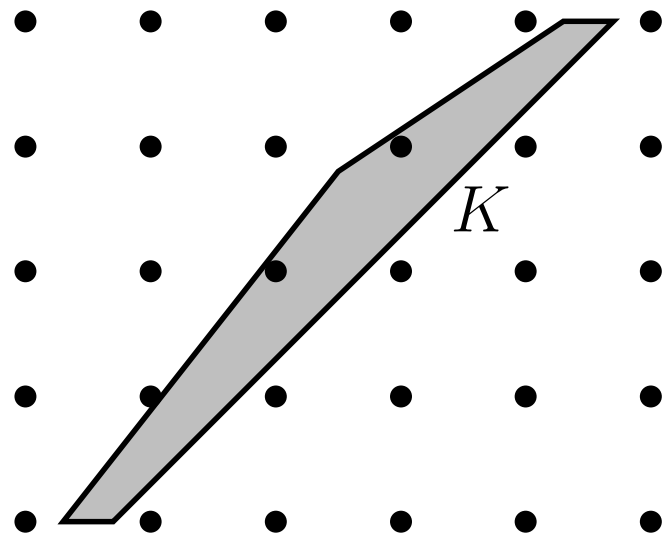
Part 1:
Introduction to Lattices

Thomas Rothvoss

Based the work
[Micciancio, Voulgaris 2010],
[Dadush, Peikert, Vempala 2011],
[Dadush, Vempala 2012], [Dadush 2012]

UNIVERSITY *of*
WASHINGTON

The main goal



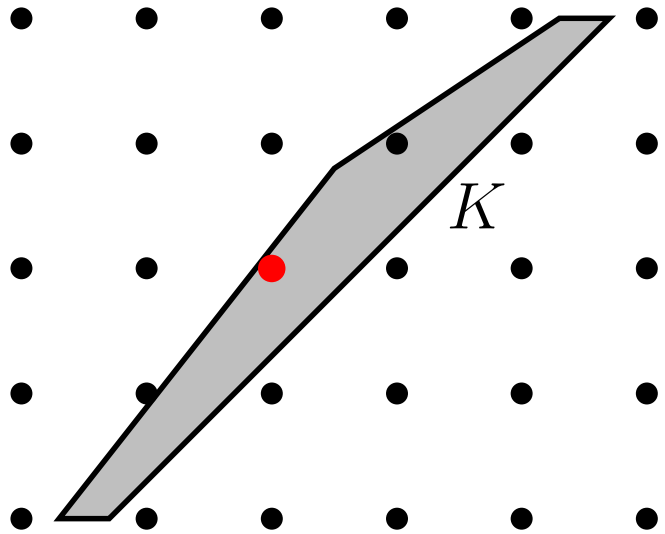
Theorem (Reis, R.'23)

For convex body $K \subseteq \mathbb{R}^n$ one can find a point in $K \cap \mathbb{Z}^n$ in time $(\log n)^{O(n)}$.

Previously best known:

- $2^{O(n^2)}$ [Lenstra '83]
- $n^{O(n)}$ [Kannan '87]
- $2^{O(n)}n^n$ [Dadush '12], [Dadush, Eisenbrand, R. '22]

The main goal



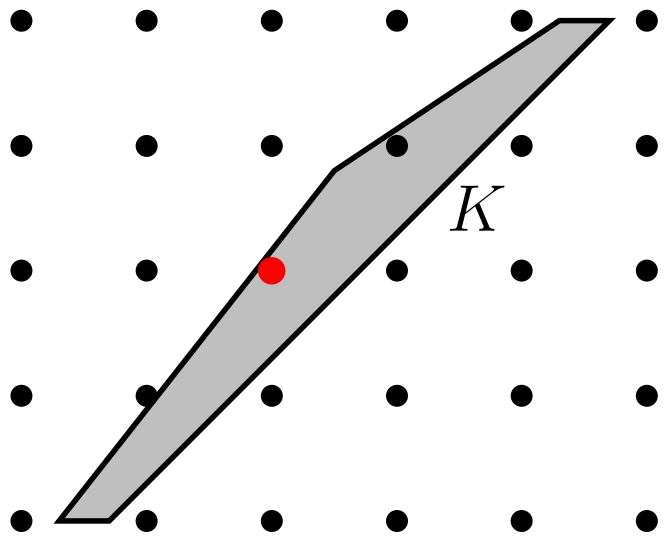
Theorem (Reis, R.'23)

For convex body $K \subseteq \mathbb{R}^n$ one can find a point in $K \cap \mathbb{Z}^n$ in time $(\log n)^{O(n)}$.

Previously best known:

- $2^{O(n^2)}$ [Lenstra '83]
- $n^{O(n)}$ [Kannan '87]
- $2^{O(n)}n^n$ [Dadush '12], [Dadush, Eisenbrand, R. '22]

The main goal



Theorem (Reis, R.'23)

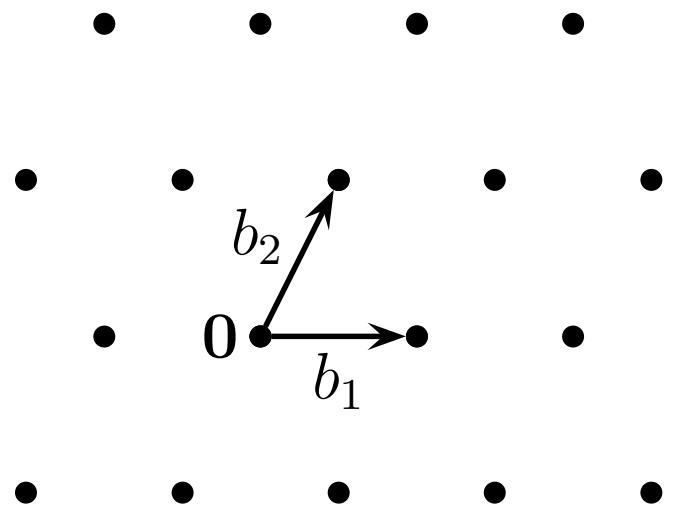
For convex body $K \subseteq \mathbb{R}^n$ one can find a point in $K \cap \mathbb{Z}^n$ in time $(\log n)^{O(n)}$.

Theorem (Reis, R.'23)

One can solve an integer program $\max\{c^T x \mid Ax \leq b, x \in \mathbb{Z}^n\}$ in time $(\log n)^{O(n)}$.

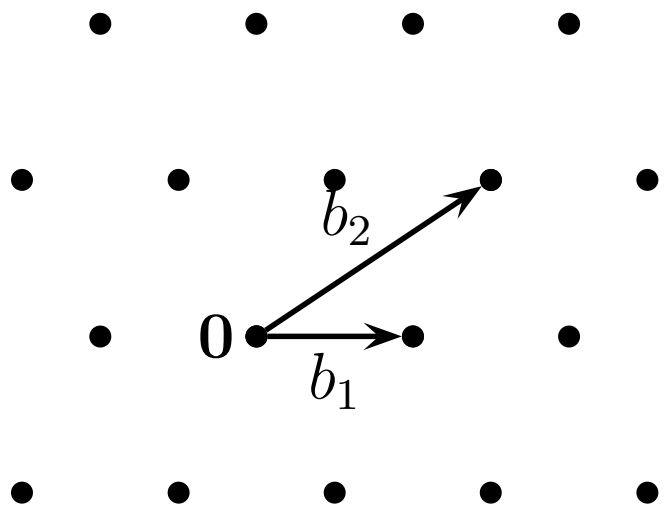
Lattices

- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.
- $B = (b_1, \ldots, b_k)$ is called **basis** of the lattice.



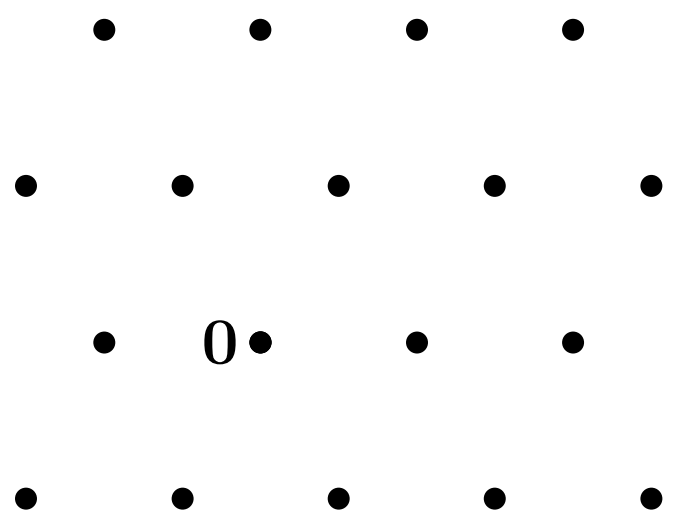
Lattices

- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.
- $B = (b_1, \ldots, b_k)$ is called **basis** of the lattice.



Lattices

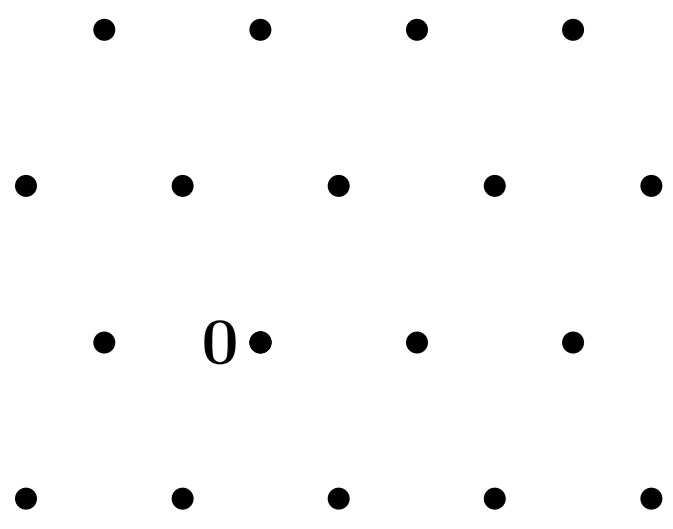
- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.
- $B = (b_1, \ldots, b_k)$ is called **basis** of the lattice.



- The **rank** of Λ is $\dim(\text{span}(\Lambda))$

Lattices

- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.
- $B = (b_1, \ldots, b_k)$ is called **basis** of the lattice.

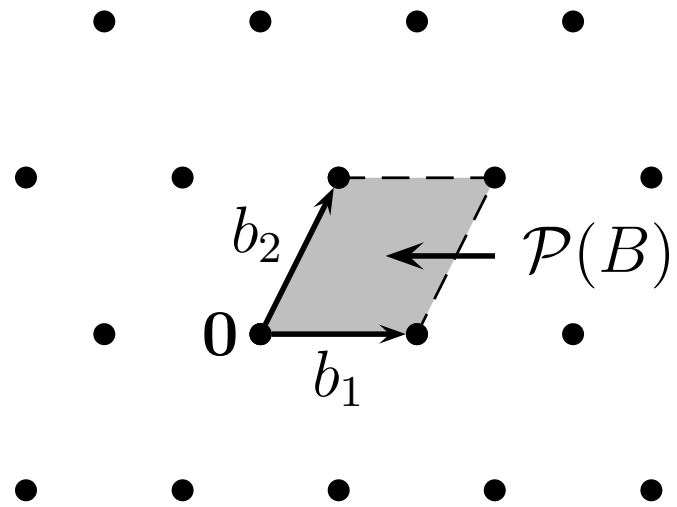


- The **rank** of Λ is $\dim(\text{span}(\Lambda))$
- A lattice has **full rank**, if $n = \text{rank}(\Lambda)$.

Determinants

- The **fundamental parallelepiped** of Λ is the polytope

$$\mathcal{P}(B) := \left\{ \sum_{i=1}^{k} \lambda_i b_i \mid 0 \leq \lambda_i < 1 \; \forall i \in [k] \right\}$$

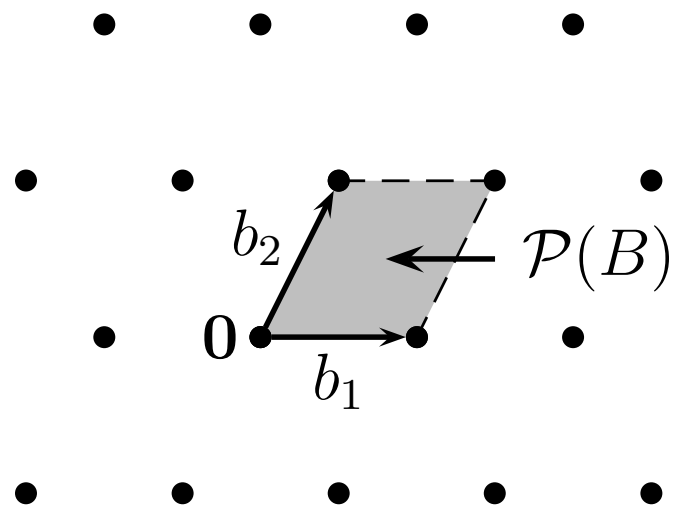


Determinants

- The **fundamental parallelepiped** of Λ is the polytope

$$\mathcal{P}(B) := \left\{ \sum_{i=1}^{k} \lambda_i b_i \mid 0 \leq \lambda_i < 1 \; \forall i \in [k] \right\}$$

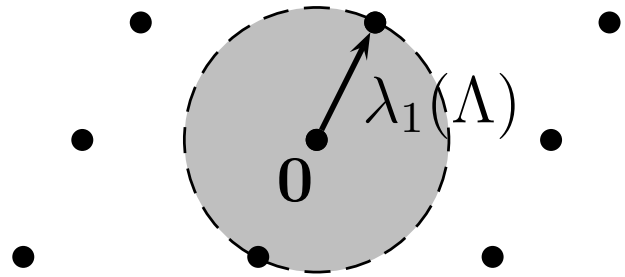
- The **determinant** of lattice is $\det(\Lambda) := \mathrm{Vol}_k(\mathcal{P}(B))$
  In full rank case, $\det(\Lambda) = |\det(B)|$



Shortest vectors

- Length of the **shortest vector** is

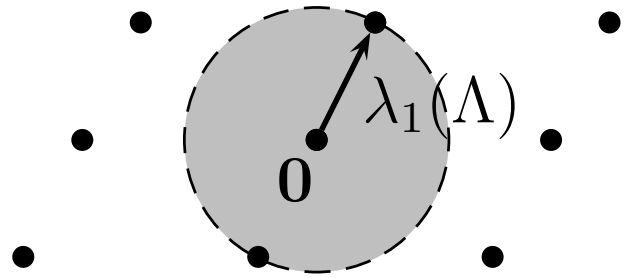
$$\lambda_1(\Lambda) := \min\{\|x\|_2 \mid x \in \Lambda \setminus \{\mathbf{0}\}\}$$



Shortest vectors

- Length of the **shortest vector** is

$$\lambda_1(\Lambda) := \min\{\|x\|_2 \mid x \in \Lambda \setminus \{\mathbf{0}\}\}$$

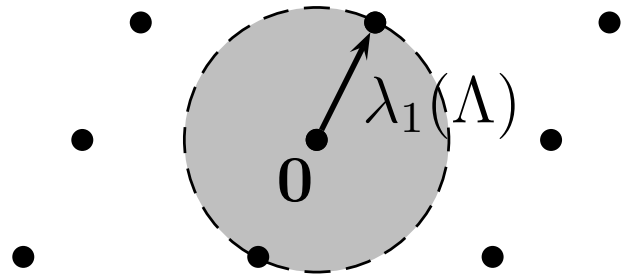


- Finding shortest vector is **NP**-hard (under randomized reductions)
- Can be approximated within 2^n-factor [LLL'82]
- Can be computed in time $2^{O(n)}$ (even w.r.t. arbitrary norms $\|\cdot\|_K$) [Ajtai, Kumar, Sivakumar '01]

Shortest vectors

- Length of the **shortest vector** is

$$\lambda_1(\Lambda) := \min\{\|x\|_2 \mid x \in \Lambda \setminus \{\mathbf{0}\}\}$$



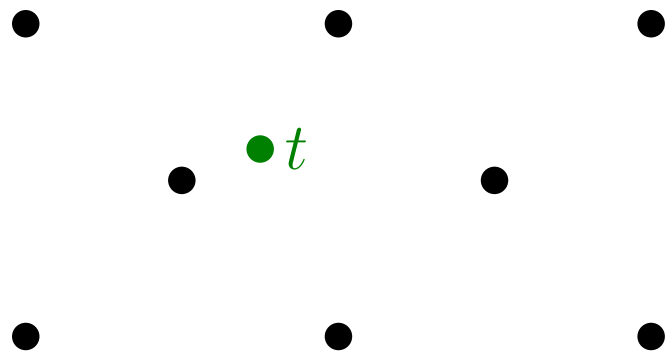
- Finding shortest vector is **NP**-hard (under randomized reductions)
- Can be approximated within 2^n-factor [LLL'82]
- Can be computed in time $2^{O(n)}$ (even w.r.t. arbitrary norms $\|\cdot\|_K$) [Ajtai, Kumar, Sivakumar '01]

Theorem (Minkowski's Theorem 1889)

Any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\lambda_1(\Lambda) \leq \sqrt{n} \cdot \det(\Lambda)^{1/n}$.

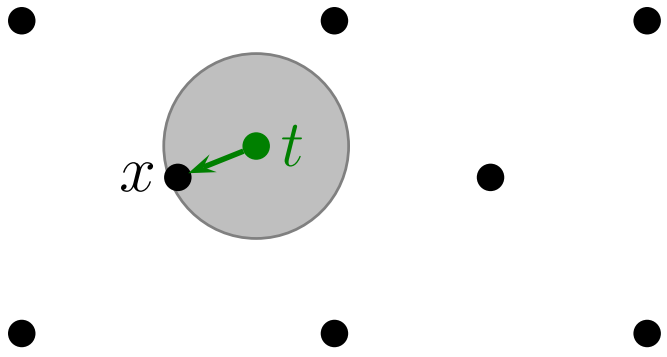
Closest Vector

Closest Vector Problem (CVP): Given lattice Λ and target vector $t \in \mathbb{R}^n$. Find vector attaining $\min\{\|x - t\|_2 : x \in \Lambda\}$.



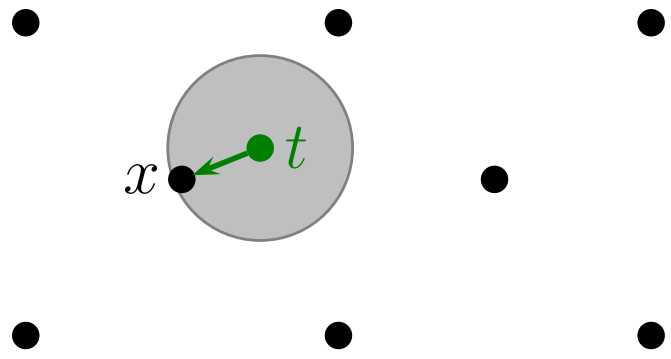
Closest Vector

Closest Vector Problem (CVP): Given lattice Λ and target vector $t \in \mathbb{R}^n$. Find vector attaining $\min\{\|x - t\|_2 : x \in \Lambda\}$.



Closest Vector

Closest Vector Problem (CVP): Given lattice Λ and target vector $t \in \mathbb{R}^n$. Find vector attaining $\min\{\|x - t\|_2 : x \in \Lambda\}$.



Theorem (Micciancio, Voulgaris '10)

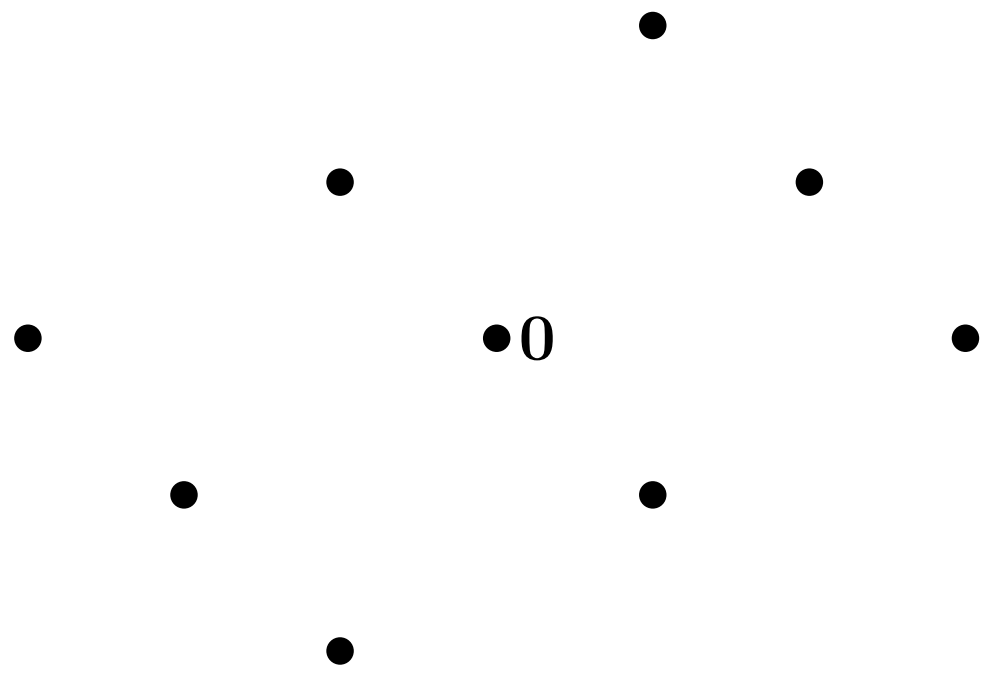
CVP can be solved (deterministically) in time $2^{O(n)}$.

- Only works for $\|\cdot\|_2$

The Voronoi cell

Let $\Lambda \subseteq \mathbb{R}^n$ be full rank lattice. The **Voronoi cell** is

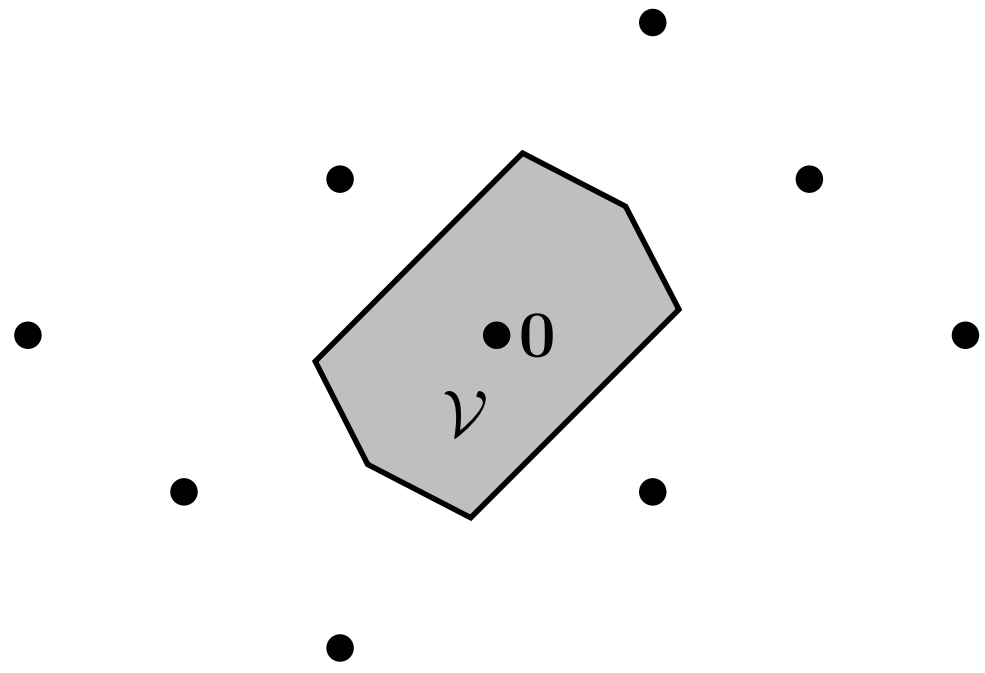
$$\mathcal{V} = \{x \in \mathbb{R}^n : \|x\|_2 \leq \|x - v\|_2 \; \forall v \in \Lambda \setminus \{\mathbf{0}\}\}$$



The Voronoi cell

Let $\Lambda \subseteq \mathbb{R}^n$ be full rank lattice. The **Voronoi cell** is

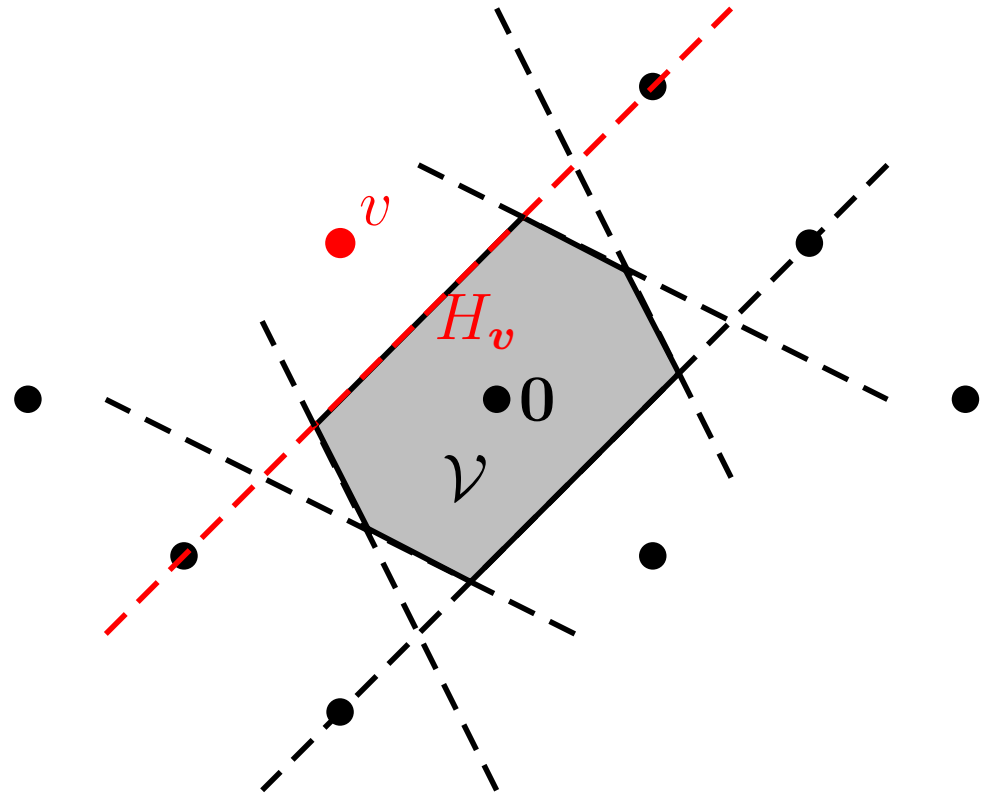
$$\mathcal{V} = \{x \in \mathbb{R}^n : \|x\|_2 \leq \|x - v\|_2 \; \forall v \in \Lambda \setminus \{\mathbf{0}\}\}$$



The Voronoi cell

Let $\Lambda \subseteq \mathbb{R}^n$ be full rank lattice. The **Voronoi cell** is

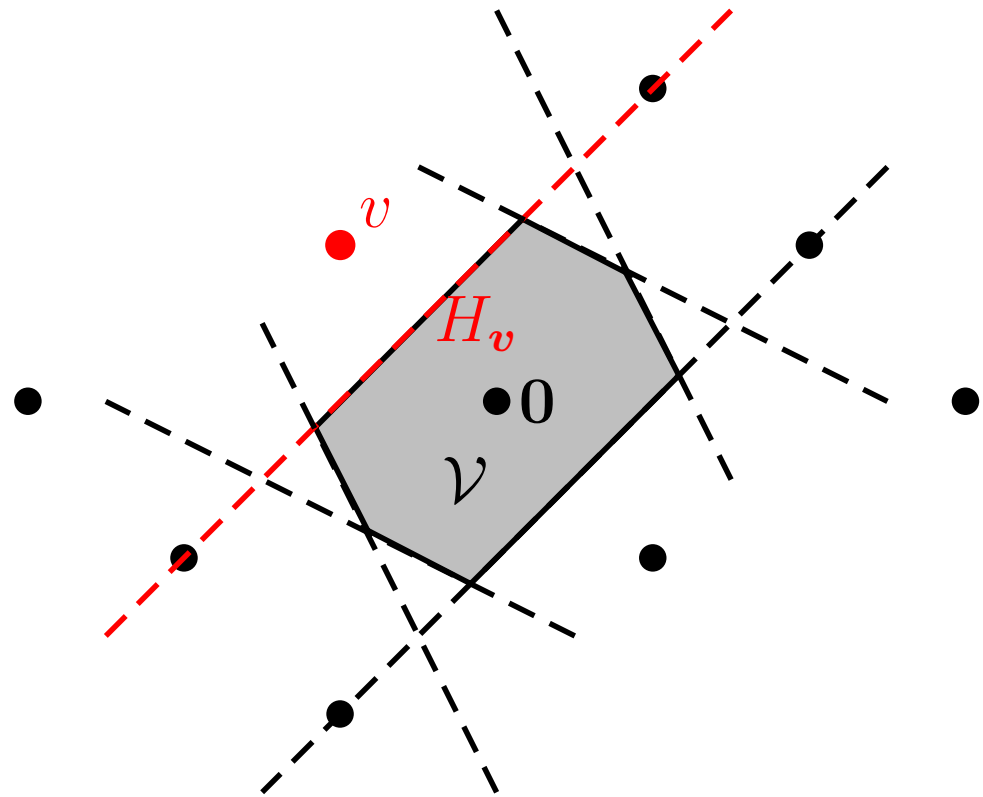
$$\mathcal{V} = \{x \in \mathbb{R}^n : \|x\|_2 \leq \|x - v\|_2 \; \forall v \in \Lambda \setminus \{\mathbf{0}\}\}$$



The Voronoi cell

Let $\Lambda \subseteq \mathbb{R}^n$ be full rank lattice. The **Voronoi cell** is

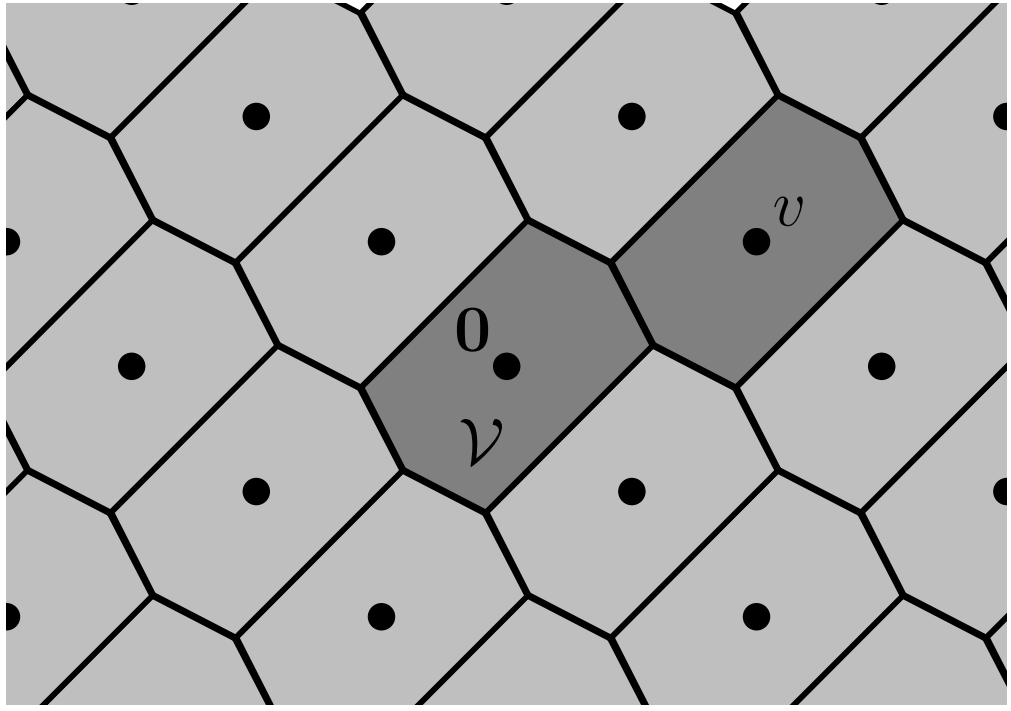
$$\mathcal{V} = \{x \in \mathbb{R}^n : \|x\|_2 \leq \|x - v\|_2 \; \forall v \in \Lambda \setminus \{\mathbf{0}\}\}$$



- $\mathcal{V}$ is a symmetric, convex, compact set
- $t \in \mathcal{V} \Leftrightarrow \min\{\|x - t\|_2 : x \in \Lambda\}$ attained by $\mathbf{0}$

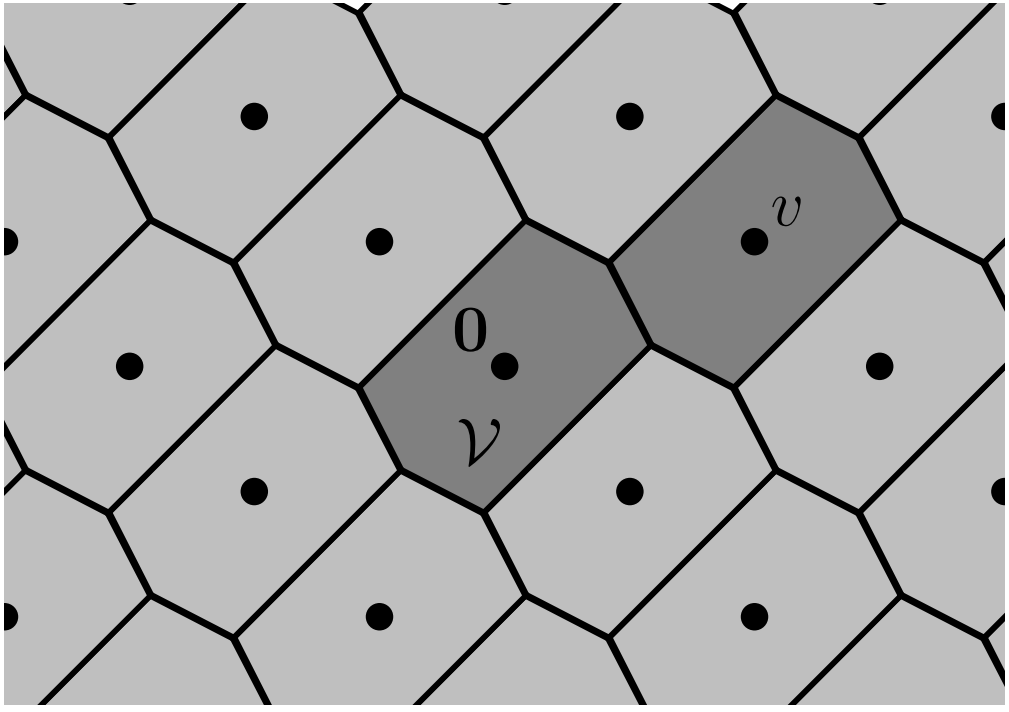
The Voronoi relevant vectors

- $v \in \Lambda$ is called **Voronoi relevant** if H_v is a facet of $\mathcal{V}$.



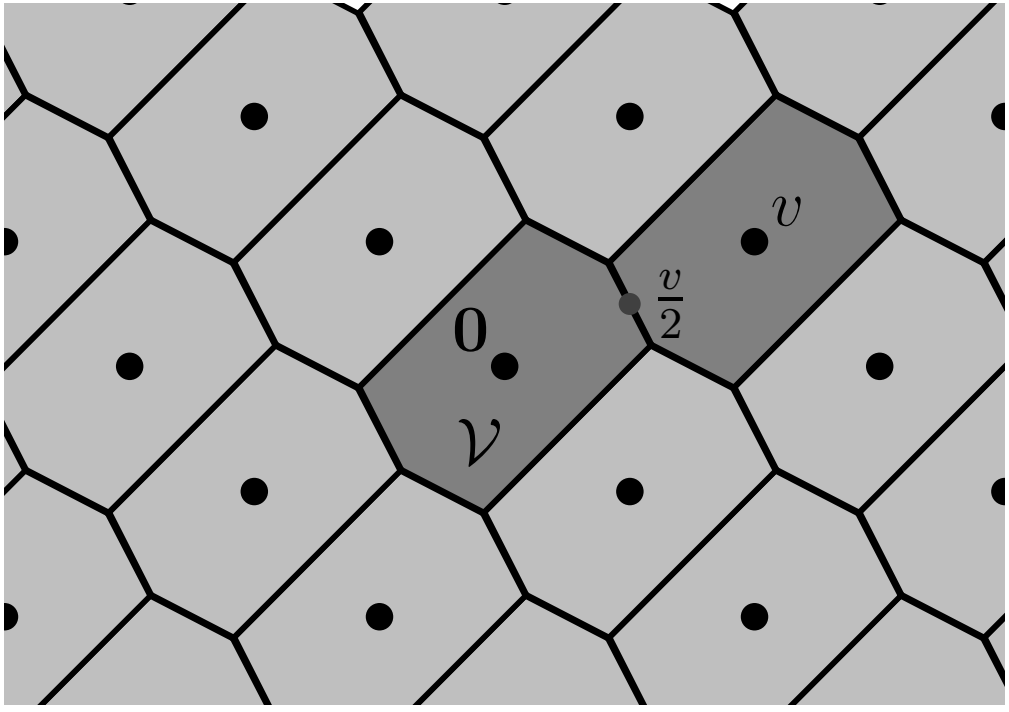
The Voronoi relevant vectors

- $v \in \Lambda$ is called **Voronoi relevant** if H_v is a facet of $\mathcal{V}$.
- **Obs 1:** $\mathcal{V} = \bigcap_{v \text{ Voronoi rel}} H_v$



The Voronoi relevant vectors

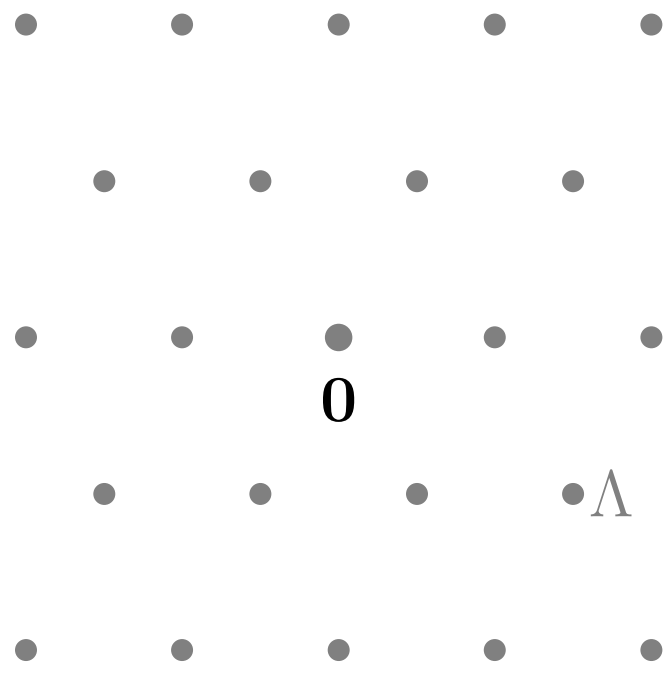
- $v \in \Lambda$ is called **Voronoi relevant** if H_v is a facet of $\mathcal{V}$.
- **Obs 1:** $\mathcal{V} = \bigcap_{v \text{ Voronoi rel}} H_v$
- **Obs 2:** If v Voronoi relevant, then unique closest lattice points to $\frac{v}{2}$ are $\mathbf{0}$ and v.



The Voronoi relevant vectors (2)

Lemma

The number of Voronoi relevant vectors is $|R| \leq 2^{n+1}$.

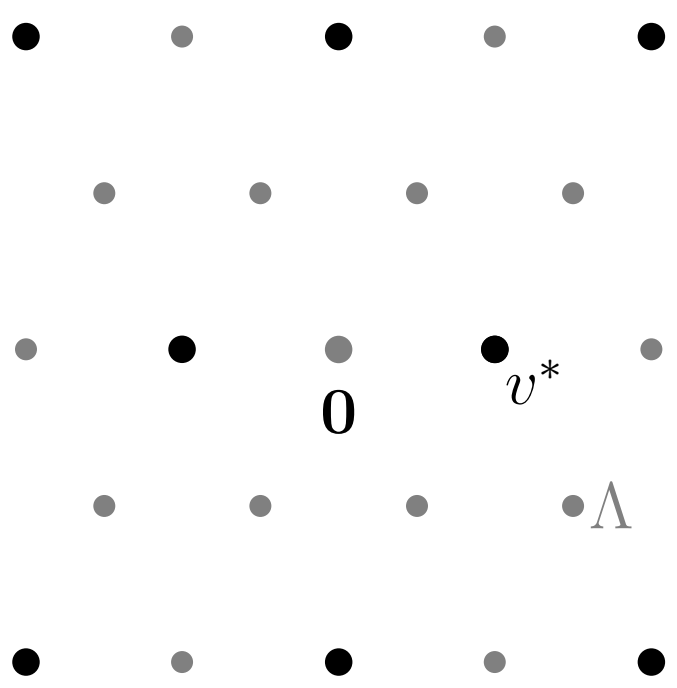


The Voronoi relevant vectors (2)

Lemma

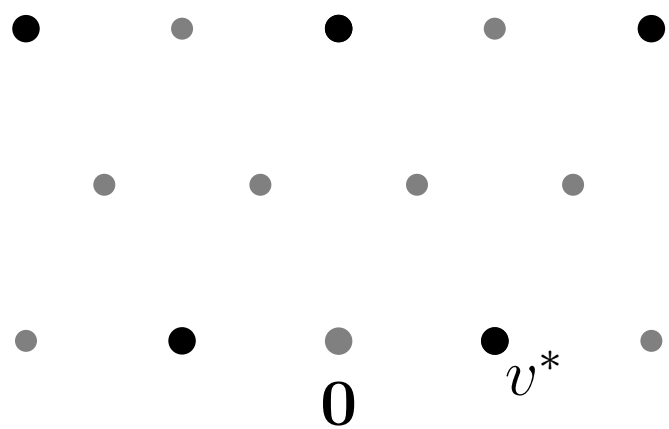
The number of Voronoi relevant vectors is $|R| \leq 2^{n+1}$.

Claim. For $v \in \Lambda$, consider coset $\Lambda' := v + 2\Lambda$. Apart from $v^* := \operatorname{argmin}\{\|x\|_2 : x \in \Lambda'\}$ and $-v^*$, there is no other Voronoi relevant vector in Λ'.



The Voronoi relevant vectors (3)

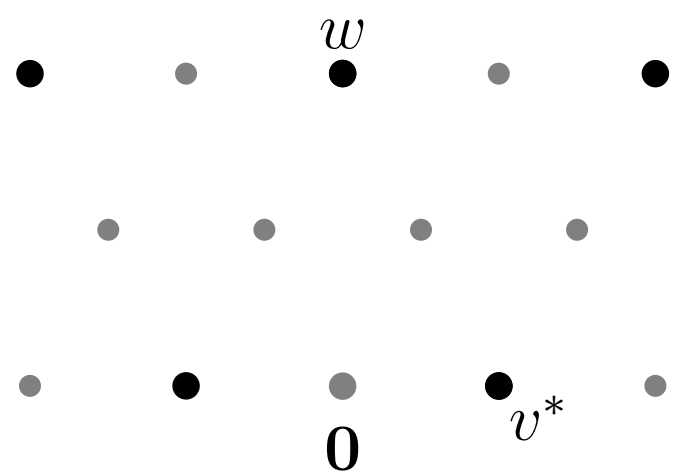
Proof.



The Voronoi relevant vectors (3)

Proof.

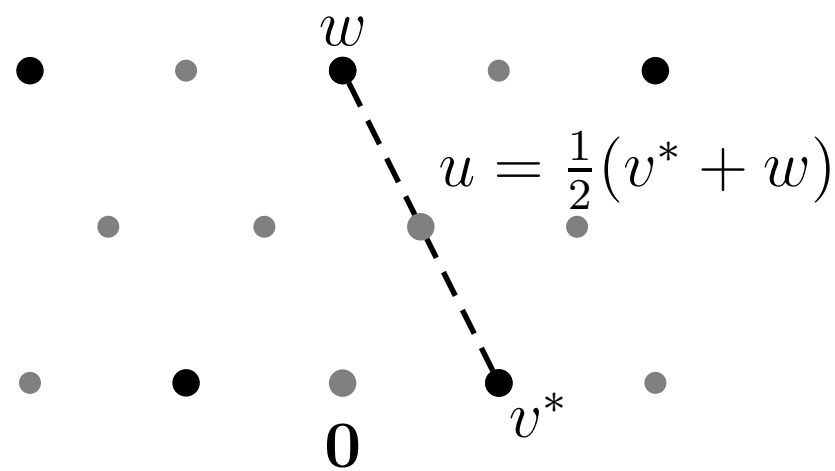
- Suppose that $w \in \Lambda'$ is Voronoi-relevant where $w \notin \{v^*, -v^*\}$



The Voronoi relevant vectors (3)

Proof.

- Suppose that $w \in \Lambda'$ is Voronoi-relevant where $w \notin \{v^*, -v^*\}$
- Consider $u := \frac{1}{2}(v^* + w) \in \Lambda$



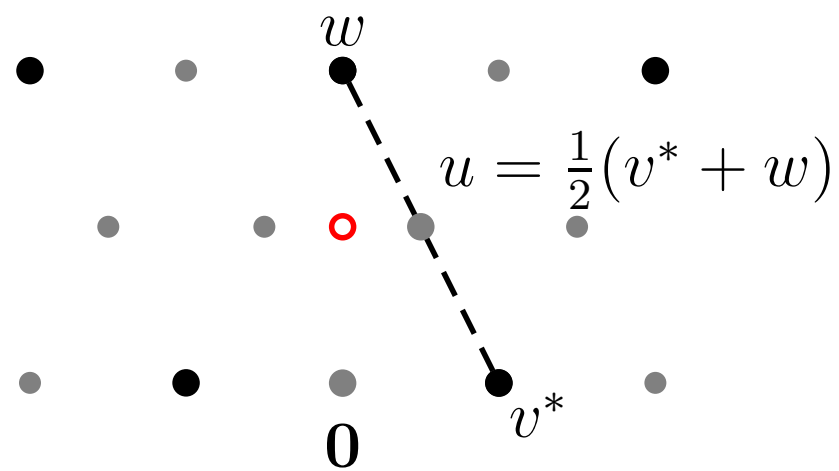
The Voronoi relevant vectors (3)

Proof.

- Suppose that $w \in \Lambda'$ is Voronoi-relevant where $w \notin \{v^*, -v^*\}$
- Consider $u := \frac{1}{2}(v^* + w) \in \Lambda$
- Then

$$\left\| \frac{w}{2} - u \right\|_2 = \left\| \frac{w}{2} - \frac{1}{2}(v^* + w) \right\|_2 = \frac{1}{2}\|v^*\|_2 \leq \frac{1}{2}\|w\|_2$$

which is a contradiction. □



The Voronoi relevant vectors (4)

Observation: We can find all Voronoi-relevant vectors by solving 2^n many CVPs in the same lattice, because

$$\min\{\|x\|_2 : x \in v + 2\Lambda\} = \min\{\|x - v\|_2 : x \in 2\Lambda\}$$

The Voronoi relevant vectors (4)

Observation: We can find all Voronoi-relevant vectors by solving 2^n many CVPs in the same lattice, because

$$\min\{\|x\|_2 : x \in v + 2\Lambda\} = \min\{\|x - v\|_2 : x \in 2\Lambda\}$$

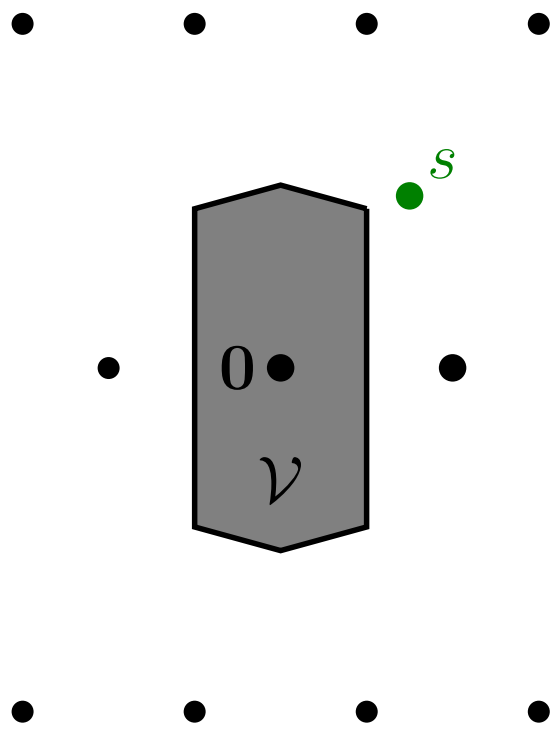
Now assume:

- We know the Voronoi-relevant vectors R
- We have a target vector $t \in 2\mathcal{V}$ (scaling handles the general case)

The Voronoi cell algorithm

Algorithm:

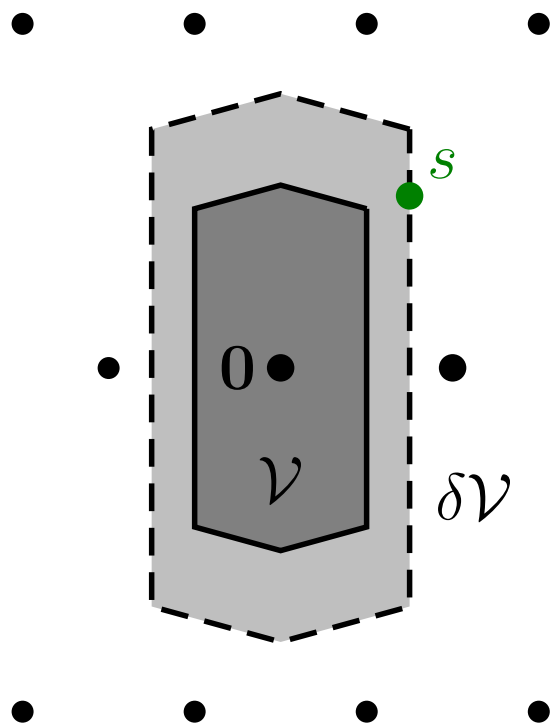
(1) Set $s := t$
(2) WHILE $s \notin \mathcal{V}$ DO
  (3) Set $\delta := \|s\|_{\mathcal{V}}$
  (4) Find $v \in R$ so that s lies on the boundary of δH_v
  (5) Update $s := s - v$
(6) Return $t - s$



The Voronoi cell algorithm

Algorithm:

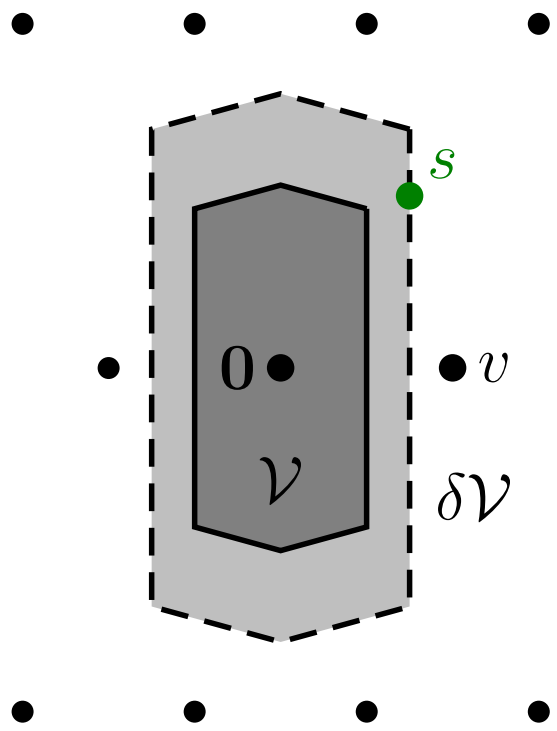
(1) Set $s := t$
(2) WHILE $s \notin \mathcal{V}$ DO
  (3) Set $\delta := \|s\|_{\mathcal{V}}$
  (4) Find $v \in R$ so that s lies on the boundary of δH_v
  (5) Update $s := s - v$
(6) Return $t - s$



The Voronoi cell algorithm

Algorithm:

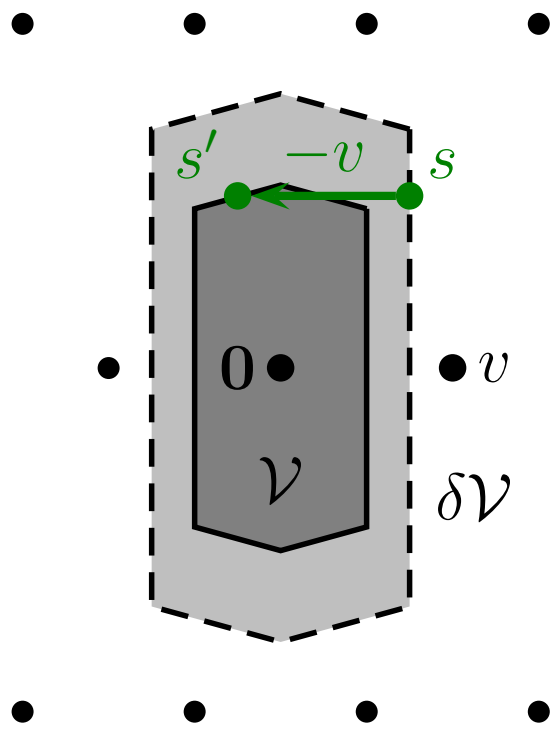
(1) Set $s := t$
(2) WHILE $s \notin \mathcal{V}$ DO
  (3) Set $\delta := \|s\|_{\mathcal{V}}$
  (4) Find $v \in R$ so that s lies on the boundary of δH_v
  (5) Update $s := s - v$
(6) Return $t - s$



The Voronoi cell algorithm

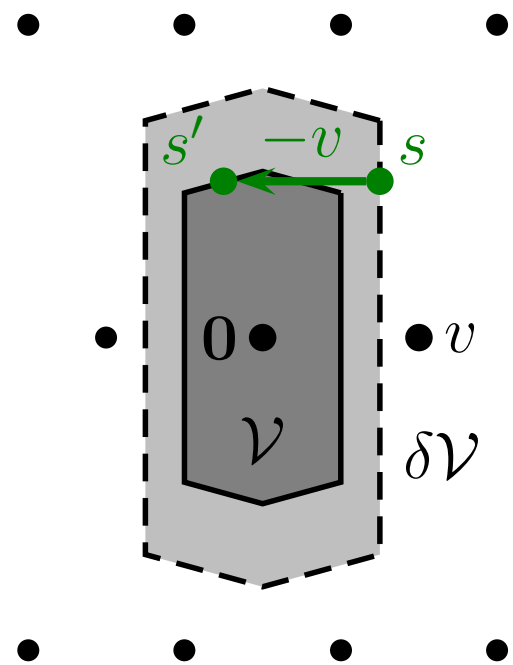
Algorithm:

(1) Set $s := t$
(2) WHILE $s \notin \mathcal{V}$ DO
  (3) Set $\delta := \|s\|_{\mathcal{V}}$
  (4) Find $v \in R$ so that s lies on the boundary of δH_v
  (5) Update $s := s - v$
(6) Return $t - s$



The Voronoi cell algorithm (2)

Claim. In each iteration $\|s - v\|_{\mathcal{V}} \leq \|s\|_{\mathcal{V}}$ and $\|s - v\|_2 < \|s\|_2$.



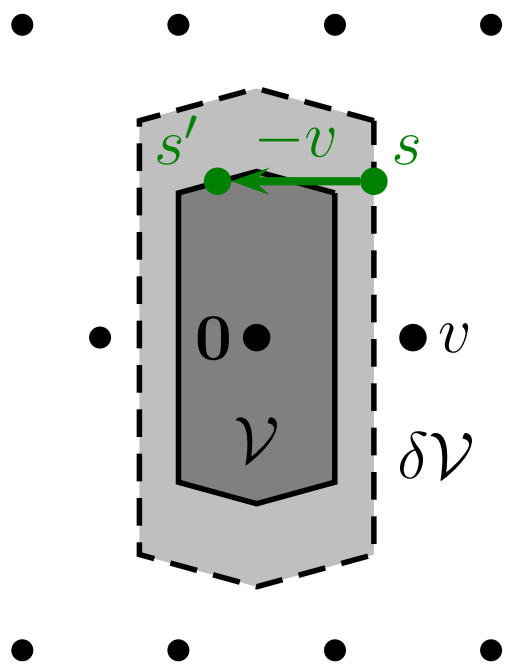
The Voronoi cell algorithm (2)

Claim. In each iteration $\|s-v\|_{\mathcal{V}} \leq \|s\|_{\mathcal{V}}$ and $\|s-v\|_2 < \|s\|_2$.
Proof.

- By assumption $\frac{s}{\delta} \in v + \mathcal{V}$ and so by triangle inequality

$$\|s-v\|_{\mathcal{V}} \leq \underbrace{\left\|\frac{s}{\delta} - v\right\|_{\mathcal{V}}}_{\leq 1} + \left(1-\frac{1}{\delta}\right) \underbrace{\|s\|_{\mathcal{V}}}_{\leq \delta} \leq \delta$$

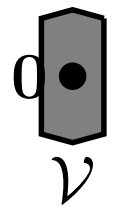
- Bound on $\|\cdot\|_2$ clear.



The Voronoi cell algorithm (3)

Lemma

For any $t \in \mathbb{R}^n$, $|(t - \Lambda) \cap 2\mathcal{V}| \leq 2^{O(n)}$.



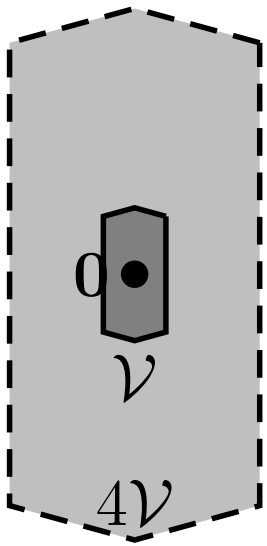
The Voronoi cell algorithm (3)

Lemma

For any $t \in \mathbb{R}^n$, $|(t - \Lambda) \cap 2\mathcal{V}| \leq 2^{O(n)}$.

Proof.

- Suffices to prove $|\Lambda \cap 4\mathcal{V}| \leq 4^n$.



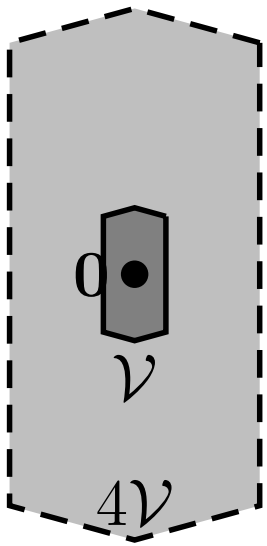
The Voronoi cell algorithm (3)

Lemma

For any $t \in \mathbb{R}^n$, $|(t - \Lambda) \cap 2\mathcal{V}| \leq 2^{O(n)}$.

Proof.

- Suffices to prove $|\Lambda \cap 4\mathcal{V}| \leq 4^n$. Suppose otherwise.



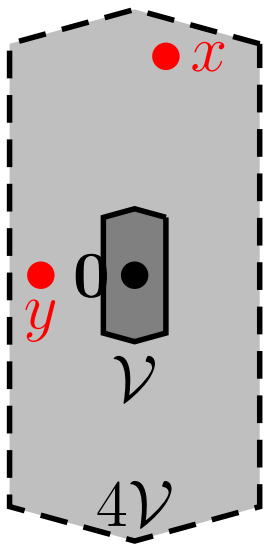
The Voronoi cell algorithm (3)

Lemma

For any $t \in \mathbb{R}^n$, $|(t - \Lambda) \cap 2\mathcal{V}| \leq 2^{O(n)}$.

Proof.

- Suffices to prove $|\Lambda \cap 4\mathcal{V}| \leq 4^n$. Suppose otherwise.
- By pigeonhole principle, there are distinct $x, y \in \Lambda \cap 4\mathcal{V}$ with $x - y \in 4\Lambda$.



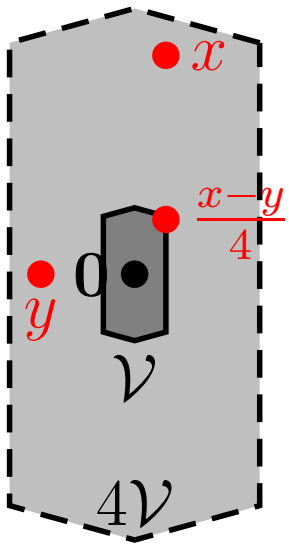
The Voronoi cell algorithm (3)

Lemma

For any $t \in \mathbb{R}^n$, $|(t - \Lambda) \cap 2\mathcal{V}| \leq 2^{O(n)}$.

Proof.

- Suffices to prove $|\Lambda \cap 4\mathcal{V}| \leq 4^n$. Suppose otherwise.
- By pigeonhole principle, there are distinct $x, y \in \Lambda \cap 4\mathcal{V}$ with $x - y \in 4\Lambda$.
- Then $\|\frac{x-y}{4}\|_{\mathcal{V}} \leq 1$ — contradiction as $\Lambda \cap \mathcal{V} = \{\mathbf{0}\}$. □



The Voronoi cell algorithm (3)

Lemma

For any $t \in \mathbb{R}^n$, $|(t - \Lambda) \cap 2\mathcal{V}| \leq 2^{O(n)}$.

Proof.

- Suffices to prove $|\Lambda \cap 4\mathcal{V}| \leq 4^n$. Suppose otherwise.
- By pigeonhole principle, there are distinct $x, y \in \Lambda \cap 4\mathcal{V}$ with $x - y \in 4\Lambda$.
- Then $\|\frac{x-y}{4}\|_{\mathcal{V}} \leq 1$ — contradiction as $\Lambda \cap \mathcal{V} = \{\mathbf{0}\}$. □

More generally: given $t \in 2^k\mathcal{V}$, after $2^{O(n)}$ iteration we are in $2^{k-1}\mathcal{V}$ using update steps $2^{k-1}v$ with $v \in \Lambda$.

Putting things together

- Define

$$\begin{aligned} T_{\text{Voronoi}}(n) &= \text{time to compute Voronoi cell for } \Lambda \subseteq \mathbb{R}^n \\ T_{\text{CVP}}(n,k) &= \text{time to solve } k \text{ many CVPs in the} \\ &\quad \text{same } n\text{-dim. lattice} \end{aligned}$$

Putting things together

- Define

$$\begin{aligned} T_{\text{Voronoi}}(n) &= \text{time to compute Voronoi cell for } \Lambda \subseteq \mathbb{R}^n \\ T_{\text{CVP}}(n,k) &= \text{time to solve } k \text{ many CVPs in the} \\ &\quad \text{same } n\text{-dim. lattice} \end{aligned}$$

- We obtain

$$T_{\text{Voronoi}}(n) \overset{(*)}{\leq} T_{\text{CVP}}(n, 2^{O(n)})$$

- $(*)$ char. of Voronoi relevant Vectors

Putting things together

- Define

$$\begin{aligned} T_{\text{Voronoi}}(n) &= \text{time to compute Voronoi cell for } \Lambda \subseteq \mathbb{R}^n \\ T_{\text{CVP}}(n,k) &= \text{time to solve } k \text{ many CVPs in the} \\ &\quad \text{same } n\text{-dim. lattice} \end{aligned}$$

- We obtain

$$T_{\text{Voronoi}}(n) \overset{(*)}{\leq} T_{\text{CVP}}(n, 2^{O(n)}) \overset{(**)}{\leq} T_{\text{Voronoi}}(n) + 2^{O(n)} \cdot 2^{O(n)}$$

- $(*)$ char. of Voronoi relevant Vectors
- $(**)$ main algorithm

Putting things together

- Define

$$\begin{aligned} T_{\text{Voronoi}}(n) &= \text{time to compute Voronoi cell for } \Lambda \subseteq \mathbb{R}^n \\ T_{\text{CVP}}(n,k) &= \text{time to solve } k \text{ many CVPs in the} \\ &\quad \text{same } n\text{-dim. lattice} \end{aligned}$$

- We obtain

$$T_{\text{Voronoi}}(n) \overset{(*)}{\leq} T_{\text{CVP}}(n, 2^{O(n)}) \overset{(**)}{\leq} T_{\text{Voronoi}}(n) + 2^{O(n)} \cdot 2^{O(n)}$$

- $(*)$ char. of Voronoi relevant Vectors
- $(**)$ main algorithm
- $(***)$ **By LLL algorithm**: Can reduce CVP in dim n to $2^{O(n)}$ instances of CVP in same $n-1$ dim. lattice.

Putting things together

- We obtain

$$\begin{aligned} T_{\text{Voronoi}}(n) &\overset{(*)}{\leq} T_{\text{CVP}}(n, 2^{O(n)}) \\ &\overset{(***)}{\leq} T_{\text{CVP}}(n-1, 2^{O(n)} \cdot 2^{O(n)}) \\ &\overset{(**)}{\leq} T_{\text{Voronoi}}(n-1) + 2^{O(n)} \cdot 2^{O(n)} \cdot 2^{O(n)}. \end{aligned}$$

- $(*)$ char. of Voronoi relevant Vectors
- $(**)$ main algorithm
- $(***)$ **By LLL algorithm**: Can reduce CVP in dim n to $2^{O(n)}$ instances of CVP in same $n-1$ dim. lattice.

Putting things together

- We obtain

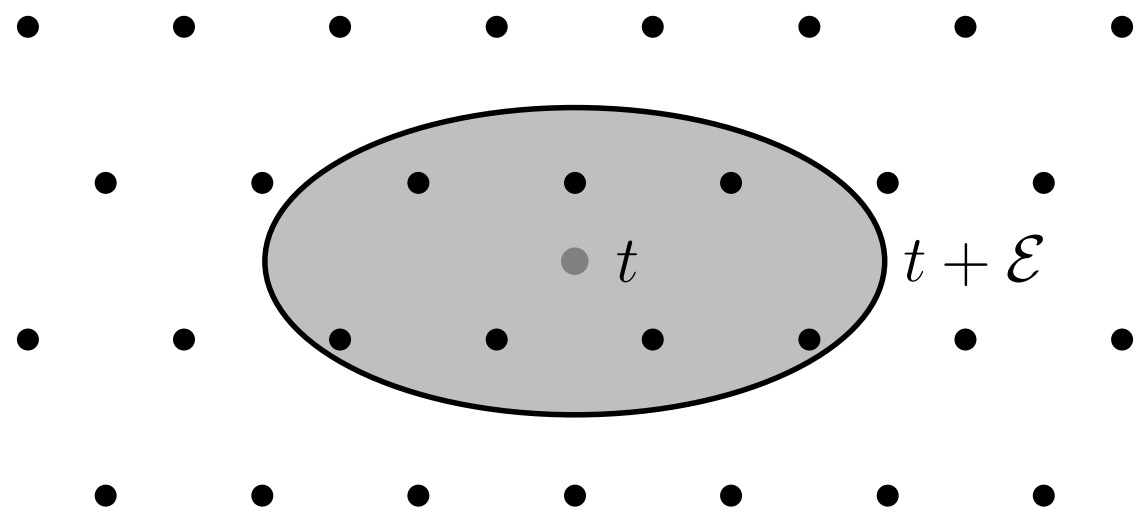
$$\begin{aligned} T_{\text{Voronoi}}(n) &\overset{(*)}{\leq} T_{\text{CVP}}(n, 2^{O(n)}) \\ &\overset{(***)}{\leq} T_{\text{CVP}}(n-1, 2^{O(n)} \cdot 2^{O(n)}) \\ &\overset{(**)}{\leq} T_{\text{Voronoi}}(n-1) + 2^{O(n)} \cdot 2^{O(n)} \cdot 2^{O(n)}. \end{aligned}$$

- $(*)$ char. of Voronoi relevant Vectors
- $(**)$ main algorithm
- $(***)$ **By LLL algorithm**: Can reduce CVP in dim n to $2^{O(n)}$ instances of CVP in same $n-1$ dim. lattice.
- Resolve recursion to $T_{\text{Voronoi}}(n), T_{\text{CVP}}(n, 2^{O(n)}) \leq 2^{O(n)}$ □

Enumeration of points

Theorem

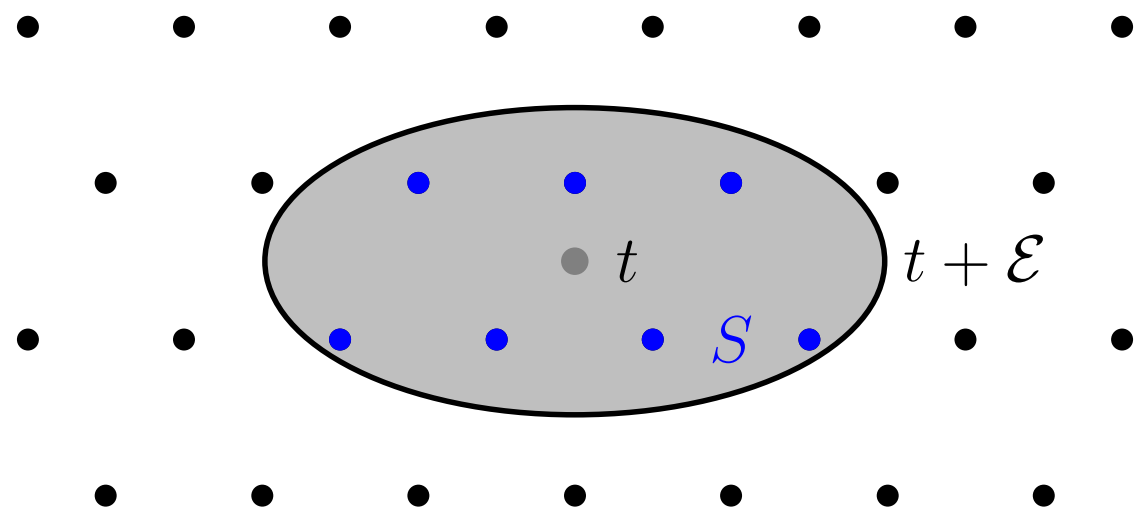
For any ellipsoid $\mathcal{E}$, one can enumerate points $S := \Lambda \cap (\mathcal{E} + t)$ in time $2^{O(n)} \cdot (|S| + 1)$.



Enumeration of points

Theorem

For any ellipsoid $\mathcal{E}$, one can enumerate points $S := \Lambda \cap (\mathcal{E} + t)$ in time $2^{O(n)} \cdot (|S| + 1)$.

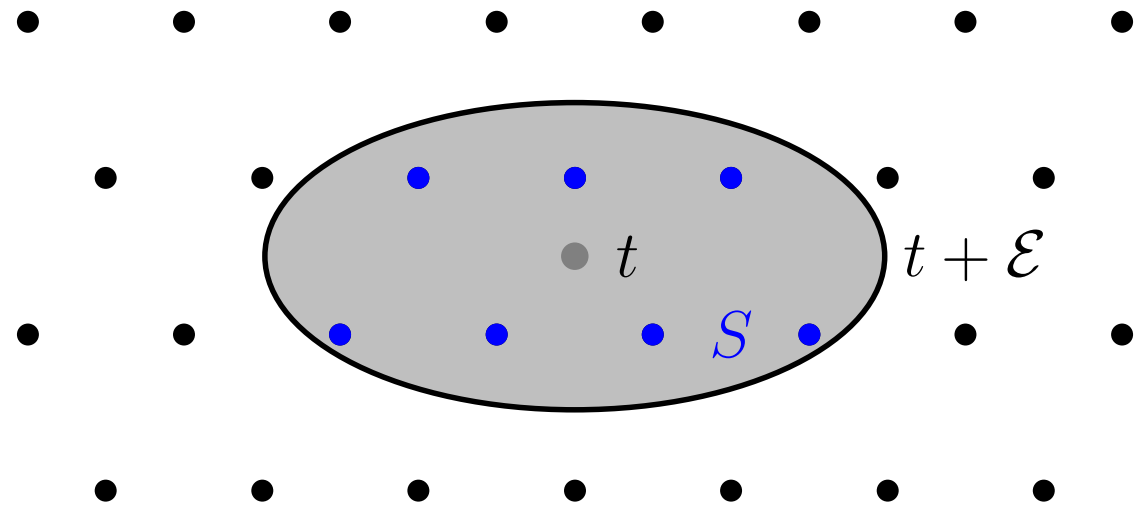


Enumeration of points

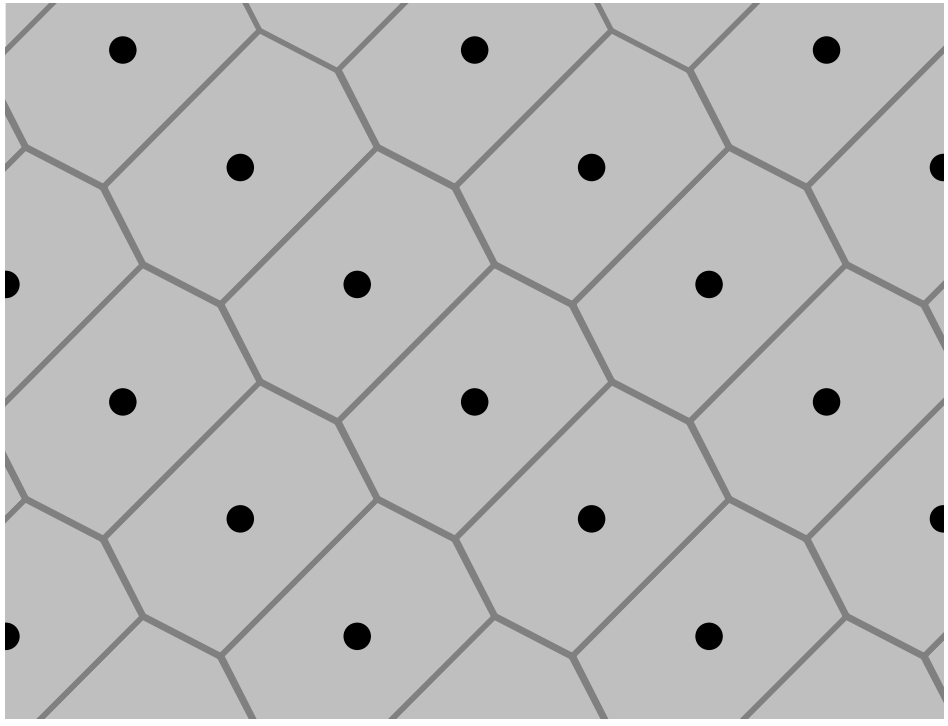
Theorem

For any ellipsoid $\mathcal{E}$, one can enumerate points $S := \Lambda \cap (\mathcal{E} + t)$ in time $2^{O(n)} \cdot (|S| + 1)$.

- After applying linear transformation, assume $\mathcal{E} = B_2^n$.

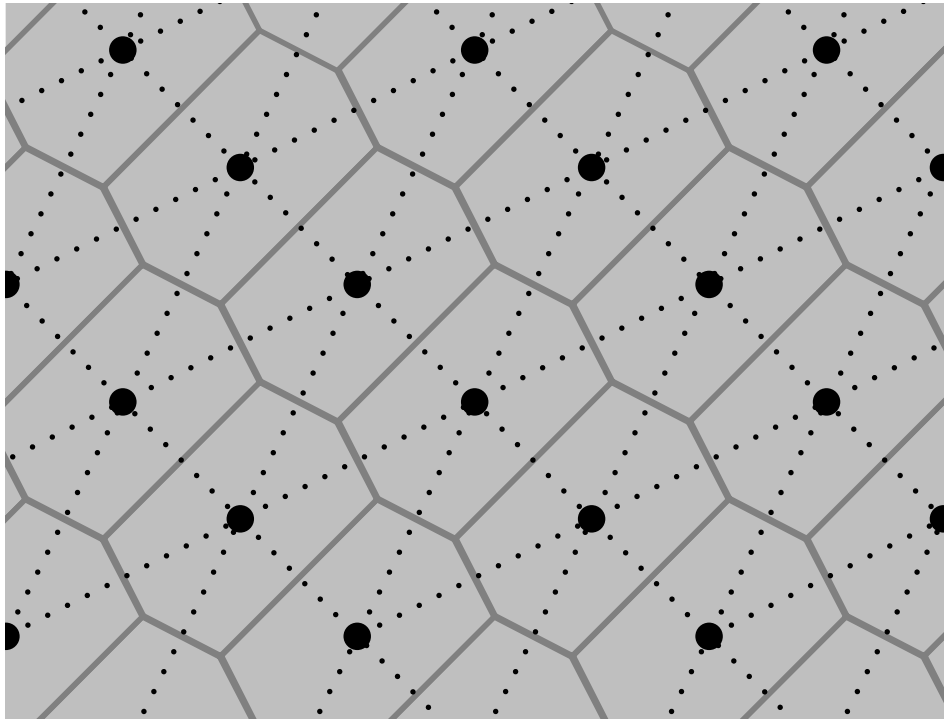


Enumeration of points (2)



Enumeration of points (2)

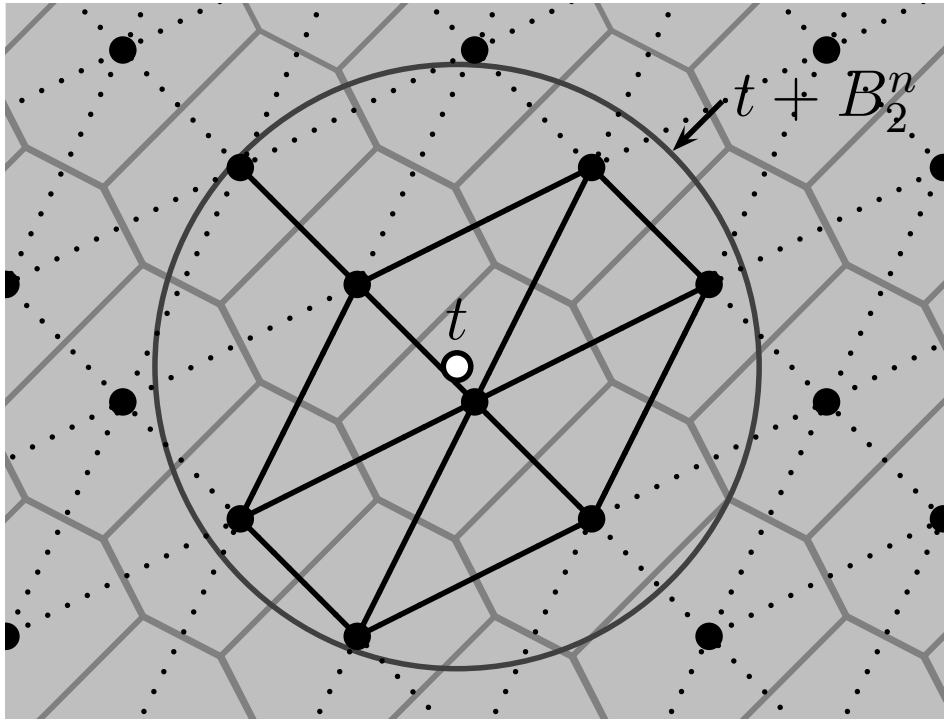
- Define graph $G = (\Lambda, E)$ with $E = \{\{x, y\} \mid x, y \in \Lambda, x - y \in R\}$. G has degree $|R|$.



Enumeration of points (2)

- Define graph $G = (\Lambda, E)$ with
  $E = \{\{x, y\} \mid x, y \in \Lambda, x - y \in R\}$. G has degree $|R|$.

Claim. $G[S]$ with $S := \Lambda \cap (B_2^n + t)$ is connected.

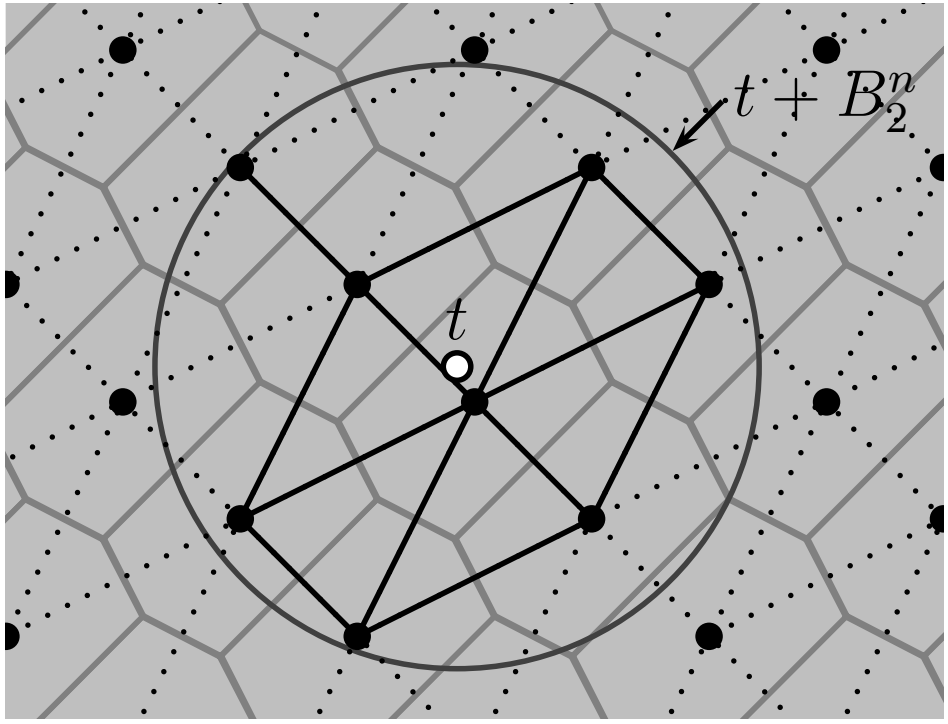


Enumeration of points (2)

- Define graph $G = (\Lambda, E)$ with
  $E = \{\{x, y\} \mid x, y \in \Lambda, x - y \in R\}$. G has degree $|R|$.

Claim. $G[S]$ with $S := \Lambda \cap (B_2^n + t)$ is connected.

Proof. [MV'10] shows $\exists$ path $x_0, x_1, x_2, \ldots \in S$ with $\|x_0 - t\|_2 > \|x_1 - t\|_2 > \ldots$ □

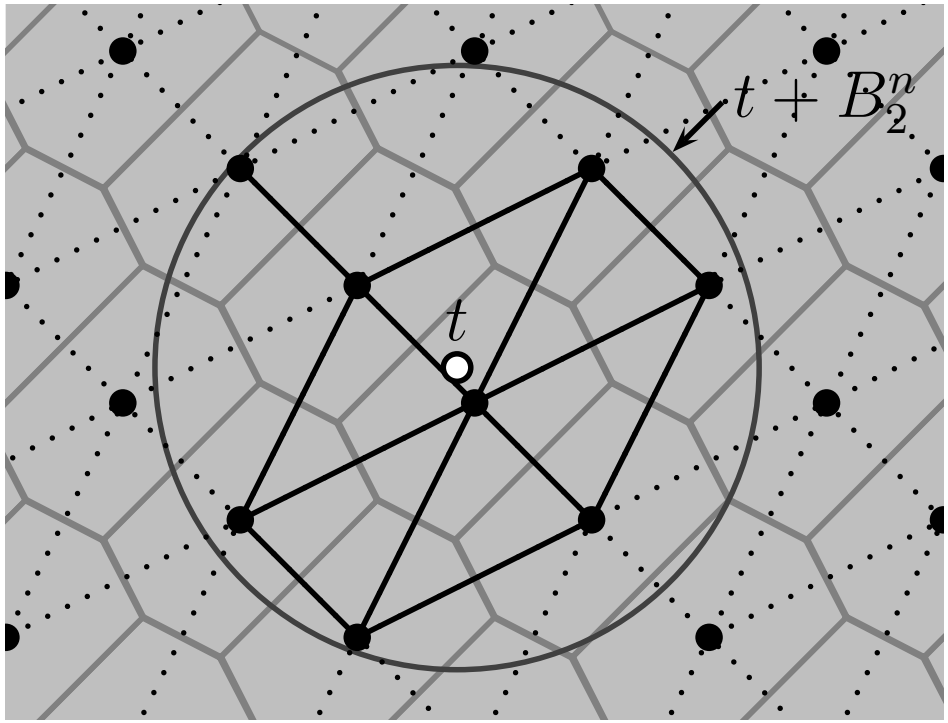


Enumeration of points (2)

- Define graph $G = (\Lambda, E)$ with
  $E = \{\{x, y\} \mid x, y \in \Lambda, x - y \in R\}$. G has degree $|R|$.

Claim. $G[S]$ with $S := \Lambda \cap (B_2^n + t)$ is connected.

Proof. [MV'10] shows $\exists$ path $x_0, x_1, x_2, \ldots \in S$ with $\|x_0 - t\|_2 > \|x_1 - t\|_2 > \ldots$ □



- Then explore $G[S]$ from point attaining $\mathrm{CVP}(\Lambda, t)$

M-ellipsoids

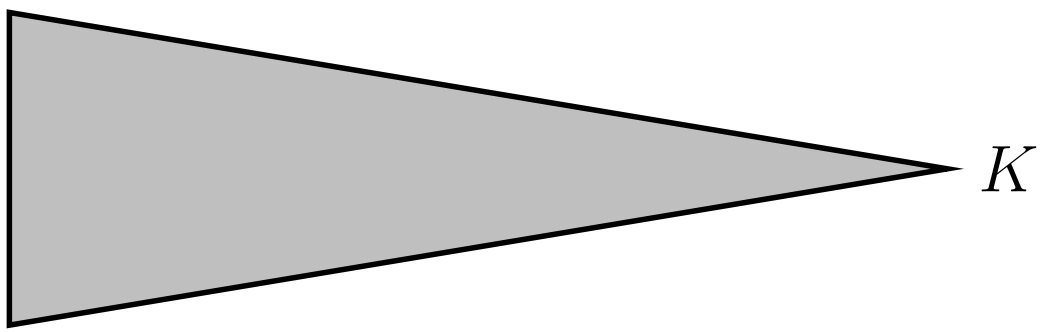
- For convex bodies, $A, B \subseteq \mathbb{R}^n$, let $N(A, B)$ be the minimum number of translates of B to cover A.

M-ellipsoids

- For convex bodies, $A, B \subseteq \mathbb{R}^n$, let $N(A, B)$ be the minimum number of translates of B to cover A.

Theorem (Dadush, Vempala '12)

For any convex body $K \subseteq \mathbb{R}^n$, one can compute an ellipsoid $\mathcal{E}$ so that $N(K, \mathcal{E}), N(\mathcal{E}, K) \leq 2^{O(n)}$ in deterministic time $2^{O(n)}$.

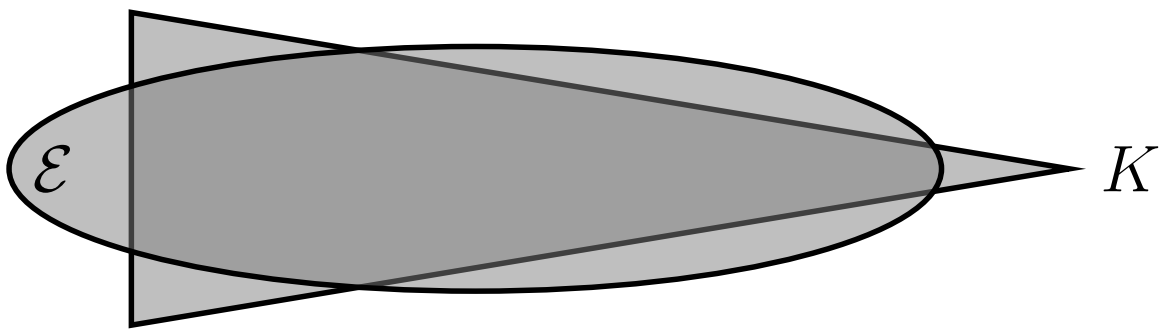


M-ellipsoids

- For convex bodies, $A, B \subseteq \mathbb{R}^n$, let $N(A, B)$ be the minimum number of translates of B to cover A.

Theorem (Dadush, Vempala '12)

For any convex body $K \subseteq \mathbb{R}^n$, one can compute an ellipsoid $\mathcal{E}$ so that $N(K, \mathcal{E}), N(\mathcal{E}, K) \leq 2^{O(n)}$ in deterministic time $2^{O(n)}$.

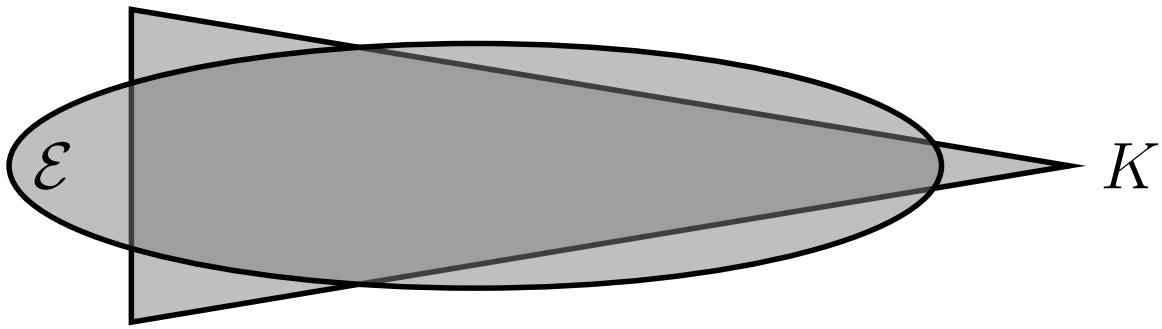


M-ellipsoids

- For convex bodies, $A, B \subseteq \mathbb{R}^n$, let $N(A, B)$ be the minimum number of translates of B to cover A.

Theorem (Dadush, Vempala '12)

For any convex body $K \subseteq \mathbb{R}^n$, one can compute an ellipsoid $\mathcal{E}$ so that $N(K, \mathcal{E}), N(\mathcal{E}, K) \leq 2^{O(n)}$ in deterministic time $2^{O(n)}$. Moreover one can compute the points $x_1, \ldots, x_N$ with $K \subseteq \bigcup_{i=1}^{N} (x_i + \mathcal{E})$ and $N \leq 2^{O(n)}$ as well.

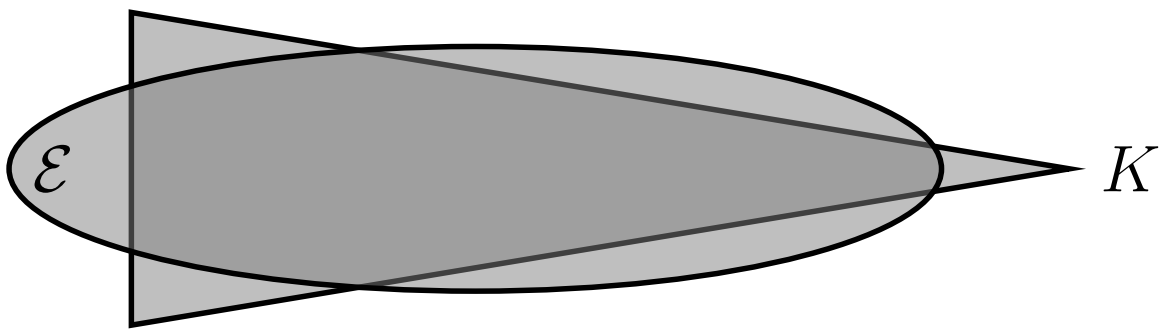


M-ellipsoids

- For convex bodies, $A, B \subseteq \mathbb{R}^n$, let $N(A, B)$ be the minimum number of translates of B to cover A.

Theorem (Dadush, Vempala '12)

For any convex body $K \subseteq \mathbb{R}^n$, one can compute an ellipsoid $\mathcal{E}$ so that $N(K, \mathcal{E}), N(\mathcal{E}, K) \leq 2^{O(n)}$ in deterministic time $2^{O(n)}$. Moreover one can compute the points $x_1, \ldots, x_N$ with $K \subseteq \bigcup_{i=1}^{N} (x_i + \mathcal{E})$ and $N \leq 2^{O(n)}$ as well.



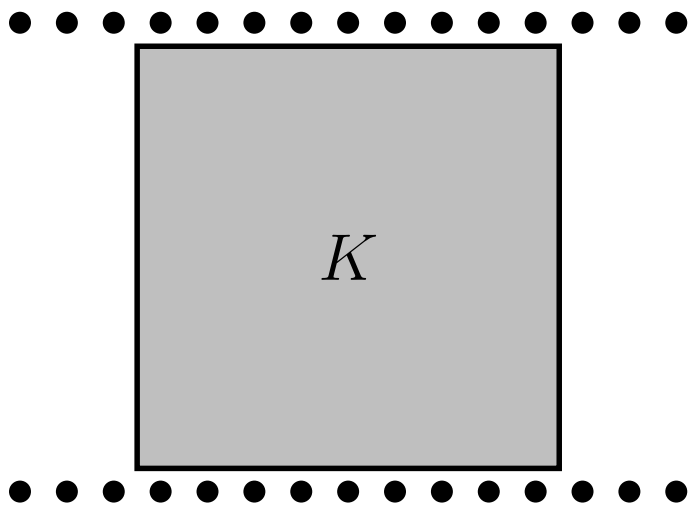
- In convex geometry these are called **M-ellipsoids**

Application to arbitrary convex K

Idea: Cover K by $2^{O(n)}$ many M-ellipsoids, then find/enumerate points in ellipsoids.

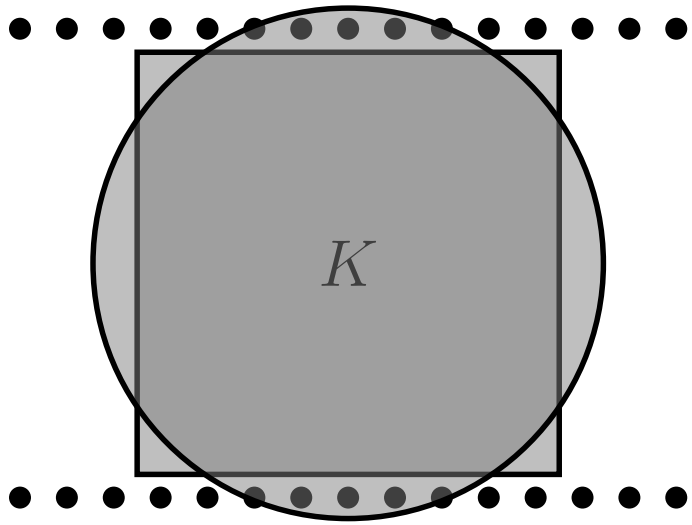
Application to arbitrary convex K

Idea: Cover K by $2^{O(n)}$ many M-ellipsoids, then find/enumerate points in ellipsoids.



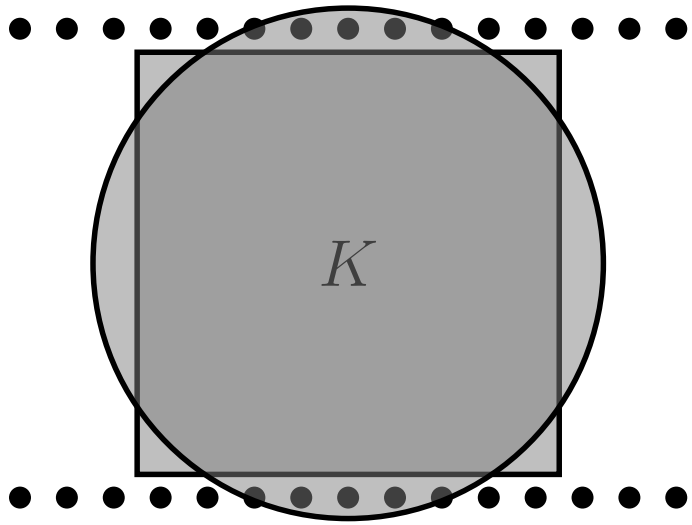
Application to arbitrary convex K

Idea: Cover K by $2^{O(n)}$ many M-ellipsoids, then find/enumerate points in ellipsoids.



Application to arbitrary convex K

Idea: Cover K by $2^{O(n)}$ many M-ellipsoids, then find/enumerate points in ellipsoids.

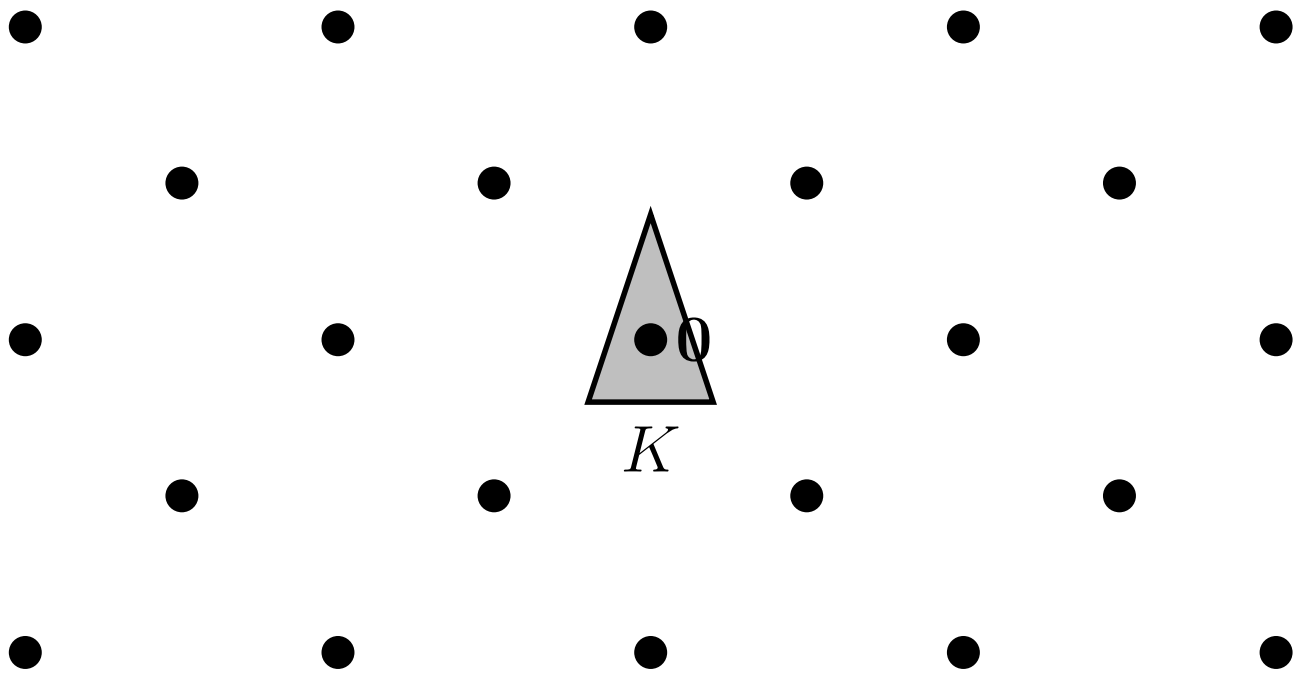


- But the method does actually work if the **covering radius** is lower bounded..

Covering radius

- For K convex, the **covering radius** is

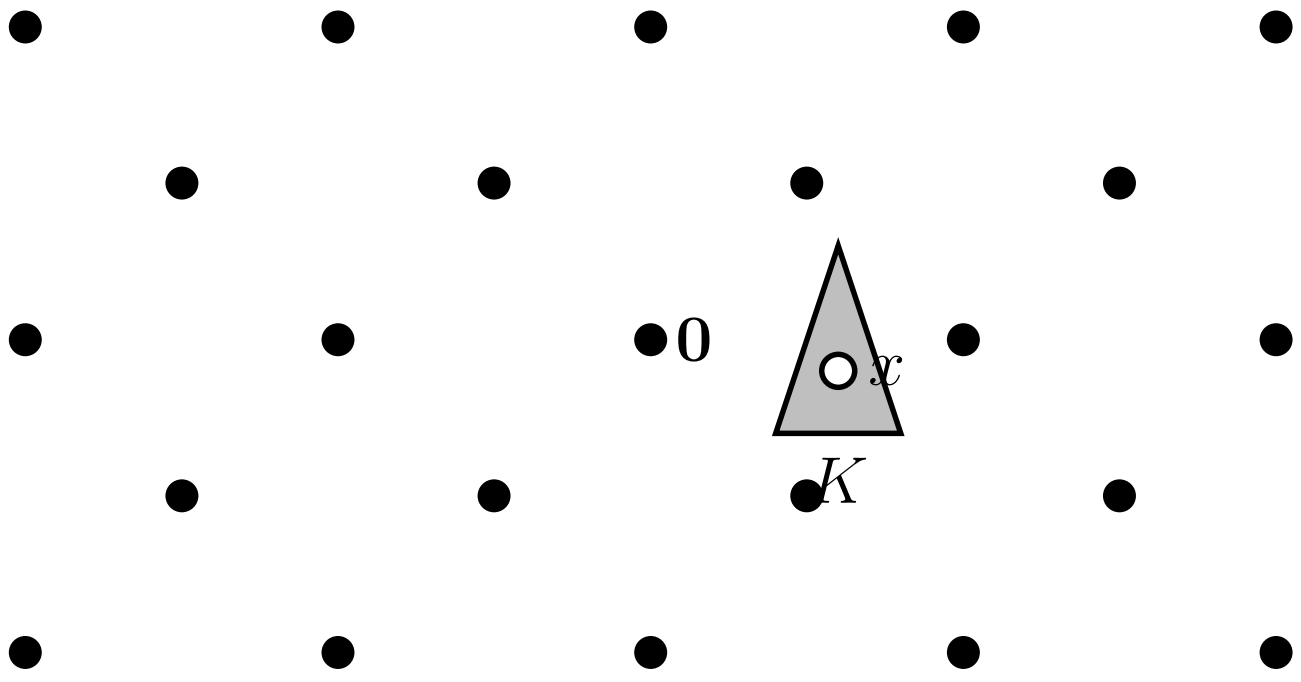
$$\mu(\Lambda, K) \quad = \quad \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\}$$



Covering radius

- For K convex, the **covering radius** is

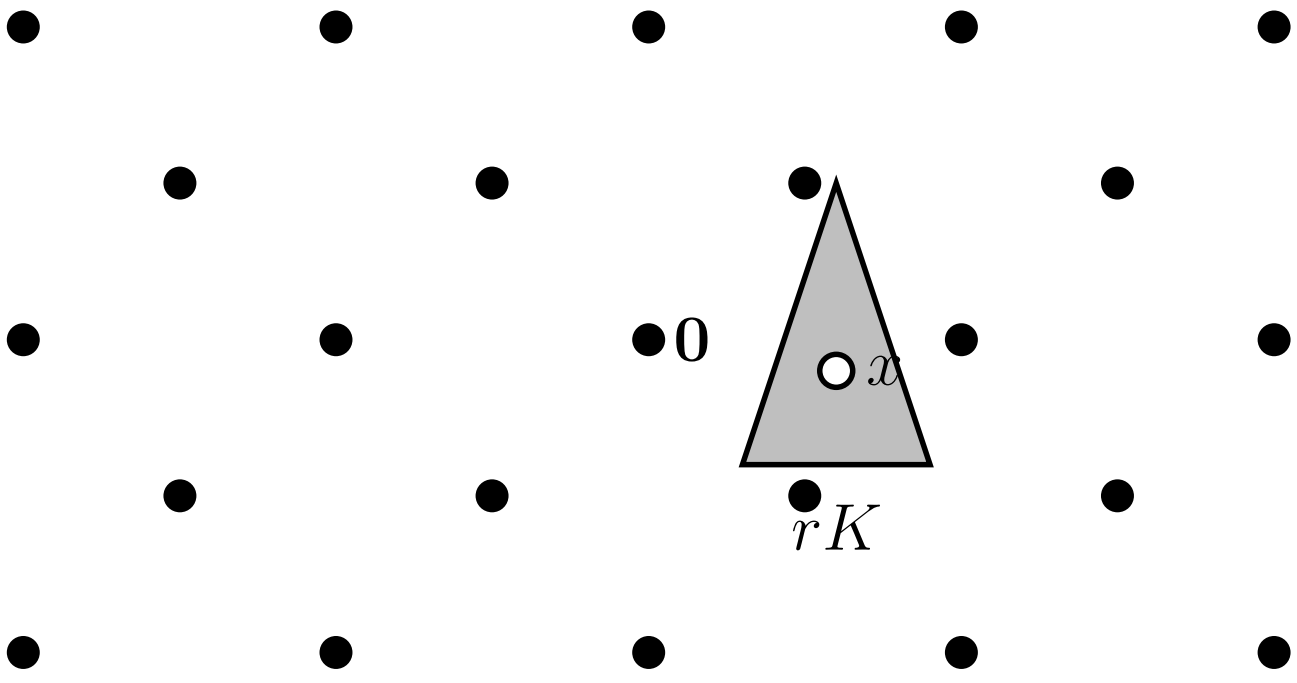
$$\begin{aligned}\mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \ \forall x \in \mathbb{R}^n\}\end{aligned}$$



Covering radius

- For K convex, the **covering radius** is

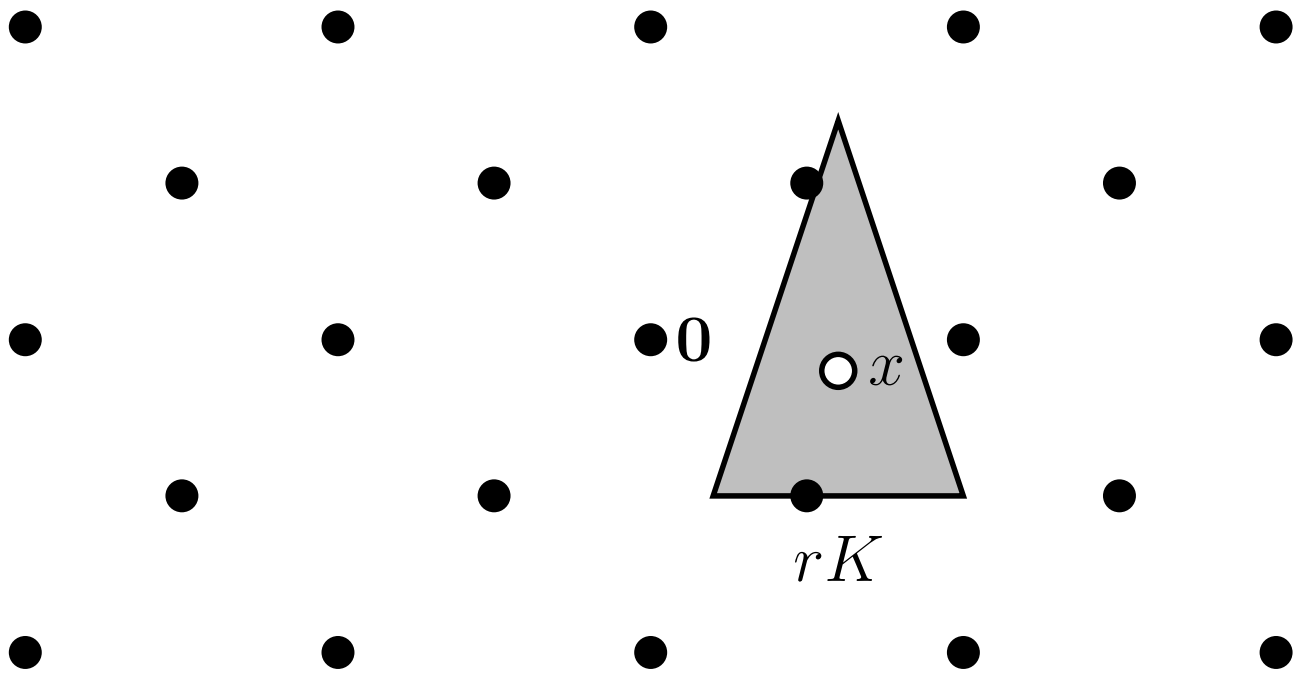
$$\begin{aligned}\mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \ \forall x \in \mathbb{R}^n\}\end{aligned}$$



Covering radius

- For K convex, the **covering radius** is

$$\begin{aligned}\mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \ \forall x \in \mathbb{R}^n\}\end{aligned}$$



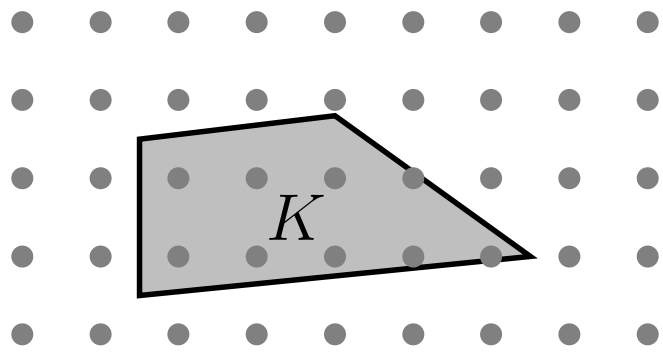
Dadush's lattice point upper bound

Theorem (Dadush 2012)

For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$|K \cap \Lambda| \leq N := 2^n \max\{\mu(\Lambda, K)^n, 1\} \cdot \frac{Vol_n(K)}{\det(\Lambda)}.$$

Moreover, can compute points in same time.



Dadush's lattice point upper bound

Theorem (Dadush 2012)

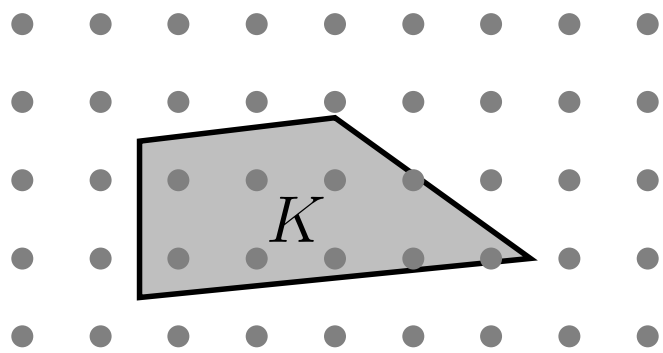
For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$|K \cap \Lambda| \leq N := 2^n \max\{\mu(\Lambda, K)^n, 1\} \cdot \frac{Vol_n(K)}{\det(\Lambda)}.$$

Moreover, can compute points in same time.

Proof of moreover part:

- Bound holds for any translate of K



Dadush's lattice point upper bound

Theorem (Dadush 2012)

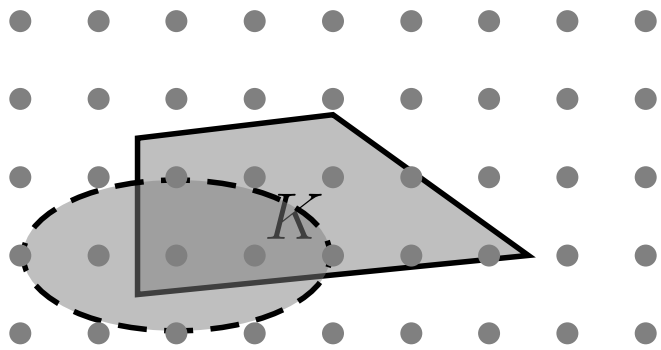
For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$|K \cap \Lambda| \leq N := 2^n \max\{\mu(\Lambda, K)^n, 1\} \cdot \frac{Vol_n(K)}{\det(\Lambda)}.$$

Moreover, can compute points in same time.

Proof of moreover part:

- Bound holds for any translate of K



Dadush's lattice point upper bound

Theorem (Dadush 2012)

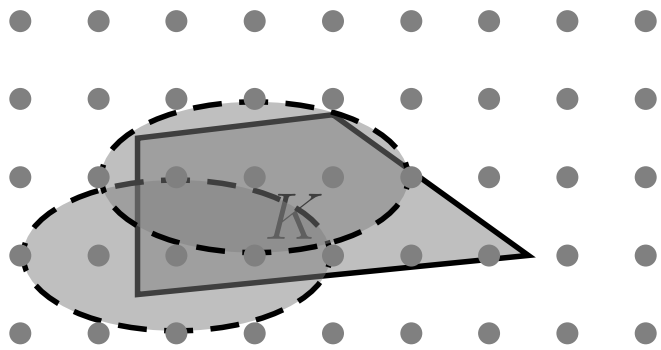
For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$|K \cap \Lambda| \leq N := 2^n \max\{\mu(\Lambda, K)^n, 1\} \cdot \frac{Vol_n(K)}{\det(\Lambda)}.$$

Moreover, can compute points in same time.

Proof of moreover part:

- Bound holds for any translate of K



Dadush's lattice point upper bound

Theorem (Dadush 2012)

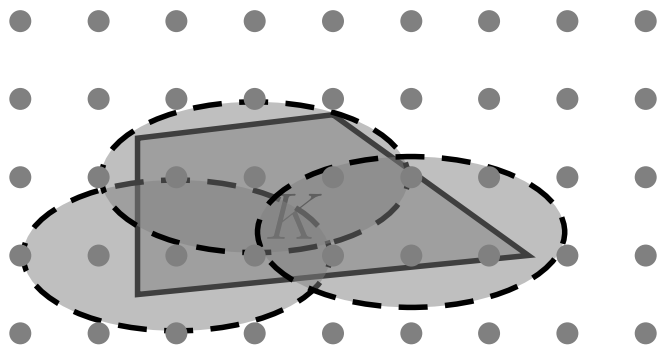
For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$|K \cap \Lambda| \leq N := 2^n \max\{\mu(\Lambda, K)^n, 1\} \cdot \frac{Vol_n(K)}{\det(\Lambda)}.$$

Moreover, can compute points in same time.

Proof of moreover part:

- Bound holds for any translate of K



Dadush's lattice point upper bound

Theorem (Dadush 2012)

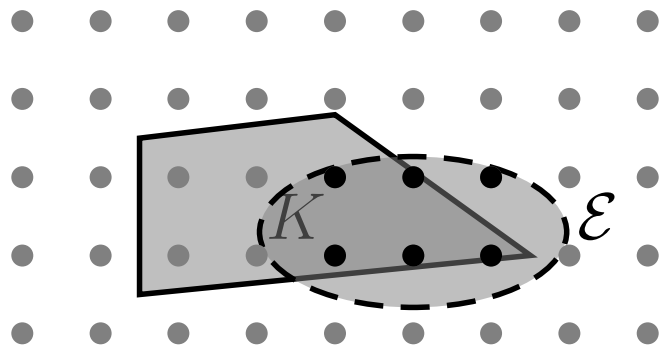
For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$|K \cap \Lambda| \leq N := 2^n \max\{\mu(\Lambda, K)^n, 1\} \cdot \frac{Vol_n(K)}{\det(\Lambda)}.$$

Moreover, can compute points in same time.

Proof of moreover part:

- Bound holds for any translate of K
- Any shifted M-ellipsoid $\mathcal{E}$ also has $|\mathcal{E} \cap \Lambda| \leq 2^{O(n)} N$



Dadush's lattice point upper bound

Theorem (Dadush 2012)

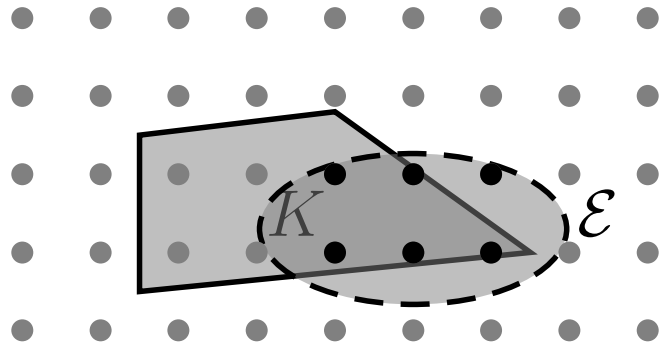
For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$|K \cap \Lambda| \leq N := 2^n \max\{\mu(\Lambda, K)^n, 1\} \cdot \frac{Vol_n(K)}{\det(\Lambda)}.$$

Moreover, can compute points in same time.

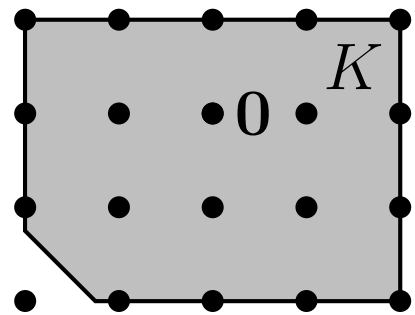
Proof of moreover part:

- Bound holds for any translate of K
- Any shifted M-ellipsoid $\mathcal{E}$ also has $|\mathcal{E} \cap \Lambda| \leq 2^{O(n)} N$
- Hence can enumerate all points in K in time $2^{O(n)} N$.



Dadush's lattice point upper bound

Claim. For any convex body $K \subseteq \mathbb{R}^n$ with $\mu(\mathbb{Z}^n, K) \leq 1$ and any $x \in \mathbb{R}^n$ one has $|K \cap (x + \mathbb{Z}^n)| \leq 2^n \mathrm{Vol}_n(K)$.

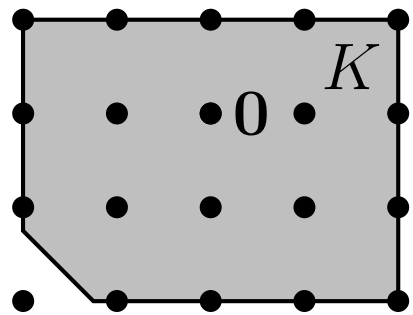


Dadush's lattice point upper bound

Claim. For any convex body $K \subseteq \mathbb{R}^n$ with $\mu(\mathbb{Z}^n, K) \leq 1$ and any $x \in \mathbb{R}^n$ one has $|K \cap (x + \mathbb{Z}^n)| \leq 2^n \mathrm{Vol}_n(K)$.

Proof of Claim.

- Assume $\mathbf{0} \in K$

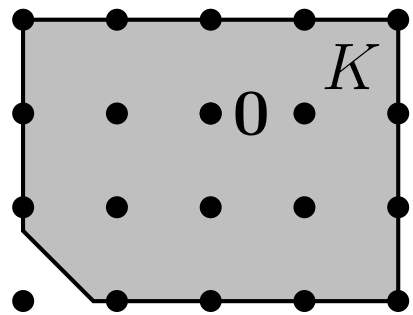


Dadush's lattice point upper bound

Claim. For any convex body $K \subseteq \mathbb{R}^n$ with $\mu(\mathbb{Z}^n, K) \leq 1$ and any $x \in \mathbb{R}^n$ one has $|K \cap (x + \mathbb{Z}^n)| \leq 2^n \mathrm{Vol}_n(K)$.

Proof of Claim.

- Assume $\mathbf{0} \in K$
- Define **equivalence relation** with $x \equiv y \Leftrightarrow x - y \in \mathbb{Z}^n$.

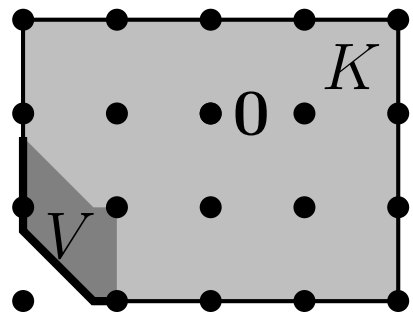


Dadush's lattice point upper bound

Claim. For any convex body $K \subseteq \mathbb{R}^n$ with $\mu(\mathbb{Z}^n, K) \leq 1$ and any $x \in \mathbb{R}^n$ one has $|K \cap (x + \mathbb{Z}^n)| \leq 2^n \mathrm{Vol}_n(K)$.

Proof of Claim.

- Assume $\mathbf{0} \in K$
- Define **equivalence relation** with $x \equiv y \Leftrightarrow x - y \in \mathbb{Z}^n$.
- Let $V = \left\{ x \in K \mid x \leq_{\text{lex}} y \quad \forall y \in (x + \mathbb{Z}^n) \cap K \right\}$ (picks 1 element from each equiv. class)

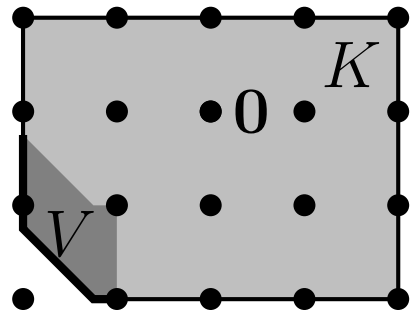


Dadush's lattice point upper bound

Claim. For any convex body $K \subseteq \mathbb{R}^n$ with $\mu(\mathbb{Z}^n, K) \leq 1$ and any $x \in \mathbb{R}^n$ one has $|K \cap (x + \mathbb{Z}^n)| \leq 2^n \mathrm{Vol}_n(K)$.

Proof of Claim.

- Assume $\mathbf{0} \in K$
- Define **equivalence relation** with $x \equiv y \Leftrightarrow x - y \in \mathbb{Z}^n$.
- Let $V = \left\{ x \in K \mid x \leq_{\text{lex}} y \quad \forall y \in (x + \mathbb{Z}^n) \cap K \right\}$ (picks 1 element from each equiv. class)



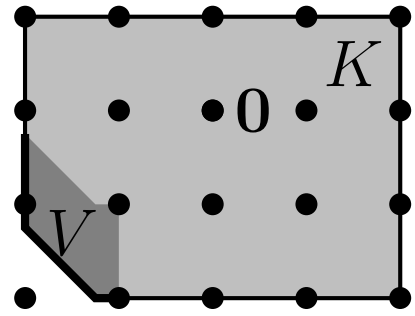
- Picking one per class $\Rightarrow \mathrm{Vol}_n(V) \leq 1$

Dadush's lattice point upper bound

Claim. For any convex body $K \subseteq \mathbb{R}^n$ with $\mu(\mathbb{Z}^n, K) \leq 1$ and any $x \in \mathbb{R}^n$ one has $|K \cap (x + \mathbb{Z}^n)| \leq 2^n \mathrm{Vol}_n(K)$.

Proof of Claim.

- Assume $\mathbf{0} \in K$
- Define **equivalence relation** with $x \equiv y \Leftrightarrow x - y \in \mathbb{Z}^n$.
- Let $V = \left\{ x \in K \mid x \leq_{\text{lex}} y \quad \forall y \in (x + \mathbb{Z}^n) \cap K \right\}$ (picks 1 element from each equiv. class)



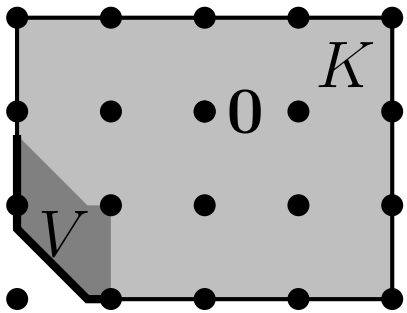
- Picking one per class $\Rightarrow \mathrm{Vol}_n(V) \leq 1$
- For all $x \in \mathbb{R}^n$ one has $(x + \mathbb{Z}^n) \cap K \neq \emptyset \Rightarrow \mathrm{Vol}_n(V) = 1$

Dadush's lattice point upper bound

Claim. For any convex body $K \subseteq \mathbb{R}^n$ with $\mu(\mathbb{Z}^n, K) \leq 1$ and any $x \in \mathbb{R}^n$ one has $|K \cap (x + \mathbb{Z}^n)| \leq 2^n \mathrm{Vol}_n(K)$.

Proof of Claim.

- Assume $\mathbf{0} \in K$
- Define **equivalence relation** with $x \equiv y \Leftrightarrow x - y \in \mathbb{Z}^n$.
- Let $V = \left\{ x \in K \mid x \leq_{\text{lex}} y \quad \forall y \in (x + \mathbb{Z}^n) \cap K \right\}$ (picks 1 element from each equiv. class)



- Picking one per class $\Rightarrow \mathrm{Vol}_n(V) \leq 1$
- For all $x \in \mathbb{R}^n$ one has $(x + \mathbb{Z}^n) \cap K \neq \emptyset \Rightarrow \mathrm{Vol}_n(V) = 1$
- Translates $x + V$ disjoint for $x \in \mathbb{Z}^n$. Hence

$$|K \cap \mathbb{Z}^n| = \sum_{x \in K \cap \mathbb{Z}^n} \underbrace{\mathrm{Vol}_n(x + V)}_{=1} \overset{\text{disj.}}{=} \mathrm{Vol}_n\Big(\bigcup_{x \in K \cap \mathbb{Z}^n} (x + V) \Big) \leq \mathrm{Vol}_n(2K)$$

End of part 1

Open problem 1

Can one even solve Closest Vector problem (or shortest vector) in $\|\cdot\|_2$ in time $2^{O(n)}$ and **polynomial space**?

- In poly space so far only $n^{O(n)}$-time known [Kannan '87]

End of part 1

Open problem 1

Can one even solve Closest Vector problem (or shortest vector) in $\|\cdot\|_2$ in time $2^{O(n)}$ and **polynomial space**?

- In poly space so far only $n^{O(n)}$-time known [Kannan '87]

Thanks for your attention!

Part 2:
The Reverse Minkowski Theorem

Thomas Rothvoss

Based the work
[Regev, Stephens-Davidowitz 2016]

UNIVERSITY *of*
WASHINGTON

Revisiting Minkowski's Theorem

Theorem (Minkowski's Theorem 1889)

Any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ *with* $det(\Lambda) = 1$ *one has* $\lambda_1(\Lambda) \leq \sqrt{n}$.

Revisiting Minkowski's Theorem

Theorem (Minkowski's Theorem 1889)

Any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ *with* $det(\Lambda) = 1$ *one has* $\lambda_1(\Lambda) \leq \sqrt{n}$.

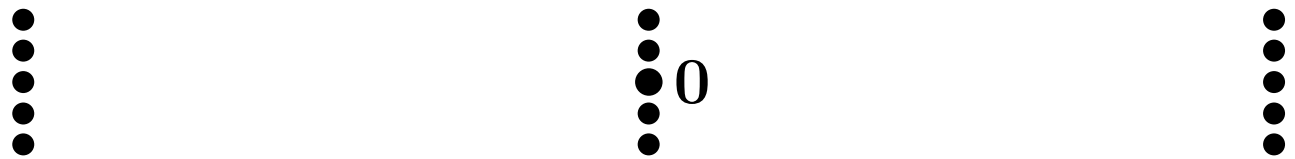
- Can also give a **lower bound** on the number of short vectors.

Revisiting Minkowski's Theorem

Theorem (Minkowski's Theorem 1889)

Any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ *with* $det(\Lambda) = 1$ *one has* $\lambda_1(\Lambda) \leq \sqrt{n}$.

- Can also give a **lower bound** on the number of short vectors. How about an **upper bound**?

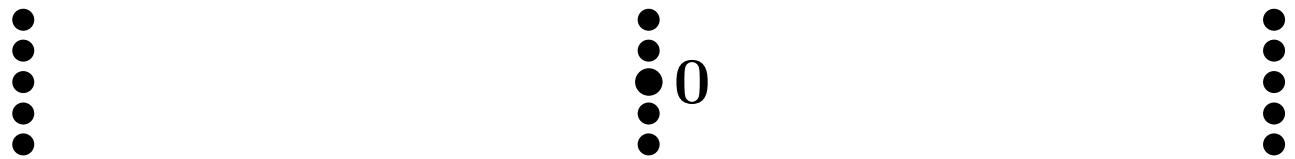


Revisiting Minkowski's Theorem

Theorem (Minkowski's Theorem 1889)

Any full rank lattice $\Lambda \subseteq \mathbb{R}^n$ *with* $det(\Lambda) = 1$ *one has* $\lambda_1(\Lambda) \leq \sqrt{n}$.

- Can also give a **lower bound** on the number of short vectors. How about an **upper bound**?



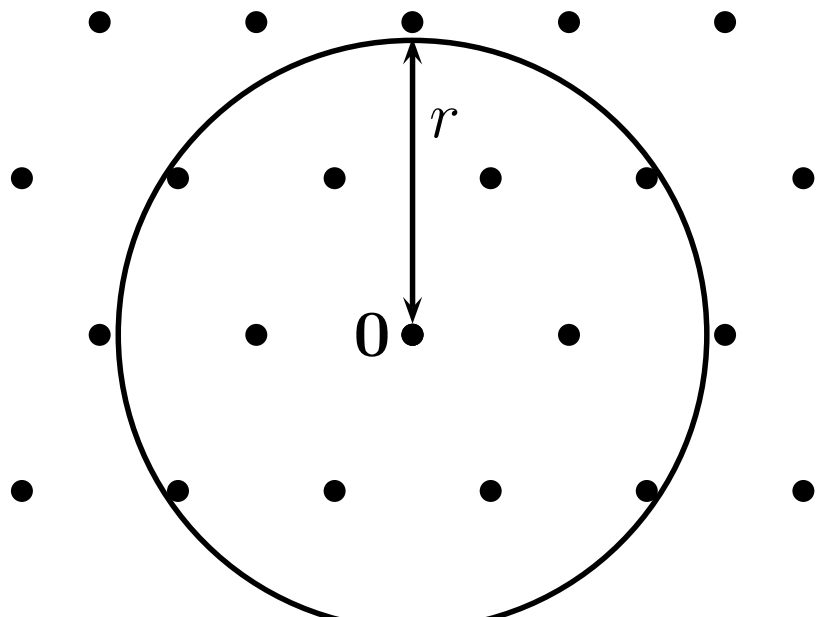
- What if $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$?

Warmup

Lemma

Let $\Lambda \subseteq \mathbb{R}^n$ be lattice with $\det(\Lambda') \geq 1 \; \forall \Lambda' \subseteq \Lambda$. For all $r \geq 1$ one has $N := |\Lambda \cap rB_2^n| \leq (3r)^n$

Proof.



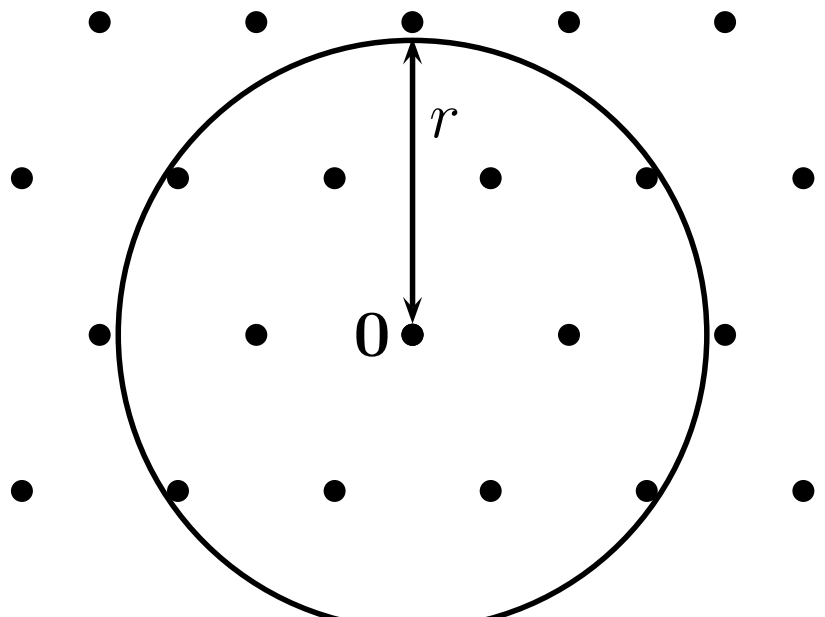
Warmup

Lemma

Let $\Lambda \subseteq \mathbb{R}^n$ be lattice with $\det(\Lambda') \geq 1 \; \forall \Lambda' \subseteq \Lambda$. For all $r \geq 1$ one has $N := |\Lambda \cap rB_2^n| \leq (3r)^n$

Proof.

- Clearly $\lambda_1(\Lambda) \geq 1$.



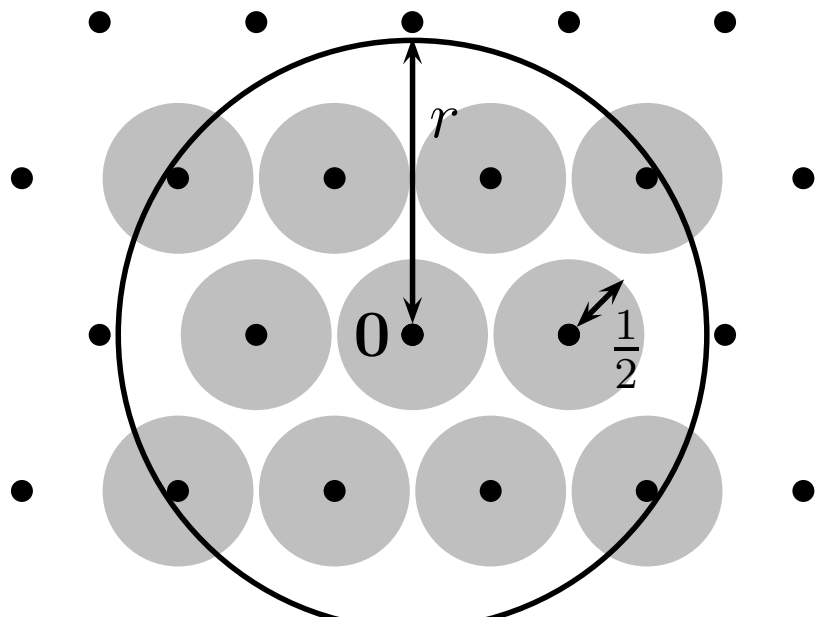
Warmup

Lemma

Let $\Lambda \subseteq \mathbb{R}^n$ be lattice with $\det(\Lambda') \geq 1 \; \forall \Lambda' \subseteq \Lambda$. For all $r \geq 1$ one has $N := |\Lambda \cap rB_2^n| \leq (3r)^n$

Proof.

- Clearly $\lambda_1(\Lambda) \geq 1$.
- Can pack N disjoint balls of radius $\frac{1}{2}$ into $(r + \frac{1}{2})B_2^n$.



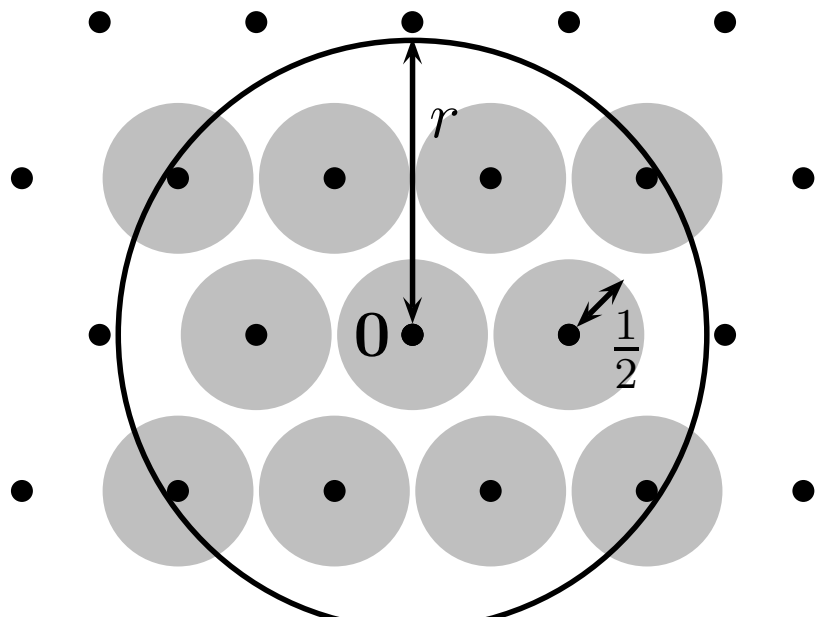
Warmup

Lemma

Let $\Lambda \subseteq \mathbb{R}^n$ be lattice with $\det(\Lambda') \geq 1 \; \forall \Lambda' \subseteq \Lambda$. For all $r \geq 1$ one has $N := |\Lambda \cap rB_2^n| \leq (3r)^n$

Proof.

- Clearly $\lambda_1(\Lambda) \geq 1$.
- Can pack N disjoint balls of radius $\frac{1}{2}$ into $(r + \frac{1}{2})B_2^n$. So $N \cdot \mathrm{Vol}_n(\frac{1}{2}B_2^n) \leq \mathrm{Vol}_n((r + \frac{1}{2})B_2^n)$. Then $N \leq (3r)^n$. □



The Reverse Minkowski Theorem

Reverse Minkowski Theorem (Regev, Stephens-Da.)

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for $s = \Theta(\log n)$,

$$\rho_{1/s}(\Lambda) = \sum_{x \in \Lambda} \exp(-\pi s^2 \|x\|_2^2) \leq \frac{3}{2}$$

- Means for all $r \geq 1$, $|\Lambda \cap rB_2^n| \leq n^{\Theta(\log(n)) \cdot r^2}$ (i.e. # of points grows **quasi-polynomial** in r)

The Reverse Minkowski Theorem

Reverse Minkowski Theorem (Regev, Stephens-Da.)

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for $s = \Theta(\log n)$,

$$\rho_{1/s}(\Lambda) = \sum_{x \in \Lambda} \exp(-\pi s^2 \|x\|_2^2) \leq \frac{3}{2}$$

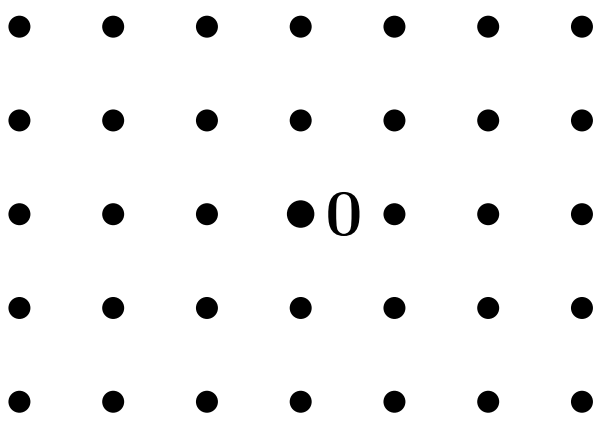
- Means for all $r \geq 1$, $|\Lambda \cap rB_2^n| \leq n^{\Theta(\log(n)) \cdot r^2}$ (i.e. # of points grows **quasi-polynomial** in r)
- First conjectured by [Dadush, Regev 2016].
- Conjectured that $s = \Theta(\sqrt{\log(n)})$ is enough which would give $|\Lambda \cap rB_2^n| \leq n^{O(r^2)}$ for $r \geq 1$.

Stable lattice

Definition

A lattice Λ is called **stable** if $\det(\Lambda) = 1$ and $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$.

Example: $\mathbb{Z}^n$ is stable.

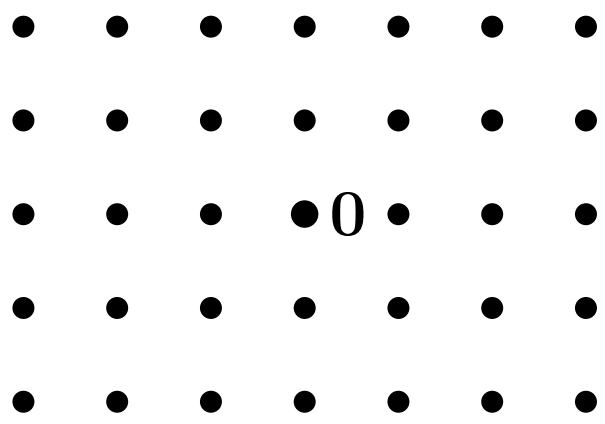


Stable lattice

Definition

A lattice Λ is called **stable** if $\det(\Lambda) = 1$ and $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$.

Example: $\mathbb{Z}^n$ is stable.

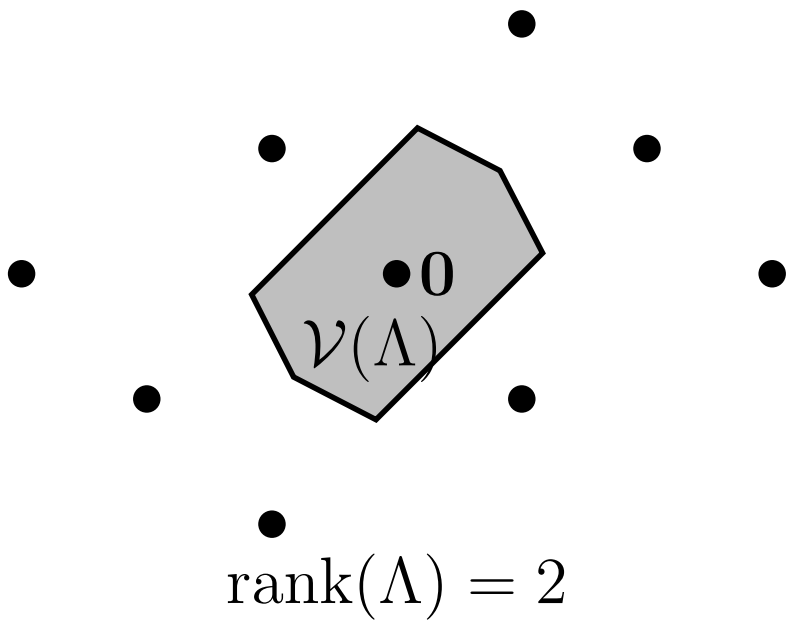


- It suffices to prove Reverse Minkowski for stable lattices (later more on that..).

The Voronoi cell

- **Recap:** Let $\Lambda \subseteq \mathbb{R}^n$ be lattice. The **Voronoi cell** is

$$\mathcal{V}(\Lambda) = \{x \in \mathbb{R}^n : \|x\|_2 \leq \|x - v\|_2 \; \forall v \in \Lambda \setminus \{\mathbf{0}\}\}$$

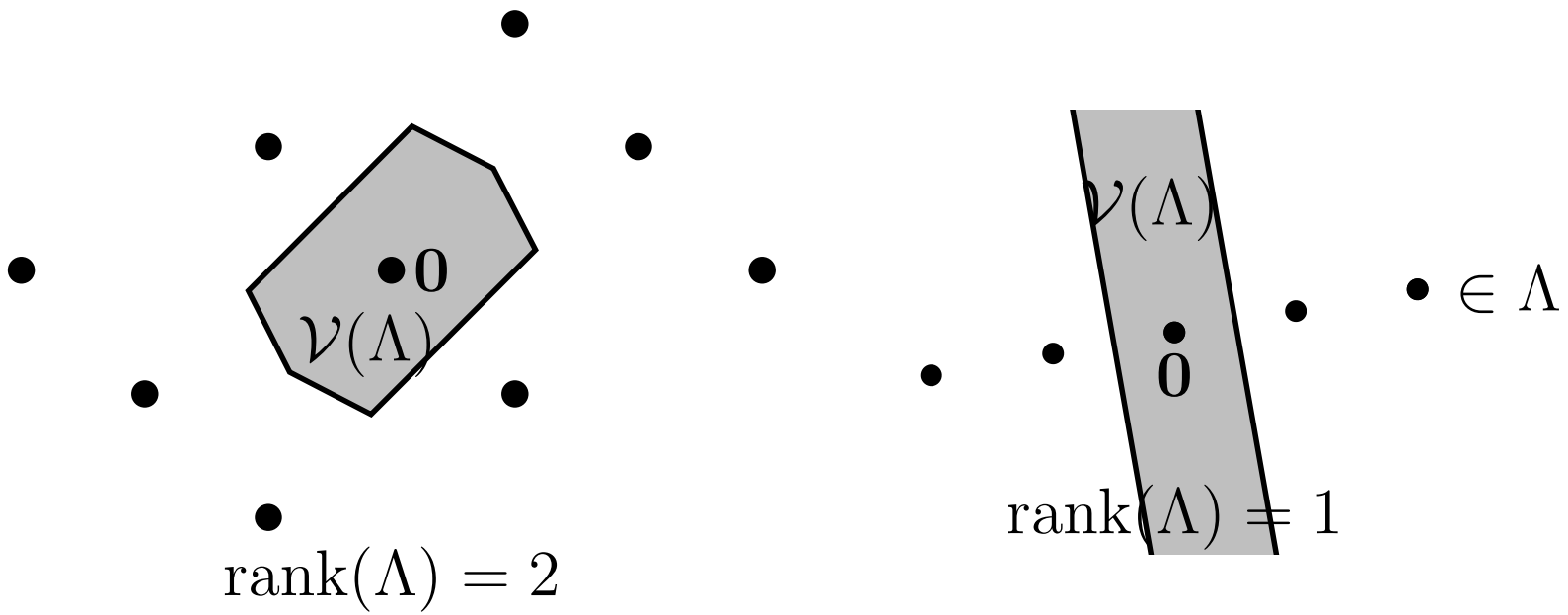


$\text{rank}(\Lambda) = 2$

The Voronoi cell

- **Recap:** Let $\Lambda \subseteq \mathbb{R}^n$ be lattice. The **Voronoi cell** is

$$\mathcal{V}(\Lambda) = \{x \in \mathbb{R}^n : \|x\|_2 \leq \|x - v\|_2 \; \forall v \in \Lambda \setminus \{\mathbf{0}\}\}$$



$\text{rank}(\Lambda) = 2$

$\text{rank}(\Lambda) = 1$

Volume of the Voronoi cell

Lemma

A full rank stable lattice Λ *has* $Vol_n(\mathcal{V}(\Lambda)) = 1$.

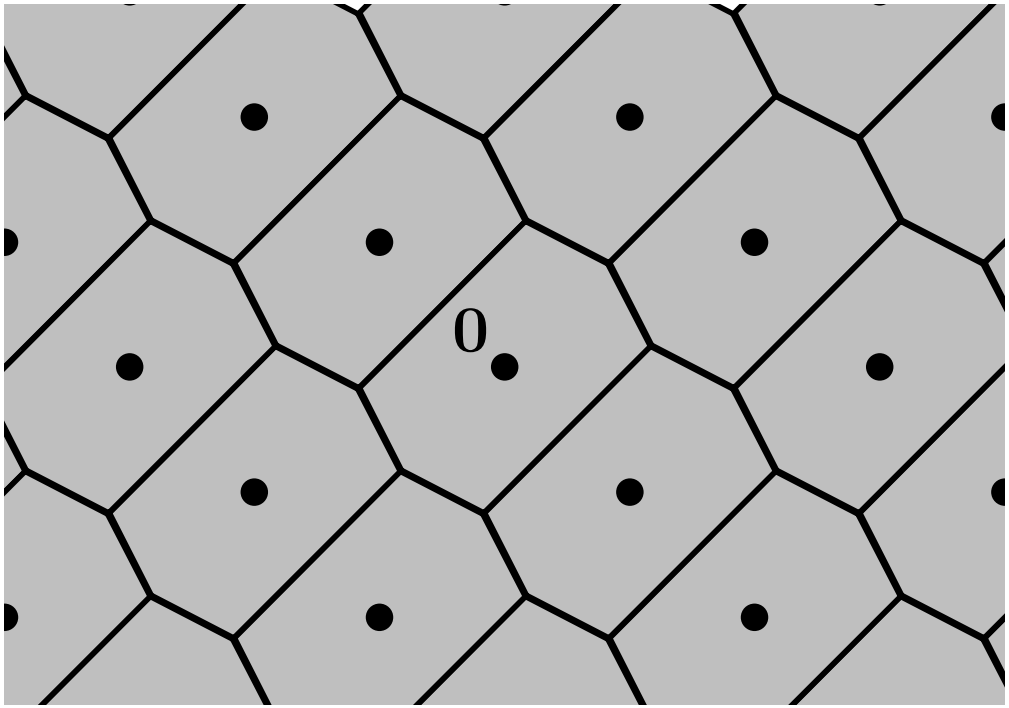
Volume of the Voronoi cell

Lemma

A full rank stable lattice Λ has $Vol_n(\mathcal{V}(\Lambda)) = 1$.

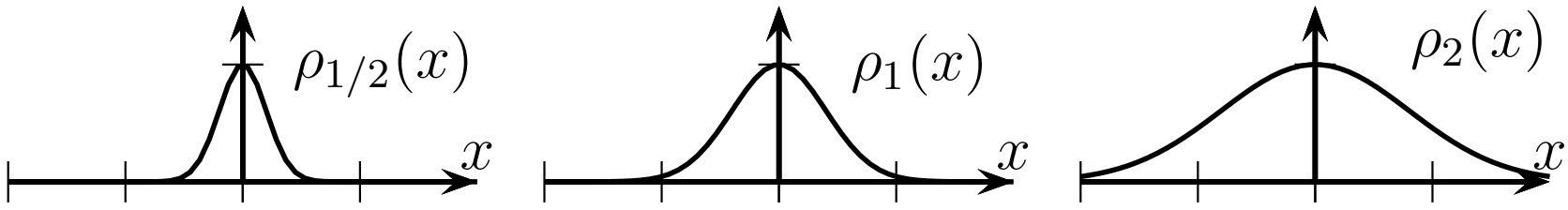
Proof.

- Translates $v + \mathcal{V}(\Lambda)$ tile $\mathbb{R}^n$ and density is $\frac{1}{\det(\Lambda)} = 1$.



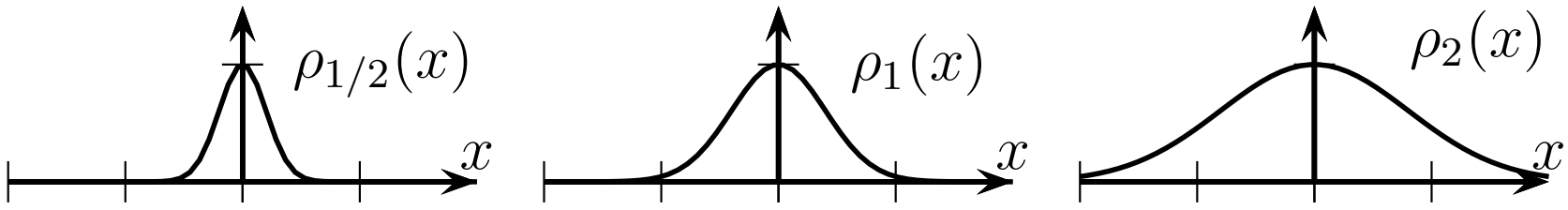
Some notation

- **Gaussian density** $\rho_s(x) = \exp(-\pi \|x/s\|_2^2)$



Some notation

- **Gaussian density** $\rho_s(x) = \exp(-\pi\|x/s\|_2^2)$

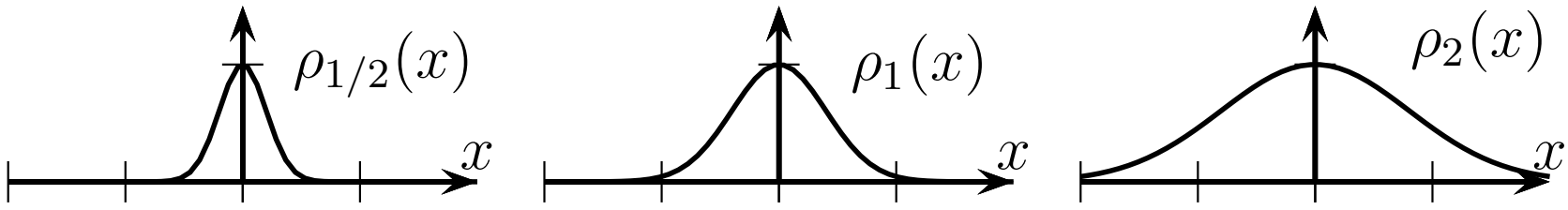


- **Gaussian measure**

$$\gamma_{n,s}(K) = \frac{1}{\rho_s(\mathbb{R}^n)} \int_K \rho_s(x)dx$$

Some notation

- **Gaussian density** $\rho_s(x) = \exp(-\pi\|x/s\|_2^2)$



- **Gaussian measure**

$$\gamma_{n,s}(K) = \frac{1}{\rho_s(\mathbb{R}^n)} \int_K \rho_s(x)dx$$

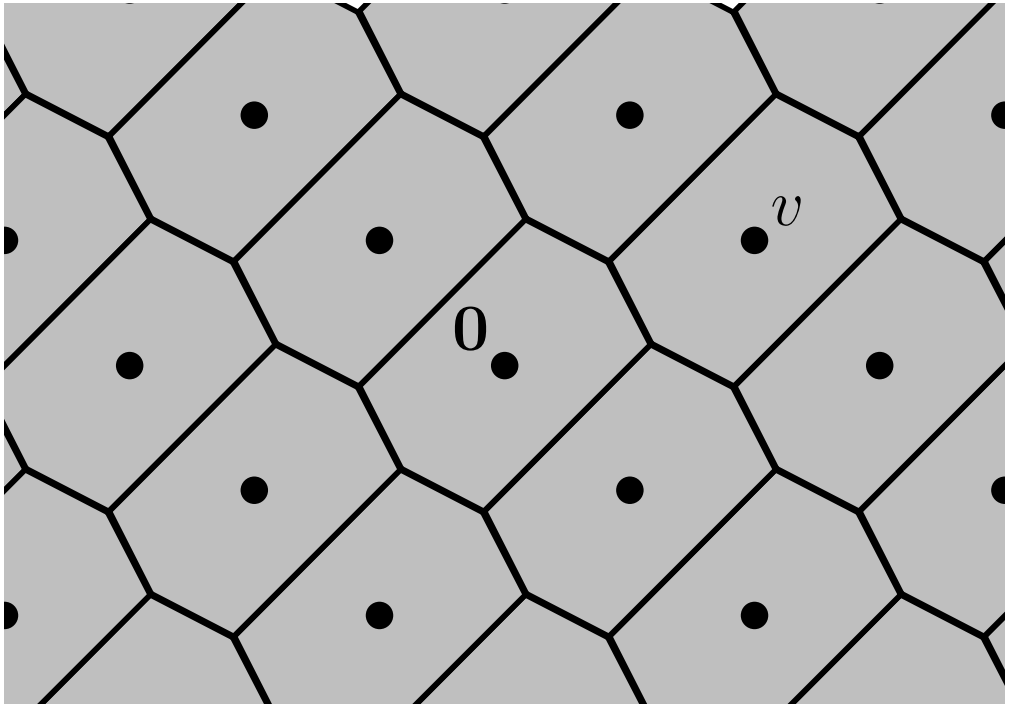
- **Standard gaussian measure**

$$\gamma_n(K) = \frac{1}{(2\pi)^{n/2}} \int_K \exp\Big(-\frac{\|x\|_2^2}{2}\Big)dx = \gamma_{n,\sqrt{2\pi}}(K)$$

Voronoi cell large $\Rightarrow$ $\rho(\Lambda)$ small

Lemma

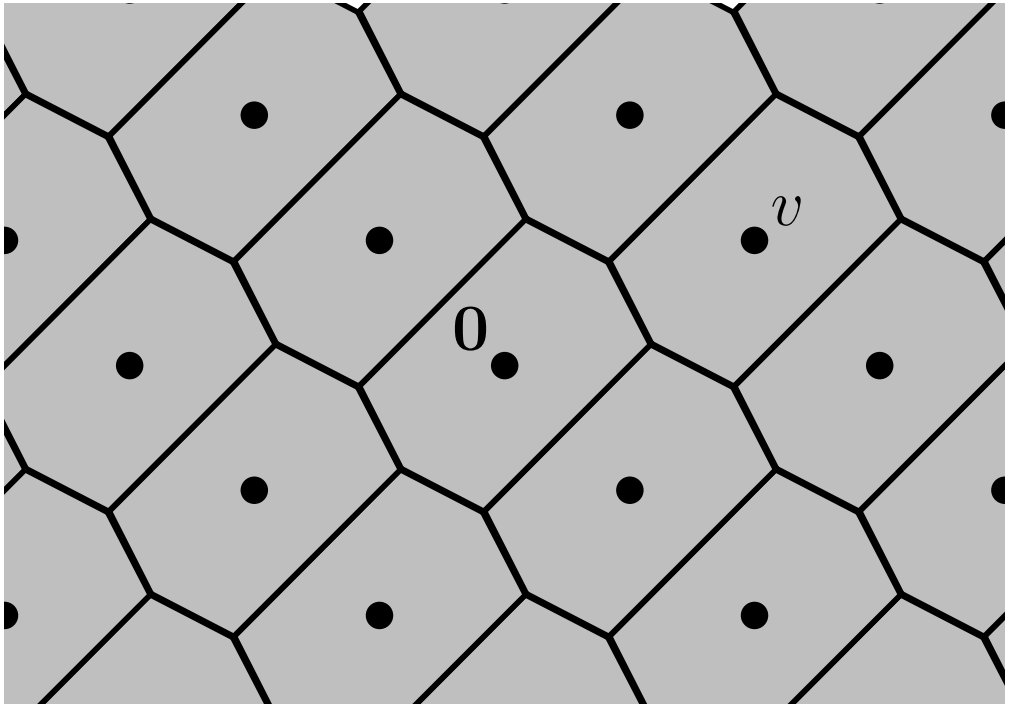
For any lattice $\Lambda \subseteq \mathbb{R}^n$ and $s > 0$, $\rho_s(\Lambda) \cdot \gamma_{n,s}(\mathcal{V}(\Lambda)) \leq 1$.



Voronoi cell large $\Rightarrow$ $\rho(\Lambda)$ small

Lemma

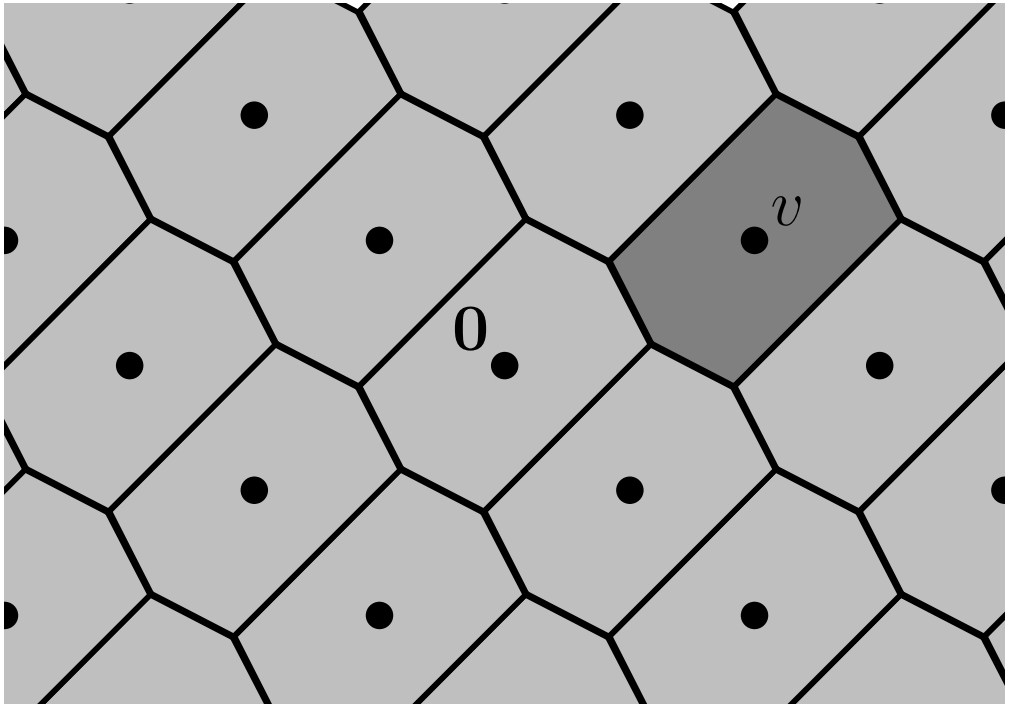
For any lattice $\Lambda \subseteq \mathbb{R}^n$, $\rho_1(\Lambda) \cdot \gamma_{n,1}(\mathcal{V}(\Lambda)) \leq 1$.



Voronoi cell large $\Rightarrow$ $\rho(\Lambda)$ small

Lemma

For any lattice $\Lambda \subseteq \mathbb{R}^n$, $\rho_1(\Lambda) \cdot \gamma_{n,1}(\mathcal{V}(\Lambda)) \leq 1$.

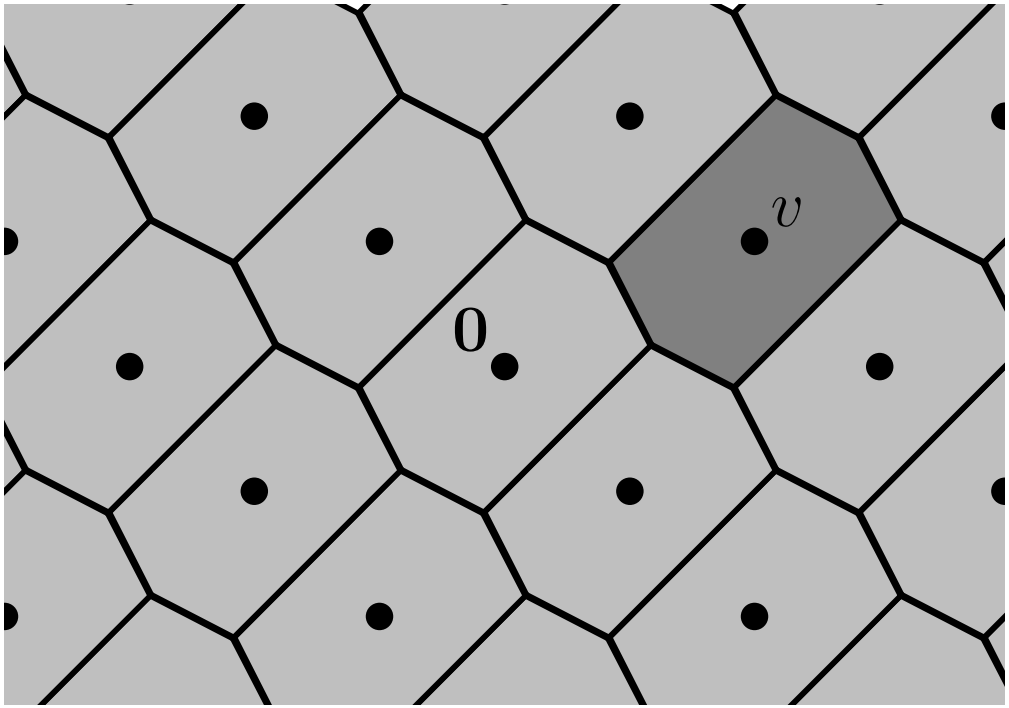


- For $v \in \Lambda$ one has $\gamma_{n,1}(v + \mathcal{V}) \geq e^{-\pi\|v\|_2^2}\gamma_{n,1}(\mathcal{V})$.

Voronoi cell large $\Rightarrow$ $\rho(\Lambda)$ small

Lemma

For any lattice $\Lambda \subseteq \mathbb{R}^n$, $\rho_1(\Lambda) \cdot \gamma_{n,1}(\mathcal{V}(\Lambda)) \leq 1$.



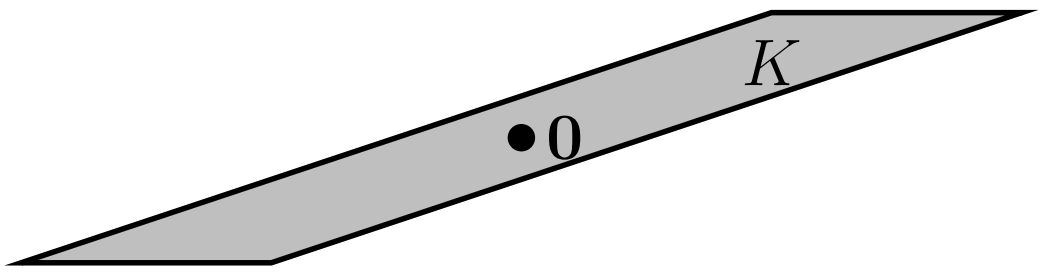
- For $v \in \Lambda$ one has $\gamma_{n,1}(v + \mathcal{V}) \geq e^{-\pi\|v\|_2^2}\gamma_{n,1}(\mathcal{V})$.
- Summing gives $1 = \sum_{v\in\Lambda} \gamma_{n,1}(v + \mathcal{V}) \geq \rho_1(\Lambda) \cdot \gamma_{n,1}(\mathcal{V})$ $\square$

Convex geometry

- Is it true that a symmetric convex body K with $\mathrm{Vol}_n(K) = 1$ has large Gaussian measure (after scaling with $\Theta(\log n)$?
- Maybe, maybe not..

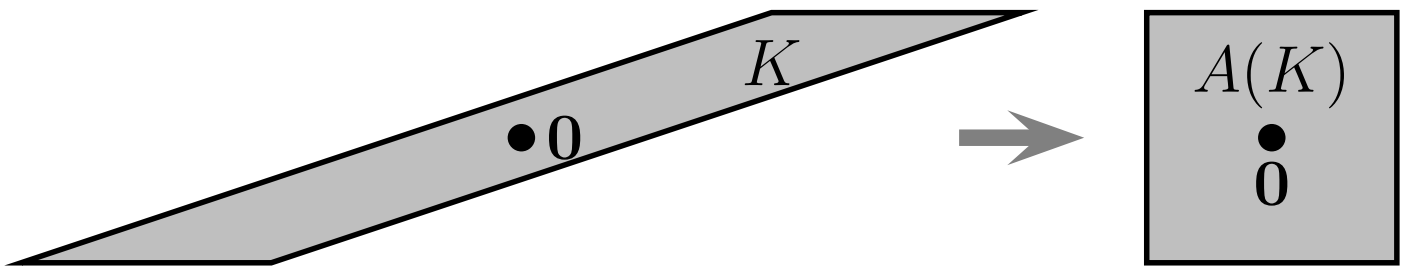
Convex geometry

- Is it true that a symmetric convex body K with $\mathrm{Vol}_n(K) = 1$ has large Gaussian measure (after scaling with $\Theta(\log n)$?
- Maybe, maybe not..



Convex geometry

- Is it true that a symmetric convex body K with $\mathrm{Vol}_n(K) = 1$ has large Gaussian measure (after scaling with $\Theta(\log n)$?
- Maybe, maybe not..



Theorem

For any symmetric convex body $K \subseteq \mathbb{R}^n$ with $Vol_n(K) = 1$ there is a matrix $A \in \mathbb{R}^{n \times n}$ with $|\det(A)| = 1$ so that $\gamma_n(\Theta(\log n) \cdot A(K)) \geq \frac{2}{3}$.

Isotropic position

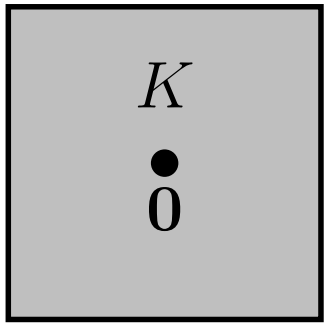
Definition

A symmetric convex body $K \subseteq \mathbb{R}^n$ is in **isotropic s-Gaussian position** if

$$\int_K \rho_s(x) \cdot xx^T dx = \alpha I_n$$

for some $\alpha > 0$.

- Means Gaussian mass is equally spread in all directions.

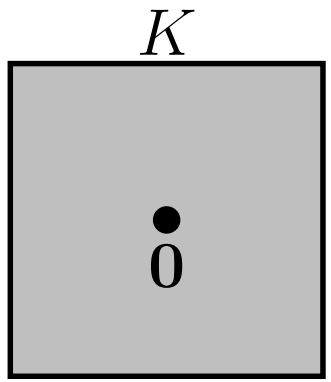


Isotropic position (2)

- If K is in isotropic position, then K maximizes Gaussian measure under volume-preserving rescaling:

Theorem (Bobkov 2011)

Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body and let $s > 0$. If K is in isotropic s-Gaussian position then $\gamma_{n,s}(K) \geq \gamma_{n,s}(A(K))$ for all $A \in \mathbb{R}^{n \times n}$ with $|\det(A)| = 1$.

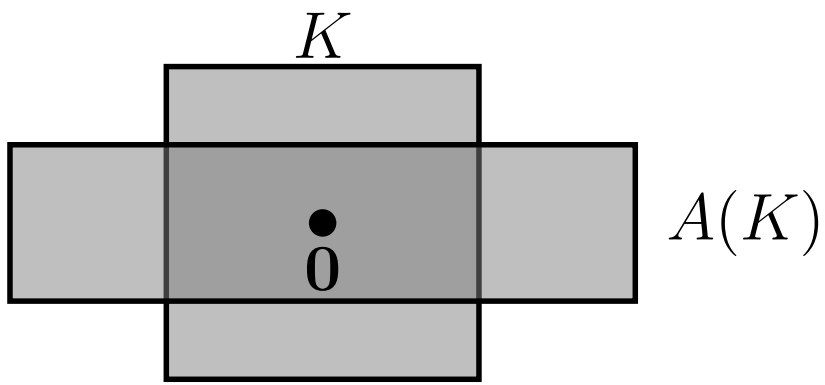


Isotropic position (2)

- If K is in isotropic position, then K maximizes Gaussian measure under volume-preserving rescaling:

Theorem (Bobkov 2011)

Let $K \subseteq \mathbb{R}^n$ be a symmetric convex body and let $s > 0$. If K is in isotropic s-Gaussian position then $\gamma_{n,s}(K) \geq \gamma_{n,s}(A(K))$ for all $A \in \mathbb{R}^{n \times n}$ with $|\det(A)| = 1$.



The main technical theorem

Theorem

For stable lattice Λ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

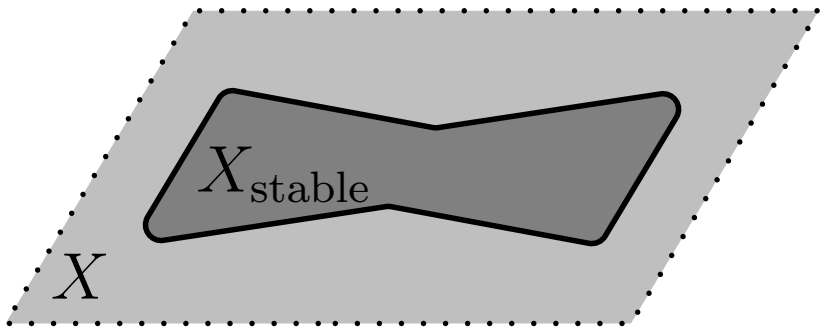
The main technical theorem

Theorem

For stable lattice Λ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Consider

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$



The main technical theorem

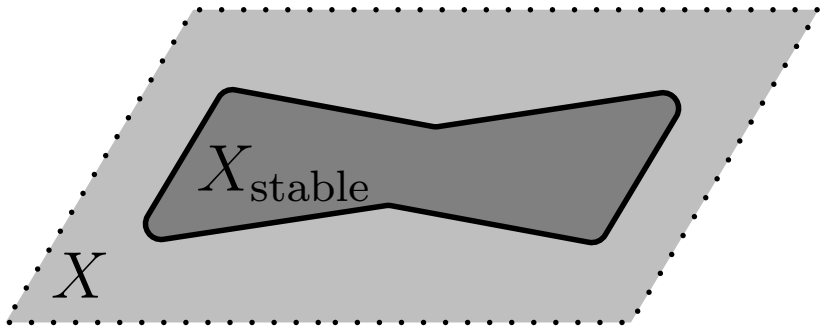
Theorem

For stable lattice Λ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Consider

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

- Fix $B \in X_{\text{stable}}$ min. $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.



The main technical theorem

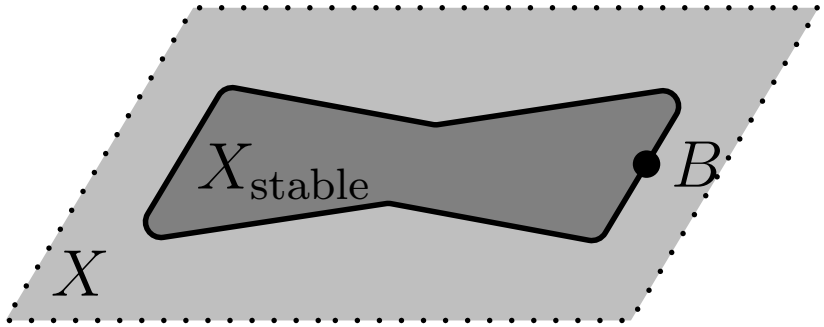
Theorem

For stable lattice Λ one has $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Consider

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

- Fix $B \in X_{\text{stable}}$ min. $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.



- **Case (I).** B is on boundary of X_{stable}.

The main technical theorem

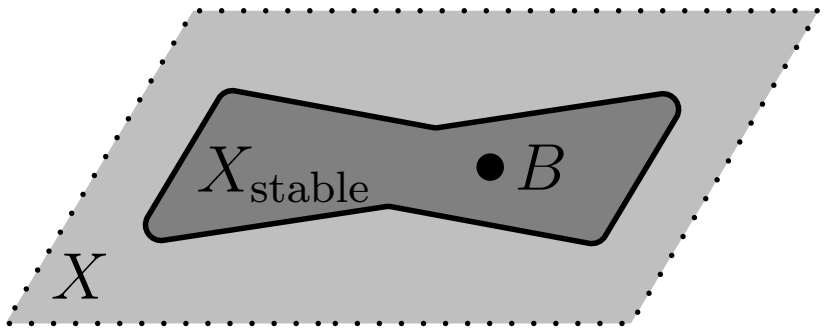
Theorem

For stable lattice Λ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Consider

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

- Fix $B \in X_{\text{stable}}$ min. $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.



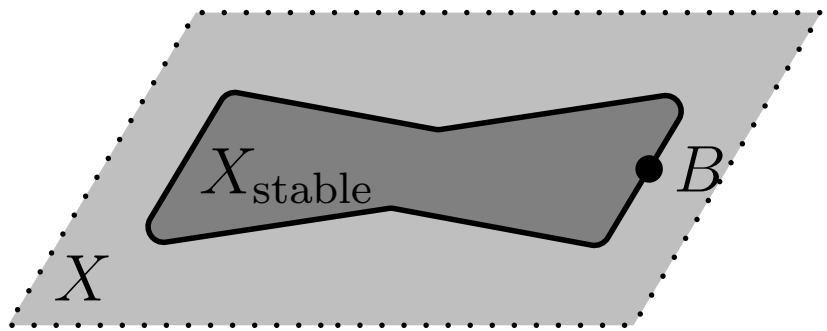
- **Case (I).** B is on boundary of X_{stable}.
- **Case (II).** B not on boundary of X_{stable}.

The main technical theorem (2)

Recall:

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

Case (I). B is on the boundary on X_{stable}.



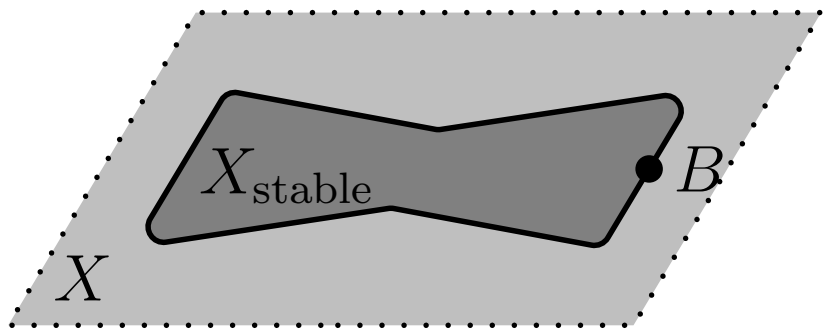
The main technical theorem (2)

Recall:

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

Case (I). B is on the boundary on X_{stable}.

- Then $\exists$ sublattice $\Lambda' \subseteq \Lambda$ with $\det(\Lambda') = 1$.



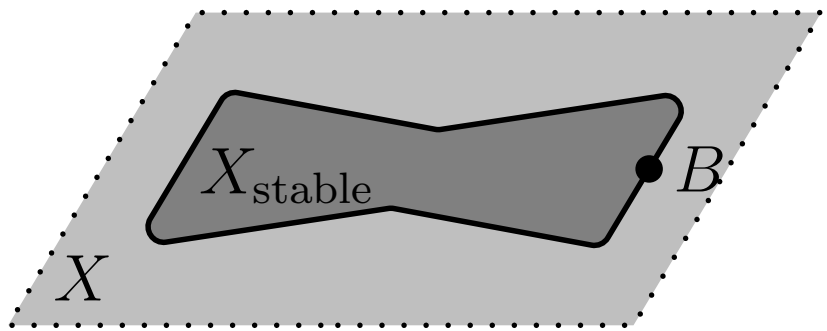
The main technical theorem (2)

Recall:

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

Case (I). B is on the boundary on X_{stable}.

- Then $\exists$ sublattice $\Lambda' \subseteq \Lambda$ with $\det(\Lambda') = 1$.
- Λ' also stable. Case incomplete for now... but we made progress..



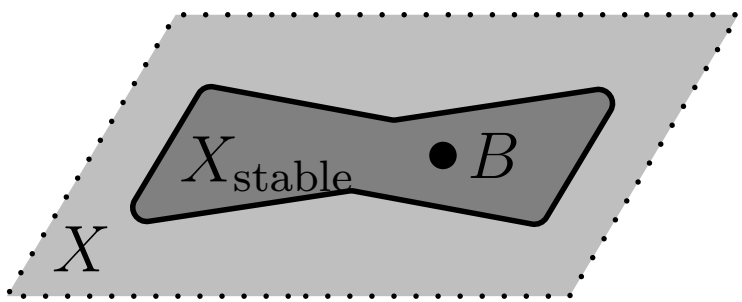
The main technical theorem (3)

Recall

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

- $B \in X_{\text{stable}}$ minimizer of $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.

Case (II). B not on the boundary of X_{stable}



The main technical theorem (3)

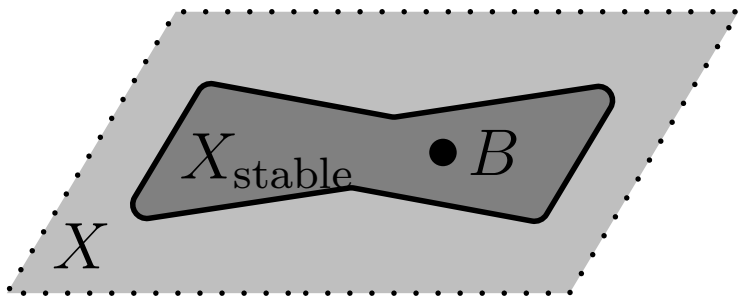
Recall

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

- $B \in X_{\text{stable}}$ minimizer of $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.

Case (II). B not on the boundary of X_{stable}

- Then B is **local minimum** of function $F : X \to \mathbb{R}$



The main technical theorem (3)

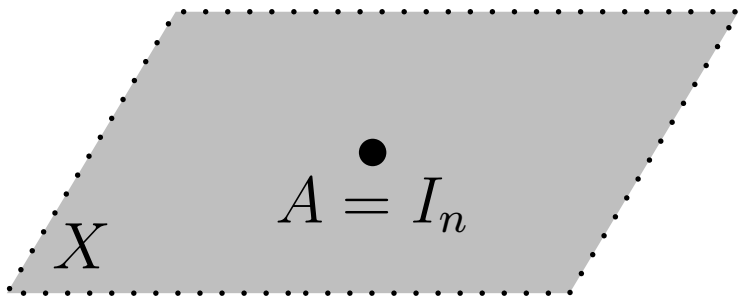
Recall

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \le 3n^{2.5}\} \end{aligned}$$

- $B \in X_{\text{stable}}$ minimizer of $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.

Case (II). B not on the boundary of X_{stable}

- Then B is **local minimum** of function $F : X \to \mathbb{R}$



- Set $\Lambda := \Lambda(B)$.
- Let $G(A) := \frac{F(AB)}{|\det(A)|} = \frac{1}{|\det(A)|}\gamma_n(\Theta(\log n) \cdot \mathcal{V}(A(\Lambda)))$

The main technical theorem (3)

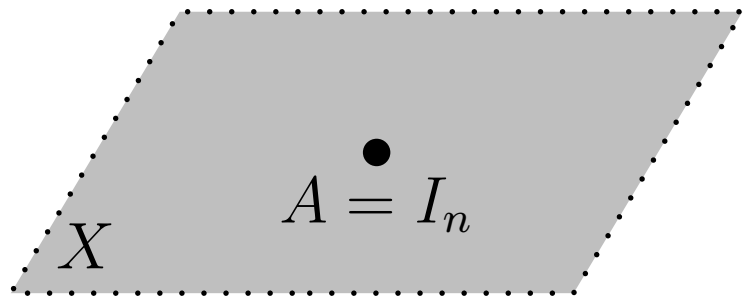
Recall

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

- $B \in X_{\text{stable}}$ minimizer of $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.

Case (II). B not on the boundary of X_{stable}

- Then B is **local minimum** of function $F : X \to \mathbb{R}$



- Set $\Lambda := \Lambda(B)$.
- Let $G(A) := \frac{F(AB)}{|\det(A)|} = \frac{1}{|\det(A)|}\gamma_n(\Theta(\log n) \cdot \mathcal{V}(A(\Lambda)))$
- Then $G_{|X}$ has a **local minimum** at I_n

The main technical theorem (3)

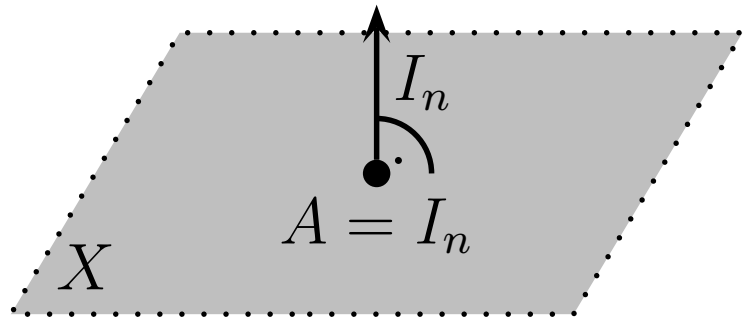
Recall

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

- $B \in X_{\text{stable}}$ minimizer of $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.

Case (II). B not on the boundary of X_{stable}

- Then B is **local minimum** of function $F : X \to \mathbb{R}$



- Set $\Lambda := \Lambda(B)$.
- Let $G(A) := \frac{F(AB)}{|\det(A)|} = \frac{1}{|\det(A)|}\gamma_n(\Theta(\log n) \cdot \mathcal{V}(A(\Lambda)))$
- Then $G_{|X}$ has a **local minimum** at I_n
- X determined by $\det(A) = 1$ and $(\nabla_A \det(A))_{|A=I_n} = I_n$

The main technical theorem (3)

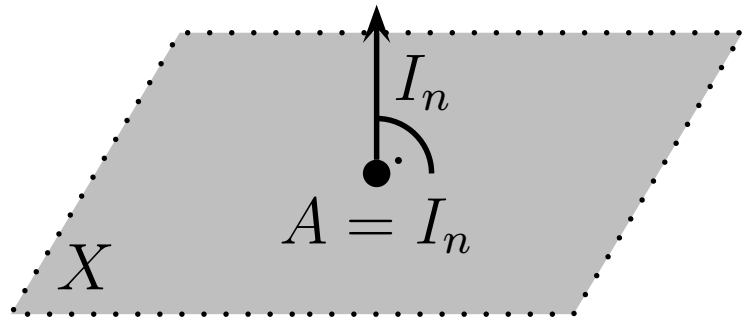
Recall

$$\begin{aligned} X &:= \{B \in \mathbb{R}^{n\times n} \mid |\det(B)| = 1\} \\ X_{\text{stable}} &:= \{B \in \mathbb{R}^{n\times n} \mid \Lambda(B) \text{ is stable and } \|B\|_F \leq 3n^{2.5}\} \end{aligned}$$

- $B \in X_{\text{stable}}$ minimizer of $F(B) := \gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda(B)))$.

Case (II). B not on the boundary of X_{stable}

- Then B is **local minimum** of function $F : X \to \mathbb{R}$



- Set $\Lambda := \Lambda(B)$.
- Let $G(A) := \frac{F(AB)}{|\det(A)|} = \frac{1}{|\det(A)|}\gamma_n(\Theta(\log n) \cdot \mathcal{V}(A(\Lambda)))$
- Then $G_{|X}$ has a **local minimum** at I_n
- X determined by $\det(A) = 1$ and $(\nabla_A \det(A))_{|A=I_n} = I_n$
- Then $\nabla_A G(A)_{|A=I_n} = \lambda I_n$ for some $\lambda \in \mathbb{R}$

The main technical theorem (4)

The main technical theorem (4)

Theorem

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ *and lattice* $\Lambda \subseteq \mathbb{R}^n$, *let*

$$G(A) \quad := \quad \frac{1}{|\det(A)|} \int_{\mathcal{V}(A(\Lambda))} f(\|x\|_2^2) dx$$

Then

$$(\nabla_A G(A))_{|A=I_n} = 2 \int_{\mathcal{V}(\Lambda)} f'(\|x\|_2^2) x x^T dx$$

The main technical theorem (4)

Theorem

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ *and lattice* $\Lambda \subseteq \mathbb{R}^n$, *let*

$$G(A) \quad := \quad \frac{1}{|\det(A)|} \int_{\mathcal{V}(A(\Lambda))} f(\|x\|_2^2) dx$$

Then

$$(\nabla_A G(A))_{|A=I_n} = 2 \int_{\mathcal{V}(\Lambda)} f'(\|x\|_2^2) x x^T dx$$

- Then set $f(z) := \frac{e^{-\pi t^2 z}}{\rho_{1/t}(\mathbb{R}^n)}$ with $f'(z) = -\frac{\pi t^2}{\rho_{1/t}(\mathbb{R}^n)} \cdot f(z)$

$$\lambda I_n \quad = \quad \nabla_A (G(A))_{|A=I_n} = 2 \int_{\mathcal{V}(\Lambda)} f'(\|x\|_2^2) x x^T dx$$

The main technical theorem (4)

Theorem

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ *and lattice* $\Lambda \subseteq \mathbb{R}^n$, *let*

$$G(A) \quad := \quad \frac{1}{|\det(A)|} \int_{\mathcal{V}(A(\Lambda))} f(\|x\|_2^2) dx$$

Then

$$(\nabla_A G(A))_{|A=I_n} = 2 \int_{\mathcal{V}(\Lambda)} f'(\|x\|_2^2) x x^T dx$$

- Then set $f(z) := \frac{e^{-\pi t^2 z}}{\rho_{1/t}(\mathbb{R}^n)}$ with $f'(z) = -\frac{\pi t^2}{\rho_{1/t}(\mathbb{R}^n)} \cdot f(z)$

$$\begin{aligned} \lambda I_n \quad &= \quad \nabla_A (G(A))_{|A=I_n} = 2 \int_{\mathcal{V}(\Lambda)} f'(\|x\|_2^2) x x^T dx \\ &= \quad -\frac{2\pi t^2}{\rho_{1/t}(\mathbb{R}^n)} \int_{\mathcal{V}(\Lambda)} \rho_{1/t}(x) x x^T dx \end{aligned}$$

The main technical theorem (4)

Theorem

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ *and lattice* $\Lambda \subseteq \mathbb{R}^n$, *let*

$$G(A) \quad := \quad \frac{1}{|\det(A)|} \int_{\mathcal{V}(A(\Lambda))} f(\|x\|_2^2) dx$$

Then

$$(\nabla_A G(A))_{|A=I_n} = 2 \int_{\mathcal{V}(\Lambda)} f'(\|x\|_2^2) x x^T dx$$

- Then set $f(z) := \frac{e^{-\pi t^2 z}}{\rho_{1/t}(\mathbb{R}^n)}$ with $f'(z) = -\frac{\pi t^2}{\rho_{1/t}(\mathbb{R}^n)} \cdot f(z)$

$$\begin{aligned} \lambda I_n \quad &= \quad \nabla_A (G(A))_{|A=I_n} = 2 \int_{\mathcal{V}(\Lambda)} f'(\|x\|_2^2) x x^T dx \\ &= \quad - \frac{2\pi t^2}{\rho_{1/t}(\mathbb{R}^n)} \int_{\mathcal{V}(\Lambda)} \rho_{1/t}(x) x x^T dx \end{aligned}$$

- $\mathcal{V}(\Lambda)$ is in **Gaussian isotropic position!**

The main technical theorem (5)

- $\mathcal{V}(\Lambda)$ is in **Gaussian isotropic position!**

The main technical theorem (5)

- $\mathcal{V}(\Lambda)$ is in **Gaussian isotropic position!**
- By Bobkov: $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \gamma_n(\Theta(\log n) \cdot A(\mathcal{V}(\Lambda)))$ for any A with $\det(A) = 1$

The main technical theorem (5)

- $\mathcal{V}(\Lambda)$ is in **Gaussian isotropic position!**
- By Bobkov: $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \gamma_n(\Theta(\log n) \cdot A(\mathcal{V}(\Lambda)))$ for any A with $\det(A) = 1$
- Pick A so that $\gamma_n(\Theta(\log n) \cdot A(\mathcal{V}(\Lambda))) \geq \frac{2}{3}$.

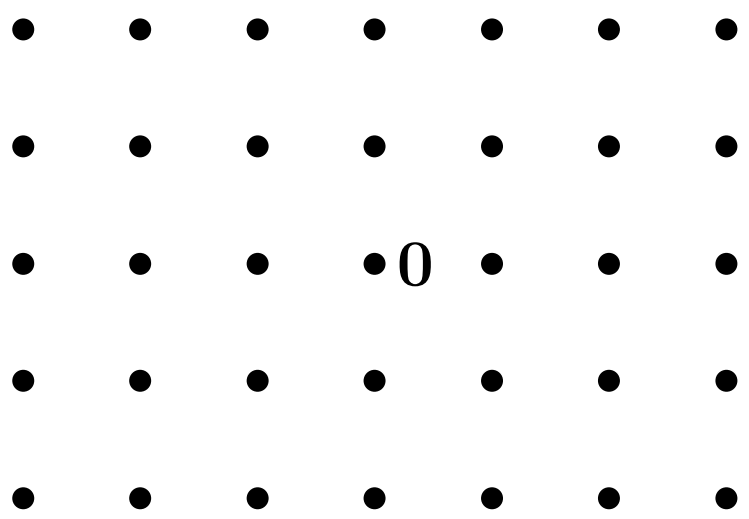
The main technical theorem (5)

- $\mathcal{V}(\Lambda)$ is in **Gaussian isotropic position!**
- By Bobkov: $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \gamma_n(\Theta(\log n) \cdot A(\mathcal{V}(\Lambda)))$ for any A with $\det(A) = 1$
- Pick A so that $\gamma_n(\Theta(\log n) \cdot A(\mathcal{V}(\Lambda))) \geq \frac{2}{3}$.
- Then $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \gamma_n(\Theta(\log n) \cdot A(\mathcal{V}(\Lambda))) \geq \frac{2}{3}$. **Done!**

Quotient lattices

Definition

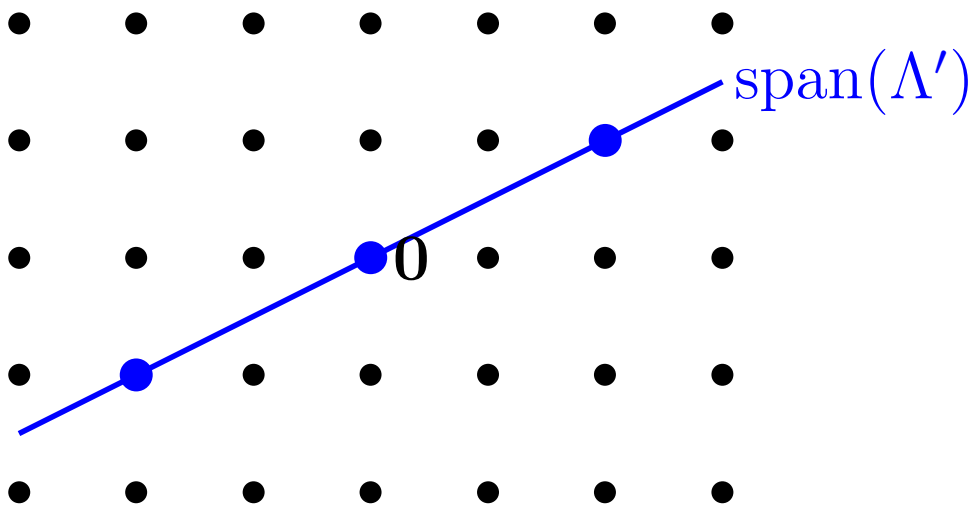
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$.



Quotient lattices

Definition

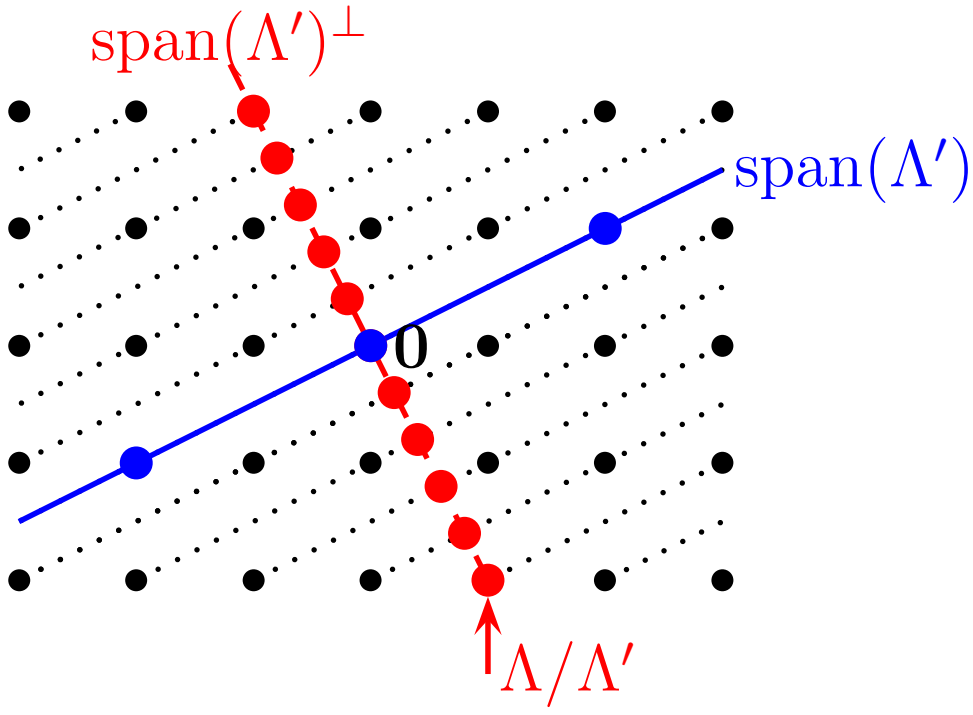
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$.



Quotient lattices

Definition

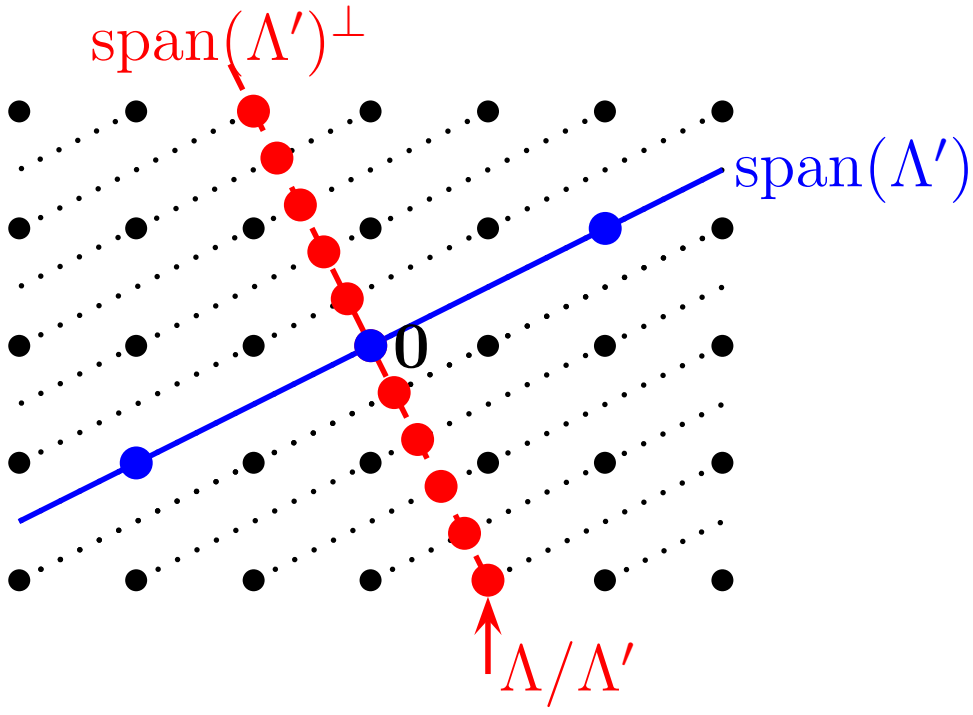
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$.



Quotient lattices

Definition

Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$.



- **Intuition:** We can factor Λ into Λ' and Λ/Λ'

Quotient lattices (2)

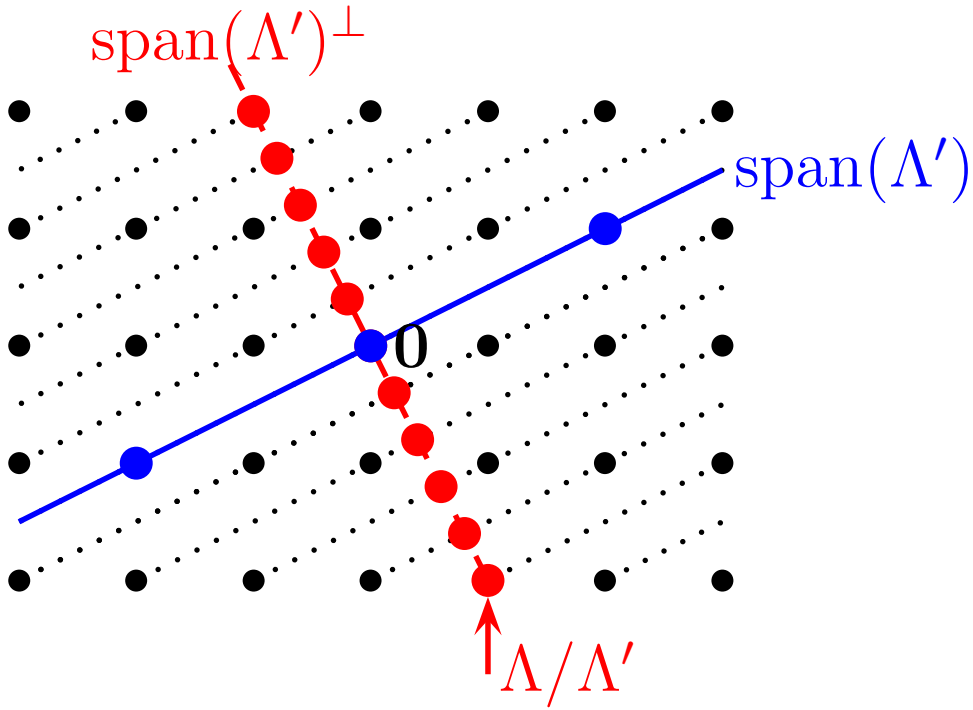
Lemma

For lattice Λ and a primitive sublattice $\Lambda' \subseteq \Lambda$:

(i) $\det(\Lambda) = \det(\Lambda') \cdot \det(\Lambda/\Lambda')$

(ii) *For any* $s > 0$, $\rho_s(\Lambda) \leq \rho_s(\Lambda') \cdot \rho_s(\Lambda/\Lambda')$

(iii) $\gamma_n(\mathcal{V}(\Lambda)) \geq \gamma_n(\mathcal{V}(\Lambda')) \cdot \gamma_n(\mathcal{V}(\Lambda/\Lambda'))$



The main technical theorem (6)

Theorem

For stable lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

The main technical theorem (6)

Theorem

For stable lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Fix n. Prove by induction over rank, any stable $\Lambda \subseteq \mathbb{R}^n$ has $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \exp(-\frac{\mathrm{rank}(\Lambda))}{3n}) \geq 1 - \frac{\mathrm{rank}(\Lambda)}{3n}$

The main technical theorem (6)

Theorem

For stable lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Fix n. Prove by induction over rank, any stable $\Lambda \subseteq \mathbb{R}^n$ has $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \exp(-\frac{\mathrm{rank}(\Lambda))}{3n}) \geq 1 - \frac{\mathrm{rank}(\Lambda)}{3n}$
- Fix the stable lattice Λ minimizing $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda))$

The main technical theorem (6)

Theorem

For stable lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Fix n. Prove by induction over rank, any stable $\Lambda \subseteq \mathbb{R}^n$ has $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \exp(-\frac{\mathrm{rank}(\Lambda))}{3n}) \geq 1 - \frac{\mathrm{rank}(\Lambda)}{3n}$
- Fix the stable lattice Λ minimizing $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda))$

Case (II). DONE! (after some boosting)

Case (I). $\exists$ prim. sublattice $\{\mathbf{0}\} \subset \Lambda' \subset \Lambda$ with $\det(\Lambda') = 1$

The main technical theorem (6)

Theorem

For stable lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Fix n. Prove by induction over rank, any stable $\Lambda \subseteq \mathbb{R}^n$ has $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \exp(-\frac{\mathrm{rank}(\Lambda))}{3n}) \geq 1 - \frac{\mathrm{rank}(\Lambda)}{3n}$
- Fix the stable lattice Λ minimizing $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda))$

Case (II). DONE! (after some boosting)

Case (I). $\exists$ prim. sublattice $\{\mathbf{0}\} \subset \Lambda' \subset \Lambda$ with $\det(\Lambda') = 1$

- Λ' and Λ/Λ' are stable

The main technical theorem (6)

Theorem

For stable lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Fix n. Prove by induction over rank, any stable $\Lambda \subseteq \mathbb{R}^n$ has $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \exp(-\frac{\mathrm{rank}(\Lambda))}{3n}) \geq 1 - \frac{\mathrm{rank}(\Lambda)}{3n}$
- Fix the stable lattice Λ minimizing $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda))$

Case (II). DONE! (after some boosting)

Case (I). $\exists$ prim. sublattice $\{\mathbf{0}\} \subset \Lambda' \subset \Lambda$ with $\det(\Lambda') = 1$

- Λ' and Λ/Λ' are stable
- Then for $t := \Theta(\log n)$

$$\gamma_n(t \cdot \mathcal{V}(\Lambda)) \quad \geq \quad \gamma_n(t \cdot \mathcal{V}(\Lambda')) \cdot \gamma_n(t \cdot \mathcal{V}(\Lambda/\Lambda'))$$

The main technical theorem (6)

Theorem

For stable lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Fix n. Prove by induction over rank, any stable $\Lambda \subseteq \mathbb{R}^n$ has $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \exp(-\frac{\mathrm{rank}(\Lambda))}{3n}) \geq 1 - \frac{\mathrm{rank}(\Lambda)}{3n}$
- Fix the stable lattice Λ minimizing $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda))$

Case (II). DONE! (after some boosting)

Case (I). $\exists$ prim. sublattice $\{\mathbf{0}\} \subset \Lambda' \subset \Lambda$ with $\det(\Lambda') = 1$

- Λ' and Λ/Λ' are stable
- Then for $t := \Theta(\log n)$

$$\begin{aligned} \gamma_n(t \cdot \mathcal{V}(\Lambda)) &\geq \gamma_n(t \cdot \mathcal{V}(\Lambda')) \cdot \gamma_n(t \cdot \mathcal{V}(\Lambda/\Lambda')) \\ &\overset{\text{ind.}}{\geq} \exp\Big(-\frac{\mathrm{rank}(\Lambda')}{3n}\Big) \cdot \exp\Big(-\frac{\mathrm{rank}(\Lambda/\Lambda')}{3n}\Big) \end{aligned}$$

The main technical theorem (6)

Theorem

For stable lattice $\Lambda \subseteq \mathbb{R}^n$ *one has* $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \frac{2}{3}$.

- Fix n. Prove by induction over rank, any stable $\Lambda \subseteq \mathbb{R}^n$ has $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda)) \geq \exp(-\frac{\mathrm{rank}(\Lambda))}{3n}) \geq 1 - \frac{\mathrm{rank}(\Lambda)}{3n}$
- Fix the stable lattice Λ minimizing $\gamma_n(\Theta(\log n) \cdot \mathcal{V}(\Lambda))$

Case (II). DONE! (after some boosting)

Case (I). $\exists$ prim. sublattice $\{\mathbf{0}\} \subset \Lambda' \subset \Lambda$ with $\det(\Lambda') = 1$

- Λ' and Λ/Λ' are stable
- Then for $t := \Theta(\log n)$

$$\begin{aligned}
\gamma_n(t \cdot \mathcal{V}(\Lambda)) &\geq \gamma_n(t \cdot \mathcal{V}(\Lambda')) \cdot \gamma_n(t \cdot \mathcal{V}(\Lambda/\Lambda')) \\
&\overset{\text{ind.}}{\geq} \exp\left(-\frac{\mathrm{rank}(\Lambda')}{3n}\right) \cdot \exp\left(-\frac{\mathrm{rank}(\Lambda/\Lambda')}{3n}\right) \\
&= \exp\left(-\frac{\mathrm{rank}(\Lambda)}{3n}\right) \quad \square
\end{aligned}$$

Proof for non-stable lattices

Corollary

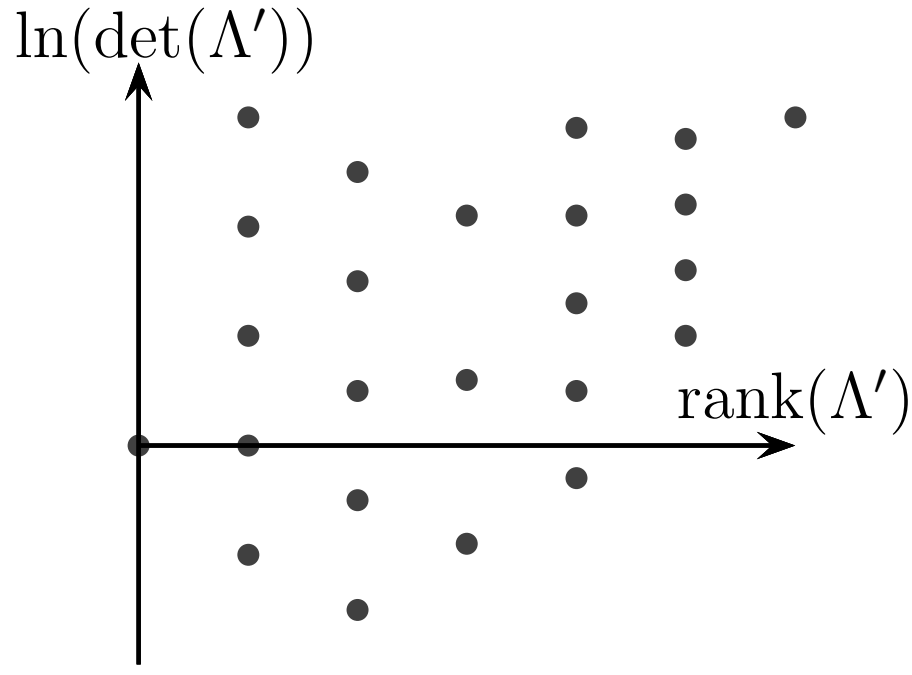
For stable lattice $\Lambda \subseteq \mathbb{R}^n$, $\rho_{1/\Theta(\log n)}(\Lambda) \leq \frac{3}{2}$.

- But what if Λ is not stable (only $\det(\Lambda') \geq 1 \; \forall \Lambda' \subseteq \Lambda$)?

The canonical filtration

- For lattice $\Lambda \subseteq \mathbb{R}^n$, consider **canonical plot**

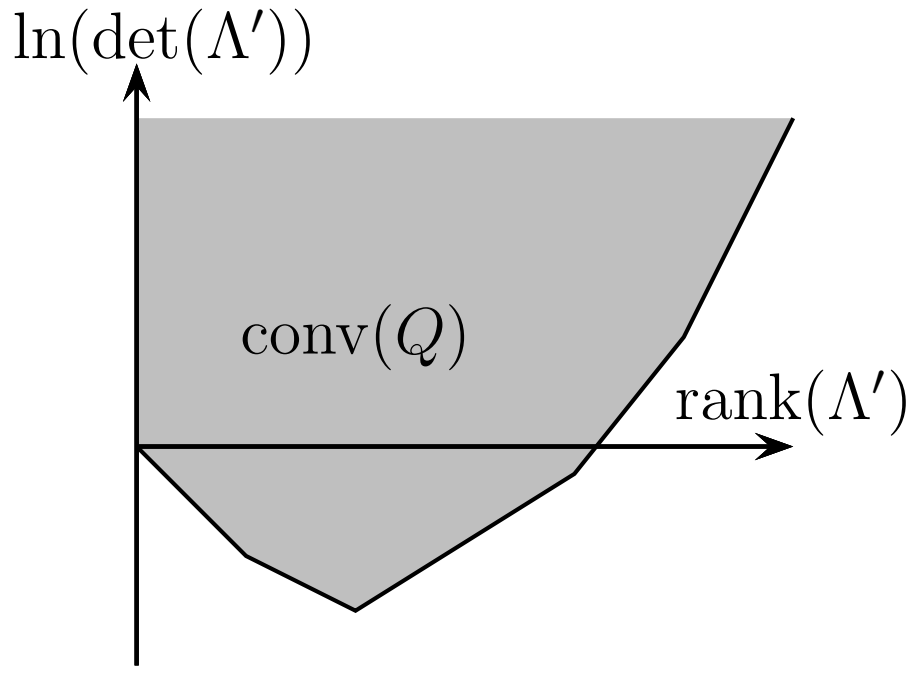
$$Q := \left\{ \left(\operatorname{rank}(\Lambda'), \ln(\det(\Lambda')) \right) \mid \text{sublattice } \Lambda' \subseteq \Lambda \right\}$$



The canonical filtration

- For lattice $\Lambda \subseteq \mathbb{R}^n$, consider **canonical plot**

$$Q := \left\{ \left(\operatorname{rank}(\Lambda'), \ln(\det(\Lambda')) \right) \mid \text{sublattice } \Lambda' \subseteq \Lambda \right\}$$

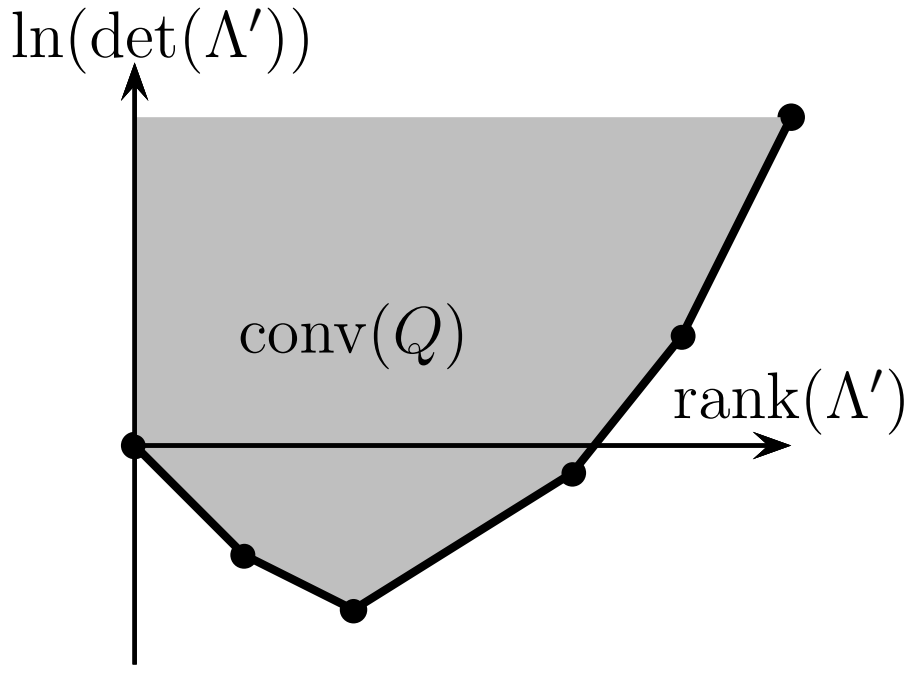


The canonical filtration

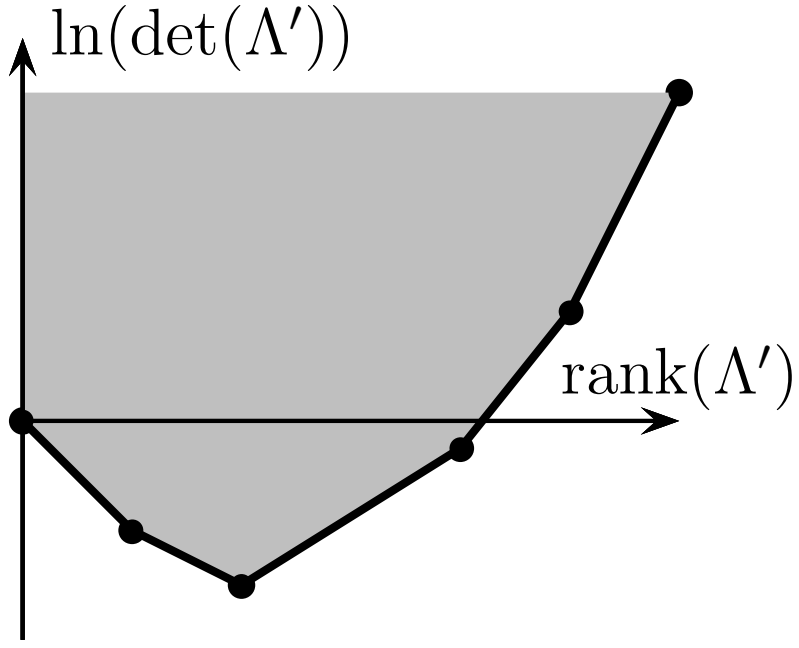
- For lattice $\Lambda \subseteq \mathbb{R}^n$, consider **canonical plot**

$$Q := \left\{ \left(\operatorname{rank}(\Lambda'), \ln(\det(\Lambda')) \right) \mid \text{sublattice } \Lambda' \subseteq \Lambda \right\}$$

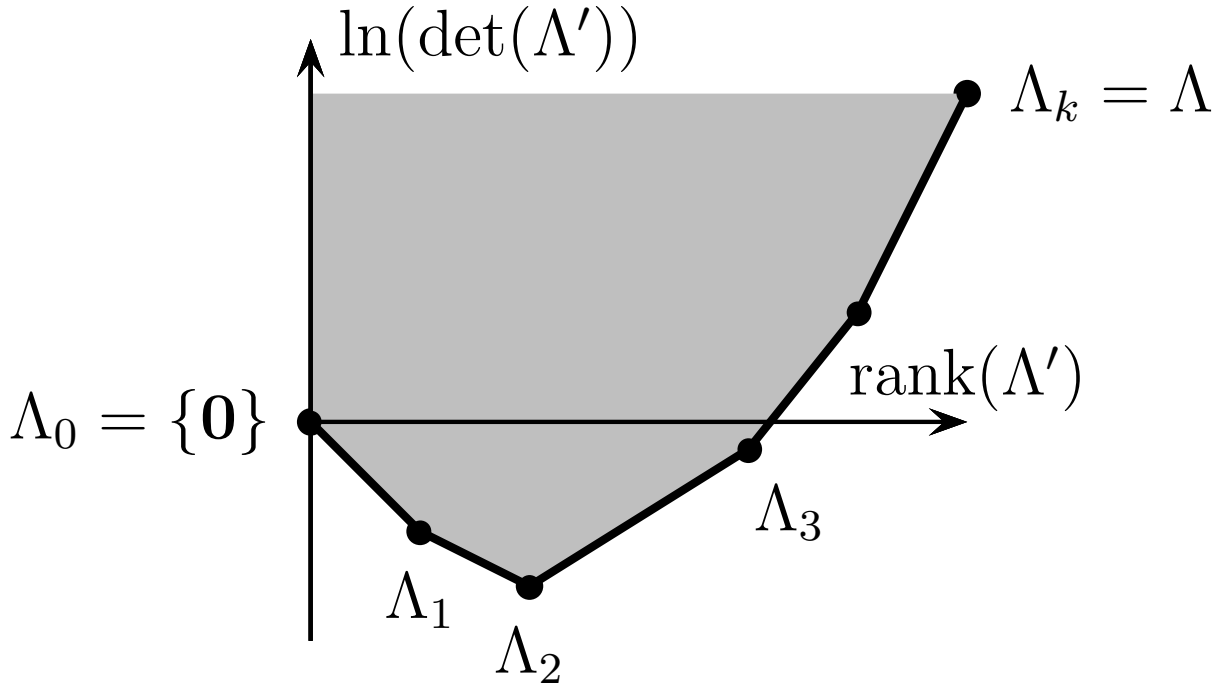
- Lower envelope of $\operatorname{conv}(Q)$ is called **canonical polygon**



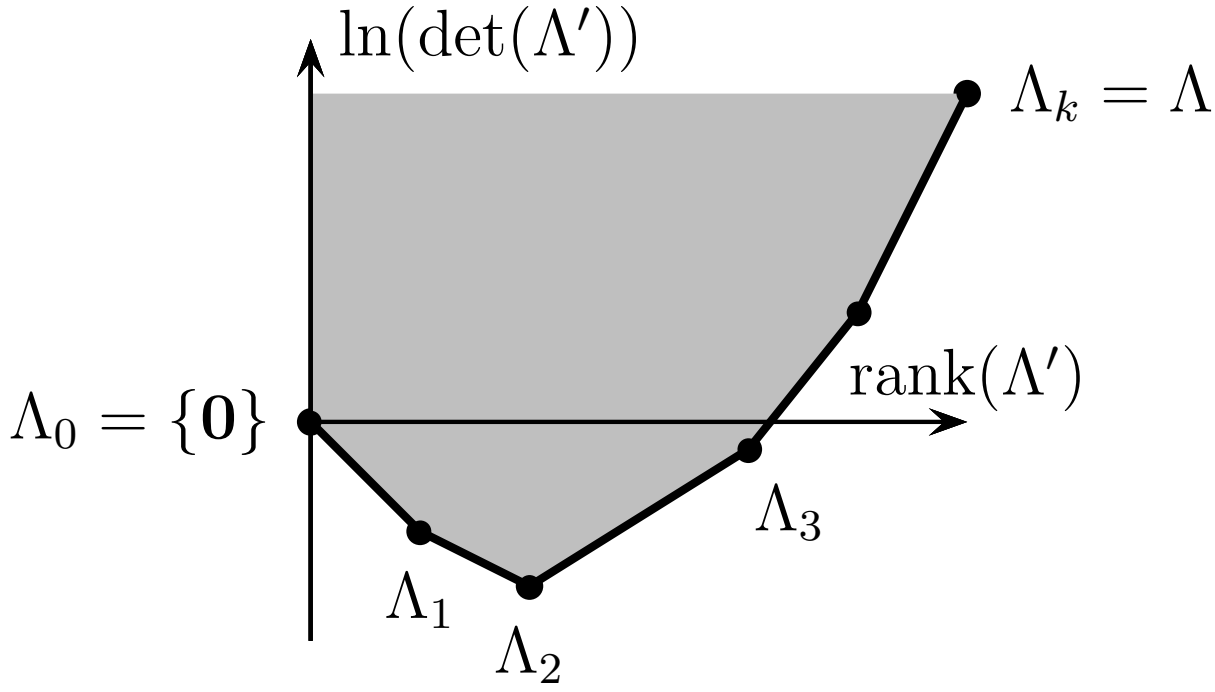
The canonical filtration (2)



The canonical filtration (2)



The canonical filtration (2)



Theorem (Canonical filtration)

(a) *The vertices of the canonical plot form a chain*

$$\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda.$$

(b) $r_i := \det(\Lambda_i/\Lambda_{i-1})^{1/rank(\Lambda_i/\Lambda_{i-1})}$ *satisfy* $r_1 < \ldots < r_k$

(c) *Each* $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ *is stable.*

Proof of Reverse Minkowski Theorem

Reverse Minkowski Theorem (Regev, Stephens-Da.)

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for $t = \Theta(\log n)$, $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

Proof of Reverse Minkowski Theorem

Reverse Minkowski Theorem (Regev, Stephens-Da.)

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for $t = \Theta(\log n)$, $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

Proof.

- Consider canonical filtration

$$\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$$

Proof of Reverse Minkowski Theorem

Reverse Minkowski Theorem (Regev, Stephens-Da.)

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for $t = \Theta(\log n)$, $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

Proof.

- Consider canonical filtration

$$\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$$

- We know $r_k > \ldots > r_1 = \det(\Lambda_0) \geq 1$

Proof of Reverse Minkowski Theorem

Reverse Minkowski Theorem (Regev, Stephens-Da.)

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for $t = \Theta(\log n)$, $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

Proof.

- Consider canonical filtration

$$\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$$

- We know $r_k > \ldots > r_1 = \det(\Lambda_0) \geq 1$
- Then

$$\rho_{1/t}(\Lambda) \quad \leq \quad \prod_{i=1}^{k} \rho_{1/t}(\Lambda_i/\Lambda_{i-1})$$

Proof of Reverse Minkowski Theorem

Reverse Minkowski Theorem (Regev, Stephens-Da.)

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for $t = \Theta(\log n)$, $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

Proof.

- Consider canonical filtration

$$\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$$

- We know $r_k > \ldots > r_1 = \det(\Lambda_0) \geq 1$
- Then

$$\rho_{1/t}(\Lambda) \quad \leq \quad \prod_{i=1}^{k} \rho_{1/t}(\Lambda_i/\Lambda_{i-1}) \overset{r_i \geq 1}{\leq} \prod_{i=1}^{k} \rho_{1/t}\Big(\overbrace{\frac{1}{r_i}\Lambda_i/\Lambda_{i-1}}^{\text{stable lattice}}\Big)$$

Proof of Reverse Minkowski Theorem

Reverse Minkowski Theorem (Regev, Stephens-Da.)

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice that satisfies $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$. Then for $t = \Theta(\log n)$, $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

Proof.

- Consider canonical filtration

$$\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda$$

- We know $r_k > \ldots > r_1 = \det(\Lambda_0) \geq 1$
- Then

$$\begin{aligned} \rho_{1/t}(\Lambda) &\leq \prod_{i=1}^{k} \rho_{1/t}(\Lambda_i/\Lambda_{i-1}) \overset{r_i \geq 1}{\leq} \prod_{i=1}^{k} \rho_{1/t}\Big(\overbrace{\frac{1}{r_i}\Lambda_i/\Lambda_{i-1}}^{\text{stable lattice}}\Big) \\ &\leq \prod_{i=1}^{k} \exp\left(\frac{\operatorname{rank}(\Lambda_i/\Lambda_{i-1})}{3n}\right) \leq \frac{3}{2} \end{aligned}$$

□

End of part 2

Open problem 1

Is it true that already for $t = \Theta(\sqrt{\log n})$ and any stable lattice Λ one has $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

- Known proof works for $t = \Theta(\log n)$.

End of part 2

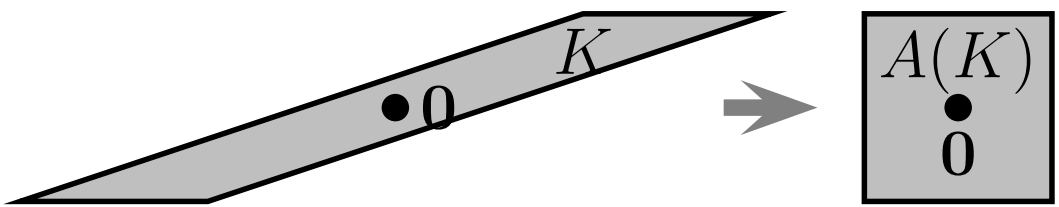
Open problem 1

Is it true that already for $t = \Theta(\sqrt{\log n})$ and any stable lattice Λ one has $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

- Known proof works for $t = \Theta(\log n)$.

Open problem 2

Is it true that for any symmetric convex body $K \subseteq \mathbb{R}^n$ with $\mathrm{Vol}_n(K) = 1$, there is a volume-preserving linear map A so that $\gamma_n(\Theta(\sqrt{\log(n)}) \cdot A(K)) \geq \frac{2}{3}$



- Problem 2 $\Rightarrow$ Problem 1

End of part 2

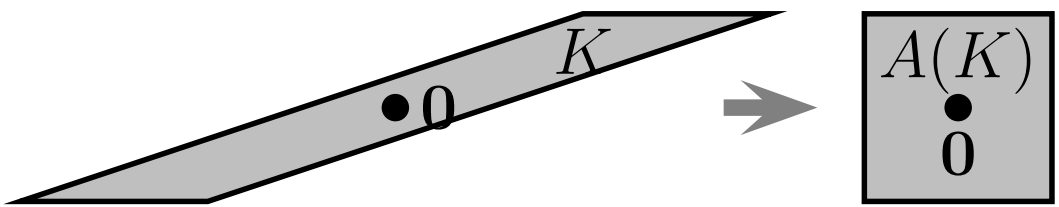
Open problem 1

Is it true that already for $t = \Theta(\sqrt{\log n})$ and any stable lattice Λ one has $\rho_{1/t}(\Lambda) \leq \frac{3}{2}$.

- Known proof works for $t = \Theta(\log n)$.

Open problem 2

Is it true that for any symmetric convex body $K \subseteq \mathbb{R}^n$ with $\mathrm{Vol}_n(K) = 1$, there is a volume-preserving linear map A so that $\gamma_n(\Theta(\sqrt{\log(n)}) \cdot A(K)) \geq \frac{2}{3}$



- Problem 2 $\Rightarrow$ Problem 1

Thanks for your attention!

Part 3:
The Subspace Flatness Conjecture and Faster Integer Programming

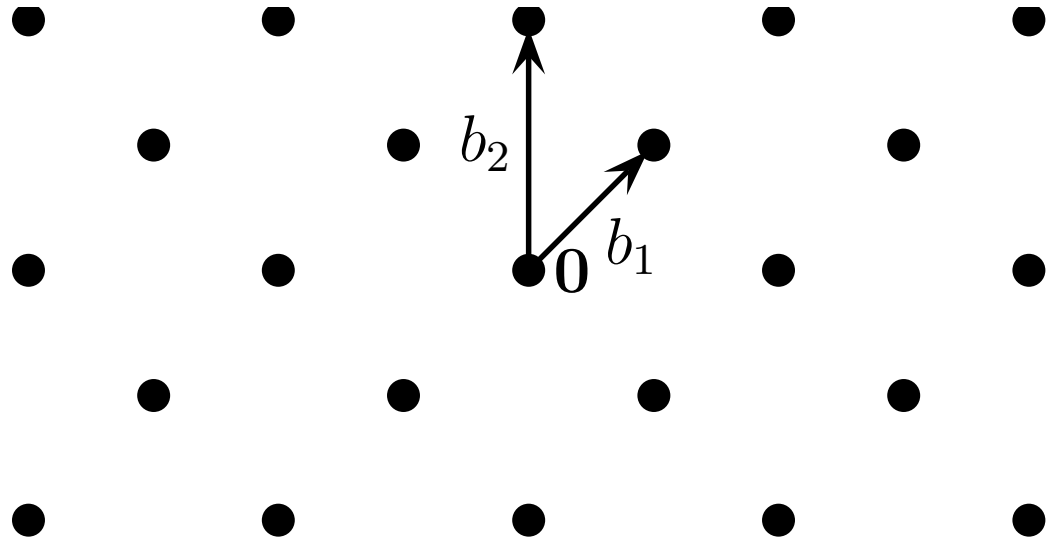
Thomas Rothvoss

Joint work with Victor Reis

UNIVERSITY *of*
WASHINGTON

Covering radius

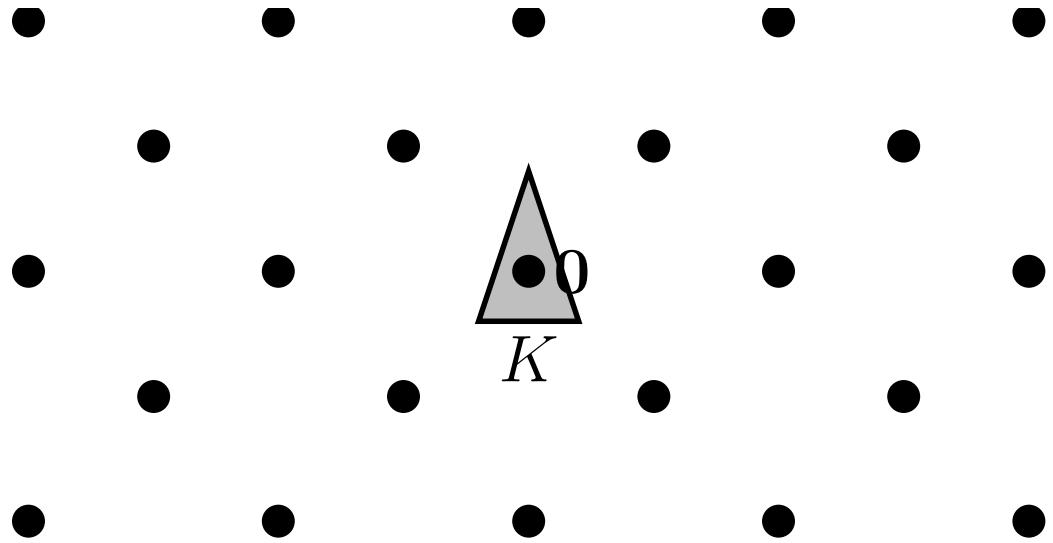
- Consider a **lattice** $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ with $B \in \mathbb{R}^{n \times k}$



Covering radius

- Consider a **lattice** $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ with $B \in \mathbb{R}^{n \times k}$
- For a convex body K, the **covering radius** of a (full rank) lattice Λ is

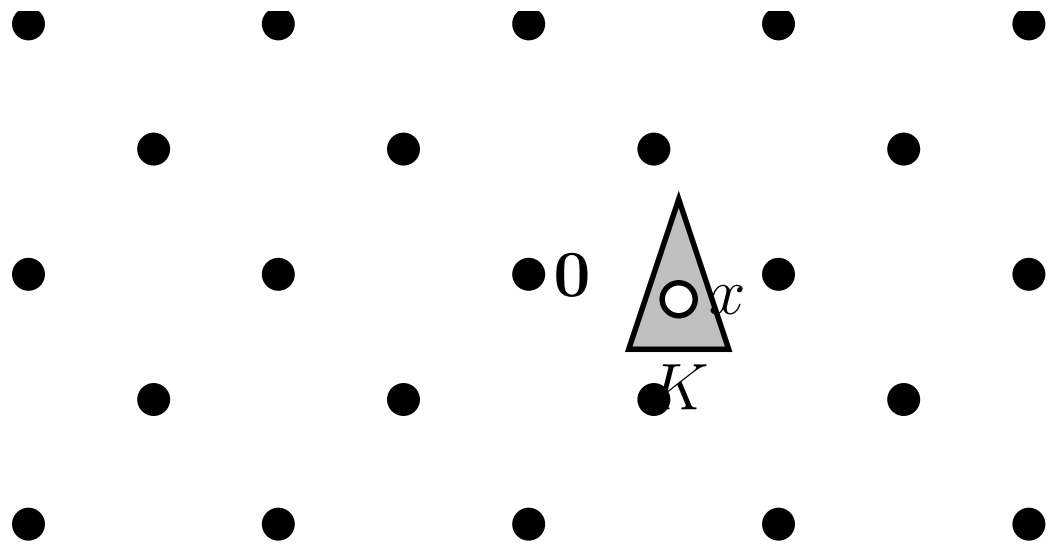
$$\mu(\Lambda, K) \quad = \quad \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\}$$



Covering radius

- Consider a **lattice** $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ with $B \in \mathbb{R}^{n \times k}$
- For a convex body K, the **covering radius** of a (full rank) lattice Λ is

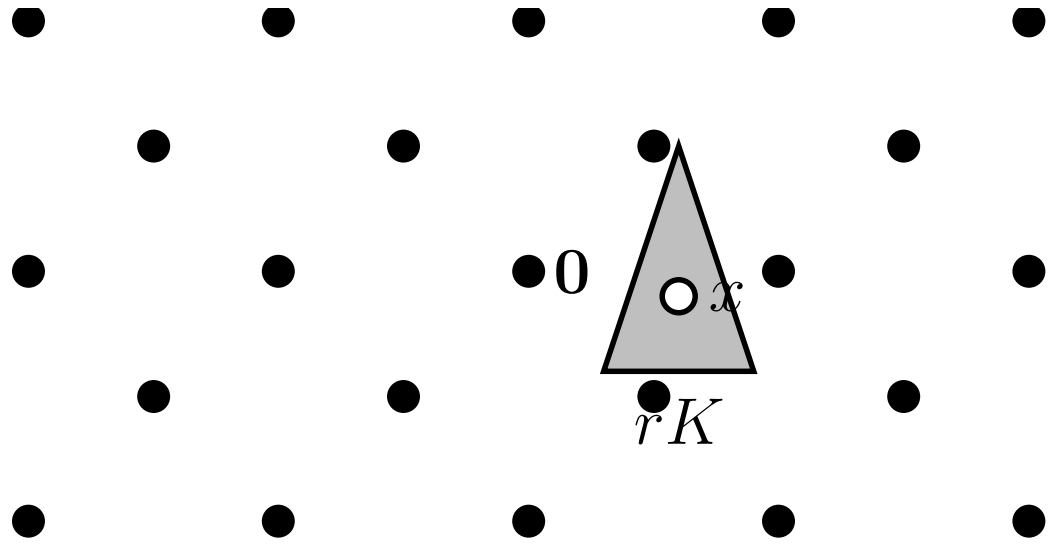
$$\begin{aligned} \mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \ \forall x \in \mathbb{R}^n\} \end{aligned}$$



Covering radius

- Consider a **lattice** $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ with $B \in \mathbb{R}^{n \times k}$
- For a convex body K, the **covering radius** of a (full rank) lattice Λ is

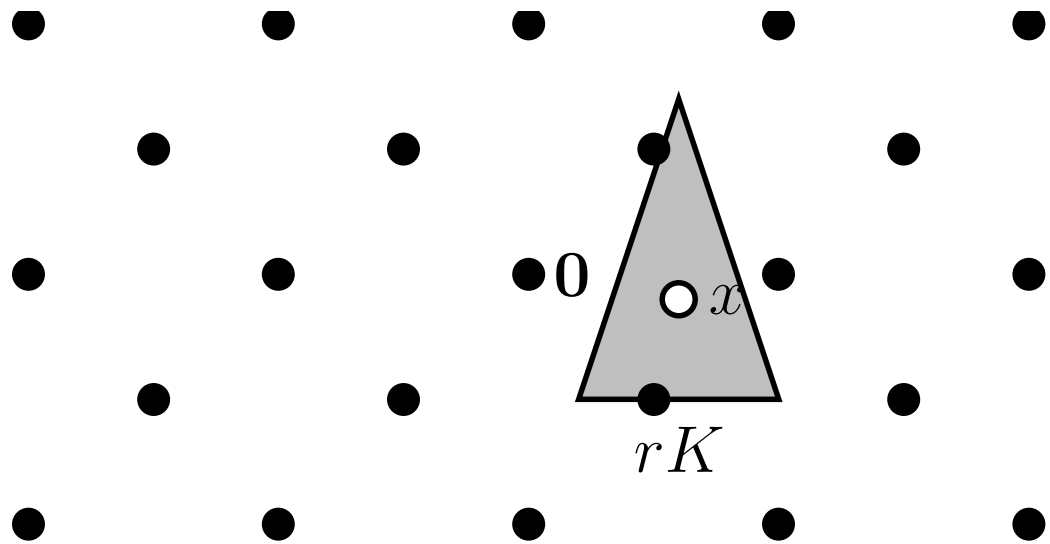
$$\begin{aligned} \mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \; \forall x \in \mathbb{R}^n\} \end{aligned}$$



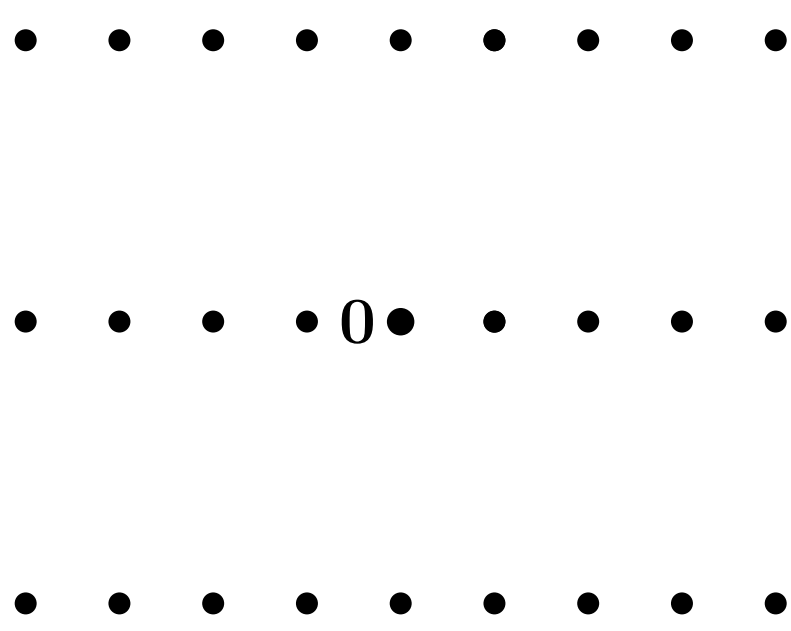
Covering radius

- Consider a **lattice** $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ with $B \in \mathbb{R}^{n \times k}$
- For a convex body K, the **covering radius** of a (full rank) lattice Λ is

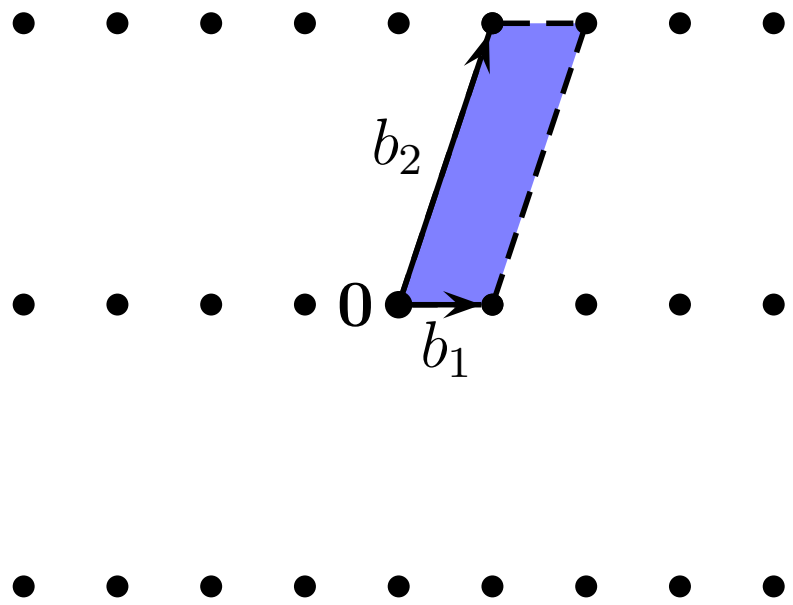
$$\begin{aligned} \mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \; \forall x \in \mathbb{R}^n\} \end{aligned}$$



Lower bounds on the covering radius

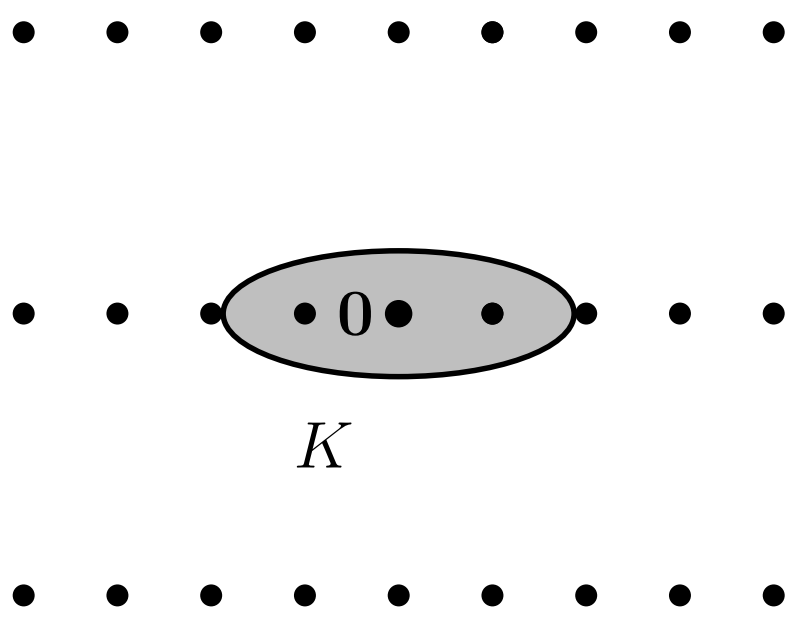


Lower bounds on the covering radius



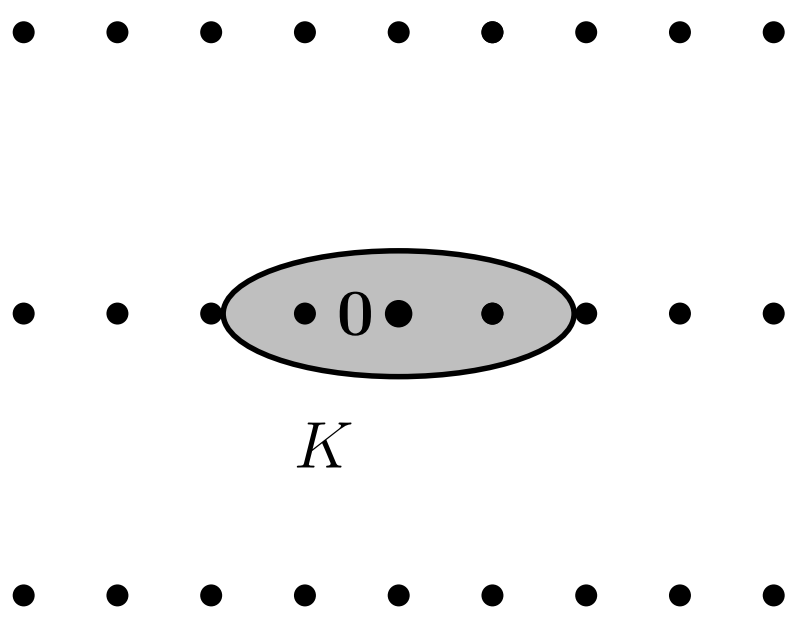
- **Recall:** $\det(\Lambda)$ =volume of fundamental parallelepiped

Lower bounds on the covering radius



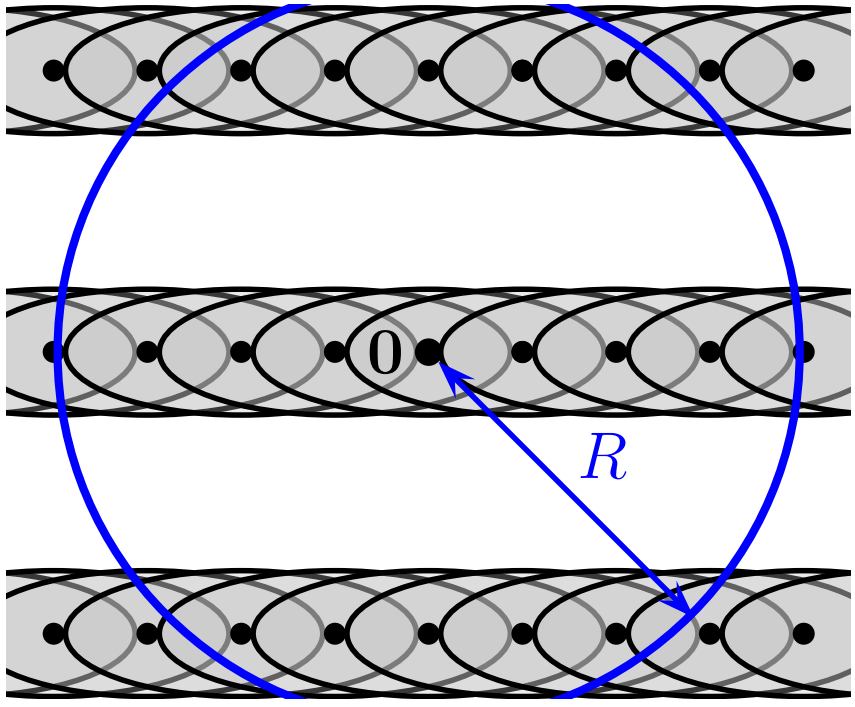
- **Recall:** $\det(\Lambda)$ =volume of fundamental parallelepiped

Lower bounds on the covering radius



- **Recall:** $\det(\Lambda)$ =volume of fundamental parallelepiped
- Simple lower bound: $\mu(\Lambda, K) \geq (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$

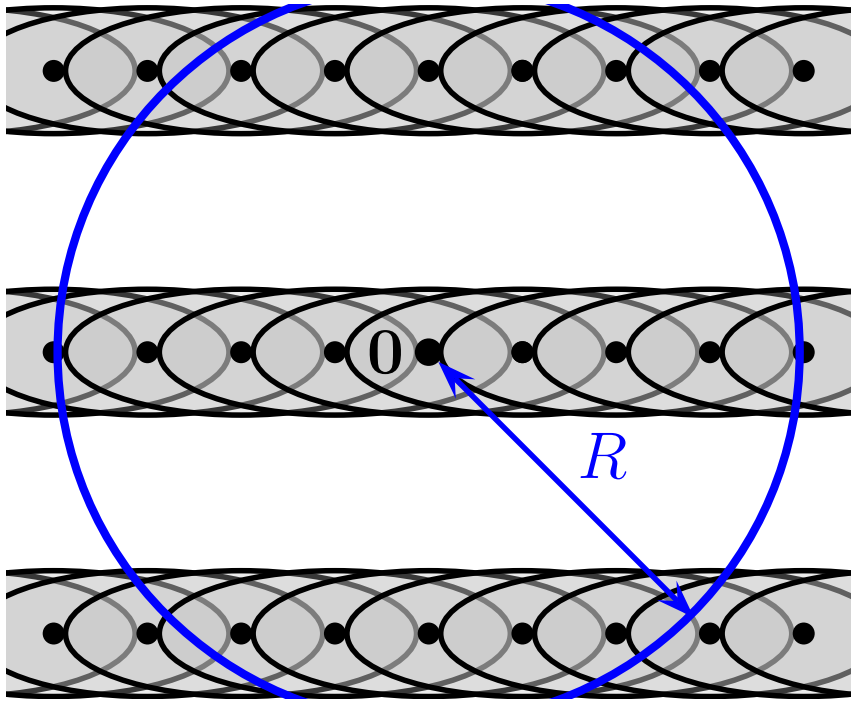
Lower bounds on the covering radius



- **Recall:** $\det(\Lambda)$ =volume of fundamental parallelepiped
- Simple lower bound: $\mu(\Lambda, K) \geq (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$
- For all $r > 0$,

$$\mathop{\mathbb{E}}_{x \sim RB_2^n} [\#y \in \Lambda : x \in y + rK] \overset{R \to \infty}{\approx} \frac{\mathrm{Vol}_n(rK)}{\det(\Lambda)}$$

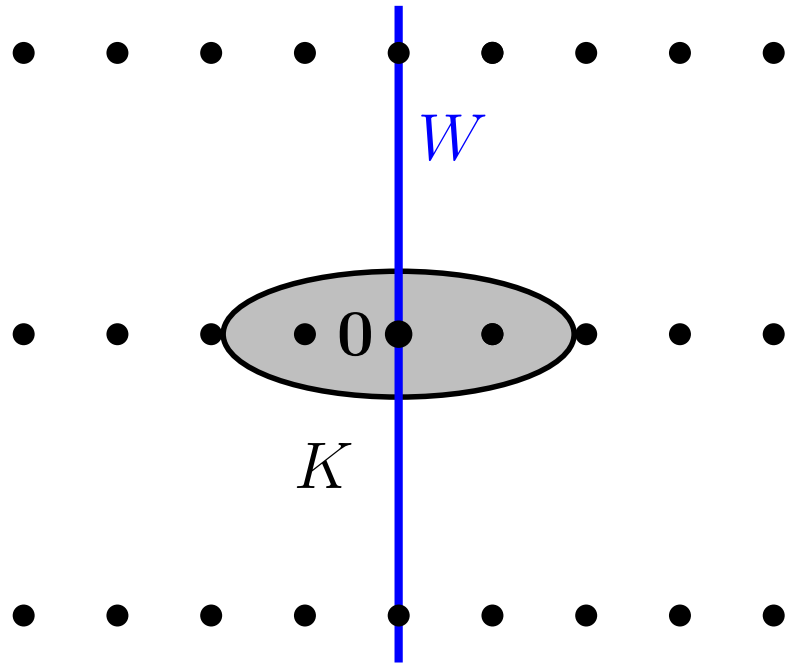
Lower bounds on the covering radius



- **Recall:** $\det(\Lambda)$ =volume of fundamental parallelepiped
- Simple lower bound: $\mu(\Lambda, K) \geq (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$
- For $r := \mu(\Lambda, K)$,

$$\mathop{\mathbb{E}}_{x \sim RB_2^n} [\#y \in \Lambda : x \in y + rK] \overset{R \to \infty}{\approx} \frac{\mathrm{Vol}_n(rK)}{\det(\Lambda)} \geq 1$$

Lower bounds on the covering radius



- **Recall:** $\det(\Lambda)$ =volume of fundamental parallelepiped
- Simple lower bound: $\mu(\Lambda, K) \geq (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$
- For $r := \mu(\Lambda, K)$,

$$\mathop{\mathbb{E}}_{x \sim RB_2^n} [\#y \in \Lambda : x \in y + rK] \overset{R \to \infty}{\approx} \frac{\mathrm{Vol}_n(rK)}{\det(\Lambda)} \geq 1$$

- For any subspace $\mu(\Lambda, K) \geq \mu(\Pi_W(\Lambda), \Pi_W(K))$

Kannan, Lovász (1988)

- Consider the best volume-based lower bound

$$\mu_{KL}(\Lambda, K) = \max_{\substack{W \subseteq \text{span}(\Lambda) \text{ subspace} \\ d := \dim(W)}} \left(\frac{\det(\Pi_W(\Lambda))}{\text{Vol}_d(\Pi_W(K))} \right)^{1/d}$$

Kannan, Lovász (1988)

- Consider the best volume-based lower bound

$$\mu_{KL}(\Lambda, K) = \max_{\substack{W \subseteq \text{span}(\Lambda) \text{ subspace} \\ d := \dim(W)}} \left(\frac{\det(\Pi_W(\Lambda))}{\text{Vol}_d(\Pi_W(K))} \right)^{1/d}$$

Theorem (Kannan, Lovász (1988))

For any full rank lattice Λ, convex body $K \subseteq \mathbb{R}^n$

$$\mu_{KL}(\Lambda, K) \leq \mu(\Lambda, K) \leq n \cdot \mu_{KL}(\Lambda, K)$$

Kannan, Lovász (1988)

- Consider the best volume-based lower bound

$$\mu_{KL}(\Lambda, K) = \max_{\substack{W \subseteq \text{span}(\Lambda) \text{ subspace} \\ d := \dim(W)}} \left(\frac{\det(\Pi_W(\Lambda))}{\text{Vol}_d(\Pi_W(K))} \right)^{1/d}$$

Theorem (Kannan, Lovász (1988))

For any full rank lattice Λ, convex body $K \subseteq \mathbb{R}^n$

$$\mu_{KL}(\Lambda, K) \leq \mu(\Lambda, K) \leq n \cdot \mu_{KL}(\Lambda, K)$$

Subspace Flatness Conjecture (Dadush 2012)

For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$\mu(\Lambda, K) \leq O(\log(n)) \cdot \mu_{KL}(\Lambda, K)$$

- Dadush shows consequences for solving IPs.

Main results

Theorem (Reis, R.'23)

For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$\mu(\Lambda, K) \leq O(\log^3(n)) \cdot \mu_{KL}(\Lambda, K)$$

Main results

Theorem (Reis, R.'23)

For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$\mu(\Lambda, K) \leq O(\log^3(n)) \cdot \mu_{KL}(\Lambda, K)$$

Theorem (Reis, R.'23)

For convex body $K \subseteq \mathbb{R}^n$ one can find a point in $K \cap \mathbb{Z}^n$ in time $(\log n)^{O(n)}$.

Previously best known:

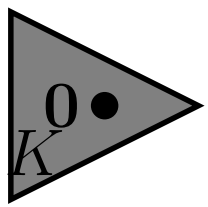
- $2^{O(n^2)}$ [Lenstra '83]
- $n^{O(n)}$ [Kannan '87]
- $2^{O(n)} n^n$ [Dadush '12], [Dadush, Eisenbrand, R. '22]

Main results (2)

Theorem (Reis, R.'23)

For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$\mu(\Lambda, K) \leq O(\log^3(n)) \cdot \mu(\Lambda, K - K)$$

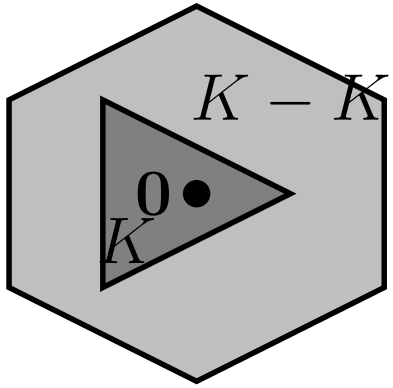


Main results (2)

Theorem (Reis, R.'23)

For full rank lattice $\Lambda \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ one has

$$\mu(\Lambda, K) \leq O(\log^3(n)) \cdot \mu(\Lambda, K - K)$$



Main results (2)

Theorem (Reis, R.'23)

Flatness constant in dimension n is at most $O(n \log^3(n))$.

- Previously best known: $O(n^{4/3} \log^{O(1)} n)$
  [Rudelson '98+Banaszczyk, Litvak, Pajor, Szarek '99]

Main results (2)

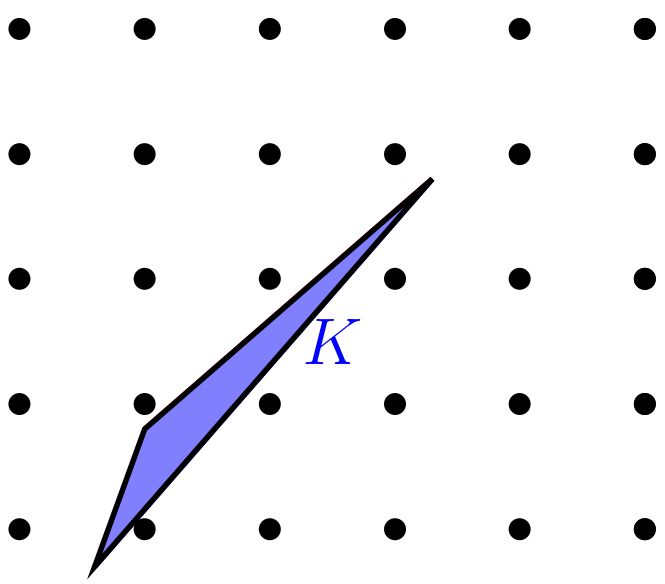
Theorem (Reis, R.'23)

Flatness constant in dimension n is at most $O(n \log^3(n))$.

- Previously best known: $O(n^{4/3} \log^{O(1)} n)$
  [Rudelson '98+Banaszczyk, Litvak, Pajor, Szarek '99]

Equivalently:

- If $K \cap \mathbb{Z}^n = \emptyset$, then $\exists c \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ so that at most $O(n \log^3(n))$ many hyperplanes $\langle c, x \rangle \in \mathbb{Z}$ intersect K.



Main results (2)

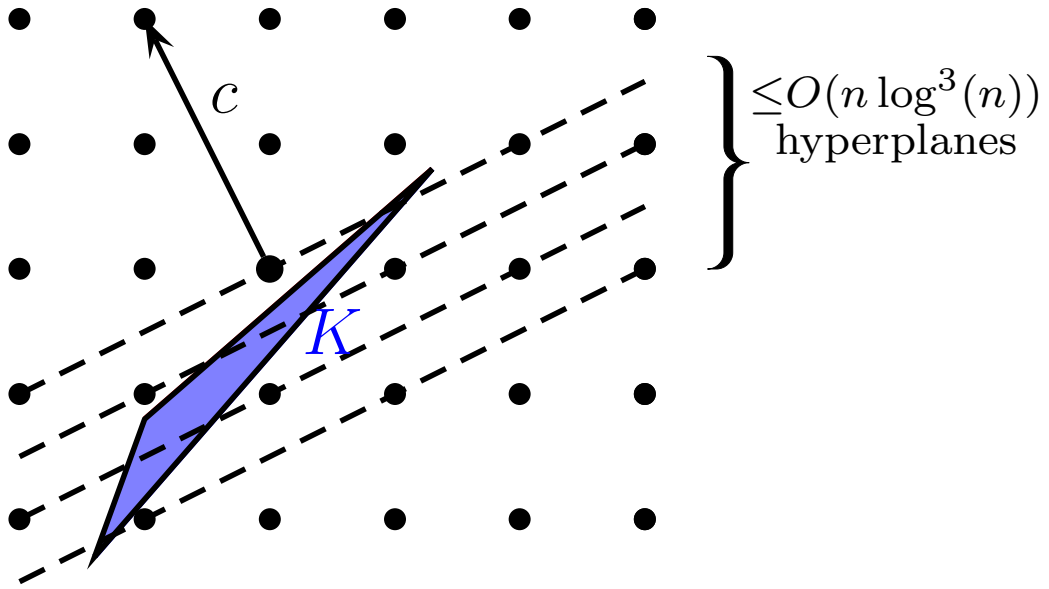
Theorem (Reis, R.'23)

Flatness constant in dimension n is at most $O(n \log^3(n))$.

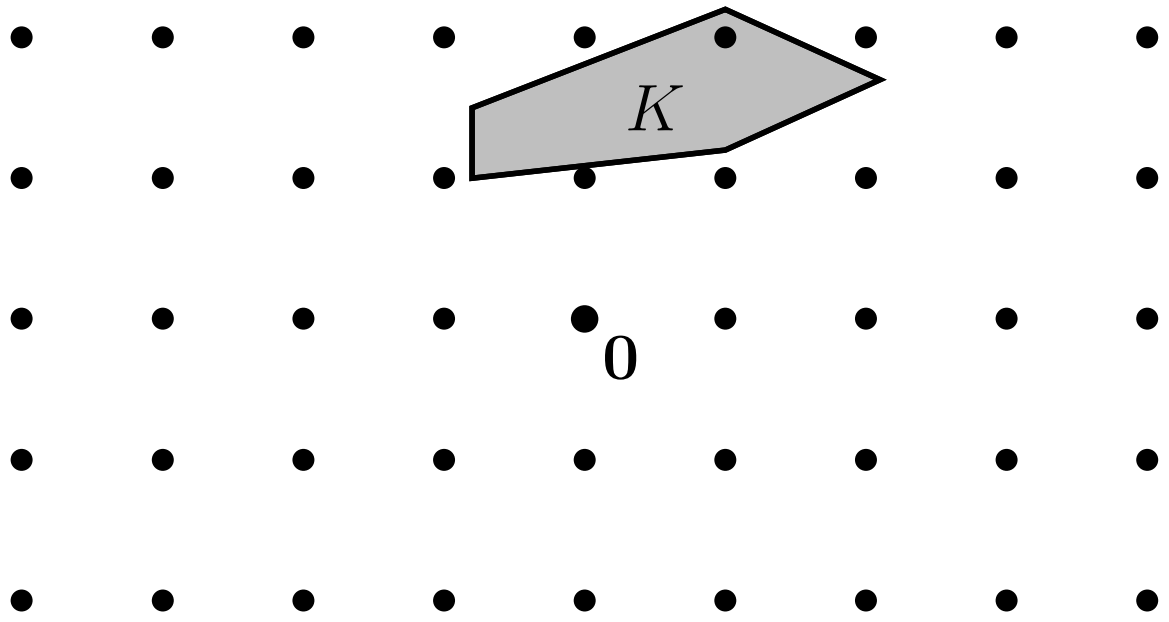
- Previously best known: $O(n^{4/3} \log^{O(1)} n)$ [Rudelson '98+Banaszczyk, Litvak, Pajor, Szarek '99]

Equivalently:

- If $K \cap \mathbb{Z}^n = \emptyset$, then $\exists c \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ so that at most $O(n \log^3(n))$ many hyperplanes $\langle c, x \rangle \in \mathbb{Z}$ intersect K.



Dadush's algorithm



Input: $K \subseteq \mathbb{R}^n$, lattice Λ

Output: Point in $K \cap \Lambda$

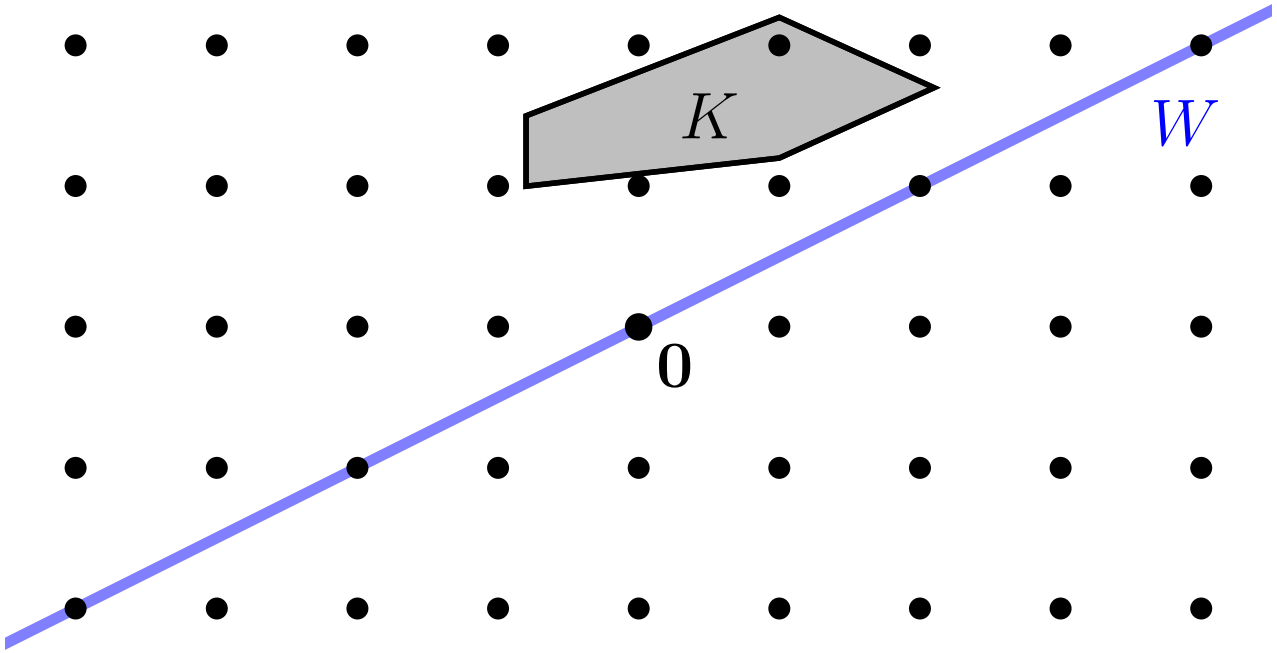
(1) Shrink K so that $\mu(\Lambda, K) \geq 1$

(2) Find subspace W attaining $\mu_{KL}(\Lambda, K)$ approx.

(3) Compute $X := \Pi_W(K) \cap \Pi_W(\Lambda)$

(4) Recurse on fibers $K \cap \Pi_W^{-1}(x)$ for all $x \in X$

Dadush's algorithm



Input: $K \subseteq \mathbb{R}^n$, lattice Λ

Output: Point in $K \cap \Lambda$

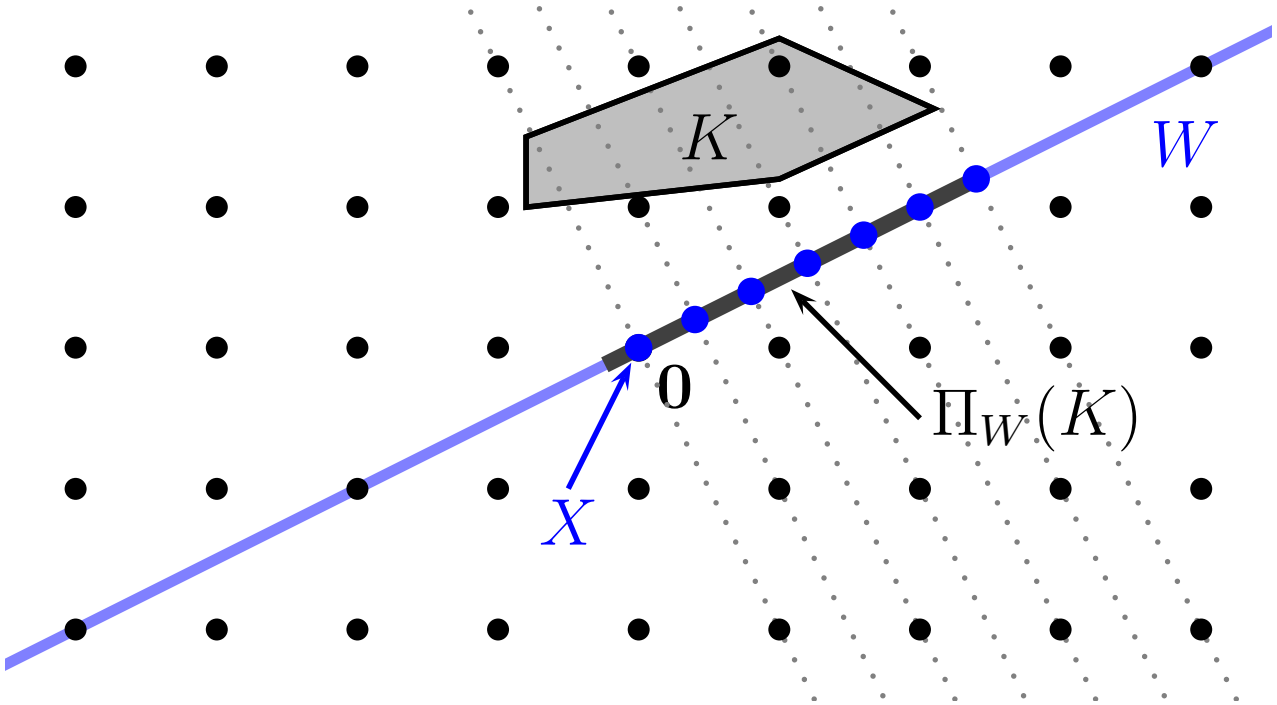
(1) Shrink K so that $\mu(\Lambda, K) \geq 1$

(2) Find subspace W attaining $\mu_{KL}(\Lambda, K)$ approx.

(3) Compute $X := \Pi_W(K) \cap \Pi_W(\Lambda)$

(4) Recurse on fibers $K \cap \Pi_W^{-1}(x)$ for all $x \in X$

Dadush's algorithm



Input: $K \subseteq \mathbb{R}^n$, lattice Λ

Output: Point in $K \cap \Lambda$

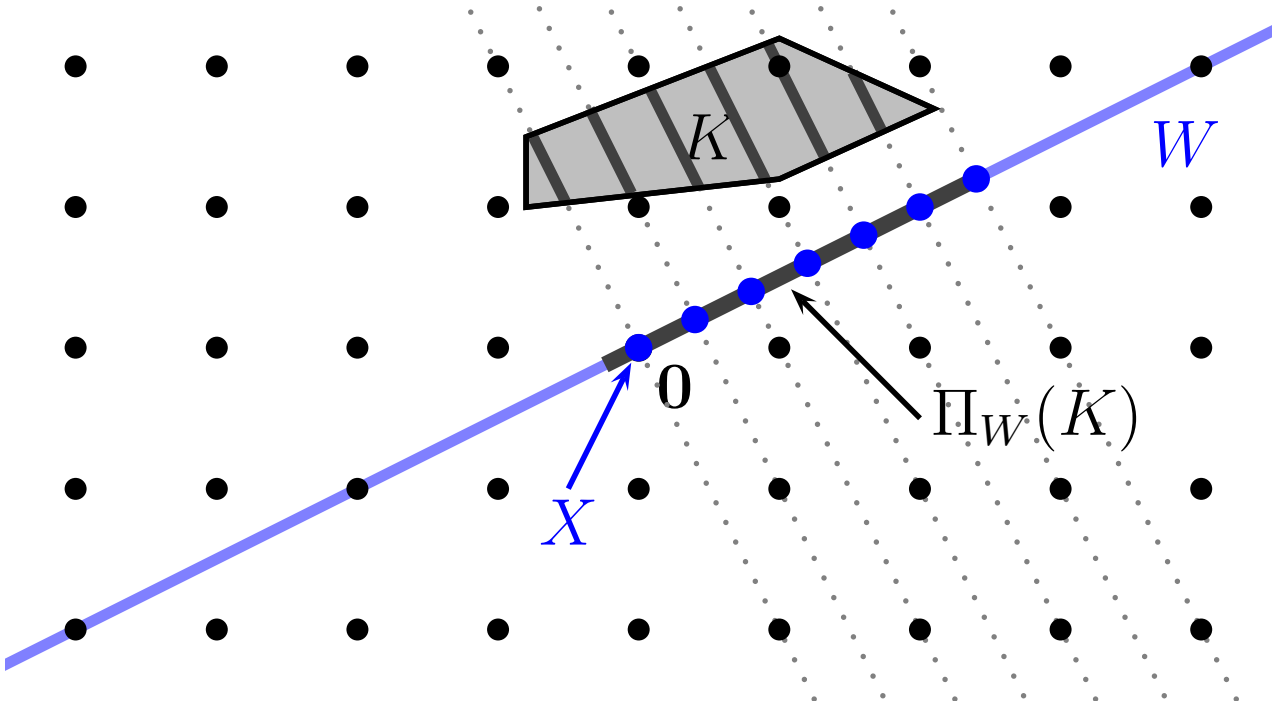
(1) Shrink K so that $\mu(\Lambda, K) \geq 1$

(2) Find subspace W attaining $\mu_{KL}(\Lambda, K)$ approx.

(3) Compute $X := \Pi_W(K) \cap \Pi_W(\Lambda)$

(4) Recurse on fibers $K \cap \Pi_W^{-1}(x)$ for all $x \in X$

Dadush's algorithm



Input: $K \subseteq \mathbb{R}^n$, lattice Λ

Output: Point in $K \cap \Lambda$

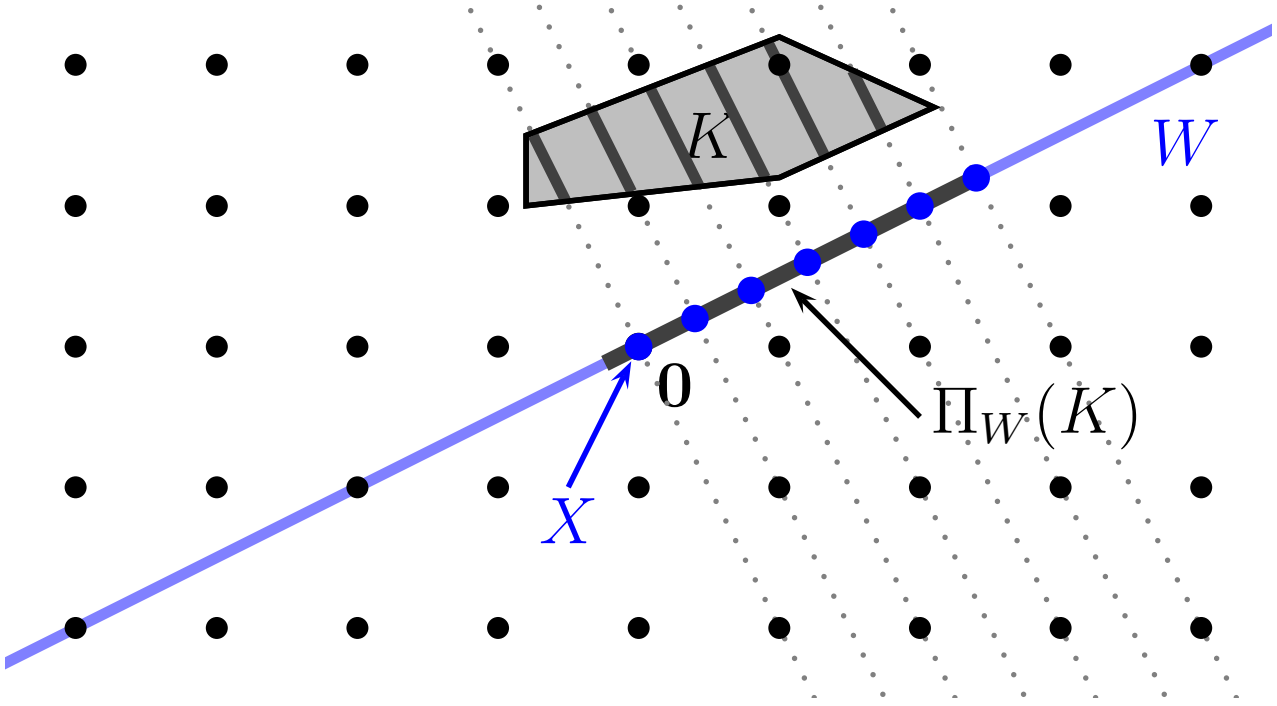
(1) Shrink K so that $\mu(\Lambda, K) \geq 1$

(2) Find subspace W attaining $\mu_{KL}(\Lambda, K)$ approx.

(3) Compute $X := \Pi_W(K) \cap \Pi_W(\Lambda)$

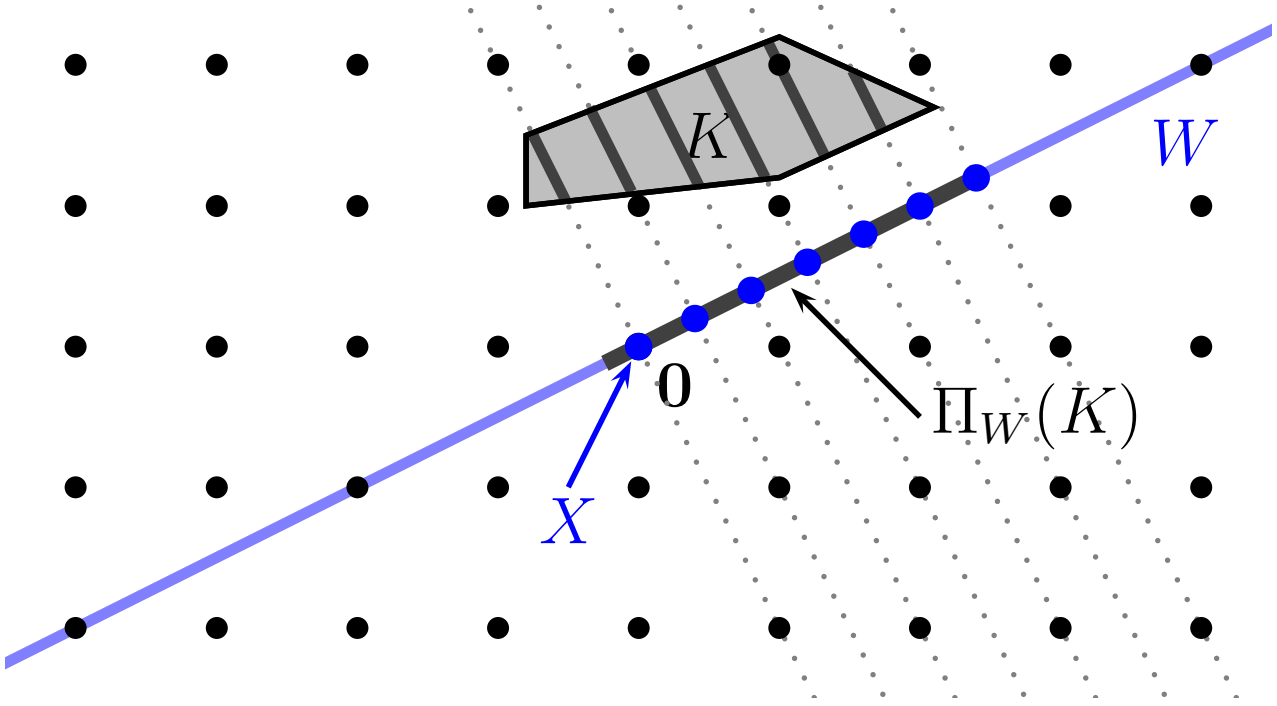
(4) Recurse on fibers $K \cap \Pi_W^{-1}(x)$ for all $x \in X$

Dadush's algorithm (analysis)



Analysis:

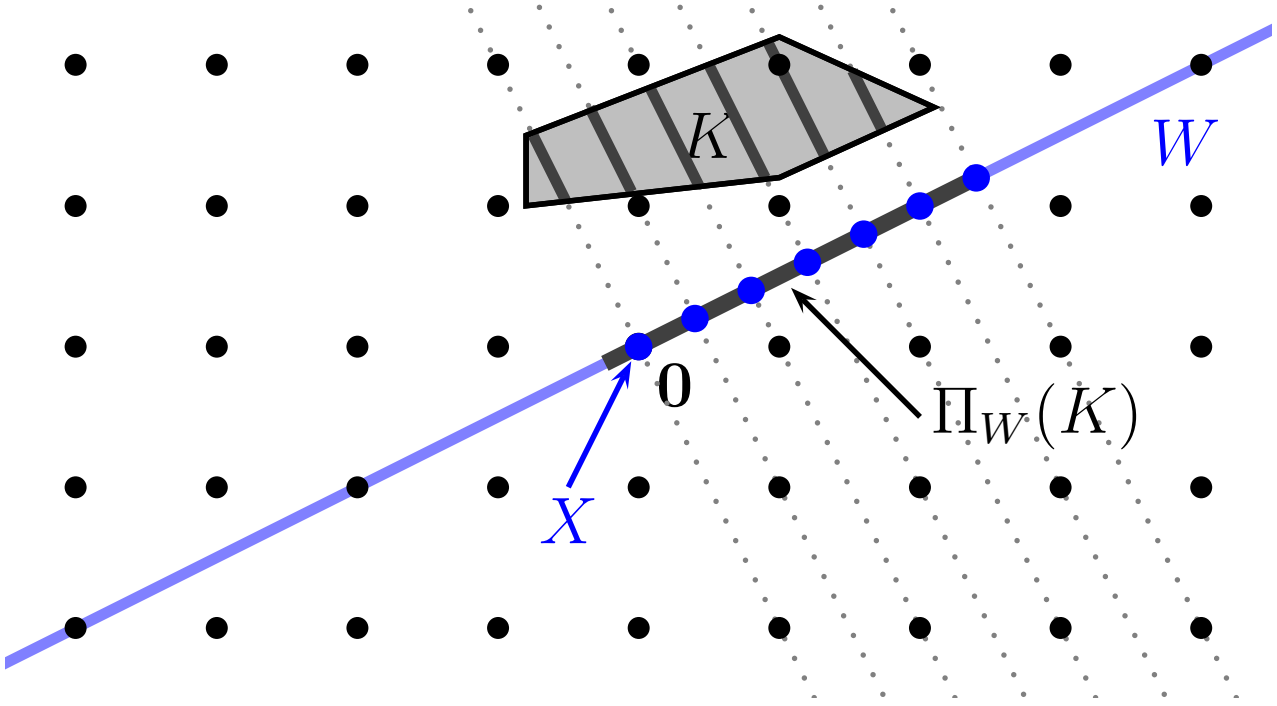
Dadush's algorithm (analysis)



Analysis:

- Can find W in time $2^{O(n)}$ [Dadush '19]

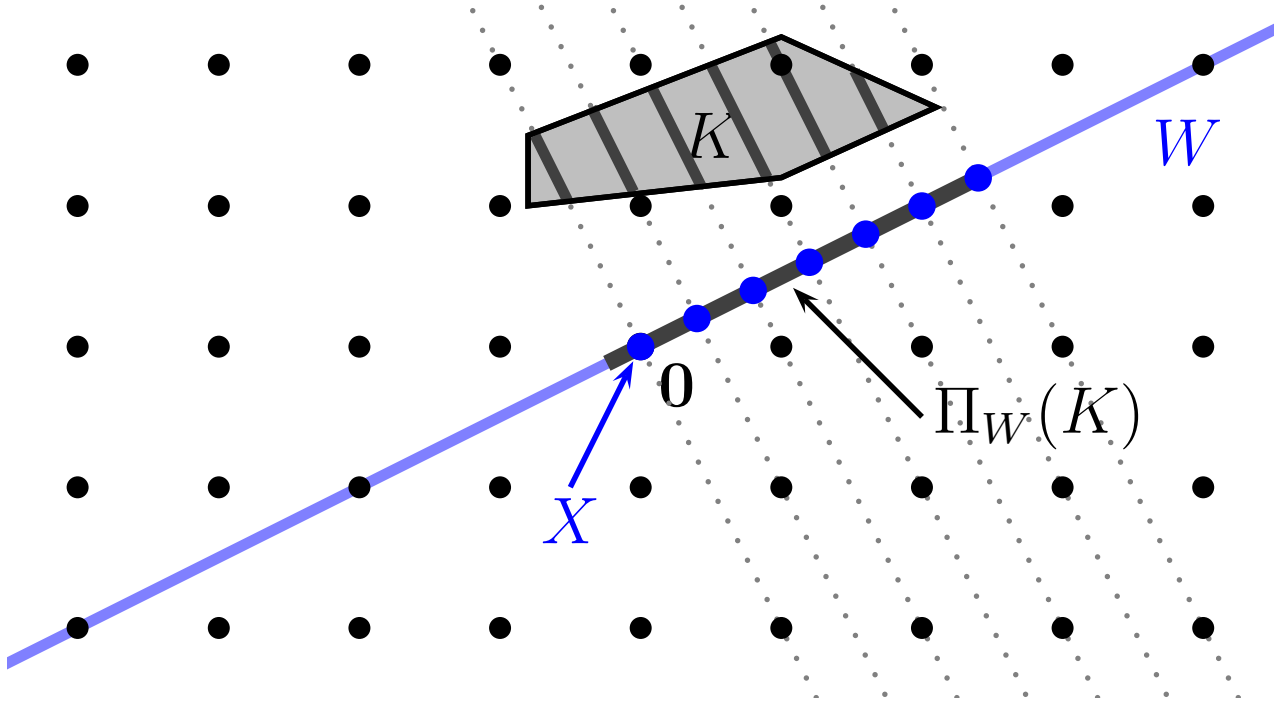
Dadush's algorithm (analysis)



Analysis:

- Can find W in time $2^{O(n)}$ [Dadush '19]
- One has $|\Pi_W(K) \cap \Pi_W(\Lambda)| \leq O(\log^4 n)^d$ w. $d := \dim(W)$
- Can **enumerate** those points in time $O(\log^4 n)^d$

Dadush's algorithm (analysis)

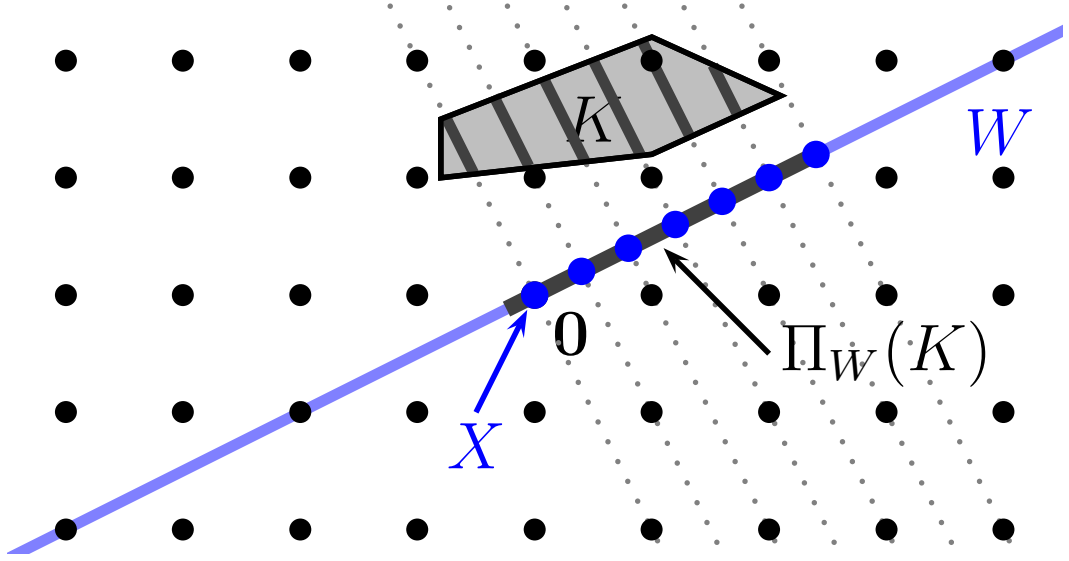


Analysis:

- Can find W in time $2^{O(n)}$ [Dadush '19]
- One has $|\Pi_W(K) \cap \Pi_W(\Lambda)| \leq O(\log^4 n)^d$ w. $d := \dim(W)$
- Can **enumerate** those points in time $O(\log^4 n)^d$
- Recursion

$$T(n) = 2^{O(n)} + \text{polylog}(n)^d \cdot T(n-d) \quad \Rightarrow \quad T(n) \leq \text{polylog}(n)^n$$

Dadush's algorithm (analysis) (2)



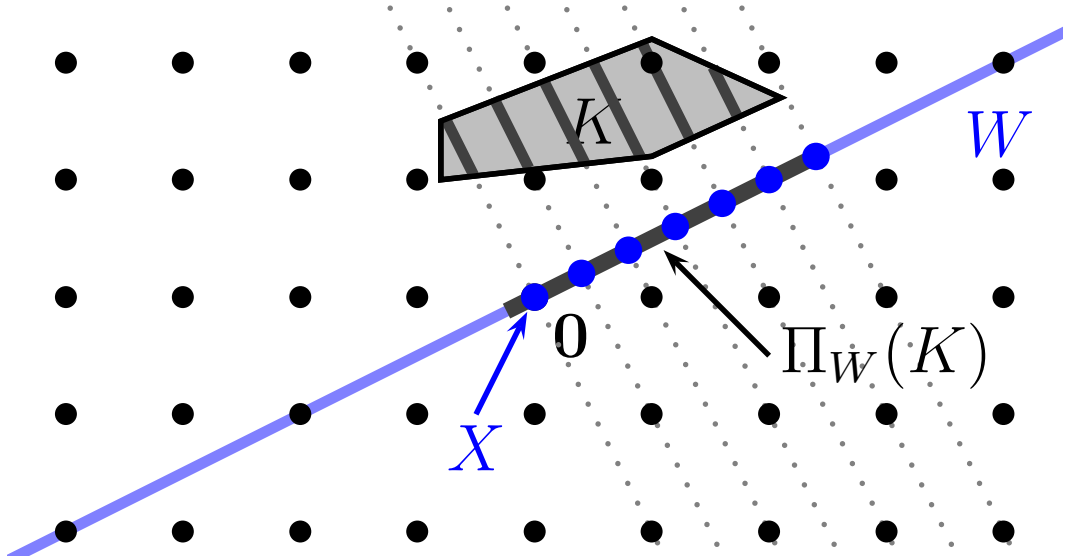
Theorem (Dadush)

For full rank lattice $\Lambda \subseteq \mathbb{R}^d$ and convex body $P \subseteq \mathbb{R}^d$ one has

$$|P \cap \Lambda| \leq 2^d \max\{\mu(\Lambda, P)^d, 1\} \cdot \frac{Vol_d(P)}{\det(\Lambda)} \quad (*).$$

Can compute points in same time.

Dadush's algorithm (analysis) (2)



Theorem (Dadush)

For full rank lattice $\Lambda \subseteq \mathbb{R}^d$ and convex body $P \subseteq \mathbb{R}^d$ one has

$$|P \cap \Lambda| \leq 2^d \max\{\mu(\Lambda, P)^d, 1\} \cdot \frac{Vol_d(P)}{\det(\Lambda)} \quad (*).$$

Can compute points in same time.

- Then $(\frac{\mathrm{Vol}_d(\Pi_W(K))}{\det(\Pi_W(\Lambda))})^{1/d} \leq \frac{O(\log^4(n))}{\mu(\Lambda,K)}$
- In any case $(*) \leq O(\log n)^{4d}$

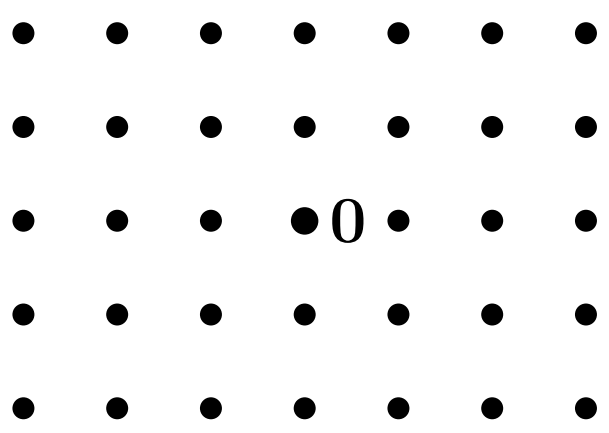
Sketch of Main proof

$$\mu(\Lambda, K) \leq O(\log^3 n) \cdot \mu_{KL}(\Lambda, K)$$

Recap: Stable lattices

Definition

A lattice Λ is called **stable** if $\det(\Lambda) = 1$ and $\det(\Lambda') \geq 1$ for all sublattices $\Lambda' \subseteq \Lambda$.



Example: $\mathbb{Z}^n$ is stable

ℓ-position

- For a symmetric convex body $K \subseteq \mathbb{R}^n$,

$$\ell_K = \mathop{\mathbb{E}}_{x \sim N(0, I_n)} [\|x\|_K^2]^{1/2}$$

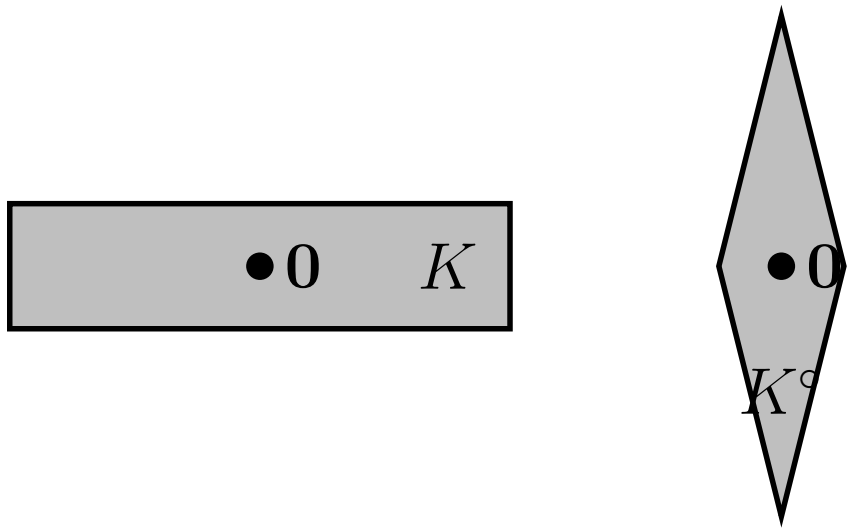
- **Intuitively:** $\ell_K =$ "average thinness" of K

ℓ-position

- For a symmetric convex body $K \subseteq \mathbb{R}^n$,

$$\ell_K = \mathop{\mathbb{E}}_{x \sim N(0, I_n)} [\|x\|_K^2]^{1/2}$$

- **Intuitively:** ℓ_K = "average thinness" of K
- **Polar** is $K^\circ = \{x \in \mathbb{R}^n \mid \langle x, y \rangle \leq 1 \ \forall y \in K\}$
- Possible that ℓ_K and ℓ_{K° arbitrarily large



ℓ-position

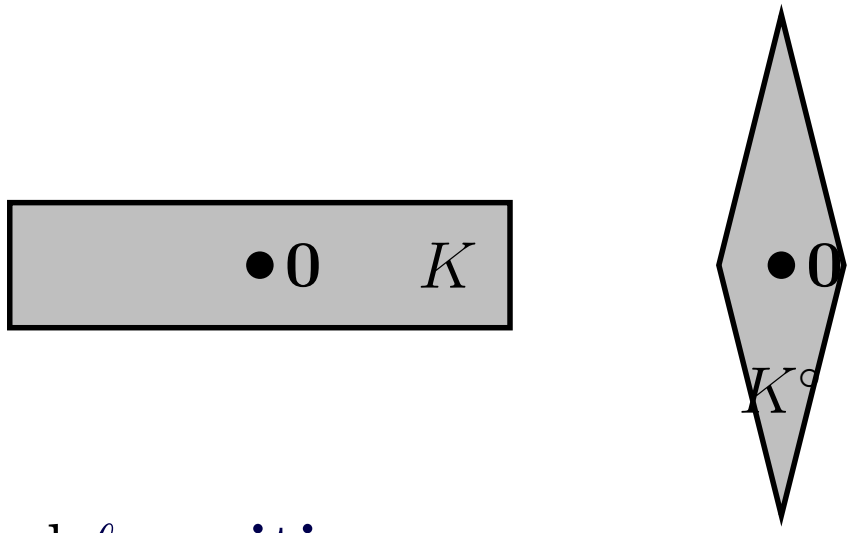
- For a symmetric convex body $K \subseteq \mathbb{R}^n$,

$$\ell_K = \mathop{\mathbb{E}}_{x \sim N(0, I_n)} [\|x\|_K^2]^{1/2}$$

- **Intuitively:** ℓ_K = "average thinness" of K

Theorem (Figiel, Tomczak-Jaegerman, Pisier)

For any symmetric convex body $K \subseteq \mathbb{R}^n$, there is an invertible linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ so that $\ell_{T(K)} \cdot \ell_{(T(K))^\circ} \leq O(n \log n)$.



- Also called **ℓ-position**

ℓ-position

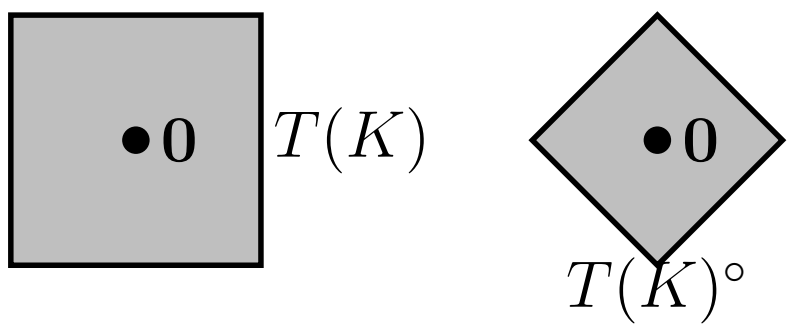
- For a symmetric convex body $K \subseteq \mathbb{R}^n$,

$$\ell_K = \mathop{\mathbb{E}}_{x \sim N(0, I_n)} [\|x\|_K^2]^{1/2}$$

- **Intuitively:** ℓ_K = "average thinness" of K

Theorem (Figiel, Tomczak-Jaegerman, Pisier)

For any symmetric convex body $K \subseteq \mathbb{R}^n$, there is an invertible linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ so that $\ell_{T(K)} \cdot \ell_{(T(K))^\circ} \leq O(n \log n)$.

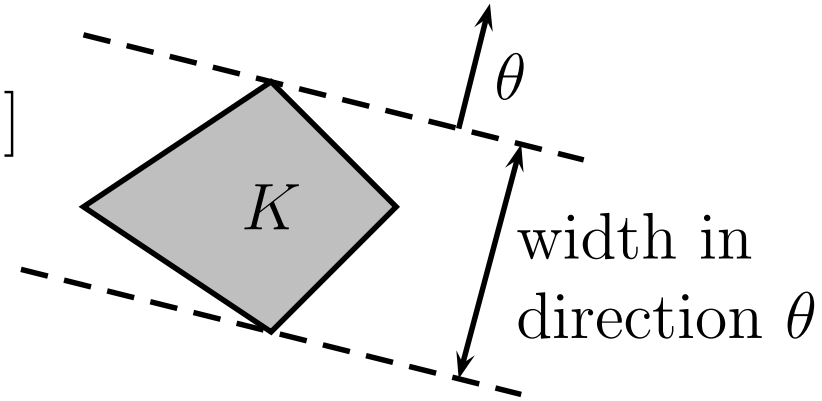


- Also called **ℓ-position**

Urysohn Inequality

- The **mean width** of a convex body K is

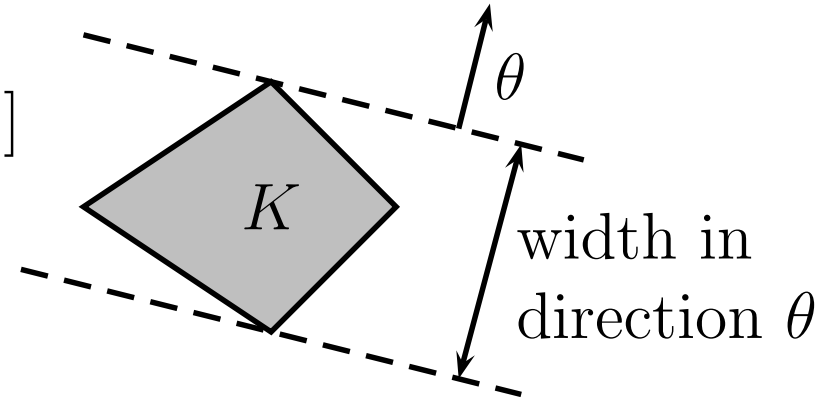
$$w(K) := \mathop{\mathbb{E}}_{\theta \sim S^{n-1}} [\max\{\langle \theta, x - y \rangle : x, y \in K\}]$$



Urysohn Inequality

- The **mean width** of a convex body K is

$$w(K) := \mathop{\mathbb{E}}_{\theta \sim S^{n-1}} [\max\{\langle \theta, x - y \rangle : x, y \in K\}]$$



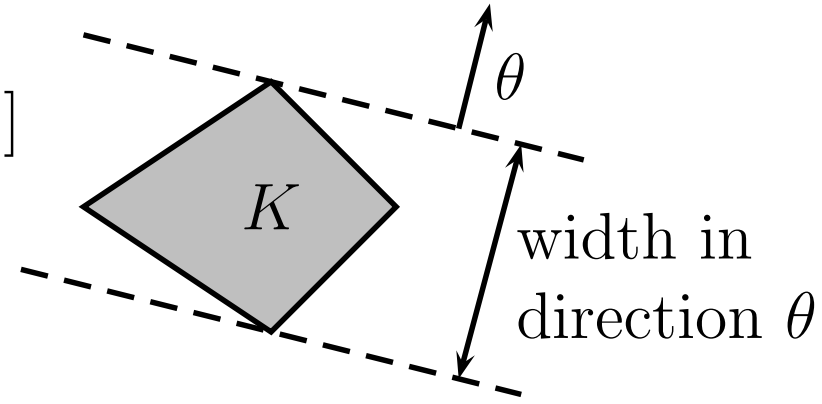
Theorem (Urysohn Inequality)

Among convex bodies of the same volume, the Euclidean ball minimizes the mean width.

Urysohn Inequality

- The **mean width** of a convex body K is

$$w(K) := \mathop{\mathbb{E}}_{\theta \sim S^{n-1}} [\max\{\langle \theta, x - y \rangle : x, y \in K\}]$$



Theorem (Urysohn Inequality)

Among convex bodies of the same volume, the Euclidean ball minimizes the mean width.

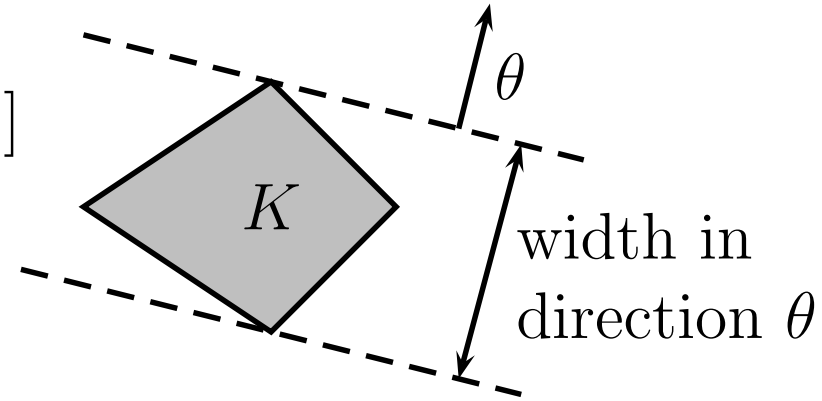
Consequences:

- For any convex body $K \subseteq \mathbb{R}^n$, $w(K) \geq 2 \cdot \left(\frac{\mathrm{Vol}_n(K)}{\mathrm{Vol}_n(B_2^n)} \right)^{1/n}$.

Urysohn Inequality

- The **mean width** of a convex body K is

$$w(K) := \mathop{\mathbb{E}}_{\theta \sim S^{n-1}} [\max\{\langle \theta, x - y \rangle : x, y \in K\}]$$



Theorem (Urysohn Inequality)

Among convex bodies of the same volume, the Euclidean ball minimizes the mean width.

Consequences:

- For any convex body $K \subseteq \mathbb{R}^n$, $w(K) \geq 2 \cdot \left(\frac{\mathrm{Vol}_n(K)}{\mathrm{Vol}_n(B_2^n)} \right)^{1/n}$.
- For symmetric convex body K, $\ell_{K^\circ} \asymp \sqrt{n} \cdot w(K)$ and so $\mathrm{Vol}_n(K)^{1/n} \lesssim \frac{\ell_{K^\circ}}{n}$

Main theorem for stable + ℓ-position

Proposition

Let K be a symmetric convex body and let Λ be **stable lattice**.

(a) If K in **ℓ-position** then $\mu(\Lambda, K) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

(b) One has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

Main theorem for stable + ℓ-position

Proposition

Let K be a symmetric convex body and let Λ be **stable lattice**.

(a) If K in **ℓ-position** then $\mu(\Lambda, K) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

(b) One has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

- First (b). Set $t := \Theta(\log n)$. After scaling $\ell_K \leq o(1)$.

Main theorem for stable + ℓ-position

Proposition

Let K be a symmetric convex body and let Λ be **stable lattice**.

(a) If K in **ℓ-position** then $\mu(\Lambda, K) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

(b) One has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

- First (b). Set $t := \Theta(\log n)$. After scaling $\ell_K \leq o(1)$.
- Suppose for contradiction that $(u + \Lambda) \cap tK = \emptyset$.

Main theorem for stable + ℓ-position

Proposition

Let K be a symmetric convex body and let Λ be **stable lattice**.

(a) If K in **ℓ-position** then $\mu(\Lambda, K) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

(b) One has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

- First (b). Set $t := \Theta(\log n)$. After scaling $\ell_K \leq o(1)$.
- Suppose for contradiction that $(u + \Lambda) \cap tK = \emptyset$.
- Then $\rho_t((u + \Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]

Main theorem for stable + ℓ-position

Proposition

Let K be a symmetric convex body and let Λ be **stable lattice**.

(a) If K in **ℓ-position** then $\mu(\Lambda, K) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

(b) One has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

- First (b). Set $t := \Theta(\log n)$. After scaling $\ell_K \leq o(1)$.
- Suppose for contradiction that $(u + \Lambda) \cap tK = \emptyset$.
- Then $\rho_t((u + \Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
- Λ^* also stable.

Main theorem for stable + ℓ-position

Proposition

Let K be a symmetric convex body and let Λ be **stable lattice**.

(a) If K in **ℓ-position** then $\mu(\Lambda, K) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

(b) One has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

- First (b). Set $t := \Theta(\log n)$. After scaling $\ell_K \leq o(1)$.
- Suppose for contradiction that $(u + \Lambda) \cap tK = \emptyset$.
- Then $\rho_t((u + \Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
- Λ^* also stable.
- $\rho_{1/t}(\Lambda^* \setminus \{\mathbf{0}\}) \leq o(1)$ [Reverse Minkowski Theorem, RS]

Main theorem for stable + ℓ-position

Proposition

Let K be a symmetric convex body and let Λ be **stable lattice**.

(a) If K in **ℓ-position** then $\mu(\Lambda, K) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

(b) One has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

- First (b). Set $t := \Theta(\log n)$. After scaling $\ell_K \leq o(1)$.
- Suppose for contradiction that $(u + \Lambda) \cap tK = \emptyset$.
- Then $\rho_t((u + \Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
- Λ^* also stable.
- $\rho_{1/t}(\Lambda^* \setminus \{\mathbf{0}\}) \leq o(1)$ [Reverse Minkowski Theorem, RS]

Lemma (Variant of Poisson Summ. Formula)

For full rank lattice $\Lambda \subseteq \mathbb{R}^n$, $u \in \mathbb{R}^n$ and $t > 0$ one has

$$\left| \frac{\rho_t(\Lambda + u)}{t^n \det(\Lambda^*)} - 1 \right| \leq \rho_{1/t}(\Lambda^* \setminus \{\mathbf{0}\}).$$

Main theorem for stable + ℓ-position (2)

- We summarize
  - (i) Then $\rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
  - (ii) $(u+\Lambda) \cap tK = \emptyset$.
  - (iii) $\rho_t(\Lambda) \approx \rho_t(u+\Lambda)$ for all u.

Main theorem for stable + ℓ-position (2)

- We summarize
  - (i) Then $\rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
  - (ii) $(u+\Lambda) \cap tK = \emptyset$.
  - (iii) $\rho_t(\Lambda) \approx \rho_t(u+\Lambda)$ for all u.
- Hence

$$\rho_t(\Lambda) \approx \rho_t(u+\Lambda) = \rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$$

Main theorem for stable + ℓ-position (2)

- We summarize
  - (i) Then $\rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
  - (ii) $(u+\Lambda) \cap tK = \emptyset$.
  - (iii) $\rho_t(\Lambda) \approx \rho_t(u+\Lambda)$ for all u.
- Hence

$$\rho_t(\Lambda) \approx \rho_t(u+\Lambda) = \rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$$

- Contradiction! Hence $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$, giving (b).

Main theorem for stable + ℓ-position (2)

- We summarize
  - (i) Then $\rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
  - (ii) $(u+\Lambda) \cap tK = \emptyset$.
  - (iii) $\rho_t(\Lambda) \approx \rho_t(u+\Lambda)$ for all u.
- Hence

$$\rho_t(\Lambda) \approx \rho_t(u+\Lambda) = \rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$$

- Contradiction! Hence $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$, giving (b).
- For (a), choose $W := \mathbb{R}^n$. Then

$$\mu_{KL}(\Lambda, K) \geq \left(\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)}\right)^{1/n}$$

Main theorem for stable + ℓ-position (2)

- We summarize
  - (i) Then $\rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
  - (ii) $(u+\Lambda) \cap tK = \emptyset$.
  - (iii) $\rho_t(\Lambda) \approx \rho_t(u+\Lambda)$ for all u.
- Hence

$$\rho_t(\Lambda) \approx \rho_t(u+\Lambda) = \rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$$

- Contradiction! Hence $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$, giving (b).
- For (a), choose $W := \mathbb{R}^n$. Then

$$\mu_{KL}(\Lambda, K) \geq \left(\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)}\right)^{1/n} \gtrsim \frac{n}{\ell_{K^\circ}}$$

- Use $\det(\Lambda) = 1$ and **Urysohn inequality.**

Main theorem for stable + ℓ-position (2)

- We summarize
  - (i) Then $\rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$ [Banaszczyk 1996]
  - (ii) $(u+\Lambda) \cap tK = \emptyset$.
  - (iii) $\rho_t(\Lambda) \approx \rho_t(u+\Lambda)$ for all u.
- Hence

$$\rho_t(\Lambda) \approx \rho_t(u+\Lambda) = \rho_t((u+\Lambda) \setminus t \cdot K) \leq o(1) \cdot \rho_t(\Lambda)$$

- Contradiction! Hence $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$, giving (b).
- For (a), choose $W := \mathbb{R}^n$. Then

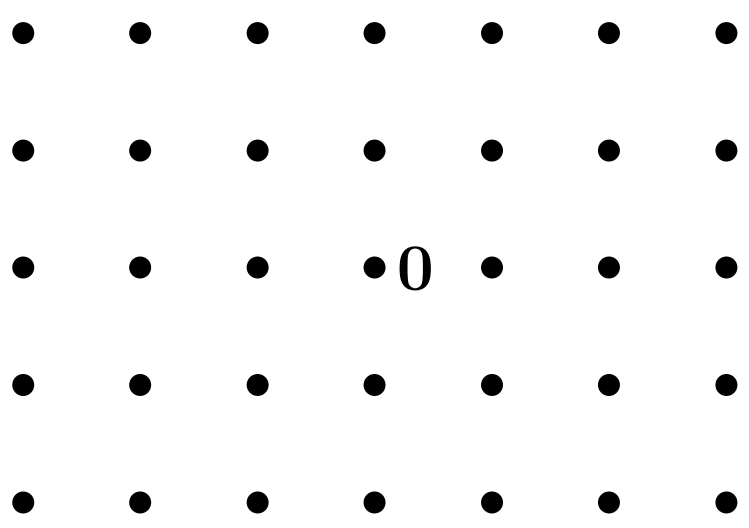
$$\mu_{KL}(\Lambda, K) \geq \left(\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)}\right)^{1/n} \gtrsim \frac{n}{\ell_{K^\circ}} \overset{\ell\text{-position}}{\gtrsim} \frac{\ell_K}{\log(n)}$$

- Use $\det(\Lambda) = 1$ and **Urysohn inequality.** □

Recap: Quotient lattices

Definition

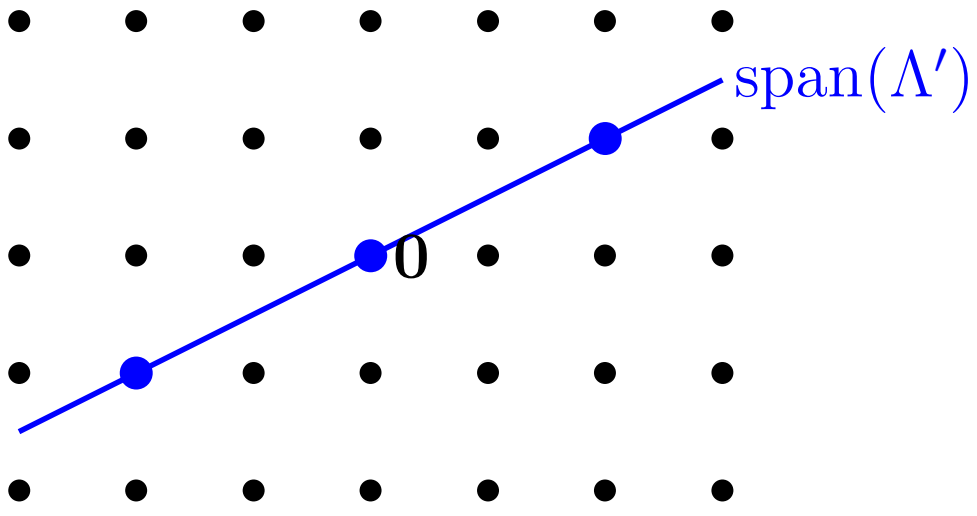
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$.



Recap: Quotient lattices

Definition

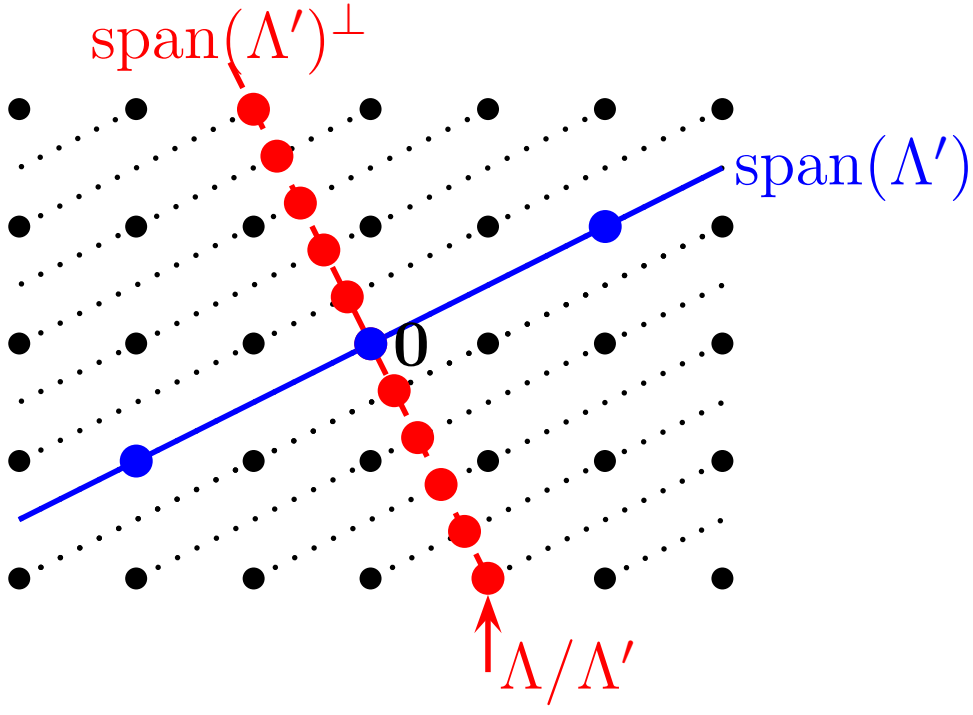
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$.



Recap: Quotient lattices

Definition

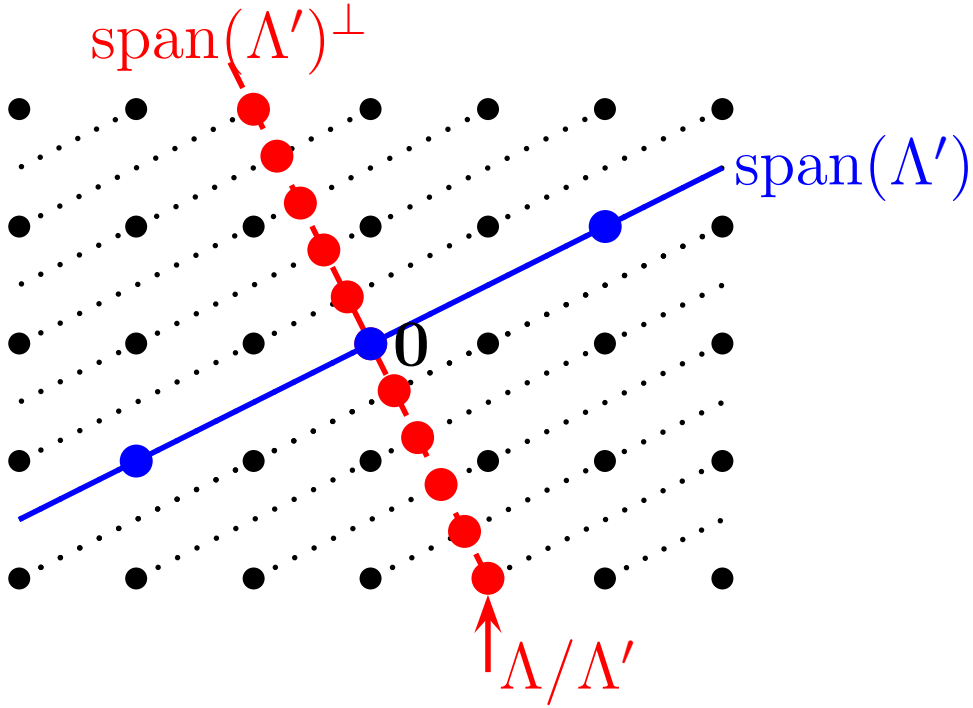
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$.



Recap: Quotient lattices

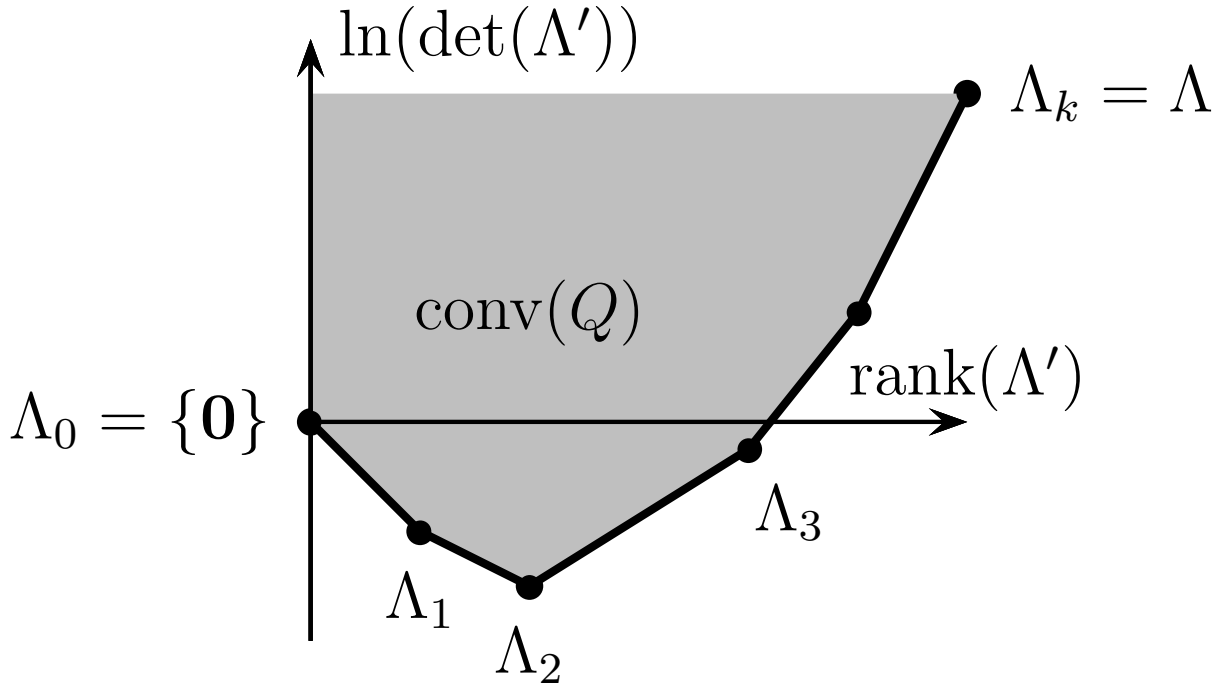
Definition

Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\mathrm{span}(\Lambda')^\perp}(\Lambda)$.



- **Intuition:** We can factor Λ into Λ' and Λ/Λ'
- For example $\det(\Lambda) = \det(\Lambda') \cdot \det(\Lambda/\Lambda')$.

Recap: The canonical filtration



Theorem (Canonical filtration)

(a) *The vertices of the canonical plot form a chain*

$$\{\mathbf{0}\} = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_k = \Lambda.$$

(b) $r_i := \det(\Lambda_i/\Lambda_{i-1})^{1/rank(\Lambda_i/\Lambda_{i-1})}$ *satisfy* $r_1 < \ldots < r_k$

(c) *Each* $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ *is stable.*

Main proof

Simplifying assumption: K symmetric.

Main proof

Simplifying assumption: K symmetric.

First proof attempt:

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$

Main proof

Simplifying assumption: K symmetric.

First proof attempt:

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$
- Now treat K like scaling of B_2^n and use only information from Canonical Filtration of Λ (as [Regev, Stephens-Davidowitz 2016] do it).

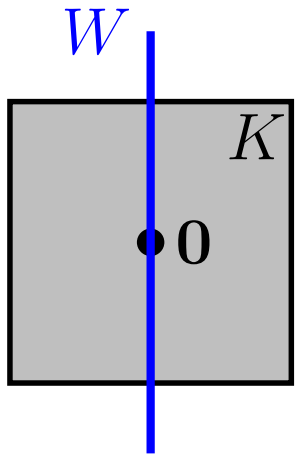
Main proof

Simplifying assumption: K symmetric.

First proof attempt:

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$
- Now treat K like scaling of B_2^n and use only information from Canonical Filtration of Λ (as [Regev, Stephens-Davidowitz 2016] do it).

Problem: $\mu(\Lambda, K)$ might be determined by a low-dimensional subspace and for a subspace $W \subseteq \mathbb{R}^n$ with say $\dim(W) = \Theta(1)$, $\mathrm{Vol}_d(\Pi_W(K))^{1/d}$ only determined up to $\Theta(\sqrt{n})$ factor!



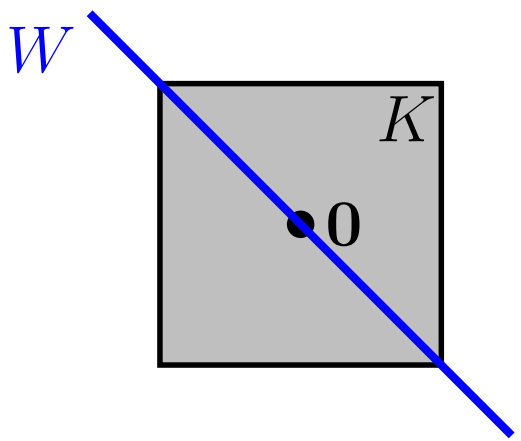
Main proof

Simplifying assumption: K symmetric.

First proof attempt:

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$
- Now treat K like scaling of B_2^n and use only information from Canonical Filtration of Λ (as [Regev, Stephens-Davidowitz 2016] do it).

Problem: $\mu(\Lambda, K)$ might be determined by a low-dimensional subspace and for a subspace $W \subseteq \mathbb{R}^n$ with say $\dim(W) = \Theta(1)$, $\mathrm{Vol}_d(\Pi_W(K))^{1/d}$ only determined up to $\Theta(\sqrt{n})$ factor!



Main proof

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

Main proof

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Full result follows by induction paying an extra $\log(n)$ factor!

Main proof

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Full result follows by induction paying an extra $\log(n)$ factor!

Proof.

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$

Main proof

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Full result follows by induction paying an extra $\log(n)$ factor!

Proof.

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$
- Consider canonical filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$.

Main proof

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Full result follows by induction paying an extra $\log(n)$ factor!

Proof.

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$
- Consider canonical filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$.
- Define

$$d_i := \operatorname{rank}(\Lambda_i / \Lambda_{i-1}) \quad \text{and} \quad r_i := \det(\Lambda_i / \Lambda_{i-1})^{1/d_i}$$

Main proof

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Full result follows by induction paying an extra $\log(n)$ factor!

Proof.

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$
- Consider canonical filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$.
- Define

$$d_i := \operatorname{rank}(\Lambda_i / \Lambda_{i-1}) \quad \text{and} \quad r_i := \det(\Lambda_i / \Lambda_{i-1})^{1/d_i}$$

- Group indices of similar density together: $r_i \leq \frac{1}{2} r_{i+2}$

Main proof

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Full result follows by induction paying an extra $\log(n)$ factor!

Proof.

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$
- Consider canonical filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$.
- Define

$$d_i := \operatorname{rank}(\Lambda_i / \Lambda_{i-1}) \quad \text{and} \quad r_i := \det(\Lambda_i / \Lambda_{i-1})^{1/d_i}$$

- Group indices of similar density together: $r_i \leq \frac{1}{2} r_{i+2}$
- Let $i^* \in \{1, \ldots, k\}$ minimal s.t. $\operatorname{rank}(\Lambda_{i^*}) \geq \frac{n}{2}$.

Main proof

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Full result follows by induction paying an extra $\log(n)$ factor!

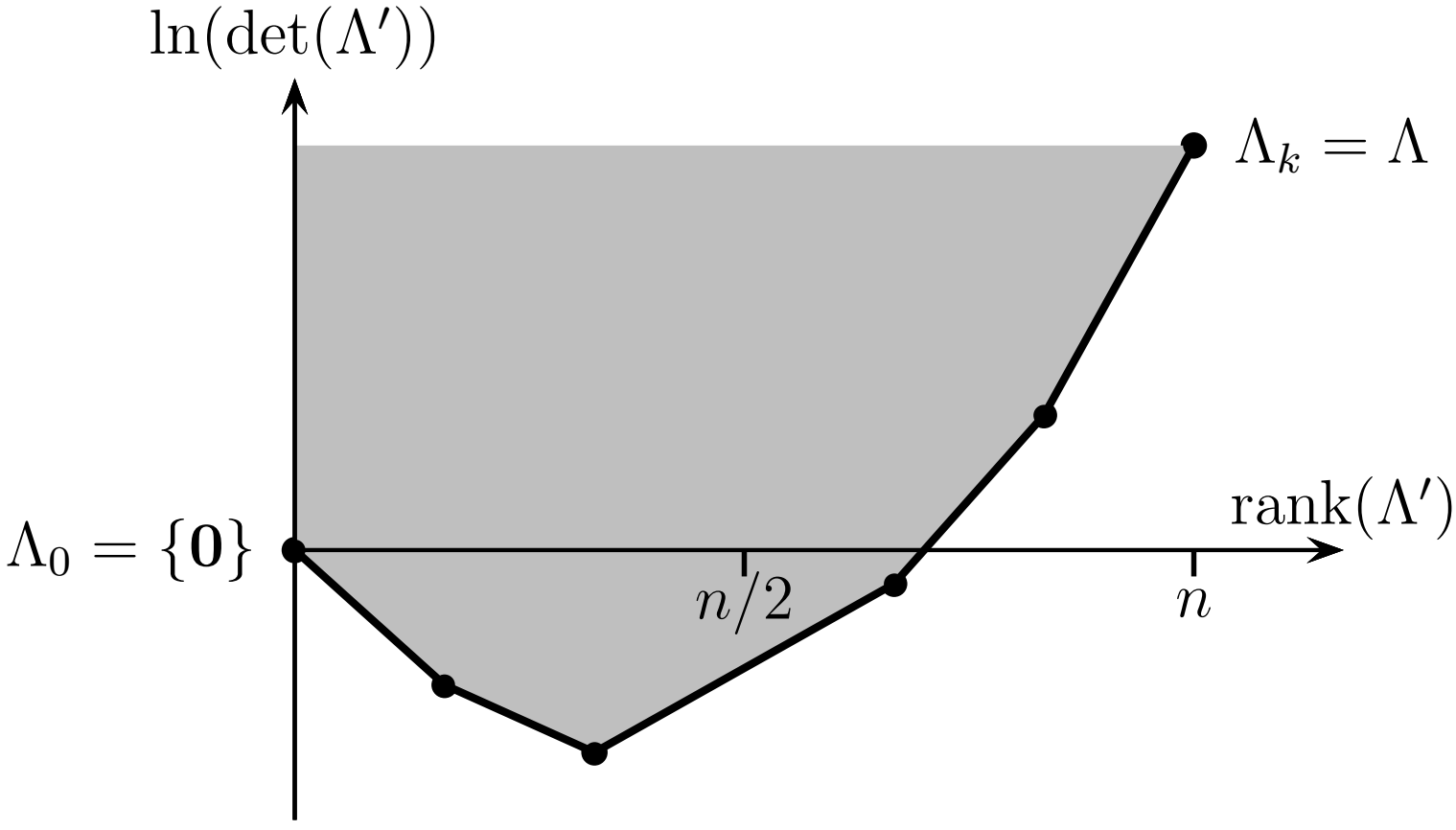
Proof.

- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$
- Consider canonical filtration $\{\mathbf{0}\} = \Lambda_0 \subset \ldots \subset \Lambda_k = \Lambda$.
- Define

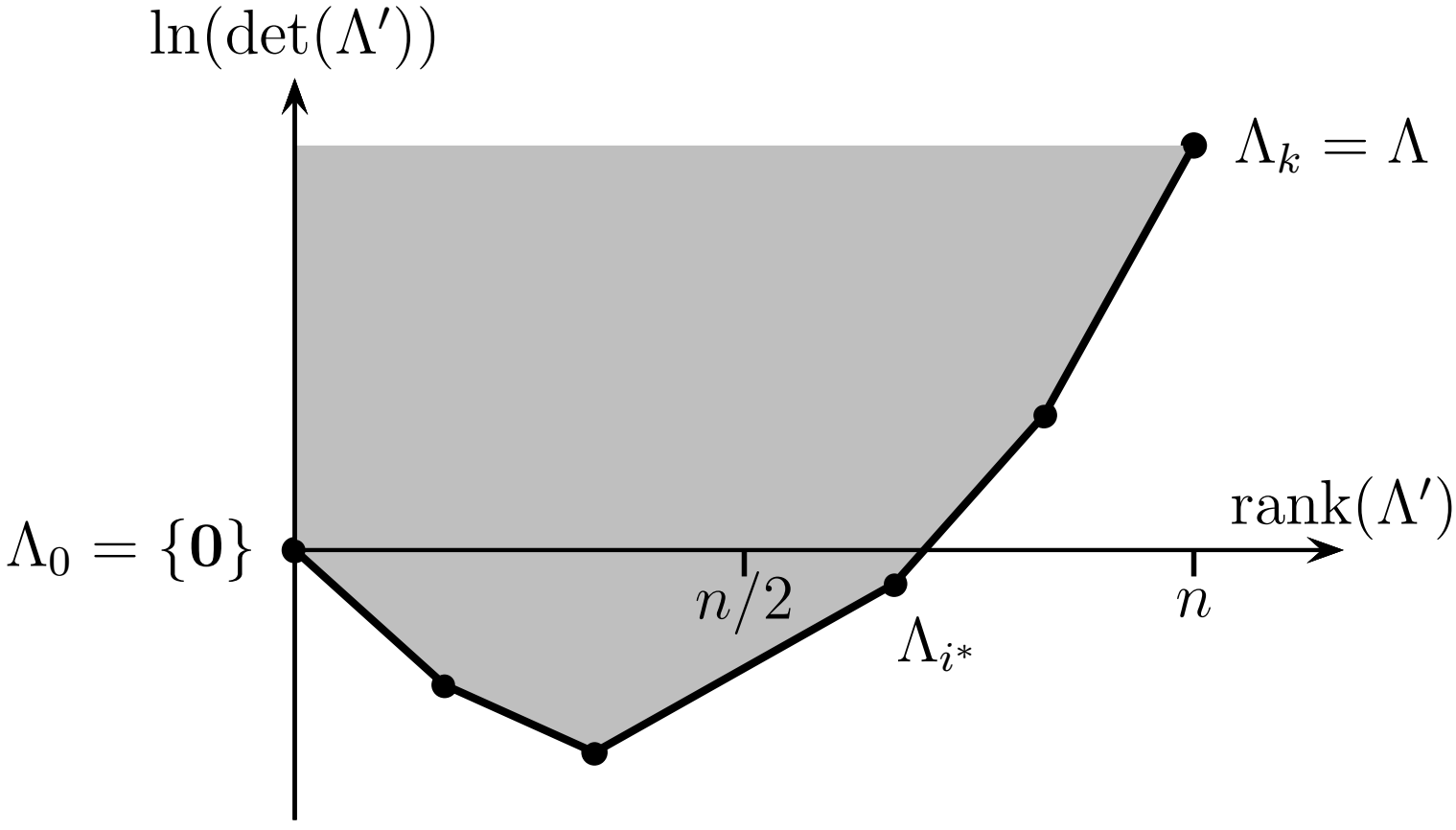
$$d_i := \operatorname{rank}(\Lambda_i / \Lambda_{i-1}) \quad \text{and} \quad r_i := \det(\Lambda_i / \Lambda_{i-1})^{1/d_i}$$

- Group indices of similar density together: $r_i \leq \frac{1}{2} r_{i+2}$
- Let $i^* \in \{1, \ldots, k\}$ minimal s.t. $\operatorname{rank}(\Lambda_{i^*}) \geq \frac{n}{2}$.
- Set $U := \operatorname{span}(\Lambda_{i^*})$

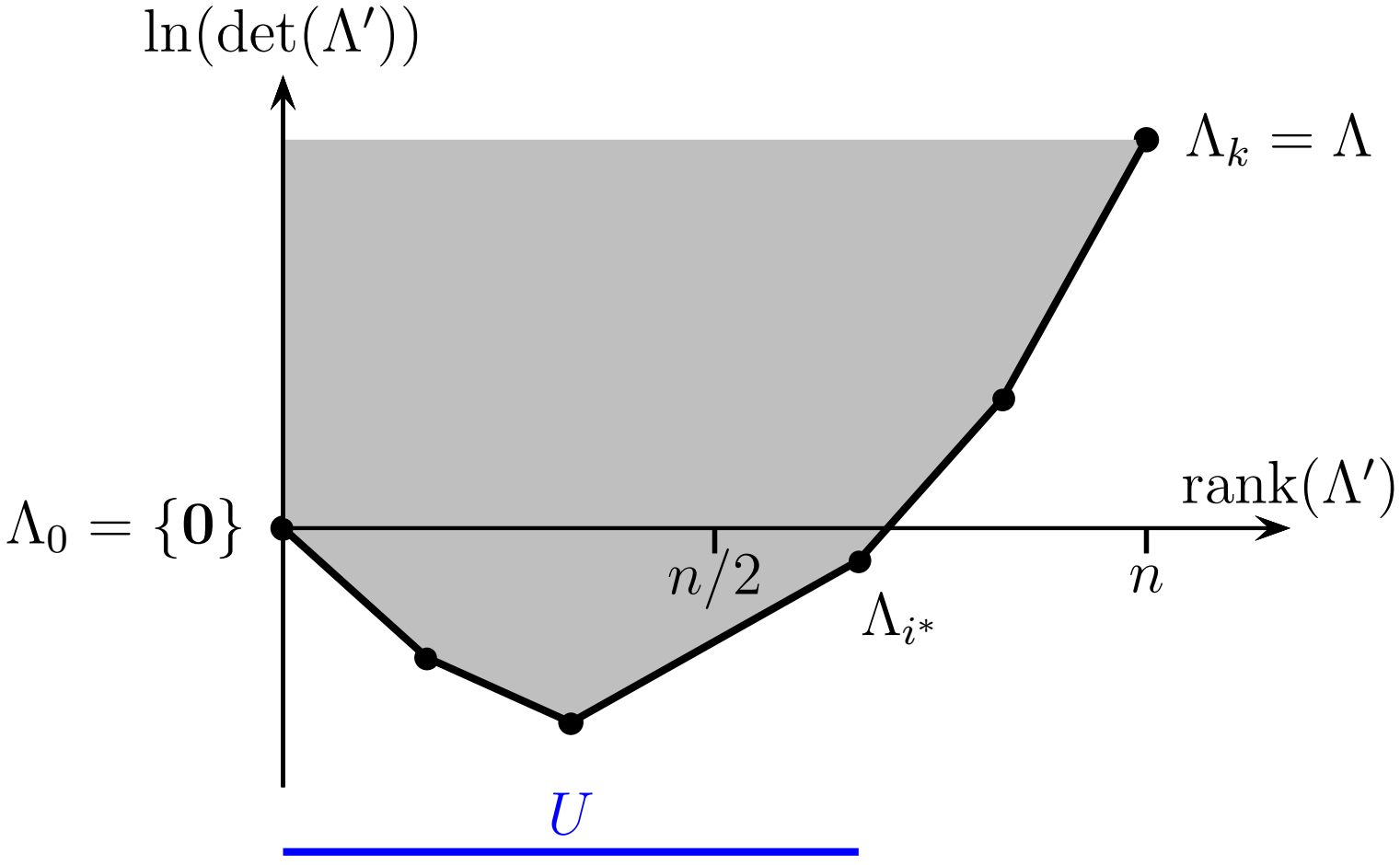
Main proof (2)



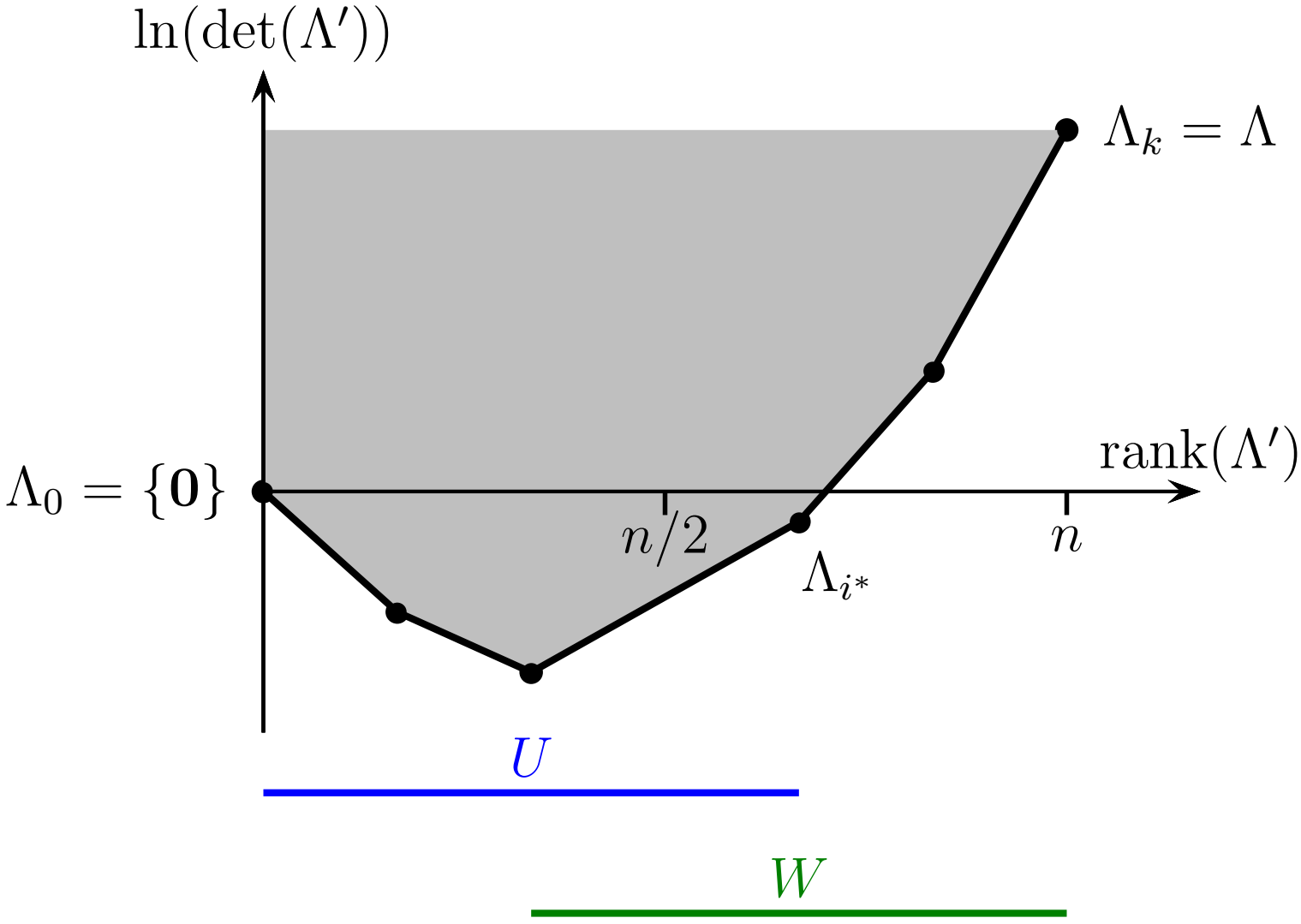
Main proof (2)



Main proof (2)



Main proof (2)


$\ln(\det(\Lambda'))$
$\Lambda_k = \Lambda$
$\Lambda_0 = \{\mathbf{0}\}$
$\mathrm{rank}(\Lambda')$
$n/2$
n
Λ_{i*}
U
W

Main proof (3)

Claim I. $\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K$

Main proof (3)

Claim I. $\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K$

Proof of Claim I. We bound

$$\mu(\Lambda \cap U, K \cap U) \overset{\text{triangle ineq.}}{\leq} \sum_{i=1}^{i^*} \mu\big(\Lambda_i / \Lambda_{i-1}, K_i\big)$$

- $K_i := \Pi_{\mathrm{span}(\Lambda_{i-1})^\perp}(K \cap \mathrm{span}(\Lambda_i))$

Main proof (3)

Claim I. $\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K$

Proof of Claim I. We bound

$$\mu(\Lambda \cap U, K \cap U) \overset{\text{triangle ineq.}}{\leq} \sum_{i=1}^{i^*} \mu\big(\underbrace{\Lambda_i/\Lambda_{i-1}}_{r_i\cdot\text{stable lattice}}, K_i\big)$$

- $K_i := \Pi_{\mathrm{span}(\Lambda_{i-1})^\perp}(K \cap \mathrm{span}(\Lambda_i))$
- Recall: $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ stable

Main proof (3)

Claim I. $\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K$

Proof of Claim I. We bound

$$\mu(\Lambda \cap U, K \cap U) \overset{\text{triangle ineq.}}{\leq} \sum_{i=1}^{i^*} \mu\big(\underbrace{\Lambda_i/\Lambda_{i-1}}_{r_i\cdot\text{stable lattice}}, K_i\big)$$

$$\lesssim \sum_{i=1}^{i^*} \log(n) \cdot r_i \cdot \ell_{K_i}$$

- $K_i := \Pi_{\mathrm{span}(\Lambda_{i-1})^\perp}(K \cap \mathrm{span}(\Lambda_i))$
- Recall: $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ stable

Main proof (3)

Claim I. $\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K$

Proof of Claim I. We bound

$$\begin{aligned}
\mu(\Lambda \cap U, K \cap U) &\overset{\text{triangle ineq.}}{\leq} \sum_{i=1}^{i^*} \mu\big(\underbrace{\Lambda_i/\Lambda_{i-1}}_{r_i\cdot\text{stable lattice}}, K_i\big) \\
&\lesssim \sum_{i=1}^{i^*} \log(n) \cdot r_i \cdot \ell_{K_i} \\
&\lesssim \log(n) \cdot r_{i^*} \cdot \ell_K
\end{aligned}$$

- $K_i := \Pi_{\mathrm{span}(\Lambda_{i-1})^\perp}(K \cap \mathrm{span}(\Lambda_i))$
- Recall: $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ stable
- Use monotonicity of ℓ-value: $\ell_{K\cap F} \leq \ell_K$ for subspace F (potentially huge loss!!)

Main proof (4)

Claim II. $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_{i^*}}{\log(n)} \cdot \ell_K$.

Main proof (4)

Claim II. $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_{i^*}}{\log(n)} \cdot \ell_K$.

- Set $W := \mathrm{span}(\Lambda_{i^*-1})^{\perp}$ and $d := \dim(W) = \sum_{i=i^*}^{k} d_i \geq \frac{n}{2}$

Main proof (4)

Claim II. $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_{i^*}}{\log(n)} \cdot \ell_K$.

- Set $W := \mathrm{span}(\Lambda_{i^*-1})^\perp$ and $d := \dim(W) = \sum_{i=i^*}^{k} d_i \geq \frac{n}{2}$

$$\mu_{KL}(\Lambda, K) \quad \geq \quad \left(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))} \right)^{1/d}$$

Main proof (4)

Claim II. $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_{i^*}}{\log(n)} \cdot \ell_K$.

- Set $W := \mathrm{span}(\Lambda_{i^*-1})^\perp$ and $d := \dim(W) = \sum_{i=i^*}^{k} d_i \geq \frac{n}{2}$

$$\begin{aligned} \mu_{KL}(\Lambda, K) &\geq \left(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\right)^{1/d} \\ &\geq \frac{r_{i^*}}{\mathrm{Vol}_d(\Pi_W(K))^{1/d}} \end{aligned}$$

We use

- $\det(\Pi_W(\Lambda)) = \det(\Lambda/\Lambda_{i^*-1}) \geq r_{i^*}^d$

Main proof (4)

Claim II. $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_{i^*}}{\log(n)} \cdot \ell_K$.

- Set $W := \mathrm{span}(\Lambda_{i^*-1})^\perp$ and $d := \dim(W) = \sum_{i=i^*}^{k} d_i \geq \frac{n}{2}$

$$\begin{aligned} \mu_{KL}(\Lambda, K) &\geq \left(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\right)^{1/d} \\ &\geq \frac{r_{i^*}}{\mathrm{Vol}_d(\Pi_W(K))^{1/d}} \\ &\gtrsim r_{i^*} \cdot \frac{d}{\ell_{K^\circ}} \end{aligned}$$

We use

- $\det(\Pi_W(\Lambda)) = \det(\Lambda/\Lambda_{i^*-1}) \geq r_{i^*}^d$
- **Urysohn inequality** and $\Pi_W(K)^\circ = K^\circ \cap W$

Main proof (4)

Claim II. $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_{i^*}}{\log(n)} \cdot \ell_K$.

- Set $W := \mathrm{span}(\Lambda_{i^*-1})^\perp$ and $d := \dim(W) = \sum_{i=i^*}^{k} d_i \geq \frac{n}{2}$

$$\begin{aligned}
\mu_{KL}(\Lambda, K) &\geq \left(\frac{\det(\Pi_W(\Lambda))}{\mathrm{Vol}_d(\Pi_W(K))}\right)^{1/d} \\
&\geq \frac{r_{i^*}}{\mathrm{Vol}_d(\Pi_W(K))^{1/d}} \\
&\gtrsim r_{i^*} \cdot \frac{d}{\ell_{K^\circ}} \overset{\ell\text{-position}}{\gtrsim} \frac{r_{i^*}}{\log(n)} \cdot \underbrace{\frac{d}{n}}_{\geq 1/2} \cdot \ell_K
\end{aligned}$$

We use

- $\det(\Pi_W(\Lambda)) = \det(\Lambda/\Lambda_{i^*-1}) \geq r_{i^*}^d$
- **Urysohn inequality** and $\Pi_W(K)^\circ = K^\circ \cap W$ □

Main proof (5)

Claim I. $\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K$

Claim II. $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_{i^*}}{\log(n)} \cdot \ell_K$.

Main proof (5)

Claim I. $\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K$
Claim II. $\mu_{KL}(\Lambda, K) \gtrsim \frac{r_{i^*}}{\log(n)} \cdot \ell_K$.

Putting everything together

$$\mu(\Lambda, K) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K \lesssim \log^2(n) \cdot \mu_{KL}(\Lambda, K) \quad \square$$

The asymmetric case

Proposition

Let $K \subseteq \mathbb{R}^n$ be symmetric and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

The asymmetric case

Proposition

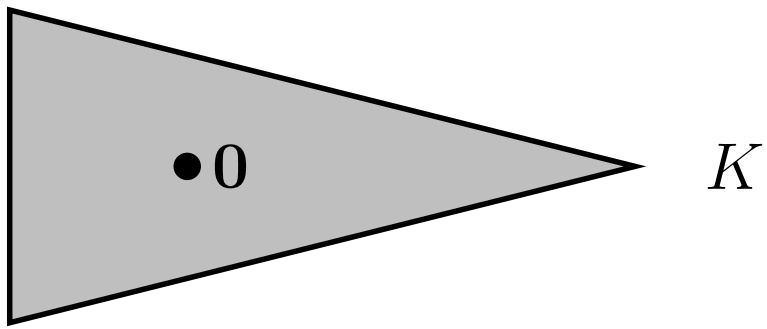
Let $K \subseteq \mathbb{R}^n$ be ~~symmetric~~ and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

The asymmetric case

Proposition

Let $K \subseteq \mathbb{R}^n$ be ~~symmetric~~ and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Assume barycenter is at $\mathbf{0}$

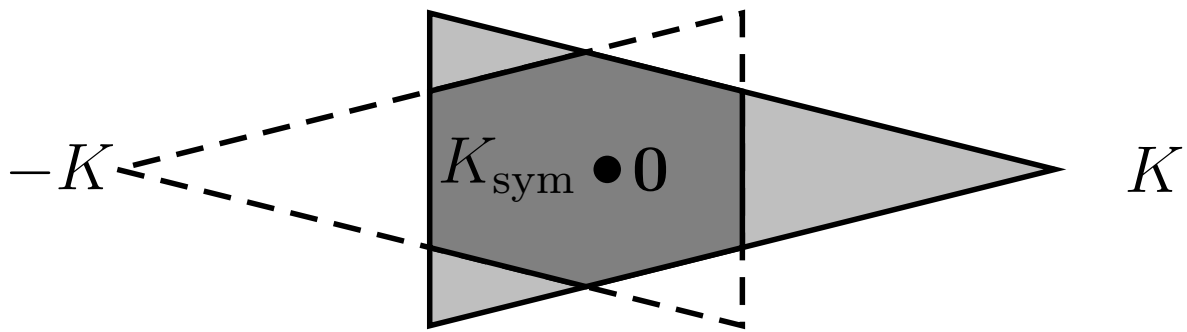


The asymmetric case

Proposition

Let $K \subseteq \mathbb{R}^n$ be ~~symmetric~~ and convex, let $\Lambda \subseteq \mathbb{R}^n$. $\exists$ subspace $U : \dim(U) \geq \frac{n}{2}$ and $\mu(\Lambda \cap U, K \cap U) \leq O(\log^2 n) \cdot \mu_{KL}(\Lambda, K)$.

- Assume barycenter is at $\mathbf{0}$
- Let $K_{\text{sym}} := K \cap -K$ (**inner symmetrizer**)



The asymmetric case

- Use $\mu(\Lambda \cap U, K \cap U) \leq \mu(\Lambda \cap U, K_{\mathrm{sym}} \cap U)$.

The asymmetric case

- Use $\mu(\Lambda \cap U, K \cap U) \leq \mu(\Lambda \cap U, K_{\mathrm{sym}} \cap U)$.
- Need that

$$\mathrm{Vol}_d(\Pi_W(K))^{1/d} \lesssim \mathrm{Vol}_d(\Pi_W(K_{\mathrm{sym}}))^{1/d}$$

The asymmetric case

- Use $\mu(\Lambda \cap U, K \cap U) \leq \mu(\Lambda \cap U, K_{\mathrm{sym}} \cap U)$.
- Need that

$$\mathrm{Vol}_d(\Pi_W(K))^{1/d} \lesssim \mathrm{Vol}_d(\Pi_W(K_{\mathrm{sym}}))^{1/d}$$

Proposition (Vritsiou '23)

Let $K \subseteq \mathbb{R}^n$ be a convex body with barycenter at $\mathbf{0}$. Let $F \subseteq \mathbb{R}^n$ be a d-dimensional subspace. Then

$$\mathrm{Vol}_d(\Pi_F(K))^{1/d} \lesssim \left(\frac{n}{d}\right)^6 \cdot \mathrm{Vol}_d(\Pi_F(K \cap -K))^{1/d}.$$

The asymmetric case

- Use $\mu(\Lambda \cap U, K \cap U) \leq \mu(\Lambda \cap U, K_{\mathrm{sym}} \cap U)$.
- Need that

$$\mathrm{Vol}_d(\Pi_W(K))^{1/d} \lesssim \mathrm{Vol}_d(\Pi_W(K_{\mathrm{sym}}))^{1/d}$$

- Works for us since we have $d \geq \frac{n}{2}$!

Proposition (Vritsiou '23)

Let $K \subseteq \mathbb{R}^n$ be a convex body with barycenter at $\mathbf{0}$. Let $F \subseteq \mathbb{R}^n$ be a d-dimensional subspace. Then

$$\mathrm{Vol}_d(\Pi_F(K))^{1/d} \lesssim \left(\frac{n}{d}\right)^6 \cdot \mathrm{Vol}_d(\Pi_F(K \cap -K))^{1/d}.$$

End of part 3

Open problem 1

Can one solve every **n-variable integer program** in time $2^{O(n)}$?

- Right now, no candidate pathway known!

End of part 3

Open problem 1

Can one solve every n-**variable integer program** in time $2^{O(n)}$?

- Right now, no candidate pathway known!

Open problem 2

Is there a **certificate** for $K \cap \mathbb{Z}^n = \emptyset$ that can be verified in time $2^{O(n)}$?

End of part 3

Open problem 1

Can one solve every n-**variable integer program** in time $2^{O(n)}$?

- Right now, no candidate pathway known!

Open problem 2

Is there a **certificate** for $K \cap \mathbb{Z}^n = \emptyset$ that can be verified in time $2^{O(n)}$?

Thanks for your attention!