Improved Reduction from BDD to uSVP in Lattices

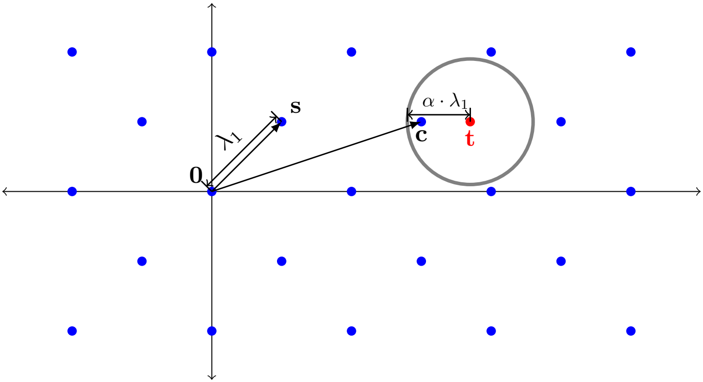
Shi Bai, Damien Stehlé, **Weiqiang Wen**

AriC Team, LIP, ENS de Lyon

Séminaires Cryptologie et Sécurité, Université de Caen, Oct. 5, 2016

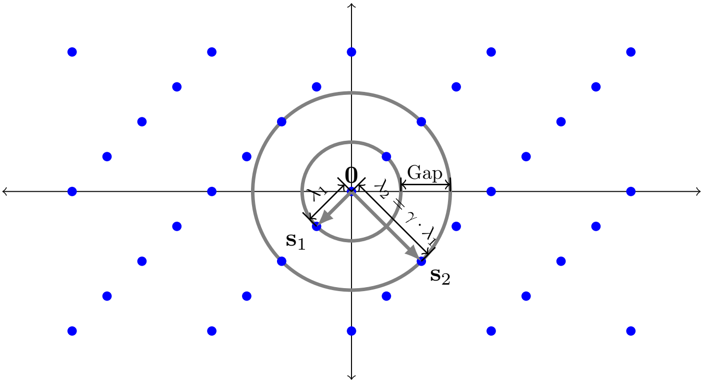
European Research Council

ENS DE LYON



Bounded Distance Decoding for $\alpha \geq 0$ (BDD$_\alpha$)

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$, a vector $\mathbf{t} \in \mathbb{Q}^n$ such that $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \leq \alpha \cdot \lambda_1(\mathbf{B})$.
Output: a lattice vector $\mathbf{c} \in \mathcal{L}(\mathbf{B})$ closest to $\mathbf{t}$.



Unique Shortest Vector Problem for $\gamma \geq 1$ (uSVP$_\gamma$)

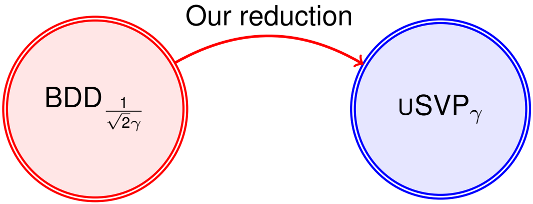
Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$ such that $\lambda_2(\mathcal{L}(\mathbf{B})) \geq \gamma \cdot \lambda_1(\mathcal{L}(\mathbf{B}))$.
Output: a non-zero vector $\mathbf{s}_1 \in \mathcal{L}(\mathbf{B})$ of norm $\lambda_1(\mathcal{L}(\mathbf{B}))$.

Main result

Improved reduction from BDD to uSVP (ICALP 2016)

For $1 \leq \gamma \leq \mathrm{poly}(n)$, we have

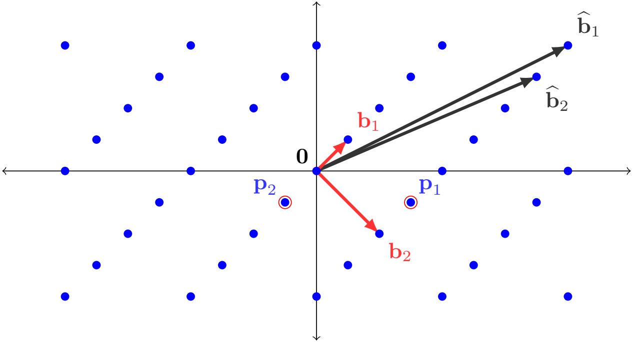
$$\mathrm{BDD}_{1/(\sqrt{2}\gamma)} \leq \mathrm{uSVP}_\gamma.$$



Road map

- Background
- The Lyubashevsky and Micciancio reduction and its limitation
- New reduction:
  - lattice sparsification.
  - reduction for $\gamma = 1$.
  - sphere packing.
- Open problems

Lattices

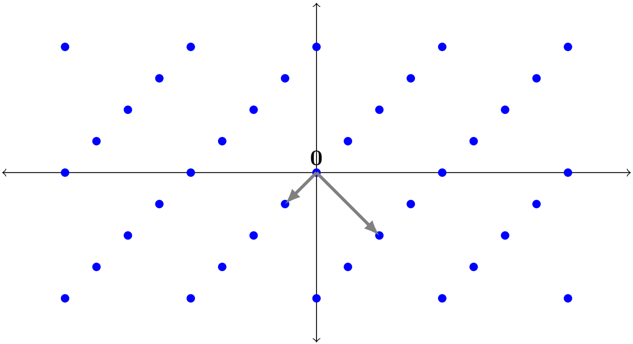


A definition of lattice

Given $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subseteq \mathbb{Q}^m$ a set of linear independent vectors, the lattice $\mathcal{L}$ spanned by the $\mathbf{b}_i'$s is

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i \in [n]} u_i \mathbf{b}_i \, : \, \mathbf{u} \in \mathbb{Z}^n \right\}.$$

Lattice Minima

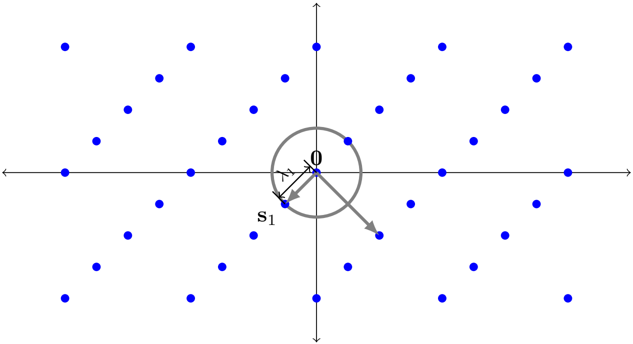


Lattice minimum

Given a lattice $\mathcal{L}$, the i-th minimum of $\mathcal{L}$ is defined as:

$$\lambda_i(\mathcal{L}) = \inf\{r : \dim(\mathrm{span}(\mathcal{L} \cap \mathcal{B}(\mathbf{0}, r))) \geq i\}.$$

Lattice Minima – first minimum

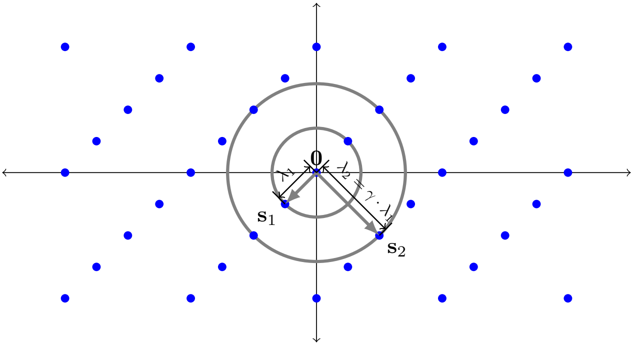


Lattice minimum

Given a lattice $\mathcal{L}$, the i-th minimum of $\mathcal{L}$ is defined as:

$$\lambda_i(\mathcal{L}) = \inf\{r : \ \dim(\mathrm{span}(\mathcal{L} \cap \mathcal{B}(\mathbf{0}, r))) \geq i\}.$$

Lattice Minima – second minimum

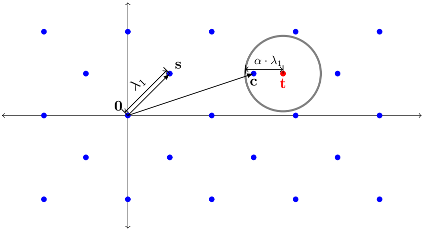


Lattice minimum

Given a lattice $\mathcal{L}$, the i-th minimum of $\mathcal{L}$ is defined as:

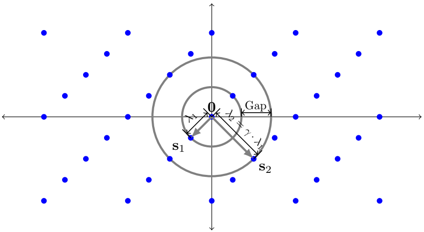
$$\lambda_i(\mathcal{L}) = \inf\{r : \dim(\mathrm{span}(\mathcal{L} \cap \mathcal{B}(\mathbf{0}, r))) \geq i\}.$$

Why is BDD interesting?



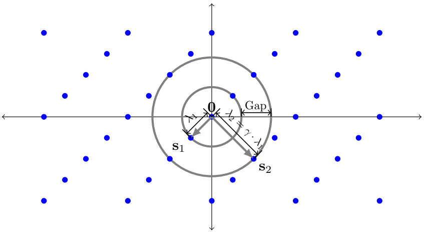
- In **cryptography**:
  - Learning With Error (LWE) problem serves as a security foundation.
  - LWE is an average-case variant of BDD.
- In **communication theory** – white Gaussian noise channel:
  - Wifi, mobile phone *etc*;
  - View message as a lattice point, Gaussian noise is added in channel transmission, decoding is solving BDD.

Why is uSVP interesting?



- Best known algorithm (especially in practice) for solving BDD is via solving uSVP:
  - First, reduce BDD to uSVP.
  - Second, solve **uSVP** by lattice reduction, *e.g.*, LLL and BKZ.

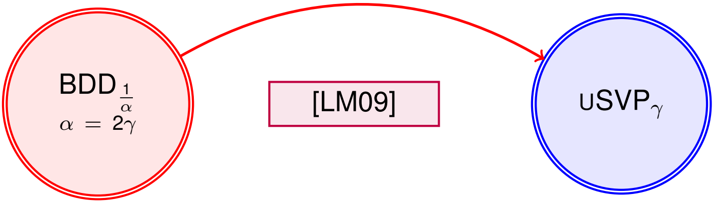
Why is uSVP interesting?



- Best known algorithm (especially in practice) for solving BDD is via solving uSVP:
  - First, reduce BDD to uSVP.
  - Second, solve **uSVP** by lattice reduction, *e.g.*, LLL and BKZ.

$\mathrm{BDD}_{\frac{1}{\mathrm{poly}(n)}}$ and $\mathrm{uSVP}_{\mathrm{poly}(n)}$ are hard;
Best known algorithm takes **exponential** time in dimension n.

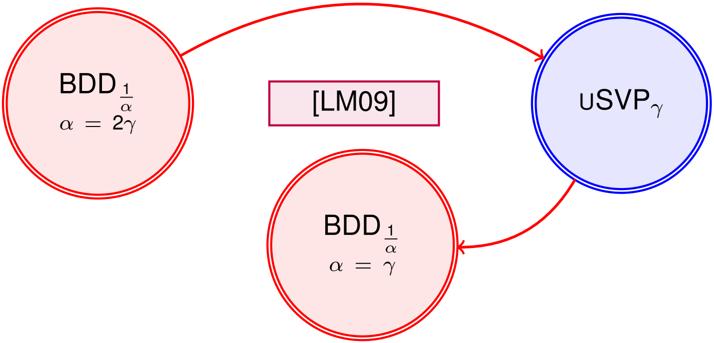
Prior works on BDD to uSVP



- Slightly improved for some α, Liu *et al*, 2014; Galbraith; Micciancio, 2015.

[LM09]: V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO, 2009.
[LWXZ14]: M. Liu, X. Wang, G. Xu and X. Zheng. A note on BDD problems with λ_2-gap. Inf. Process. Lett., 2014.
[Ga15]: Private communication, 2015.
[Mi15]: Private communication, 2015.

Prior works on BDD to uSVP



There is a factor **2** to be improved.

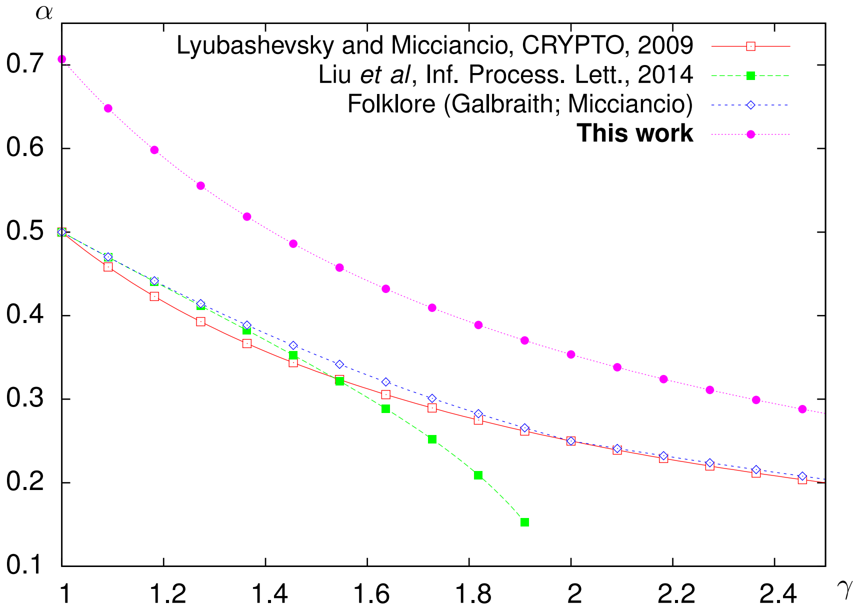
[LM09]: V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO, 2009.

[LWXZ14]: M. Liu, X. Wang, G. Xu and X. Zheng. A note on BDD problems with λ_2-gap. Inf. Process. Lett., 2014.

[Ga15]: Private communication, 2015.

[Mi15]: Private communication, 2015.

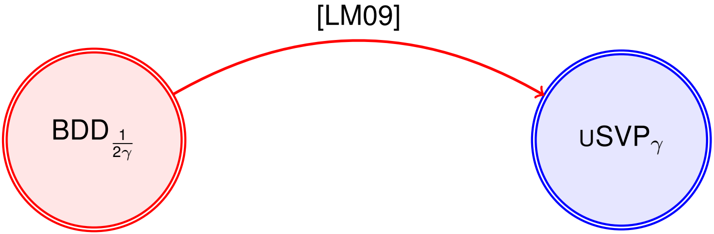
Comparison with prior works



The Lyubashevsky and Micciancio reduction

For any $\gamma \geq 1$, we have

$$\mathrm{BDD}_{1/(2\gamma)} \leq \mathrm{uSVP}_{\gamma}.$$



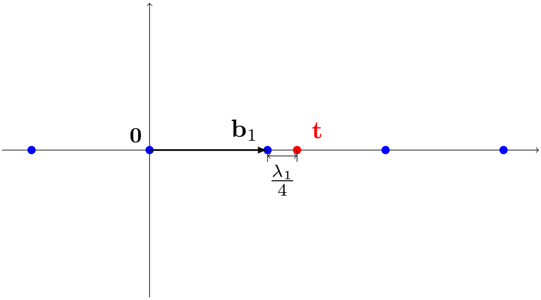
[LM09]: V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO, 2009.

A simple case

- $\mathrm{BDD}_{1/4}$ instance: $(\mathcal{L}(\mathbf{b}_1), \mathbf{t})$.

$$\mathrm{BDD}_{\frac{1}{2\gamma}}\left(\boxed{\mathbf{B}}\,,\,\boxed{\mathbf{t}}\right)$$

$$(n = 1,\ \gamma = 2)$$

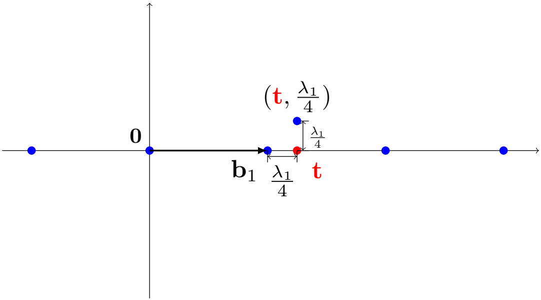


A simple case

- Lift vector **t** into a higher dimension space by $\lambda_1(\mathcal{L}(\mathbf{b}_1))/4$.

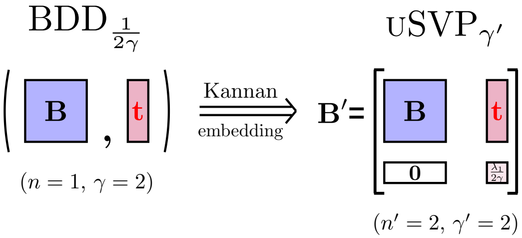
$$\mathrm{BDD}_{\frac{1}{2\gamma}}\left(\boxed{\mathbf{B}}, \boxed{\mathbf{t}} \right)$$

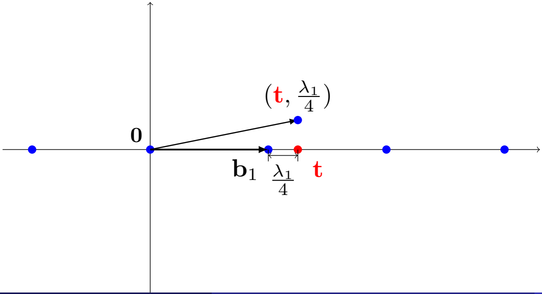
$$(n = 1,\ \gamma = 2)$$



A simple case

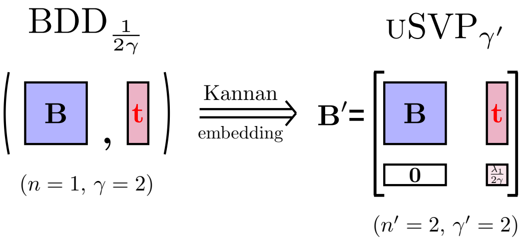
- Kannan embedding.

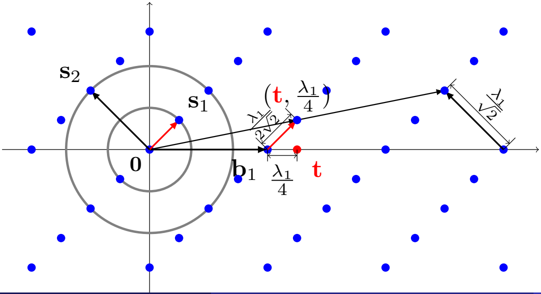




A simple case

- Finally, we obtain a uSVP instance with $\lambda'_2 = 2\lambda'_1$.





Algorithm for solving BDD

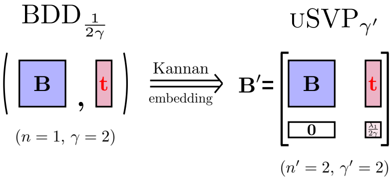
Version 1. The $\mathrm{BDD}_{1/(2\gamma)}$ to uSVP_γ reduction.

Input: a basis $\mathbf{B} = \{\mathbf{b}_i\}_{i\in[n]}$, and a target point $\mathbf{t}$.
Output: a lattice point $\mathbf{c}$ such that $\|\mathbf{c} - \mathbf{t}\| = \mathrm{dist}(\mathbf{t}, \mathcal{L})$.

0. Define

$$\mathbf{B}' = \begin{pmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & \frac{\lambda_1(\mathcal{L}(\mathbf{B}))}{2\gamma} \end{pmatrix}.$$

1. Run the uSVP_γ solver on input $\mathbf{B}'$. Let $\mathbf{s}' = \begin{pmatrix} \mathbf{s}'_1 \\ s'_2 \end{pmatrix}$ be its output.
2. Output $\mathbf{t} - \mathbf{s}'_1$.



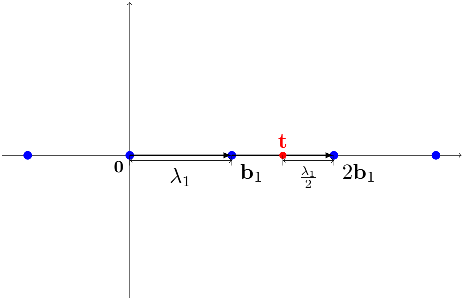
Limiting case of the reduction

- $\mathrm{BDD}_{1/2}$ instance: $(\mathcal{L}(\mathbf{b}_1), \mathbf{t})$.

$$\mathrm{BDD}_{\frac{1}{2\gamma}}$$

$$\left(\boxed{\mathbf{B}}, \boxed{\mathbf{t}} \right)$$

$$(n = 1,\ \gamma = 1)$$

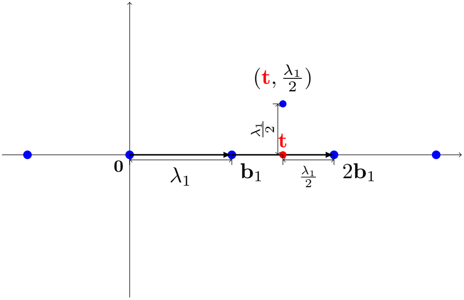


Limiting case of the reduction

- Lift vector **t** into a higher dimension space by $\lambda_1(\mathcal{L}(\mathbf{b}_1))/2$.

$$\mathrm{BDD}_{\frac{1}{2\gamma}}\left(\boxed{\mathbf{B}}, \boxed{\mathbf{t}}\right)$$

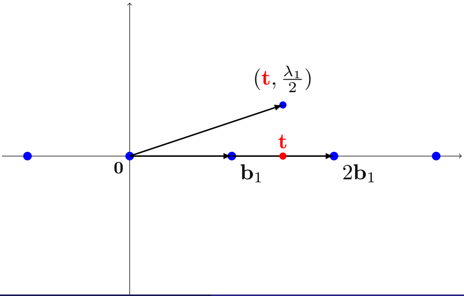
$$(n = 1,\ \gamma = 1)$$



Limiting case of the reduction

- Kannan embedding.

$$\mathrm{BDD}_{\frac{1}{2\gamma}} \left(\mathbf{B}, \mathbf{t} \right) \quad (n = 1,\ \gamma = 1) \quad \xrightarrow[\text{embedding}]{\text{Kannan}} \quad \mathrm{uSVP}_{\gamma'} \quad \mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & \frac{\lambda_1}{2\gamma} \end{bmatrix} \quad (n' = 2,\ \gamma' = 1)$$

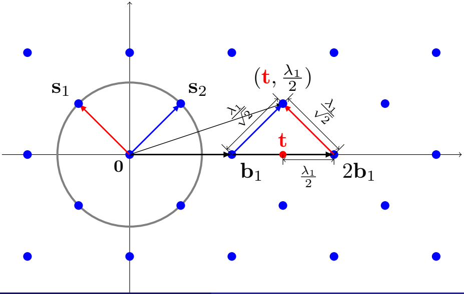


- We are at the limit: $\lambda_1' = \lambda_2'$.

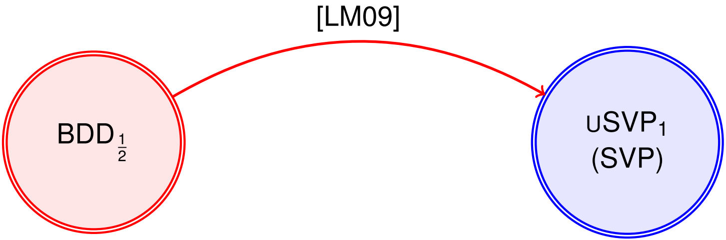
$$\mathrm{BDD}_{\frac{1}{2\gamma}} \qquad\qquad \mathrm{uSVP}_{\gamma'}$$

$$\left(\mathbf{B}, \mathbf{t}\right) \xRightarrow[\text{embedding}]{\text{Kannan}} \mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & \frac{\lambda_1}{2\gamma} \end{bmatrix}$$

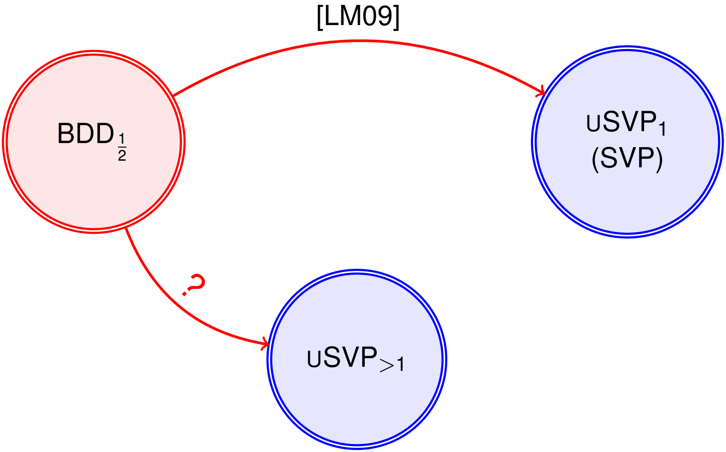
$$(n = 1,\ \gamma = 1) \qquad\qquad (n' = 2,\ \gamma' = 1)$$



This is the best this reduction can achieve

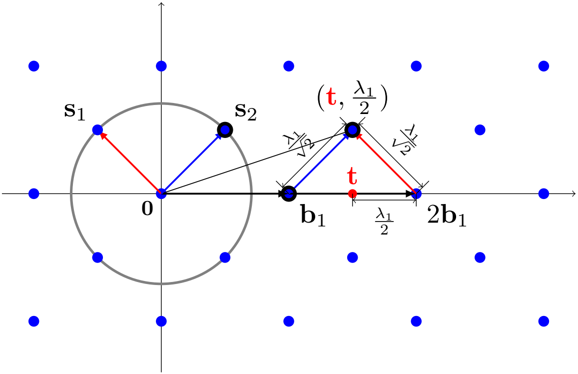


Can we improve it?



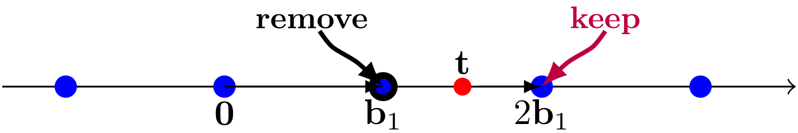
An attempt to circumvent the limitation

- Limitation in the Lyubushevsky and Micciancio reduction.



An attempt to circumvent the limitation

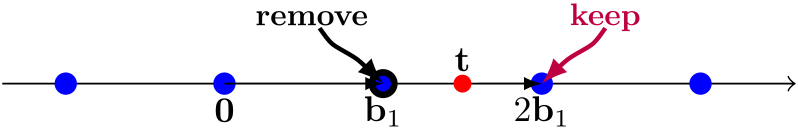
- A simple deterministic sparsification.
- Lattice $\mathcal{L}(\mathbf{B})$ with $\mathbf{B} = [\mathbf{b}_1]$.



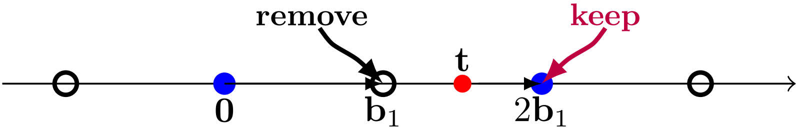
An attempt to circumvent the limitation

- A simple deterministic sparsification.

- Lattice $\mathcal{L}(\mathbf{B})$ with $\mathbf{B} = [\mathbf{b}_1]$.

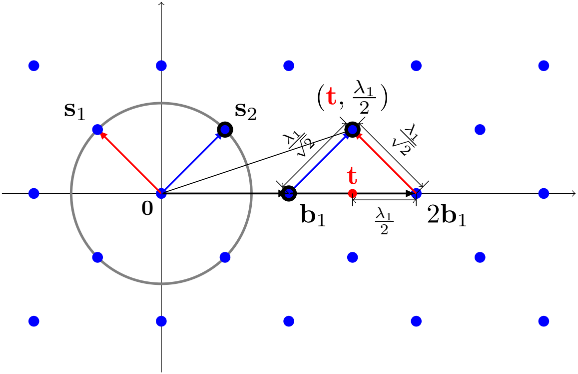


- Lattice $\mathcal{L}(\widetilde{\mathbf{B}})$ with $\widetilde{\mathbf{B}} = [2\mathbf{b}_1]$.



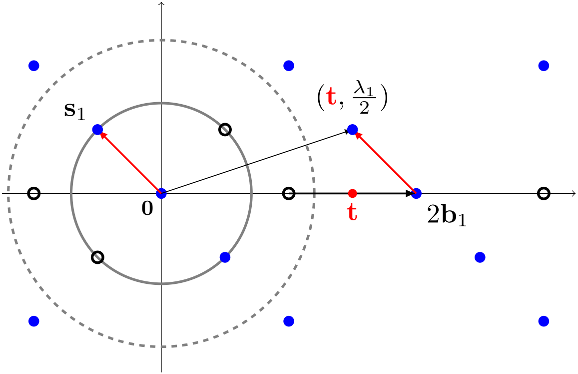
An attempt to circumvent the limitation

- Recall the limitation: $\lambda'_2 = \lambda'_1$



An attempt to circumvent the limitation

- Limitation is circumvented (for this example): $\lambda_2' > \lambda_1'$ now!

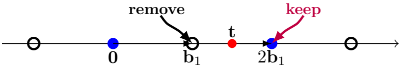


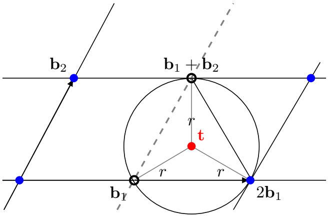
Road map

- Background
- The Lyubashevsky and Micciancio's reduction and its limitation
- New reduction:
  - lattice sparsification.
  - example for $\gamma = 1$.
  - sphere packing.
- Open problems

Main idea

- Deterministic sparsification leads to a combinatorial explosion.





- But we want more...

> • keep only $\boxed{1}$ closest vector to target **t**.
> • remove all other somewhat close $\boxed{N}$ vectors to **t**.

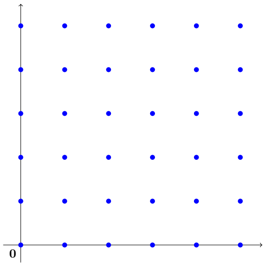
Lattice Sparsification

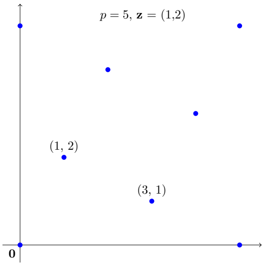
Khot's Lattice Sparsification [K03]

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.





[K03]: S. Khot. Hardness of approximating the shortest vector problem in high L_p norms. FOCS'03, 2003.

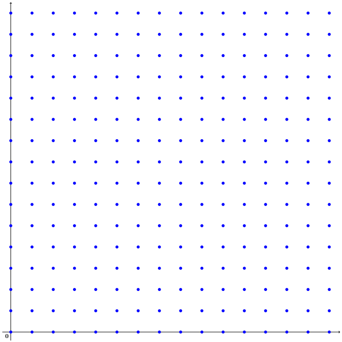
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **1**st sparsification: $p = 5$, $\mathbf{z} = (0, 0)$.

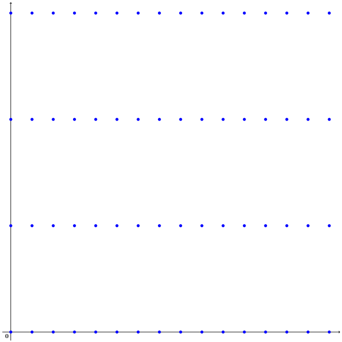
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **2**nd sparsification: $p = 5$, $\mathbf{z} = (0, 1)$.

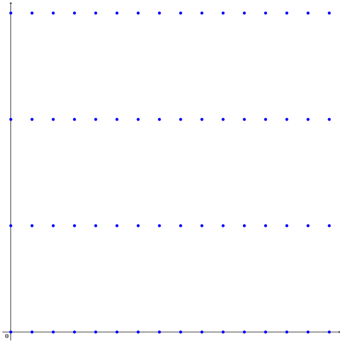
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **3**rd sparsification: $p = 5$, $\mathbf{z} = (0, 2)$.

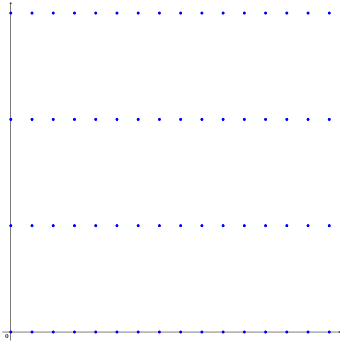
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **4**th sparsification: $p = 5$, $\mathbf{z} = (0, 3)$.

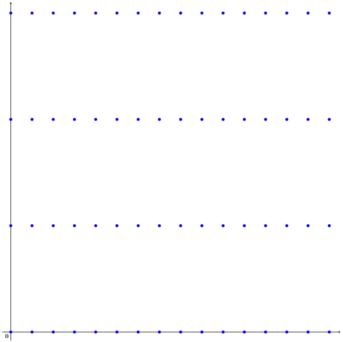
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **5**th sparsification: $p = 5$, $\mathbf{z} = (0, 4)$.

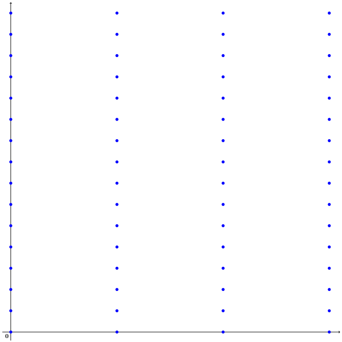
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **6**th sparsification: $p = 5$, $\mathbf{z} = (1, 0)$.

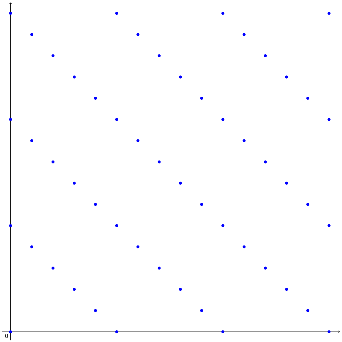
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **7**th sparsification: $p = 5$, $\mathbf{z} = (1, 1)$.

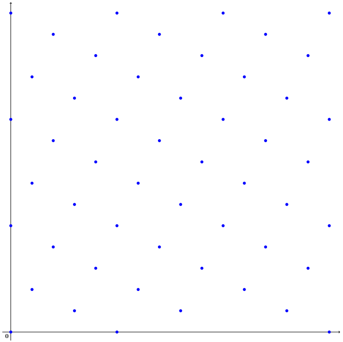
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **8**th sparsification: $p = 5$, $\mathbf{z} = (1, 2)$.

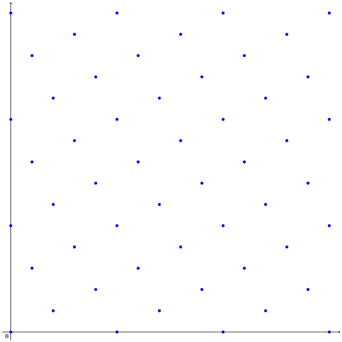
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **9**th sparsification: $p = 5$, $\mathbf{z} = (1, 3)$.

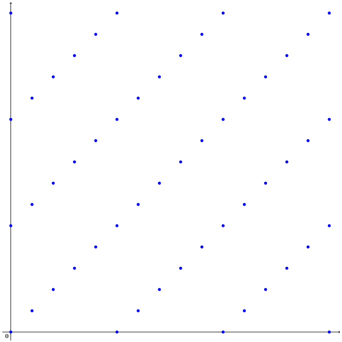
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **10**th sparsification: $p = 5$, $\mathbf{z} = (1, 4)$.

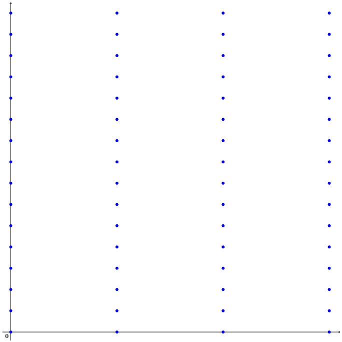
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **11**th sparsification: $p = 5$, $\mathbf{z} = (2, 0)$.

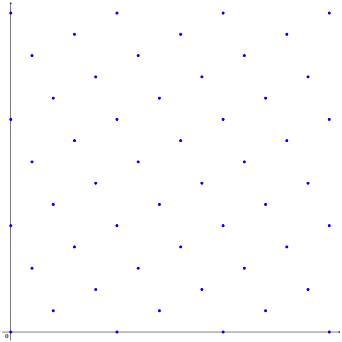
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **12**th sparsification: $p = 5$, $\mathbf{z} = (2, 1)$.

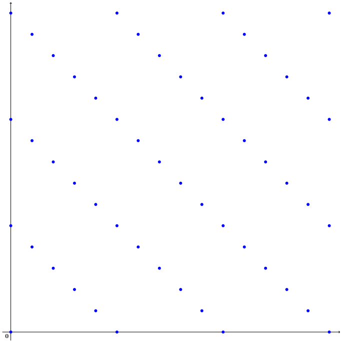
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n\times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x}\rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **13**th sparsification: $p = 5$, $\mathbf{z} = (2, 2)$.

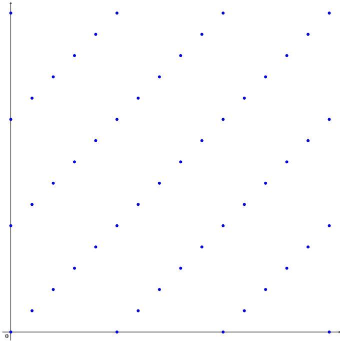
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **14**th sparsification: $p = 5$, $\mathbf{z} = (2, 3)$.

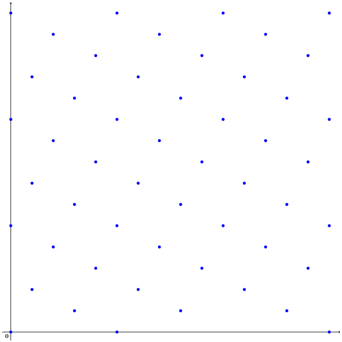
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **15**th sparsification: $p = 5$, $\mathbf{z} = (2, 4)$.

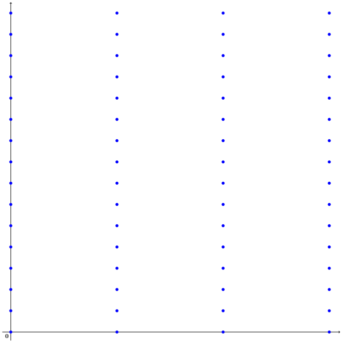
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **16**th sparsification: $p = 5$, $\mathbf{z} = (3, 0)$.

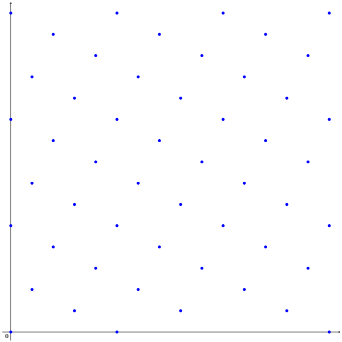
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **17**th sparsification: $p = 5$, $\mathbf{z} = (3, 1)$.

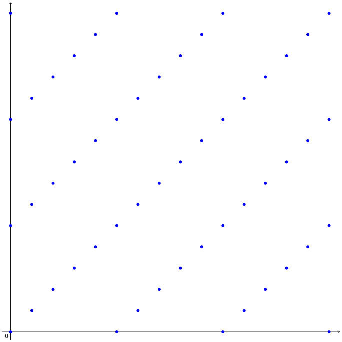
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **18**th sparsification: $p = 5$, $\mathbf{z} = (3, 2)$.

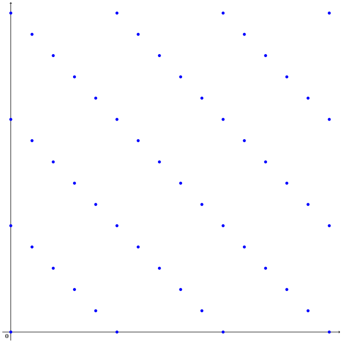
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **19**th sparsification: $p = 5$, $\mathbf{z} = (3, 3)$.

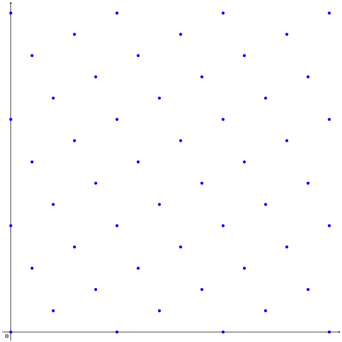
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **20**th sparsification: $p = 5$, $\mathbf{z} = (3, 4)$.

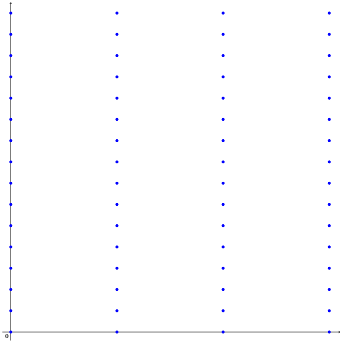
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **21**st sparsification: $p = 5$, $\mathbf{z} = (4, 0)$.

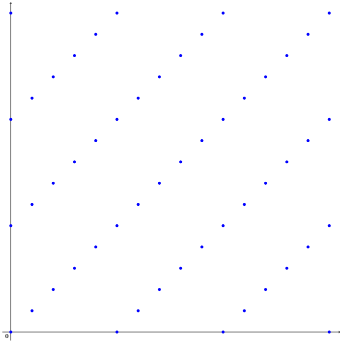
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **22**nd sparsification: $p = 5$, $\mathbf{z} = (4, 1)$.

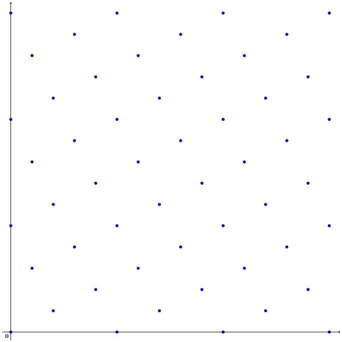
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **23**rd sparsification: $p = 5$, $\mathbf{z} = (4, 2)$.

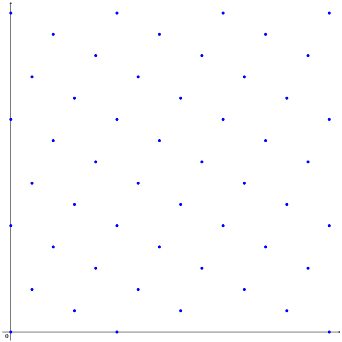
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **24**th sparsification: $p = 5$, $\mathbf{z} = (4, 3)$.

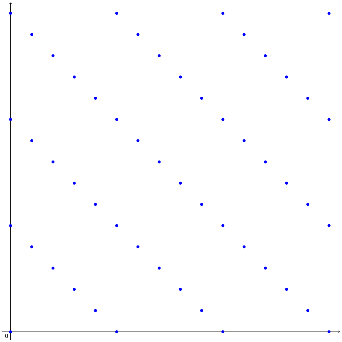
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



- **25**th sparsification: $p = 5$, $\mathbf{z} = (4, 4)$.

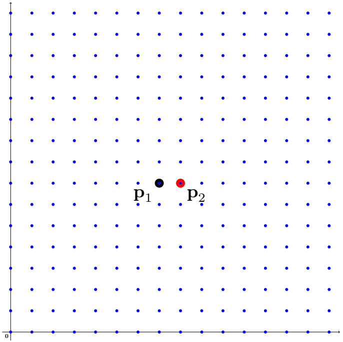
Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.



In the overall 25 sparsifications:

- $\mathbf{p}_1$ is in: $\underline{5}$ times; prob. $\frac{1}{5}$.
- $\mathbf{p}_2$ is out: $\underline{20}$ times; prob. $1 - \frac{1}{5}$.

Sparsification on lattice

Khot's Lattice Sparsification

Input: $\mathbf{B} \in \mathbb{Q}^{n\times n}$.
Output: a sparsified sub-lattice of $\mathcal{L}(\mathbf{B})$:

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x}\rangle = 0 \bmod p\},$$

where p is a prime integer and $\mathbf{z} \in \mathbb{Z}_p^n$.

- Each individual point is **kept** with probability $\frac{1}{p}$;
- and is **removed** with probability $1 - \frac{1}{p}$.
- Two issues:
  - The origin $\mathbf{0}$ is never removed.
  - There are dependencies among some points.

An argument of this probability result

A probabilistic argument on Khot's sparsification [S14]

Given a basis $\mathbf{B}$, vectors $\mathbf{x}, \mathbf{v}_1, \cdots, \mathbf{v}_N \in \mathcal{L}(\mathbf{B})$, s.t. $\mathbf{B}^{-1}\mathbf{x} \notin \{\mathbf{B}^{-1}\mathbf{v}_i\}_{i \leq N}$, for any prime p, we have

$$\Pr_{\mathbf{z} \hookleftarrow U(\mathbb{Z}_q^n)} \left[\begin{array}{rll} & \langle \mathbf{z}, \mathbf{B}^{-1}(\mathbf{x}+\mathbf{w})\rangle & = 0 \bmod p \\ \forall i, & \langle \mathbf{z}, \mathbf{B}^{-1}(\mathbf{v}_i+\mathbf{w})\rangle & \neq 0 \bmod p \end{array} \right] \geq \frac{1}{p} - \frac{N}{p^2} - \frac{N}{p^{n-1}},$$

where $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \hookleftarrow U(\mathbb{Z}_q^n)$.

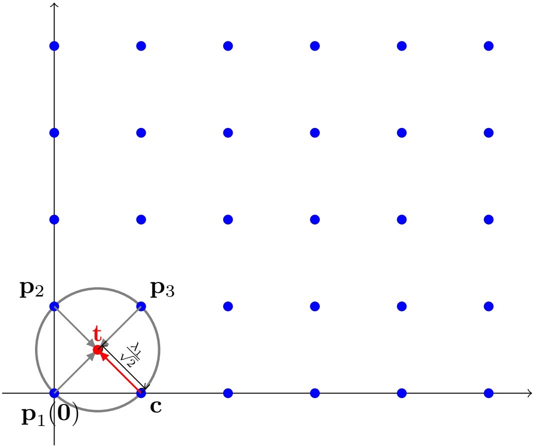
$$\frac{1}{p} - \frac{N}{p^2} \approx \frac{1}{p} \cdot (1 - \frac{1}{p})^N.$$

- The latter formula is the (approximate) probability we get to
  - **keep** $\boxed{1}$ point;
  - **remove** $\boxed{\text{N}}$ points.

[S14]: N. Stephens-Davidowitz. Discrete Gaussian sampling reduces to CVP and SVP. In *Proc. of SODA*, 2016.

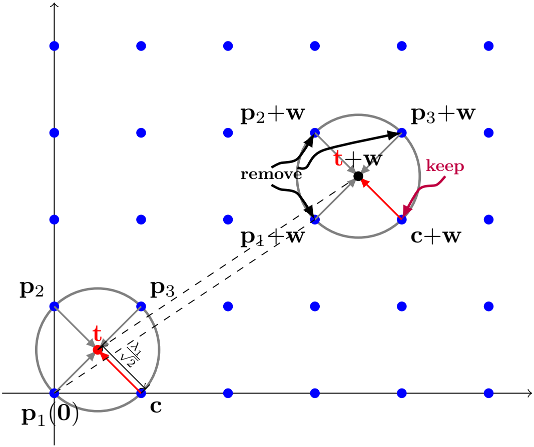
New reduction for $\gamma = 1$

- $\text{BDD}_{1/\sqrt{2}}$ instance: $(\mathcal{L}(\mathbf{B}), \mathbf{t})$.



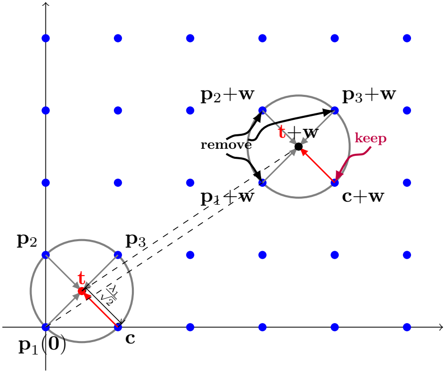
New reduction for $\gamma = 1$

- Remove annoying points around the shifted target $\mathbf{t} + \mathbf{w}$.



- Sparsify it!

$$\mathcal{L}_{p,\mathbf{z}} = \{\mathbf{x} \in \mathcal{L}(\mathbf{B}) \mid \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{x} \rangle = 0 \bmod p\}$$



Choose p a prime, $\mathbf{z} \hookleftarrow \mathbb{Z}_p^n$;
compute $\mathbf{w} = \mathbf{Bu}$ for $\mathbf{u} \hookleftarrow U(\mathbb{Z}_q^n)$;
hope the following conditions hold.

$$\begin{cases} & \langle \mathbf{z}, \mathbf{B}^{-1}(\mathbf{c}+\mathbf{w}) \rangle = 0 \bmod p \\ \forall i, & \langle \mathbf{z}, \mathbf{B}^{-1}(\mathbf{p}_i+\mathbf{w}) \rangle \neq 0 \bmod p, \end{cases}$$

Equivalently, we have

$$\begin{cases} & \mathbf{c}+\mathbf{w} \in \mathcal{L}_{p,\mathbf{z}} \\ \forall i, & \mathbf{p}_i+\mathbf{w} \notin \mathcal{L}_{p,\mathbf{z}}. \end{cases}$$

Algorithm for solving BDD

Version 2. The $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ to $\mathrm{uSVP}_{\gamma'}$ reduction.

Input: a basis $\mathbf{B} = \{\mathbf{b}_i\}_{i\in[n]}$, and a target point $\mathbf{t}$.
Output: a lattice point $\mathbf{c}$ such that $\|\mathbf{c}-\mathbf{t}\| = \mathrm{dist}(\mathbf{t},\mathcal{L})$.

0. Choose $\boxed{p > N}$ to be prime;
   sample $\mathbf{z},\mathbf{u} \hookleftarrow \mathbb{Z}_p^n$; compute $\mathbf{w} = \mathbf{B}\mathbf{u} \in \mathcal{L}$.
   Let $\mathbf{B}_{p,\mathbf{z}}$ denote the basis of $\mathcal{L}_{p,\mathbf{z}}$.
1. Define
$$\mathbf{B}' = \begin{pmatrix} \mathbf{B}_{p,\mathbf{z}} & \mathbf{t}+\mathbf{w} \\ \mathbf{0} & \frac{\lambda_1(\mathcal{L}(\mathbf{B}))}{2\gamma} \end{pmatrix}.$$
2. Run the $\mathrm{uSVP}_{\gamma'}$ solver on input $\mathbf{B}'$. Let $\mathbf{s}' = \begin{pmatrix} \mathbf{s}_1' \\ s_2' \end{pmatrix}$ be its output.
3. Output $\mathbf{t} - \mathbf{s}_1'$.

Algorithm for solving BDD

Version 2. The $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ to $\mathrm{uSVP}_{\gamma'}$ reduction.

Input: a basis $\mathbf{B} = \{\mathbf{b}_i\}_{i\in[n]}$, and a target point $\mathbf{t}$.
Output: a lattice point $\mathbf{c}$ such that $\|\mathbf{c} - \mathbf{t}\| = \mathrm{dist}(\mathbf{t}, \mathcal{L})$.

0. Choose $\boxed{p > N}$ to be prime;
   sample $\mathbf{z}, \mathbf{u} \hookleftarrow \mathbb{Z}_p^n$; compute $\mathbf{w} = \mathbf{Bu} \in \mathcal{L}$.
   Let $\mathbf{B}_{p,\mathbf{z}}$ denote the basis of $\mathcal{L}_{p,\mathbf{z}}$.
1. Define
$$\mathbf{B}' = \begin{pmatrix} \mathbf{B}_{p,\mathbf{z}} & \mathbf{t}+\mathbf{w} \\ \mathbf{0} & \frac{\lambda_1(\mathcal{L}(\mathbf{B}))}{2\gamma} \end{pmatrix}.$$
2. Run the $\mathrm{uSVP}_{\gamma'}$ solver on input $\mathbf{B}'$. Let $\mathbf{s}' = \begin{pmatrix} \mathbf{s}_1' \\ s_2' \end{pmatrix}$ be its output.
3. Output $\mathbf{t} - \mathbf{s}_1'$.

How sparse can the sublattice $\mathcal{L}_{p,\mathbf{z}}$ be?

How sparse?

Recall the probability to keep $\boxed{1}$ point and **remove** $\boxed{N}$ points:

$$\boxed{\frac{1}{p} - \frac{N}{p^2}.}$$

How sparse?

Recall the probability to keep $\boxed{1}$ point and **remove** $\boxed{N}$ points:

$$\frac{1}{p} - \frac{N}{p^2}.$$

- We want it to be at least $\frac{1}{\mathrm{poly}(n)}$;
- thus, $p \geq N$ and both should be $\leq \mathrm{poly}(n)$.

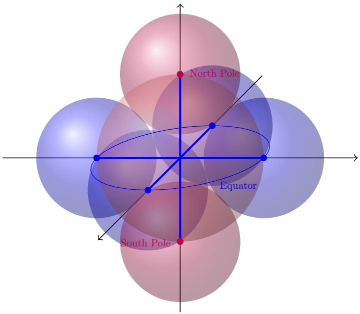
We can sparsify the lattice by removing polynomially many points.

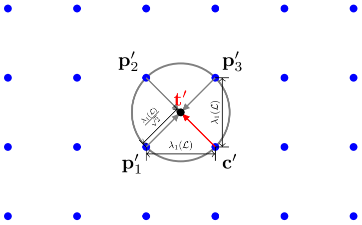
So what is the worst list decoding radius?

Approaching the limit

Within $\lambda_1/\sqrt{2}$, adapted from [MG02, Th. 5.2]

For any n-dimensional lattice $\mathcal{L}$ and any vector $\mathbf{t} \in \mathrm{Span}(\mathcal{L})$, we have $\#\mathcal{L} \cap \mathcal{B}(\mathbf{t}, \lambda_1(\mathcal{L})/\sqrt{2}) \leq 2n$.



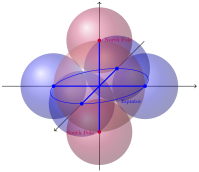


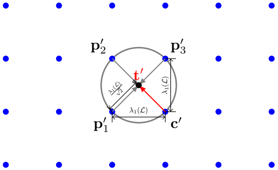
[MG02]: D. Micciancio and S. Goldwasser. Complexity of lattice problem: A cryptography perspective. Kluwer, 2009.

Approaching the limit

Within $\lambda_1/\sqrt{2}$, adapted from [MG02, Th. 5.2]

For any n-dimensional lattice $\mathcal{L}$ and any vector $\mathbf{t} \in \mathrm{Span}(\mathcal{L})$, we have $\#\mathcal{L} \cap \mathcal{B}(\mathbf{t}, \lambda_1(\mathcal{L})/\sqrt{2}) \leq 2n$.





Extremely dense lattice, adapted from [MG02, Lem. 4.1]

For any $\alpha > 1/\sqrt{2}$, there exists $\epsilon > 0$ such that for any sufficiently large n we can find an n-dimensional lattice $\mathcal{L}$ and a vector $\mathbf{t} \in \mathrm{Span}(\mathcal{L})$, such that $\#\mathcal{L} \cap \mathcal{B}(\mathbf{t}, \alpha \cdot \lambda_1(\mathcal{L})) \geq 2^{n^{\epsilon}}$.

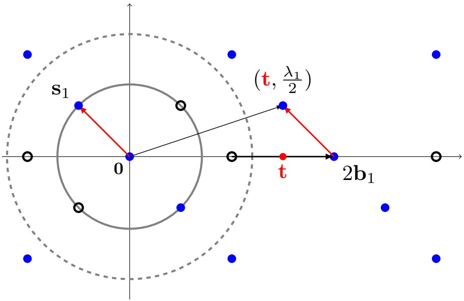
[MG02]: D. Micciancio and S. Goldwasser. Complexity of lattice problem: A cryptography perspective. Kluwer, 2009.

Optimize the embedding

- Recall the last embedded lattice we got.

$$\mathrm{BDD}_{\frac{1}{2\gamma}} \quad \left(\boxed{\mathbf{B}}, \boxed{\mathbf{t}} \right) \xRightarrow[\text{embedding}]{\text{Kannan}} \mathbf{B}' = \begin{bmatrix} \widetilde{\mathbf{B}} & \mathbf{t} \\ \mathbf{0} & \frac{\lambda_1}{2\gamma} \end{bmatrix} \quad \mathrm{uSVP}_{\gamma'}$$

$(n = 1,\ \gamma = 1)$ $\qquad$ $(n' = 2,\ \gamma' > 1)$



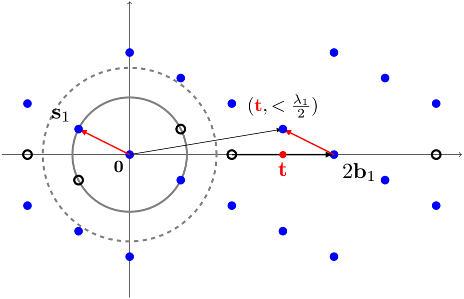
Optimize the embedding

- Decrease embedding height

$$\mathrm{BDD}_{\frac{1}{2\gamma}} \qquad\qquad\qquad \mathrm{uSVP}_{\gamma'}$$

$$\left(\boxed{\mathbf{B}}, \boxed{\mathbf{t}}\right) \xrightarrow[\text{embedding}]{\text{Kannan}} \mathbf{B}' = \begin{bmatrix} \widetilde{\mathbf{B}} & \mathbf{t} \\ \mathbf{0} & \frac{\lambda_1}{2\gamma n} \end{bmatrix}$$

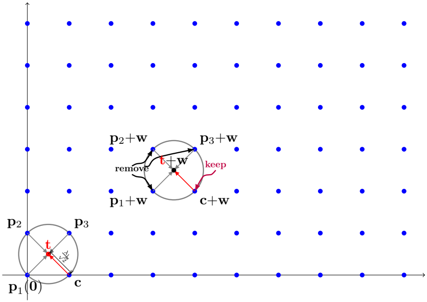
$$(n,\ \gamma = 1) \qquad\qquad\qquad (n' = n+1,\ \gamma' > 1)$$



Optimize the embedding

- Decrease embedding height –> focus on the original lattice.

$$\mathrm{BDD}_{\frac{1}{\sqrt{2}\gamma}}\left(\boxed{\mathbf{B}},\ \boxed{\mathbf{t}}\right) \quad (n,\ \gamma = 1) \xrightarrow[\text{embedding}]{\text{Kannan}} \mathrm{uSVP}_{\gamma'} \quad \mathbf{B}' = \begin{bmatrix} \widetilde{\mathbf{B}} & \mathbf{t}' \\ \mathbf{0} & \frac{\lambda_1}{\sqrt{2}\gamma n} \end{bmatrix} \quad (n' = n+1,\ \gamma' > 1)$$



Optimize the embedding

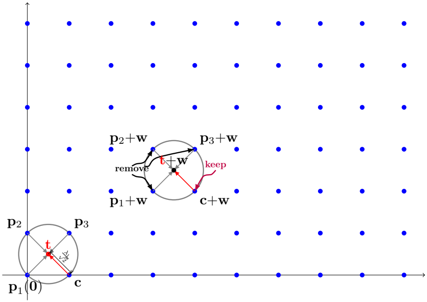
- Decrease embedding height –> focus on the original lattice.

$$\mathrm{BDD}_{\frac{1}{\sqrt{2}\gamma}} \qquad \left(\boxed{\mathbf{B}} \,,\, \boxed{\mathbf{t}} \right) \qquad (n,\, \gamma = 1)$$

$$\xRightarrow[\text{embedding}]{\text{Kannan}}$$

$$\mathrm{uSVP}_{\gamma'} \qquad \lambda_2' > \lambda_1/\sqrt{2}$$

$$\mathbf{B}' = \begin{bmatrix} \widetilde{\mathbf{B}} & \mathbf{t}' \\ \mathbf{0} & \frac{\lambda_1}{\sqrt{2}\gamma n} \end{bmatrix} \qquad (n' = n+1,\, \gamma' > 1)$$



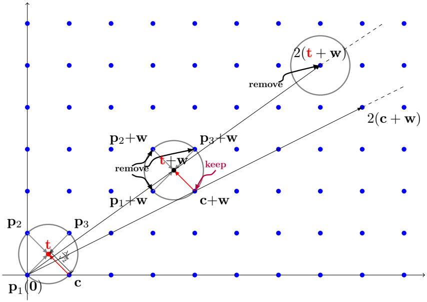
Optimize the embedding

- Accumulate embedding height – sparsify sufficiently many balls.

$$\mathrm{BDD}_{\frac{1}{\sqrt{2}\gamma}}\left(\boxed{\mathbf{B}}, \boxed{\mathbf{t}}\right) \xrightarrow[\text{embedding}]{\text{Kannan}} \mathrm{uSVP}_{\gamma'} \quad \lambda_2' > \lambda_1/\sqrt{2} \ ([1, \gamma n])$$

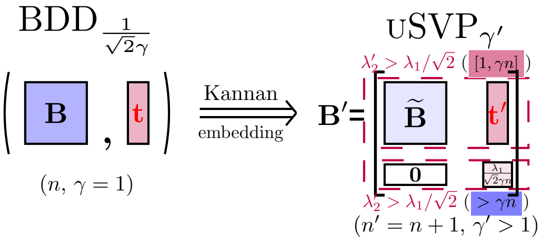
$$\mathbf{B}' = \begin{bmatrix} \widetilde{\mathbf{B}} & \mathbf{t}' \\ \mathbf{0} & \frac{\lambda_1}{\sqrt{2}\gamma n} \end{bmatrix}$$

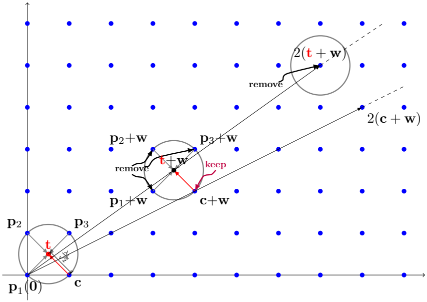
$(n, \gamma = 1)$ $\qquad$ $(n' = n + 1, \gamma' > 1)$



Optimize the embedding

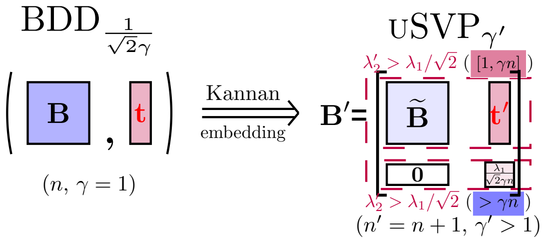
- Accumulate embedding height – sparsify sufficiently many balls.

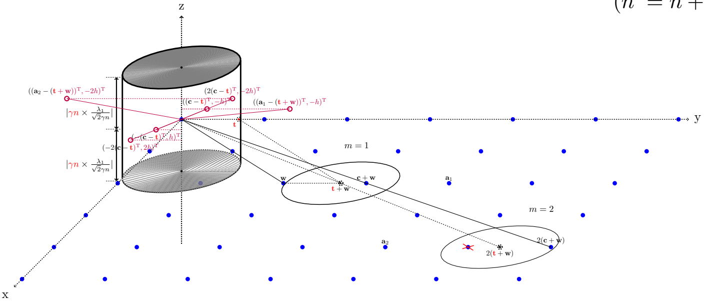




Optimize the embedding

- Accumulate embedding height – sparsify sufficiently many balls.





Algorithm for solving BDD

Version 3. The $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ to uSVP_γ reduction.

Input: a basis $\mathbf{B} = \{\mathbf{b}_i\}_{i\in[n]}$, and a target point $\mathbf{t}$.
Output: a lattice point $\mathbf{c}$ such that $\|\mathbf{c}-\mathbf{t}\| = \mathrm{dist}(\mathbf{t},\mathcal{L})$.

0. Choose $p \geq \gamma n \cdot 2n$ to be prime;
   sample $\mathbf{z}, \mathbf{u} \hookleftarrow \mathbb{Z}_p^n$; compute $\mathbf{w} = \mathbf{B}\bar{\mathbf{u}} \in \mathcal{L}$.
   Let $\mathbf{B}_{p,\mathbf{z}}$ denote the basis of $\mathcal{L}_{p,\mathbf{z}}$.
1. Define
$$\mathbf{B}' = \begin{pmatrix} \mathbf{B}_{p,\mathbf{z}} & \mathbf{t}+\mathbf{w} \\ \mathbf{0} & \frac{\lambda_1(\mathcal{L}(\mathbf{B}))}{\sqrt{2}\gamma n} \end{pmatrix}.$$
2. Run the uSVP_γ solver on input $\mathbf{B}'$. Let $\mathbf{s}' = \begin{pmatrix} \mathbf{s}_1' \\ s_2' \end{pmatrix}$ be its output.
3. Output $\mathbf{t} - \mathbf{s}_1'$.

Algorithm for solving BDD

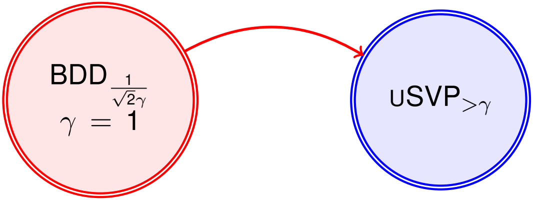
Version 3. The $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ to uSVP_γ reduction.

Input: a basis $\mathbf{B} = \{\mathbf{b}_i\}_{i \in [n]}$, and a target point $\mathbf{t}$.
Output: a lattice point $\mathbf{c}$ such that $\|\mathbf{c} - \mathbf{t}\| = \mathrm{dist}(\mathbf{t}, \mathcal{L})$.

0. Choose $p \geq \gamma n \cdot 2n$ to be prime;
   sample $\mathbf{z}, \mathbf{u} \hookleftarrow \mathbb{Z}_p^n$; compute $\mathbf{w} = \mathbf{B}\bar{\mathbf{u}} \in \mathcal{L}$.
   Let $\mathbf{B}_{p,\mathbf{z}}$ denote the basis of $\mathcal{L}_{p,\mathbf{z}}$.
1. Define
$$\mathbf{B}' = \begin{pmatrix} \mathbf{B}_{p,\mathbf{z}} & \mathbf{t} + \mathbf{w} \\ \mathbf{0} & \frac{\lambda_1(\mathcal{L}(\mathbf{B}))}{\sqrt{2}\gamma n} \end{pmatrix}.$$
2. Run the uSVP_γ solver on input $\mathbf{B}'$. Let $\mathbf{s}' = \begin{pmatrix} \mathbf{s}'_1 \\ s'_2 \end{pmatrix}$ be its output.
3. Output $\mathbf{t} - \mathbf{s}'_1$.

Reduction is efficient for $\gamma \leq \mathrm{poly}(n)$.

Our result

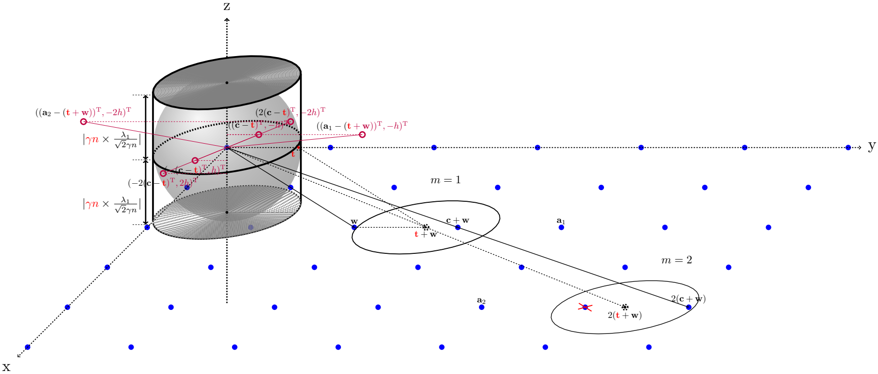


The reduction algorithm also works for any γ with $\gamma \leq \mathrm{poly}(n)$.

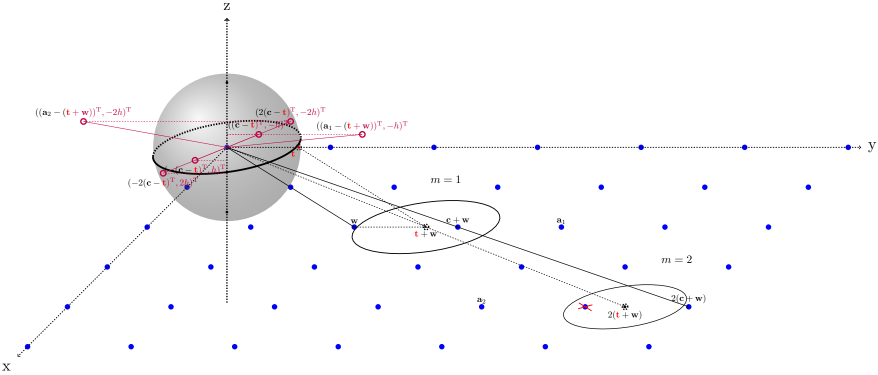
This algorithm actually works for any $\gamma \geq 1$,
thanks Stephens-Davidowitz for the observation.

Intuition of extension for any $\gamma > 1$

- A tighter view on the reduction.

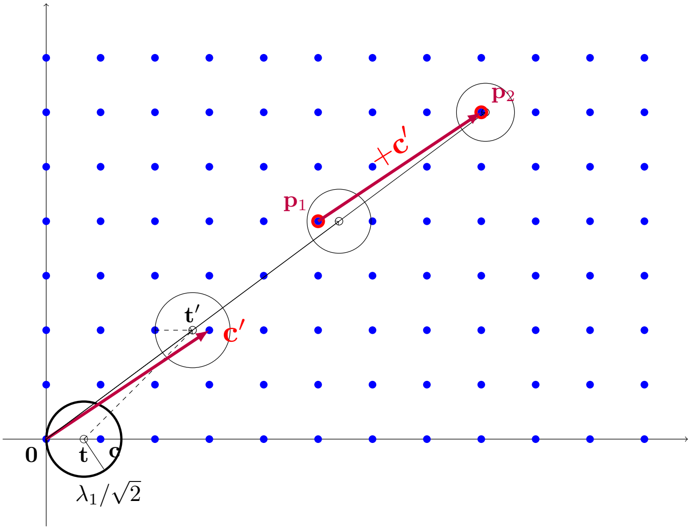


- A tighter view on the reduction.



Intuition of extension for any $\gamma > 1$

- Intuition of the improvement.



Road map

- Background
- The Lyubashevsky and Micciancio reduction and its limitation
- New reduction:
  - lattice sparsification.
  - example for $\gamma = 1$.
  - sphere packing.
- Open problems

Open problems

- The sparsification in our reduction heavily relies on randomness.

  - Problem 1. Remove the sparsification randomness.

- In practice, randomly chosen lattice is sparse enough such that there is almost no point within $\lambda_1/\sqrt{2}$-radius.

  - Problem 2. Is sparsification just an artifact?

Open problems

- Conjecture: BDD and uSVP are computationally identical.

$$\text{BDD}_{\frac{1}{c\cdot\gamma}} = \text{uSVP}_{\gamma}$$

$$c \in [1, \sqrt{2}]$$

- Problem 3. What is the constant c? Is $c = \sqrt{2}$?