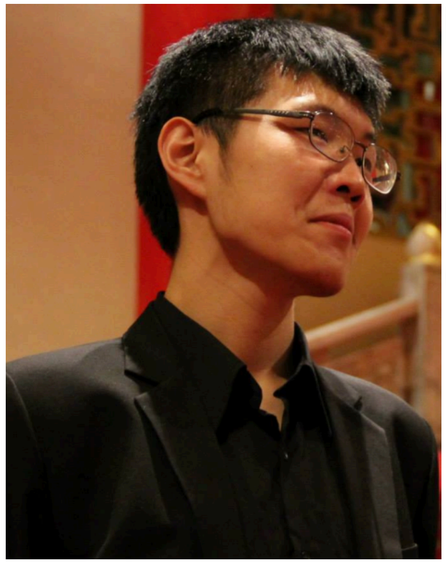
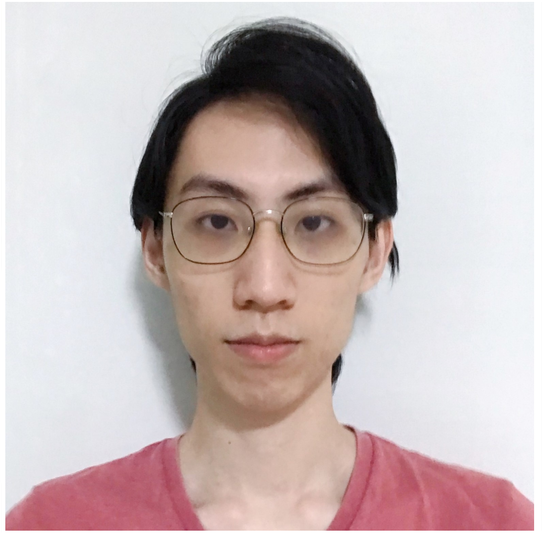
Dimension Preserving Reductions Between SVP and CVP in Different p-Norms

Divesh Aggarwal
CQT and SoC, NUS



Yanlin Chen
CWI

Rajendra Kumar
IITK & SoC, NUS
——> CQT, NUS



Zeyong Li
CQT, NUS

Noah Stephens-Davidowitz
Cornell University

SIGTACS, IIT Kanpur

Lattice-based Cryptography

Lattice-based Cryptography

- Conjectured to be secure even after Quantum computers.

Lattice-based Cryptography

- Conjectured to be secure even after Quantum computers.

- Unlike other cryptosystem, there security can be based on worst case hardness of lattice problems [Ajtai,1996].

Lattice-based Cryptography

- Conjectured to be secure even after Quantum computers.

- Unlike other cryptosystem, there security can be based on worst case hardness of lattice problems [Ajtai,1996].

- Many powerful crypto primitives are only known via lattices (such as Fully homomorphic encryption).

Lattice-based Cryptography

- Conjectured to be secure even after Quantum computers.

- Unlike other cryptosystem, there security can be based on worst case hardness of lattice problems [Ajtai,1996].

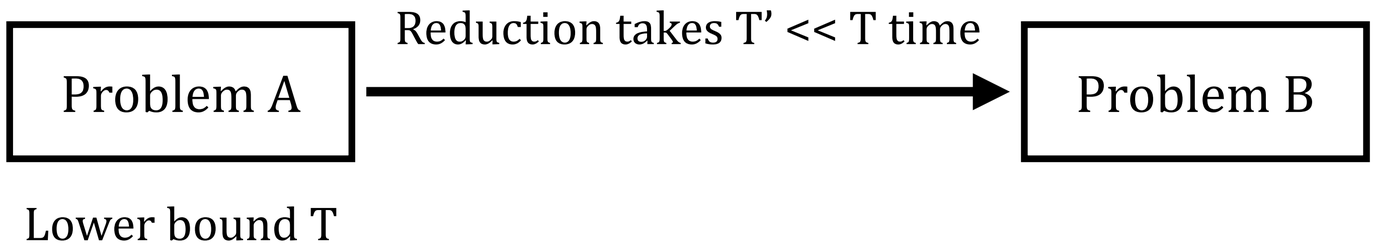
- Many powerful crypto primitives are only known via lattices (such as Fully homomorphic encryption).

- Most popular candidate for post-quantum cryptography (classical crypto system secure even after quantum computer)

Exponential Time Reductions

- Polynomial Time Reduction are used to prove the NP-Hardness of the problem.

- Exponential Time Reductions:
  - If we believe problem is exponentially hard.
  - Implies the fine-grained hardness.



Lattices

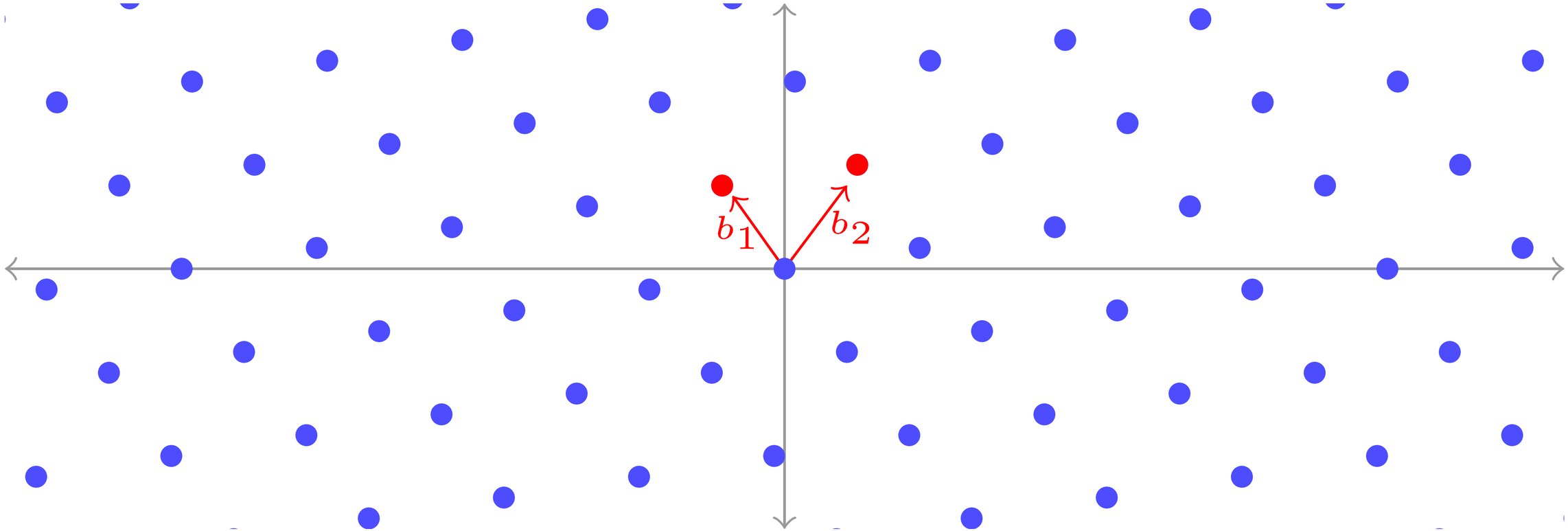
Lattices

Lattices

- A Lattice $\mathscr{L}$ is a discrete set of points in $\mathbb{R}^m$.

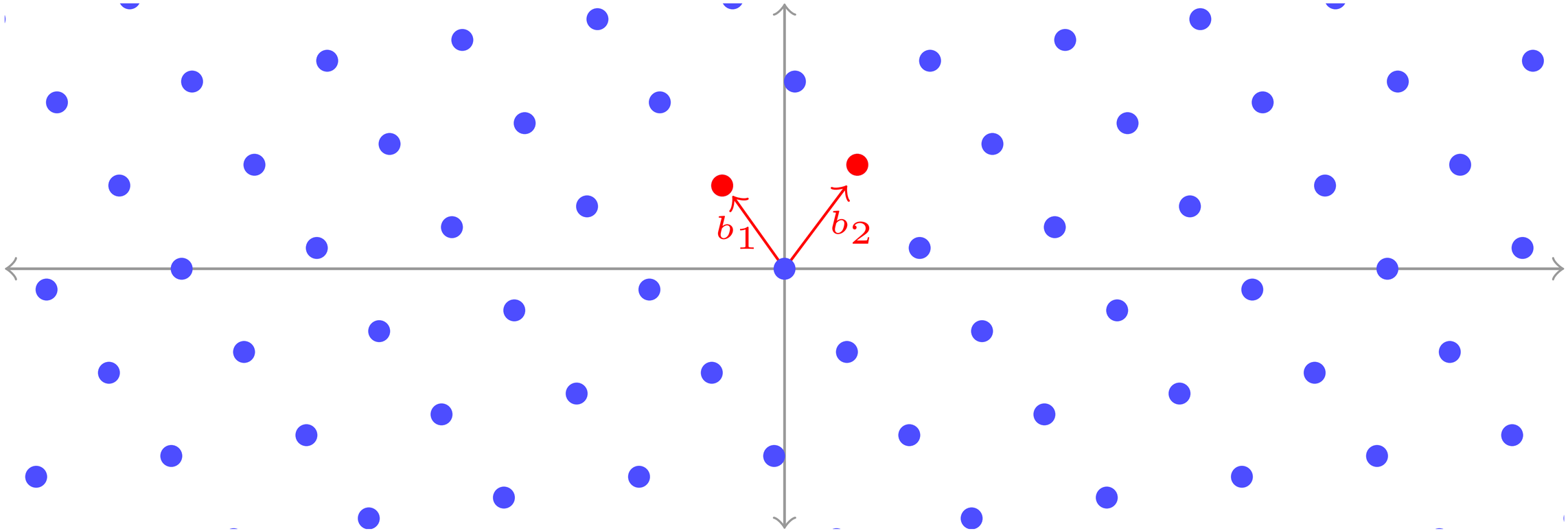
Lattices

- A Lattice $\mathscr{L}$ is a discrete set of points in $\mathbb{R}^m$.



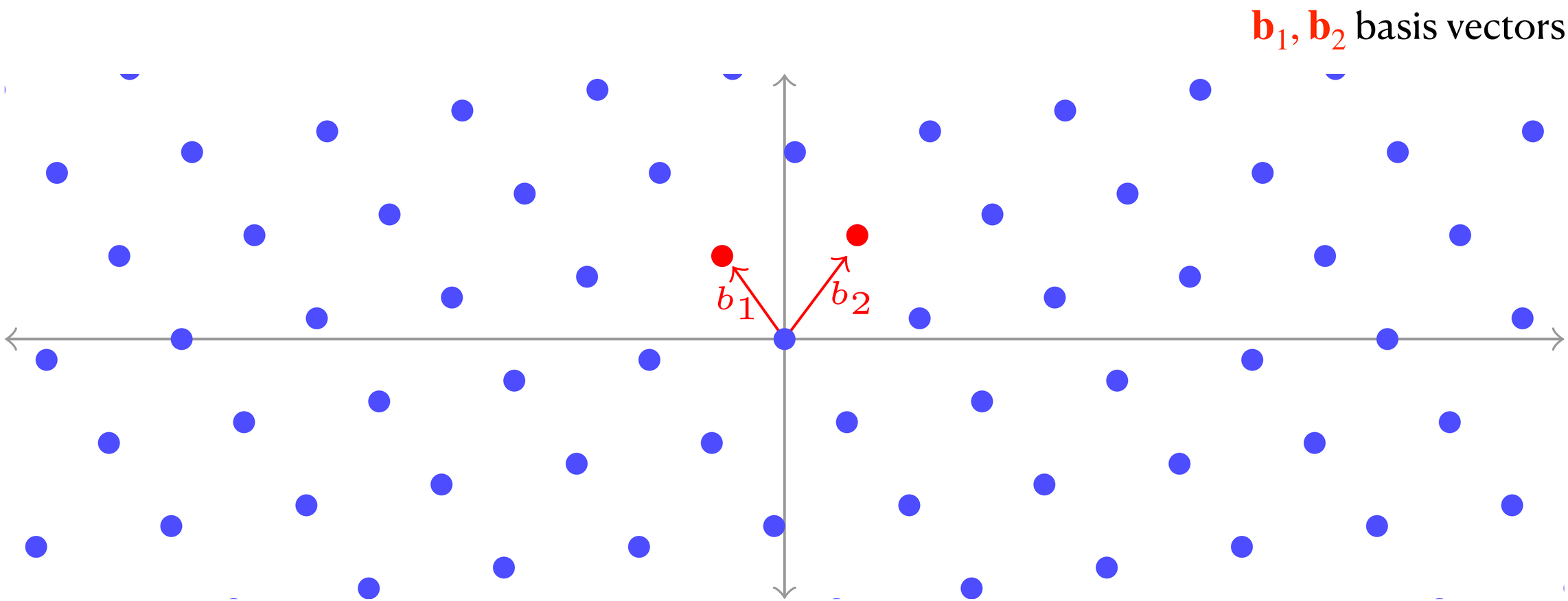
Lattices

- A Lattice $\mathscr{L}$ is a discrete set of points in $\mathbb{R}^m$.
- Specified by a basis $\mathbf{b}_1, \cdots, \mathbf{b}_n$, linearly independent vectors.



Lattices

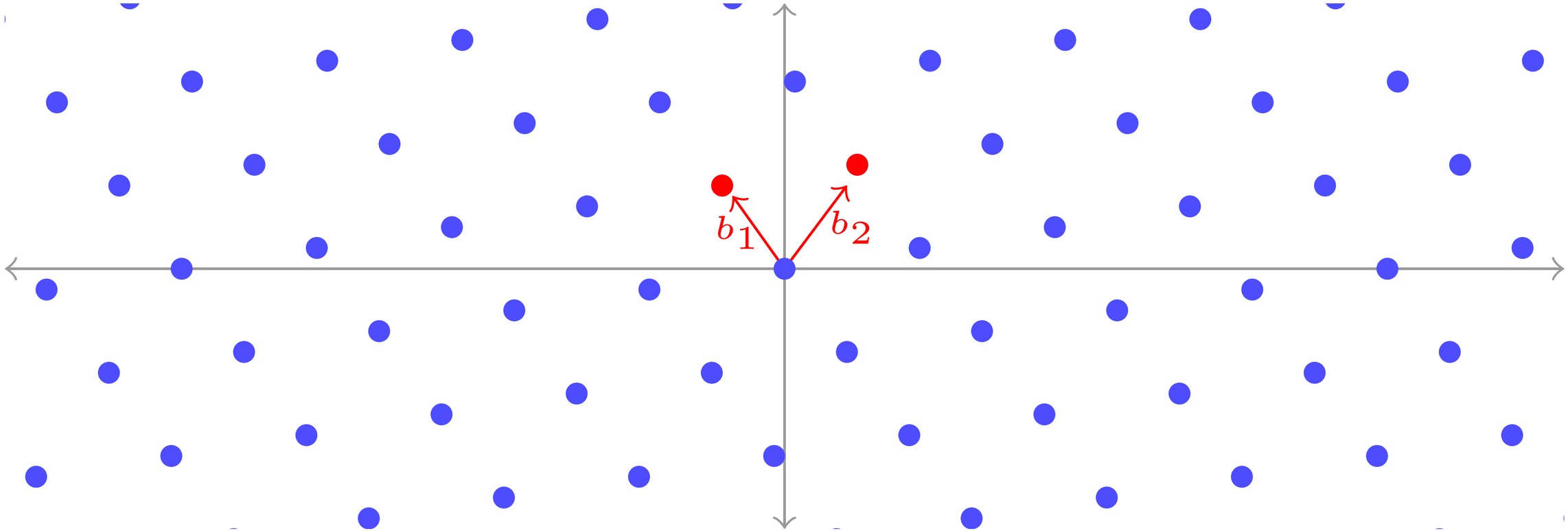
- A Lattice $\mathscr{L}$ is a discrete set of points in $\mathbb{R}^m$.
- Specified by a basis $\mathbf{b}_1, \cdots, \mathbf{b}_n$, linearly independent vectors.



Lattices

- A Lattice $\mathscr{L}$ is a discrete set of points in $\mathbb{R}^m$.
- Specified by a basis $\mathbf{b}_1, \cdots, \mathbf{b}_n$, linearly independent vectors.
- $\mathscr{L} = \{z_1\mathbf{b}_1 + \cdots + z_n\mathbf{b}_n \,|\, z_i \in \mathbb{Z}\}$, rank=$n$, dimension=$m$.

$\mathbf{b}_1, \mathbf{b}_2$ basis vectors



Notations

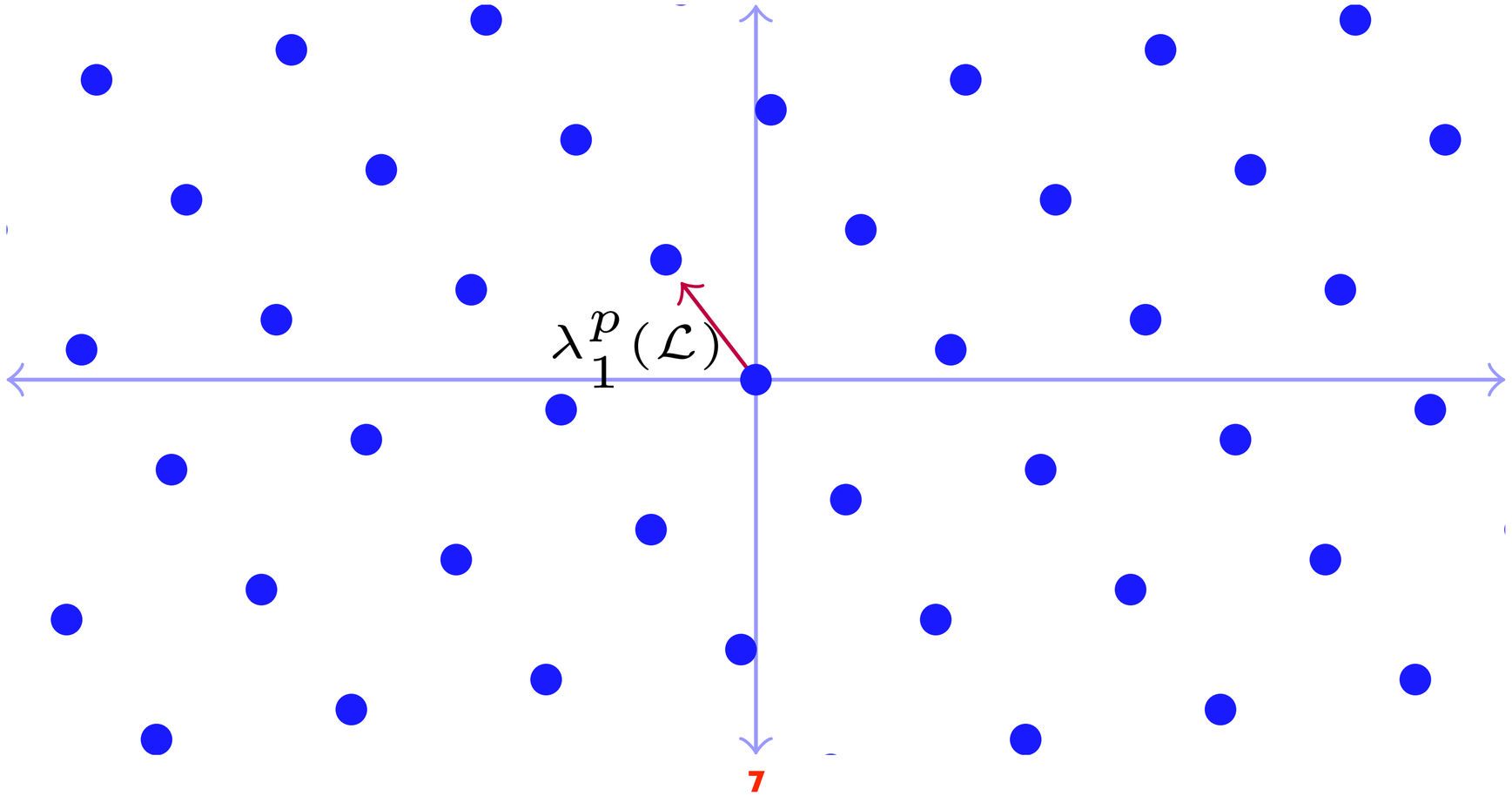
- ℓ_p norm:

$$p \in [1,\infty),\ \|\mathbf{v}\|_p := \left(\sum_{i=1}^{m} |v_i|^p \right)^{1/p}$$

$$p = \infty,\ \|\mathbf{v}\|_\infty := \max_i |v_i| .$$

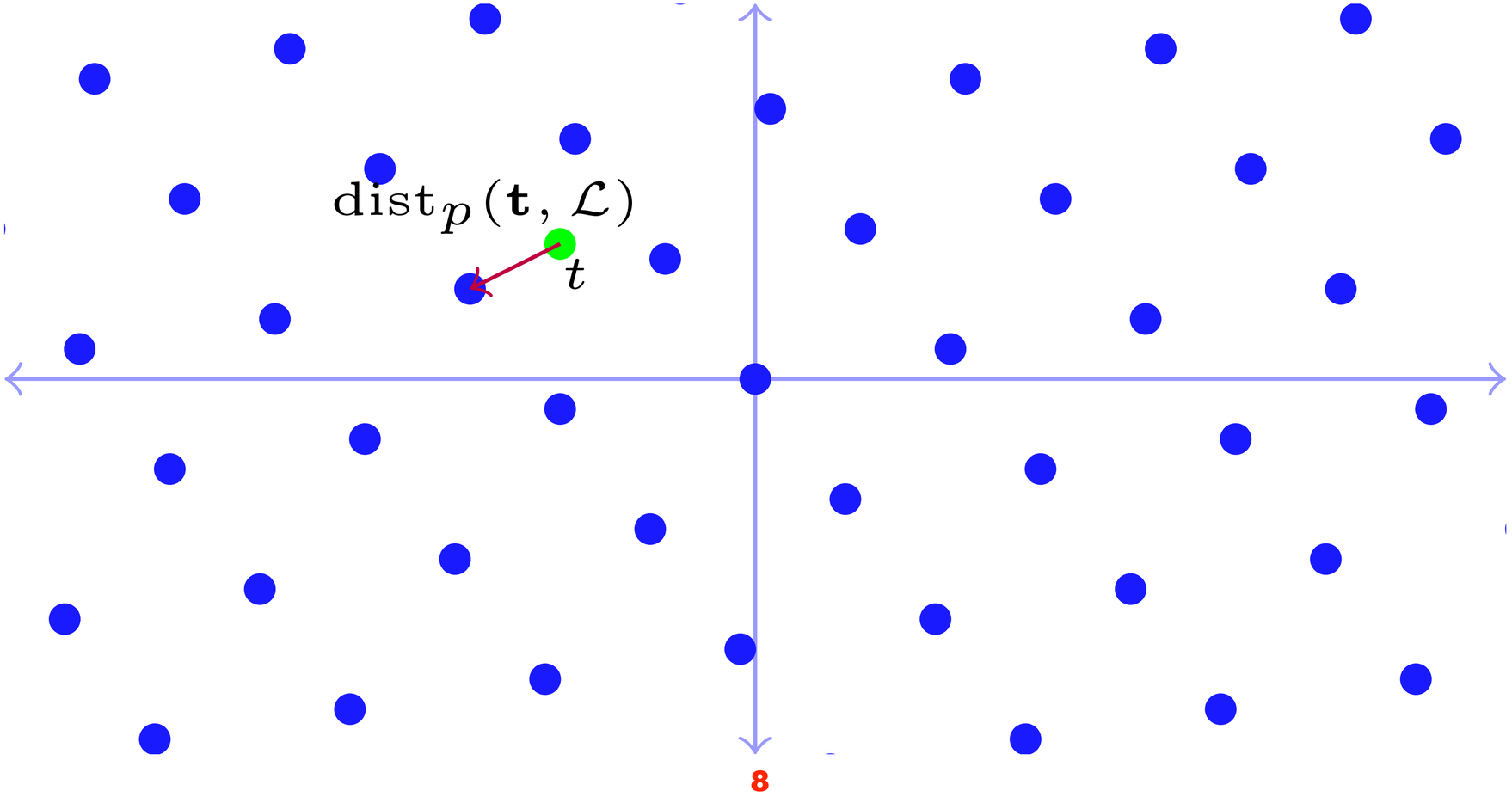
Notations

- For any lattice $\mathscr{L}$, $\lambda_1^p(\mathscr{L}) = \min_{\mathbf{u}\neq\mathbf{0},\mathbf{u}\in\mathscr{L}} \|\mathbf{u}\|_p$.



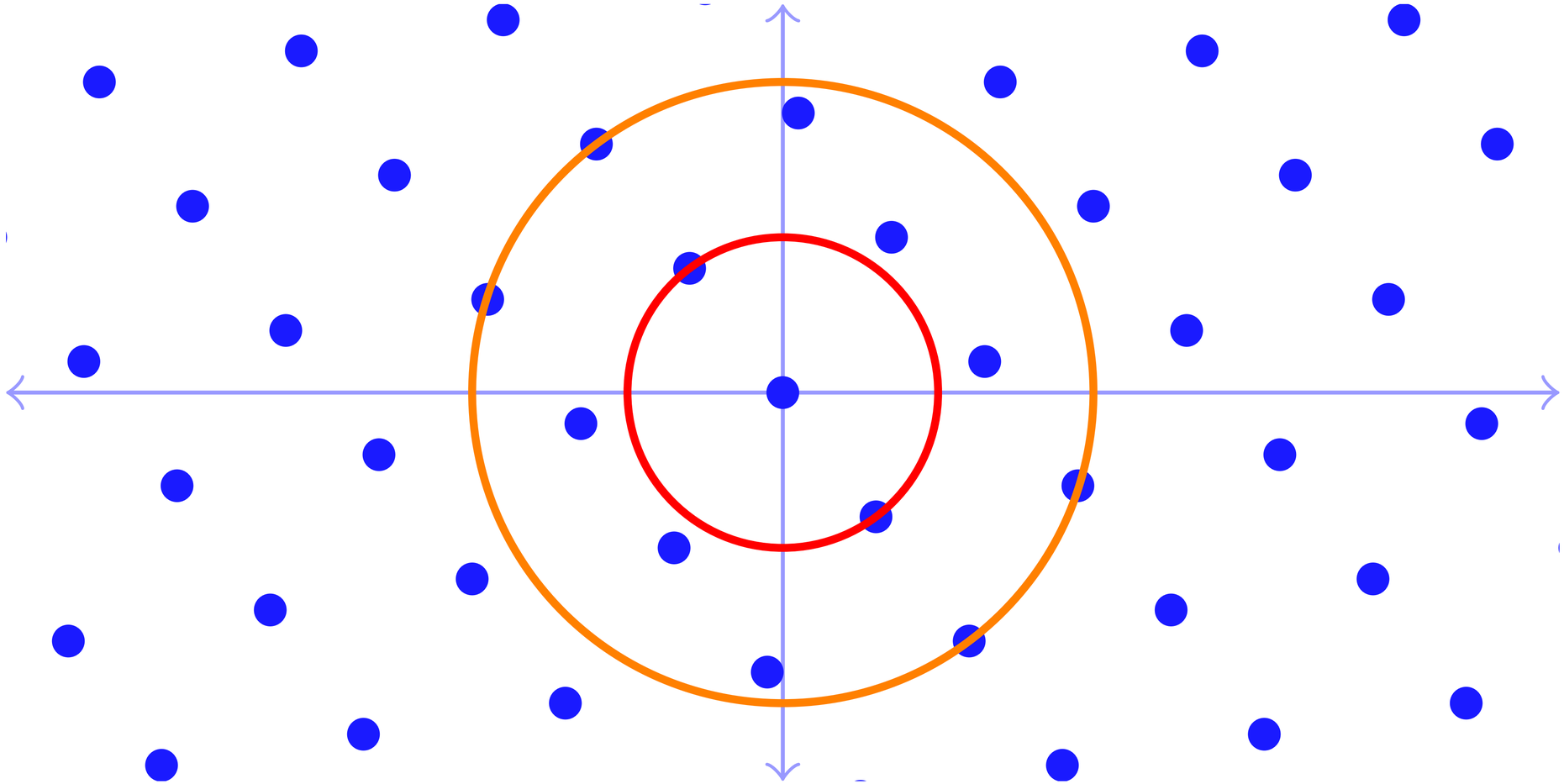
Notations

- For any lattice $\mathscr{L}$ and target vector $\mathbf{t}$, $\mathrm{dist}_p(\mathbf{t}, \mathscr{L}) = \min_{\mathbf{u} \in \mathscr{L}} \|\mathbf{u} - \mathbf{t}\|_p$.



Notations

- ℓ_p ball, $r\mathcal{B}_p^m := \{\mathbf{x} \in \mathbb{R}^m : \|\mathbf{x}\|_p \leq r\}$.



$\lambda_1^p(\mathscr{L})\mathcal{B}_p^m$ $2\lambda_1^p(\mathscr{L})\mathcal{B}_p^m$

Shortest Vector Problem

Shortest Vector Problem

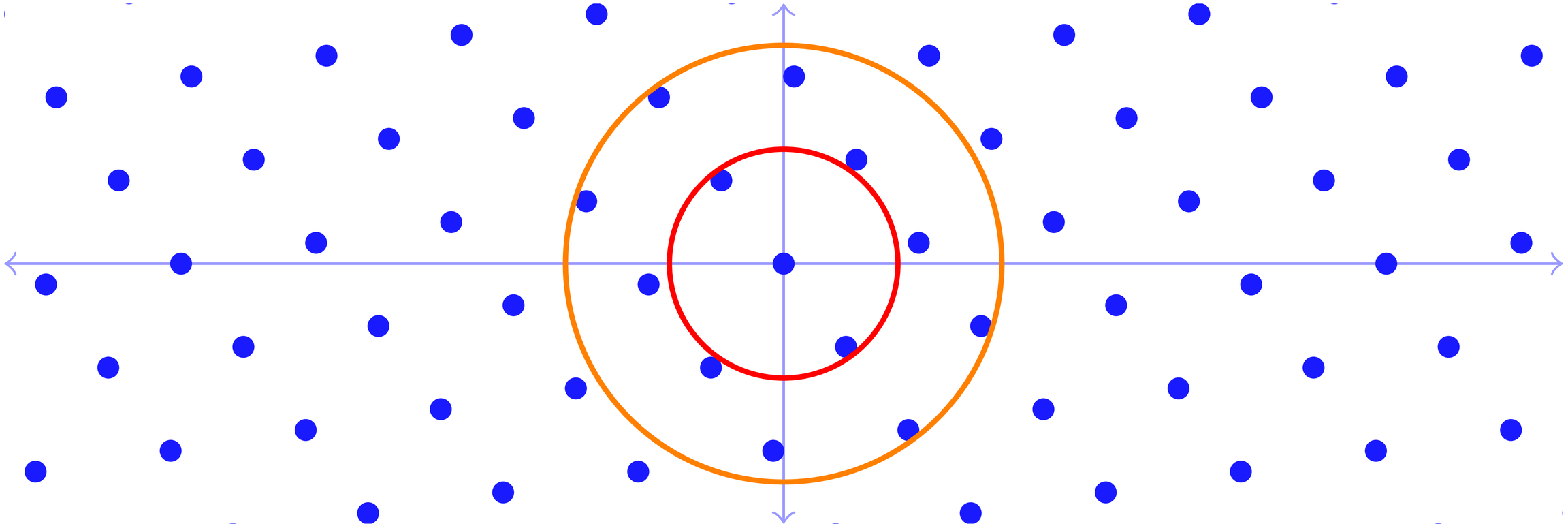
Shortest Vector Problem (γ-SVP$_p$) : Given a basis $\mathbf{B}$ of lattice $\mathscr{L}$, find a lattice vector $\mathbf{v}$ such that,

$$0 < \|\mathbf{v}\|_p \leq \gamma \cdot \lambda_1^p(\mathscr{L}) \text{ where } \lambda_1^p(\mathscr{L}) = \min_{\mathbf{u} \neq \mathbf{0}, \mathbf{u} \in \mathscr{L}} \|\mathbf{u}\|_p.$$

Shortest Vector Problem

Shortest Vector Problem (γ-SVP$_p$) : Given a basis $\mathbf{B}$ of lattice $\mathscr{L}$, find a lattice vector $\mathbf{v}$ such that,

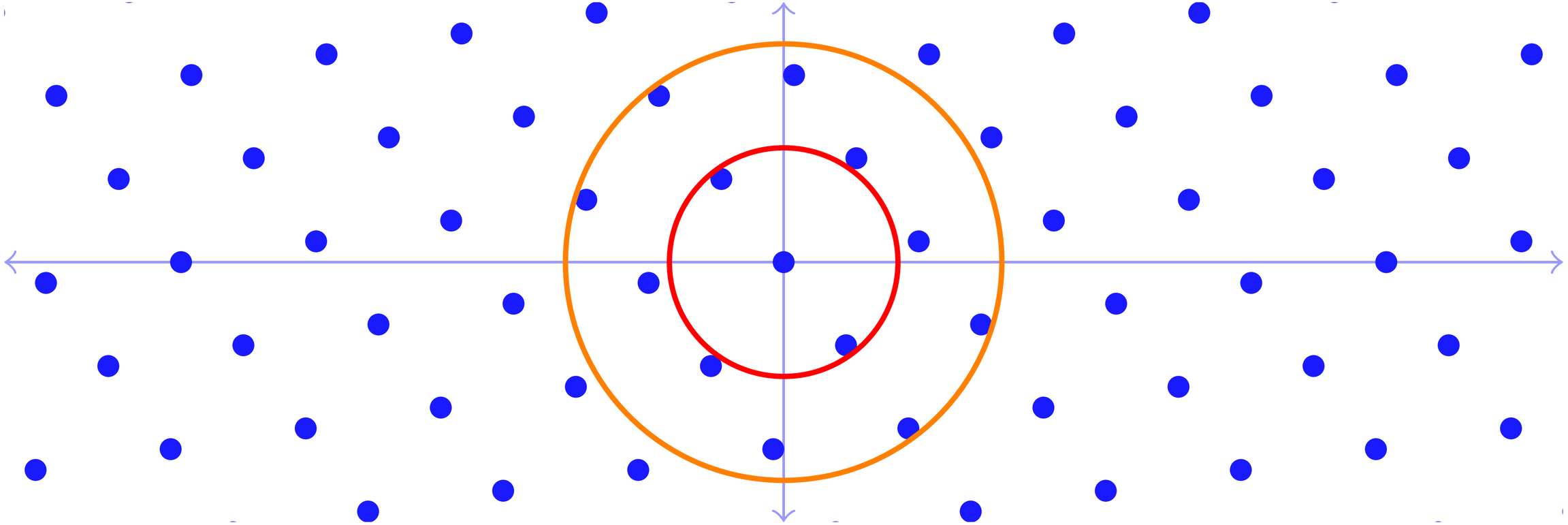
$$0 < \|\mathbf{v}\|_p \leq \gamma \cdot \lambda_1^p(\mathscr{L}) \text{ where } \lambda_1^p(\mathscr{L}) = \min_{\mathbf{u} \neq \mathbf{0}, \mathbf{u} \in \mathscr{L}} \|\mathbf{u}\|_p.$$



Shortest Vector Problem

Shortest Vector Problem (γ-SVP$_p$) : Given a basis $\mathbf{B}$ of lattice $\mathscr{L}$, find a lattice vector $\mathbf{v}$ such that,

$$0 < \|\mathbf{v}\|_p \leq \gamma \cdot \lambda_1^p(\mathscr{L}) \text{ where } \lambda_1^p(\mathscr{L}) = \min_{\mathbf{u}\neq\mathbf{0},\mathbf{u}\in\mathscr{L}} \|\mathbf{u}\|_p.$$



$\lambda_1^p(\mathscr{L})\mathscr{B}_p^m$ $2\lambda_1^p(\mathscr{L})\mathscr{B}_p^m$

Closest Vector Problem

Closest Vector Problem

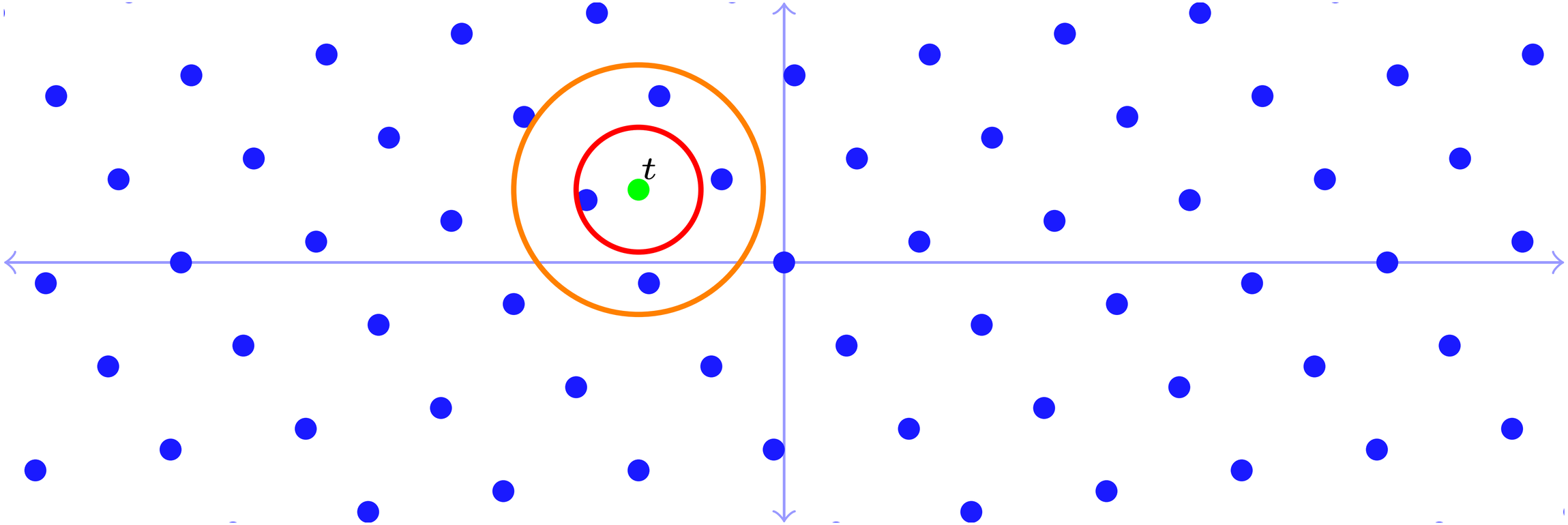
Closest Vector Problem (γ-CVP$_p$) : Given a basis $\mathbf{B}$ of lattice $\mathscr{L}$ and target vector $\mathbf{t}$, find a lattice vector $\mathbf{v}$ such that,

$$\|\mathbf{v}-\mathbf{t}\|_p \leq \gamma \cdot \mathrm{dist}_p(\mathbf{t},\mathscr{L}) \text{ where } \mathrm{dist}_p(\mathbf{t},\mathscr{L}) = \min_{\mathbf{u}\in\mathscr{L}} \|\mathbf{u}-\mathbf{t}\|_p .$$

Closest Vector Problem

Closest Vector Problem (γ-CVP$_p$) : Given a basis $\mathbf{B}$ of lattice $\mathscr{L}$ and target vector $\mathbf{t}$, find a lattice vector $\mathbf{v}$ such that,

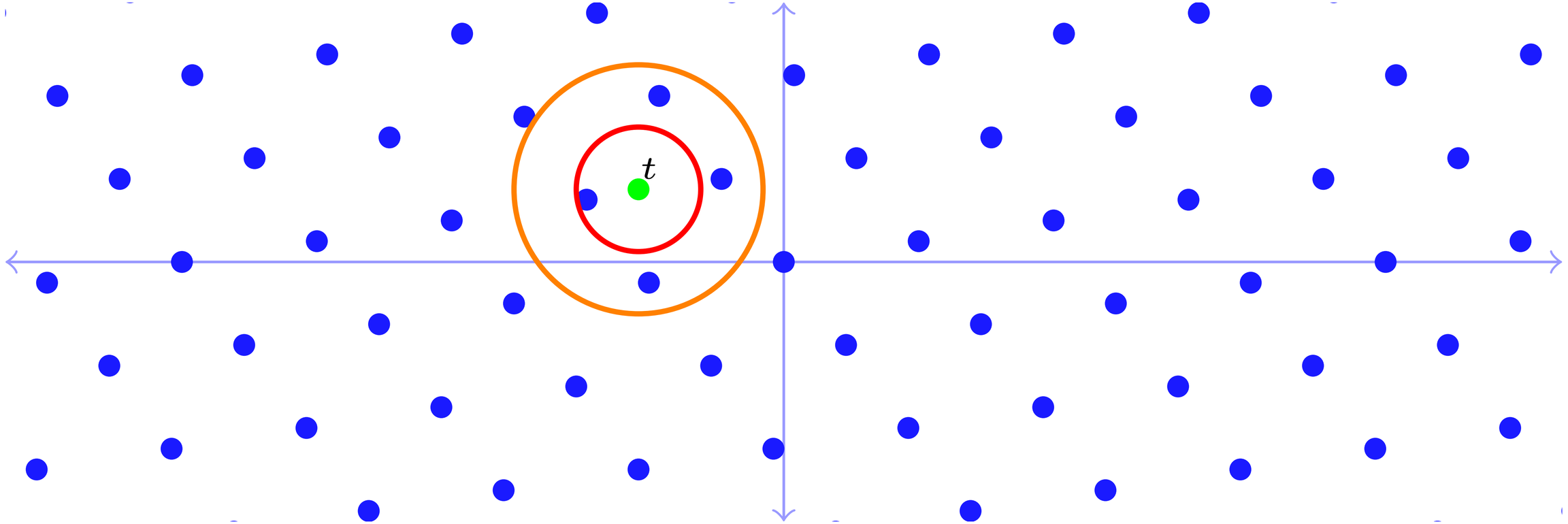
$$\|\mathbf{v}-\mathbf{t}\|_p \leq \gamma \cdot \mathrm{dist}_p(\mathbf{t},\mathscr{L}) \text{ where } \mathrm{dist}_p(\mathbf{t},\mathscr{L}) = \min_{\mathbf{u}\in\mathscr{L}} \|\mathbf{u}-\mathbf{t}\|_p .$$



Closest Vector Problem

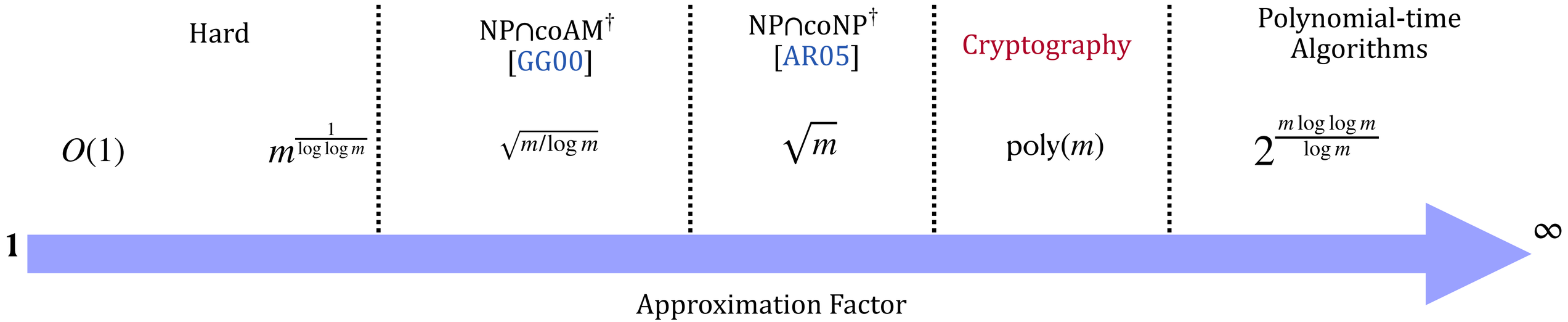
Closest Vector Problem (γ-CVP$_p$) : Given a basis $\mathbf{B}$ of lattice $\mathscr{L}$ and target vector $\mathbf{t}$, find a lattice vector $\mathbf{v}$ such that,

$$\|\mathbf{v}-\mathbf{t}\|_p \le \gamma \cdot \mathrm{dist}_p(\mathbf{t},\mathscr{L}) \text{ where } \mathrm{dist}_p(\mathbf{t},\mathscr{L}) = \min_{\mathbf{u}\in\mathscr{L}} \|\mathbf{u}-\mathbf{t}\|_p .$$



$\mathrm{dist}_p(\mathbf{t},\mathscr{L})\mathscr{B}_p^m$ $2\mathrm{dist}_p(\mathbf{t},\mathscr{L})\mathscr{B}_p^m$

Approximation of SVP and CVP



† Only for ℓ_2 norm. Extend to ℓ_p norm by [RR06]

Reduction between Lattice Problems

Polynomial time reductions

Polynomial time reductions

- Approximation factor, dimension and rank preserving reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$

  [Goldreich, Micciancio, Safra, Seifert ‘99].

Polynomial time reductions

- Approximation factor, dimension and rank preserving reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$

  [Goldreich, Micciancio, Safra, Seifert ‘99].

- $\gamma^2\sqrt{m}$-$\mathbf{CVP}_2$ reduces to γ-$\mathbf{SVP}_2$ [Dubey, Holenstein ’11].

Polynomial time reductions

- Approximation factor, dimension and rank preserving reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$

  [Goldreich, Micciancio, Safra, Seifert ‘99].

- $\gamma^2\sqrt{m}$-$\mathbf{CVP}_2$ reduces to γ-$\mathbf{SVP}_2$ [Dubey, Holenstein ’11].

- A trivial reduction between $\mathbf{SVP}_p$ and $\mathbf{SVP}_q$ (similarly for $\mathbf{CVP}$) increase the approximation factor by $m^{|1/p-1/q|}$.

Polynomial time reductions

- Approximation factor, dimension and rank preserving reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$ [Goldreich, Micciancio, Safra, Seifert ‘99].
- $\gamma^2\sqrt{m}$-$\mathbf{CVP}_2$ reduces to γ-$\mathbf{SVP}_2$ [Dubey, Holenstein ’11].
- A trivial reduction between $\mathbf{SVP}_p$ and $\mathbf{SVP}_q$ (similarly for $\mathbf{CVP}$) increase the approximation factor by $m^{|1/p-1/q|}$.
- $C\gamma$-$\mathbf{SVP}_2$ reduces to γ-$\mathbf{SVP}_p$ for any p and any constant $C > 1$ (Similarly for $\mathbf{CVP}$) [Regev, Rosen ’06].

Polynomial time reductions

- Approximation factor, dimension and rank preserving reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$ [Goldreich, Micciancio, Safra, Seifert '99].
- $\gamma^2\sqrt{m}$-$\mathbf{CVP}_2$ reduces to γ-$\mathbf{SVP}_2$ [Dubey, Holenstein '11].
- A trivial reduction between $\mathbf{SVP}_p$ and $\mathbf{SVP}_q$ (similarly for $\mathbf{CVP}$) increase the approximation factor by $m^{|1/p-1/q|}$.
- $C\gamma$-$\mathbf{SVP}_2$ reduces to γ-$\mathbf{SVP}_p$ for any p and any constant $C > 1$ (Similarly for $\mathbf{CVP}$) [Regev, Rosen '06].
- When $p > 2$, there is super constant increment in dimension.

Algorithms for SVP_p and CVP_p

Algorithms for $\mathbf{SVP}_p$ and $\mathbf{CVP}_p$

- Fastest Known algorithm for γ-$\mathbf{SVP}_2$ for $1 \leq \gamma \leq \text{poly}(m)$ run in time 2^{Cm} for some constant $C \leq 1$, where C depends on γ.

Algorithms for $\mathbf{SVP}_p$ and $\mathbf{CVP}_p$

- Fastest Known algorithm for γ-$\mathbf{SVP}_2$ for $1 \leq \gamma \leq \text{poly}(m)$ run in time 2^{Cm} for some constant $C \leq 1$, where C depends on γ.

- For γ-$\mathbf{CVP}_p$ for $1 \leq \gamma \leq m^{|1/p-1/2|}$ run in time $\min\{2^{Cm}, n^{Cn}\}$ [Blömer, Naewe '07].

Algorithms for $\mathbf{SVP}_p$ and $\mathbf{CVP}_p$

- Fastest Known algorithm for γ-$\mathbf{SVP}_2$ for $1 \leq \gamma \leq \text{poly}(m)$ run in time 2^{Cm} for some constant $C \leq 1$, where C depends on γ.

- For γ-$\mathbf{CVP}_p$ for $1 \leq \gamma \leq m^{|1/p-1/2|}$ run in time $\min\{2^{Cm}, n^{Cn}\}$ [Blömer, Naewe '07].

- For $O(1)$-$\mathbf{SVP}_p$, in 2^{Cn} time [Dadush, Peikert, Vempala '11].

Algorithms for $\mathbf{SVP}_p$ and $\mathbf{CVP}_p$

- Fastest Known algorithm for γ-$\mathbf{SVP}_2$ for $1 \leq \gamma \leq \text{poly}(m)$ run in time 2^{Cm} for some constant $C \leq 1$, where C depends on γ.

- For γ-$\mathbf{CVP}_p$ for $1 \leq \gamma \leq m^{|1/p-1/2|}$ run in time $\min\{2^{Cm}, n^{Cn}\}$ [Blömer, Naewe '07].

- For $O(1)$-$\mathbf{SVP}_p$, in 2^{Cn} time [Dadush, Peikert, Vempala '11].

For $p \neq 2$,the constant C is not well studied.

Algorithms for $\mathbf{SVP}_p$ and $\mathbf{CVP}_p$

- Fastest Known algorithm for γ-$\mathbf{SVP}_2$ for $1 \leq \gamma \leq \text{poly}(m)$ run in time 2^{Cm} for some constant $C \leq 1$, where C depends on γ.
- For γ-$\mathbf{CVP}_p$ for $1 \leq \gamma \leq m^{|1/p-1/2|}$ run in time $\min\{2^{Cm}, n^{Cn}\}$ [Blömer, Naewe '07].
- For $O(1)$-$\mathbf{SVP}_p$, in 2^{Cn} time [Dadush, Peikert, Vempala '11].

For $p \neq 2$,the constant C is not well studied.

- $2^{(1-\epsilon)n}$ lower bound for small constant approximation of $\mathbf{CVP}_p$ and $\mathbf{SVP}_\infty$ assuming (gap) Strong Exponential time Hypothesis [BGS17; AS18; Aggarwal, Bennett, Golovnev, Stephens-Davidowitz '20].

Exponential time reductions

Exponential time reductions

- There is a $2^{O(m)}$-reduction from $O(1)$-$\mathbf{CVP}_2$ to almost uniformly sampling lattice vectors of bounded length [Ajtai, Kumar and Sivakumar '02].

Exponential time reductions

- There is a $2^{O(m)}$-reduction from $O(1)$-$\mathbf{CVP}_2$ to almost uniformly sampling lattice vectors of bounded length [Ajtai, Kumar and Sivakumar '02].

- Blömer and Naewe generalised this to ℓ_p norm [BN07].

Exponential time reductions

- There is a $2^{O(m)}$-reduction from $O(1)$-$\mathbf{CVP}_2$ to almost uniformly sampling lattice vectors of bounded length [Ajtai, Kumar and Sivakumar '02].

- Blömer and Naewe generalised this to ℓ_p norm [BN07].

- Eisenbrand and Venzin gave an algorithm of $O(1)$-$\mathbf{SVP}_p$ and $O(1)$-$\mathbf{CVP}_p$ by using the current fastest algorithm of $O(1)$-$\mathbf{SVP}_2$ as a subroutine [EV20].

Exponential time reductions

- There is a $2^{O(m)}$-reduction from $O(1)$-$\mathbf{CVP}_2$ to almost uniformly sampling lattice vectors of bounded length [Ajtai, Kumar and Sivakumar '02].

- Blömer and Naewe generalised this to ℓ_p norm [BN07].

- Eisenbrand and Venzin gave an algorithm of $O(1)$-$\mathbf{SVP}_p$ and $O(1)$-$\mathbf{CVP}_p$ by using the current fastest algorithm of $O(1)$-$\mathbf{SVP}_2$ as a subroutine [EV20].

- Uses some specific properties of the $O(1)$-$\mathbf{SVP}_2$ algorithm.

Our Contribution

Our Result

Our Result

- For any $1 \leq p \leq q \leq \infty$, we present following $2^{\epsilon m}$ time reductions

Our Result

- For any $1 \leq p \leq q \leq \infty$, we present following $2^{\epsilon m}$ time reductions

    1. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1/p})\gamma$-$\mathbf{SVP}_q$ to γ-$\mathbf{SVP}_p$.

Our Result

- For any $1 \leq p \leq q \leq \infty$, we present following $2^{\epsilon m}$ time reductions

    1. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1/p})\gamma$-$\mathbf{SVP}_q$ to γ-$\mathbf{SVP}_p$.

    2. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1/p})\gamma$-$\mathbf{CVP}_p$ to γ-$\mathbf{CVP}_q$.

Our Result

- For any $1 \leq p \leq q \leq \infty$, we present following $2^{\epsilon m}$ time reductions

    1. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1/p})\gamma$-$\mathbf{SVP}_q$ to γ-$\mathbf{SVP}_p$.
    2. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1/p})\gamma$-$\mathbf{CVP}_p$ to γ-$\mathbf{CVP}_q$.
    3. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1+1/p})$-$\mathbf{CVP}_q$ to $(1+\epsilon)$-$\mathbf{SVP}_p$.

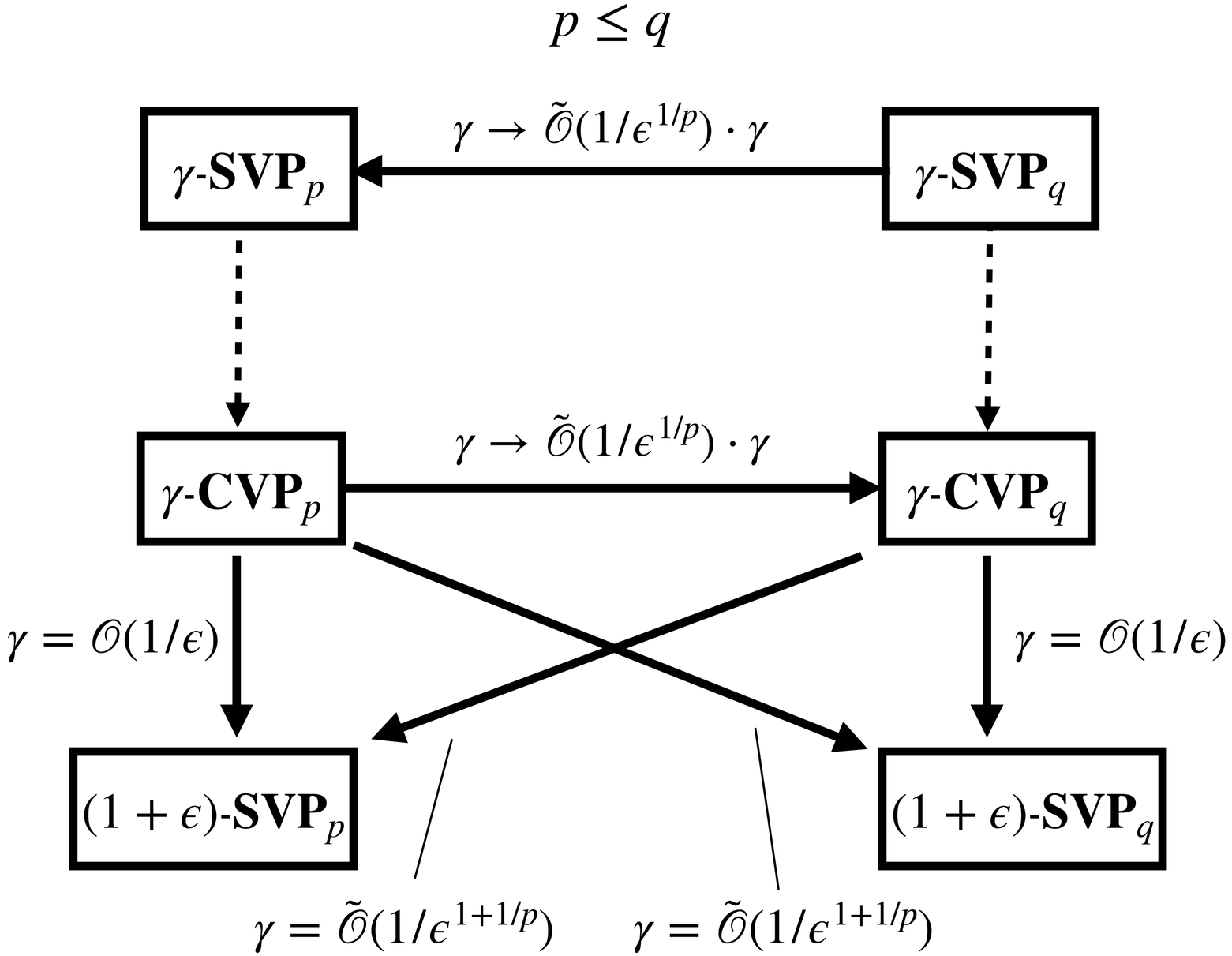
Our Result

- For any $1 \leq p \leq q \leq \infty$, we present following $2^{\epsilon m}$ time reductions

    1. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1/p})\gamma$-$\mathbf{SVP}_q$ to γ-$\mathbf{SVP}_p$.
    2. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1/p})\gamma$-$\mathbf{CVP}_p$ to γ-$\mathbf{CVP}_q$.
    3. Reduction from $\tilde{\mathcal{O}}(1/\epsilon^{1+1/p})$-$\mathbf{CVP}_q$ to $(1+\epsilon)$-$\mathbf{SVP}_p$.

Either preserves the rank and dimension or increases them by atmost one.

Our Result: Exponential time reductions



- Dimension and rank increase by at most one.
- Dotted lines represent polynomial time reduction by Goldreich, Micciancio, Safra, Seifert ’99.
- Solid lines represent $2^{\epsilon m}$ time reductions .

Our Result: A better reduction for $p \in [1,2]$

Our Result: A better reduction for $p \in [1,2]$

- For $p \in [1,2]$, we get a better reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$.

Our Result: A better reduction for $p \in [1,2]$

- For $p \in [1,2]$, we get a better reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$.

- $2^{\epsilon m}$ time reduction from $O(1/\epsilon^{1/p})$-$\mathbf{CVP}_p$ to $\mathbf{SVP}_p$.

Our Result: A better reduction for $p \in [1,2]$

- For $p \in [1,2]$, we get a better reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$.

- $2^{\epsilon m}$ time reduction from $O(1/\epsilon^{1/p})$-$\mathbf{CVP}_p$ to $\mathbf{SVP}_p$.

- Plugging in $p = 2$ and $\epsilon = \log m/m$, we get polynomial time reduction from $\sqrt{m/\log m}$-$\mathbf{CVP}_2$ to $\mathbf{SVP}_2$.

Our Result: A better reduction for $p \in [1,2]$

- For $p \in [1,2]$, we get a better reduction from $\mathbf{CVP}_p$ to $\mathbf{SVP}_p$.

- $2^{\epsilon m}$ time reduction from $O(1/\epsilon^{1/p})$-$\mathbf{CVP}_p$ to $\mathbf{SVP}_p$.

- Plugging in $p = 2$ and $\epsilon = \log m/m$, we get polynomial time reduction from $\sqrt{m/\log m}$-$\mathbf{CVP}_2$ to $\mathbf{SVP}_2$.

- Improves on Kannan's celebrated polynomial time reduction from $\sqrt{m}$-$\mathbf{CVP}_2$ to $\mathbf{SVP}_2$.

Reduction from CVP_q to SVP_p

Kannan's Embedding

Kannan's Embedding

- Using $\mathbf{SVP}_p$ oracle to find the lattice vector close to a small integer multiple of $\mathbf{t}$ (target vector).

Kannan's Embedding

- Using $\mathbf{SVP}_p$ oracle to find the lattice vector close to a small integer multiple of $\mathbf{t}$ (target vector).

$$\mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & s \end{bmatrix}$$

Kannan's Embedding

- Using $\mathbf{SVP}_p$ oracle to find the lattice vector close to a small integer multiple of $\mathbf{t}$ (target vector).

$$\mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & s \end{bmatrix}$$

- Short lattice vector of $\mathscr{L}(\mathbf{B}')$ is of the form $(\mathbf{v} + k\mathbf{t}, ks)$.

Kannan's Embedding

- Using $\mathbf{SVP}_p$ oracle to find the lattice vector close to a small integer multiple of $\mathbf{t}$ (target vector).

$$\mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & s \end{bmatrix}$$

- Short lattice vector of $\mathscr{L}(\mathbf{B}')$ is of the form $(\mathbf{v} + k\mathbf{t}, ks)$.

- $\mathbf{CVP}_p$ algorithm forces the algorithm to output a solution with $k = 1$.

Kannan's Embedding

- Using $\mathbf{SVP}_p$ oracle to find the lattice vector close to a small integer multiple of $\mathbf{t}$ (target vector).

$$\mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & s \end{bmatrix}$$

- Short lattice vector of $\mathscr{L}(\mathbf{B}')$ is of the form $(\mathbf{v} + k\mathbf{t}, ks)$.

- $\mathbf{CVP}_p$ algorithm forces the algorithm to output a solution with $k = 1$.

- Eisenbrand and Venzin observed that it suffices to simultaneously find a lattice vector close to $k\mathbf{t}$ and a lattice vector close to $(k-1)\mathbf{t}$.

Our reduction

Our reduction

- Reduction from γ-$\mathbf{CVP}_q$ to $\mathbf{SVP}_p$.

Our reduction

- Reduction from γ-$\mathbf{CVP}_q$ to $\mathbf{SVP}_p$.

- Given a basis $\mathbf{B}$ of the lattice $\mathscr{L}$ and a target vector $\mathbf{t}$.

Our reduction

- Reduction from γ-$\mathbf{CVP}_q$ to $\mathbf{SVP}_p$.

- Given a basis $\mathbf{B}$ of the lattice $\mathscr{L}$ and a target vector $\mathbf{t}$.

$$\mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & s \end{bmatrix}$$

Our reduction

- Reduction from γ-$\mathbf{CVP}_q$ to $\mathbf{SVP}_p$.

- Given a basis $\mathbf{B}$ of the lattice $\mathscr{L}$ and a target vector $\mathbf{t}$.

$$\mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & s \end{bmatrix}$$

- With carefully chosen s, sample two short lattice vectors from $\mathscr{L}(\mathbf{B}')$ and check if the difference of the vectors is of the form $(\mathbf{y} + \mathbf{t}, s)$ with small ℓ_q norm. If yes, then terminate.

Our reduction

- Reduction from γ-$\mathbf{CVP}_q$ to $\mathbf{SVP}_p$.

- Given a basis $\mathbf{B}$ of the lattice $\mathscr{L}$ and a target vector $\mathbf{t}$.

$$\mathbf{B}' = \begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0} & s \end{bmatrix}$$

- With carefully chosen s, sample two short lattice vectors from $\mathscr{L}(\mathbf{B}')$ and check if the difference of the vectors is of the form $(\mathbf{y} + \mathbf{t}, s)$ with small ℓ_q norm. If yes, then terminate.

- Otherwise, repeat this.

Lattice Sparsification

Lattice Sparsification

- For a prime p and uniformly random $\mathbf{z} \in \mathbb{Z}_p^n$

Lattice Sparsification

- For a prime p and uniformly random $\mathbf{z} \in \mathbb{Z}_p^n$

$$\mathscr{L}'_{\mathbf{z}} = \{\mathbf{v} \in \mathscr{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{v} \rangle = 0 \mod p\}$$

Lattice Sparsification

- For a prime p and uniformly random $\mathbf{z} \in \mathbb{Z}_p^n$

$$\mathscr{L}'_{\mathbf{z}} = \{\mathbf{v} \in \mathscr{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{v} \rangle = 0 \mod p\}$$

- For a prime p, lattice $\mathscr{L}$ and vector $\mathbf{v} \in \mathscr{L} \setminus p\mathscr{L}$

Lattice Sparsification

- For a prime p and uniformly random $\mathbf{z} \in \mathbb{Z}_p^n$

$$\mathscr{L}'_{\mathbf{z}} = \{\mathbf{v} \in \mathscr{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{v} \rangle = 0 \mod p\}$$

- For a prime p, lattice $\mathscr{L}$ and vector $\mathbf{v} \in \mathscr{L} \setminus p\mathscr{L}$

$$\Pr[\mathbf{v} \in \mathscr{L}'_{\mathbf{z}}] \approx \frac{1}{p}$$

Lattice Sparsification

- For a prime p and uniformly random $\mathbf{z} \in \mathbb{Z}_p^n$

$$\mathscr{L}'_{\mathbf{z}} = \{\mathbf{v} \in \mathscr{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{v} \rangle = 0 \mod p\}$$

- For a prime p, lattice $\mathscr{L}$ and vector $\mathbf{v} \in \mathscr{L} \setminus p\mathscr{L}$

$$\Pr[\mathbf{v} \in \mathscr{L}'_{\mathbf{z}}] \approx \frac{1}{p}$$

where $\mathbf{z}$ is sampled uniformly at random form $\mathbb{Z}_p^n$.

Lattice Sparsification

- For a prime p and uniformly random $\mathbf{z} \in \mathbb{Z}_p^n$

$$\mathscr{L}'_{\mathbf{z}} = \{\mathbf{v} \in \mathscr{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{v} \rangle = 0 \mod p\}$$

- For a prime p, lattice $\mathscr{L}$ and vector $\mathbf{v} \in \mathscr{L} \setminus p\mathscr{L}$

$$\Pr[\mathbf{v} \in \mathscr{L}'_{\mathbf{z}}] \approx \frac{1}{p}$$

where $\mathbf{z}$ is sampled uniformly at random form $\mathbb{Z}_p^n$.

Lattice Sparsification

- For a prime p and uniformly random $\mathbf{z} \in \mathbb{Z}_p^n$

$$\mathscr{L}'_{\mathbf{z}} = \{\mathbf{v} \in \mathscr{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{v} \rangle = 0 \mod p\}$$

- For a prime p, lattice $\mathscr{L}$ and vector $\mathbf{v} \in \mathscr{L} \setminus p\mathscr{L}$

$$\Pr[\mathbf{v} \in \mathscr{L}'_{\mathbf{z}}] \approx \frac{1}{p}$$

where $\mathbf{z}$ is sampled uniformly at random form $\mathbb{Z}_p^n$.

- By making poly(n) calls to $\mathbf{SVP}_2$ oracle we can sample uniformly random lattice vector in a sphere.[Stephens-Davidowitz '16]

Lattice Sparsification

- For a prime p and uniformly random $\mathbf{z} \in \mathbb{Z}_p^n$

$$\mathscr{L}'_{\mathbf{z}} = \{\mathbf{v} \in \mathscr{L} : \langle \mathbf{z}, \mathbf{B}^{-1}\mathbf{v} \rangle = 0 \mod p\}$$

- For a prime p, lattice $\mathscr{L}$ and vector $\mathbf{v} \in \mathscr{L} \setminus p\mathscr{L}$

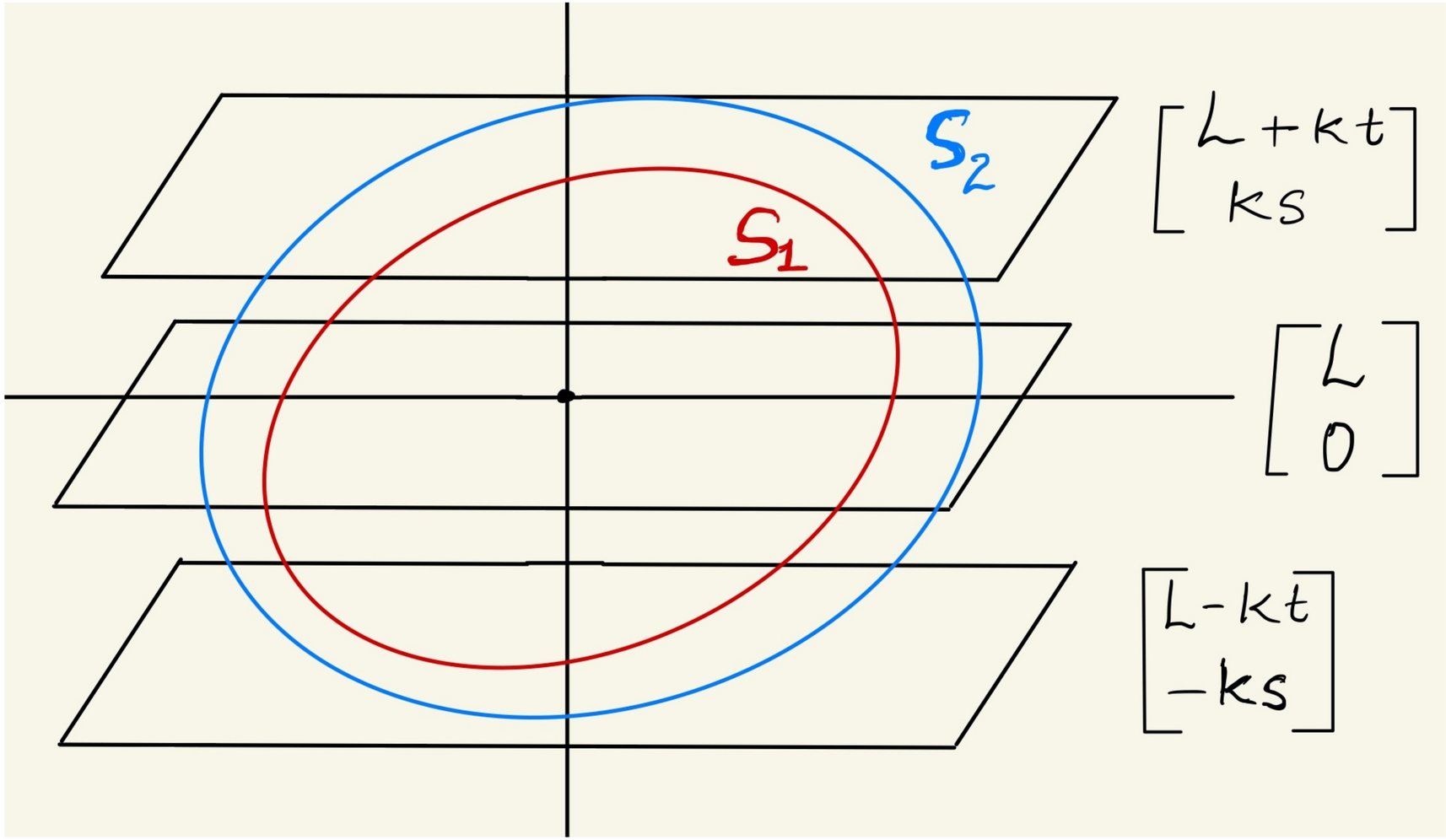
$$\Pr[\mathbf{v} \in \mathscr{L}'_{\mathbf{z}}] \approx \frac{1}{p}$$

where $\mathbf{z}$ is sampled uniformly at random form $\mathbb{Z}_p^n$.

- By making poly(n) calls to $\mathbf{SVP}_2$ oracle we can sample uniformly random lattice vector in a sphere.[Stephens-Davidowitz '16]
- We use generalisation of this to any ℓ_p norm, to sample a uniformly random lattice vector.

Proof sketch

- $\exists r > 0,\ r' = r - m^{1/p-1/q}\mathrm{dist}_q(\mathbf{t}, \mathscr{L}) - s,\ S_1 = r'\mathscr{B}_p^m,\ S_2 = r\mathscr{B}_p^m$ such that $\frac{|S_2|}{|S_1|} \leq 2^{\epsilon m}$.
- $S \subseteq S_1 \cap (\mathscr{L} + k'\mathbf{t}, k's)$
- $T = S + (-\mathbf{v} + \mathbf{t}, s) \in S_2$
- $2^{2\epsilon m}|S| = 2^{2\epsilon m}|T| \geq |S_2|$



Conclusion

Conclusion

- We gave $2^{\epsilon m}$ time reductions for lattice problems in different ℓ_p norms .

Conclusion

- We gave $2^{\epsilon m}$ time reductions for lattice problems in different ℓ_p norms .
- As a corollary, we get a polynomial time reduction from $\sqrt{m/\log m}$-$\mathbf{CVP}_2$ to $\mathbf{SVP}_2$.

Conclusion

- We gave $2^{\epsilon m}$ time reductions for lattice problems in different ℓ_p norms .
- As a corollary, we get a polynomial time reduction from $\sqrt{m/\log m}$-$\mathbf{CVP}_2$ to $\mathbf{SVP}_2$.

Thanks!

Conclusion

- We gave $2^{\epsilon m}$ time reductions for lattice problems in different ℓ_p norms .
- As a corollary, we get a polynomial time reduction from $\sqrt{m/\log m}$-$\mathbf{CVP}_2$ to $\mathbf{SVP}_2$.

Thanks!

Questions?