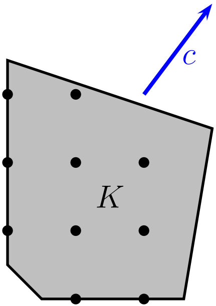
From approximate to exact integer programming

Daniel Dadush, Fritz Eisenbrand,
Thomas Rothvoss

CWI EPFL UNIVERSITY of WASHINGTON

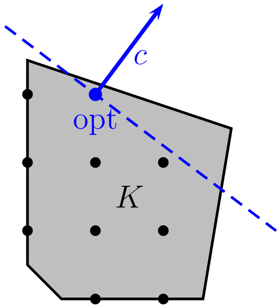
Integer programming

$$\max\{c^T x \mid Ax \leq b, x \in \mathbb{Z}^n\}$$



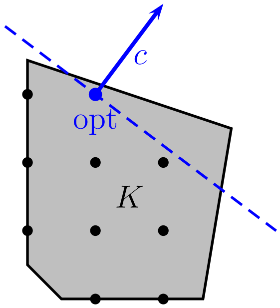
Integer programming

$$\max\{c^T x \mid Ax \le b, x \in \mathbb{Z}^n\}$$



Integer programming

$$\max\{c^T x \mid Ax \leq b, x \in \mathbb{Z}^n\}$$

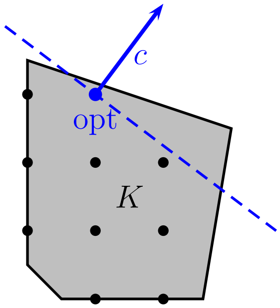


Applications:

- Logistics / transportation
- Scheduling / timetabling
- Chip design
- Inventory management

Integer programming

$$\max\{c^T x \mid Ax \leq b, x \in \mathbb{Z}^n\}$$



Mathematics at intersection of

- Convex geometry
- Geometry of numbers
- Convex optimization

Integer programming

Known results:

- **NP**-hard [Karp '72]

Integer programming

Known results:

- **NP**-hard [Karp '72]
- Can be solved in time $f(n) \cdot \mathrm{poly}(m, \langle A, b, c \rangle)$ [Lenstra 1983]
- Improved to $n^{O(n)}$-time algorithm [Kannan 1983]

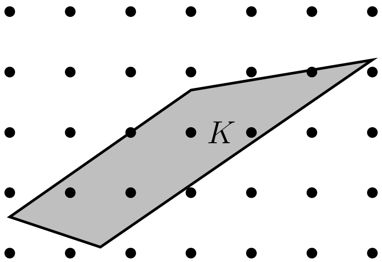
Integer programming

Known results:

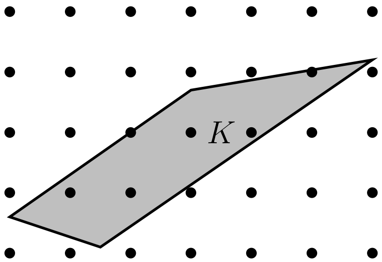
- **NP**-hard [Karp '72]
- Can be solved in time $f(n) \cdot \text{poly}(m, \langle A, b, c \rangle)$ [Lenstra 1983]
- Improved to $n^{O(n)}$-time algorithm [Kannan 1983]
- Very different $2^{O(n)} n^n$-time algorithm by [Dadush 2012] (rather involved, following [Kannan, Lovász 1988])

Currently best Lenstra-type bound: $(\tilde{O}(n^{4/3}))^n$

Modern interp. of Lenstra's algorithm

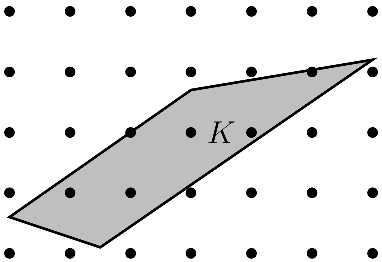


Modern interp. of Lenstra's algorithm



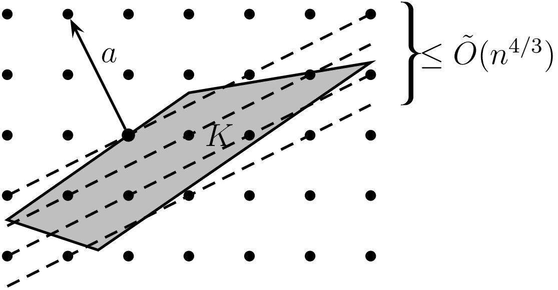
- Banaszczyk (1996) + Rudelson (1998):
  $\mu(\mathbb{Z}^n, K) \cdot \lambda_1(\mathbb{Z}^n, (K-K)^\circ) \leq \tilde{O}(n^{4/3})$

Modern interp. of Lenstra's algorithm



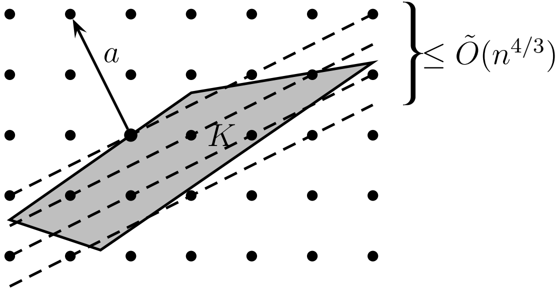
- Banaszczyk (1996) + Rudelson (1998):
  $\mu(\mathbb{Z}^n, K) \cdot \lambda_1(\mathbb{Z}^n, (K-K)^\circ) \leq \tilde{O}(n^{4/3})$
- **Translation:** If some translate of K is lattice point free, then $K \cap \mathbb{Z}^n$ is contained in $\tilde{O}(n^{4/3})$ hyperplanes $a^T x = \mathbb{Z}$ where $a \in \mathbb{Z}^n$

Modern interp. of Lenstra's algorithm



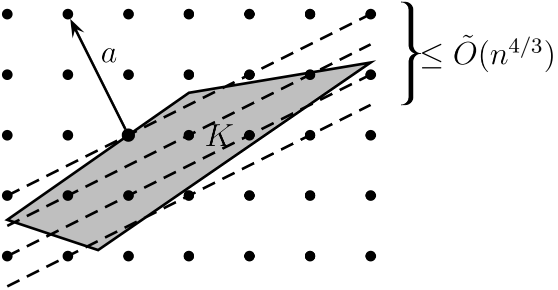
- Banaszczyk (1996) + Rudelson (1998):
  $\mu(\mathbb{Z}^n, K) \cdot \lambda_1(\mathbb{Z}^n, (K-K)^\circ) \leq \tilde{O}(n^{4/3})$
- **Translation:** If some translate of K is lattice point free, then $K \cap \mathbb{Z}^n$ is contained in $\tilde{O}(n^{4/3})$ hyperplanes $a^T x = \mathbb{Z}$ where $a \in \mathbb{Z}^n$

Modern interp. of Lenstra's algorithm



- Banaszczyk (1996) + Rudelson (1998): $\mu(\mathbb{Z}^n, K) \cdot \lambda_1(\mathbb{Z}^n, (K-K)^\circ) \leq \tilde{O}(n^{4/3})$
- **Translation:** If some translate of K is lattice point free, then $K \cap \mathbb{Z}^n$ is contained in $\tilde{O}(n^{4/3})$ hyperplanes $a^T x = \mathbb{Z}$ where $a \in \mathbb{Z}^n$
- Recurse on $\tilde{O}(n^{4/3})$ many $(n-1)$-dimensional subproblems

Modern interp. of Lenstra's algorithm

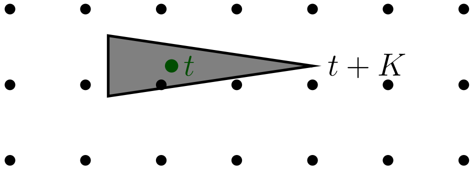


- Banaszczyk (1996) + Rudelson (1998):
  $\mu(\mathbb{Z}^n, K) \cdot \lambda_1(\mathbb{Z}^n, (K-K)^\circ) \leq \tilde{O}(n^{4/3})$
- **Translation:** If some translate of K is lattice point free, then $K \cap \mathbb{Z}^n$ is contained in $\tilde{O}(n^{4/3})$ hyperplanes $a^T x = \mathbb{Z}$ where $a \in \mathbb{Z}^n$
- Recurse on $\tilde{O}(n^{4/3})$ many $(n-1)$-dimensional subproblems
- $\Rightarrow \tilde{O}(n^{4/3})^n$-time algorithm

Approximate IP

Theorem (Dadush 2014)

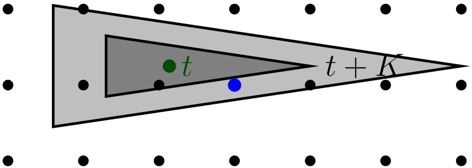
Given convex set K with barycenter $\mathbf{0}$, can find a 2-apx to $\min\{\|x - t\|_K : x \in \mathbb{Z}^n\}$ in time $2^{O(n)}$.



Approximate IP

Theorem (Dadush 2014)

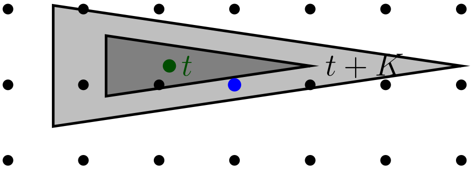
Given convex set K with barycenter $\mathbf{0}$, can find a 2-apx to $\min\{\|x - t\|_K : x \in \mathbb{Z}^n\}$ in time $2^{O(n)}$.



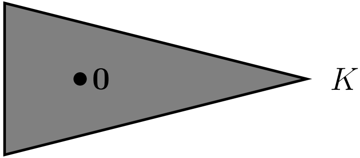
Approximate IP

Theorem (Dadush 2014)

Given convex set K with barycenter $\mathbf{0}$, can find a 2-apx to $\min\{\|x - t\|_K : x \in \mathbb{Z}^n\}$ *in time* $2^{O(n)}$.



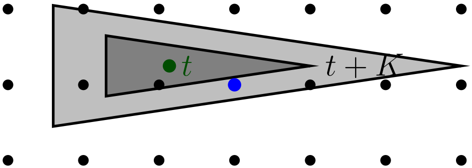
- Suffices if $\mathrm{Vol}_n(K \cap (-K)) \geq 2^{-\Theta(n)} \mathrm{Vol}_n(K)$



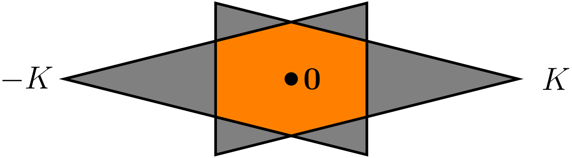
Approximate IP

Theorem (Dadush 2014)

Given convex set K with barycenter $\mathbf{0}$, can find a 2-apx to $\min\{\|x - t\|_K : x \in \mathbb{Z}^n\}$ *in time* $2^{O(n)}$.



- Suffices if $\mathrm{Vol}_n(K \cap (-K)) \geq 2^{-\Theta(n)} \mathrm{Vol}_n(K)$



Main results

- Using approximate IP we can get:

Theorem (Dadush, Eisenbrand, R.)

There is a (simpler) $2^{O(n)}n^n$ time algorithm for integer programming. Moreover if we are given $x^* \mod 5(n+1)$ for some feasible $x^* \in K \cap \mathbb{Z}^n$ we can solve IP in time $2^{O(n)}$.

Main results

- Using approximate IP we can get:

Theorem (Dadush, Eisenbrand, R.)

There is a (simpler) $2^{O(n)}n^n$ time algorithm for integer programming. Moreover if we are given $x^* \mod 5(n+1)$ for some feasible $x^* \in K \cap \mathbb{Z}^n$ we can solve IP in time $2^{O(n)}$.

Theorem (Dadush, Eisenbrand, R.)

The capacitated IP

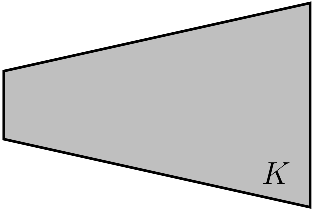
$$\max\{c^T x \mid Ax = b,\ \mathbf{0} \leq x \leq u,\ x \in \mathbb{Z}^n\}$$

can be solved in time $(\log \|u\|_\infty)^{O(n)}$.

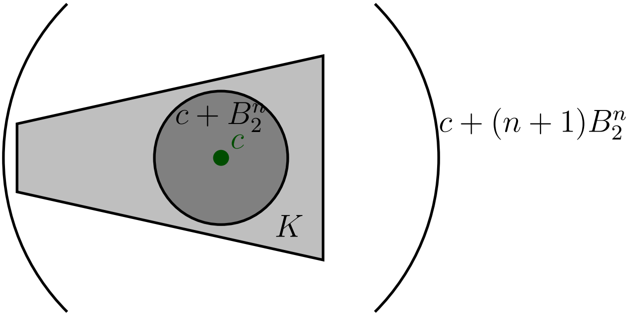
Part I

A new $2^{O(n)}n^n$-time algorithm for general IP

Algorithm I

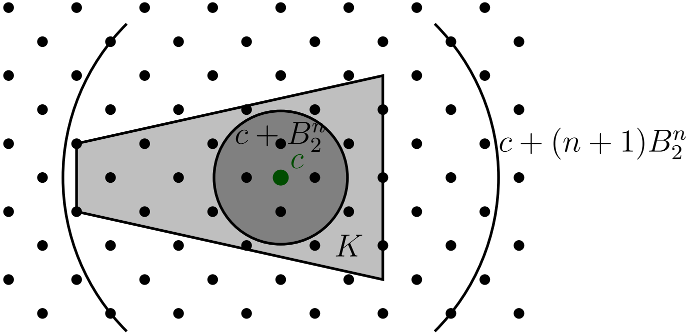


Algorithm I



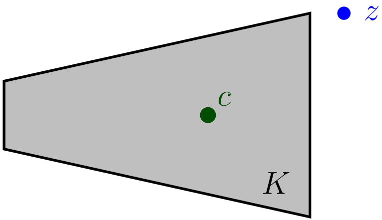
(1) After lin. transf. $c + B_2^n \subseteq K \subseteq c + (n+1)B_2^n$, c baryc.

Algorithm I



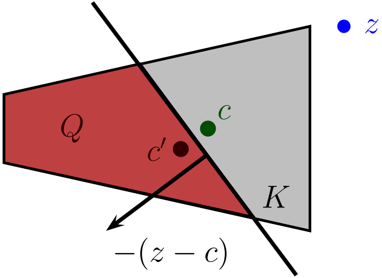
(1) After lin. transf. $c + B_2^n \subseteq K \subseteq c + (n+1)B_2^n$, c baryc.

Algorithm I



(1) After lin. transf. $c + B_2^n \subseteq K \subseteq c + (n+1)B_2^n$, c baryc.
(2) Find $z \in \Lambda$ in 2-scaling of K

Algorithm I



(1) After lin. transf. $c + B_2^n \subseteq K \subseteq c + (n+1)B_2^n$, c baryc.

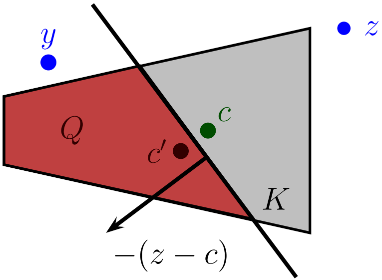
(2) Find $z \in \Lambda$ in 2-scaling of K

(2) FOR $k = 1$ TO poly(n) DO

  (3) Find $y \in \Lambda$ in 2-scaling of
  $Q := K \cap \{x \mid \langle z - c, x - c\rangle \leq -\frac{1}{\text{poly}(n)}\}$

  (4) Update $z' := (1 - \frac{1}{k})z + \frac{1}{k}y$

Algorithm I



(1) After lin. transf. $c + B_2^n \subseteq K \subseteq c + (n+1)B_2^n$, c baryc.

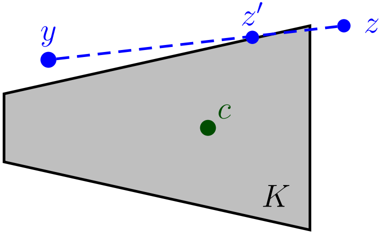
(2) Find $z \in \Lambda$ in 2-scaling of K

(2) FOR $k = 1$ TO poly(n) DO

  (3) Find $y \in \Lambda$ in 2-scaling of
  $Q := K \cap \{x \mid \langle z-c, x-c\rangle \leq -\frac{1}{\text{poly}(n)}\}$

  (4) Update $z' := (1-\frac{1}{k})z + \frac{1}{k}y$

Algorithm I



(1) After lin. transf. $c + B_2^n \subseteq K \subseteq c + (n+1)B_2^n$, c baryc.

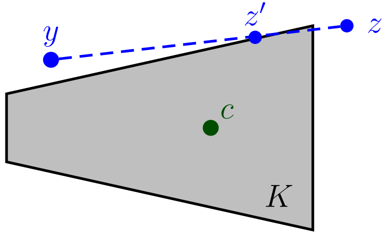
(2) Find $z \in \Lambda$ in 2-scaling of K

(2) FOR $k = 1$ TO poly(n) DO

  (3) Find $y \in \Lambda$ in 2-scaling of
  $Q := K \cap \{x \mid \langle z - c, x - c\rangle \leq -\frac{1}{\text{poly}(n)}\}$

  (4) Update $z' := (1 - \frac{1}{k})z + \frac{1}{k}y$

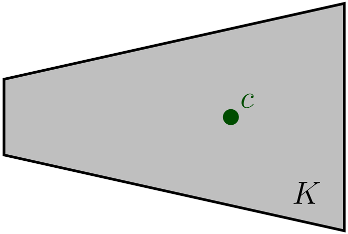
Algorithm I



(1) After lin. transf. $c + B_2^n \subseteq K \subseteq c + (n+1)B_2^n$, c baryc.
(2) Find $z \in \Lambda$ in 2-scaling of K
(2) FOR $k = 1$ TO poly(n) DO
  (3) Find $y \in \Lambda$ in 2-scaling of
  $Q := K \cap \{x \mid \langle z - c, x - c\rangle \leq -\frac{1}{\text{poly}(n)}\}$
  (4) Update $z' := (1 - \frac{1}{k})z + \frac{1}{k}y$
(5) IF successfull THEN find point in $K \cap \frac{\Lambda}{5(n+1)}$
(6) ELSE update $K' := K \cap \{x \mid \langle z - c, x - c\rangle \geq -\frac{1}{\text{poly}(n)}\}$

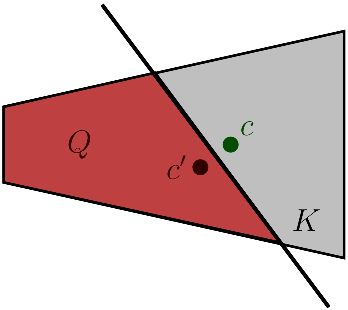
Analysis (1)

Case I: No lattice point in $Q \Rightarrow$ volume of K decreases by constant factor.



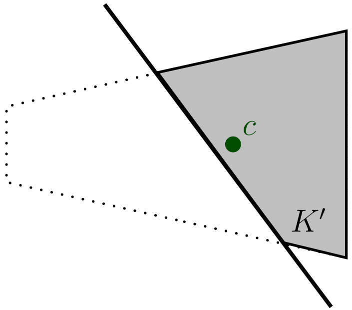
Analysis (1)

Case I: No lattice point in $Q \Rightarrow$ volume of K decreases by constant factor.



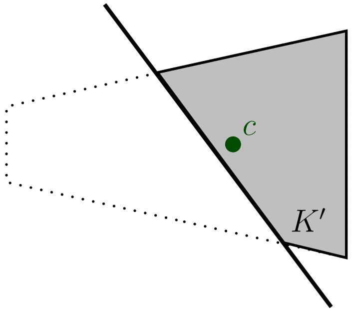
Analysis (1)

Case I: No lattice point in $Q \Rightarrow$ volume of K decreases by constant factor.



Analysis (1)

Case I: No lattice point in $Q \Rightarrow$ volume of K decreases by constant factor.

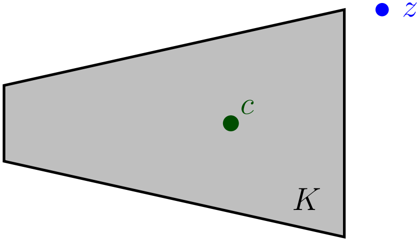


Theorem (Grünbaum)

Let $K \subseteq \mathbb{R}^n$ be a convex body. Any hyperplane H through the barycenter splits K into two parts with volume $\geq \frac{1}{e} Vol_n(K)$ each.

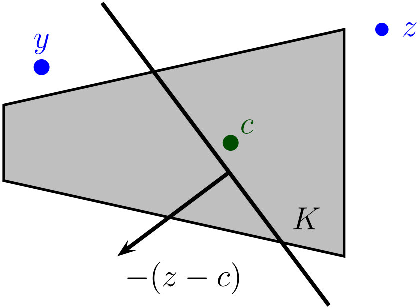
Anaylsis (2)

Case II: If we always find a lattice point in Q (scaled by factor 2), then c is (approx) convex combination of lattice points $X \subseteq \Lambda \cap 3(K - c) + c$.



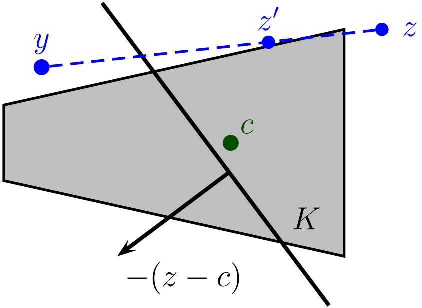
Anaylsis (2)

Case II: If we always find a lattice point in Q (scaled by factor 2), then c is (approx) convex combination of lattice points $X \subseteq \Lambda \cap 3(K - c) + c$.



Anaylsis (2)

Case II: If we always find a lattice point in Q (scaled by factor 2), then c is (approx) convex combination of lattice points $X \subseteq \Lambda \cap 3(K - c) + c$.

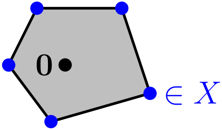


- After k iterations $\|z - c\|_2 \leq O(\frac{n}{\sqrt{k}})$.
- After $k = \text{poly}(n)$ iterations $z \approx c$

Asym. Approximate Caratheodory Thm

Lemma

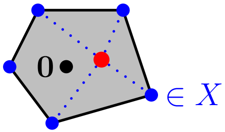
If $\mathbf{0} \in P := conv(X)$, *then for any* k, *there are* $u_1, \ldots, u_k \in X$ *with* $\|\frac{1}{k}\sum_{i=1}^{k} u_i\|_P \leq \frac{n+1}{k}$.



Asym. Approximate Caratheodory Thm

Lemma

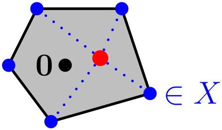
If $\mathbf{0} \in P := conv(X)$, then for any k, there are $u_1, \ldots, u_k \in X$ with $\|\frac{1}{k}\sum_{i=1}^{k} u_i\|_P \leq \frac{n+1}{k}$.



Asym. Approximate Caratheodory Thm

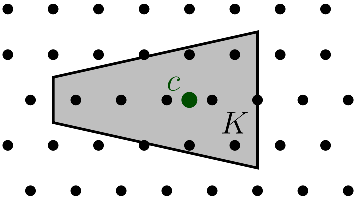
Lemma

If $\mathbf{0} \in P := conv(X)$, then for any k, there are $u_1, \ldots, u_k \in X$ with $\|\frac{1}{k}\sum_{i=1}^{k} u_i\|_P \leq \frac{n+1}{k}$.



Our application: $P :=$ 3-scaling of K.

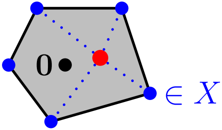
- $c \approx$ convex comb. of lattice points in 3-scaling
  $\Rightarrow$ unweighted average of $5(n+1)$ lattice points in K



Asym. Approximate Caratheodory Thm

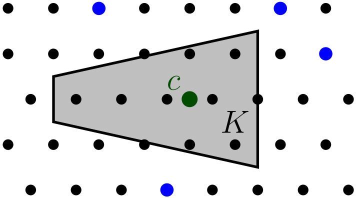
Lemma

If $\mathbf{0} \in P := conv(X)$, then for any k, there are $u_1, \ldots, u_k \in X$ with $\|\frac{1}{k}\sum_{i=1}^{k} u_i\|_P \leq \frac{n+1}{k}$.



Our application: $P :=$ 3-scaling of K.

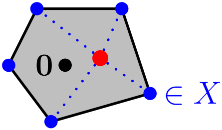
- $c \approx$ convex comb. of lattice points in 3-scaling
  $\Rightarrow$ unweighted average of $5(n+1)$ lattice points in K



Asym. Approximate Caratheodory Thm

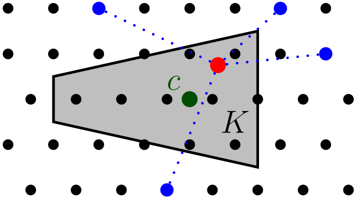
Lemma

If $\mathbf{0} \in P := conv(X)$*, then for any* k*, there are* $u_1, \ldots, u_k \in X$ *with* $\|\frac{1}{k}\sum_{i=1}^{k} u_i\|_P \leq \frac{n+1}{k}$.



Our application: $P :=$ 3-scaling of K.

- $c \approx$ convex comb. of lattice points in 3-scaling
  $\Rightarrow$ unweighted average of $5(n+1)$ lattice points in K

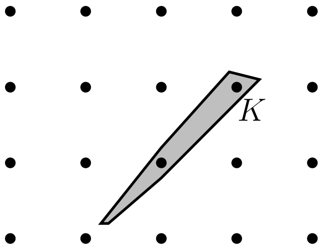


Recursion is needed

- Recursion similar to **Ellipsoid method** is needed

Lemma

Suppose initially $K \subseteq rB_2^n$. Then after $O(n^2 \log(\frac{nr}{\lambda_1(\Lambda)}))$ iterations all points in $K \cap \Lambda$ contained in $(n-1)$-dim. subspace (which can be found in time $2^{O(n)}$)

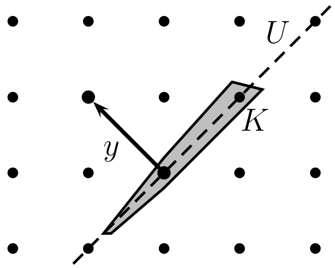


Recursion is needed

- Recursion similar to **Ellipsoid method** is needed

Lemma

Suppose initially $K \subseteq rB_2^n$. Then after $O(n^2 \log(\frac{nr}{\lambda_1(\Lambda)}))$ iterations all points in $K \cap \Lambda$ contained in $(n-1)$-dim. subspace (which can be found in time $2^{O(n)}$)



Conclusion

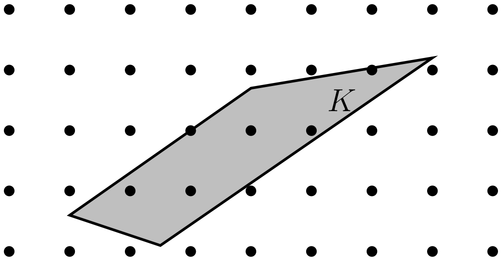
Conclusion: For any lattice Λ, if $K \cap \Lambda \neq \emptyset$ then we can find a point in $K \cap \frac{\Lambda}{5(n+1)}$ in time $2^{O(n)}$.

Conclusion

Conclusion: For any lattice Λ, if $K \cap \Lambda \neq \emptyset$ then we can find a point in $K \cap \frac{\Lambda}{5(n+1)}$ in time $2^{O(n)}$.

Theorem

One can find a point in $K \cap \mathbb{Z}^n$ in time $(O(n))^n$.

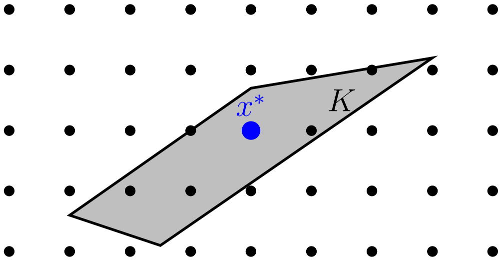


Conclusion

Conclusion: For any lattice Λ, if $K \cap \Lambda \neq \emptyset$ then we can find a point in $K \cap \frac{\Lambda}{5(n+1)}$ in time $2^{O(n)}$.

Theorem

One can find a point in $K \cap \mathbb{Z}^n$ in time $(O(n))^n$.



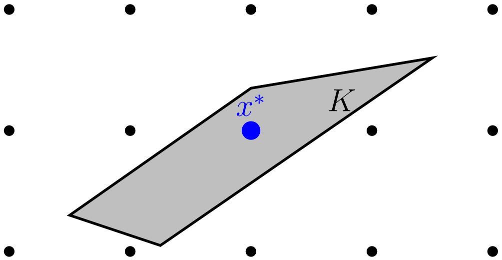
- For some $x^* \in K \cap \mathbb{Z}^n$, guess x^* mod $(5n+1)$

Conclusion

Conclusion: For any lattice Λ, if $K \cap \Lambda \neq \emptyset$ then we can find a point in $K \cap \frac{\Lambda}{5(n+1)}$ in time $2^{O(n)}$.

Theorem

One can find a point in $K \cap \mathbb{Z}^n$ in time $(O(n))^n$.



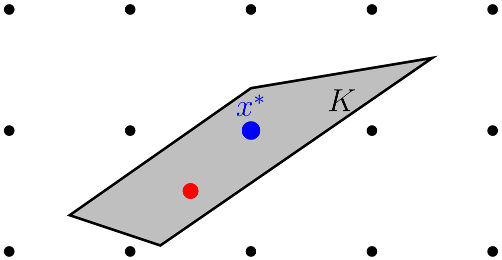
- For some $x^* \in K \cap \mathbb{Z}^n$, guess $x^* \bmod (5n+1)$
- Run algorithm with $\Lambda := (5n+1)\mathbb{Z}^n + (x^* \bmod (5n+1))$ and K

Conclusion

Conclusion: For any lattice Λ, if $K \cap \Lambda \neq \emptyset$ then we can find a point in $K \cap \frac{\Lambda}{5(n+1)}$ in time $2^{O(n)}$.

Theorem

One can find a point in $K \cap \mathbb{Z}^n$ in time $(O(n))^n$.



- For some $x^* \in K \cap \mathbb{Z}^n$, guess $x^* \bmod (5n+1)$
- Run algorithm with $\Lambda := (5n+1)\mathbb{Z}^n + (x^* \bmod (5n+1))$ and K

Part II

A new algorithm for capacitated IPs

Solving IPs in equality form

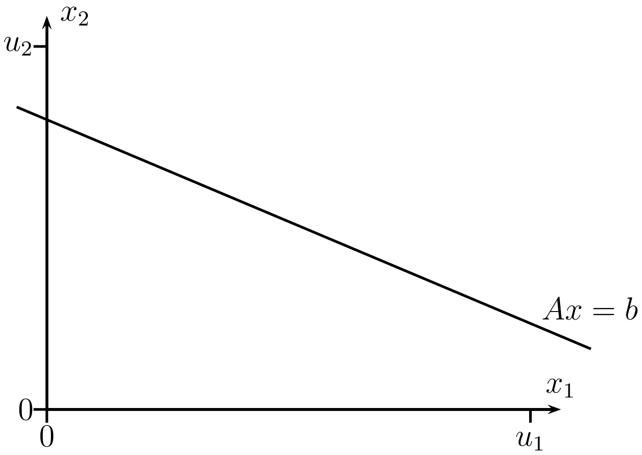
Theorem (Dadush, Eisenbrand, R.)

One can find a feasible point with

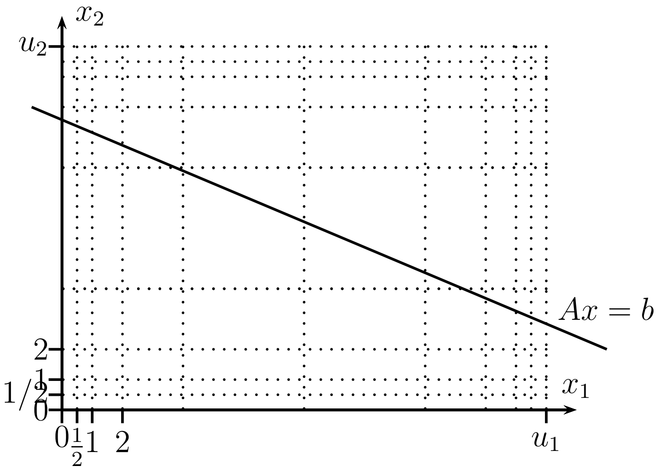
$$Ax = b,\ \mathbf{0} \leq x \leq u,\ x \in \mathbb{Z}^n$$

in time $(\log \|u\|_\infty)^{O(n)}$.

Solving IPs in equality form (2)

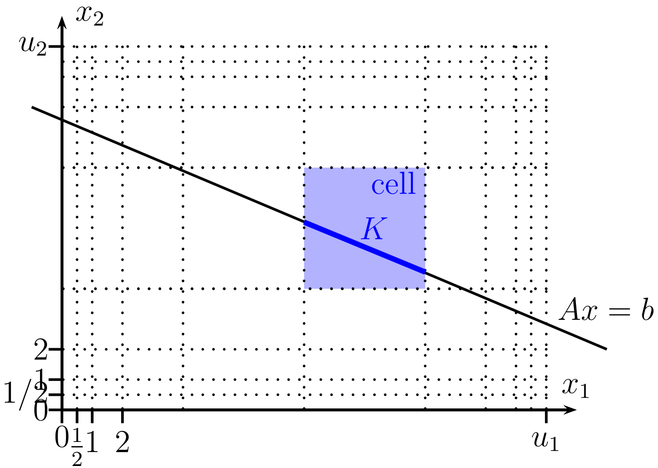


Solving IPs in equality form (2)



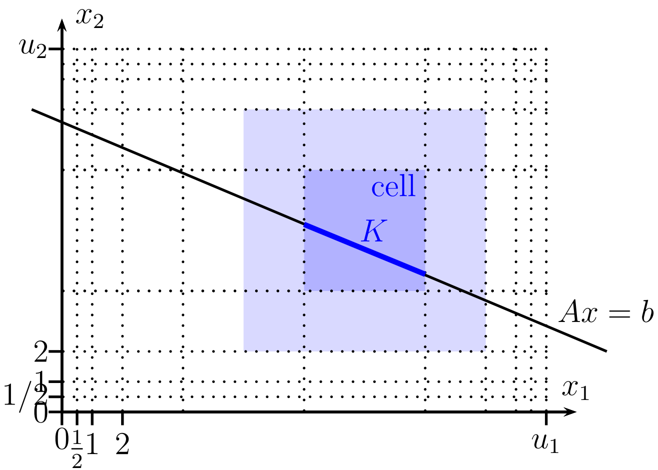
- Consider hyperplanes $\mathcal{H}$ of the form $x_i = 2^{\mathbb{Z}_{\geq -1}}$, $x_i = u_i - 2^{\mathbb{Z}_{\geq -1}}$, $x_i = 0$, $x_i = u_i$.

Solving IPs in equality form (2)



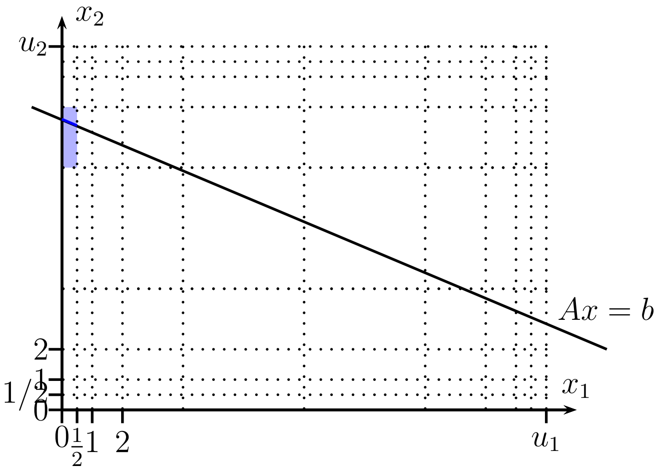
- Consider hyperplanes $\mathcal{H}$ of the form $x_i = 2^{\mathbb{Z}_{\geq -1}}$, $x_i = u_i - 2^{\mathbb{Z}_{\geq -1}}$, $x_i = 0$, $x_i = u_i$.
- Call 2-apx IP for any $K := \{x \mid Ax = b\} \cap \text{cell}$

Solving IPs in equality form (2)



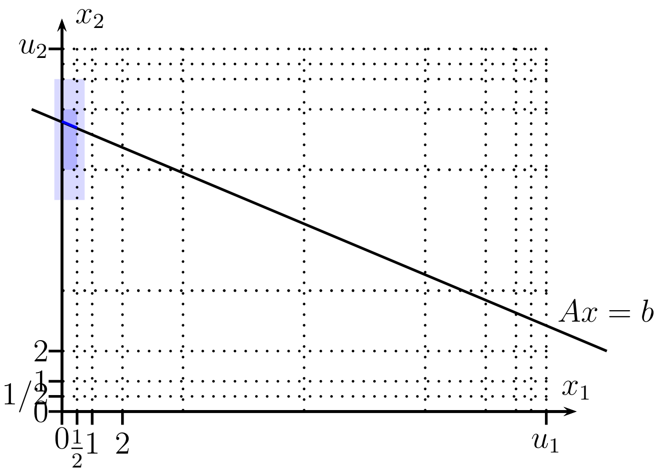
- Consider hyperplanes $\mathcal{H}$ of the form $x_i = 2^{\mathbb{Z}_{\geq -1}}$, $x_i = u_i - 2^{\mathbb{Z}_{\geq -1}}$, $x_i = 0$, $x_i = u_i$.
- Call 2-apx IP for any $K := \{x \mid Ax = b\} \cap \text{cell}$

Solving IPs in equality form (2)



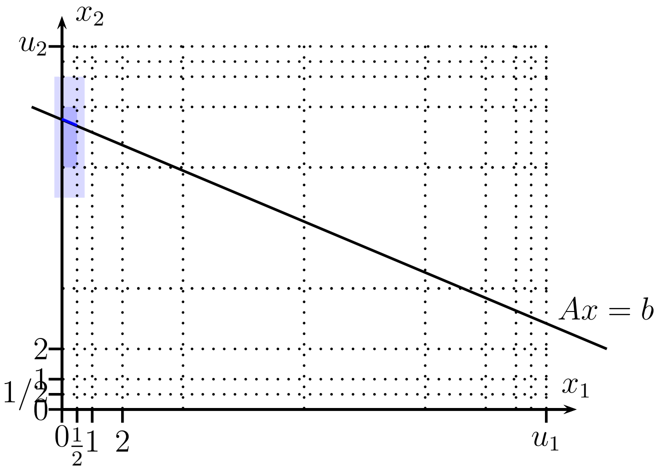
- Consider hyperplanes $\mathcal{H}$ of the form $x_i = 2^{\mathbb{Z}_{\geq -1}}$, $x_i = u_i - 2^{\mathbb{Z}_{\geq -1}}$, $x_i = 0$, $x_i = u_i$.
- Call 2-apx IP for any $K := \{x \mid Ax = b\} \cap \text{cell}$

Solving IPs in equality form (2)



- Consider hyperplanes $\mathcal{H}$ of the form $x_i = 2^{\mathbb{Z}_{\geq -1}}$, $x_i = u_i - 2^{\mathbb{Z}_{\geq -1}}$, $x_i = 0$, $x_i = u_i$.
- Call 2-apx IP for any $K := \{x \mid Ax = b\} \cap \text{cell}$

Solving IPs in equality form (2)



- Number of cells is $|\mathcal{H}| \leq O(\log \|u\|_\infty)^n$

Extension

Theorem (Dadush, Eisenbrand, R.)

One can solve

$$\max\{c^T x \mid Ax \le b,\ \mathbf{0} \le x \le u,\ x \in \mathbb{Z}^n\}$$

in time $n^{O(m)} \cdot (\log \|u\|_\infty)^{O(n)}$.

Extension

Theorem (Dadush, Eisenbrand, R.)

One can solve

$$\max\{c^T x \mid Ax \leq b,\ \mathbf{0} \leq x \leq u,\ x \in \mathbb{Z}^n\}$$

in time $n^{O(m)} \cdot (\log \|u\|_\infty)^{O(n)}$.

- Suffices to solve feasibility
- May assume A, b integral with $\|A\|_\infty, \|b\|_\infty \leq 2^{O(n^3)} \|u\|_\infty^{O(n^2)}$ [Frank, Tardos '87]

Extension

Theorem (Dadush, Eisenbrand, R.)

One can solve

$$\max\{c^T x \mid Ax \leq b,\ \mathbf{0} \leq x \leq u,\ x \in \mathbb{Z}^n\}$$

in time $n^{O(m)} \cdot (\log \|u\|_\infty)^{O(n)}$.

- Suffices to solve feasibility
- May assume A, b integral with $\|A\|_\infty, \|b\|_\infty \leq 2^{O(n^3)} \|u\|_\infty^{O(n^2)}$ [Frank, Tardos '87]
- Then transform

$$A_i x \leq b_i \quad \rightarrow \quad A_i x + s_i = b_i, \quad 0 \leq s_i \leq 2^{O(n^3)} \|u\|_\infty^{O(n^2)}$$

Follow-up and open problems

More recently:

Theorem (Reis, R. '23)

One can solve any n-variable IP in time $(\log n)^{O(n)}$.

Follow-up and open problems

More recently:

Theorem (Reis, R. '23)

One can solve any n-variable IP in time $(\log n)^{O(n)}$.

Open problems:

(1) Can one solve n-variable IPs in time $2^{O(n)}$?

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

(3) Can one solve **shortest vector** w.r.t. $\|\cdot\|_2$ in time $2^{O(n)}$ and **polynomial space**?

(4) Can one find a point in $K \cap \mathbb{Z}^n$ in time $2^{O(n)}$ if K is a **simplex**?

Follow-up and open problems

More recently:

Theorem (Reis, R. '23)

One can solve any n-variable IP in time $(\log n)^{O(n)}$.

Open problems:

(1) Can one solve n-variable IPs in time $2^{O(n)}$?

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

(3) Can one solve **shortest vector** w.r.t. $\| \cdot \|_2$ in time $2^{O(n)}$ and **polynomial space**?

(4) Can one find a point in $K \cap \mathbb{Z}^n$ in time $2^{O(n)}$ if K is a **simplex**?

Thanks for your attention!