Lattice problems are (sort of) equivalent in all norms (and the mysterious wiggle)

Frederick Eisenbrand   Moritz Venzin

Divesh Aggarwal   Yanlin Chen   Rajendra Kumar

Zeyong Li   Noah Stephens-Davidowitz

Thomas Rothvoss   Moritz Venzin

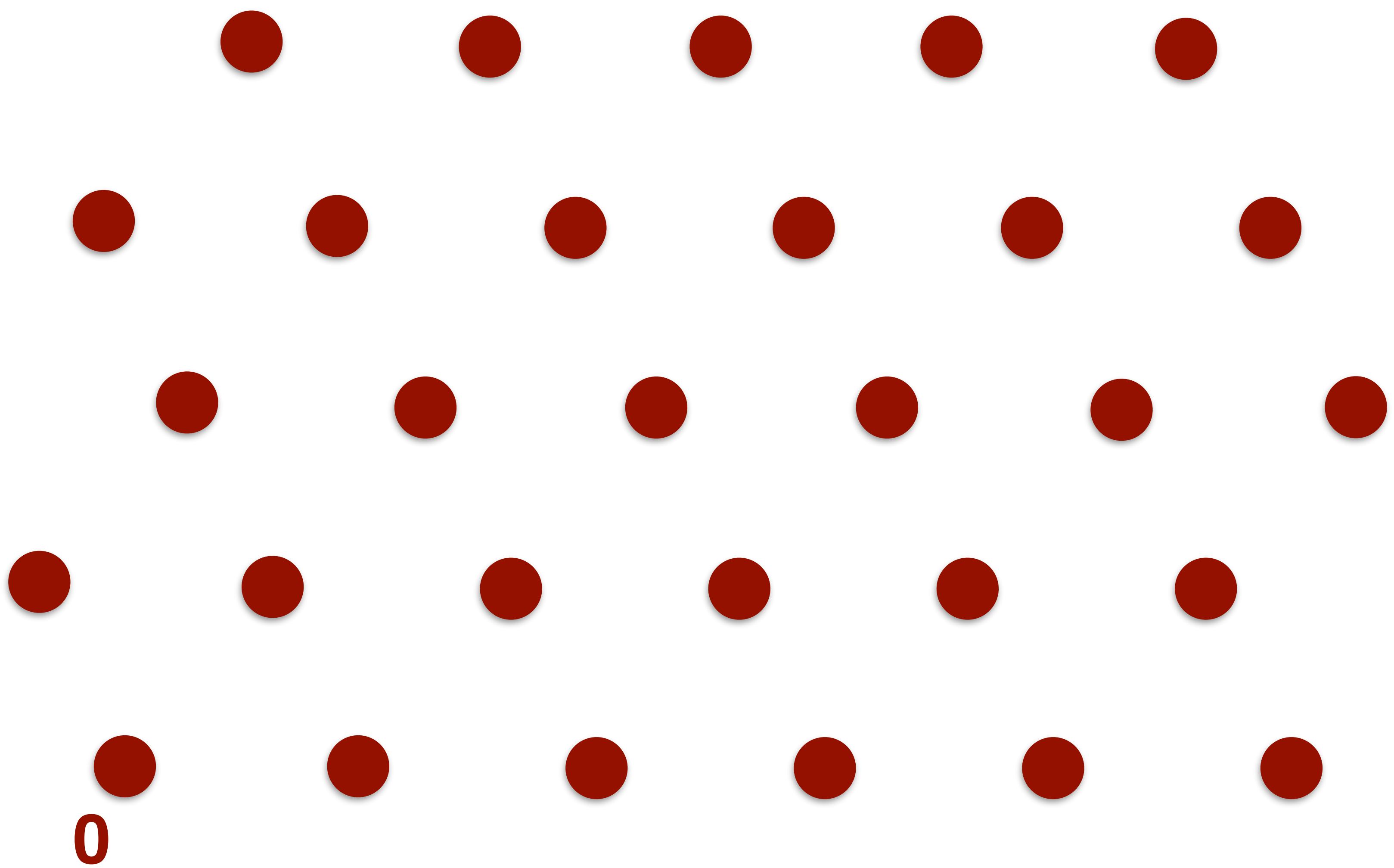
Lattices

Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$.

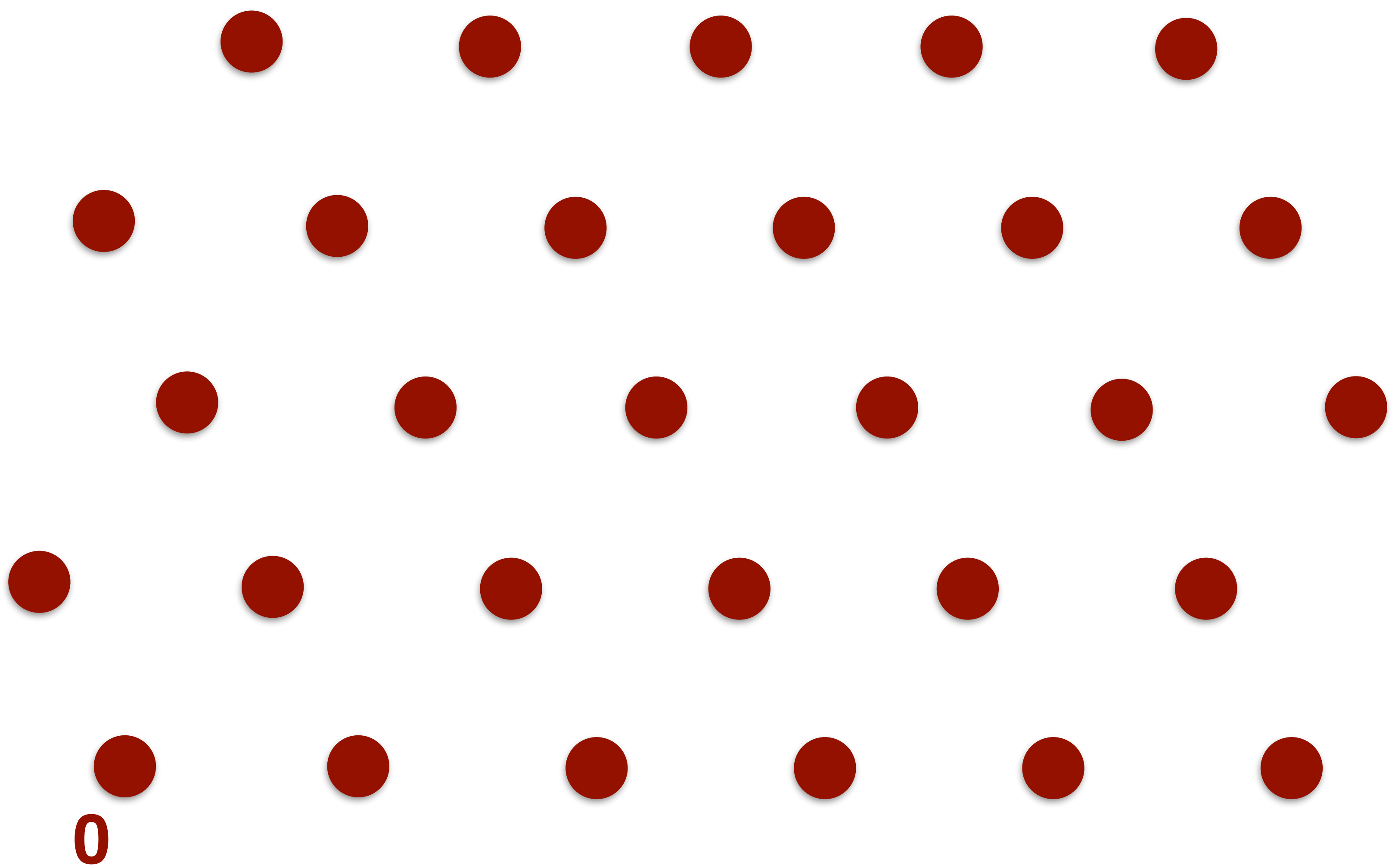
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$.



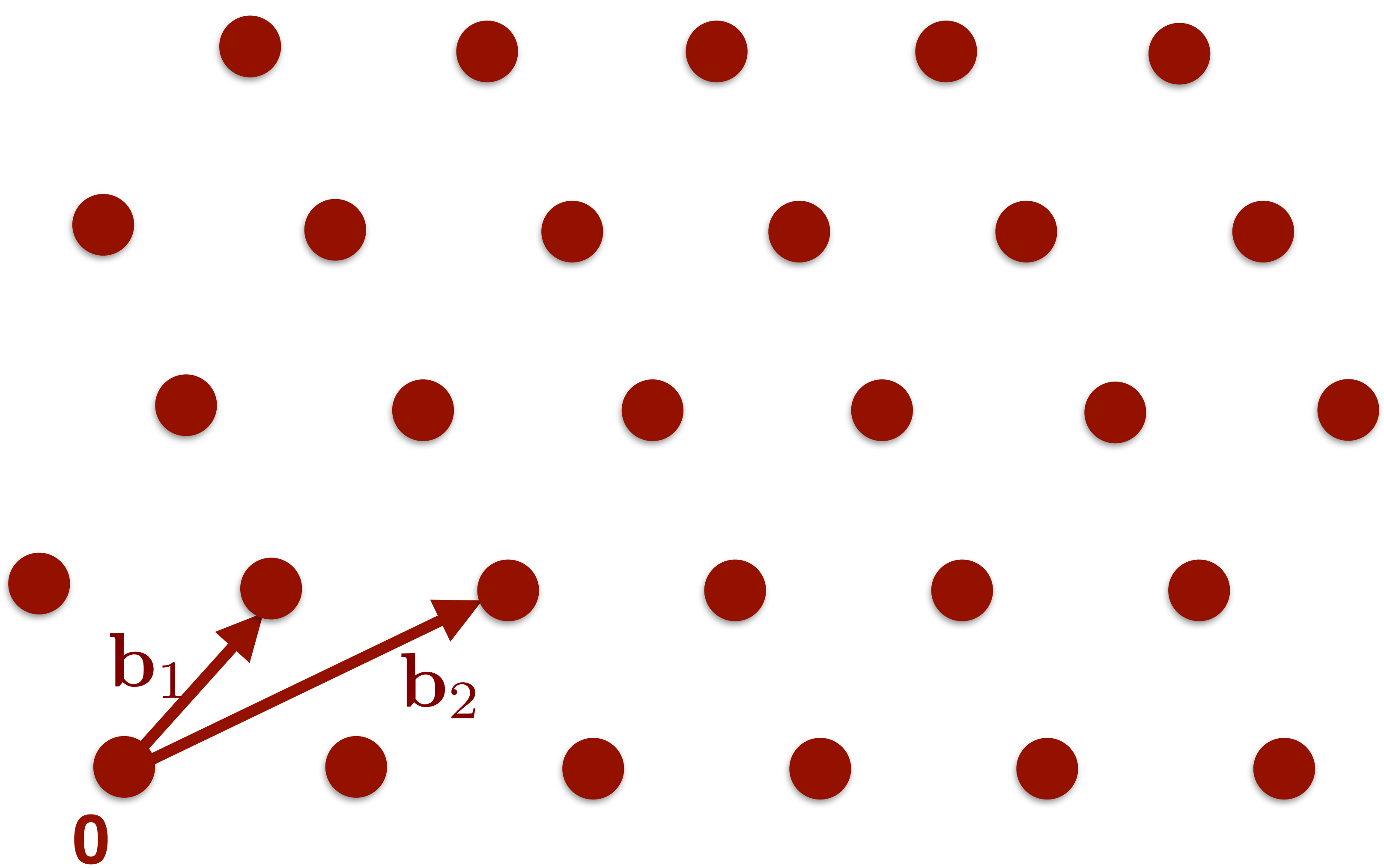
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$.
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, linearly independent vectors



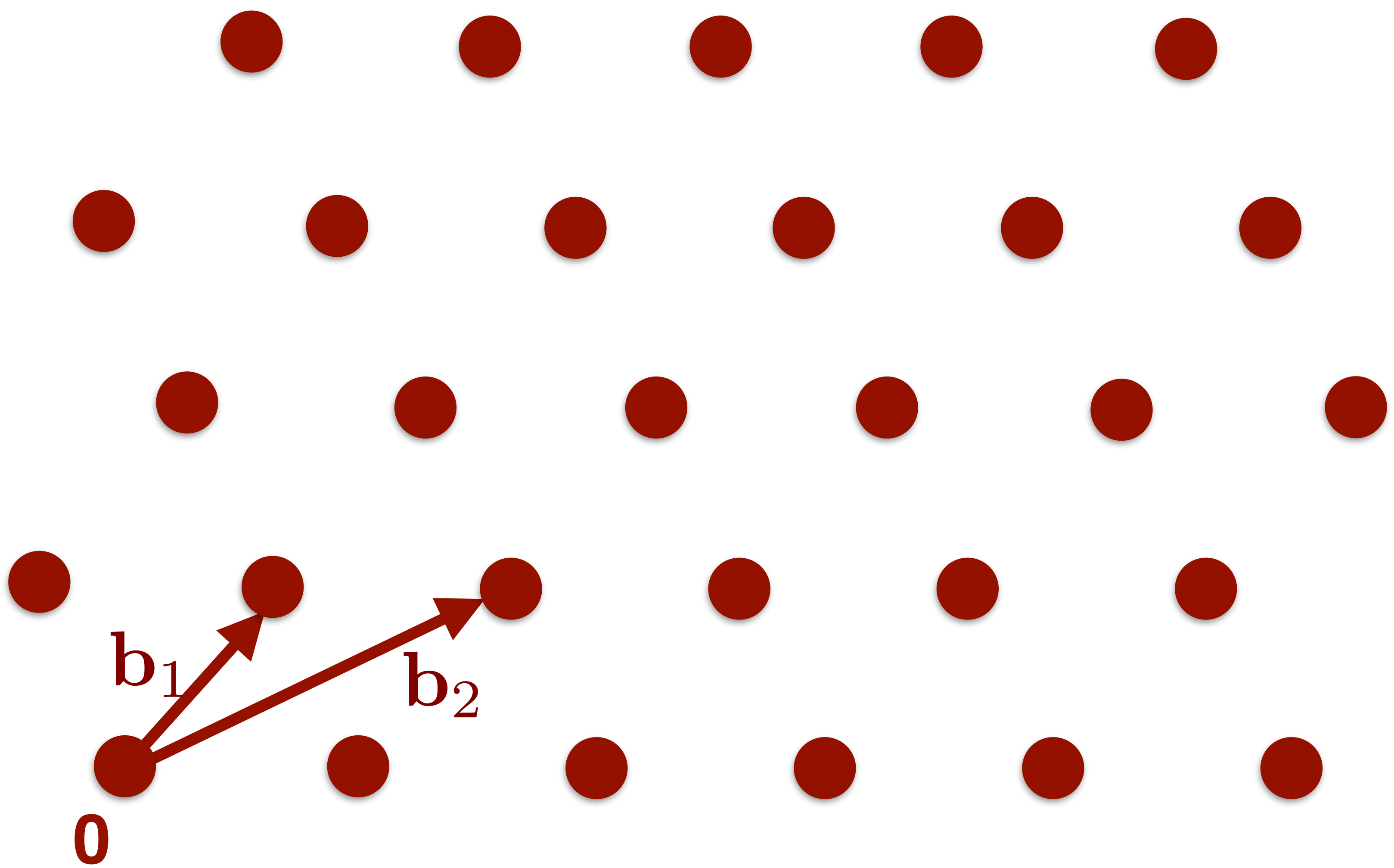
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$.
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, linearly independent vectors



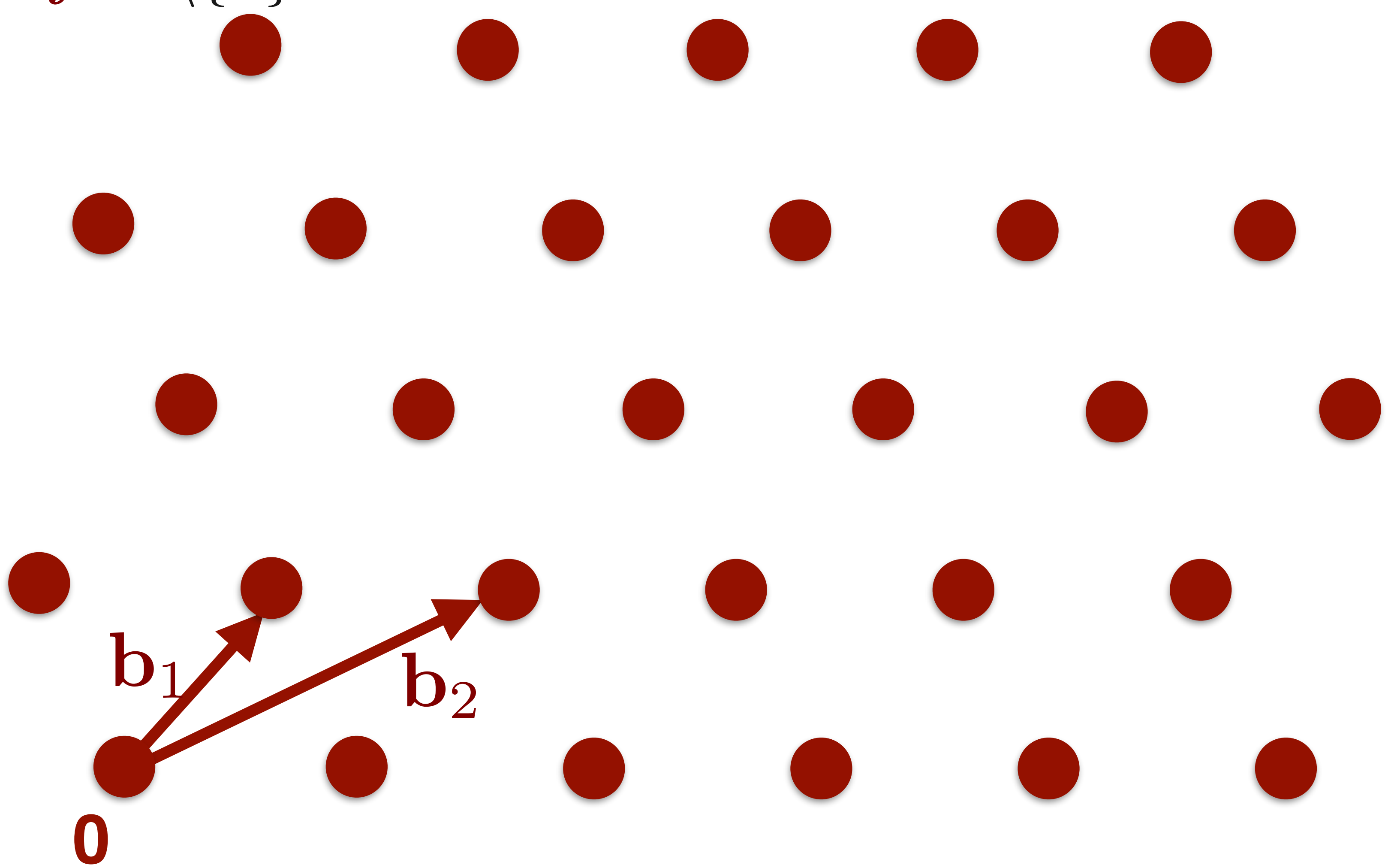
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$.
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, linearly independent vectors
- $\mathcal{L} = \{a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n \mid a_i \in \mathbb{Z}\}$



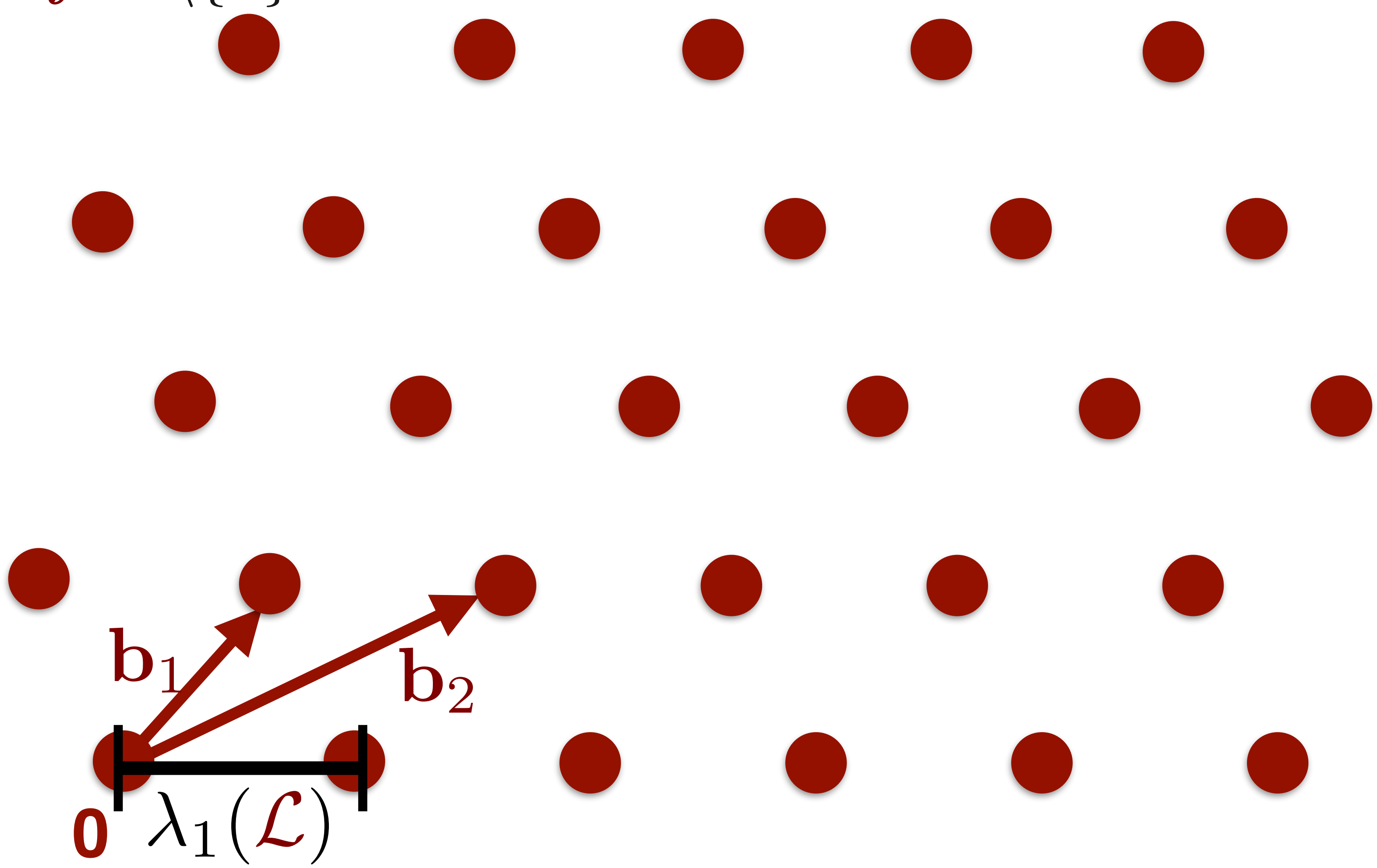
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$.
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, linearly independent vectors
- $\mathcal{L} = \{a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n \mid a_i \in \mathbb{Z}\}$
- $\lambda_1(\mathcal{L}) := \min_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|$



Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$.
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, linearly independent vectors
- $\mathcal{L} = \{a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n \mid a_i \in \mathbb{Z}\}$
- $\lambda_1(\mathcal{L}) := \min_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|$



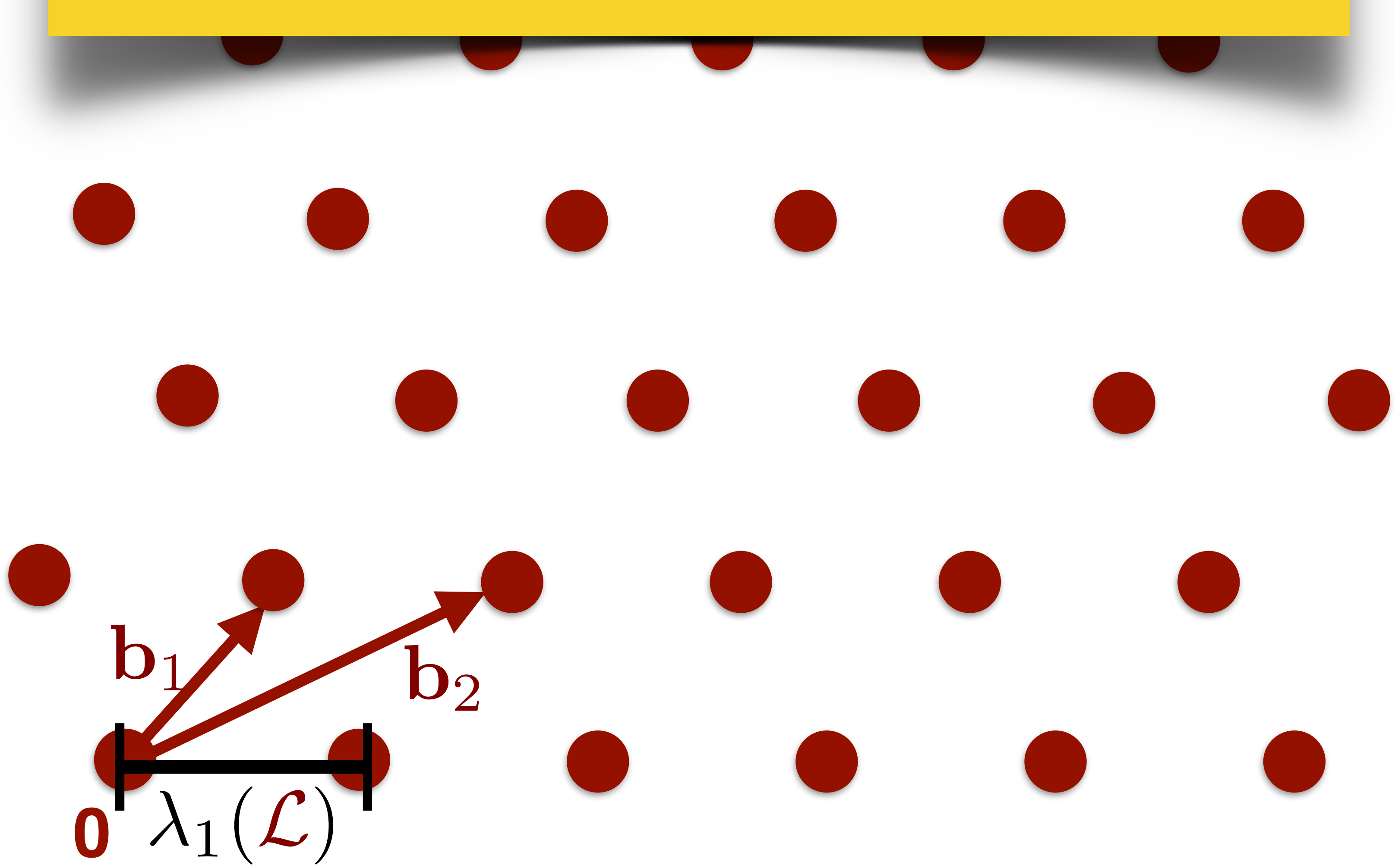
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$
- Specified ... ndent vectors
- $\mathcal{L} = \{a_1 \mathbf{b}$ ...
- $\lambda_1(\mathcal{L}) :=$ ...

Different norms of interest:

$$\|\mathbf{x}\|_p := (|x_1|^p + \cdots + |x_n|^p)^{1/p}.$$

$$\|\mathbf{x}\|_\infty := \max_i |x_i|.$$



Lattices

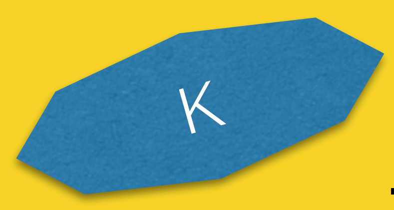
- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$
- Specified ... ndent vectors
- $\mathcal{L} = \{a_1 \mathbf{b}$ ...
- $\lambda_1(\mathcal{L}) :=$ ...

Different norms of interest:

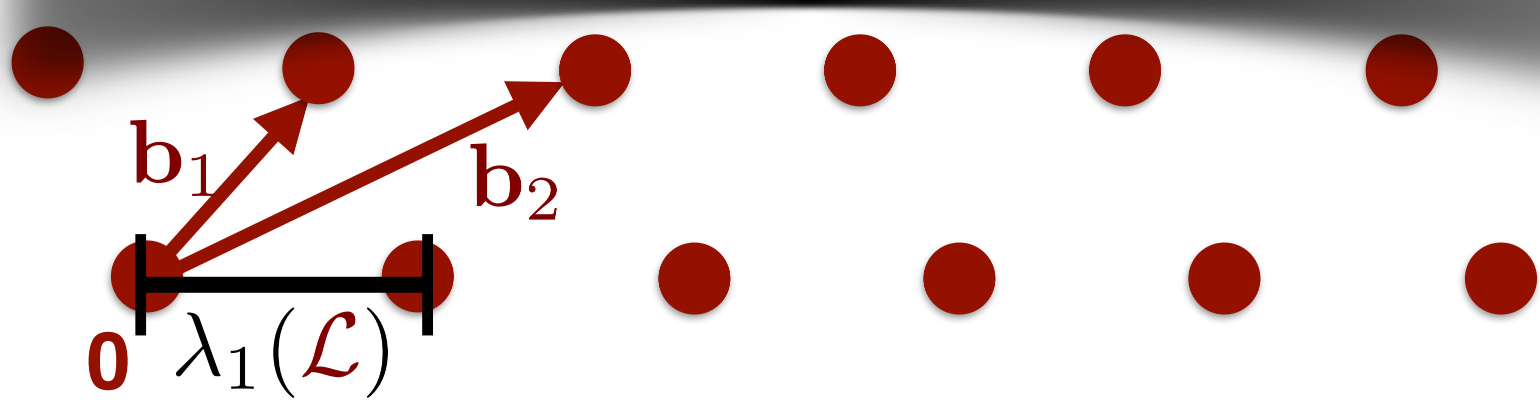
$$\|\mathbf{x}\|_p := (|x_1|^p + \cdots + |x_n|^p)^{1/p} .$$

$$\|\mathbf{x}\|_\infty := \max_i |x_i| .$$

$$\|\mathbf{x}\|_K := \min\{r \geq 0 \;:\; \mathbf{x} \in rK\} .$$

K is a symmetric convex body 

.



Lattices

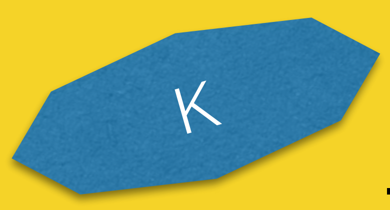
- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$
- Specified ... ndent vectors
- $\mathcal{L} = \{a_1\mathbf{b}$ ...
- $\lambda_1(\mathcal{L}) :=$ ...

Different norms of interest:

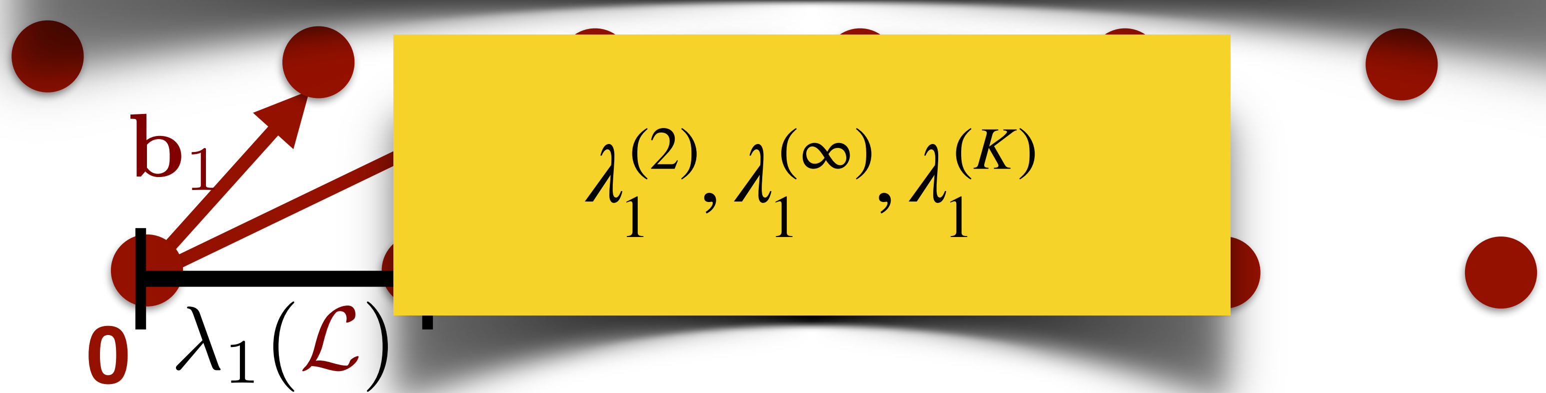
$$\|\mathbf{x}\|_p := (|x_1|^p + \cdots + |x_n|^p)^{1/p}.$$

$$\|\mathbf{x}\|_\infty := \max_i |x_i|.$$

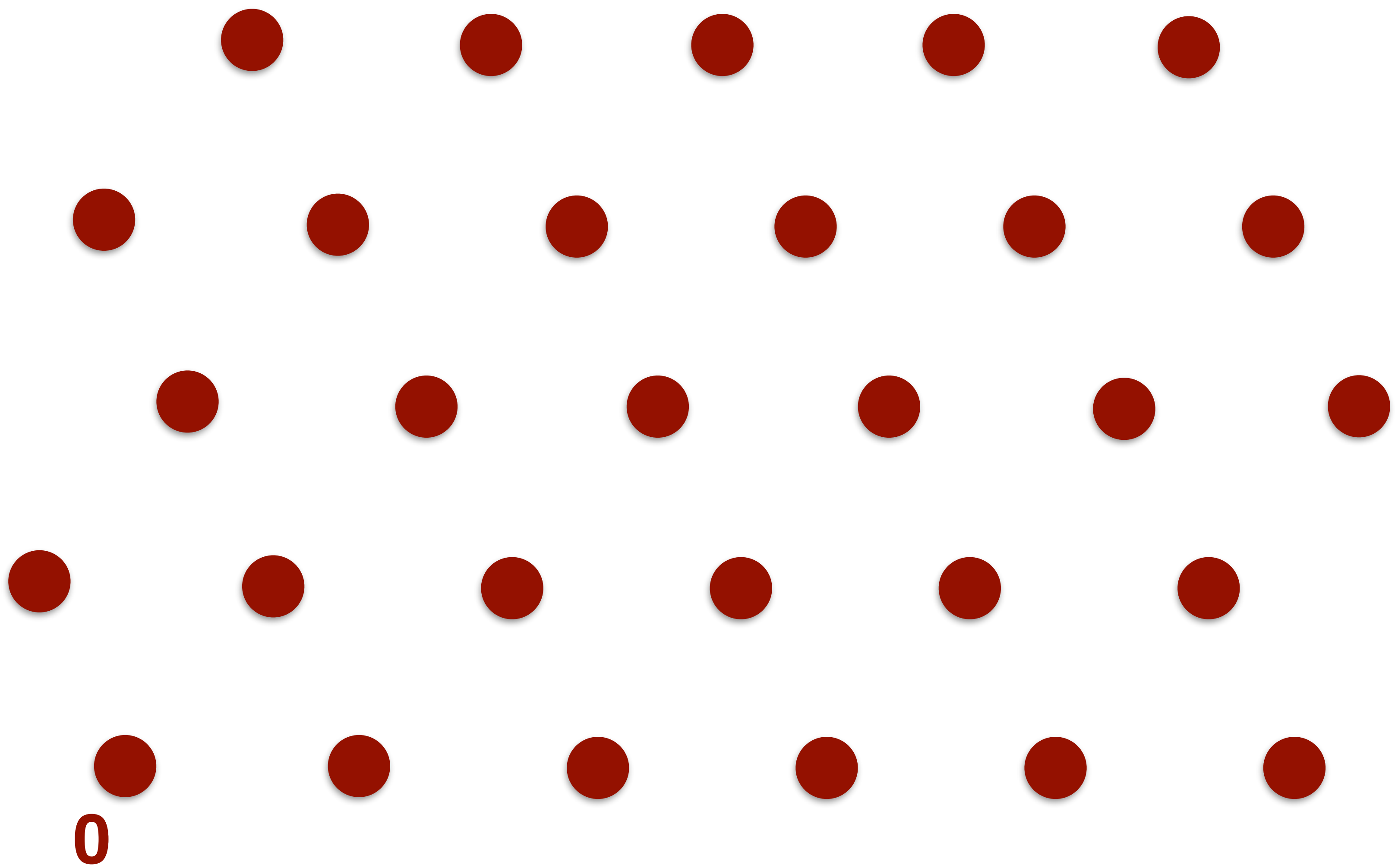
$$\|\mathbf{x}\|_K := \min\{r \geq 0 \ : \ \mathbf{x} \in rK\}.$$

K is a symmetric convex body .

$$\lambda_1^{(2)}, \lambda_1^{(\infty)}, \lambda_1^{(K)}$$

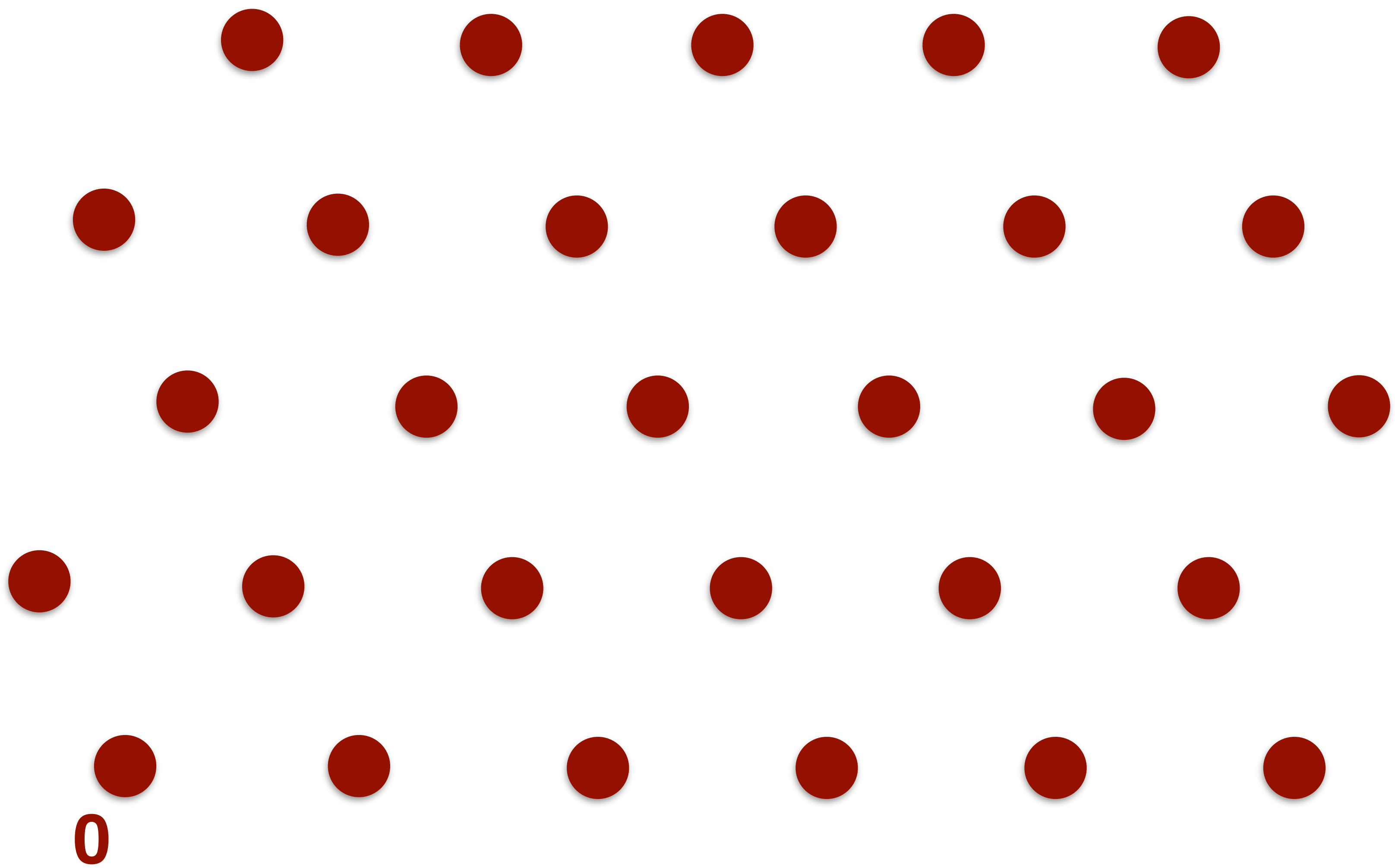


Shortest Vector Problem (SVP)



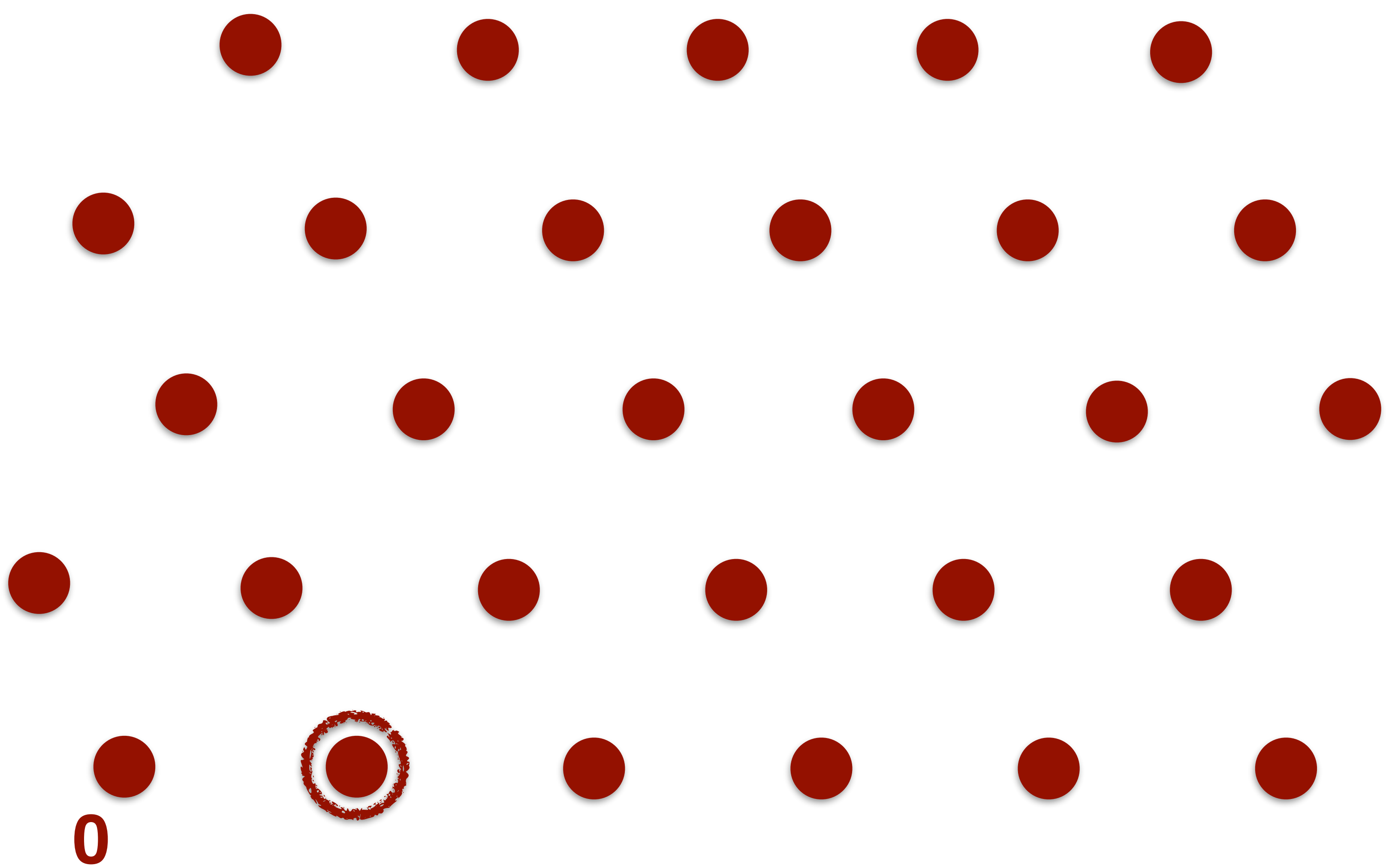
Shortest Vector Problem (SVP)

- SVP$_K(\mathcal{L})$: output a shortest non-zero $\mathbf{y} \in \mathcal{L}$



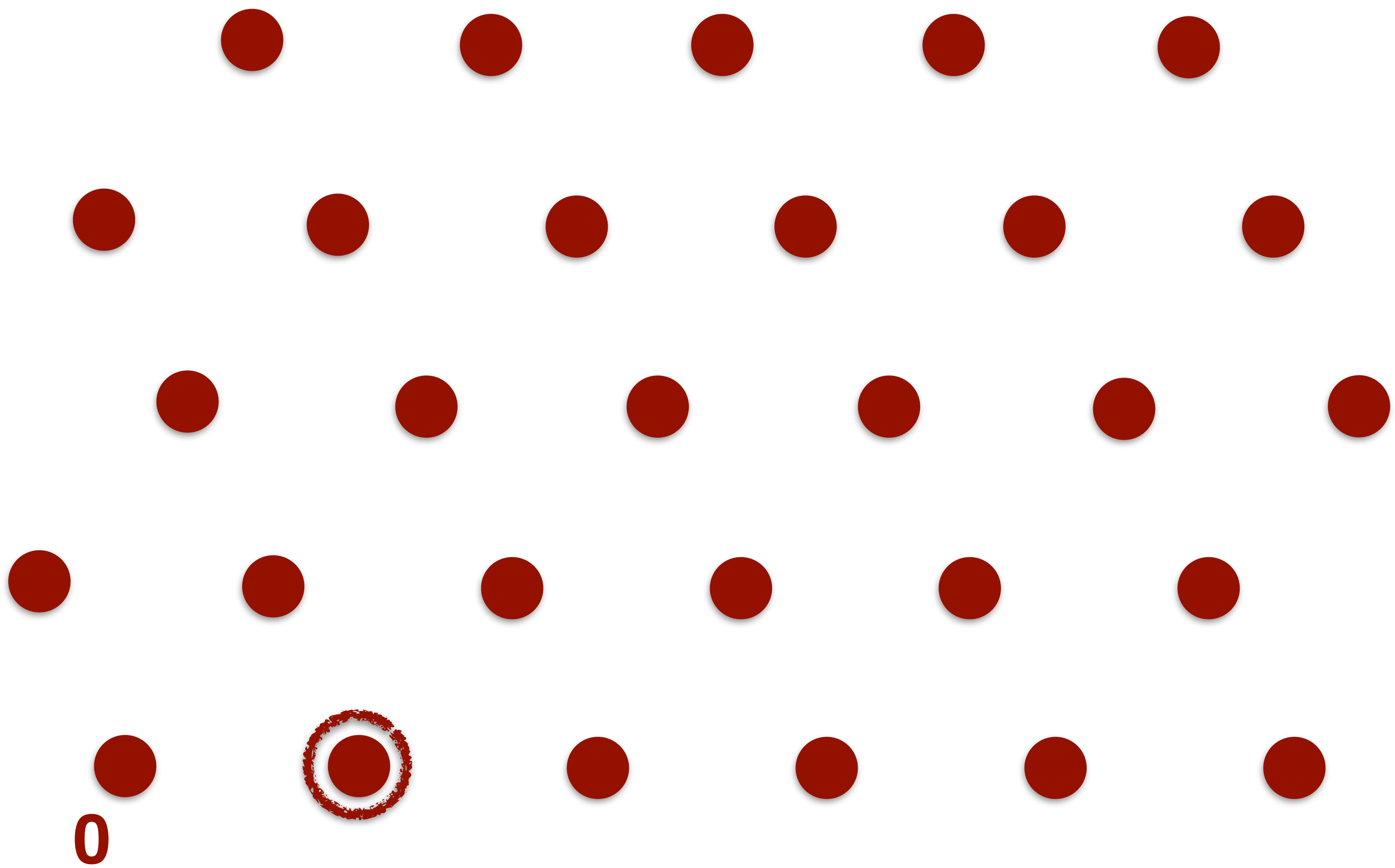
Shortest Vector Problem (SVP)

- $\mathsf{SVP}_K(\mathcal{L})$: output a shortest non-zero $\mathbf{y} \in \mathcal{L}$



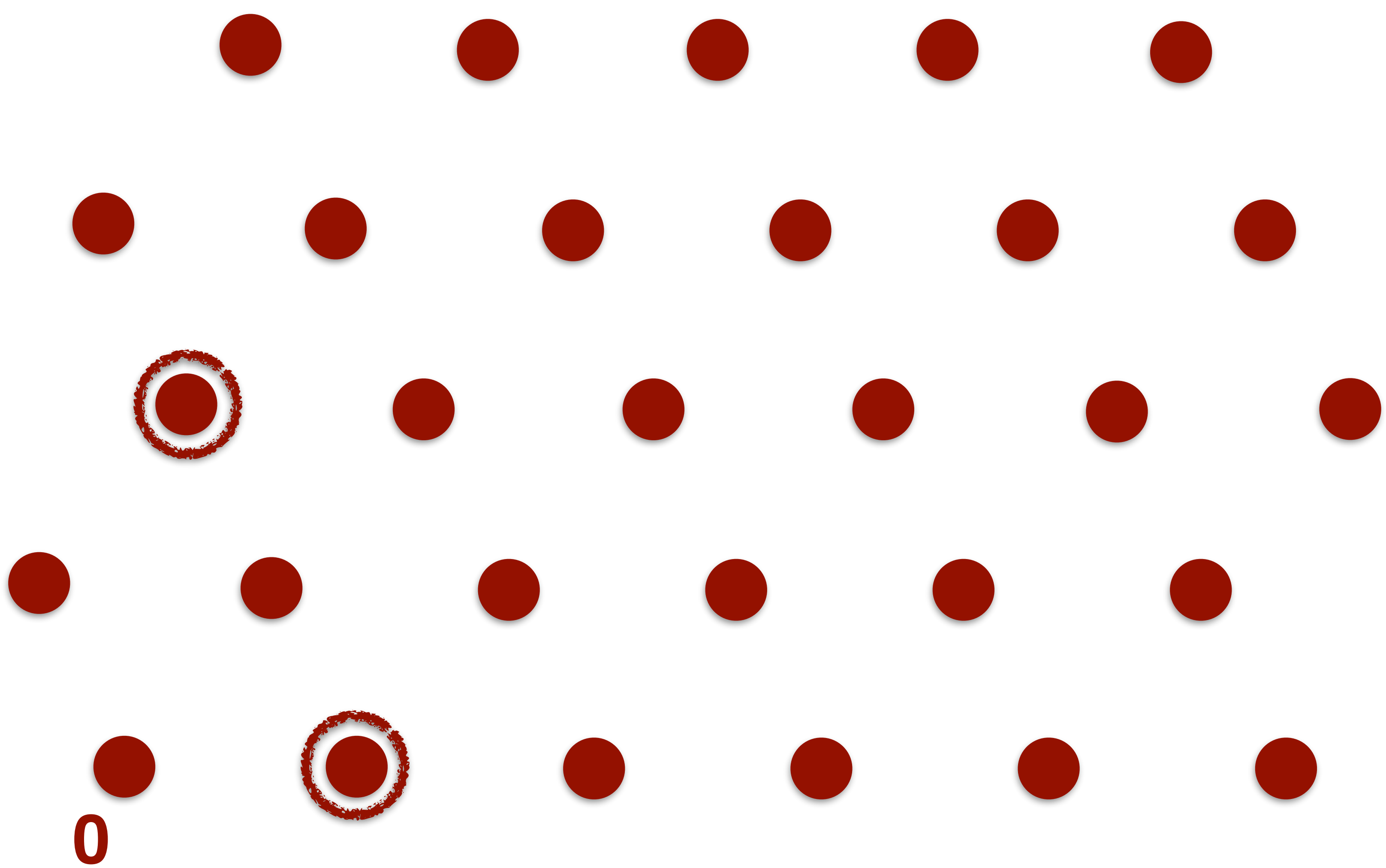
Shortest Vector Problem (SVP)

- SVP$_K(\mathcal{L})$: output a shortest non-zero $\mathbf{y} \in \mathcal{L}$
- γ-SVP$_K(\mathcal{L})$: Output $\mathbf{y} \in \mathcal{L}$ such that $0 < \|\mathbf{y}\| \le \gamma \lambda_1^{(K)}(\mathcal{L})$



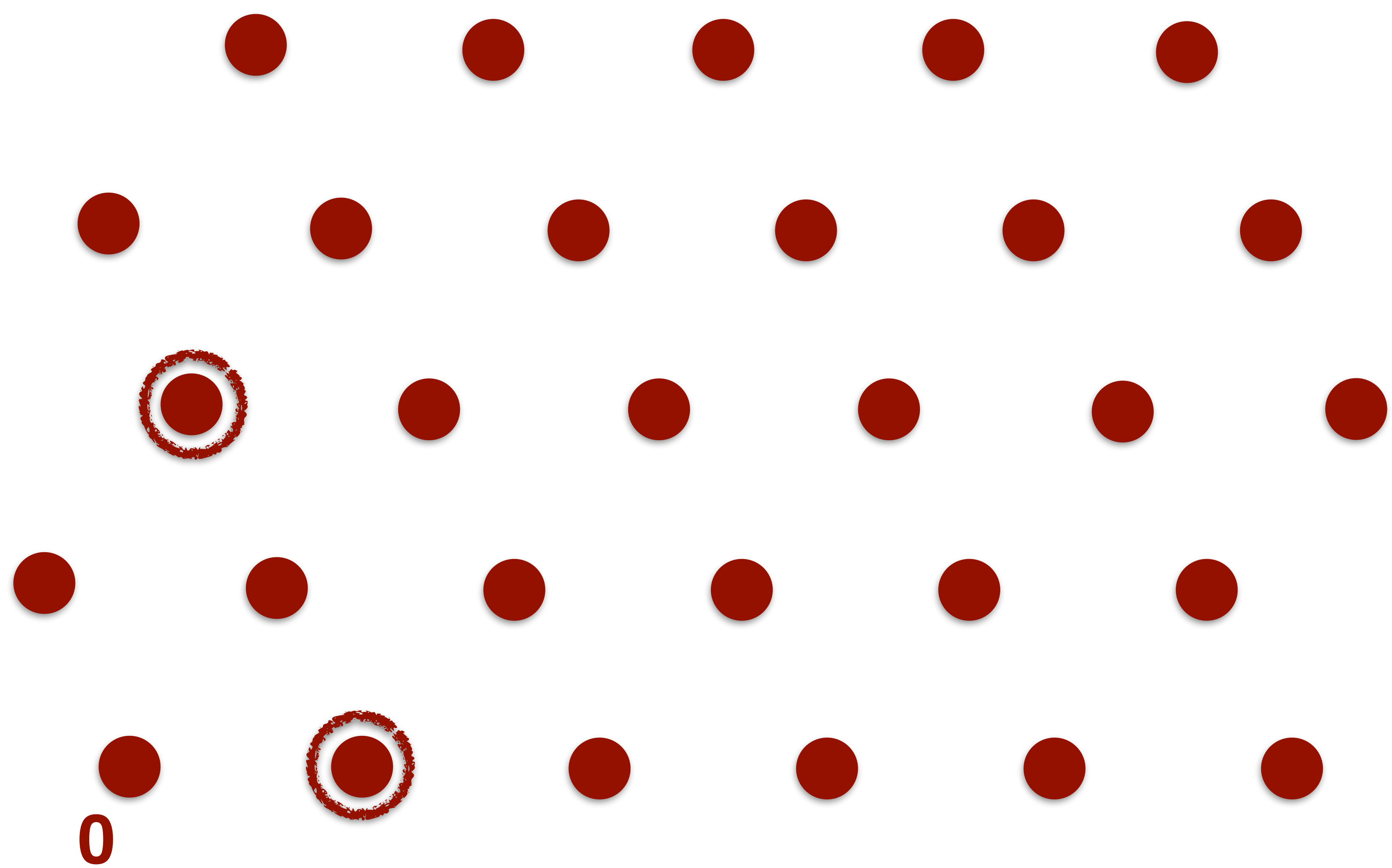
Shortest Vector Problem (SVP)

- SVP$_K(\mathcal{L})$: output a shortest non-zero $\mathbf{y} \in \mathcal{L}$
- γ-SVP$_K(\mathcal{L})$: Output $\mathbf{y} \in \mathcal{L}$ such that $0 < \|\mathbf{y}\| \leq \gamma \lambda_1^{(K)}(\mathcal{L})$



Shortest Vector Problem (SVP)

- $\text{SVP}_K(\mathcal{L})$: output a shortest non-zero $\mathbf{y} \in \mathcal{L}$
- $\gamma\text{-SVP}_K(\mathcal{L})$: Output $\mathbf{y} \in \mathcal{L}$ such that $0 < \|\mathbf{y}\| \le \gamma \lambda_1^{(K)}(\mathcal{L})$
- Hard for $\gamma \le n^{1/\log \log n}$.



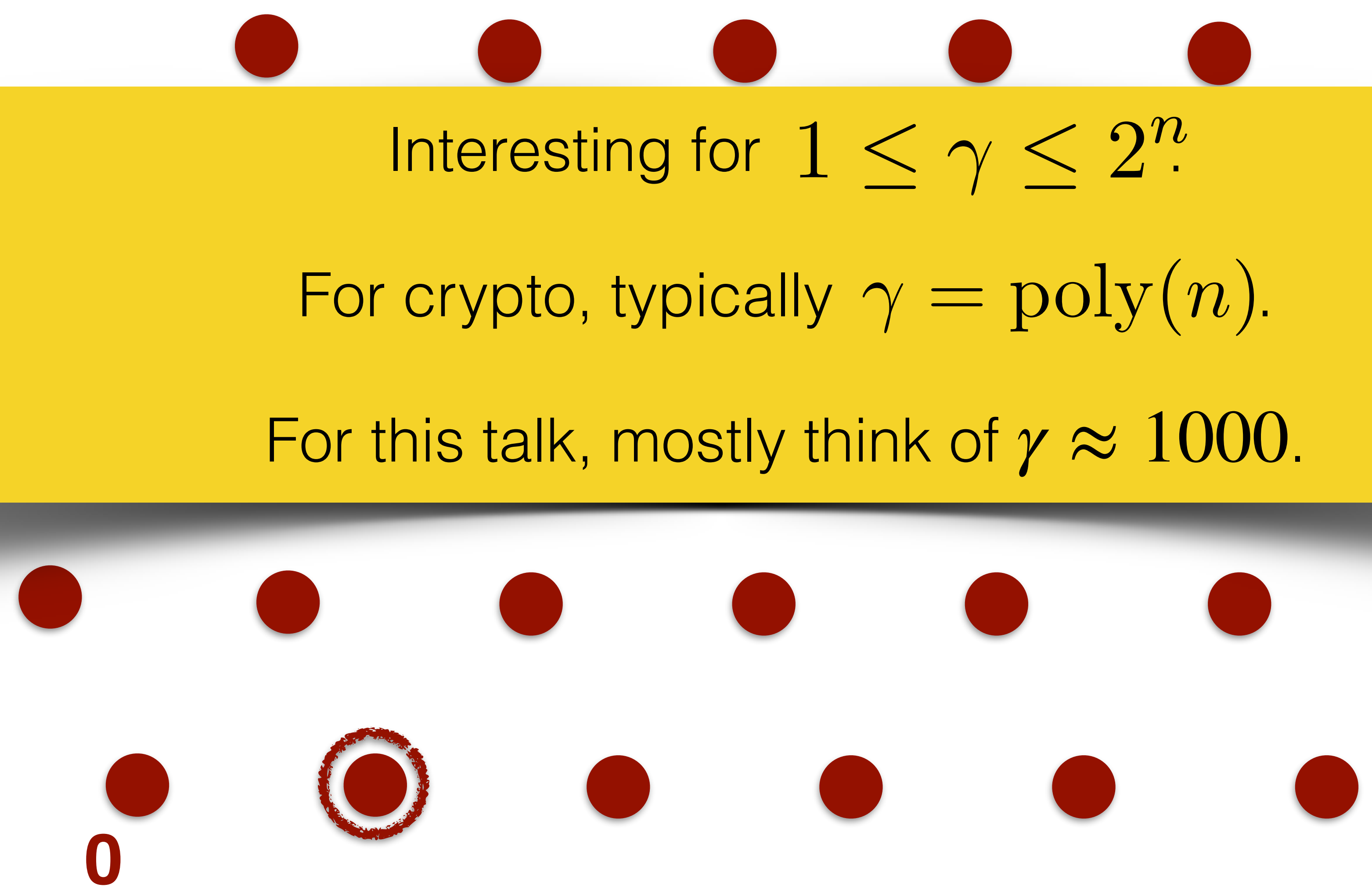
Shortest Vector Problem (SVP)

- SVP$_K(\mathcal{L})$: output a shortest non-zero $\mathbf{y} \in \mathcal{L}$
- γ-SVP$_K(\mathcal{L})$: Output $\mathbf{y} \in \mathcal{L}$ such that $0 < \|\mathbf{y}\| \leq \gamma \lambda_1^{(K)}(\mathcal{L})$
- Hard for $\gamma \leq n^{1/\log \log n}$.

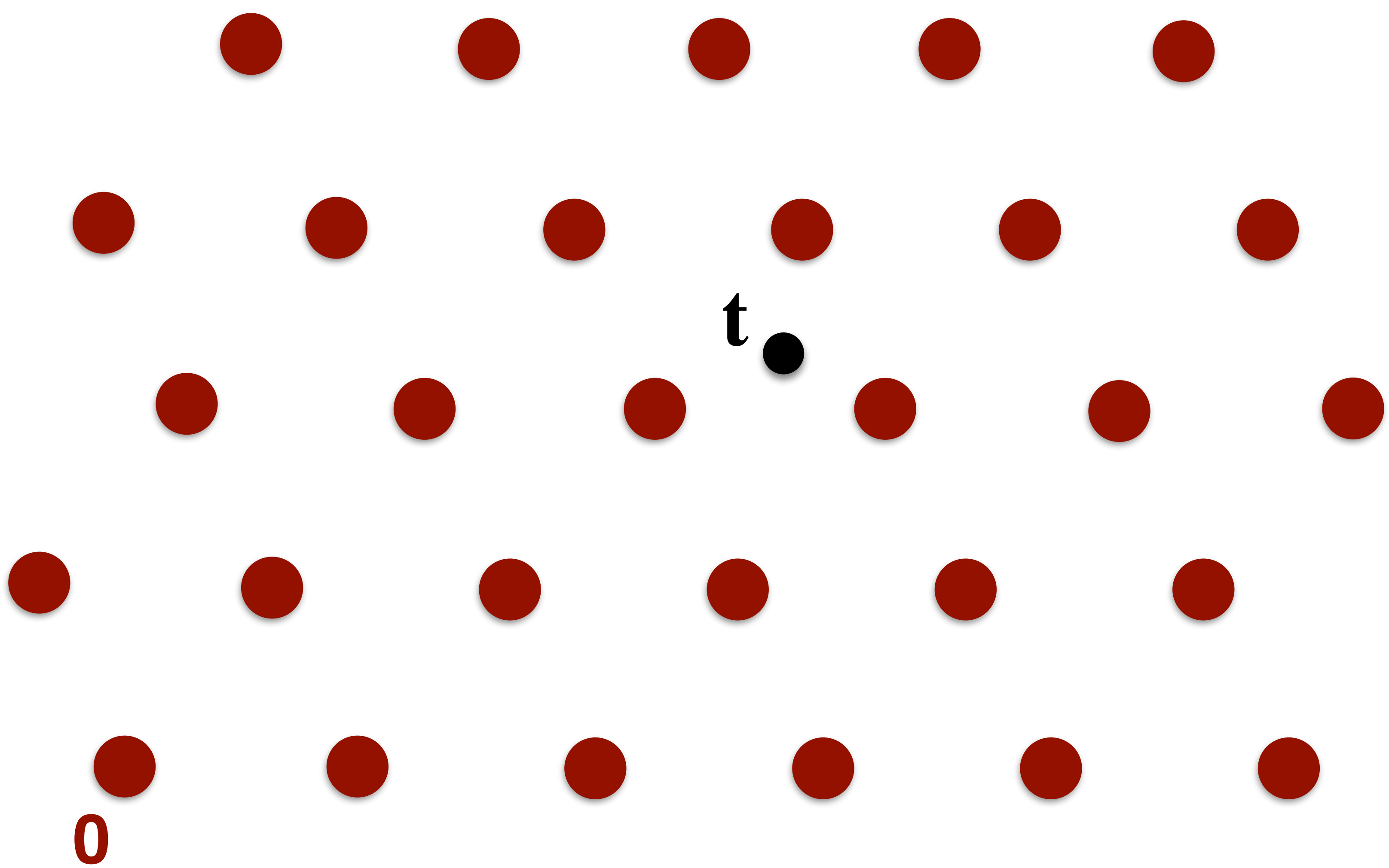
Interesting for $1 \leq \gamma \leq 2^n$.

For crypto, typically $\gamma = \mathrm{poly}(n)$.

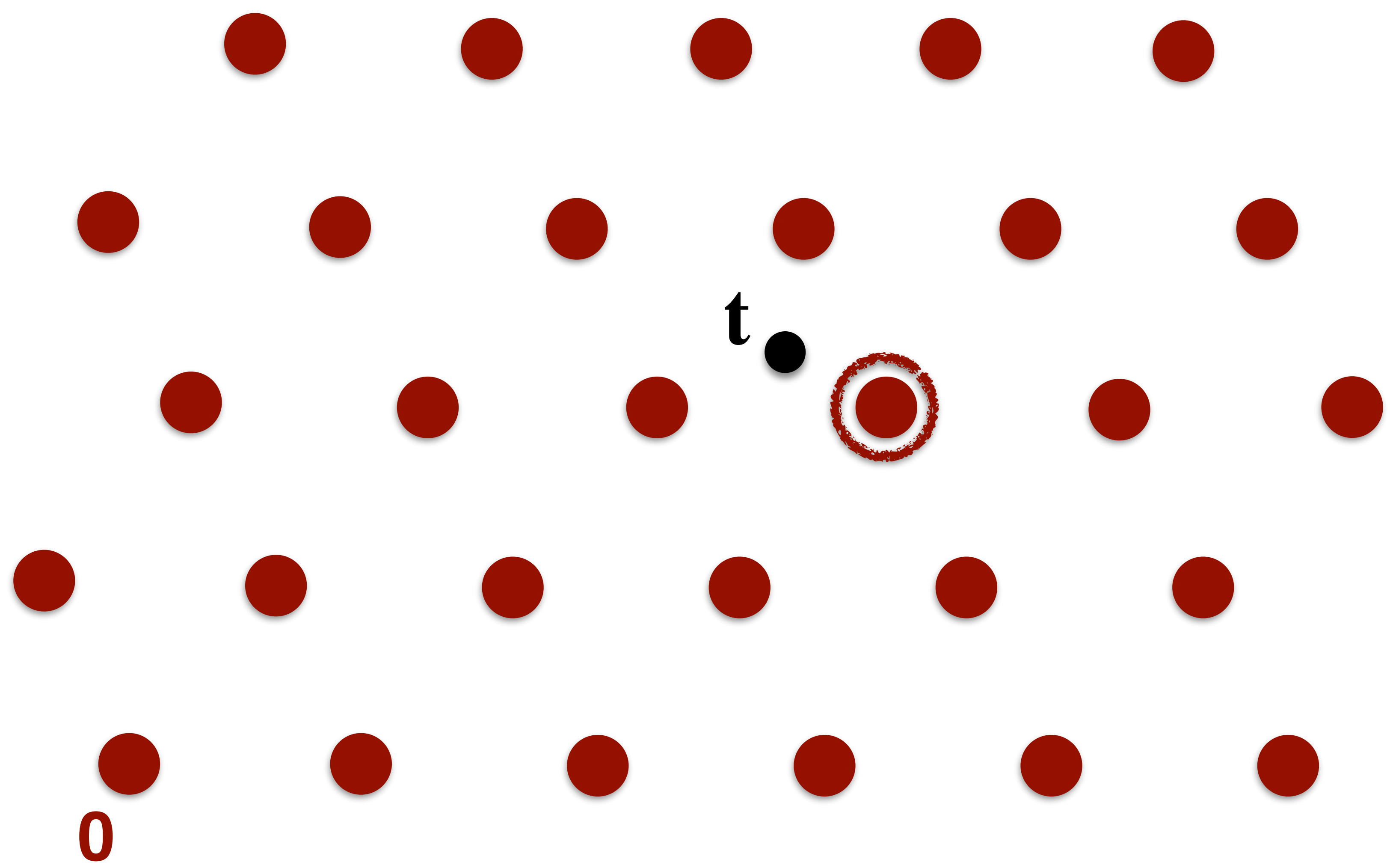
For this talk, mostly think of $\gamma \approx 1000$.



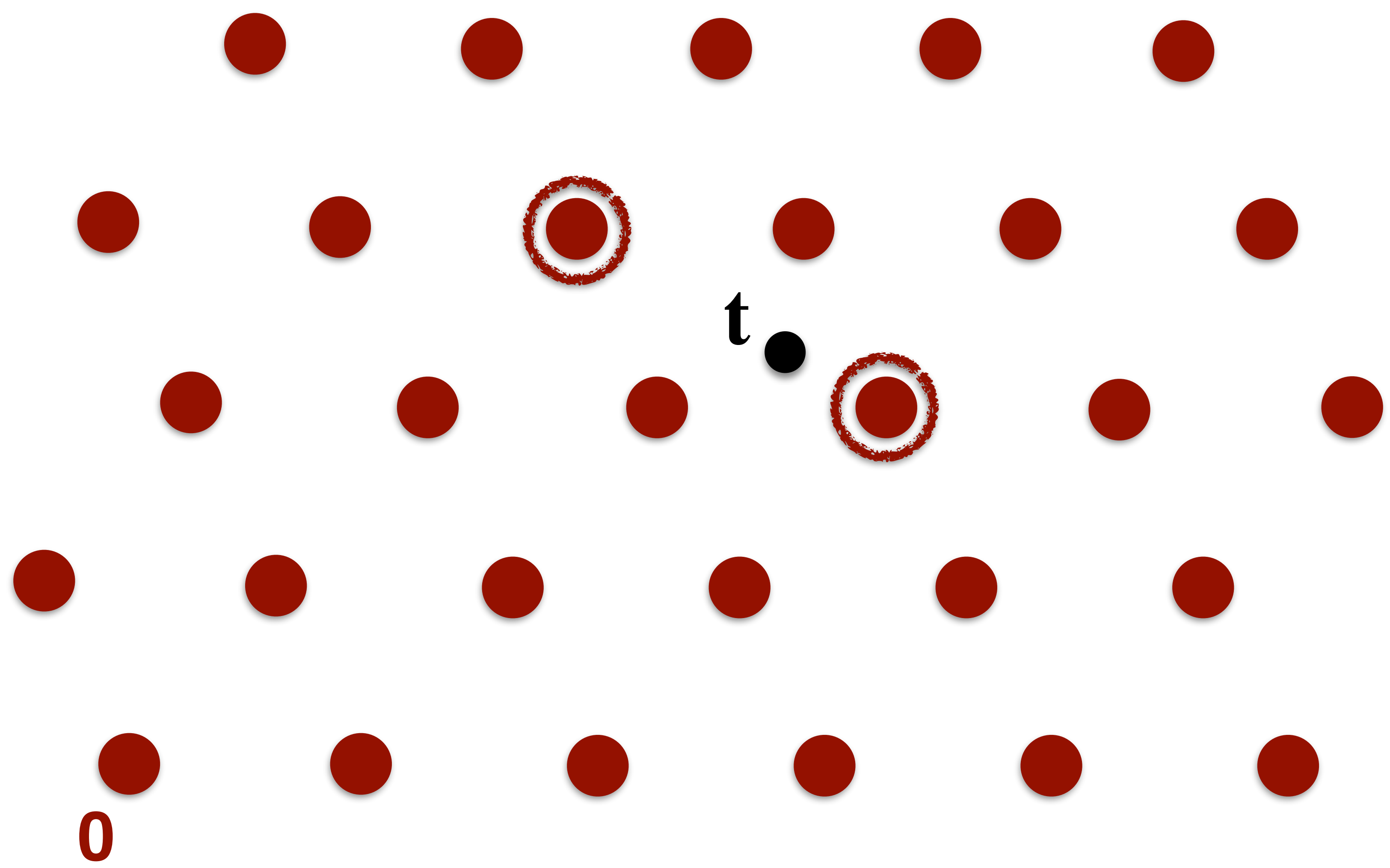
Closest Vector Problem (CVP)



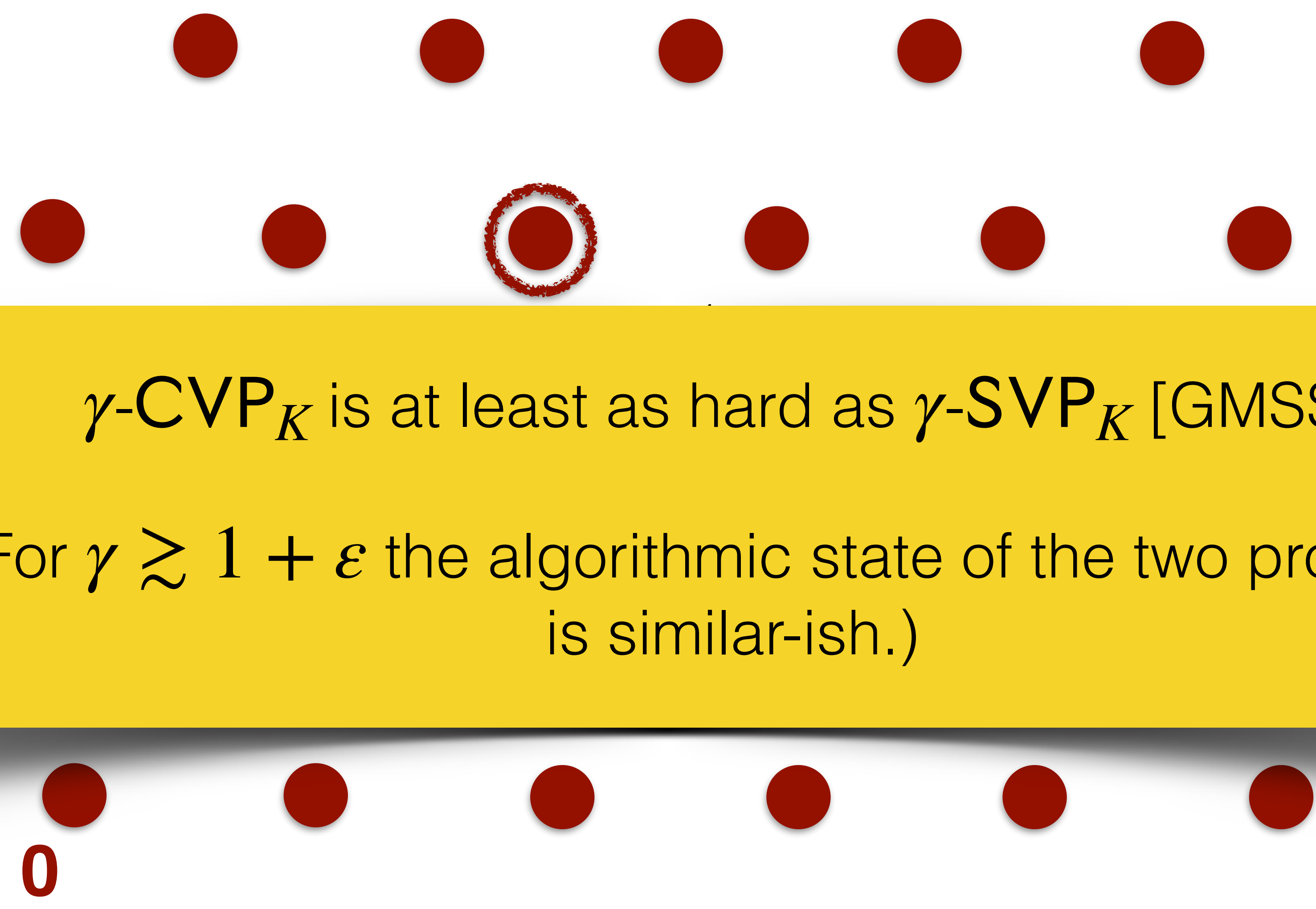
Closest Vector Problem (CVP)



Closest Vector Problem (CVP)



Closest Vector Problem (CVP)

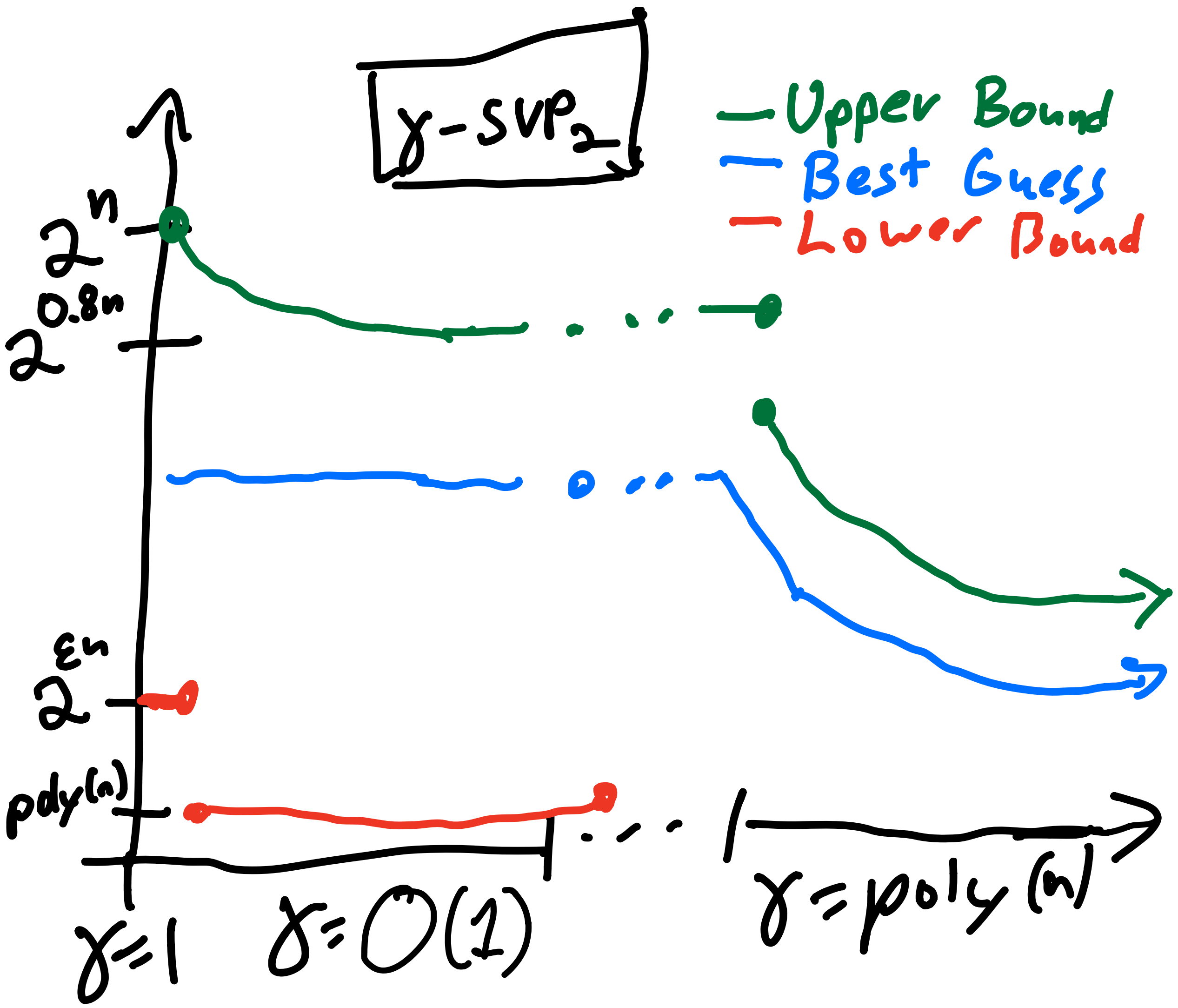


γ-CVP$_K$ is at least as hard as γ-SVP$_K$ [GMSS].

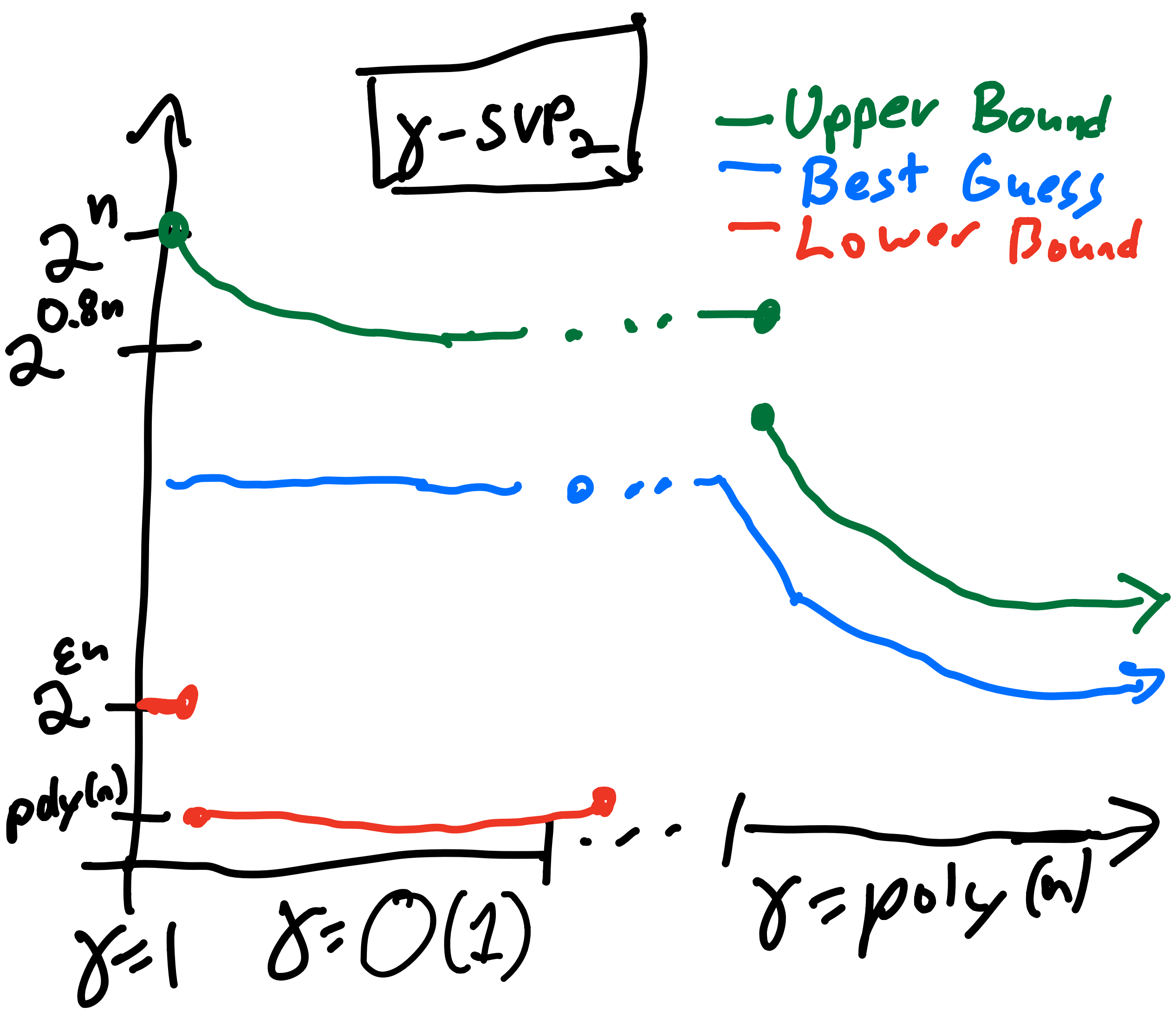
(For $\gamma \gtrsim 1 + \varepsilon$ the algorithmic state of the two problems is similar-ish.)

The World Before May 7, 2020

The World Before May 7, 2020

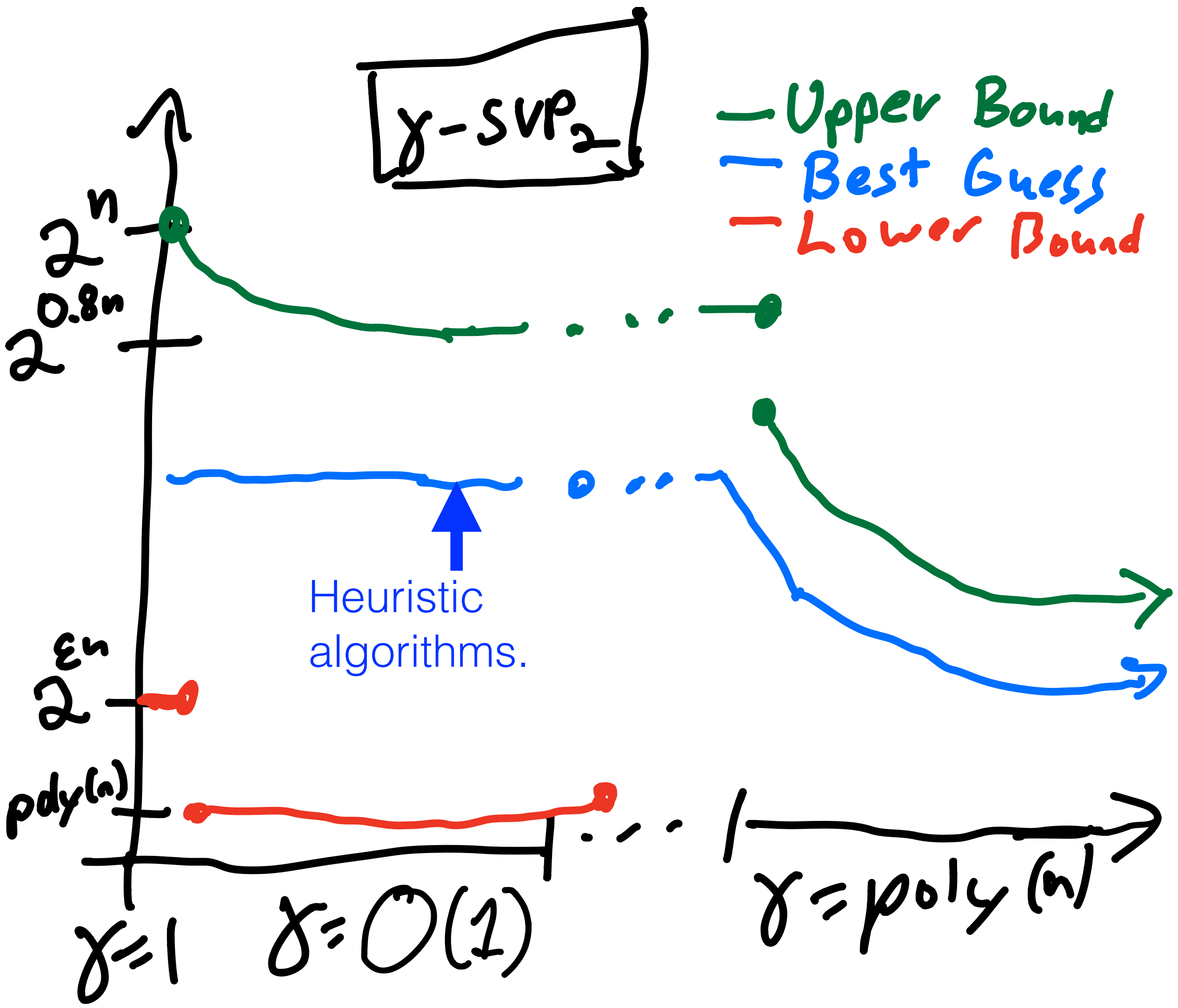


The World Before May 7, 2020



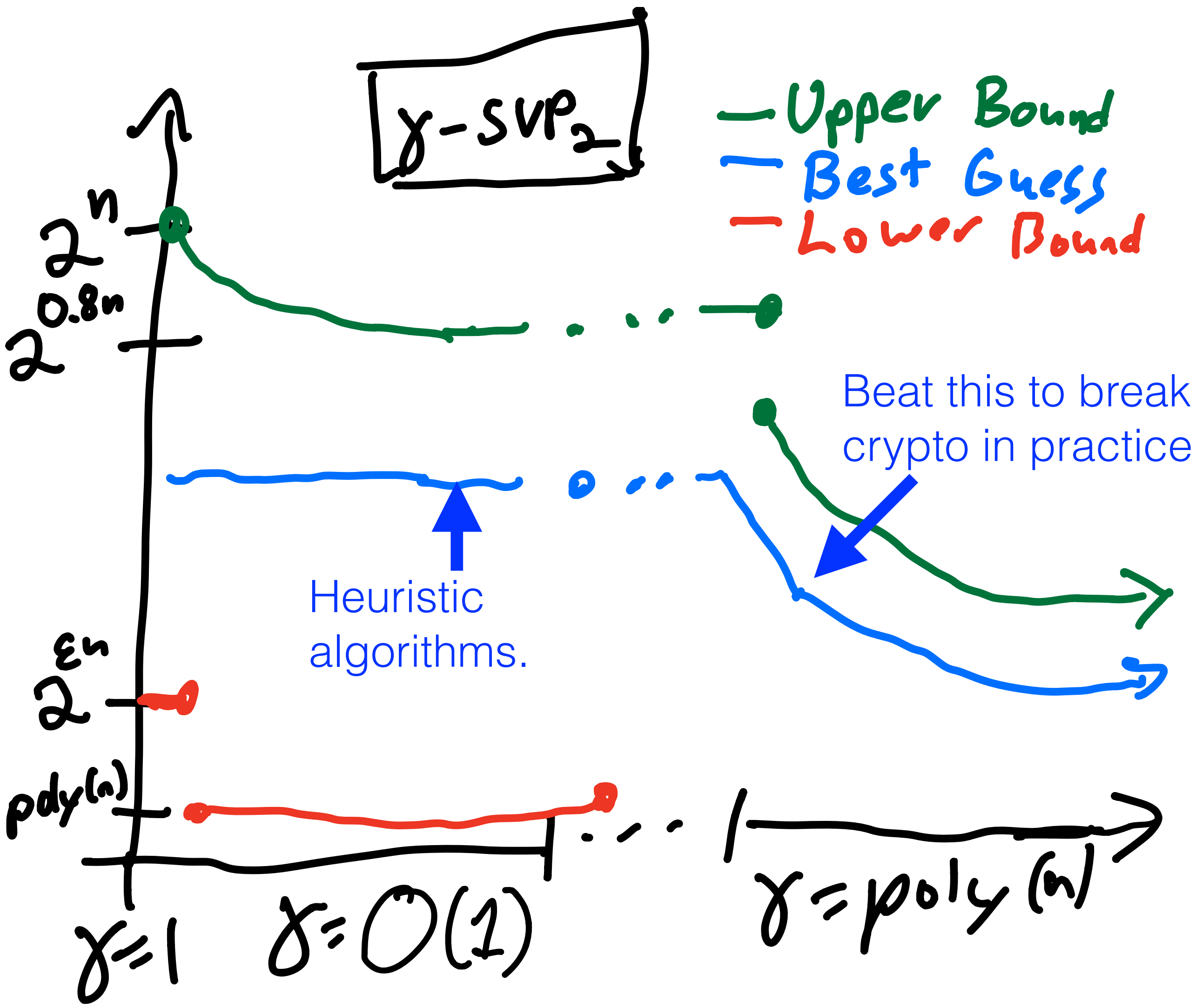
(See [ALS21, Table 1].)

The World Before May 7, 2020



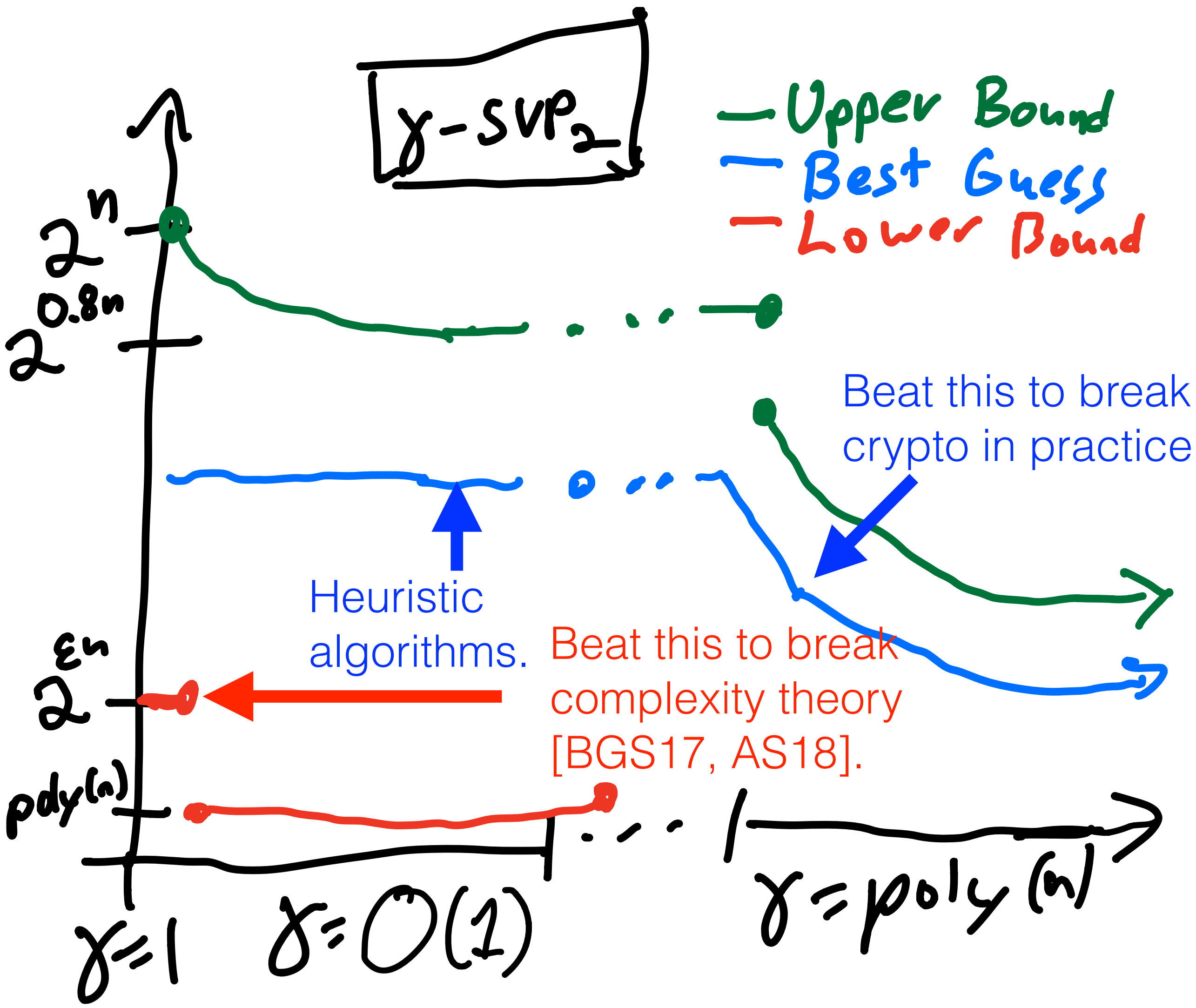
(See [ALS21, Table 1].)

The World Before May 7, 2020



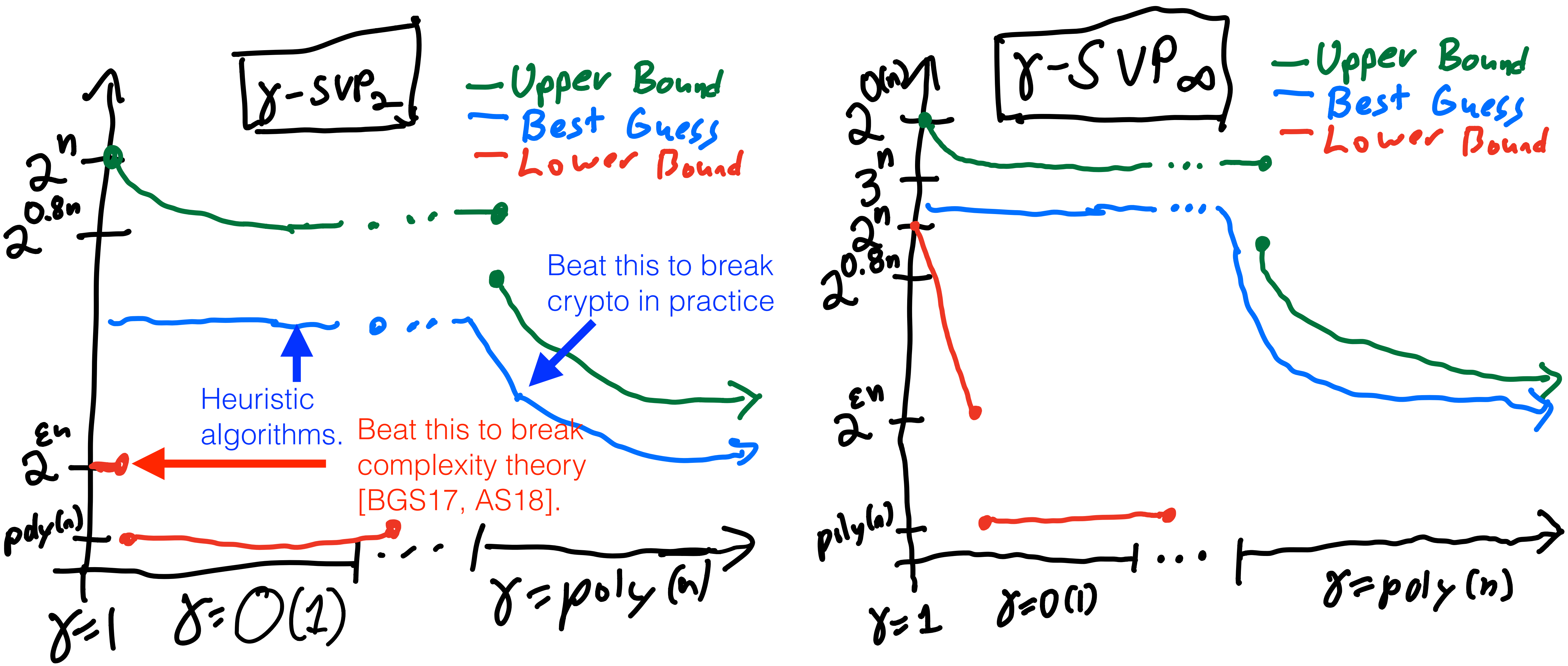
(See [ALS21, Table 1].)

The World Before May 7, 2020



(See [ALS21, Table 1].)

The World Before May 7, 2020



(See [ALS21, Table 1].)

The World Before May 7, 2020

List of Open Problems

- ♦ 1. Tight fine-grained hardness for exact CVP in the Euclidean norm?
- ♦ 2. Hardness for polynomial approximation factor?
- ♦ 3. Tight fine-grained hardness for exact SVP in the Euclidean norm?
- ● 4. Better algorithms in L_p norms?
- ■ 5. Better understanding of locally dense lattices?
- ■ 6. ***NP***-hardness of $n^{1/\log \log n}$-SVP?
- ■/♦ 7. Fine-grained hardness of approximation? (CVP/SVP)
- ■ 8. Upper bound between $n^{1/\log \log n}$ and $\sqrt{n/\log n}$?

● Easy

■ Medium

♦ Hard

Noah Stephens-Davidowitz | Lattice Problems

MAY 7, 2020!!

MAY 7, 2020!!

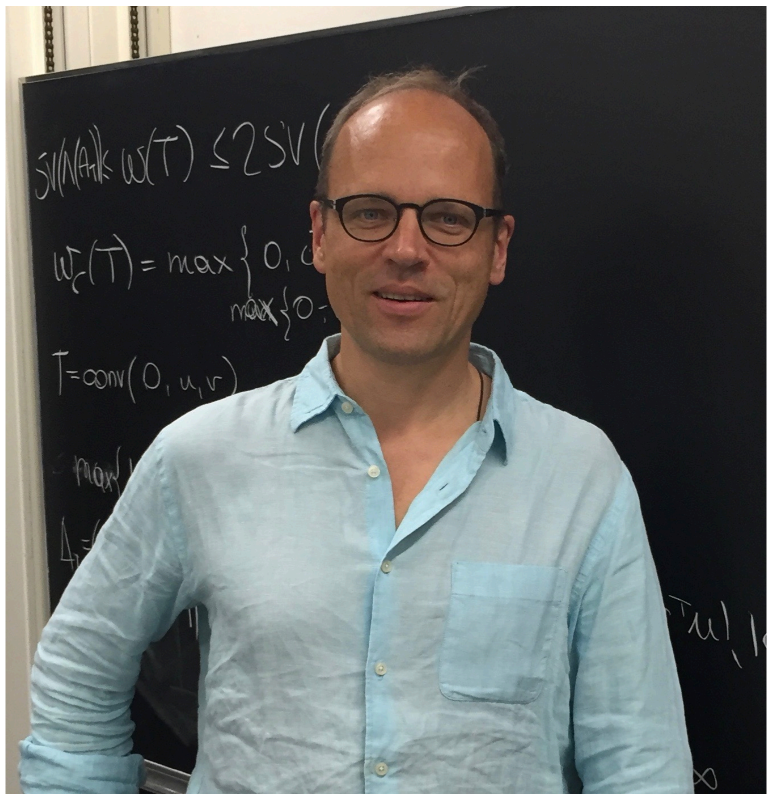
Faster algorithms for SVP_p/CVP_p (question at Simons) Inbox ×

Venzin Moritz Andreas moritz.venzin@epfl.ch via gmail.com — Thu, May 7, 2020, 4:28 PM

to noahsd@gmail.com

Dear Noah

Eisenbrand and Venzin



Friedrich Eisenbrand

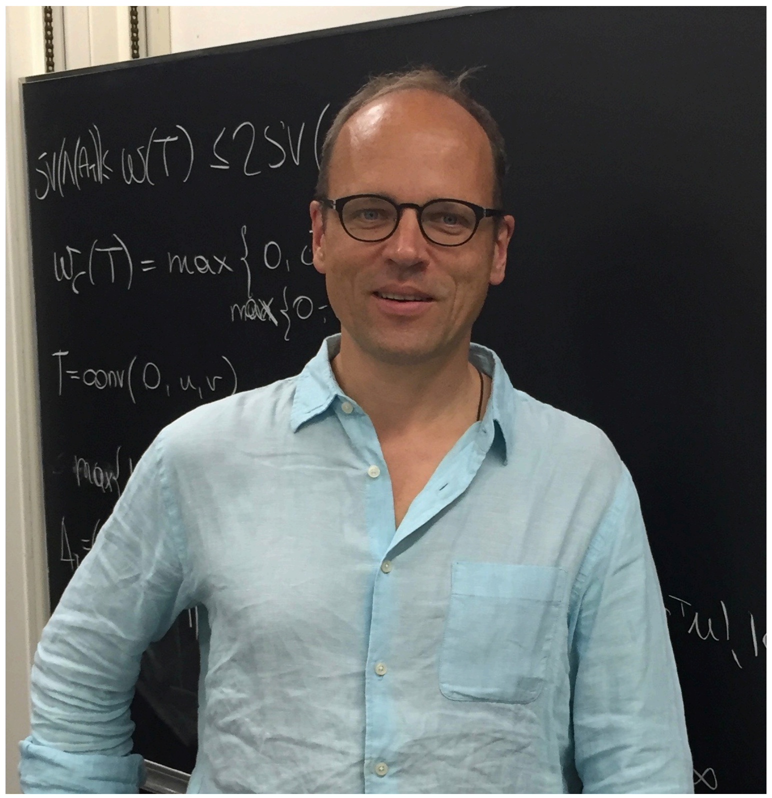
Moritz Venzin

Approximate CVP_p in time $2^{0.802\,n}$

Friedrich Eisenbrand *
EPFL
Switzerland
friedrich.eisenbrand@epfl.ch

Moritz Venzin
EPFL
Switzerland
moritz.venzin@epfl.ch

Eisenbrand and Venzin



Friedrich Eisenbrand

Moritz Venzin

Approximate CVP_p in time $2^{0.802\,n}$

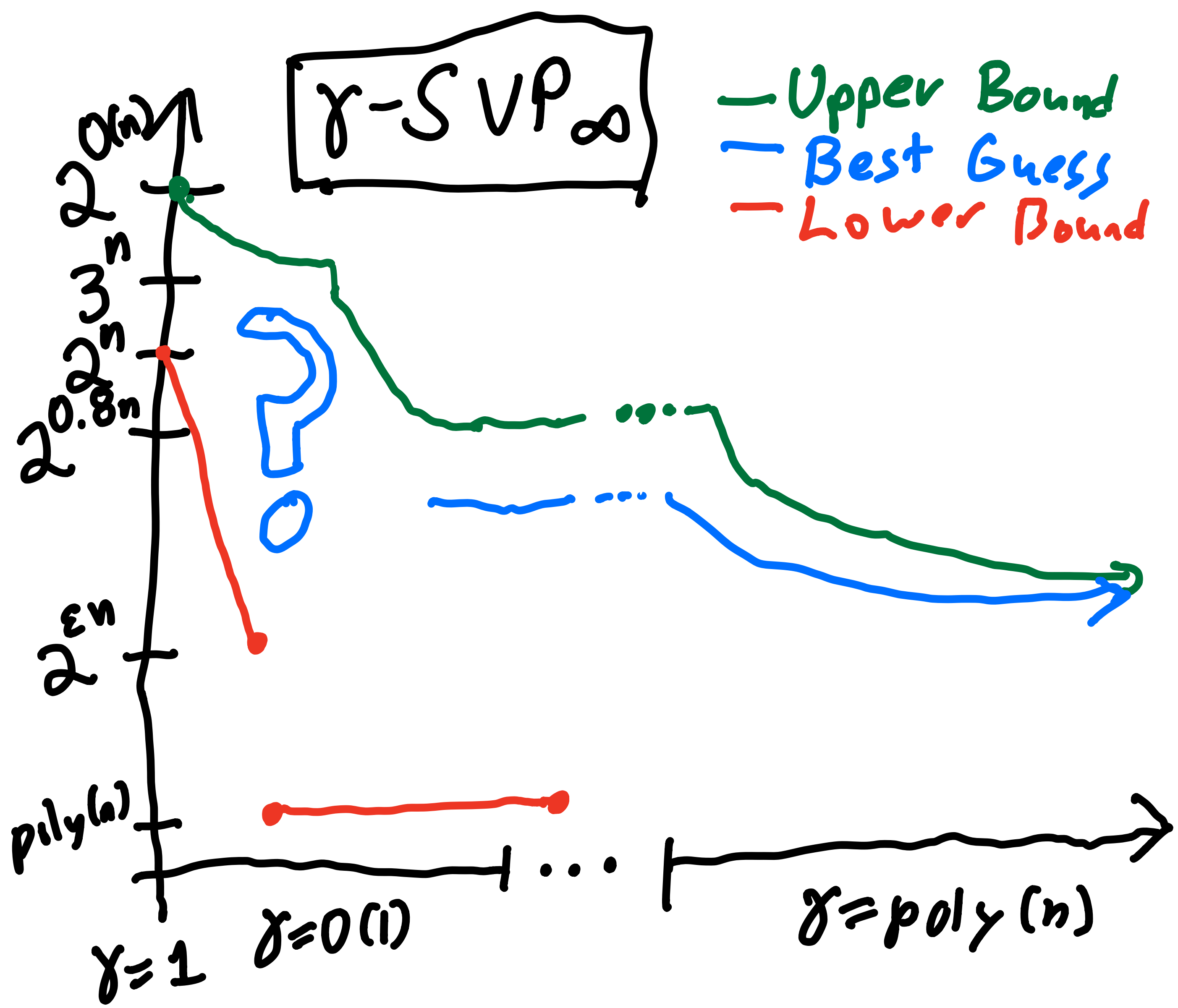
Friedrich Eisenbrand *
EPFL
Switzerland
friedrich.eisenbrand@epfl.ch

Moritz Venzin
EPFL
Switzerland
moritz.venzin@epfl.ch

Best known running time for $O(1)$-SVP_2 [LWXZ11, WLW15, AUV19]

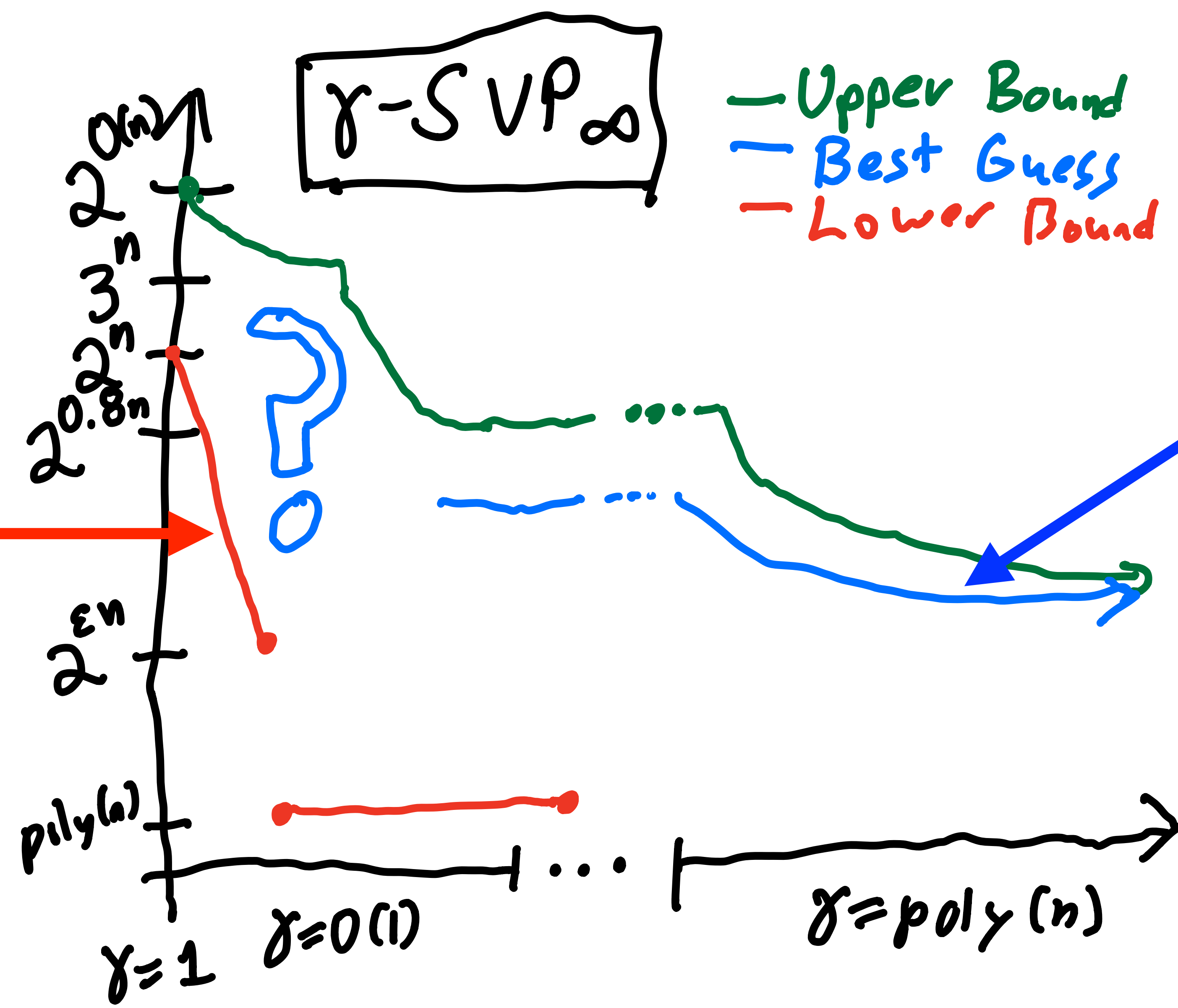
The World After May 7, 2020

The World After May 7, 2020



The World After May 7, 2020

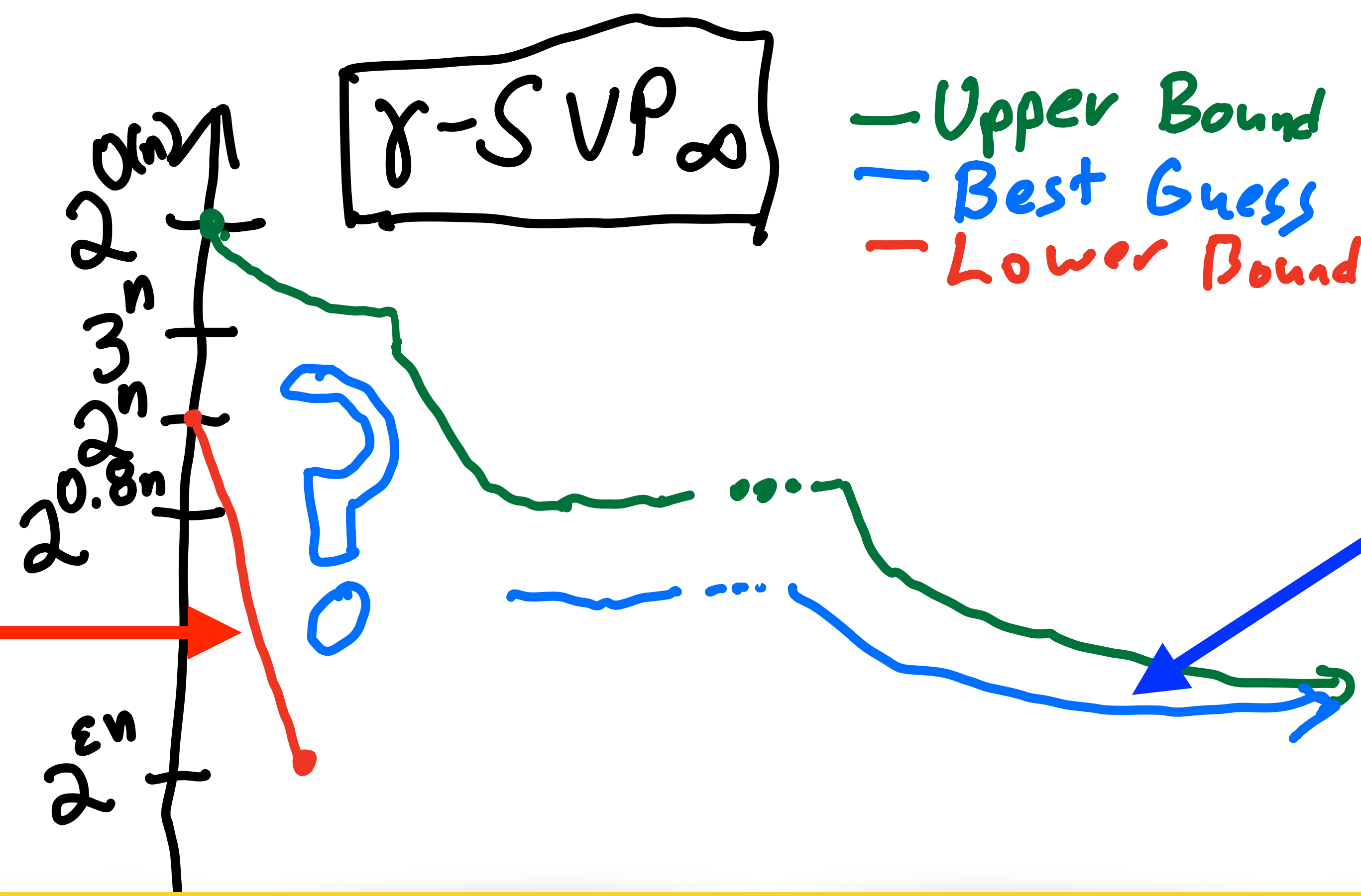
Algorithms below this line break SETH [BGS17].



Algorithms below this line break crypto in practice.

The World After May 7, 2020

Algorithms below this line break SETH [BGS17].



Algorithms below this line break crypto in practice.

Possible resolutions:

1. A strangely wiggly line.
2. SETH is false.
3. Lattice-based crypto is <u>much</u> less secure than we think.

Eisenbrand and Venzin (for ℓ_∞)

Eisenbrand and Venzin (for ℓ_∞)

- **Observation 1:** The fastest algorithm for $O(1)$-SVP_2 runs in time $2^{0.802n}$.

Eisenbrand and Venzin (for ℓ_∞)

- **Observation 1:** The fastest algorithm for $O(1)$-SVP$_2$ runs in time $2^{0.802n}$.
- **Observation 2:** It doesn't only find one $O(1)$-approximate ℓ_2-shortest vector, it finds "exponentially many ℓ_2-short vectors." *(There are issues when there are only a few such points in the lattice, but it works out.)*

Eisenbrand and Venzin (for ℓ_∞)

- **Observation 1:** The fastest algorithm for $O(1)$-SVP$_2$ runs in time $2^{0.802n}$.
- **Observation 2:** It doesn't only find one $O(1)$-approximate ℓ_2-shortest vector, it finds "exponentially many ℓ_2-short vectors." *(There are issues when there are only a few such points in the lattice, but it works out.)*
- **Observation 3:** Many ℓ_2 short vectors $\implies$ an $O(1)$ -approximate ℓ_∞-shortest vectors.

Eisenbrand and Venzin

Observation 3: Many ℓ_2 short vectors $\Longrightarrow$ one $O(1)$-approximate ℓ_∞-shortest vectors.

$$\lambda_1^{(\infty)}(L) = 1 \qquad \lambda_1^{(2)}(L) \leq \sqrt{n}$$

Eisenbrand and Venzin

Observation 3: Many ℓ_2 short vectors $\Longrightarrow$ one $O(1)$-approximate ℓ_∞-shortest vectors.

$$\lambda_1^{(\infty)}(L) = 1 \qquad \lambda_1^{(2)}(L) \leq \sqrt{n}$$

Claim. Let $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathbb{R}^n$ with $\|\mathbf{y}_i\| \leq \sqrt{n}$ and $N \geq 2^{n/10}$. Then, there exists $i \neq j$ such that $\|\mathbf{y}_i - \mathbf{y}_j\|_\infty \leq 1000$.

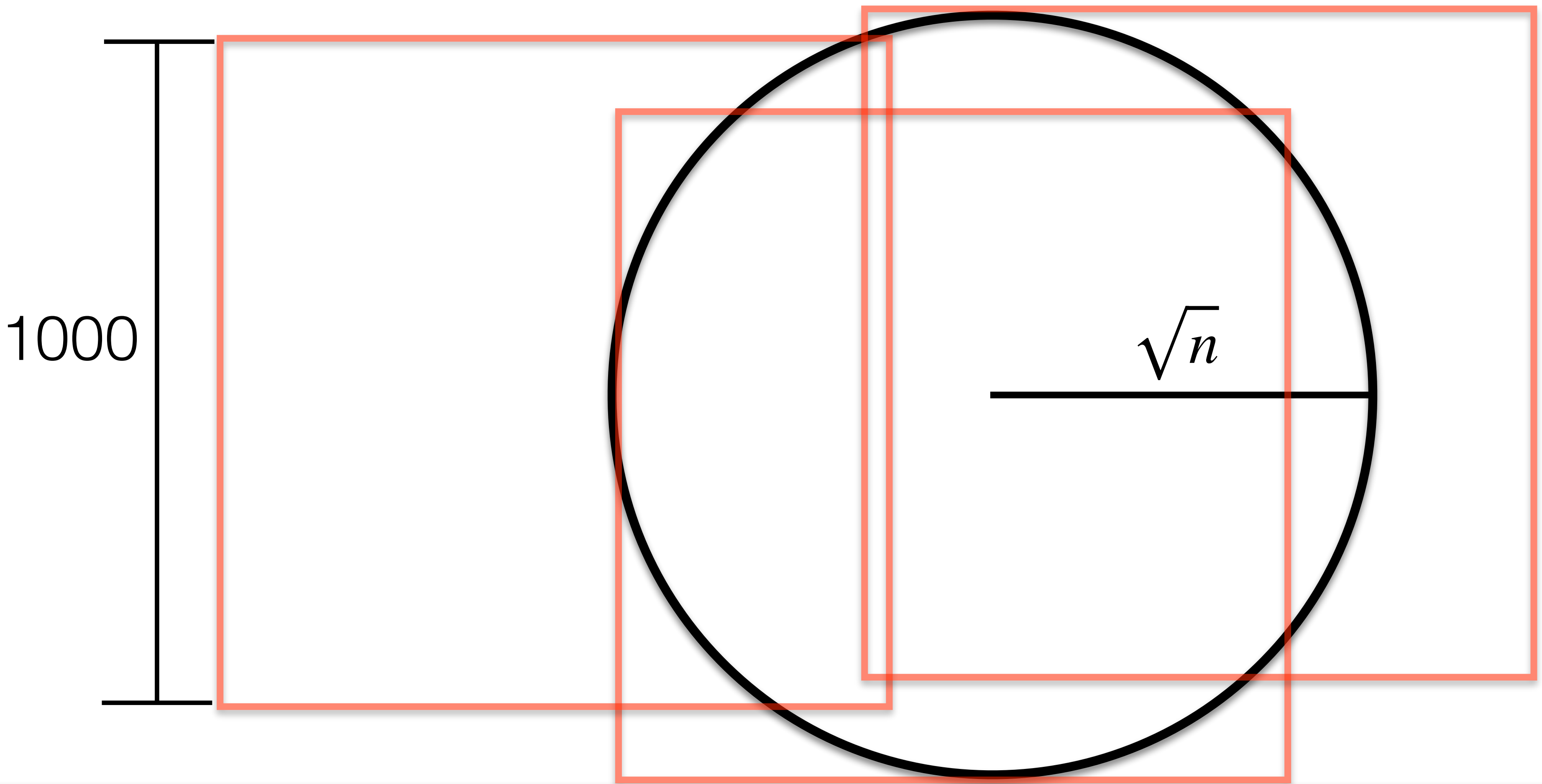
Eisenbrand and Venzin

Claim. Let $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathbb{R}^n$ with $\|\mathbf{y}_i\| \leq \sqrt{n}$ and $N \geq 2^{n/10}$. Then, there exists $i \neq j$ such that $\|\mathbf{y}_i - \mathbf{y}_j\|_\infty \leq 1000$.

Eisenbrand and Venzin

Claim. Let $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathbb{R}^n$ with $\|\mathbf{y}_i\| \le \sqrt{n}$ and $N \ge 2^{n/10}$. Then, there exists $i \ne j$ such that $\|\mathbf{y}_i - \mathbf{y}_j\|_\infty \le 1000$.

Can cover the $\sqrt{n}B_2$ by $2^{n/10}$ cubes $500B_\infty$.

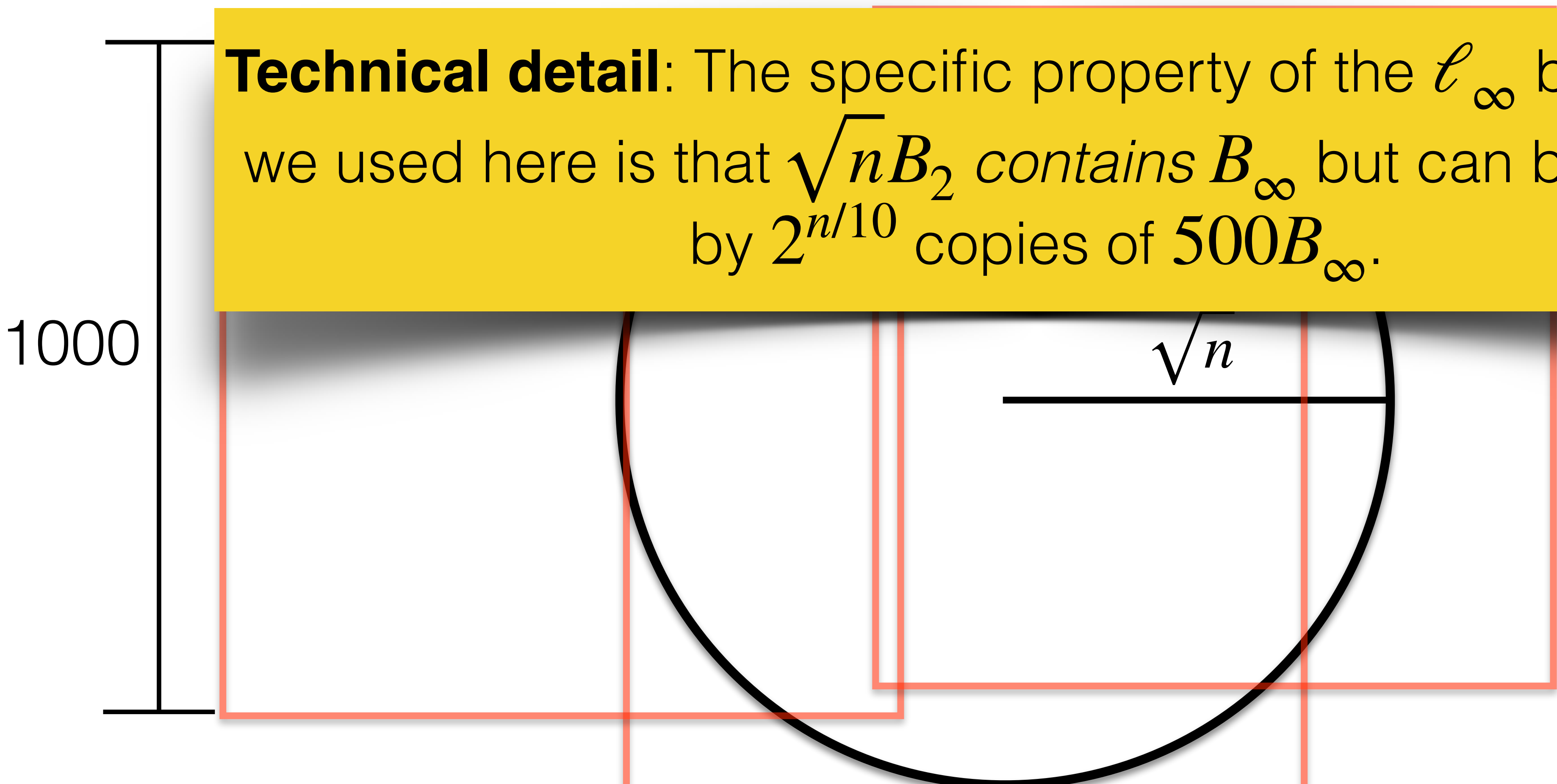


Eisenbrand and Venzin

Claim. Let $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathbb{R}^n$ with $\|\mathbf{y}_i\| \leq \sqrt{n}$ and $N \geq 2^{n/10}$. Then, there exists $i \neq j$ such that $\|\mathbf{y}_i - \mathbf{y}_j\|_\infty \leq 1000$.

Can cover the $\sqrt{n}B_2$ by $2^{n/10}$ cubes $500B_\infty$.

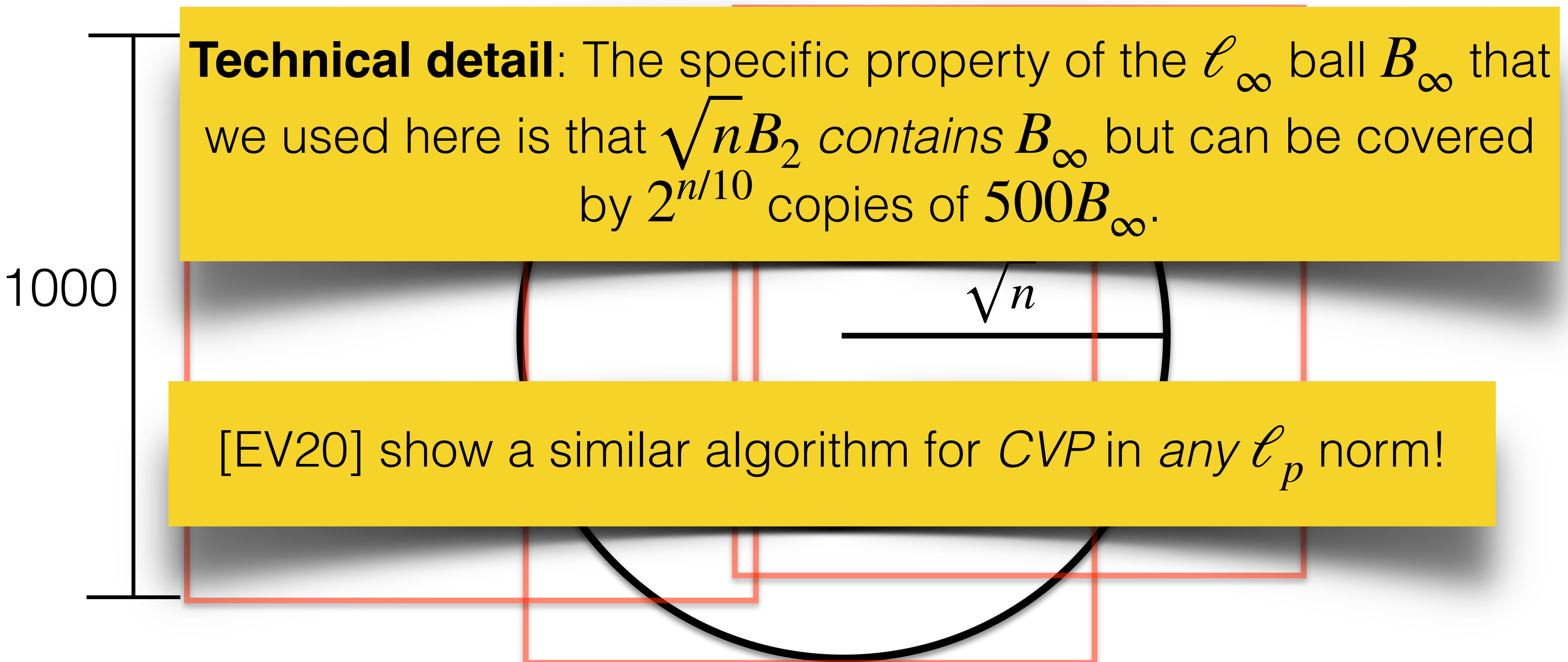
Technical detail: The specific property of the ℓ_∞ ball B_∞ that we used here is that $\sqrt{n}B_2$ *contains* B_∞ but can be covered by $2^{n/10}$ copies of $500B_\infty$.



Eisenbrand and Venzin

<u>Claim.</u> Let $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathbb{R}^n$ with $\|\mathbf{y}_i\| \le \sqrt{n}$ and $N \ge 2^{n/10}$. Then, there exists $i \neq j$ such that $\|\mathbf{y}_i - \mathbf{y}_j\|_\infty \le 1000$.

Can cover the $\sqrt{n}B_2$ by $2^{n/10}$ cubes $500B_\infty$.

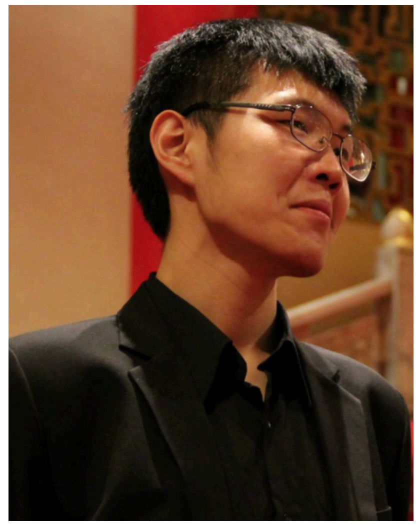


Technical detail: The specific property of the ℓ_∞ ball B_∞ that we used here is that $\sqrt{n}B_2$ *contains* B_∞ but can be covered by $2^{n/10}$ copies of $500B_\infty$.

[EV20] show a similar algorithm for *CVP* in *any* ℓ_p norm!

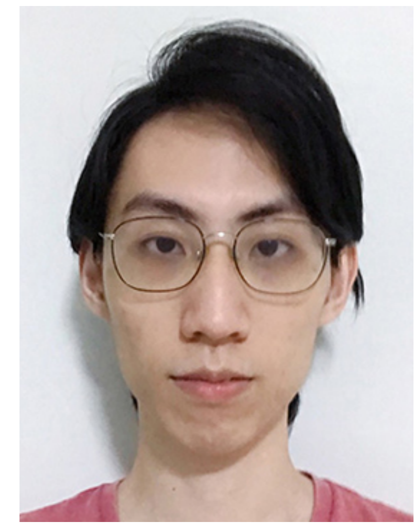
[ACKLS '21]

Divesh Aggarwal



Yanlin Chen

Rajendra Kumar



Zeyong Li

NSD

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

Divesh Aggarwal
CQT, National University of Singapore
dcsdiva@nus.edu.sg

Yanlin Chen
Centrum Wiskunde & Informatica
yanlin@cwi.nl

Rajendra Kumar
Indian Institute of Technology, Kanpur
and National University of Singapore
rjndr2503@gmail.com

Zeyong Li
CQT, National University of Singapore
li.zeyong@u.nus.edu

Noah Stephens-Davidowitz
Cornell University
noahsd@gmail.com

[ACKLS '21]

[ACKLS '21]

Any γ-SVP/CVP algorithm can be converted into an algorithm that samples "random lattice points" with bounded norm/distance. (Key word: sparsification.)

[ACKLS '21]

Any γ-SVP/CVP algorithm can be converted into an algorithm that samples "random lattice points" with bounded norm/distance. (Key word: sparsification.)

For any $q \geq p$, a $2^{\varepsilon n}$-time dimension- and rank-preserving reduction from

[ACKLS '21]

Any γ-SVP/CVP algorithm can be converted into an algorithm that samples "random lattice points" with bounded norm/distance. (Key word: sparsification.)

For any $q \geq p$, a $2^{\varepsilon n}$-time dimension- and rank-preserving reduction from

1. $O_\varepsilon(\gamma)$-SVP_q to γ-SVP_p.

[ACKLS '21]

Any γ-SVP/CVP algorithm can be converted into an algorithm that samples "random lattice points" with bounded norm/distance. (Key word: sparsification.)

For any $q \geq p$, a $2^{\varepsilon n}$-time dimension- and rank-preserving reduction from

1. $O_\varepsilon(\gamma)$-SVP$_q$ to γ-SVP$_p$.
2. $O_\varepsilon(\gamma)$-CVP$_p$ to γ-CVP$_q$.

[ACKLS '21]

Any γ-SVP/CVP algorithm can be converted into an algorithm that samples "random lattice points" with bounded norm/distance. (Key word: sparsification.)

For any $q \geq p$, a $2^{\varepsilon n}$-time dimension- and rank-preserving reduction from

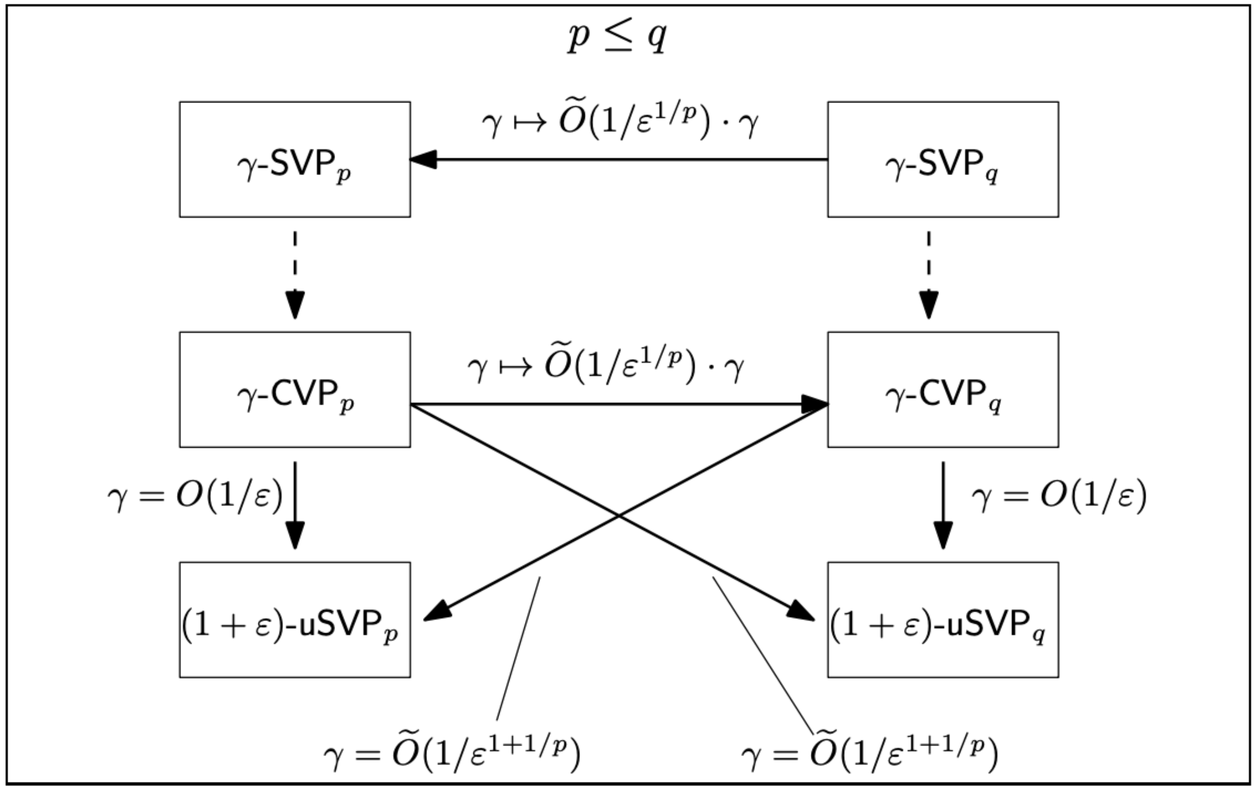
1. $O_\varepsilon(\gamma)$-SVP_q to γ-SVP_p.
2. $O_\varepsilon(\gamma)$-CVP_p to γ-CVP_q.
3. $O_\varepsilon(1)$-CVP_q to $(1+\varepsilon)$-SVP_p.

[ACKLS '21]

Any γ-SVP/CVP algorithm can be converted into an algorithm that samples "random lattice points" with bounded norm/distance. (Key word: sparsification.)

For any $q \geq p$, a $2^{\varepsilon n}$-time dimension- and rank-preserving reduction from

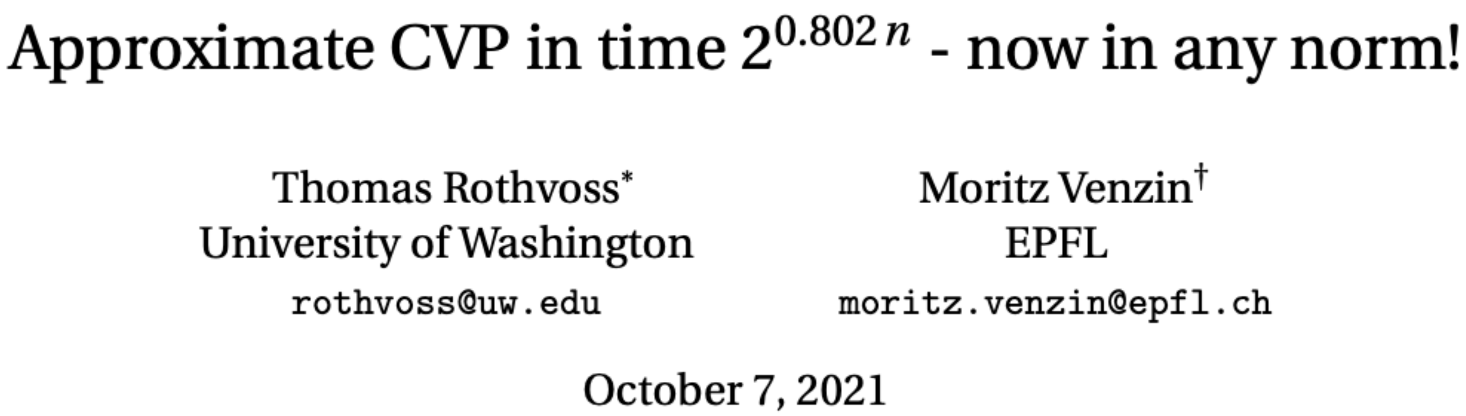
1. $O_\varepsilon(\gamma)$-SVP$_q$ to γ-SVP$_p$.
2. $O_\varepsilon(\gamma)$-CVP$_p$ to γ-CVP$_q$.
3. $O_\varepsilon(1)$-CVP$_q$ to $(1+\varepsilon)$-SVP$_p$.



Rothvoss and Venzin

Thomas Rothvoss

Moritz Venzin



Rothvoss and Venzin

Theorem. *There is a* $2^{\varepsilon n}$*-time dimension-preserving reduction from* $O_\varepsilon(\gamma)$*-approximate* SVP_K *to* γ-CVP_2 *for any norm* K*.*

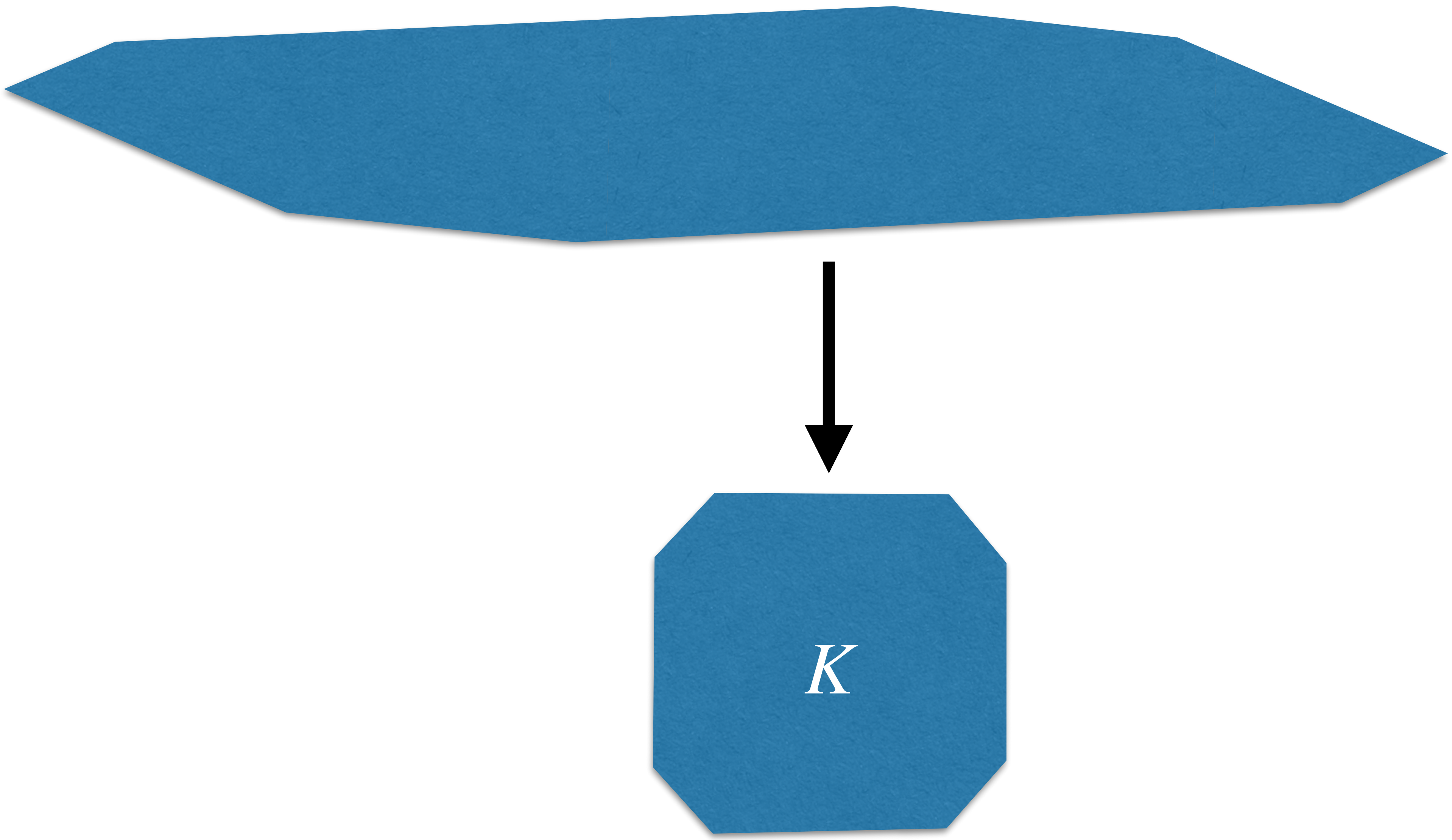
Rothvoss and Venzin

Theorem. *There is a* $2^{\varepsilon n}$*-time dimension-preserving reduction from* $O_\varepsilon(\gamma)$*-approximate* SVP_K *to* γ-CVP_2 *for any norm* K*.*

Theorem. *There is a* $2^{0.802n+o(n)}$*-time algorithm for* $O(1)$-CVP_K *for any* K*.*

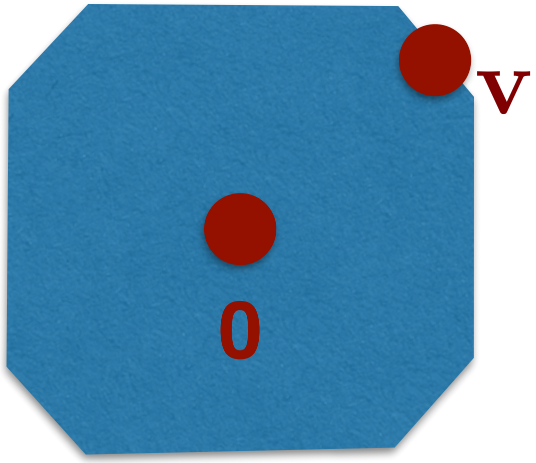
Rothvoss and Venzin

Step 0: Apply a linear transformation to K so that it "looks roughly like the scaled ℓ_2 ball $B_2/20$."



Rothvoss and Venzin

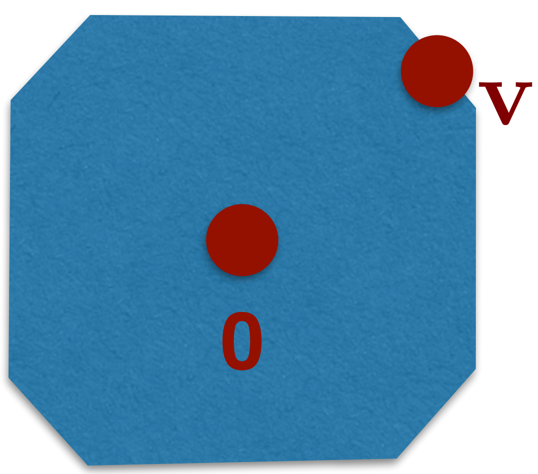
Rothvoss and Venzin



Rothvoss and Venzin

Step 1: Sample $\mathbf{t} \sim K + B_2$.

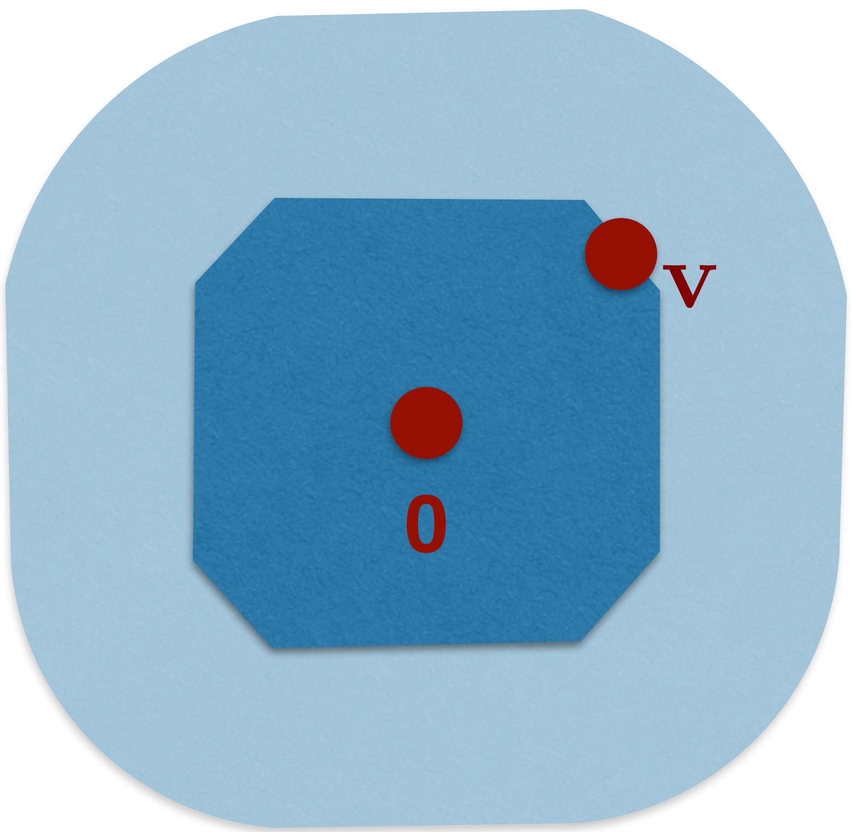
Pray that $\|\mathbf{t} - \mathbf{v}\|_2 \leq 1$ for a K-shortest non-zero vector.



Rothvoss and Venzin

Step 1: Sample $\mathbf{t} \sim K + B_2$.

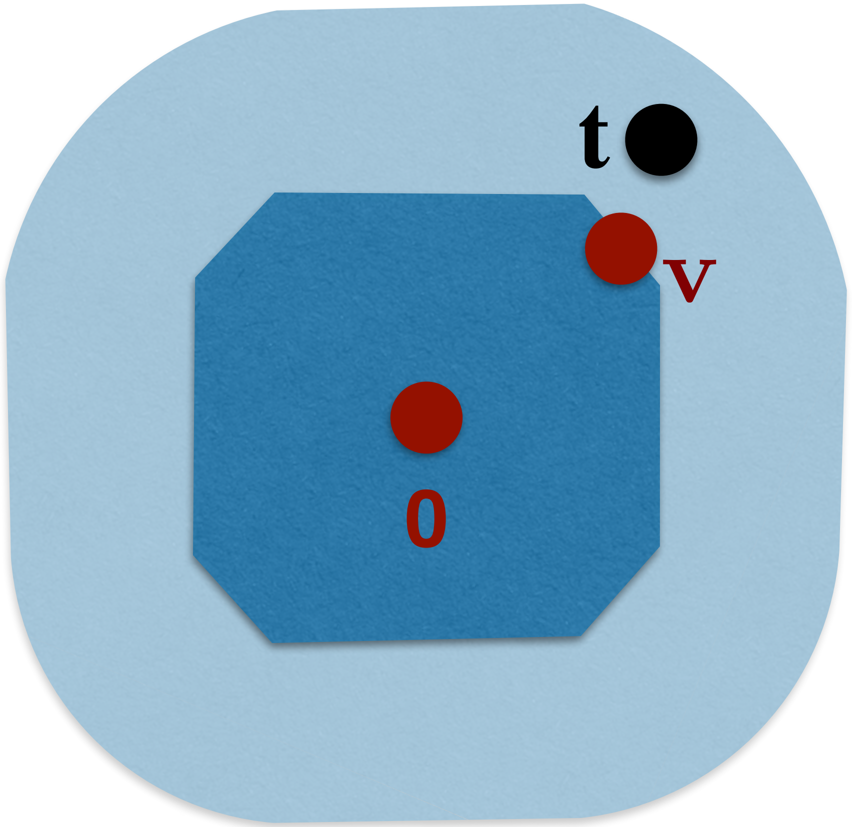
Pray that $\|\mathbf{t} - \mathbf{v}\|_2 \leq 1$ for a K-shortest non-zero vector.



Rothvoss and Venzin

Step 1: Sample $\mathbf{t} \sim K + B_2$.

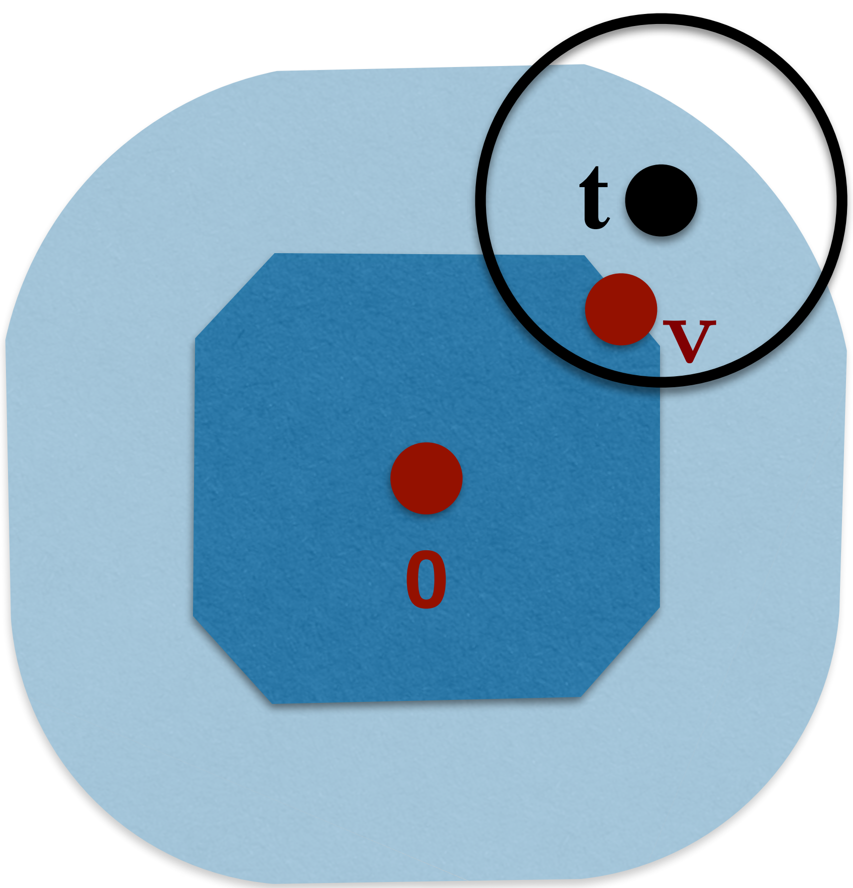
Pray that $\|\mathbf{t} - \mathbf{v}\|_2 \le 1$ for a K-shortest non-zero vector.



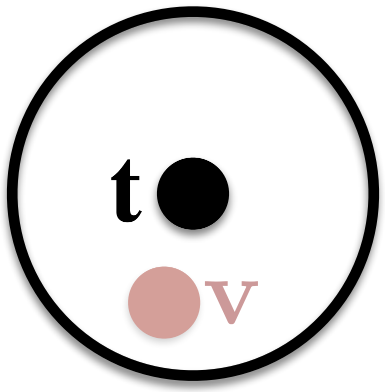
Rothvoss and Venzin

Step 1: Sample $\mathbf{t} \sim K + B_2$.

Pray that $\|\mathbf{t} - \mathbf{v}\|_2 \leq 1$ for a K-shortest non-zero vector.

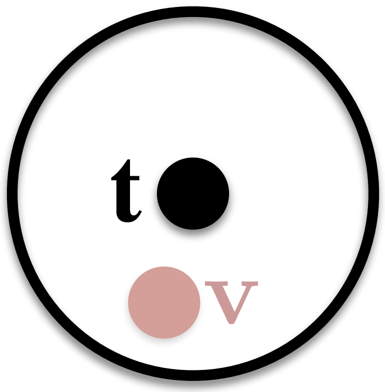


Rothvoss and Venzin



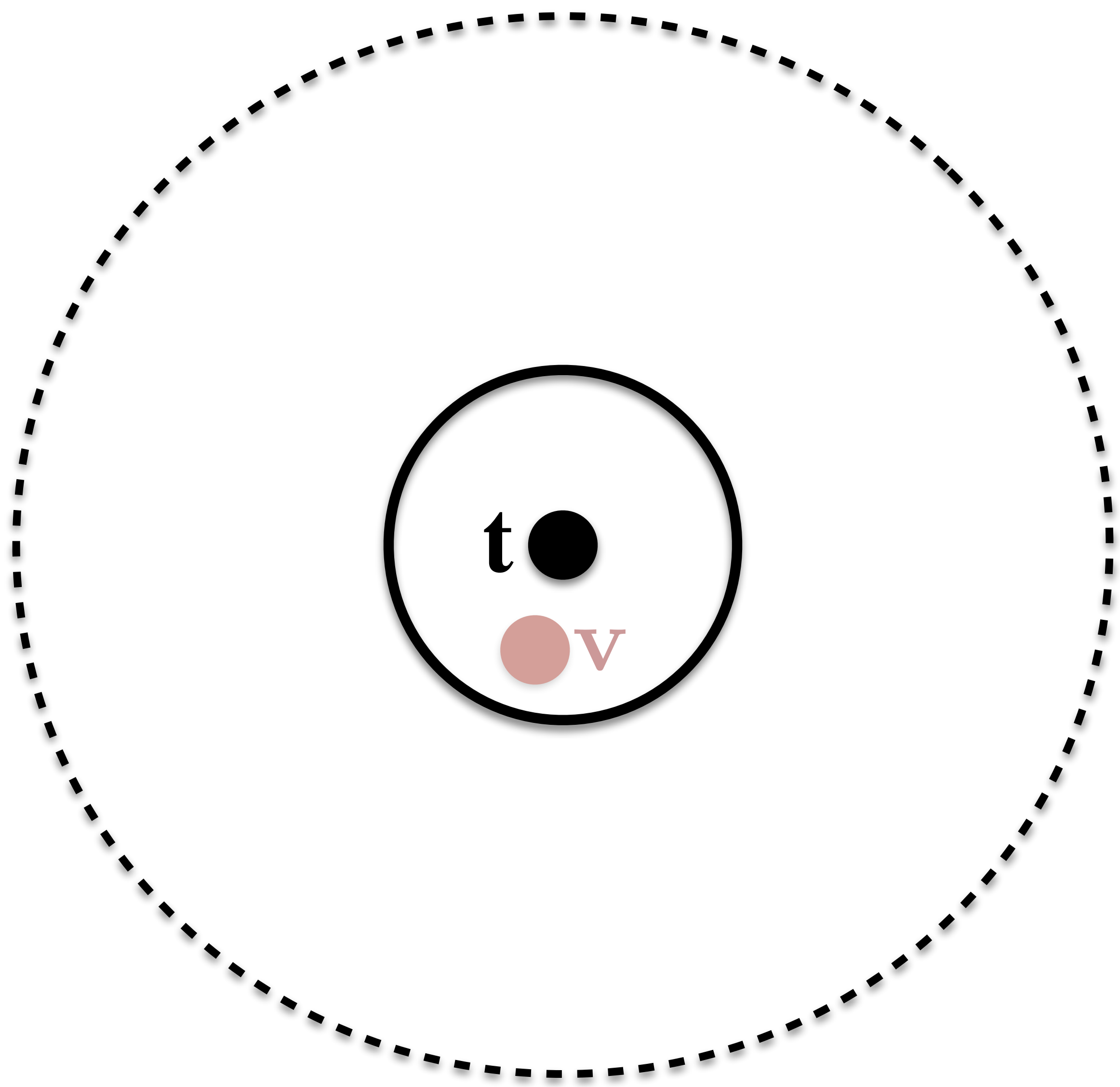
Rothvoss and Venzin

Step 2: Given $\mathbf{t} \in \mathbb{R}^n$ with $\|\mathbf{t} - \mathbf{v}\|_2 \leq 1$ for a K-shortest non-zero vector $\mathbf{v}$, use γ-CVP$_2$ oracle to find many "random" samples from $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathcal{L} \cap (\gamma B_2 + \mathbf{t})$.



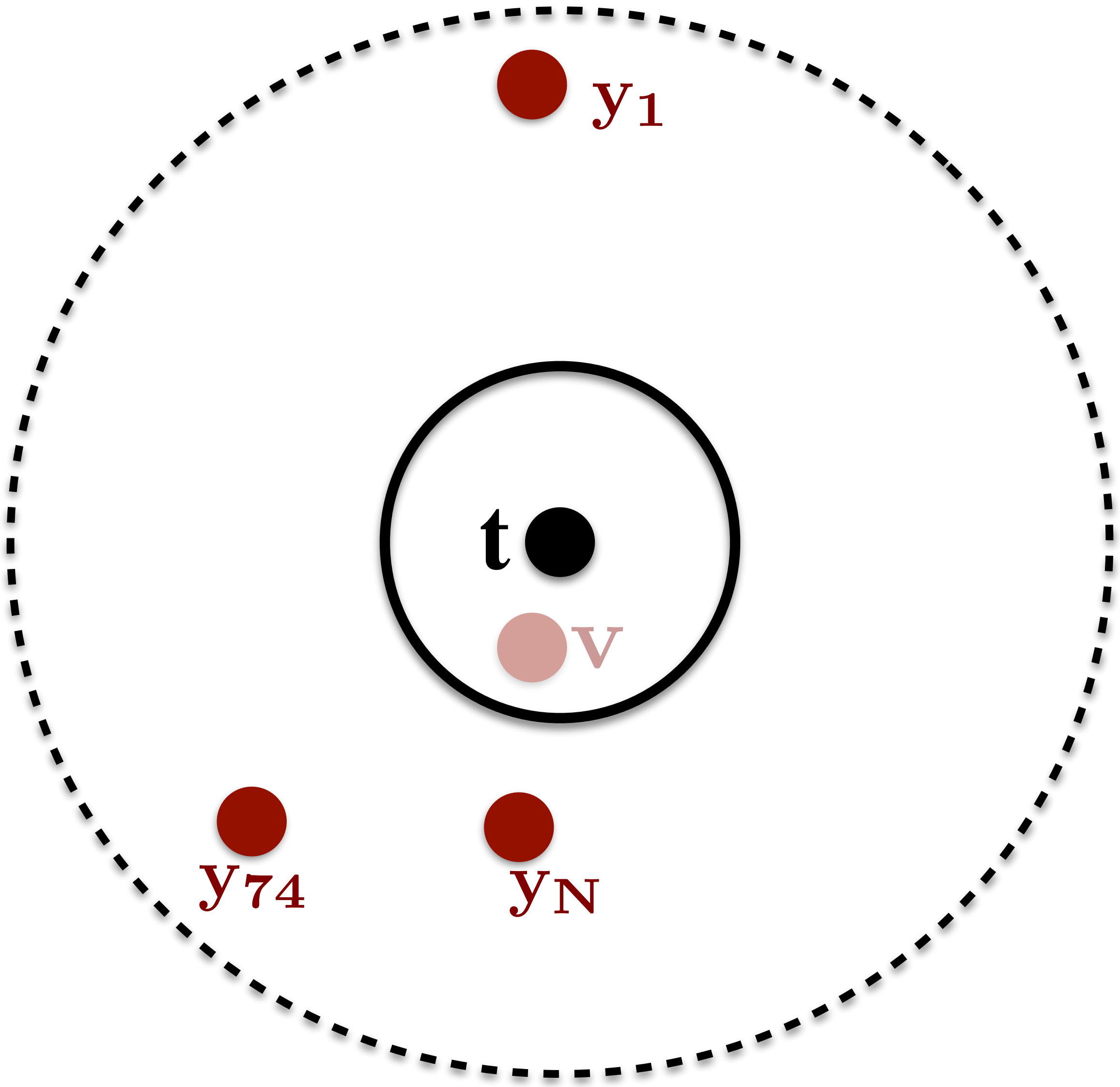
Rothvoss and Venzin

Step 2: Given $\mathbf{t} \in \mathbb{R}^n$ with $\|\mathbf{t} - \mathbf{v}\|_2 \leq 1$ for a K-shortest non-zero vector $\mathbf{v}$, use γ-CVP$_2$ oracle to find many "random" samples from $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathcal{L} \cap (\gamma B_2 + \mathbf{t})$.

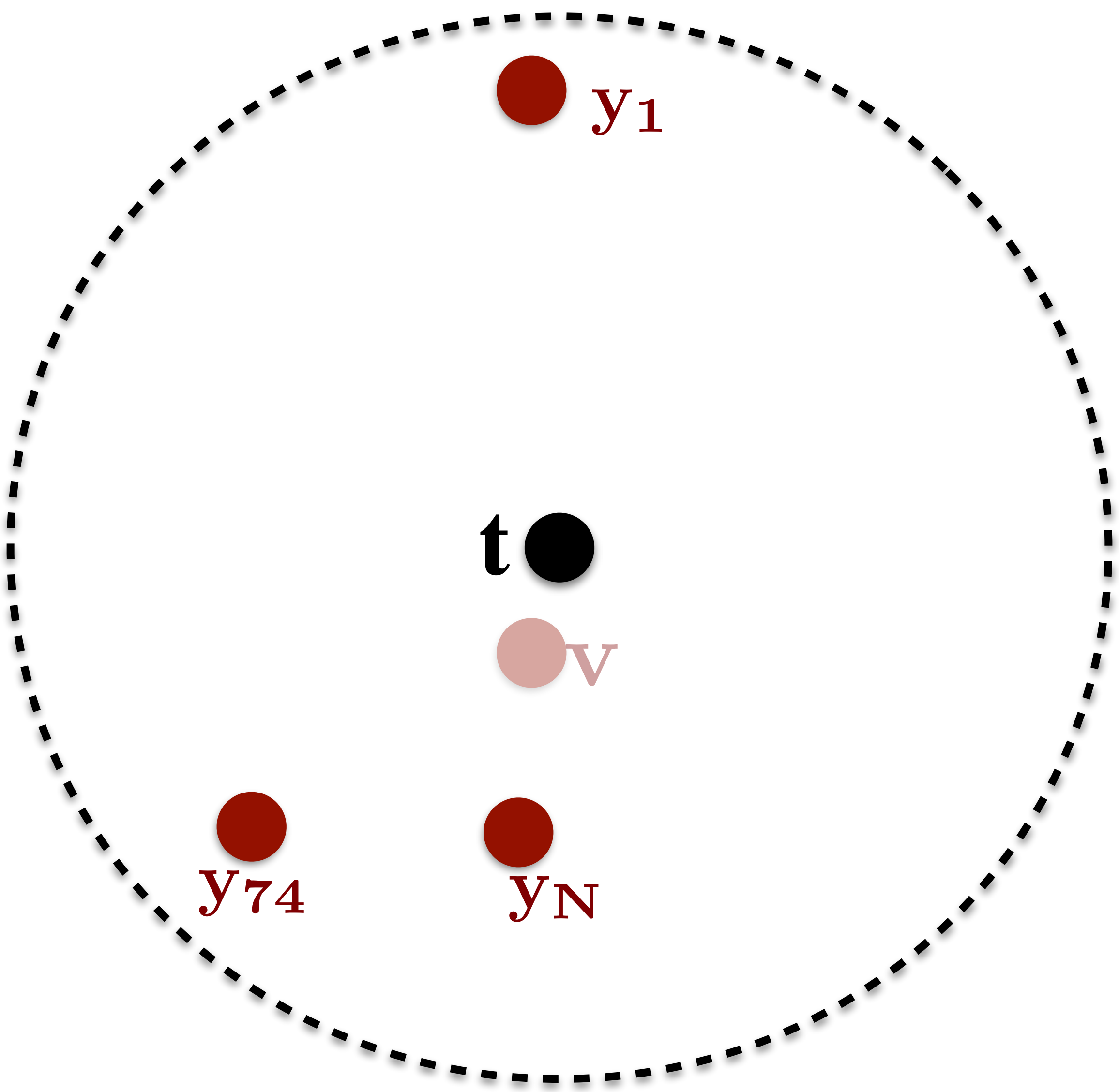


Rothvoss and Venzin

Step 2: Given $\mathbf{t} \in \mathbb{R}^n$ with $\|\mathbf{t} - \mathbf{v}\|_2 \leq 1$ for a K-shortest non-zero vector $\mathbf{v}$, use γ-CVP$_2$ oracle to find many "random" samples from $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathcal{L} \cap (\gamma B_2 + \mathbf{t})$.

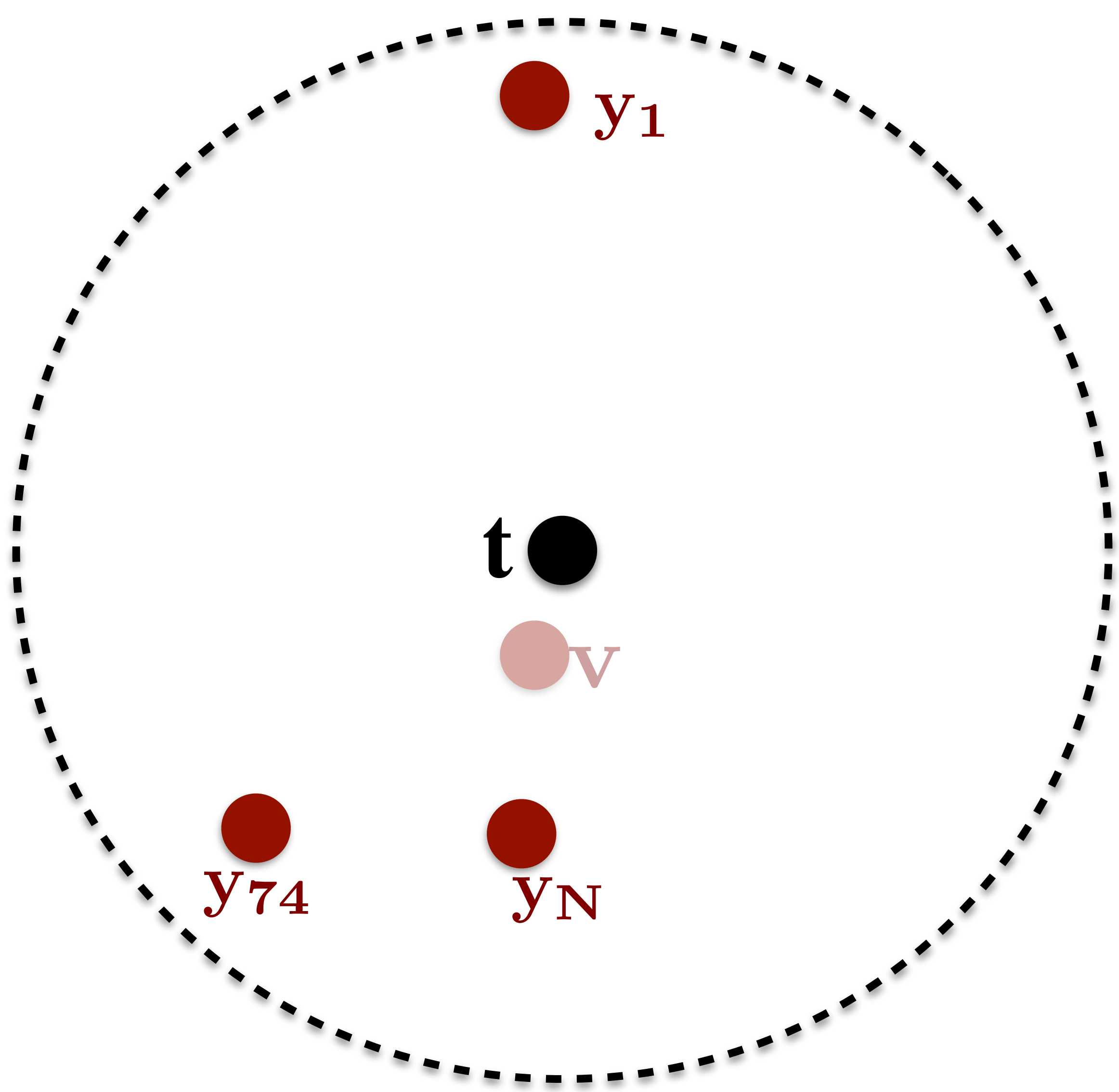


Rothvoss and Venzin



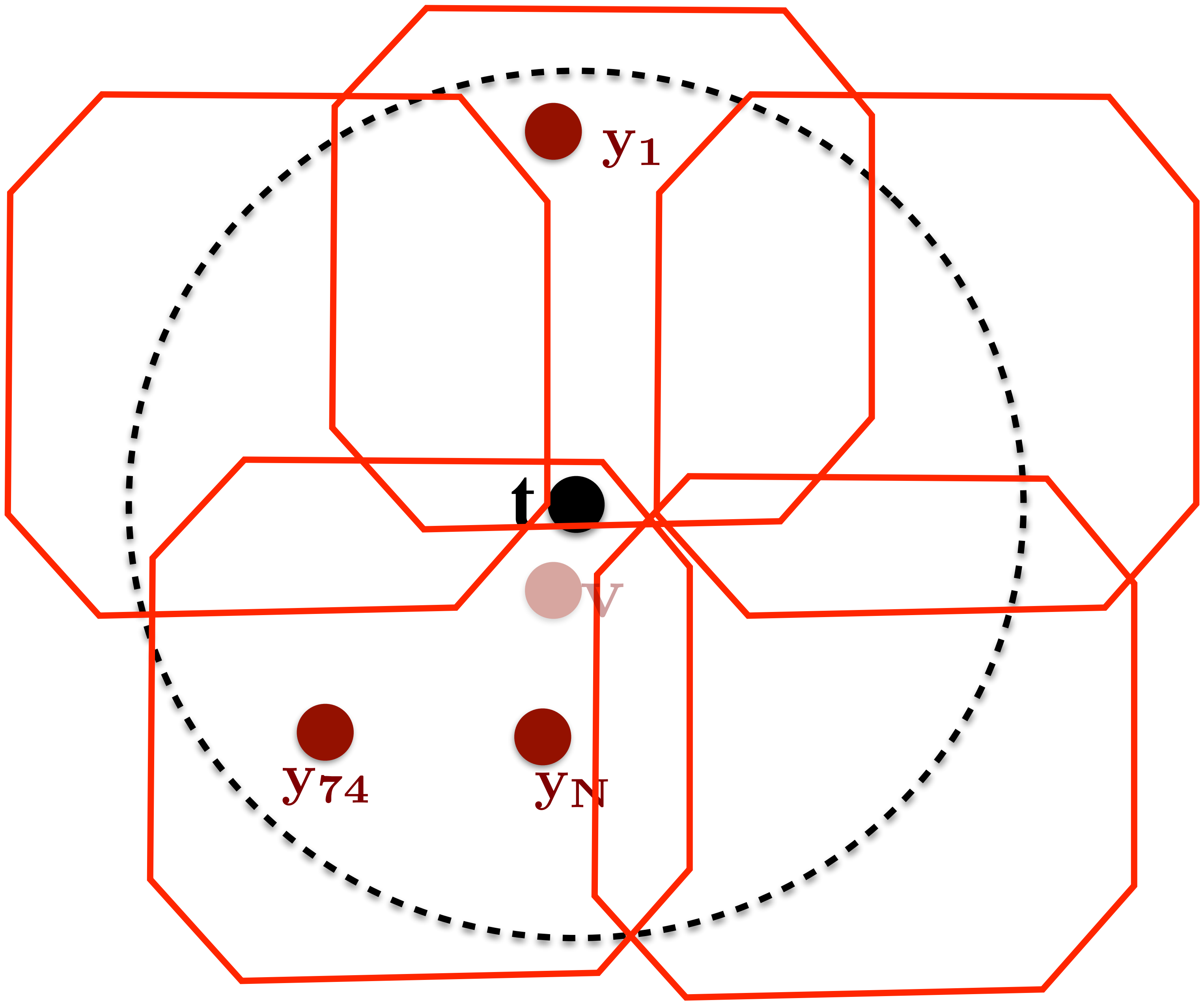
Rothvoss and Venzin

Step 3: Given a bunch of “random” lattice vectors $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathcal{L} \cap (\gamma B_2 + \mathbf{t})$, output non-zero $\mathbf{y_i} - \mathbf{y_j}$ minimizing $\|\mathbf{y_i} - \mathbf{y_j}\|_K$ (or output $\mathbf{y_i}$ itself).



Rothvoss and Venzin

Step 3: Given a bunch of "random" lattice vectors $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathcal{L} \cap (\gamma B_2 + \mathbf{t})$, output non-zero $\mathbf{y_i} - \mathbf{y_j}$ minimizing $\|\mathbf{y_i} - \mathbf{y_j}\|_K$ (or output $\mathbf{y_i}$ itself).



Rothvoss and Venzin

Step 1: Sample $\mathbf{t} \sim K + B_2$.
Pray that $\|\mathbf{t} - \mathbf{y}\|_2 < 1$ for a K-shortest non-zero vector.

Step 2: …

Step 3: Given a bunch of random lattice vectors within ℓ_2 distance γ of $\mathbf{t}$, output non-zero $\mathbf{y}_i - \mathbf{y}_j$ minimizing $\|\mathbf{y}_i - \mathbf{y}_j\|_K$ (or output $\mathbf{y}_i$ itself).

Rothvoss and Venzin

Step 1: Sample $\mathbf{t} \sim K + B_2$.
Pray that $\|\mathbf{t} - \mathbf{y}\|_2 < 1$ for a K-shortest non-zero vector.

Step 2: …

Step 3: Given a bunch of random lattice vectors within ℓ_2 distance γ of $\mathbf{t}$, output non-zero $\mathbf{y}_i - \mathbf{y}_j$ minimizing $\|\mathbf{y}_i - \mathbf{y}_j\|_K$ (or output $\mathbf{y}_i$ itself).

Need for step 1: $\mathrm{vol}(K + B_2) \leq 2^{n/10}\mathrm{vol}(B_2)$.

Rothvoss and Venzin

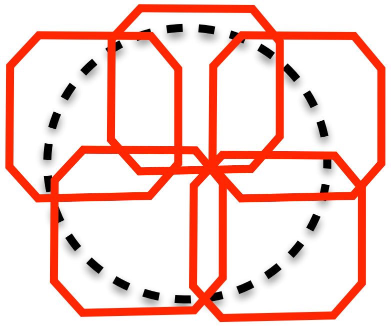
Step 1: Sample $\mathbf{t} \sim K + B_2$.
Pray that $\|\mathbf{t} - \mathbf{y}\|_2 < 1$ for a K-shortest non-zero vector.

Step 2: …

Step 3: Given a bunch of random lattice vectors within ℓ_2 distance γ of $\mathbf{t}$, output non-zero $\mathbf{y}_i - \mathbf{y}_j$ minimizing $\|\mathbf{y}_i - \mathbf{y}_j\|_K$ (or output $\mathbf{y}_i$ itself).

Need for step 1: $\mathrm{vol}(K + B_2) \leq 2^{n/10}\mathrm{vol}(B_2)$.

Need for step 3: B_2 can be covered by $2^{n/10}$ copies of $1000K$.



Rothvoss and Venzin

Step 1: Sample $\mathbf{t} \sim K + B_2$.
Pray that $\|\mathbf{t} - \mathbf{y}\|_K \le 1$ for a K shortest non-zero
ve

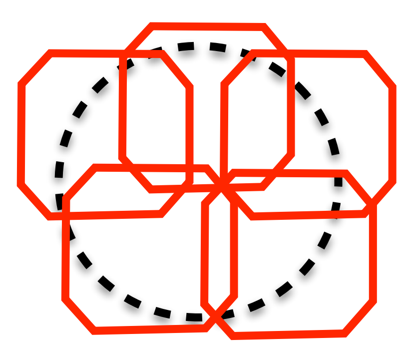
If $K \approx B_2/20$, this works.

Step 2: …

Step 3: Given a bunch of random lattice vectors within ℓ_2 distance γ of $\mathbf{t}$, output non-zero $\mathbf{y}_i - \mathbf{y}_j$ minimizing $\|\mathbf{y}_i - \mathbf{y}_j\|_K$ (or output $\mathbf{y}_i$ itself).

Need for step 1: $\mathrm{vol}(K + B_2) \le 2^{n/10}\mathrm{vol}(B_2)$.

Need for step 3: B_2 can be covered by $2^{n/10}$ copies of $1000K$.



Rothvoss and Venzin

Step 1: Sample $\mathbf{t} \sim K + B_2$.
Pray that $\|\mathbf{t} - \mathbf{y}\| \leq 1$ for a K shortest non-zero
ve

If $K \approx B_2/20$, this works.

Step 2: …

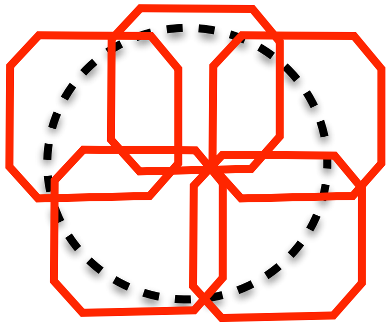
Step 3: Given a bunch of random lattice vectors

Rothvoss and Venzin show how to find a linear transformation of any convex body so that the transformed body has these properties.

(Closely related to M-position. M = Milman)

Need for step 1: $\mathrm{vol}(K + B_2) \leq 2^{n/10}\mathrm{vol}(B_2)$.

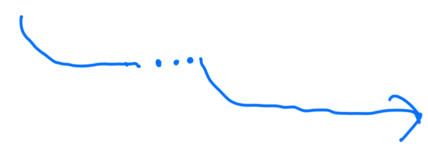
Need for step 3: B_2 can be covered by $2^{n/10}$ copies of $1000K$.



Summary

- The fastest algorithms for $O(1)$-CVP$_K$/$O(1)$-SVP$_K$ for any norm is $2^{0.802n}$!!
- We can reduce $O_\varepsilon(\gamma)$-SVP$_K$ to γ-CVP$_2$ in $2^{\varepsilon n}$ time for any K!!
- “Morally, lattice problems in any norm are equivalent up to a constant in the approximation factor!!”

Open Questions?

- ■ 1. Is there a dimension-preserving reduction from $O_\varepsilon(\gamma)$-SVP$_K$ in *any* norm to γ-SVP$_2$ in $2^{\varepsilon n}$ time? (Currently have to reduce to γ-CVP$_2$ or from γ-SVP$_p$ for $p \geq 2$.)
- ■ 2. What is the best running time for γ-SVP$_\infty$ for small constant γ?!!
  - What's going on with that wiggle? 
- ■ 3. More generally, what about γ-SVP$_K$??!
- ♦ 4. Is there a norm K for which sieving algorithms work particularly well…

● Easy

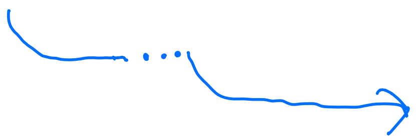
■ Medium

♦ Hard

Open Questions?

- 1. Is there a dimension-preserving reduction from $O_\varepsilon(\gamma)$-SVP$_K$ in *any* norm to γ-SVP$_2$ in $2^{\varepsilon n}$ time? (Currently have to reduce to γ-CVP$_2$ or from γ-SVP$_p$ for $p \geq 2$.)

- 2. What is the best running time for γ-SVP$_\infty$ for small constant γ?!!
  - What's going on with that wiggle?



- 3. More generally, what about γ-SVP$_K$??!

♦ 4. Is there a norm K for which sieving algorithms work particularly well…

● Easy

Thanks!

♦ Hard