# Improved Reduction from BDD to uSVP

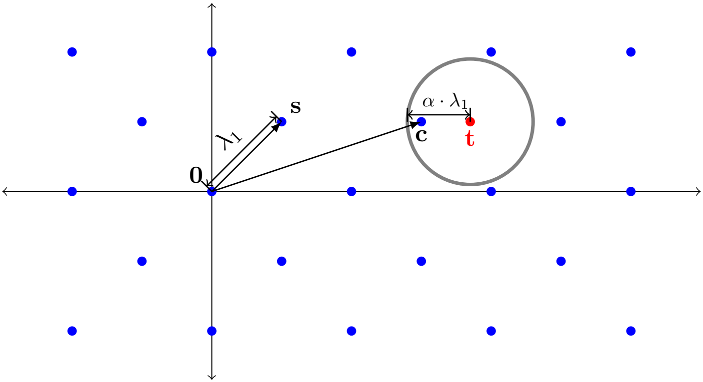
Shi Bai, Damien Stehlé, **Weiqiang Wen**

École Normale Supérieure de Lyon

ICALP, July 15, 2016, Rome, Italy

European Research Council

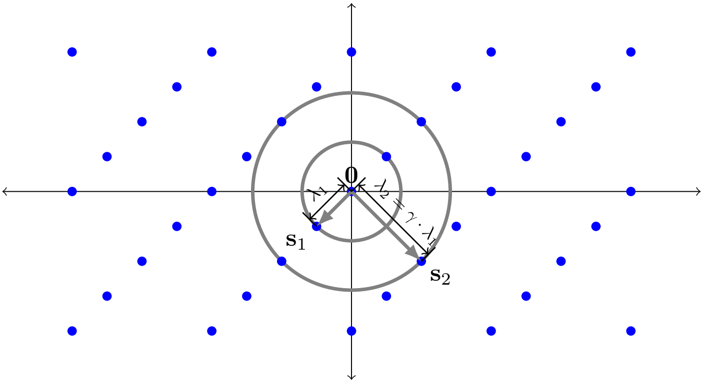
ENS DE LYON




**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 $\mathbf{t}$.

## Bounded Distance Decoding (BDD) and unique Shortest Vector Problem (uSVP)




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

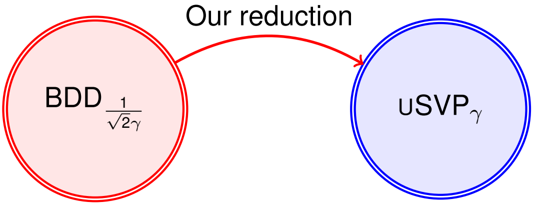
Input: $\mathbf{B} \in \mathbb{Q}^{n \times n}$ such that $\lambda_2(\mathcal{L}(\mathbf{B})) \geq \gamma \cdot \lambda_1(\mathcal{L}(\mathbf{B}))$.
Output: a non-zero vector $\mathbf{s}_1 \in \mathcal{L}(\mathbf{B})$ of norm $\lambda_1(\mathcal{L}(\mathbf{B}))$.

# Main result

## Improved reduction from BDD to uSVP

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

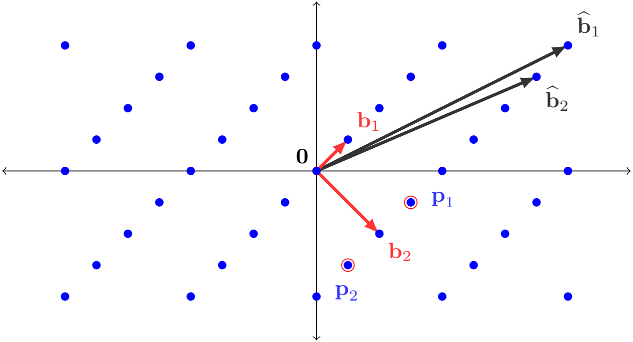
$$\mathrm{BDD}_{1/(\sqrt{2}\gamma)} \leq \mathrm{uSVP}_\gamma.$$



# Road map

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

# Lattices

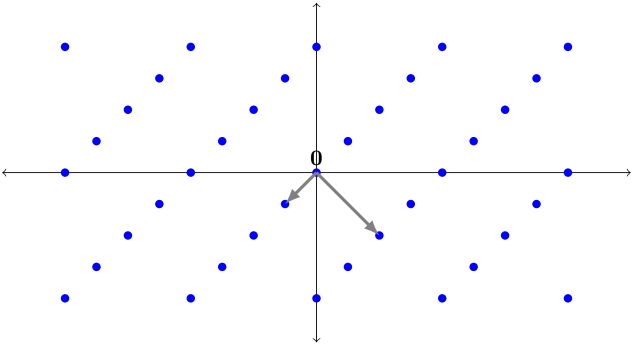



## A definition of lattice

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

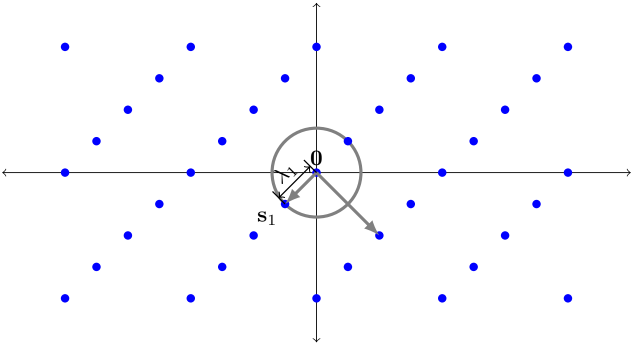



## Lattice minimum

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

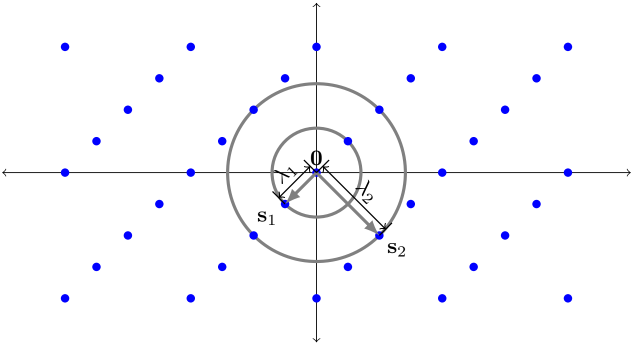



## Lattice minimum

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

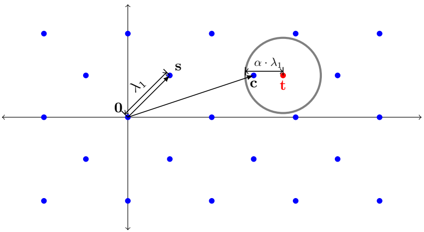



## Lattice minimum

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

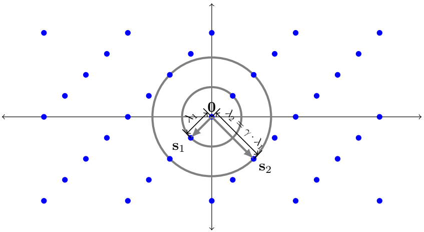
$$\lambda_i(\mathcal{L}) = \inf\{r : \dim(\mathrm{span}(\mathcal{L} \cap \mathcal{B}(\mathbf{0}, r))) \geq i\}.$$

# Why is BDD interesting?



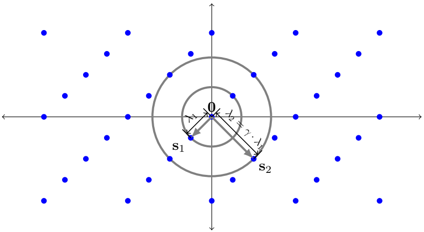

- In **cryptography**:
  - Learning With Error (LWE) problem serves as a security foundation.
  - LWE is an average-case variant of BDD.
- In **communication theory** – white Gaussian noise channel:
  - Wifi, mobile phone *etc*;
  - View message as a lattice point, Gaussian noise is added in channel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

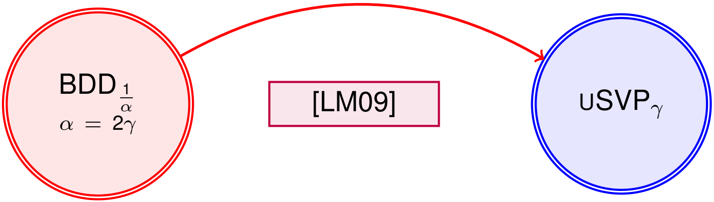
# Why is uSVP interesting?




- 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.

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

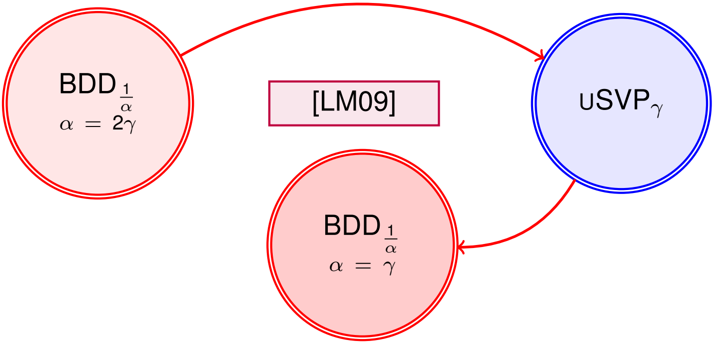
# Prior works on BDD to uSVP




- Slightly improved for some $\alpha$, 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 $\lambda_2$-gap. Inf. Process. Lett., 2014.
[Ga15]: Private communication, 2015.
[Mi15]: Private communication, 2015.

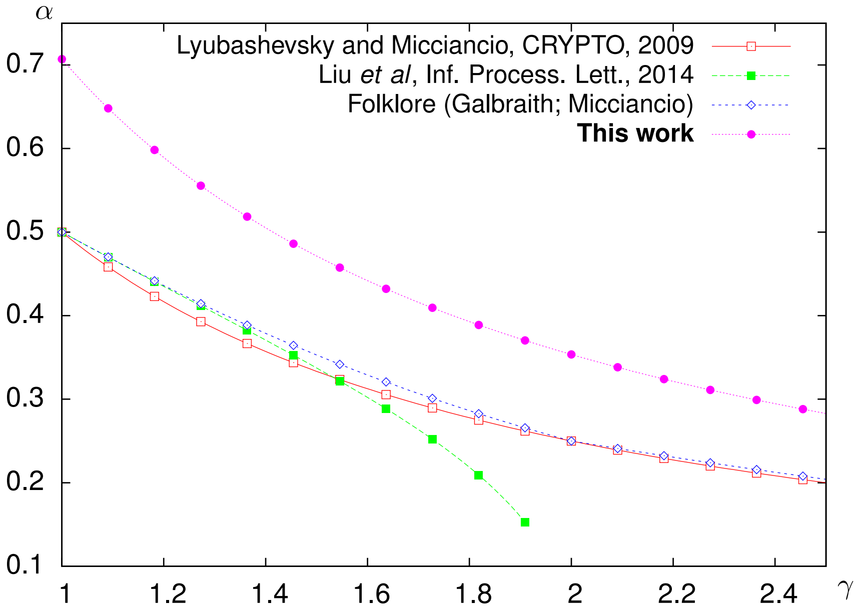
# Prior works on BDD to uSVP




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 $\lambda_2$-gap. Inf. Process. Lett., 2014.
[Ga15]: Private communication, 2015.
[Mi15]: Private communication, 2015.

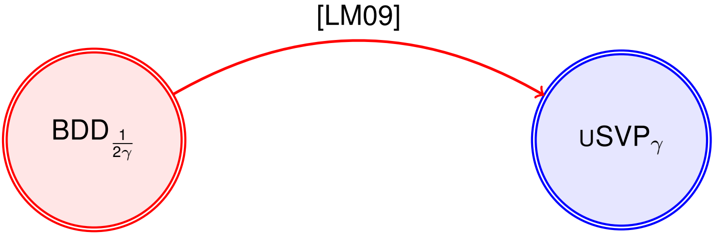
# Comparison with prior works



# The Lyubashevsky and Micciancio reduction

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

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



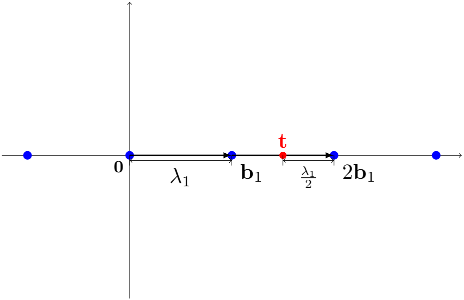

[LM09]: V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem, CRYPTO, 2009.

# Lyubashevsky-Micciancio reduction for $\gamma = 1$

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

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

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

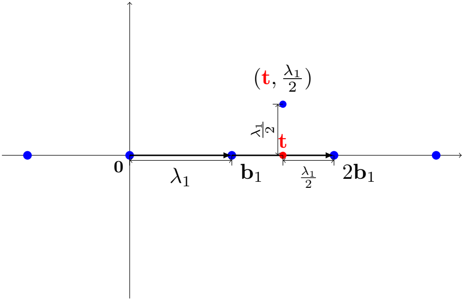


# Lyubashevsky-Micciancio reduction for $\gamma = 1$

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

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

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

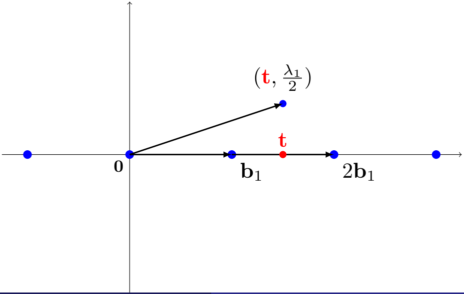


# Lyubashevsky-Micciancio reduction for $\gamma = 1$

- Kannan embedding.

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

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



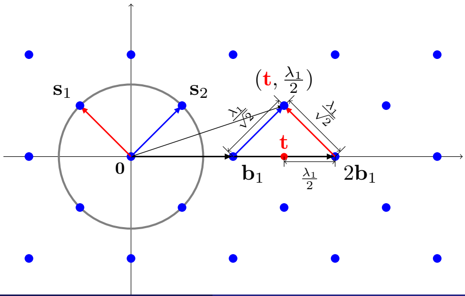
# Lyubashevsky-Micciancio reduction for $\gamma = 1$

- We are at the limit: $\lambda'_1 = \lambda'_2$.

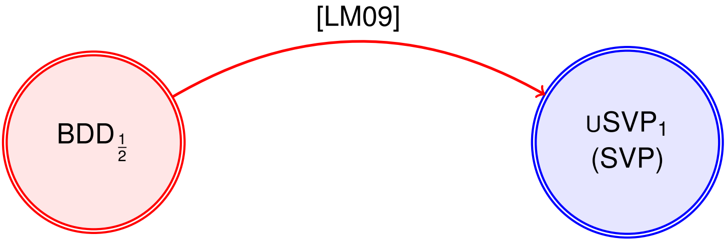
$$\mathrm{BDD}_{\frac{1}{2\gamma}} \qquad\qquad \mathrm{uSVP}_{\gamma'}$$

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

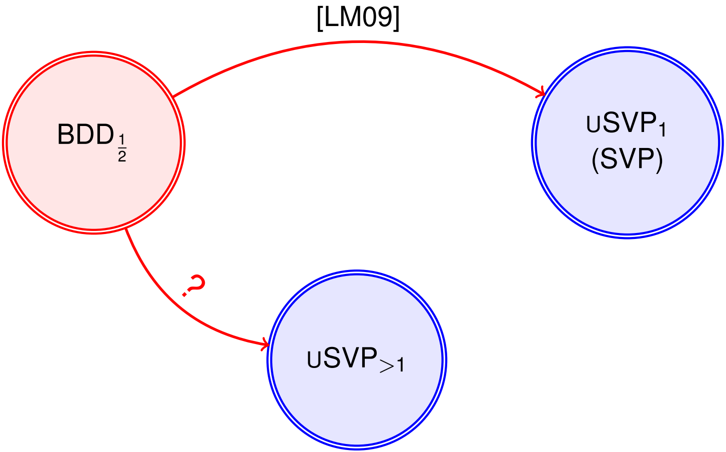
$$(n = 1,\ \gamma = 1) \qquad\qquad (n' = 2,\ \gamma' = 1)$$



# This is the best this reduction can achieve

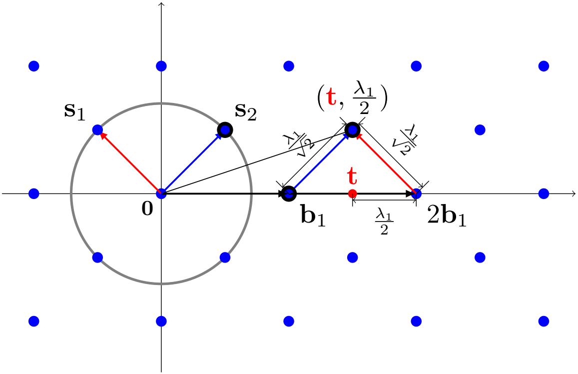


# Can we improve it?



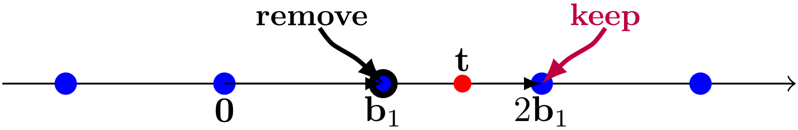
# An attempt to circumvent the limitation

- Limitation in the Lyubushevsky and Micciancio reduction.



# An attempt to circumvent the limitation

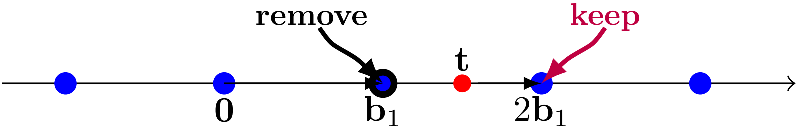
- A simple deterministic sparsification.
- Lattice $\mathcal{L}(\mathbf{B})$ with $\mathbf{B} = [\mathbf{b}_1]$.



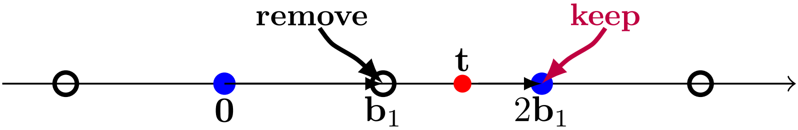
# An attempt to circumvent the limitation

- A simple deterministic sparsification.

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

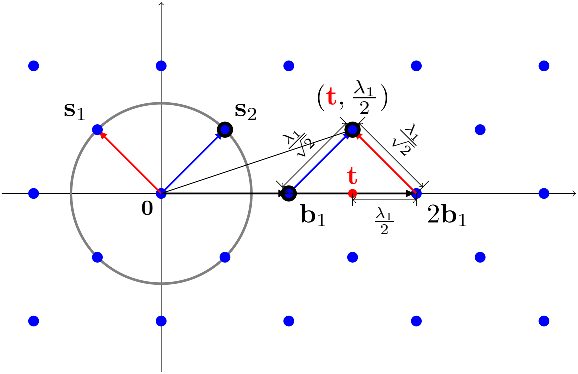



- Lattice $\mathcal{L}(\widetilde{\mathbf{B}})$ with $\widetilde{\mathbf{B}} = [2\mathbf{b}_1]$.



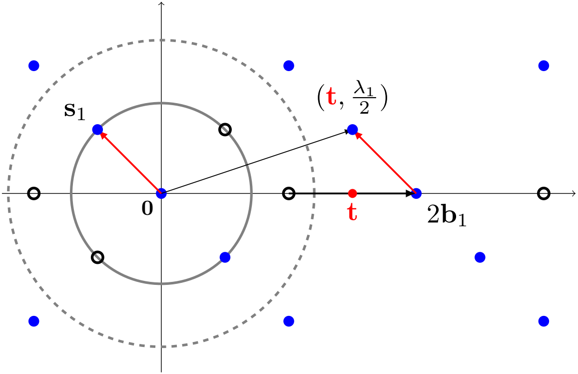
# An attempt to circumvent the limitation

- Recall the limitation: $\lambda_2' = \lambda_1'$



# An attempt to circumvent the limitation

- Limitation is circumvented (for this example): $\lambda'_2 > \lambda'_1$ now!



# Main idea

- But we want more...

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

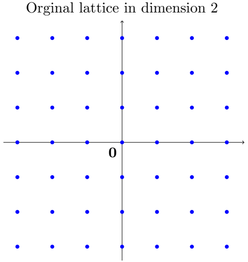
# The main tool: sparsification

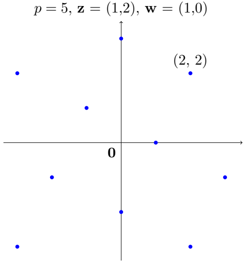
## Khot's Lattice Sparsification [K03] (Adapted by [S14])

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




[K03]: S. Khot. Hardness of approximating the shortest vector problem in high $L_p$ norms. FOCS'03, 2003.
[S14]: N. Stephens-Davidowitz. Discrete Gaussian sampling reduces to CVP and SVP. In *Proc. of SODA*, 2016.

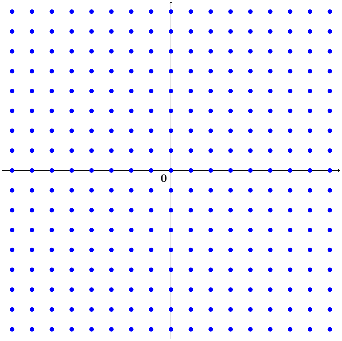
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




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

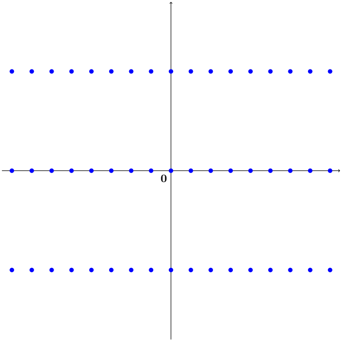
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




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

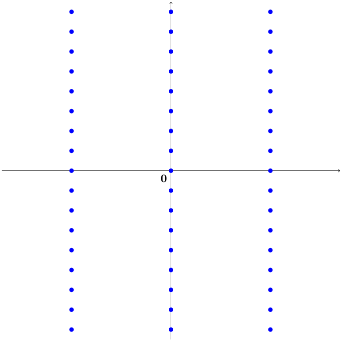
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **3**rd sublattice: $p = 5$, $\mathbf{z} = (1, 0)$.

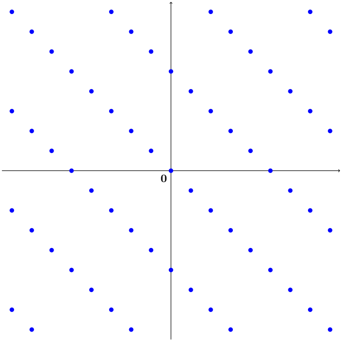
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




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

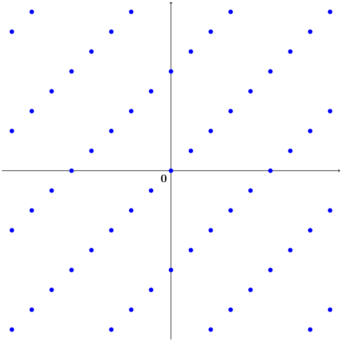
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{Bu}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




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

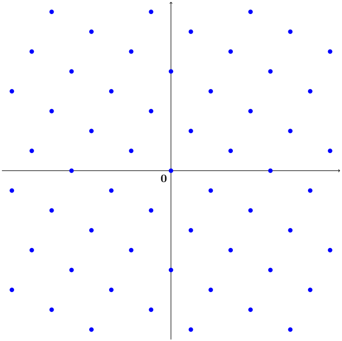
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{Bu}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




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

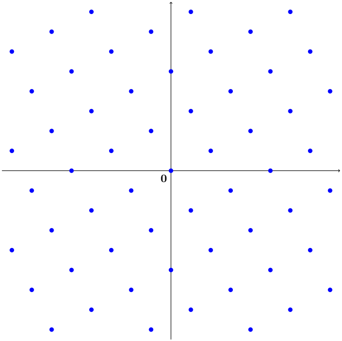
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




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

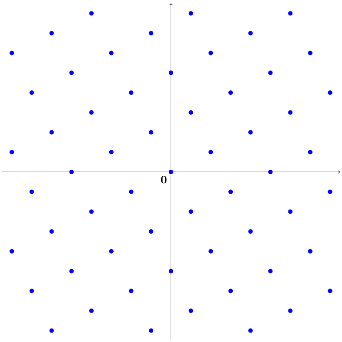
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{Bu}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **1**th shift: $\mathbf{w} = (0, 0)$.

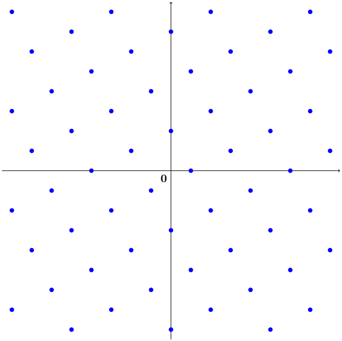
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **2**nd shift: $\mathbf{w} = (1, 0)$.

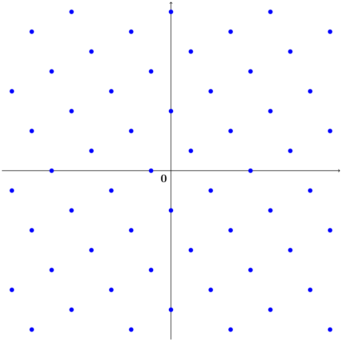
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **3**rd shift: $\mathbf{w} = (1, 1)$.

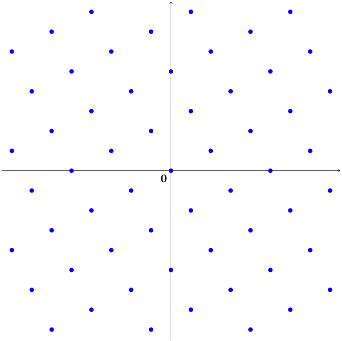
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **4**th shift: $\mathbf{w} = (2, 1)$.

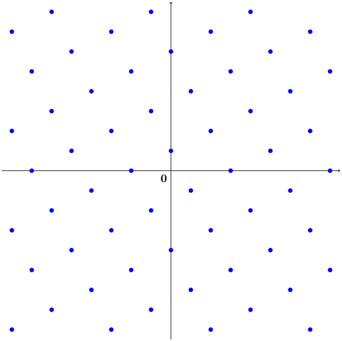
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **5**th shift: $\mathbf{w} = (2, 2)$.

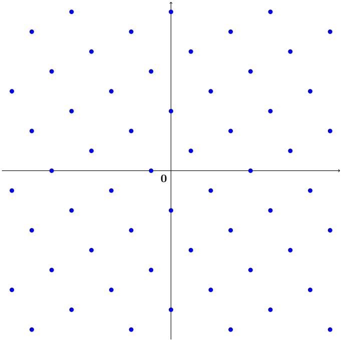
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **6**th shift: $\mathbf{w} = (3, 2)$.

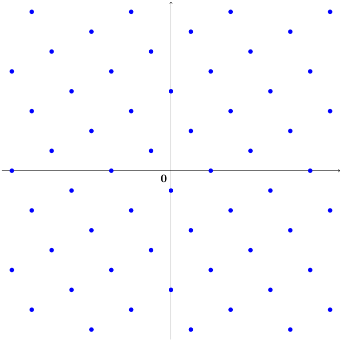
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{Bu}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **7**th shift: $\mathbf{w} = (3, 3)$.

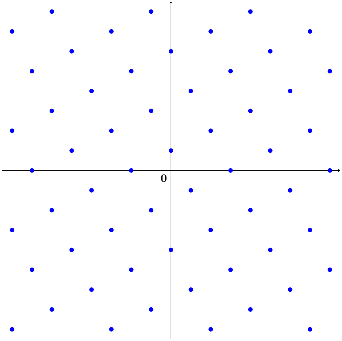
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{B}\mathbf{u}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice:
  $p = 5$, $\mathbf{z} = (1, 3)$.
- **8**th shift: $\mathbf{w} = (4, 3)$.

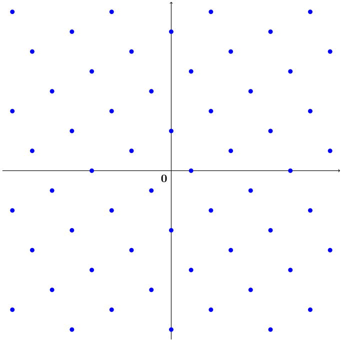
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{Bu}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **9**th shift: $\mathbf{w} = (4, 4)$.

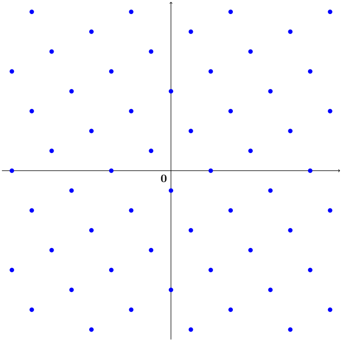
# The main tool: sparsification

## Khot's Lattice Sparsification

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

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

where $p$ is a prime integer, $\mathbf{z} \in \mathbb{Z}_p^n$ and $\mathbf{w} = \mathbf{Bu}$ for $\mathbf{u} \leftarrow U(\mathbb{Z}_p^n)$.




- **7**th sublattice: $p = 5$, $\mathbf{z} = (1, 3)$.
- **10**th shift: $\mathbf{w} = (5, 4)$.

# Main result of the sparsification

## A probabilistic argument on Khot's sparsification [S14]

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

$$\Pr_{\mathbf{z} \hookleftarrow U(\mathbb{Z}_q^n)} \left[ \forall i, \quad \begin{matrix} \mathbf{x} \in \mathcal{L}_{p,\mathbf{z}} + \mathbf{w} \\ \mathbf{v}_i \notin \mathcal{L}_{p,\mathbf{z}} + \mathbf{w} \end{matrix} \right] \geq \frac{1}{p} - \frac{N}{p^2} - \frac{N}{p^{n-1}},$$

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

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

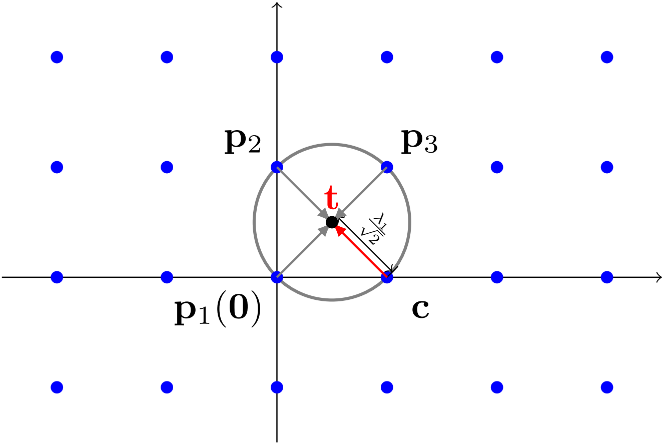
is the (approximate) probability to

- **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.

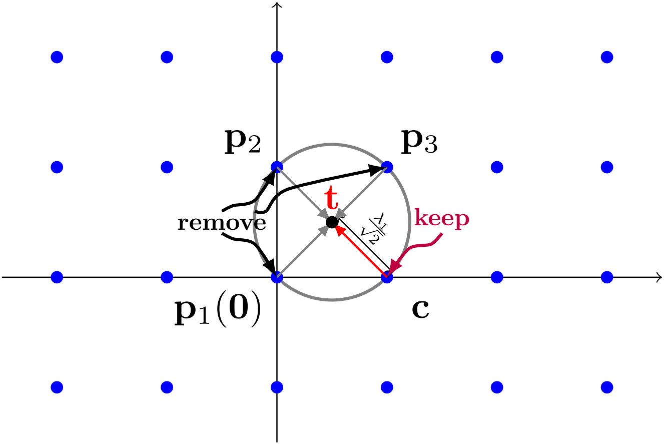
# New reduction for $\gamma = 1$

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



# New reduction for $\gamma = 1$

- Remove annoying points around the target **t**.



# 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:

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

- 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.

# 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 $\leq \mathrm{poly}(n)$.

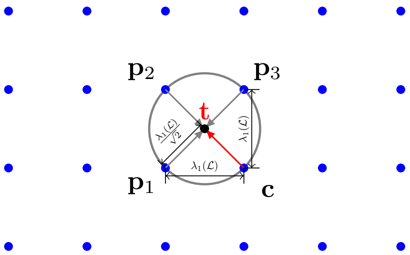
We can sparsify the lattice by removing polynomially many points.

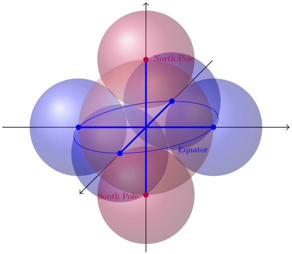
What is the worst-case list decoding radius?

# 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 $\#\mathcal{L} \cap \mathcal{B}(\mathbf{t}, \lambda_1(\mathcal{L})/\sqrt{2}) \leq 2n$.

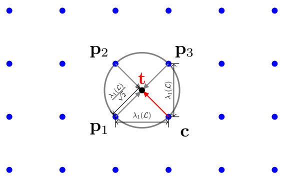


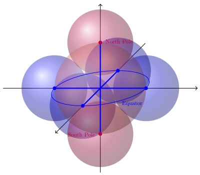




[MG02]: D. Micciancio and S. Goldwasser. Complexity of lattice problem: A cryptography perspective. Kluwer, 2009.

## 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 $\#\mathcal{L} \cap \mathcal{B}(\mathbf{t}, \lambda_1(\mathcal{L})/\sqrt{2}) \leq 2n$.



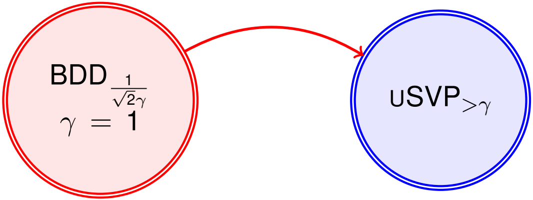




## Extremely dense lattice, adapted from [MG02, Lem. 4.1]

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.

# Our result




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

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

# 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.

$$\mathrm{BDD}_{\frac{1}{c\cdot\gamma}} = \mathrm{uSVP}_{\gamma}$$
$$c \in [1, \sqrt{2}]$$

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