

The Subspace Flatness Conjecture and Faster Integer Programming

Victor Reis (Microsoft Research)

Joint work with Thomas Rothvoss (University of Washington)

MIP 2025
June 4th

Linear Programming

- ▶ Solution $x \in \mathbb{R}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

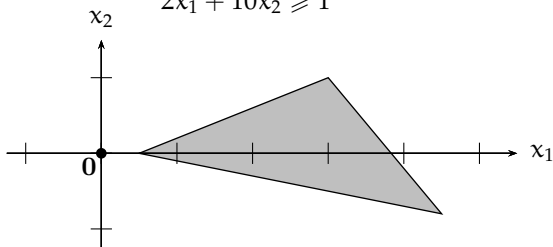
Linear Programming

- Solution $x \in \mathbb{R}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$



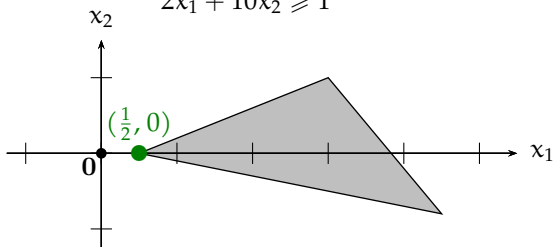
Linear Programming

- Solution $x \in \mathbb{R}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$



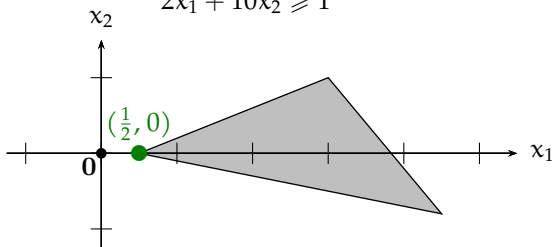
Linear Programming

- Solution $x \in \mathbb{R}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$



- Not always possible: $1 \leq x_1 \leq -1$

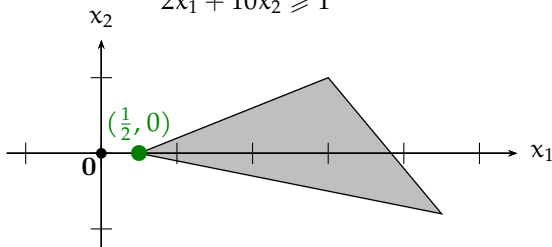
Linear Programming

- ▶ Solution $x \in \mathbb{R}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$



- ▶ Not always possible: $1 \leq x_1 \leq -1$
- ▶ Resource allocation (energy, water, capital)

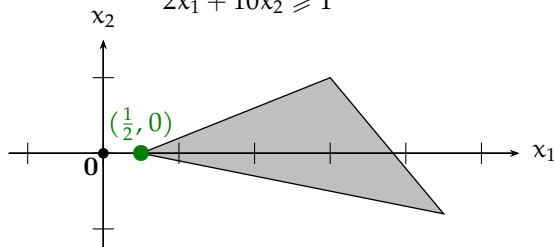
Linear Programming

- Solution $x \in \mathbb{R}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$



- Not always possible: $1 \leq x_1 \leq -1$
- Resource allocation (energy, water, capital)
- First algorithm [Fourier, 1824]; simplex method [Dantzig '47]

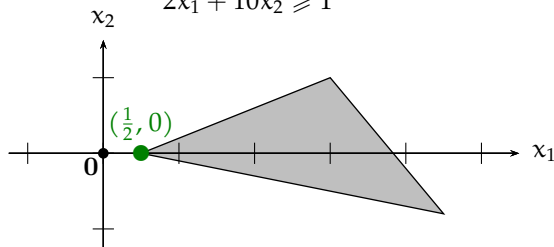
Linear Programming

- Solution $x \in \mathbb{R}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$



- Not always possible: $1 \leq x_1 \leq -1$
- Resource allocation (energy, water, capital)
- First algorithm [Fourier, 1824]; simplex method [Dantzig '47]
- Polynomial time: ellipsoid method $O(n^6)$ [Khachiyan '79]

Integer Linear Programming

- Solution $x \in \mathbb{Z}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

Integer Linear Programming

- ▶ Solution $x \in \mathbb{Z}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

- ▶ Indivisible resource allocation (scheduling, routing, labor)

Integer Linear Programming

- ▶ Solution $x \in \mathbb{Z}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

- ▶ Indivisible resource allocation (scheduling, routing, labor)
- ▶ First algorithm [Gomory '58]; branch and bound [Land, Doig '60]

Integer Linear Programming

- ▶ Solution $x \in \mathbb{Z}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

- ▶ Indivisible resource allocation (scheduling, routing, labor)
- ▶ First algorithm [Gomory '58]; branch and bound [Land, Doig '60]
- ▶ NP-hard! [Karp '72]

Integer Linear Programming

- ▶ Solution $x \in \mathbb{Z}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

- ▶ Indivisible resource allocation (scheduling, routing, labor)
- ▶ First algorithm [Gomory '58]; branch and bound [Land, Doig '60]
- ▶ NP-hard! [Karp '72]
- ▶ $2^{O(n^3)}$ [Lenstra '83]

Integer Linear Programming

- ▶ Solution $x \in \mathbb{Z}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

- ▶ Indivisible resource allocation (scheduling, routing, labor)
- ▶ First algorithm [Gomory '58]; branch and bound [Land, Doig '60]
- ▶ NP-hard! [Karp '72]
- ▶ $2^{O(n^3)}$ [Lenstra '83]
- ▶ $O(n)^{\frac{5}{2}n}$ [Kannan '83, '87], $O(n)^{2n}$ [HK '10], $\tilde{O}(n)^{\frac{4}{3}n}$ [DPV '11]

Integer Linear Programming

- ▶ Solution $x \in \mathbb{Z}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

- ▶ Indivisible resource allocation (scheduling, routing, labor)
- ▶ First algorithm [Gomory '58]; branch and bound [Land, Doig '60]
- ▶ NP-hard! [Karp '72]
- ▶ $2^{O(n^3)}$ [Lenstra '83]
- ▶ $O(n)^{\frac{5}{2}n}$ [Kannan '83, '87], $O(n)^{2n}$ [HK '10], $\tilde{O}(n)^{\frac{4}{3}n}$ [DPV '11]
- ▶ $O(n)^n$ [Dadush '12, Dadush, Eisenbrand, Rothvoss '22]

Integer Linear Programming

- ▶ Solution $x \in \mathbb{Z}^n$ to a system of linear inequalities in n variables:

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

- ▶ Indivisible resource allocation (scheduling, routing, labor)
- ▶ First algorithm [Gomory '58]; branch and bound [Land, Doig '60]
- ▶ NP-hard! [Karp '72]
- ▶ $2^{O(n^3)}$ [Lenstra '83]
- ▶ $O(n)^{\frac{5}{2}n}$ [Kannan '83, '87], $O(n)^{2n}$ [HK '10], $\tilde{O}(n)^{\frac{4}{3}n}$ [DPV '11]
- ▶ $O(n)^n$ [Dadush '12, Dadush, Eisenbrand, Rothvoss '22]
- ▶ $O(\log n)^{4n}$ [R., Rothvoss '23]

Integer Programming

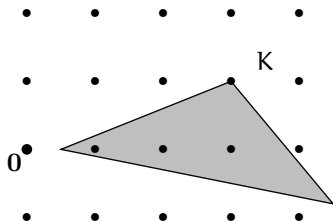
Problem

Given a convex body $K \subset \mathbb{R}^n$, find a point in $K \cap \mathbb{Z}^n$ or certify $K \cap \mathbb{Z}^n = \emptyset$.

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$



Integer Programming

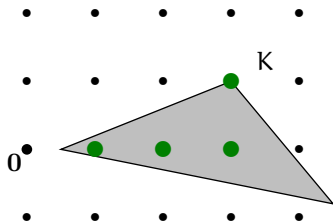
Problem

Given a convex body $K \subset \mathbb{R}^n$, find a point in $K \cap \mathbb{Z}^n$ or certify $K \cap \mathbb{Z}^n = \emptyset$.

$$6x_1 + 5x_2 \leq 23$$

$$2x_1 - 5x_2 \geq 1$$

$$2x_1 + 10x_2 \geq 1$$

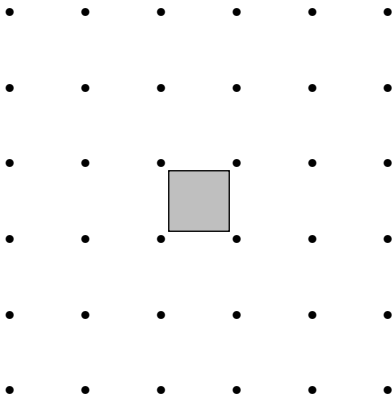


The fundamental question

What does a convex set containing no integer points *look like*?

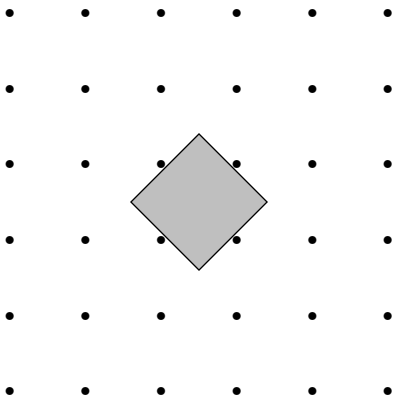
The fundamental question

What does a convex set containing no integer points *look like*?



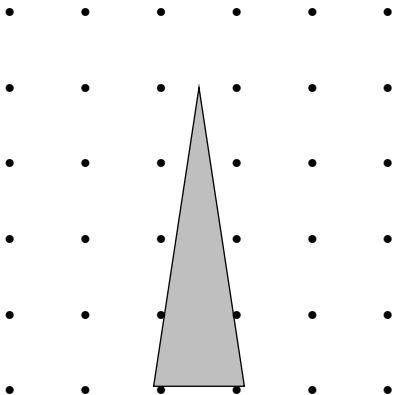
The fundamental question

What does a convex set containing no integer points *look like*?



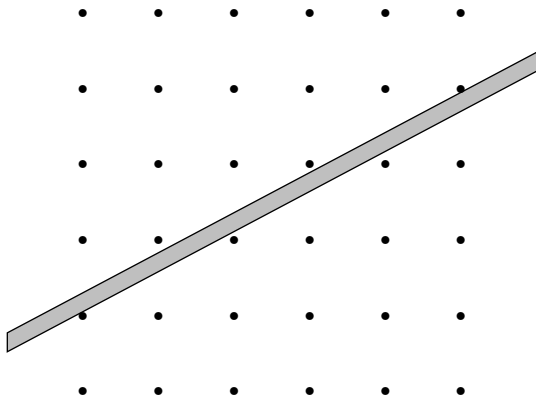
The fundamental question

What does a convex set containing no integer points *look like*?



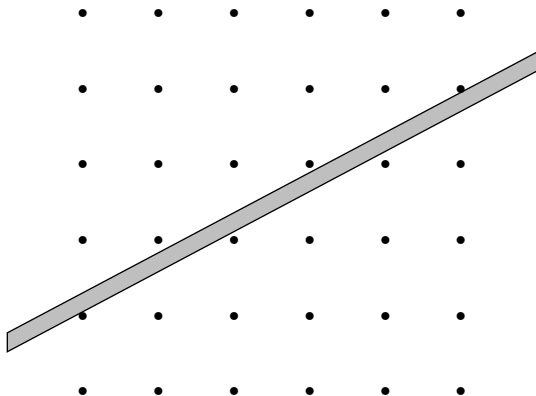
The fundamental question

What does a convex set containing no integer points *look like*?



The fundamental question

What does a convex set containing no integer points *look like*?



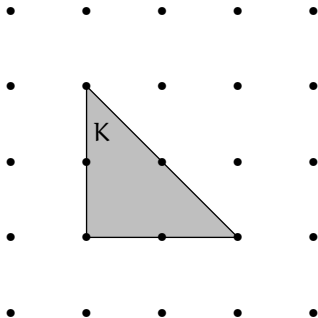
It has to be *flat*!

Lenstra's algorithm

Khintchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.

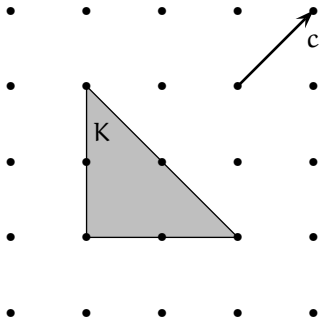


Lenstra's algorithm

Khintchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.

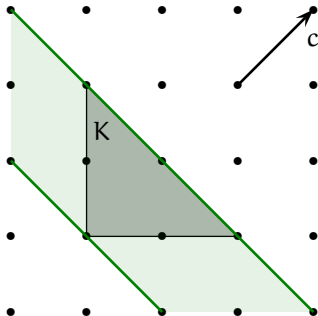


Lenstra's algorithm

Khintchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.

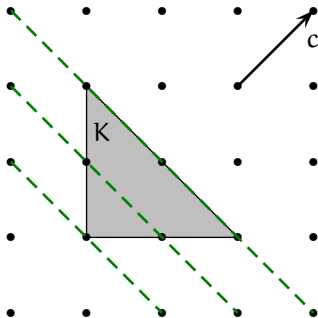


Lenstra's algorithm

Khintchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.

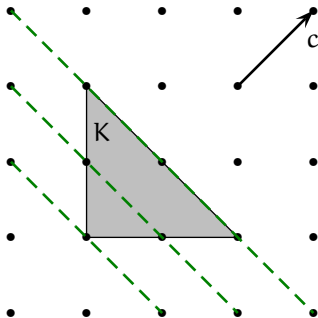


Lenstra's algorithm

Khinchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.



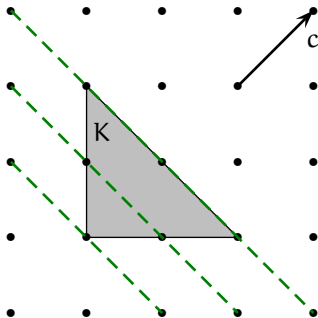
- In polynomial time: $\text{Flat}(n) \leq 2^{O(n^2)}$ [LLL '82, Lenstra '83]

Lenstra's algorithm

Khinchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.



- ▶ In polynomial time: $\text{Flat}(n) \leq 2^{O(n^2)}$ [LLL '82, Lenstra '83]
- ▶ Lenstra's algorithm: $T(n) \leq T(n-1) \cdot 2^{O(n^2)} \implies T(n) \leq 2^{O(n^3)}$.

Lenstra-type algorithm

Khintchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.

Theorem [Dadush, Peikert, Vempala 2011]

We can find a direction minimizing $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x$ in time $2^{O(n)}$, and solve IP in time $O(\text{Flat}(n))^n$.

Lenstra-type algorithm

Khintchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.

Theorem [Dadush, Peikert, Vempala 2011]

We can find a direction minimizing $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x$ in time $2^{O(n)}$, and solve IP in time $O(\text{Flat}(n))^n$.

- Best bound for $\text{Flat}(n)$ at the time: $O(n^{\frac{4}{3}} \cdot (\log n)^{O(1)})$ [BLPS '99]

Lenstra-type algorithm

Khintchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.

Theorem [Dadush, Peikert, Vempala 2011]

We can find a direction minimizing $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x$ in time $2^{O(n)}$, and solve IP in time $O(\text{Flat}(n))^n$.

- ▶ Best bound for $\text{Flat}(n)$ at the time: $O(n^{\frac{4}{3}} \cdot (\log n)^{O(1)})$ [BLPS '99]
- ▶ Barrier: $\text{Flat}(n) \geq n$

Lenstra-type algorithm

Khintchine's flatness theorem (1947)

Given a convex $K \subset \mathbb{R}^n$, there exists either

- an integer point in K or
- a direction $c \in \mathbb{Z}^n \setminus \{0\}$ so that $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x \leq \text{Flat}(n)$.

Theorem [Dadush, Peikert, Vempala 2011]

We can find a direction minimizing $\max_{x \in K} c^\top x - \min_{x \in K} c^\top x$ in time $2^{O(n)}$, and solve IP in time $O(\text{Flat}(n))^n$.

- ▶ Best bound for $\text{Flat}(n)$ at the time: $O(n^{\frac{4}{3}} \cdot (\log n)^{O(1)})$ [BLPS '99]
- ▶ Barrier: $\text{Flat}(n) \geq n$
- ▶ $\text{Flat}(n) \leq O(n \cdot (\log n)^3)$ [R., Rothvoss '23]

Daniel's vision

Can we move past hyperplane flatness with *subspaces*?

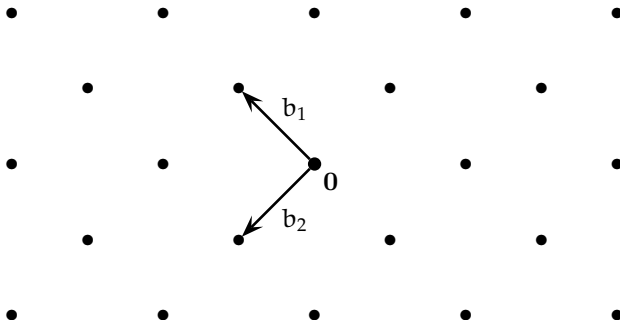
Daniel's vision

Can we move past hyperplane flatness with *subspaces*?

- ▶ While $\text{Flat}(\mathbf{n}) \geq \mathbf{n}$, for *subspace flatness* $\geq \log \mathbf{n}$ [Kannan-Lovász '88]

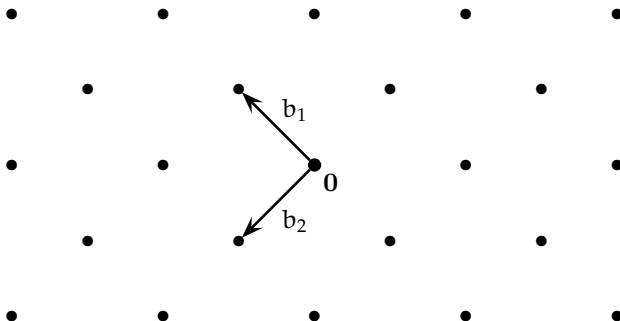
Lattices

- ▶ A lattice $\mathcal{L} := \mathbb{B}\mathbb{Z}^n$ (integer linear combinations of a basis)



Lattices

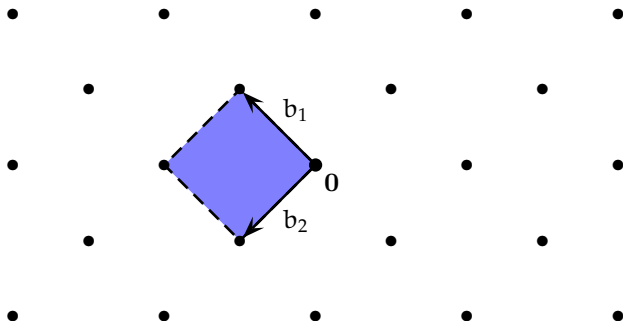
- ▶ A lattice $\mathcal{L} := B\mathbb{Z}^n$ (integer linear combinations of a basis)



- ▶ Number theory [Lagrange 1770], sphere packing [Viazovska '16], post-quantum cryptography [Regev '05], factoring [Regev '23]

Lattices

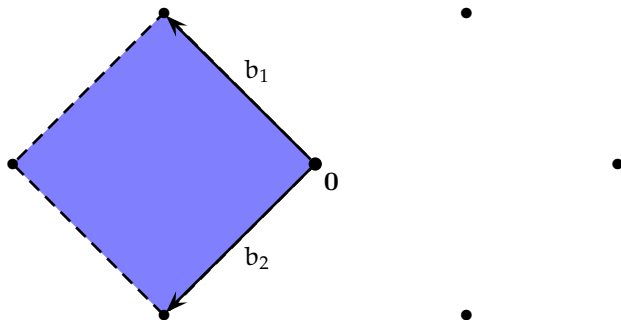
- ▶ A lattice $\mathcal{L} := B\mathbb{Z}^n$ (integer linear combinations of a basis)



- ▶ Number theory [Lagrange 1770], sphere packing [Viazovska '16], post-quantum cryptography [Regev '05], factoring [Regev '23]
- ▶ $\det(\mathcal{L}) := \text{vol}(B[0, 1]^n)$ 'sparsity' of \mathcal{L}

Lattices

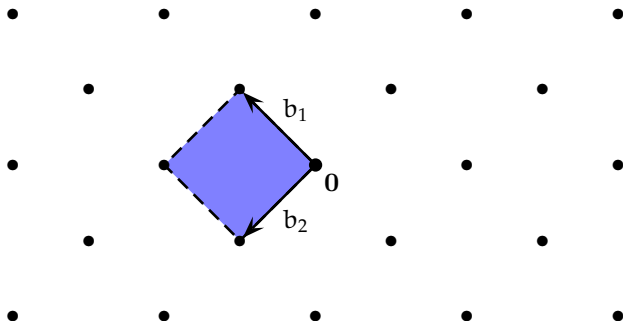
- ▶ A lattice $\mathcal{L} := B\mathbb{Z}^n$ (integer linear combinations of a basis)



- ▶ Number theory [Lagrange 1770], sphere packing [Viazovska '16], post-quantum cryptography [Regev '05], factoring [Regev '23]
- ▶ $\det(\mathcal{L}) := \text{vol}(B[0, 1]^n)$ 'sparsity' of \mathcal{L}

Lattices

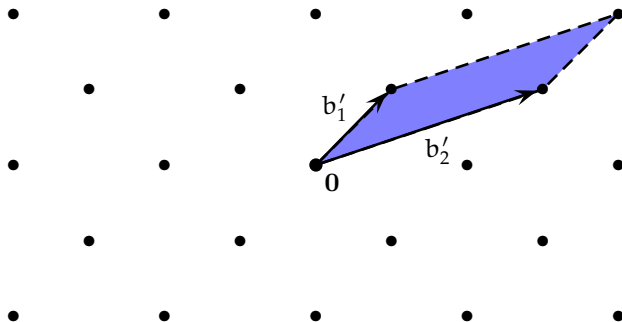
- ▶ A lattice $\mathcal{L} := B\mathbb{Z}^n$ (integer linear combinations of a basis)



- ▶ Number theory [Lagrange 1770], sphere packing [Viazovska '16], post-quantum cryptography [Regev '05], factoring [Regev '23]
- ▶ $\det(\mathcal{L}) := \text{vol}(B[0, 1]^n)$ 'sparsity' of \mathcal{L}

Lattices

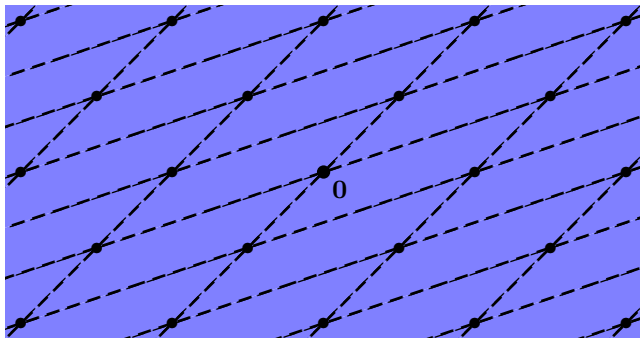
- ▶ A lattice $\mathcal{L} := B\mathbb{Z}^n$ (integer linear combinations of a basis)



- ▶ Number theory [Lagrange 1770], sphere packing [Viazovska '16], post-quantum cryptography [Regev '05], factoring [Regev '23]
- ▶ $\det(\mathcal{L}) := \text{vol}(B[0, 1]^n)$ 'sparsity' of \mathcal{L}

Lattices

- ▶ A lattice $\mathcal{L} := B\mathbb{Z}^n$ (integer linear combinations of a basis)

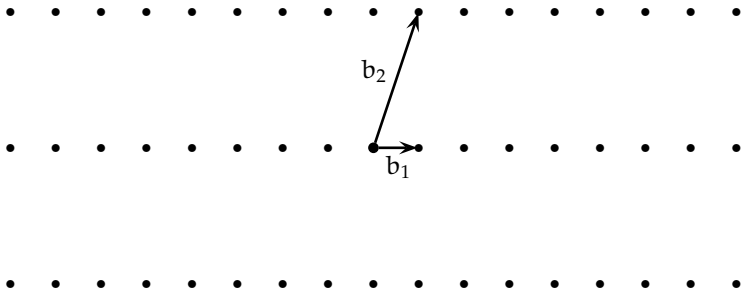


- ▶ Number theory [Lagrange 1770], sphere packing [Viazovska '16], post-quantum cryptography [Regev '05], factoring [Regev '23]
- ▶ $\det(\mathcal{L}) := \text{vol}(B[0,1]^n)$ 'sparsity' of \mathcal{L}
- ▶ $B[0,1]^n$ tiles \mathbb{R}^n for any basis B

Covering radius

- For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

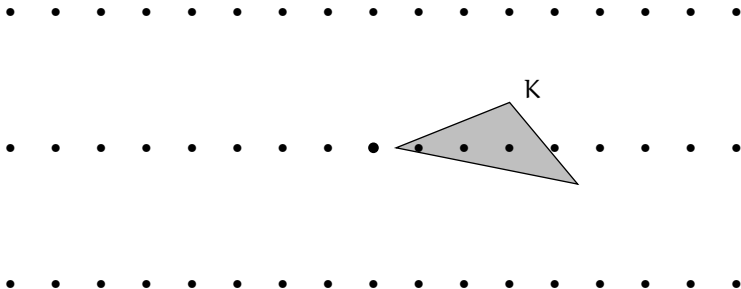
$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$



Covering radius

- For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

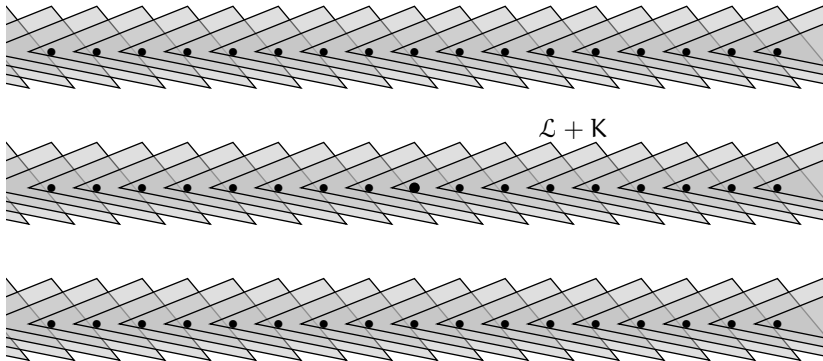
$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$



Covering radius

- For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

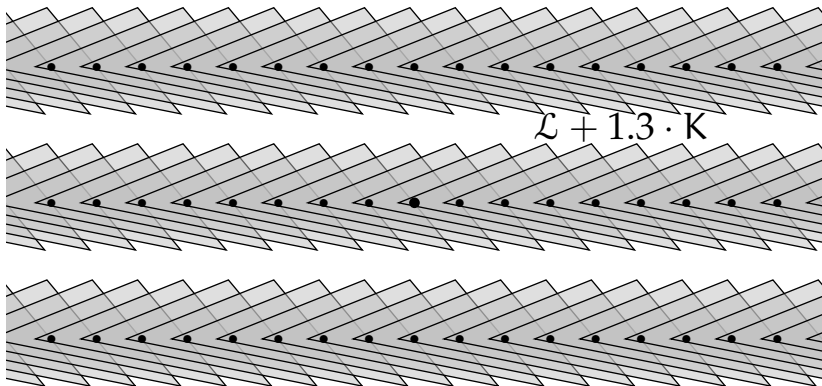
$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$



Covering radius

- For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

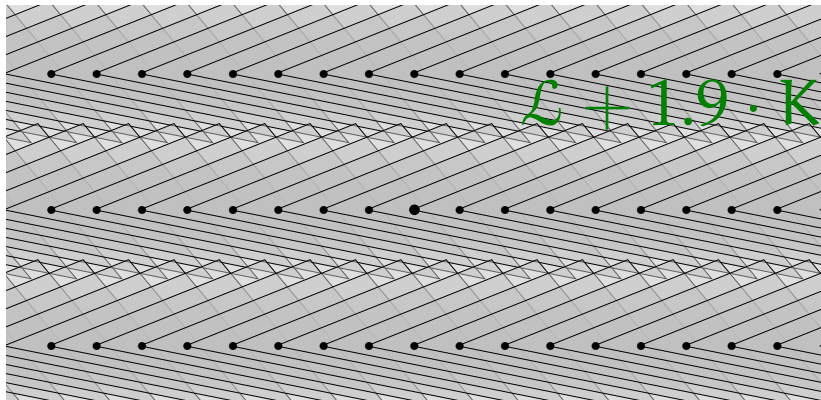
$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$



Covering radius

- ▶ For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$

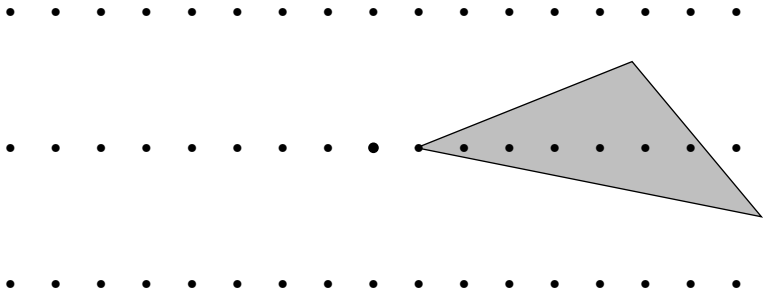


- ▶ In this example indeed $\mu(\mathcal{L}, K) = 1.9$.

Covering radius

- For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

$$\begin{aligned}\mu(\mathcal{L}, K) &:= \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\} \\ &= \min\{r > 0 : \text{every translate of } r \cdot K \text{ intersects } \mathcal{L}\}\end{aligned}$$

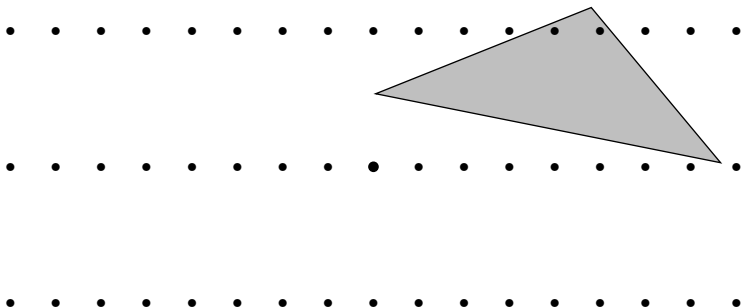


- In this example indeed $\mu(\mathcal{L}, K) = 1.9$.

Covering radius

- For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

$$\begin{aligned}\mu(\mathcal{L}, K) &:= \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\} \\ &= \min\{r > 0 : \text{every translate of } r \cdot K \text{ intersects } \mathcal{L}\}\end{aligned}$$

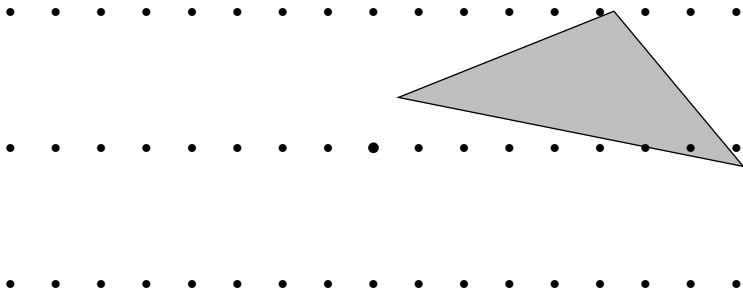


- In this example indeed $\mu(\mathcal{L}, K) = 1.9$.

Covering radius

- For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

$$\begin{aligned}\mu(\mathcal{L}, K) &:= \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\} \\ &= \min\{r > 0 : \text{every translate of } r \cdot K \text{ intersects } \mathcal{L}\}\end{aligned}$$

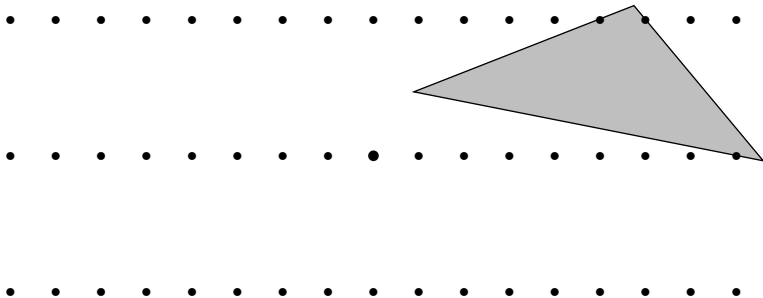


- In this example indeed $\mu(\mathcal{L}, K) = 1.9$.

Covering radius

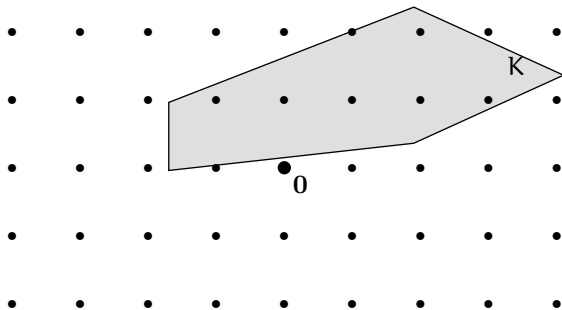
- For convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} := B\mathbb{Z}^n$, the **covering radius** is

$$\begin{aligned}\mu(\mathcal{L}, K) &:= \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\} \\ &= \min\{r > 0 : \text{every translate of } r \cdot K \text{ intersects } \mathcal{L}\}\end{aligned}$$

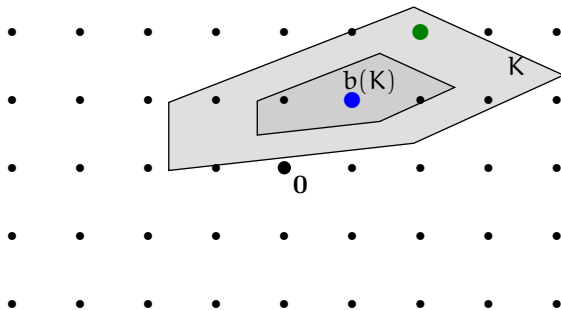


- In this example indeed $\mu(\mathcal{L}, K) = 1.9$.

Integer Programming for $\mu(\mathbb{Z}^n, K) \leq \frac{1}{2}$



Integer Programming for $\mu(\mathbb{Z}^n, K) \leq \frac{1}{2}$

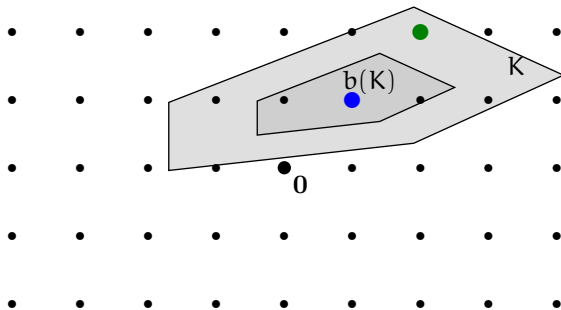


Theorem [Dadush '12]

There exists a $2^{O(n)}$ time algorithm which either:

- finds a point in $K \cap \mathbb{Z}^n$ or
- decides $\frac{1}{2}(K + b(K)) \cap \mathbb{Z}^n = \emptyset$.

Integer Programming for $\mu(\mathbb{Z}^n, K) \leq \frac{1}{2}$



Theorem [Dadush '12]

There exists a $2^{O(n)}$ time algorithm which either:

- finds a point in $K \cap \mathbb{Z}^n$ or
- decides $\frac{1}{2}(K + b(K)) \cap \mathbb{Z}^n = \emptyset$. \Leftarrow never happens when $\mu(\mathbb{Z}^n, K) \leq \frac{1}{2}$!

Lower bounds on the covering radius

- ▶ For convex $K \subset \mathbb{R}^n$ and lattice \mathcal{L} , the **covering radius** is

$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$

- ▶ How can we estimate the covering radius?

Lower bounds on the covering radius

- ▶ For convex $K \subset \mathbb{R}^n$ and lattice \mathcal{L} , the **covering radius** is

$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$

- ▶ How can we estimate the covering radius?

Lemma

If $\mathcal{L} + K = \mathbb{R}^n$ then $\text{vol}(K) \geq \det(\mathcal{L})$.

Lower bounds on the covering radius

- ▶ For convex $K \subset \mathbb{R}^n$ and lattice \mathcal{L} , the **covering radius** is

$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$

- ▶ How can we estimate the covering radius?

Lemma

If $\mathcal{L} + K = \mathbb{R}^n$ then $\text{vol}(K) \geq \det(\mathcal{L})$.

- ▶ Intuition: any covering needs as much volume as a tiling

Lower bounds on the covering radius

- ▶ For convex $K \subset \mathbb{R}^n$ and lattice \mathcal{L} , the **covering radius** is

$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$

- ▶ How can we estimate the covering radius?

Lemma

If $\mathcal{L} + K = \mathbb{R}^n$ then $\text{vol}(K) \geq \det(\mathcal{L})$.

- ▶ Intuition: any covering needs as much volume as a tiling
- ▶ As a corollary, we have for any K, \mathcal{L} :

$$\text{vol}(\mu(\mathcal{L}, K) \cdot K) \geq \det(\mathcal{L}) \implies \mu(\mathcal{L}, K)^n \geq \frac{\det(\mathcal{L})}{\text{vol}(K)}$$

Lower bounds on the covering radius

- ▶ For convex $K \subset \mathbb{R}^n$ and lattice \mathcal{L} , the **covering radius** is

$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$

- ▶ How can we estimate the covering radius?

Lemma

If $\mathcal{L} + K = \mathbb{R}^n$ then $\text{vol}(K) \geq \det(\mathcal{L})$.

- ▶ Intuition: any covering needs as much volume as a tiling
- ▶ As a corollary, we have for any K, \mathcal{L} :

$$\text{vol}(\mu(\mathcal{L}, K) \cdot K) \geq \det(\mathcal{L}) \implies \mu(\mathcal{L}, K) \geq \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n}$$

Lower bounds on the covering radius

- ▶ For convex $K \subset \mathbb{R}^n$ and lattice \mathcal{L} , the **covering radius** is

$$\mu(\mathcal{L}, K) := \min\{r > 0 : \mathcal{L} + r \cdot K = \mathbb{R}^n\}$$

- ▶ How can we estimate the covering radius?

Lemma

If $\mathcal{L} + K = \mathbb{R}^n$ then $\text{vol}(K) \geq \det(\mathcal{L})$.

- ▶ Intuition: any covering needs as much volume as a tiling
- ▶ As a corollary, we have for any K, \mathcal{L} :

$$\text{vol}(\mu(\mathcal{L}, K) \cdot K) \geq \det(\mathcal{L}) \implies \mu(\mathcal{L}, K) \geq \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n} = \text{nd}(\mathcal{L}, K).$$

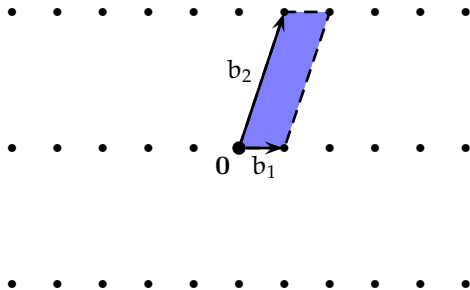
Lower bounds on the covering radius

• • • • • • • • • •

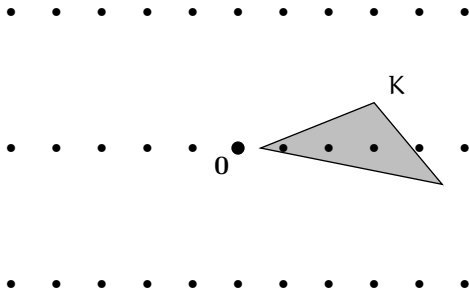
• • • • • 0 • • • • •

• • • • • • • • • •

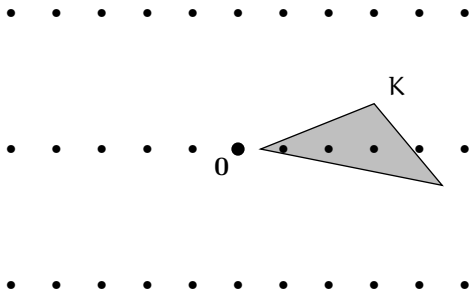
Lower bounds on the covering radius



Lower bounds on the covering radius

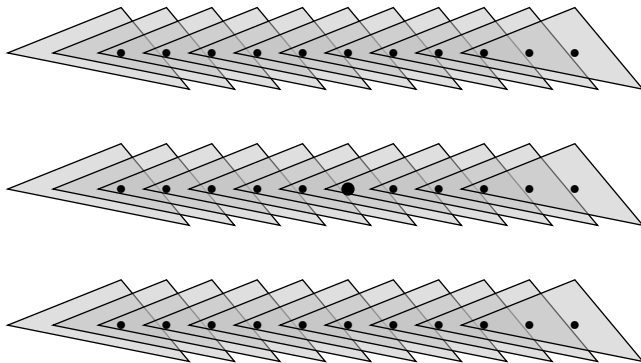


Lower bounds on the covering radius



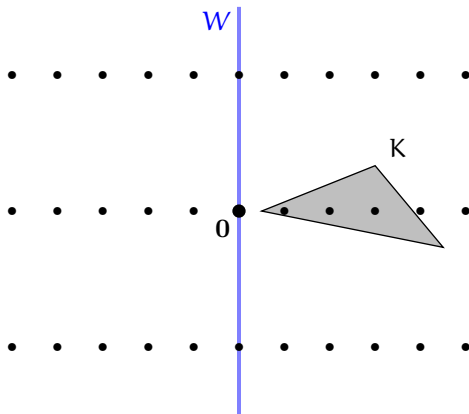
- Simple lower bound: $\mu(\mathcal{L}, K) \geq \text{nd}(\mathcal{L}, K) = \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n}$

Lower bounds on the covering radius



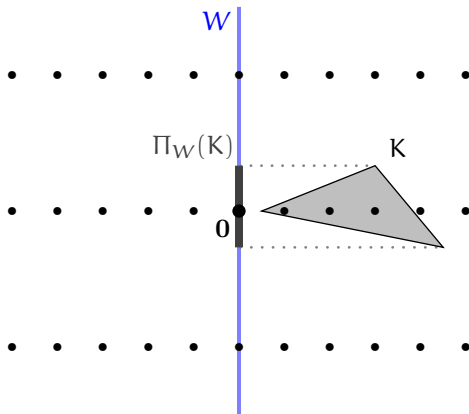
- Simple lower bound: $\mu(\mathcal{L}, K) \geq \text{nd}(\mathcal{L}, K) = \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n} = 1 \quad \text{☹}$

Lower bounds on the covering radius



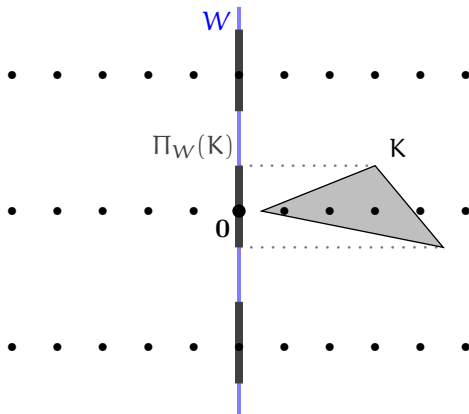
- Simple lower bound: $\mu(\mathcal{L}, K) \geq \text{nd}(\mathcal{L}, K) = \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n} = 1 \quad \text{☹}$

Lower bounds on the covering radius



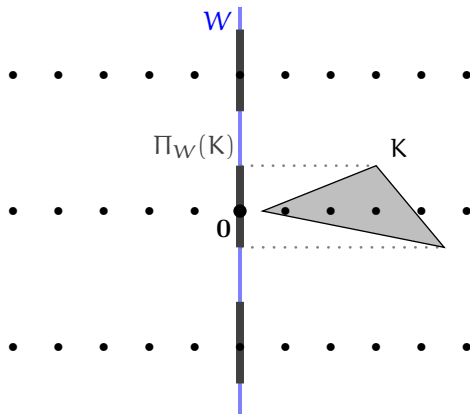
- Simple lower bound: $\mu(\mathcal{L}, K) \geq \text{nd}(\mathcal{L}, K) = \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n} = 1 \quad \text{☹}$

Lower bounds on the covering radius



- Simple lower bound: $\mu(\mathcal{L}, K) \geq \text{nd}(\mathcal{L}, K) = \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n} = 1 \quad \text{☹}$

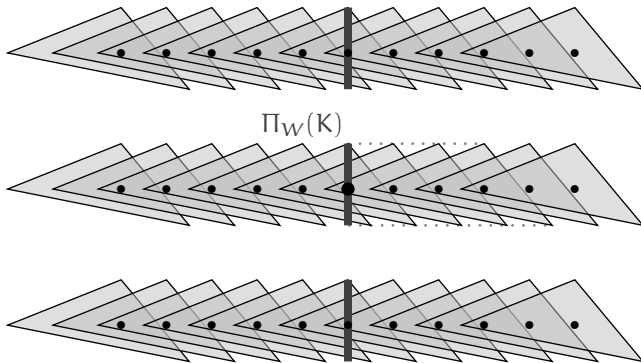
Lower bounds on the covering radius



- ▶ Simple lower bound: $\mu(\mathcal{L}, K) \geq \text{nd}(\mathcal{L}, K) = \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n} = 1 \quad \text{☹}$
- ▶ For any subspace W :

$$\mu(\mathcal{L}, K) \geq \mu(\Pi_W(\mathcal{L}), \Pi_W(K)) \geq \text{nd}(\Pi_W(\mathcal{L}), \Pi_W(K))$$

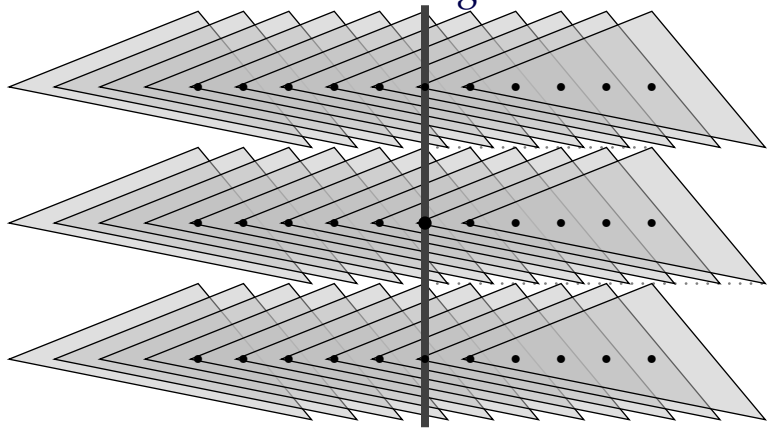
Lower bounds on the covering radius



- ▶ Simple lower bound: $\mu(\mathcal{L}, K) \geq \text{nd}(\mathcal{L}, K) = \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n} = 1 \quad \text{☹}$
- ▶ For any subspace W :

$$\mu(\mathcal{L}, K) \geq \mu(\Pi_W(\mathcal{L}), \Pi_W(K)) \geq \text{nd}(\Pi_W(\mathcal{L}), \Pi_W(K))$$

Lower bounds on the covering radius



► Simple lower bound: $\mu(\mathcal{L}, K) \geq \text{nd}(\mathcal{L}, K) = \left(\frac{\det(\mathcal{L})}{\text{vol}(K)} \right)^{1/n} = 1$ ☹

► For any subspace W :

$$\mu(\mathcal{L}, K) \geq \mu(\Pi_W(\mathcal{L}), \Pi_W(K)) \geq \text{nd}(\Pi_W(\mathcal{L}), \Pi_W(K)) = \frac{5}{3} \text{ ☺}$$

Main results

Denote

$$\alpha(\mathcal{L}, \mathbf{K}) := \max_{\text{subspace } W \subseteq \mathbb{R}^n} \text{nd}(\Pi_W(\mathcal{L}), \Pi_W(\mathbf{K})).$$

Main results

Denote

$$\alpha(\mathcal{L}, K) := \max_{\text{subspace } W \subseteq \mathbb{R}^n} \text{nd}(\Pi_W(\mathcal{L}), \Pi_W(K)).$$

Theorem [Kannan and Lovász '88]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\alpha(\mathcal{L}, K) \leq \mu(\mathcal{L}, K) \leq n \cdot \alpha(\mathcal{L}, K).$$

Main results

Denote

$$\alpha(\mathcal{L}, K) := \max_{\text{subspace } W \subseteq \mathbb{R}^n} \text{nd}(\Pi_W(\mathcal{L}), \Pi_W(K)).$$

Theorem [Kannan and Lovász '88]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\alpha(\mathcal{L}, K) \leq \mu(\mathcal{L}, K) \leq n \cdot \alpha(\mathcal{L}, K).$$

Theorem [R., Rothvoss '23]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mu(\mathcal{L}, K) \lesssim (\log n)^3 \cdot \alpha(\mathcal{L}, K).$$

Main results

Denote

$$\alpha(\mathcal{L}, K) := \max_{\text{subspace } W \subseteq \mathbb{R}^n} \text{nd}(\Pi_W(\mathcal{L}), \Pi_W(K)).$$

Theorem [Kannan and Lovász '88]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\alpha(\mathcal{L}, K) \leq \mu(\mathcal{L}, K) \leq n \cdot \alpha(\mathcal{L}, K).$$

Theorem [R., Rothvoss '23]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mu(\mathcal{L}, K) \lesssim (\log n)^3 \cdot \alpha(\mathcal{L}, K).$$

- Previously known only when K is a ball [DR '16, RSD '17]

Main results

Denote

$$\alpha(\mathcal{L}, K) := \max_{\text{subspace } W \subseteq \mathbb{R}^n} \text{nd}(\Pi_W(\mathcal{L}), \Pi_W(K)).$$

Theorem [Kannan and Lovász '88]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\alpha(\mathcal{L}, K) \leq \mu(\mathcal{L}, K) \leq n \cdot \alpha(\mathcal{L}, K).$$

Theorem [R., Rothvoss '23]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mu(\mathcal{L}, K) \lesssim (\log n)^3 \cdot \alpha(\mathcal{L}, K).$$

- Previously known only when K is a ball [DR '16, RSD '17]

Corollary [R., Rothvoss '23, following Dadush '12, '19]

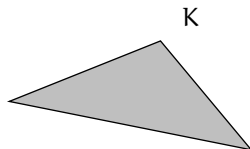
We can find a point in $K \cap \mathbb{Z}^n$ or certify $K \cap \mathbb{Z}^n = \emptyset$ in time $O(\log n)^{4n}$.

Well-rounded positions

Theorem [John '48]

For any convex $K \subset \mathbb{R}^n$ there exists an affine linear map T so that

$$B \subseteq T(K) \subseteq n \cdot B$$

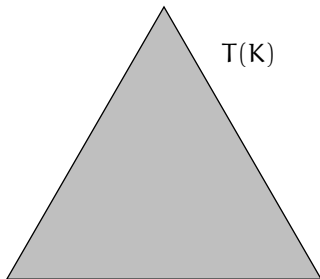


Well-rounded positions

Theorem [John '48]

For any convex $K \subset \mathbb{R}^n$ there exists an affine linear map T so that

$$B \subseteq T(K) \subseteq n \cdot B$$

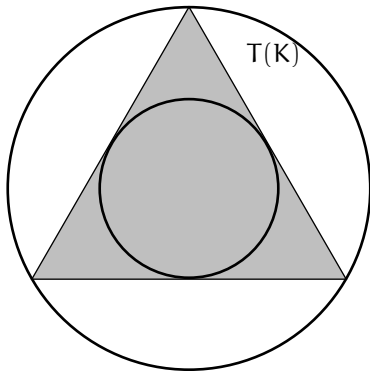


Well-rounded positions

Theorem [John '48]

For any convex $K \subset \mathbb{R}^n$ there exists an affine linear map T so that

$$B \subseteq T(K) \subseteq n \cdot B$$



Well-rounded positions

Theorem [John '48]

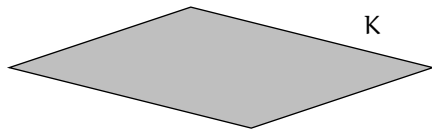
For any convex $K \subset \mathbb{R}^n$ there exists an affine linear map T so that

$$B \subseteq T(K) \subseteq n \cdot B$$

Theorem [Figiel, Tomczak-Jaegermann, Pisier '79]

For any *symmetric* convex $K \subset \mathbb{R}^n$ there exists a linear map T so that

$$\Pr_{c \sim S}[c \in T(K)] > 0.9 \quad \text{and} \quad \Pr_{c \sim S}[c^\top x \leq O(\log n) \forall x \in T(K)] > 0.9$$



Well-rounded positions

Theorem [John '48]

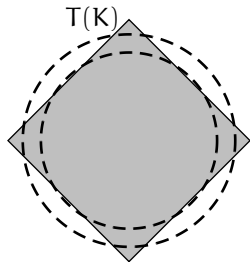
For any convex $K \subset \mathbb{R}^n$ there exists an affine linear map T so that

$$B \subseteq T(K) \subseteq n \cdot B$$

Theorem [Figiel, Tomczak-Jaegermann, Pisier '79]

For any *symmetric* convex $K \subset \mathbb{R}^n$ there exists a linear map T so that

$$\Pr_{c \sim S}[c \in T(K)] > 0.9 \quad \text{and} \quad \Pr_{c \sim S}[c^\top x \leq O(\log n) \forall x \in T(K)] > 0.9$$



Well-rounded positions

Theorem [John '48]

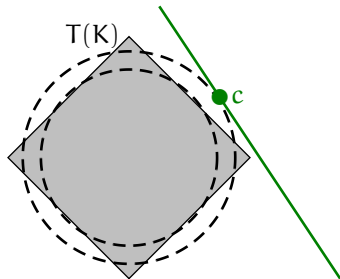
For any convex $K \subset \mathbb{R}^n$ there exists an affine linear map T so that

$$B \subseteq T(K) \subseteq n \cdot B$$

Theorem [Figiel, Tomczak-Jaegermann, Pisier '79]

For any *symmetric* convex $K \subset \mathbb{R}^n$ there exists a linear map T so that

$$\Pr_{c \sim S}[c \in T(K)] > 0.9 \quad \text{and} \quad \Pr_{c \sim S}[c^\top x \leq O(\log n) \forall x \in T(K)] > 0.9$$



Proof sketch

Theorem [R., Rothvoss '23]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mu(\mathcal{L}, K) \lesssim (\log n)^3 \cdot \alpha(\mathcal{L}, K).$$

Proof sketch

Theorem [R., Rothvoss '23]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mu(\mathcal{L}, K) \lesssim (\log n)^3 \cdot \alpha(\mathcal{L}, K).$$

- First $\log n$: Put K in ℓ -position by setting $K \leftarrow T(K), \mathcal{L} \leftarrow T(\mathcal{L})$

Proof sketch

Theorem [R., Rothvoss '23]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mu(\mathcal{L}, K) \lesssim (\log n)^3 \cdot \alpha(\mathcal{L}, K).$$

- ▶ First $\log n$: Put K in ℓ -position by setting $K \leftarrow T(K), \mathcal{L} \leftarrow T(\mathcal{L})$
- ▶ Second $\log n$: 'triangle inequality' for subspace W with $\dim W \geq \frac{n}{2}$:

$$\mu(\mathcal{L}, K) \leq \mu(\mathcal{L} \cap W, K \cap W) + \mu(\Pi_{W^\perp}(\mathcal{L}), \Pi_{W^\perp}(K))$$

and recurse $\log n$ many times on the projections.

Proof sketch

Theorem [R., Rothvoss '23]

For any convex $K \subset \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$,

$$\mu(\mathcal{L}, K) \lesssim (\log n)^3 \cdot \alpha(\mathcal{L}, K).$$

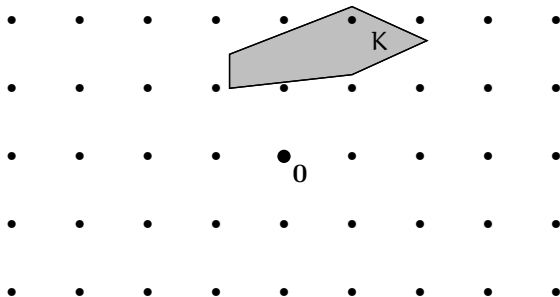
- ▶ First $\log n$: Put K in ℓ -position by setting $K \leftarrow T(K), \mathcal{L} \leftarrow T(\mathcal{L})$
- ▶ Second $\log n$: 'triangle inequality' for subspace W with $\dim W \geq \frac{n}{2}$:

$$\mu(\mathcal{L}, K) \leq \mu(\mathcal{L} \cap W, K \cap W) + \mu(\Pi_{W^\perp}(\mathcal{L}), \Pi_{W^\perp}(K))$$

and recurse $\log n$ many times on the projections.

- ▶ Third $\log n$: reverse Minkowski theorem [RSD '16]

Daniel's algorithm

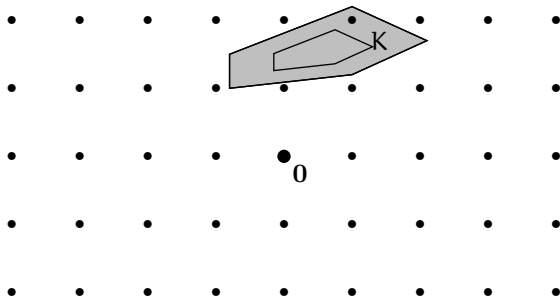


Input: $K \subset \mathbb{R}^n$ and lattice \mathcal{L}

Output: Point in $K \cap \mathcal{L}$

- (1) If $\mu(\mathcal{L}, K) \leq \frac{1}{2}$, 2-approx. IP finds a point in $K \cap \mathcal{L}$. Else $\mu(\mathcal{L}, K) > \frac{1}{2}$
- (2) Find subspace W (approximately) attaining $\alpha(\mathcal{L}, K)$
- (3) Enumerate $X := \Pi_W(K) \cap \Pi_W(\mathcal{L})$
- (4) Recurse on $K \cap \Pi_W^{-1}(x)$ for each $x \in X$

Daniel's algorithm

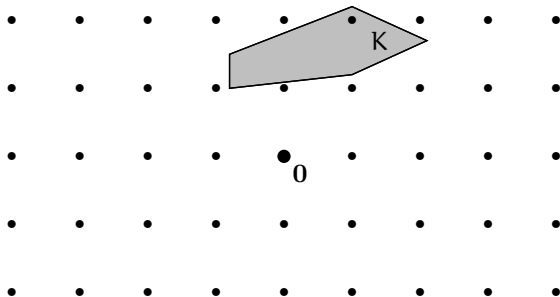


Input: $K \subset \mathbb{R}^n$ and lattice \mathcal{L}

Output: Point in $K \cap \mathcal{L}$

- (1) If $\mu(\mathcal{L}, K) \leq \frac{1}{2}$, 2-approx. IP finds a point in $K \cap \mathcal{L}$. Else $\mu(\mathcal{L}, K) > \frac{1}{2}$
- (2) Find subspace W (approximately) attaining $\alpha(\mathcal{L}, K)$
- (3) Enumerate $X := \Pi_W(K) \cap \Pi_W(\mathcal{L})$
- (4) Recurse on $K \cap \Pi_W^{-1}(x)$ for each $x \in X$

Daniel's algorithm

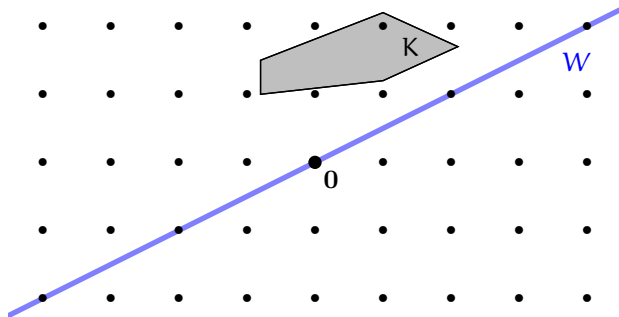


Input: $K \subset \mathbb{R}^n$ and lattice \mathcal{L}

Output: Point in $K \cap \mathcal{L}$

- (1) If $\mu(\mathcal{L}, K) \leq \frac{1}{2}$, 2-approx. IP finds a point in $K \cap \mathcal{L}$. Else $\mu(\mathcal{L}, K) > \frac{1}{2}$
- (2) Find subspace W (approximately) attaining $\alpha(\mathcal{L}, K)$
- (3) Enumerate $X := \Pi_W(K) \cap \Pi_W(\mathcal{L})$
- (4) Recurse on $K \cap \Pi_W^{-1}(x)$ for each $x \in X$

Daniel's algorithm

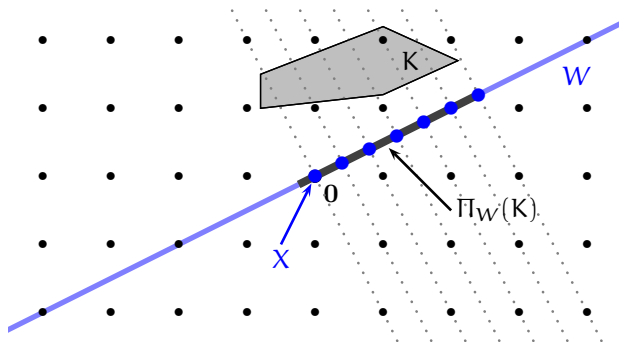


Input: $K \subset \mathbb{R}^n$ and lattice \mathcal{L}

Output: Point in $K \cap \mathcal{L}$

- (1) If $\mu(\mathcal{L}, K) \leq \frac{1}{2}$, 2-approx. IP finds a point in $K \cap \mathcal{L}$. Else $\mu(\mathcal{L}, K) > \frac{1}{2}$
- (2) Find subspace W (approximately) attaining $\alpha(\mathcal{L}, K)$
- (3) Enumerate $X := \Pi_W(K) \cap \Pi_W(\mathcal{L})$
- (4) Recurse on $K \cap \Pi_W^{-1}(x)$ for each $x \in X$

Daniel's algorithm

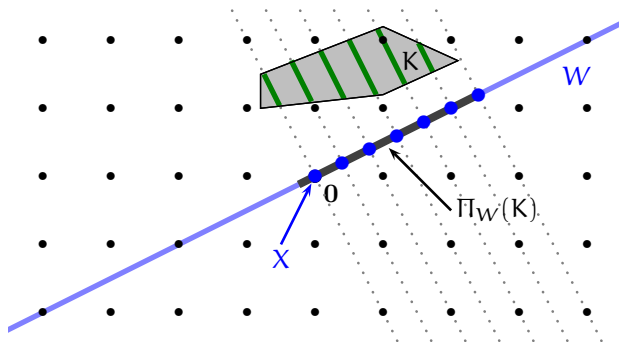


Input: $K \subset \mathbb{R}^n$ and lattice \mathcal{L}

Output: Point in $K \cap \mathcal{L}$

- (1) If $\mu(\mathcal{L}, K) \leq \frac{1}{2}$, 2-approx. IP finds a point in $K \cap \mathcal{L}$. Else $\mu(\mathcal{L}, K) > \frac{1}{2}$
- (2) Find subspace W (approximately) attaining $\alpha(\mathcal{L}, K)$
- (3) Enumerate $X := \Pi_W(K) \cap \Pi_W(\mathcal{L})$
- (4) Recurse on $K \cap \Pi_W^{-1}(x)$ for each $x \in X$

Daniel's algorithm



Input: $K \subset \mathbb{R}^n$ and lattice \mathcal{L}

Output: Point in $K \cap \mathcal{L}$

- (1) If $\mu(\mathcal{L}, K) \leq \frac{1}{2}$, 2-approx. IP finds a point in $K \cap \mathcal{L}$. Else $\mu(\mathcal{L}, K) > \frac{1}{2}$
- (2) Find subspace W (approximately) attaining $\alpha(\mathcal{L}, K)$
- (3) Enumerate $X := \Pi_W(K) \cap \Pi_W(\mathcal{L})$
- (4) Recurse on $K \cap \Pi_W^{-1}(x)$ for each $x \in X$

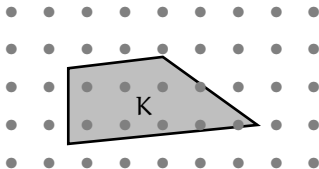
Upper bound on the number of lattice points

Theorem (Dadush 2012)

For any full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ we have

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

Moreover, we can enumerate the points in same time.



Upper bound on the number of lattice points

Theorem (Dadush 2012)

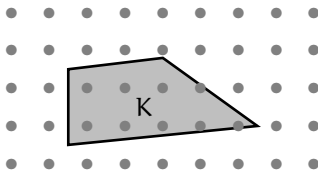
For any full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ we have

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

Moreover, we can enumerate the points in same time.

Proof of moreover part:

- Bound holds for any translate of K



Upper bound on the number of lattice points

Theorem (Dadush 2012)

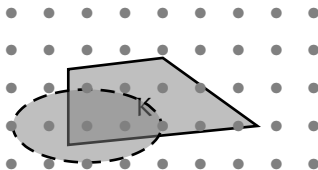
For any full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ we have

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

Moreover, we can enumerate the points in same time.

Proof of moreover part:

- Bound holds for any translate of K



Upper bound on the number of lattice points

Theorem (Dadush 2012)

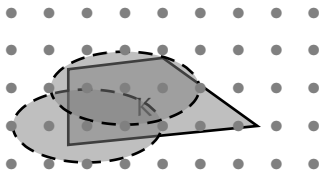
For any full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ we have

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

Moreover, we can enumerate the points in same time.

Proof of moreover part:

- Bound holds for any translate of K



Upper bound on the number of lattice points

Theorem (Dadush 2012)

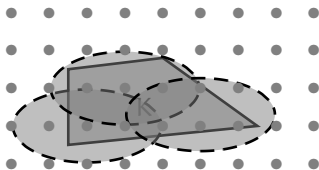
For any full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ we have

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

Moreover, we can enumerate the points in same time.

Proof of moreover part:

- Bound holds for any translate of K



Upper bound on the number of lattice points

Theorem (Dadush 2012)

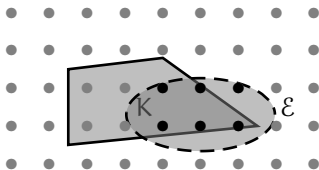
For any full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ we have

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

Moreover, we can enumerate the points in same time.

Proof of moreover part:

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



Upper bound on the number of lattice points

Theorem (Dadush 2012)

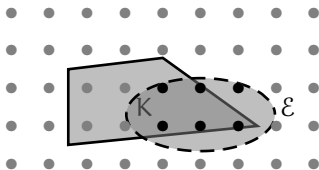
For any full rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$ and convex body $K \subseteq \mathbb{R}^n$ we have

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

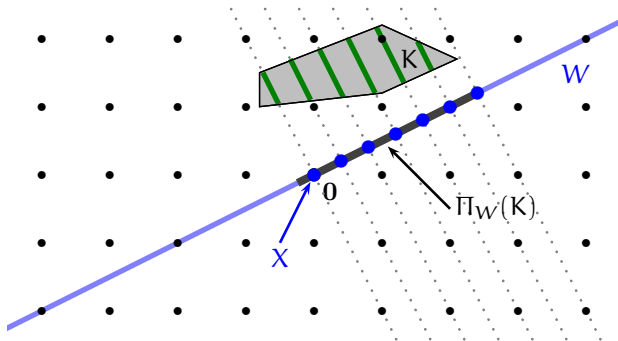
Moreover, we can enumerate the points in same time.

Proof of moreover part:

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



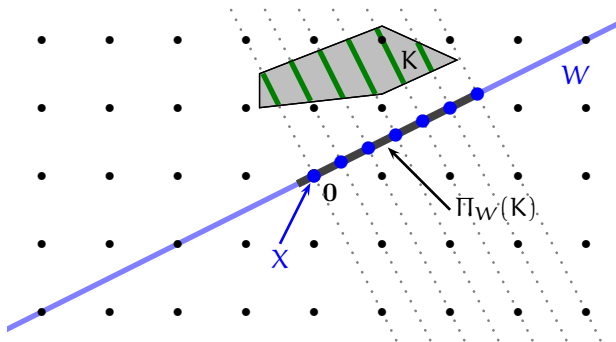
Daniel's algorithm (analysis)



Analysis:

- Can find W in time $2^{O(n)}$ [Dadush '12]

Daniel's algorithm (analysis)

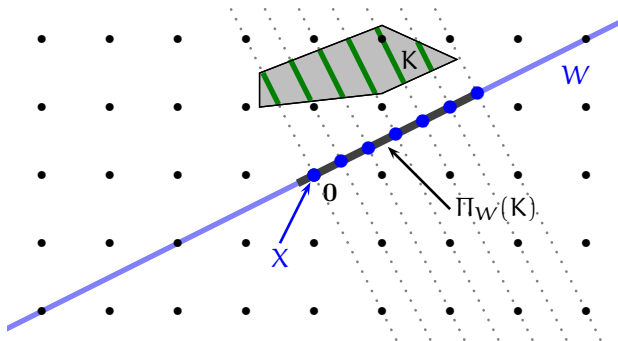


Analysis:

- ▶ Can find W in time $2^{O(n)}$ [Dadush '12]
- ▶ Recursion for runtime ($d := \dim W$):

$$T(n) \leq 2^{O(n)} + |\Pi_W(K) \cap \Pi_W(\mathcal{L})| \cdot T(n - d)$$

Daniel's algorithm (analysis)

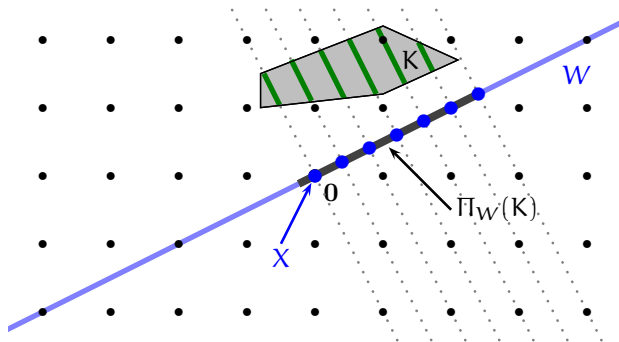


Analysis:

- ▶ Can find W in time $2^{O(n)}$ [Dadush '12]
- ▶ Recursion for runtime ($d := \dim W$):

$$T(n) \leq 2^{O(n)} + n^d \cdot T(n-d) \implies T(n) \leq O(n)^n$$

Daniel's algorithm (analysis)



Analysis:

- ▶ Can find $(\log n)$ -approximate W in time $2^{O(n)}$ [Dadush '12, '19]
- ▶ Recursion for runtime ($d := \dim W$):

$$T(n) \leq 2^{O(n)} + (\log n)^{4d} \cdot T(n-d) \implies T(n) \leq O(\log n)^{4n}$$

Future directions

- ▶ What can we do with polynomial space? Best runtime still $n^{O(n)}$

Future directions

- ▶ What can we do with polynomial space? Best runtime still $n^{O(n)}$
- ▶ Integer programming in $2^{O(n)}$ time? Even if K is a simplex?

Future directions

- ▶ What can we do with polynomial space? Best runtime still $n^{O(n)}$
- ▶ Integer programming in $2^{O(n)}$ time? Even if K is a simplex?

Thanks for your attention!