The Subspace Flatness Conjecture and Faster Integer Programming

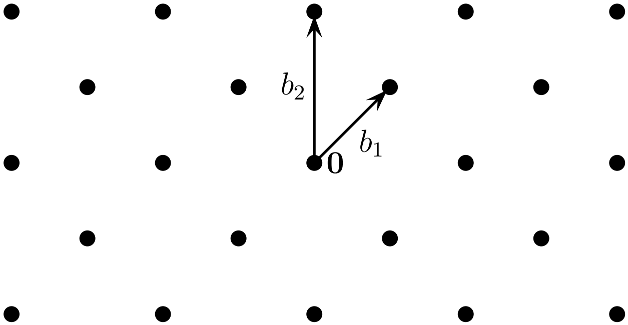
Thomas Rothvoss

Joint work with Victor Reis

UNIVERSITY *of* WASHINGTON

Covering radius

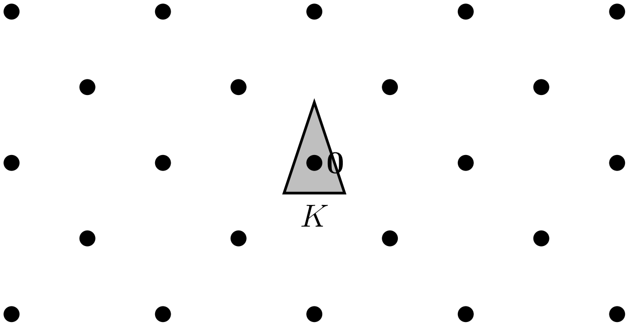
- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.



Covering radius

- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.
- For K convex, the **covering radius** is

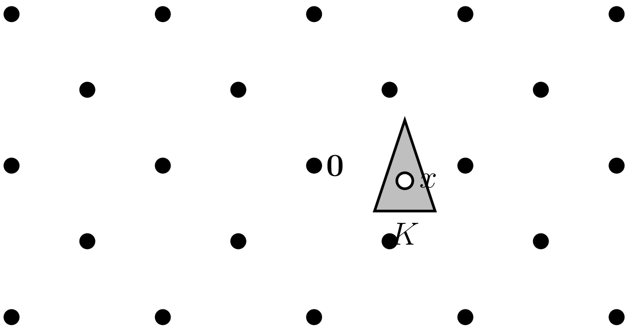
$$\mu(\Lambda, K) \quad = \quad \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\}$$



Covering radius

- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.
- For K convex, the **covering radius** is

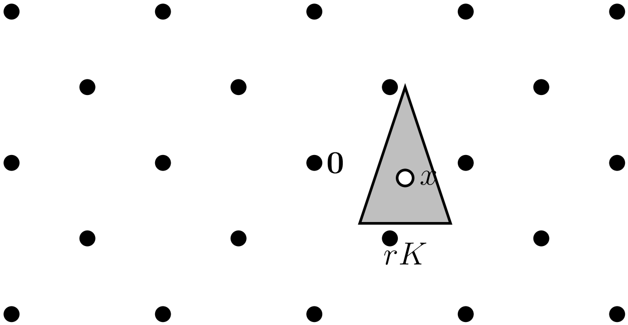
$$\begin{aligned}\mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \ \forall x \in \mathbb{R}^n\}\end{aligned}$$



Covering radius

- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.
- For K convex, the **covering radius** is

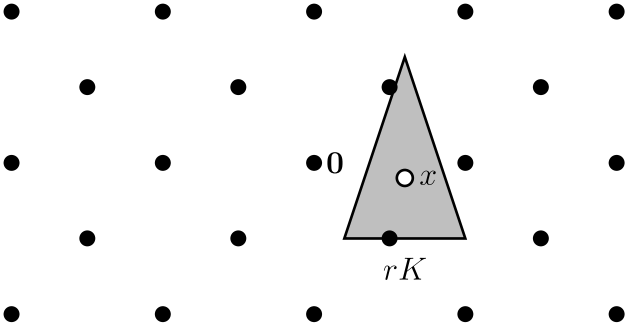
$$\begin{aligned}\mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \ \forall x \in \mathbb{R}^n\}\end{aligned}$$



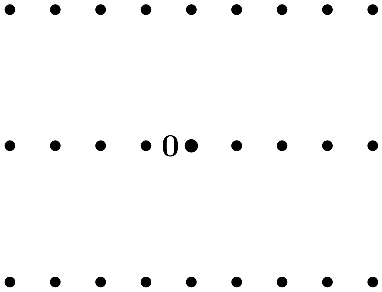
Covering radius

- A **lattice** is a set $\Lambda = \{Bx : x \in \mathbb{Z}^k\}$ where $B \in \mathbb{R}^{n \times k}$ has linearly independent columns.
- For K convex, the **covering radius** is

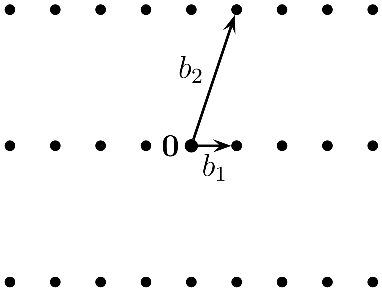
$$\begin{aligned} \mu(\Lambda, K) &= \min\{r \geq 0 \mid \Lambda + rK = \mathbb{R}^n\} \\ &= \min\{r \geq 0 \mid (x + rK) \cap \Lambda \neq \emptyset \ \forall x \in \mathbb{R}^n\} \end{aligned}$$



Lower bounds on the covering radius

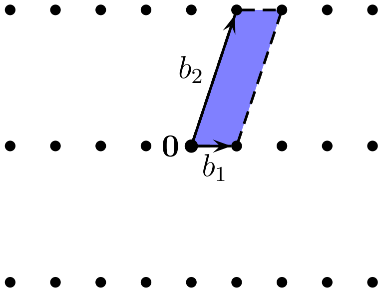


Lower bounds on the covering radius



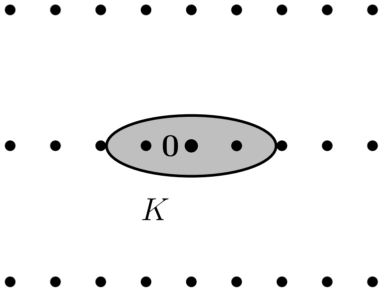
- Pick basis $B = (b_1, \ldots, b_k)$ of Λ

Lower bounds on the covering radius



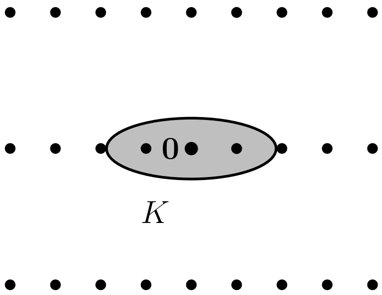
- Pick basis $B = (b_1, \ldots, b_k)$ of Λ
- $\det(\Lambda) = \sqrt{\det(B^T B)}$ =volume of parallelepiped spanned by basis

Lower bounds on the covering radius



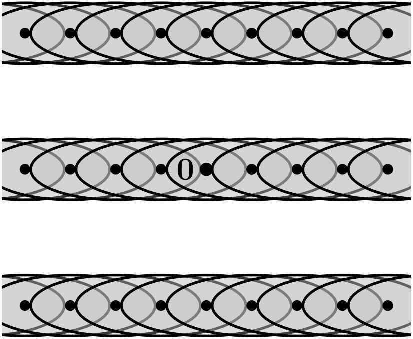
- Pick basis $B = (b_1, \ldots, b_k)$ of Λ
- $\det(\Lambda) = \sqrt{\det(B^T B)}$ =volume of parallelepiped spanned by basis

Lower bounds on the covering radius



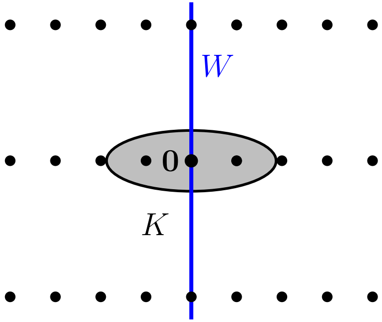
- Pick basis $B = (b_1, \ldots, b_k)$ of Λ
- $\det(\Lambda) = \sqrt{\det(B^T B)}$ =volume of parallelepiped spanned by basis
- Simple lower bound: $\mu(\Lambda, K) \geq (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$

Lower bounds on the covering radius



- Pick basis $B = (b_1, \ldots, b_k)$ of Λ
- $\det(\Lambda) = \sqrt{\det(B^T B)}$ =volume of parallelepiped spanned by basis
- Simple lower bound: $\mu(\Lambda, K) \geq (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$

Lower bounds on the covering radius



- Pick basis $B = (b_1, \ldots, b_k)$ of Λ
- $\det(\Lambda) = \sqrt{\det(B^T B)}$ =volume of parallelepiped spanned by basis
- Simple lower bound: $\mu(\Lambda, K) \geq (\frac{\det(\Lambda)}{\mathrm{Vol}_n(K)})^{1/n}$
- For any subspace $\mu(\Lambda, K) \geq \mu(\Pi_W(\Lambda), \Pi_W(K))$

Kannan, Lovász (1988)

- Consider the best volume-based lower bound

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

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

$$\mu(\Lambda, K) \leq O(\log^7(n)) \cdot \mu_{KL}(\Lambda, K)$$

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

$$\mu(\Lambda, K) \leq O(\log^7(n)) \cdot \mu_{KL}(\Lambda, K)$$

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:

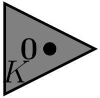
- $2^{O(n^2)}$ [Lenstra '83]
- $n^{O(n)}$ [Kannan '87]
- $2^{O(n)}n^n$ [Dadush '12], [Dadush, Eisenbrand, R. '22]

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

$$\mu(\Lambda, K) \leq O(\log^7(n)) \cdot \mu(\Lambda, K - K)$$

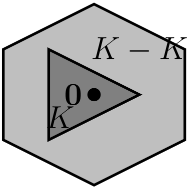


Main results (2)

Theorem (Reis, R.'23)

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

$$\mu(\Lambda, K) \leq O(\log^7(n)) \cdot \mu(\Lambda, K - K)$$

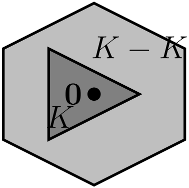


Main results (2)

Theorem (Reis, R.'23)

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

$$\mu(\Lambda, K) \leq O(\log^7(n)) \cdot \mu(\Lambda, K - K)$$



Theorem (Reis, R.'23)

Flatness constant in dimension n is at most $O(n \log^8(n))$.

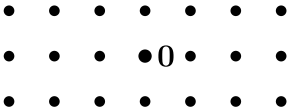
- Previously best known: $O(n^{4/3} \log^{O(1)} n)$ [Rudelson '98+Banaszczyk, Litvak, Pajor, Szarek '99]

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 $s = \Theta(\log n)$,

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

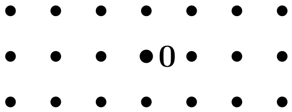


The Reverse Minkowski Theorem

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 $s = \Theta(\log n)$,

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



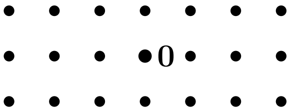
- **Reverse Minkowski Theorem** implies **Subspace Flatness** for **ellipsoids** [Dadush, Regev '16]

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 $s = \Theta(\log n)$,

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



- **Reverse Minkowski Theorem** implies **Subspace Flatness** for **ellipsoids** [Dadush, Regev '16]

Definition

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

ℓ-position

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

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

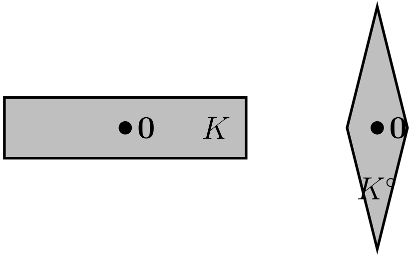
- **Intuitively:** $\ell_K =$ "average thinness" of K

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:** $\ell_K =$ "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

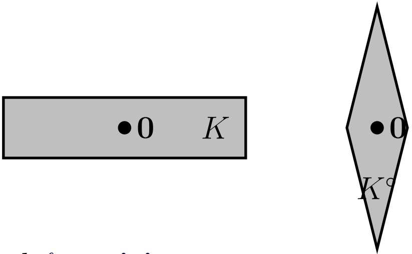
- For a symmetric convex body $K \subseteq \mathbb{R}^n$,

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

- **Intuitively:** $\ell_K =$ "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

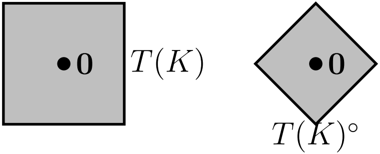
- For a symmetric convex body $K \subseteq \mathbb{R}^n$,

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

- **Intuitively:** $\ell_K =$ "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**

Covering radius of stable lattice

Lemma

For symmetric convex K and stable lattice Λ one has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

Covering radius of stable lattice

Lemma

For symmetric convex K and stable lattice Λ one has $\mu(\Lambda, K) \leq O(\log n) \cdot \ell_K$.

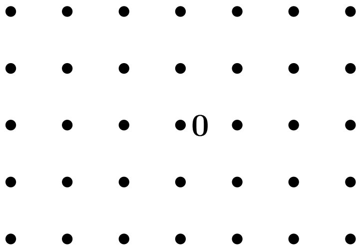
Proof uses:

- Machinery of [Banaszczyk 96]
- $\rho_{1/s}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \frac{1}{2}$ by **Reverse Minkowski Theorem** for $s = \Theta(\log n)$.

Quotient lattices

Definition

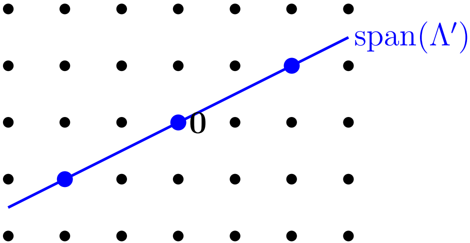
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\text{span}(\Lambda')^\perp}(\Lambda)$.



Quotient lattices

Definition

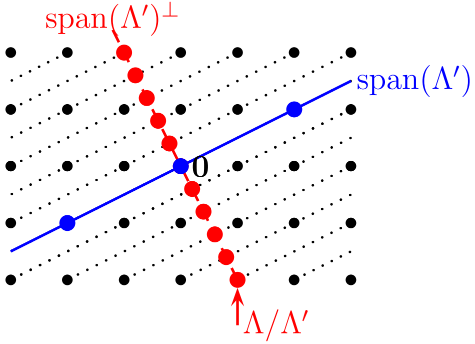
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\text{span}(\Lambda')^\perp}(\Lambda)$.



Quotient lattices

Definition

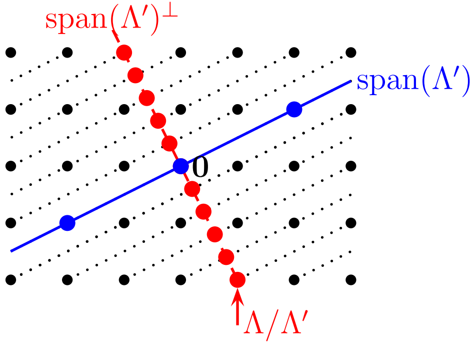
Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ with a primitive sublattice $\Lambda' \subseteq \Lambda$. The **quotient lattice** is $\Lambda/\Lambda' = \Pi_{\text{span}(\Lambda')^\perp}(\Lambda)$.



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'
- For example $\det(\Lambda) = \det(\Lambda') \cdot \det(\Lambda/\Lambda')$.

The canonical filtration

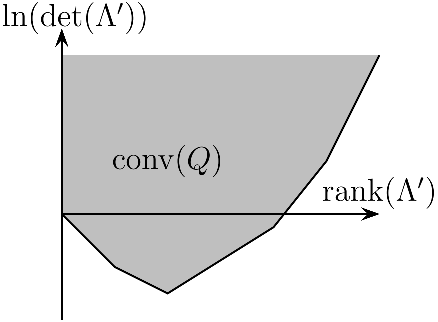
- For lattice $\Lambda \subseteq \mathbb{R}^n$, consider **canonical plot**

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

The canonical filtration

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

$$Q := \{ \big(\mathrm{rank}(\Lambda'), \ln(\det(\Lambda'))\big) \mid \text{sublattice } \Lambda' \subseteq \Lambda \}$$

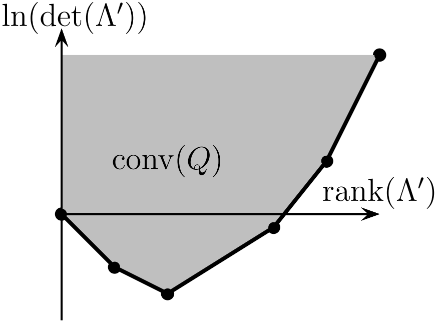


The canonical filtration

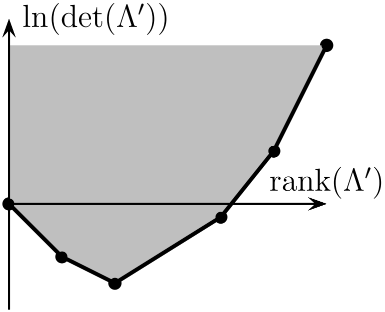
- For lattice $\Lambda \subseteq \mathbb{R}^n$, consider **canonical plot**

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

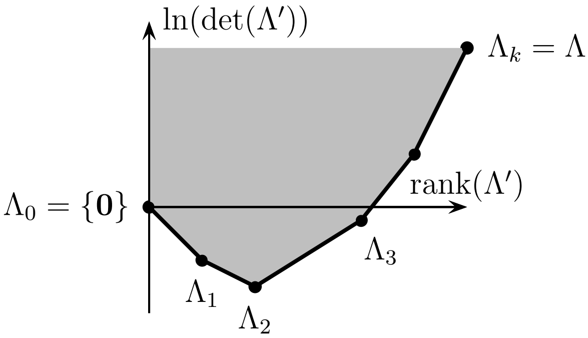
- Lower envelope of $\operatorname{conv}(Q)$ is called **canonical polygon**



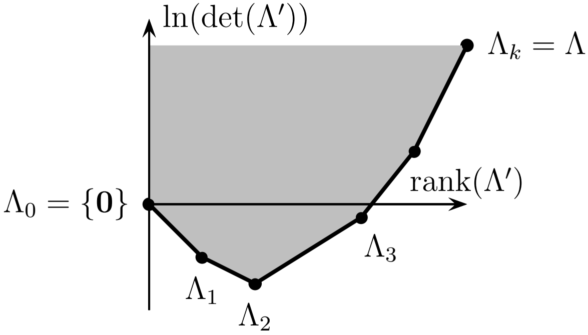
The canonical filtration (2)



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.*

Main proof

- **Simplifying assumption:** K symmetric.

Main proof

- **Simplifying assumption:** K symmetric.
- Apply a linear transformation so that $\ell_K \cdot \ell_{K^\circ} \leq O(n \log n)$

Main proof

- **Simplifying assumption:** K symmetric.
- 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

- **Simplifying assumption:** K symmetric.
- 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

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

- **Goal:**
  - Bound $\mu(\Lambda, K)$ in terms of r_i, d_i.
  - Bound r_i, d_i in terms of $\mu_{KL}(\Lambda, K)$.

Main proof (2)

We bound

$$\mu(\Lambda, K)$$

Main proof (2)

We bound

$$\mu(\Lambda, K) \overset{\text{triangle ineq.}}{\leq} \sum_{i=1}^{k} \mu\big(\Lambda_i/\Lambda_{i-1}, \Pi_{\mathrm{span}(\Lambda_{i-1})^\perp}(K \cap \mathrm{span}(\Lambda_i))\big)$$

Main proof (2)

We bound

$$\mu(\Lambda, K) \overset{\text{triangle ineq.}}{\leq} \sum_{i=1}^{k} \mu\Big(\underbrace{\Lambda_i/\Lambda_{i-1}}_{r_i\cdot\text{stable lattice}}, \Pi_{\mathrm{span}(\Lambda_{i-1})^\perp}(K \cap \mathrm{span}(\Lambda_i))\Big)$$

- Recall: $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ stable

Main proof (2)

We bound

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

$$\lesssim \sum_{i=1}^{k} \log(n) \cdot r_i \cdot \ell_K$$

- Recall: $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ stable
- Use monotonicity of ℓ-value: $\ell_{K\cap W} \leq \ell_K$ for subspace W (potentially huge loss!!)

Main proof (2)

We bound

$$\begin{aligned}
\mu(\Lambda, K) &\overset{\text{triangle ineq.}}{\leq} \sum_{i=1}^{k} \mu\Big(\underbrace{\Lambda_i/\Lambda_{i-1}}_{r_i\cdot\text{stable lattice}}, \Pi_{\text{span}(\Lambda_{i-1})^\perp}(K \cap \text{span}(\Lambda_i))\Big) \\
&\lesssim \sum_{i=1}^{k} \log(n) \cdot r_i \cdot \ell_K \\
&\lesssim \log(n) \cdot r_k \cdot \ell_K
\end{aligned}$$

- Recall: $\frac{1}{r_i}(\Lambda_i/\Lambda_{i-1})$ stable
- Use monotonicity of ℓ-value: $\ell_{K\cap W} \leq \ell_K$ for subspace W (potentially huge loss!!)
- Group indices of similar density together: $r_i \leq \frac{1}{2} r_{i+2}$

Main proof (2)

- Fix any index i.
- Set $W := \text{span}(\Lambda_{i-1})^{\perp}$, $d := \dim(W)$

Main proof (2)

- Fix any index i.
- Set $W := \text{span}(\Lambda_{i-1})^{\perp}$, $d := \dim(W)$

$$\sqrt{d_i} \cdot r_i \quad \leq \quad \sqrt{d} \cdot \det(\Pi_W(\Lambda))^{1/d}$$

- Use $r_1 < \ldots < r_k$ and $d_i \leq d$

Main proof (2)

- Fix any index i.
- Set $W := \text{span}(\Lambda_{i-1})^\perp$, $d := \dim(W)$

$$\begin{aligned}\sqrt{d_i} \cdot r_i &\leq \sqrt{d} \cdot \det(\Pi_W(\Lambda))^{1/d} \\ &\approx \Big(\frac{\text{Vol}_d(\Pi_W(K))}{\text{Vol}_d(B_2^d)}\Big)^{1/d} \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\text{Vol}_d(\Pi_W(K))}\Big)^{1/d}\end{aligned}$$

- Use $r_1 < \ldots < r_k$ and $d_i \leq d$
- Use $\text{Vol}_d(B_2^n) \approx d^{-d/2}$

Main proof (2)

- Fix any index i.
- Set $W := \text{span}(\Lambda_{i-1})^{\perp}$, $d := \dim(W)$

$$\begin{aligned}\sqrt{d_i} \cdot r_i &\leq \sqrt{d} \cdot \det(\Pi_W(\Lambda))^{1/d} \\ &\approx \Big(\frac{\text{Vol}_d(\Pi_W(K))}{\text{Vol}_d(B_2^d)}\Big)^{1/d} \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\text{Vol}_d(\Pi_W(K))}\Big)^{1/d} \\ &\leq w(\Pi_W(K)) \cdot \mu_{KL}(\Lambda, K)\end{aligned}$$

- Use $r_1 < \ldots < r_k$ and $d_i \leq d$
- Use $\text{Vol}_d(B_2^n) \approx d^{-d/2}$
- **Urysohn:** Euclidean ball minimize width (fixing volume) where $w(Q) = \mathbb{E}_{\theta \sim S^{d-1}}[\max\{\langle \theta, x - y \rangle : x, y \in Q\}]$

Main proof (2)

- Fix any index i.
- Set $W := \text{span}(\Lambda_{i-1})^{\perp}$, $d := \dim(W)$

$$\begin{aligned}
\sqrt{d_i} \cdot r_i &\leq \sqrt{d} \cdot \det(\Pi_W(\Lambda))^{1/d} \\
&\approx \Big(\frac{\text{Vol}_d(\Pi_W(K))}{\text{Vol}_d(B_2^d)}\Big)^{1/d} \cdot \Big(\frac{\det(\Pi_W(\Lambda))}{\text{Vol}_d(\Pi_W(K))}\Big)^{1/d} \\
&\leq w(\Pi_W(K)) \cdot \mu_{KL}(\Lambda, K) \\
&\lesssim \frac{\ell_{K^\circ}}{\sqrt{d}} \cdot \mu_{KL}(\Lambda, K)
\end{aligned}$$

- Use $r_1 < \ldots < r_k$ and $d_i \leq d$
- Use $\text{Vol}_d(B_2^n) \approx d^{-d/2}$
- **Urysohn:** Euclidean ball minimize width (fixing volume) where $w(Q) = \mathbb{E}_{\theta \sim S^{d-1}}[\max\{\langle \theta, x - y \rangle : x, y \in Q\}] \approx \frac{\ell_{Q^\circ}}{\sqrt{d}}$

Main proof (3)

- Putting everything together:

$$\mu(\Lambda, K) \quad \leq \quad \log(n) \cdot r_k \cdot \ell_K$$

Main proof (3)

- Putting everything together:

$$\begin{aligned} \mu(\Lambda, K) &\leq \log(n) \cdot r_k \cdot \ell_K \\ &\lesssim \log(n) \cdot \frac{1}{d_k} \cdot \ell_K \cdot \ell_{K^\circ} \cdot \mu_{KL}(\Lambda, K) \end{aligned}$$

Main proof (3)

- Putting everything together:

$$\begin{aligned}
\mu(\Lambda, K) &\leq \log(n) \cdot r_k \cdot \ell_K \\
&\lesssim \log(n) \cdot \frac{1}{d_k} \cdot \underbrace{\ell_K \cdot \ell_{K^\circ}}_{\lesssim n \log(n)} \cdot \mu_{KL}(\Lambda, K) \\
&\lesssim \log^2(n) \cdot \frac{n}{d_k} \cdot \mu_{KL}(\Lambda, k)
\end{aligned}$$

Main proof (3)

- Putting everything together:

$$\begin{aligned} \mu(\Lambda, K) &\leq \log(n) \cdot r_k \cdot \ell_K \\ &\lesssim \log(n) \cdot \frac{1}{d_k} \cdot \underbrace{\ell_K \cdot \ell_{K^\circ}}_{\lesssim n \log(n)} \cdot \mu_{KL}(\Lambda, K) \\ &\lesssim \log^2(n) \cdot \frac{n}{d_k} \cdot \mu_{KL}(\Lambda, k) \end{aligned}$$

- Works if $d_k \geq \Omega(n/\mathrm{polylog}(n))$, fails otherwise!

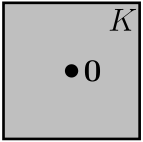
Main proof (3)

- Putting everything together:

$$
\begin{aligned}
\mu(\Lambda, K) &\leq \log(n) \cdot r_k \cdot \ell_K \\
&\lesssim \log(n) \cdot \frac{1}{d_k} \cdot \underbrace{\ell_K \cdot \ell_{K^\circ}}_{\lesssim n \log(n)} \cdot \mu_{KL}(\Lambda, K) \\
&\lesssim \log^2(n) \cdot \frac{n}{d_k} \cdot \mu_{KL}(\Lambda, k)
\end{aligned}
$$

- Works if $d_k \geq \Omega(n/\text{polylog}(n))$, fails otherwise!

Problem: If say $d_k = 1 = d$, then $\text{Vol}_d(\Pi_W(K))^{1/d}$ only determined up to $\sqrt{n}$ factor!



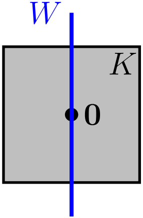
Main proof (3)

- Putting everything together:

$$\begin{aligned} \mu(\Lambda, K) &\leq \log(n) \cdot r_k \cdot \ell_K \\ &\lesssim \log(n) \cdot \frac{1}{d_k} \cdot \underbrace{\ell_K \cdot \ell_{K^\circ}}_{\lesssim n \log(n)} \cdot \mu_{KL}(\Lambda, K) \\ &\lesssim \log^2(n) \cdot \frac{n}{d_k} \cdot \mu_{KL}(\Lambda, k) \end{aligned}$$

- Works if $d_k \geq \Omega(n/\text{polylog}(n))$, fails otherwise!

Problem: If say $d_k = 1 = d$, then $\text{Vol}_d(\Pi_W(K))^{1/d}$ only determined up to $\sqrt{n}$ factor!



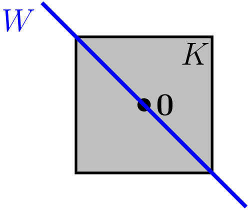
Main proof (3)

- Putting everything together:

$$\begin{aligned} \mu(\Lambda, K) &\leq \log(n) \cdot r_k \cdot \ell_K \\ &\lesssim \log(n) \cdot \frac{1}{d_k} \cdot \underbrace{\ell_K \cdot \ell_{K^\circ}}_{\lesssim n \log(n)} \cdot \mu_{KL}(\Lambda, K) \\ &\lesssim \log^2(n) \cdot \frac{n}{d_k} \cdot \mu_{KL}(\Lambda, k) \end{aligned}$$

- Works if $d_k \geq \Omega(n/\text{polylog}(n))$, fails otherwise!

Problem: If say $d_k = 1 = d$, then $\text{Vol}_d(\Pi_W(K))^{1/d}$ only determined up to $\sqrt{n}$ factor!



Main proof (4)

The fix:

Main proof (4)

The fix:

- Pick smallest index i with $\text{rank}(\Lambda_{i^*}) \geq n/2$.
  Set $U := \text{span}(\Lambda_{i^*})$

Main proof (4)

The fix:

- Pick smallest index i with $\mathrm{rank}(\Lambda_{i^*}) \geq n/2$.
  Set $U := \mathrm{span}(\Lambda_{i^*})$
- Prove $\mu(\Lambda \cap U, K \cap U) \leq \mathrm{polylog}(n) \cdot \mu_{KL}(\Lambda, K)$

Main proof (4)

The fix:

- Pick smallest index i with $\mathrm{rank}(\Lambda_{i^*}) \geq n/2$.
  Set $U := \mathrm{span}(\Lambda_{i^*})$
- Prove $\mu(\Lambda \cap U, K \cap U) \leq \mathrm{polylog}(n) \cdot \mu_{KL}(\Lambda, K)$
- Then apply **induction**!

Main proof (4)

The fix:

- Pick smallest index i with $\mathrm{rank}(\Lambda_{i^*}) \geq n/2$.
  Set $U := \mathrm{span}(\Lambda_{i^*})$
- Prove $\mu(\Lambda \cap U, K \cap U) \leq \mathrm{polylog}(n) \cdot \mu_{KL}(\Lambda, K)$
- Then apply **induction**!

Details:

- Upper bound with some index i:

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

Main proof (4)

The fix:

- Pick smallest index i with $\text{rank}(\Lambda_{i^*}) \geq n/2$.
  Set $U := \text{span}(\Lambda_{i^*})$
- Prove $\mu(\Lambda \cap U, K \cap U) \leq \text{polylog}(n) \cdot \mu_{KL}(\Lambda, K)$
- Then apply **induction**!

Details:

- Upper bound with some index i:

$$\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K \leq \log^2(n) \cdot \frac{r_{i^*}}{r_i} \cdot \frac{n}{d_i} \cdot \mu_{KL}(\Lambda, K)$$

Main proof (4)

The fix:

- Pick smallest index i with $\text{rank}(\Lambda_{i^*}) \geq n/2$.
  Set $U := \text{span}(\Lambda_{i^*})$
- Prove $\mu(\Lambda \cap U, K \cap U) \leq \text{polylog}(n) \cdot \mu_{KL}(\Lambda, K)$
- Then apply **induction**!

Details:

- Upper bound with some index i:

$$\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K \leq \log^2(n) \cdot \frac{r_{i^*}}{r_i} \cdot \frac{n}{d_i} \cdot \mu_{KL}(\Lambda, K)$$

- Need an index i with $\frac{r_{i^*}}{r_i} \cdot \frac{n}{d_i} \leq \text{polylog}(n)$!

Main proof (4)

The fix:

- Pick smallest index i with $\text{rank}(\Lambda_{i^*}) \geq n/2$.
  Set $U := \text{span}(\Lambda_{i^*})$
- Prove $\mu(\Lambda \cap U, K \cap U) \leq \text{polylog}(n) \cdot \mu_{KL}(\Lambda, K)$
- Then apply **induction**!

Details:

- Upper bound with some index i:

$$\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K \leq \log^2(n) \cdot \frac{r_{i^*}}{r_i} \cdot \frac{n}{d_i} \cdot \mu_{KL}(\Lambda, K)$$

- Need an index i with $\frac{r_{i^*}}{r_i} \cdot \frac{n}{d_i} \leq \text{polylog}(n)$!
- **Case 1.** For some $i \geq i^*$, $d_i \geq \Omega(\frac{n}{\log(n)})$. **Done!**

Main proof (4)

The fix:

- Pick smallest index i with $\text{rank}(\Lambda_{i^*}) \geq n/2$.
  Set $U := \text{span}(\Lambda_{i^*})$
- Prove $\mu(\Lambda \cap U, K \cap U) \leq \text{polylog}(n) \cdot \mu_{KL}(\Lambda, K)$
- Then apply **induction**!

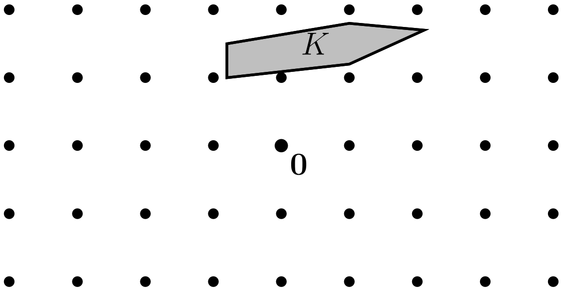
Details:

- Upper bound with some index i:

$$\mu(\Lambda \cap U, K \cap U) \lesssim \log(n) \cdot r_{i^*} \cdot \ell_K \leq \log^2(n) \cdot \frac{r_{i^*}}{r_i} \cdot \frac{n}{d_i} \cdot \mu_{KL}(\Lambda, K)$$

- Need an index i with $\frac{r_{i^*}}{r_i} \cdot \frac{n}{d_i} \leq \text{polylog}(n)$!
- **Case 1.** For some $i \geq i^*$, $d_i \geq \Omega(\frac{n}{\log(n)})$. **Done!**
- **Case 2.** All $i \geq i^*$ have $d_i \leq o(\frac{n}{\log(n)})$. Then
  $k - i^* \geq \omega(\log(n))$ and $r_k \geq n^{100} r_{i^*}$. **Done!** □

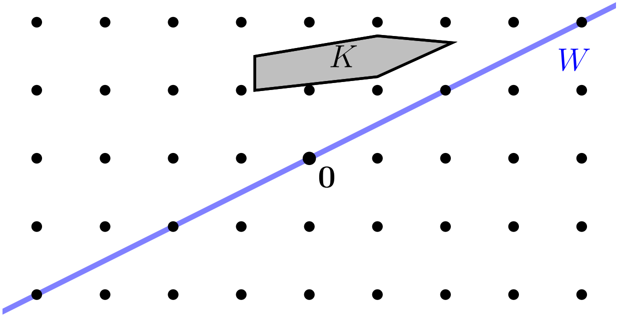
Dadush's algorithm



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 $K \cap \Lambda$

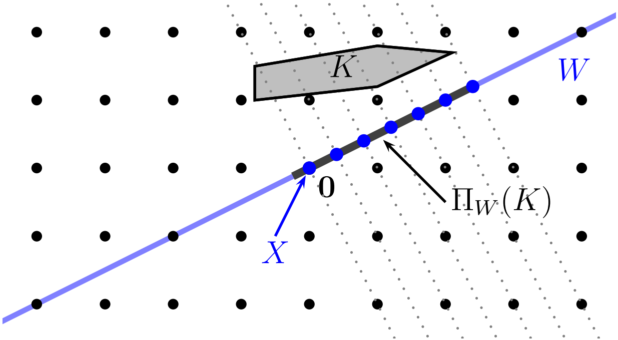
(1) Shrink K so that $\mu(\Lambda, K) \geq 1$

(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 $K \cap \Lambda$

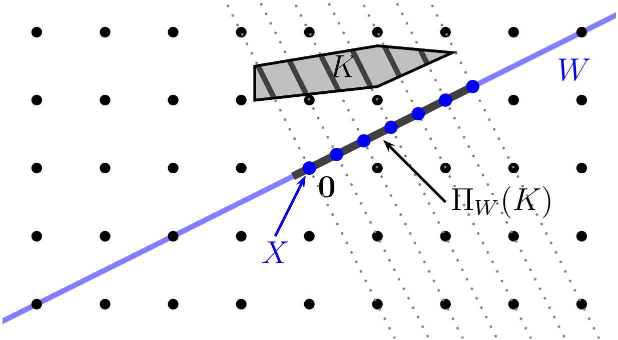
(1) Shrink K so that $\mu(\Lambda, K) \geq 1$

(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)

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 $\mu_{KL}(\Lambda, K)$ apx.
(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)

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 $\mu_{KL}(\Lambda, K)$ apx. $\rightarrow$ time $2^{O(n)}$

(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)

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 $\mu_{KL}(\Lambda, K)$ apx. $\rightarrow$ time $2^{O(n)}$
(3) Compute $X := \Pi_W(K) \cap \Pi_W(\Lambda)$ $\rightarrow$ time $O(\log^8 n)^d$
(4) Recurse on fibers $K \cap \Pi_W^{-1}(x)$ for all $x \in X$

- Let $d := \dim(W)$

Theorem (Dadush)

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

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

Can compute points in same time.

Dadush's algorithm (analysis)

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 $\mu_{KL}(\Lambda, K)$ apx. $\rightarrow$ time $2^{O(n)}$
(3) Compute $X := \Pi_W(K) \cap \Pi_W(\Lambda)$ $\rightarrow$ time $O(\log^8 n)^d$
(4) Recurse on fibers $K \cap \Pi_W^{-1}(x)$ for all $x \in X$

- Let $d := \dim(W)$

Theorem (Dadush)

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

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

Can compute points in same time.

- Recursion

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

Dadush's algorithm (analysis)

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 $\mu_{KL}(\Lambda, K)$ apx. $\rightarrow$ time $2^{O(n)}$
(3) Compute $X := \Pi_W(K) \cap \Pi_W(\Lambda)$ $\rightarrow$ time $O(\log^8 n)^d$
(4) Recurse on fibers $K \cap \Pi_W^{-1}(x)$ for all $x \in X$

- Let $d := \dim(W)$

Theorem (Dadush)

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

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

Can compute points in same time.

- Recursion

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

Open problem

Open problem

Can one solve every n variable IP in time $2^{O(n)}$?

- Right now, no candidate pathway known!

Open problem

Open problem

Can one solve every n variable IP in time $2^{O(n)}$?

- Right now, no candidate pathway known!

Thanks for your attention!

Generalization to non-symmetric K

- Translate K so that **Santaló point** is at $\mathbf{0}$ (i.e. barycenter of K° is at $\mathbf{0}$.
- Run proof with $K_{\mathrm{sym}} := K \cap (-K)$ (inner symmetrizer)
- We need:

$$\mathrm{Vol}_d(\Pi_W(K))^{1/d} \lesssim \left(\frac{n}{d}\right)^3 \cdot \mathrm{Vol}_d(\Pi_W(K_{\mathrm{sym}}))^{1/d}$$

More involved! This is a polar version of Rudelson's result on sections of the difference body:

$$\mathrm{Vol}_d((K-K)\cap W)^{1/d} \lesssim \frac{n}{d} \cdot \max_{x\in\mathbb{R}^n} \left\{ \mathrm{Vol}_d(K \cap (x+W))^{1/d} \right\}$$