The computational complexity of integer programming with alternations

Igor Pak, UCLA

Joint work with Danny Nguyen, UCLA

Computational Complexity Conference

Riga, Latvia, July 6, 2017

What is this all about?

Let $P \subset \mathbb{R}^d$ be a convex polytope given by $A\mathbf{x} \leq \bar{b}$. Say, $d = 3$.

Can one compute $\#\mathrm{E}(P)$ – the *number of integer points* in P? (Yes!)

How about $\#\mathrm{E}(P \smallsetminus Q)$? Or $\#\big[\mathrm{E}(P)\downarrow_x\big]$? (Yes, yes!)

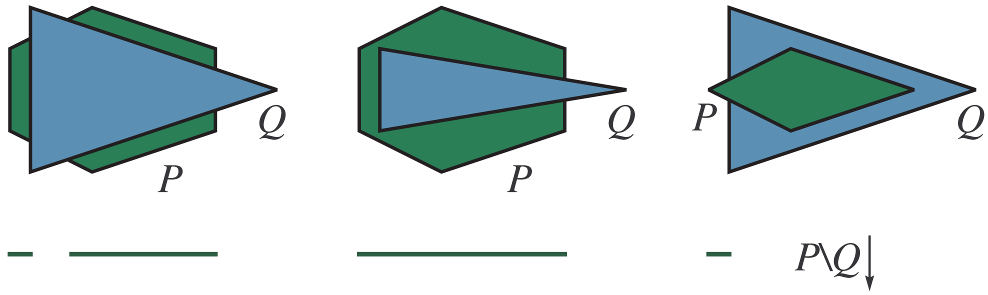
Theorem 1 (Nguyen–P.)
For $P, Q \in \mathbb{R}^3$, computing $\#\big[\mathrm{E}(P \smallsetminus Q)\downarrow_x\big]$ is $\#\mathsf{P}$-complete.

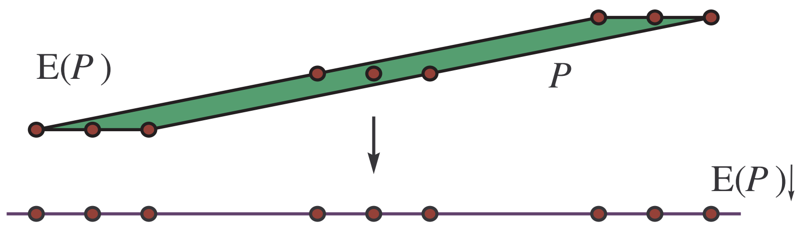
Theorem 2 (Nguyen–P.)
Given three polytopes $U_1, U_2, U_3 \subset \mathbb{R}^4$ and two boxes $I \subset \mathbb{Z}, K \subset \mathbb{Z}^3$, deciding the following sentence is NP-complete:

$$\exists x \in I \quad \forall \mathbf{z} \in K \quad : \quad (x, \mathbf{z}) \in U_1 \cup U_2 \cup U_3$$

Note: the abstract says $\mathbb{R}^4$ in Theorem 1. We improved this since then.

Examples by pictures:





Background: IP and #IP

Theorem (Lenstra, 1983) In $\mathbb{R}^d$, dimension d fixed, IP $\in \mathsf{P}$:

$$(\text{IP}) \qquad \exists \mathbf{x} \in \mathbb{Z}^d \,:\, A\mathbf{x} \,\leq\, \bar{b}.$$

Theorem (Barvinok, 1993) In $\mathbb{R}^d$, dimension d fixed, #IP $\in \mathsf{FP}$:

$$(\#\text{IP}) \qquad \#\big\{\mathbf{x} \,:\, A\mathbf{x} \,\leq\, \bar{b}\big\}.$$

Note: The system can be *long* here (i.e. has unbounded size)

Proof ideas: 1) Geometry of numbers (flatness theorem), lattice reduction (LLL).

2) Brion–Verge generating function approach, cone subdivisions, combinatorial tools.

From Long to Short

Theorem (Doignon–Bell–Scarf)

Let A be a $n \times d$ real matrix and $\bar{b} \in \mathbb{R}^d$. Suppose

$$\{\mathbf{x} \in \mathbb{Z}^d \,:\, A\mathbf{x} \le \bar{b}\} \;=\; \varnothing.$$

Then there is a subset S of rows of A, $|S| \le 2^d$, s.t.

$$\{\mathbf{x} \in \mathbb{Z}^d \,:\, A_s\mathbf{x} \le \bar{b}_S\} \;=\; \varnothing.$$

Corollary: It suffices to solve IP for short systems (of bounded size n).

Note: One should think of this as the *integral version* of the Helly Theorem.

Indeed, Helly's theorem says: $(d+1)$-intersections are nonempty $\Rightarrow$ all are nonempty.

More background: PIP and #PIP

Theorem (Kannan, 1990) For all dimensions d, k fixed, PIP $\in \mathsf{P}$:

$$(\text{PIP}) \qquad \forall \mathbf{y} \in Q \cap \mathbb{Z}^k \;\; \exists \mathbf{x} \in \mathbb{Z}^d \, : \, A\mathbf{x} + B\mathbf{y} \, \leq \, \bar{b}.$$

Theorem (Barvinok–Woods, 2003) For all dimensions d, k fixed, #PIP $\in \mathsf{FP}$:

$$(\#\text{PIP}) \qquad \#\big\{\mathbf{y} \in Q \cap \mathbb{Z}^k \;\; \exists \mathbf{x} \in \mathbb{Z}^d \, : \, A\mathbf{x} + B\mathbf{y} \, \leq \, \bar{b}\big\}.$$

Translation: These are $\mathrm{E}(Q) \subseteq_? \mathrm{E}(P){\downarrow}$ and $\#\big[\mathrm{E}(Q) \cap \mathrm{E}(P){\downarrow}\big]$.

Proof ideas: More of the same (geometry of numbers, GFs, + ad hoc arguments)

Note: DBS theorem applies, so PIP and #PIP hold for long systems.

What happens for three quantifiers?

Open Problem (Kannan, 1990) Is GIP $\in \mathsf{P}$ for all dimensions d, k, ℓ fixed?

$$\text{(GIP)} \qquad \exists \mathbf{z} \in R \cap \mathbb{Z}^\ell \;\; \forall \mathbf{y} \in Q \cap \mathbb{Z}^k \;\; \exists \mathbf{x} \in \mathbb{Z}^d \; : \; A\mathbf{x} + B\mathbf{y} + C\mathbf{z} \le \bar{b}.$$

Theorem 3 (Nguyen–P.) For dimensions $d \ge 3$, $k, \ell \ge 1$ fixed, GIP is NP-complete. The corresponding counting version #GIP is $\#\mathsf{P}$-complete.

Theorem (Nguyen–P., STOC'17) KPT implies that SHORT-GIP $\in \mathsf{P}$.

KPT = *Kannan's Partition Theorem* (1990) is the Main Lemma
in the proof of Kannan's PIP Theorem.

Note: DBS theorem no longer can be applied in this case (so no contradiction).

Many alternating quantifiers

Theorem (Schöning, 1997) Fix $k \geq 1$. Let $\Psi(\mathbf{x}, \mathbf{y})$ be a Boolean combination of linear inequalities with integer coefficients in the variables $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{Z}^k$ and $\mathbf{y} = (y_1, y_2, y_3) \in \mathbb{Z}^3$. Then deciding the sentence

$$(\star) \quad Q_1 \, x_1 \in \mathbb{Z} \quad \ldots \quad Q_k \, x_k \in \mathbb{Z} \quad Q_{k+1} \, \mathbf{y} \in \mathbb{Z}^3 \quad : \quad \Psi(\mathbf{x}, \mathbf{y})$$

is $\mathbf{\Sigma}_k^{\mathsf{P}}$-complete if $Q_1 = \exists$, and $\mathbf{\Pi}_k^{\mathsf{P}}$-complete if $Q_1 = \forall$. Here $Q_1, \ldots, Q_{k+1} \in \{\forall, \exists\}$ are $(k+1)$ alternating quantifiers.

Theorem (Nguyen–P.) Integer Programming $(\star)$ in a fixed number of variables with $(k+2)$ alternating quantifiers is $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-complete, depending on whether $Q_1 = \exists/\forall$. Here the problem is allowed to contain only a system of inequalities.

Note Tradeoff: *Boolean system* $\longleftrightarrow$ *extra quantifier.*

Proof idea: reduction to GSA

For a vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d) \in \mathbb{Q}^d$ and an integer $k \in \mathbb{Z}$, let

$$\{\{k\boldsymbol{\alpha}\}\} = \max_{1 \le i \le d} \{\{k\alpha_i\}\},$$

where for each rational $\beta \in$ Q, the quantity $\{\beta\}$ is defined as:

$$\{\{\beta\}\} := \min_{n \in \mathbb{Z}} |\beta - n| = \min\{\beta - \lfloor\beta\rfloor, \lceil\beta\rceil - \beta\}.$$

GOOD SIMULTANEOUS APPROXIMATION (GSA)

Input: A rational vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d) \in \mathbb{Q}^d$ and $N \in \mathbb{N}$, $\varepsilon \in \mathbb{Q}$.

Problem: Is an integer $x \in [1, N]$ such that $\{\{x\boldsymbol{\alpha}\}\} \le \varepsilon$?

Theorem (Lagarias, 1985) GSA is NP-complete.

Main ideas: Use continuing fraction for $\varepsilon = p/q$ to study integer points under $y \le \varepsilon x$ line. Note that for p, q Fibonacci numbers the resulting set is both large and has poly-size description. Generalize this observation. Convert the problem into a problem about polytopes by adding auxiliary variables. Proofs of all theorems 1,2 and 3 follow this pattern.

Coming attractions

Theorem (Nguyen–P., FOCS 2017)
Problem Short-GIP is NP–complete.

Note: This is a strong extension of our Theorem 3.
It should be compared to our STOC theorem: KPT $\Rightarrow$ Short-GIP $\in$ P.

Natural Questions: Did we prove P = NP? (No!)

Is STOC Theorem correct? (Yes!)

Is FOCS Theorem correct? (Yes!)

What gives? (We'll explain in Berkeley. See you then!)

Thank You!