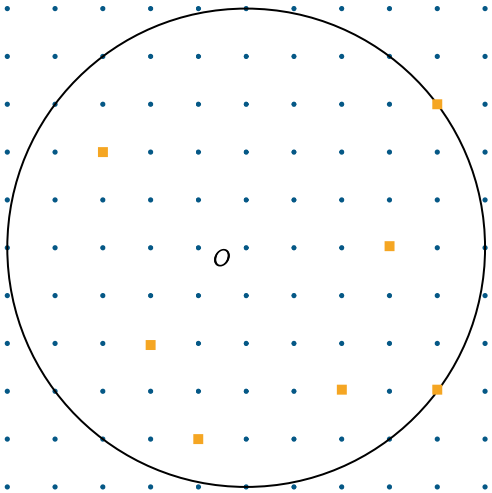
From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration



From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration

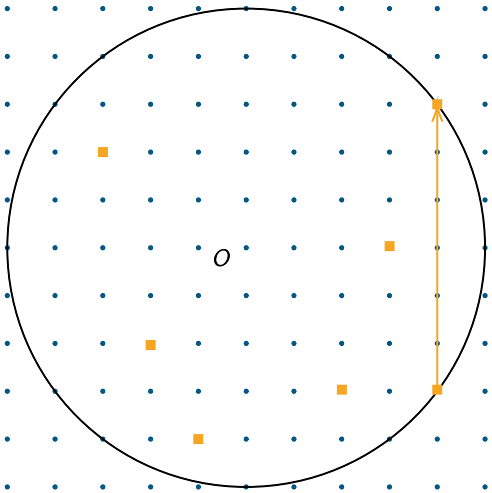


From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration



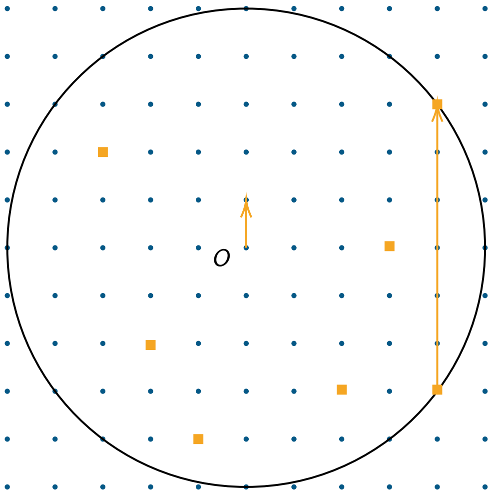
▲ lattice vectors of one orbit
■ obtained lattice vectors

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration



▲ lattice vectors of one orbit
■ obtained lattice vectors

From $\mathbb{Z}$SVP to γ-$\mathbb{Z}$SVP: illustration



▲ lattice vectors of one orbit
■ obtained lattice vectors

Main Reductions

- For any constant γ, $\mathbb{Z}$SVP $= \gamma$-$\mathbb{Z}$SVP.
- **$\mathbb{Z}$LIP $=$ $\mathbb{Z}$SCVP.**
- $\mathbb{Z}$LIP $=$ $\mathbb{Z}$LAP.

From $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP: SCVP and $\mathbb{Z}$SCVP

A lattice $\mathcal{L}$ is said to be unimodular if $\mathcal{L} = \mathcal{L}^*$.

Characteristic Vector

Suppose $\mathcal{L}$ is a unimodular lattice. A vector $\mathbf{w} \in \mathcal{L}$ is called a characteristic vector of $\mathcal{L}$ if it has $\langle \mathbf{w}, \mathbf{v} \rangle \equiv \langle \mathbf{v}, \mathbf{v} \rangle \mod 2$ for all $\mathbf{v} \in \mathcal{L}$. We denote the set of characteristic vectors as $\chi(\mathcal{L})$.

Note that $\chi(\mathcal{L}) = \mathbf{w} + 2\mathcal{L}$ for any $\mathbf{w} \in \chi(\mathcal{L})$.

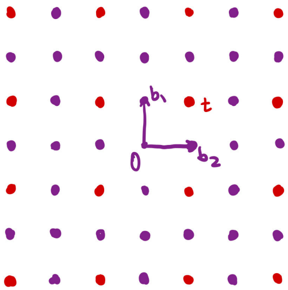
Shortest Characteristic Vector Problem (SCVP)

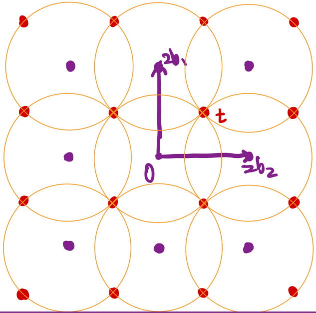
Given a basis of a unimodular lattice $\mathcal{L}$, find a shortest characteristic vector $\mathbf{w} \in \chi(\mathcal{L})$. In particular, if $\mathcal{L} \cong \mathbb{Z}^n$, we call this problem $\mathbb{Z}$SCVP.

$\mathbb{Z}$SCVP is a very special case of CVP

For $\mathcal{L} \cong \mathbb{Z}^n$, $\mathbb{Z}$SCVP is very special.

- We can efficiently compute a $\mathbf{t} \in \chi(\mathcal{L})$ from a basis of $\mathcal{L}$.
- The deep holes of $2\mathcal{L}$ are exactly $\chi(\mathcal{L})$.
- The $\mathbb{Z}$SCVP can be thought of as a CVP in the lattice $2\mathcal{L}$, with a deep hole as the target vector $\mathbf{t}$.



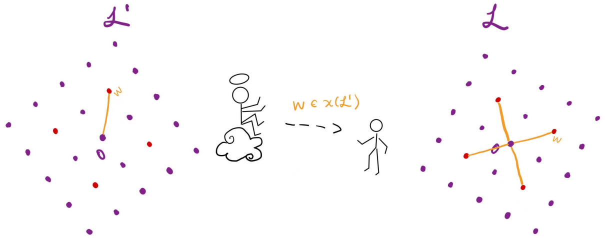


From $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP

Suppose $\mathcal{L} = \mathbf{O} \cdot \mathbb{Z}^n$. The shortest characteristic vectors of $\mathcal{L}$ are exactly $\{\mathbf{Oz} : \mathbf{z}_i = \pm 1, \forall i \in [n]\}$.

Step.1 Randomization

Given a $\mathbb{Z}$SCVP oracle $\mathcal{O}$, we can sample uniformly and independently from the set of shortest characteristic vectors of $\mathcal{L}$ by randomization.



From $\mathbb{Z}$LIP to $\mathbb{Z}$SCVP

Step.2 Recovery

Given a basis $\mathbf{B}$ of a lattice $\mathcal{L} \cong \mathbb{Z}^n$, and $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{poly(n)} \in \chi(\mathcal{L})$ that are drawn uniformly and independently from the set of shortest characteristic vectors of $\mathcal{L}$. The goal is to find the shortest vectors of $\mathcal{L}$.

- The method we used is the same as that used in [NR06], but the distribution is different.
- So we can get good approximations shortest vectors of $\mathcal{L}$.
- Finally, we can efficiently recover the shortest vectors from its approximations by some simple tricks.

Main Reductions

- For any constant γ, $\mathbb{Z}\mathrm{SVP} = \gamma\text{-}\mathbb{Z}\mathrm{SVP}$.
- $\mathbb{Z}\mathrm{LIP} = \mathbb{Z}\mathrm{SCVP}$.
- **$\mathbb{Z}\mathbf{LIP} = \mathbb{Z}\mathbf{LAP}$.**

From $\mathbb{Z}$LIP to $\mathbb{Z}$LAP

Lattice Automorphism Problem (LAP)

Given a basis of a lattice $\mathcal{L}$, find an automorphism $\mathbf{O} \in \mathrm{Aut}(\mathcal{L})$ such that $\mathbf{O} \neq \pm\mathbf{I}_n$.
If $\mathcal{L} \cong \mathbb{Z}^n$, we call this problem $\mathbb{Z}$LAP.

Given a $\mathbb{Z}$LAP oracle, we can generate automorphisms uniformly distributed over their own conjugacy class by the randomization framework.

Conjugacy Classes

- In $\mathrm{Aut}(\mathcal{L})$, two automorphisms ϕ_1 and ϕ_2 are conjugate if there exists an automorphism $\phi \in \mathrm{Aut}(\mathcal{L})$ such that $\phi_1 = \phi\phi_2\phi^{-1}$, which is denoted by $\phi_1 \sim \phi_2$.
- Conjugation is an equivalence relation that divides $\mathrm{Aut}(\mathcal{L})$ into disjoint conjugacy classes.
- For the lattice $\mathbb{Z}^n$, $\mathrm{Aut}(\mathbb{Z}^n) = \mathcal{S}_n^{\pm}$ and the number of conjugacy classes of $\mathrm{Aut}(\mathbb{Z}^n)$ is **expontential in** n.

So, it's hard to efficiently sample automorphisms from one conjugacy class.

Conjugacy Classes of $\mathbb{Z}^n$

In order to sample automorphisms from one conjugate class, we are particularly interested in the following three types of conjugacy classes.

- $\mathbf{T}_{i,j,k} = \text{diag}\{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), -\mathbf{I}_i, \mathbf{I}_j\}$, where $i, j < n$.
- $\mathbf{T}_{p,k} = \text{diag}\{\mathbf{P}_p, \ldots, \mathbf{P}_p, \mathbf{I}_{n-pk}\}$, p is an odd prime number and $\mathbf{P}_p = \begin{pmatrix} 0 & 1 \\ \mathbf{I}_{p-1} & 0 \end{pmatrix}$.
- $\mathbf{T}_n = \text{diag}\{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\}$, where n is even.

Note that the number of these types of conjugacy classes is a **polynomial of n**.

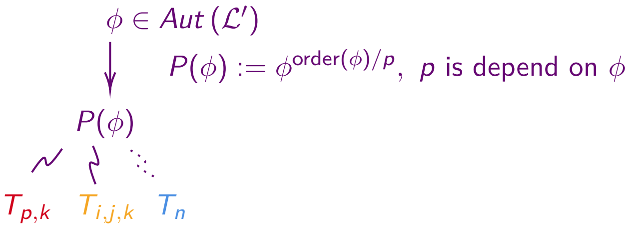
From $\mathbb{Z}$LIP to $\mathbb{Z}$LAP: illustration

$\phi \in Aut(\mathcal{L}')$

$\downarrow$ $P(\phi) := \phi^{\mathrm{order}(\phi)/p}$, p is depend on ϕ

$P(\phi)$

From ℤLIP to ℤLAP: illustration



From $\mathbb{Z}$LIP to $\mathbb{Z}$LAP: illustration

$\phi \in Aut(\mathcal{L}')$

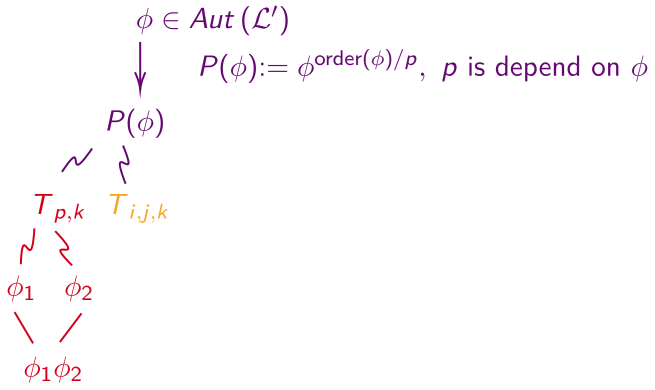
$P(\phi) := \phi^{\text{order}(\phi)/p}$, p is depend on ϕ

$P(\phi)$

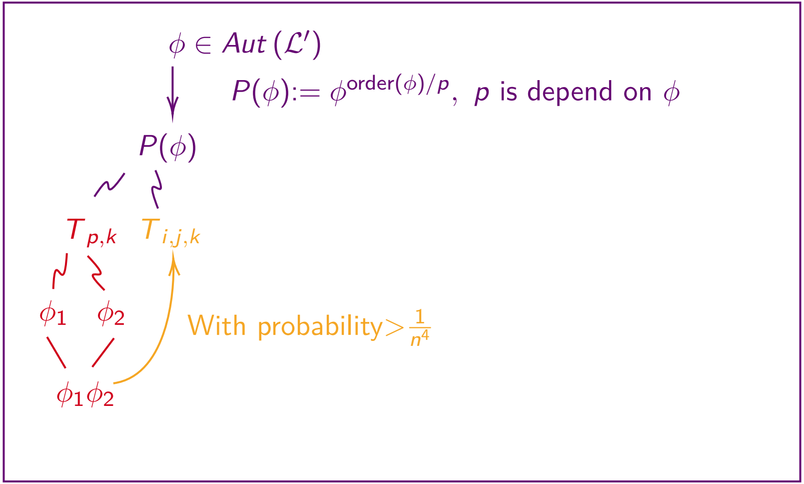
$T_{p,k}$ $T_{i,j,k}$ T_n

(It disappears when n is odd)

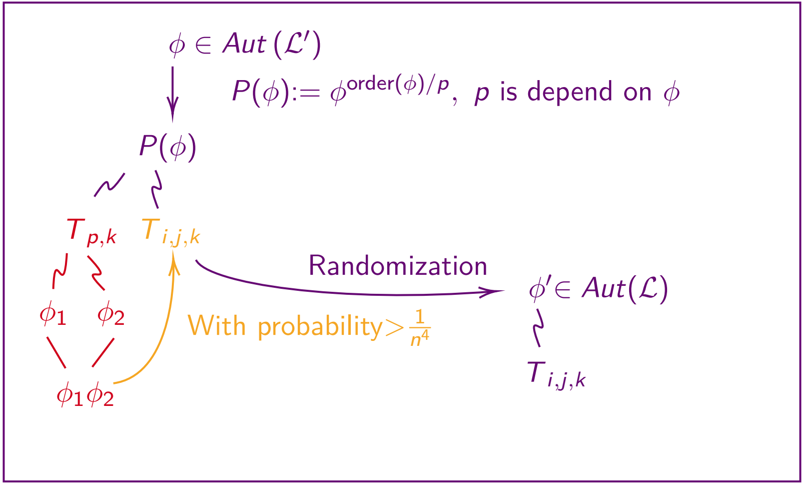
From $\mathbb{Z}$LIP to $\mathbb{Z}$LAP: illustration



From $\mathbb{Z}$LIP to $\mathbb{Z}$LAP: illustration



From $\mathbb{Z}$LIP to $\mathbb{Z}$LAP: illustration



From $\mathbb{Z}$LIP to $\mathbb{Z}$LAP

Utilizing the structure of $\mathcal{S}_n^{\pm}$ and some tricks, **we can efficiently sample automorphisms from one conjugacy class:**

Preprocessing and Randomization

Assume that n is odd and the lattice $\mathcal{L} \cong \mathbb{Z}^n$. Given a $\mathbb{Z}$LAP oracle $\mathcal{O}$ for dimension n. Then there exists i, j, k such that we efficiently obtain $poly(n)$ samples $\phi_1, \phi_2, \ldots, \phi_{poly(n)} \in \mathrm{Aut}(\mathcal{L})$ that are independently and uniformly distributed over the conjugacy class $\{\phi \in \mathrm{Aut}(\mathcal{L}) | \, \phi \sim \mathbf{T}_{i,j,k}\}$.

From $\mathbb{Z}$LIP to $\mathbb{Z}$LAP

Recovery

Given a basis $\mathbf{B}$ of a lattice $\mathcal{L} \cong \mathbb{Z}^n$, and a set of automorphisms $\phi_1, \phi_2, \ldots, \phi_{poly(n)} \in \mathrm{Aut}(\mathcal{L})$ that are drawn uniformly and independently from a conjugacy class $\mathfrak{C}_{\phi_0}$, where $\phi_0 \sim \mathbf{T}_{k_1,k_2,l}$ and k_1, k_2, l are fixed. The goal is to find the shortest vectors of $\mathcal{L}$.

- The method we used is inspired by [NR06], we consider the function:

$$g_k(\mathbf{x}) = \mathbb{E}[\langle \phi \mathbf{x}, \mathbf{x} \rangle^k], \mathbf{x} \in \mathbb{R}^n, k \in \mathbb{Z}^+.$$

- So we can find good approximations shortest vectors of $\mathcal{L}$.
- Finally, we can efficiently recover the shortest vectors from its approximations by some tricks.

Thanks for your attention!

Q & A