Polyhedra with Prescribed Number of Lattice Points and the k-Frobenius Problem

I. Aliev, J. De Loera, Q. Louveaux

Cardiff University UC Davis University of Liege

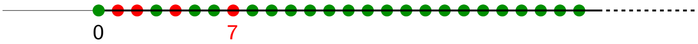
October 8th, 2014

Semigroups and Frobenius numbers

Let $A = (a_1, \ldots, a_n) \in \mathbb{Z}_{>0}^{1\times n}$ with $\gcd(a_1, \ldots, a_n) = 1$. We study

$$\mathrm{Sg}(A) = \{b : b = a_1x_1 + \cdots + a_nx_n \,, x_i \in \mathbb{Z}_{\geq 0}\} \,.$$

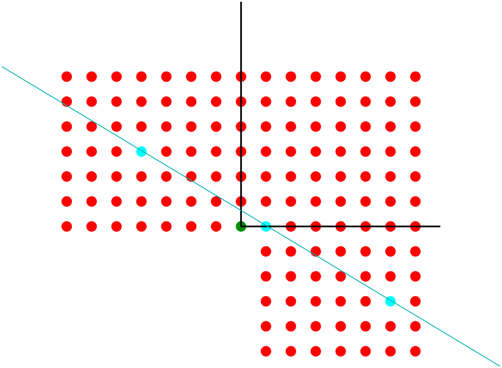
For instance, let $A = (3, 5)$. The elements of $\mathrm{Sg}(A)$ (green dots) and $\mathbb{Z}_{\geq 0} \setminus \mathrm{Sg}(A)$ (red dots):



Deciding whether $b \in \mathrm{Sg}(A)$ is NP-complete problem.

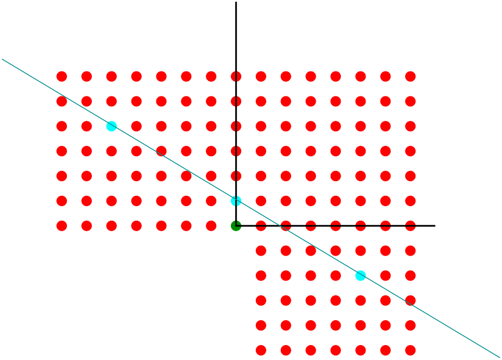
Geometrically, the problem asks whether there is at least one lattice point in the parametric polyhedron $P_A(b) = \{x : Ax = b, x \geq 0\}$.

The geometry of the problem



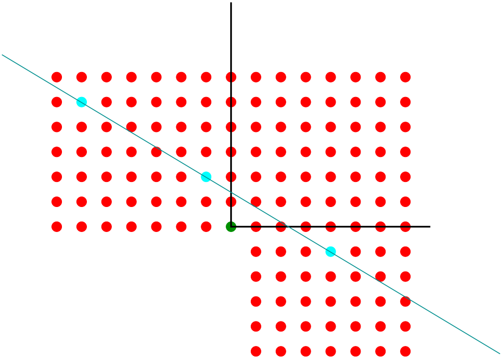
$$3x + 5y = 3$$

The geometry of the problem



$$3x + 5y = 5$$

The geometry of the problem



$$3x + 5y = 7$$

Semigroups and Frobenius numbers

Frobenius problem:

Find the Frobenius number $\mathrm{F}(A)$, that is the largest integer $b \notin \mathrm{Sg}(A)$.

In example above $\mathrm{F}(A) = 7$.

Ramirez Alfonsin (1996): When n is not fixed this is NP-hard problem.

Kannan (1992), Barvinok-Woods (2003): For fixed n Frobenius number can be computed in polynomial time.

A generalization of Frobenius numbers

Beck and Robins (2004): For a positive integer k the k-Frobenius number $\mathrm{F}_k(A)$ is the largest number which cannot be represented in at least k different ways as a non-negative integral combination of the a_i's.

They gave a formula for $n = 2$ for k-Frobenius numbers. For general n and k only bounds (by A., Fukshansky, Henk, etc) are available.

For $\mathrm{Sg}(A) = \{b : b = a_1x_1 + \cdots + a_nx_n \,, x_i \in \mathbb{Z}_{\geq 0}\}$ we can ask:

- For which b are there at least k representations?
- For which b are there exactly k representations?
  (for example there is a unique representation)
- For which b are there at most k representations?

Fundamental problems of k-feasibility

Given an integer matrix $A \in \mathbb{Z}^{d \times n}$ and a vector $b \in \mathbb{Z}^d$, we study the semigroup $\mathrm{Sg}(A) = \{b : b = Ax,\ x \in \mathbb{Z}^n, x \geq 0\}$.

The membership of b in the semigroup $\mathrm{Sg}(A)$ reduces to the challenge, given a vector b, to find whether the linear Diophantine system $IP_A(b)$

$$Ax = b, \quad x \geq 0, \quad x \in \mathbb{Z}^n\,,$$

has a solution or not.

Geometrically, we ask whether there is at least one lattice point in the parametric polyhedron $P_A(b) = \{x : Ax = b, x \geq 0\}$.

Fundamental problems of k-feasibility

For a given integer k there are three natural interesting variations of the classical feasibility problem above that in a natural way measure the number of solutions of $IP_A(b)$:

- Are there at least k distinct solutions for $IP_A(b)$? If yes, we say that the problem is $\geq k$-feasible.
- Are there exactly k distinct solutions for $IP_A(b)$? If yes, we say that the problem is $= k$-feasible.
- Are there less than k distinct solutions for $IP_A(b)$? If yes, we say that the problem is $< k$-feasible.

We call these three problems, the fundamental problems of k-feasibility.

Results

Given the integer $k \geq 1$ one can decompose $\mathrm{Sg}(A)$ taking into account the number of solutions for $IP_A(b)$:

Let $\mathrm{Sg}_{\geq k}(A)$ (respectively $\mathrm{Sg}_{=k}(A)$ and $\mathrm{Sg}_{<k}(A)$) be the set of right-hand side vectors $b \in \mathrm{Sg}(A)$ that make $IP_A(b) \geq k$-feasible (respectively $= k$-feasible, $< k$-feasible).

Theorem

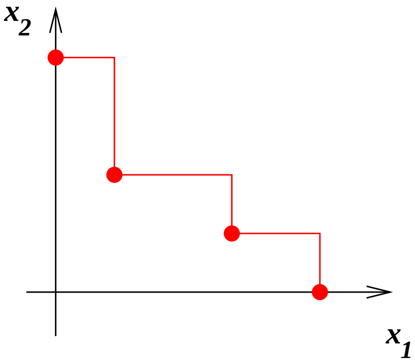
(i) *There exists a monomial ideal $I^k(A) \subset \mathbb{Q}[x_1, \ldots, x_n]$ such that*

$$\mathrm{Sg}_{\geq k}(A) = \{A\lambda : \lambda \in E^k(A)\}\,, \tag{1}$$

where $E^k(A)$ is the set of exponents of monomials in $I^k(A)$.

(ii) *The set $\mathrm{Sg}_{<k}(A)$ can be written as a finite union of translates of the sets $\{A\lambda : \lambda \in S\}$, where S is a coordinate subspace of $\mathbb{Z}^n_{\geq 0}$.*

Results



Corollary

$\mathrm{Sg}_{\geq k}(A)$ is a finite union of translated copies of the semigroup $\mathrm{Sg}(A)$.

Results

Theorem

Let $A \in \mathbb{Z}^{d \times n}$ and let M be a positive integer. Assuming that n and k are fixed, there is a polynomial time algorithm to compute a short sum of rational functions $G(t)$ which represents a formal sum

$$\sum_{b: \geq k-\text{feasible},\ b_i \leq M} t^b.$$

Moreover, from the algebraic formula, one can perform the following tasks in polynomial time:

1. *Count how many such b's are there (finite because M provides a box).*
2. *Extract the lexicographic-smallest such b, $\geq k$-feasible vector.*
3. *Find the $\geq k$-feasible vector b that maximizes $c^T b$.*

Idea of the proof

In 1993 A. Barvinok gave an algorithm for counting the lattice points inside a polyhedron P in polynomial time when the dimension of P is a constant.

The input of the algorithm is the inequality description of P, the output is a polynomial-size formula for the multivariate generating function of all lattice points in P, namely $f(P,x) = \sum_{a \in P \cap \mathbb{Z}^n} x^a$, where x^a is an abbreviation of $x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$.

A long polynomial with many monomials is encoded as a much shorter sum of rational functions of the form

$$f(P,x) \quad = \quad \sum_{i \in I} \pm \frac{x^{u_i}}{(1 - x^{c_{1,i}})(1 - x^{c_{2,i}}) \dots (1 - x^{c_{s,i}})}. \tag{2}$$

Later on Barvinok and Woods developed a way to encode the projections of lattice points of a convex polytope.

Idea of the proof

We construct a polyhedron $Q(A, k, M) \subset \mathbb{R}^{nk}$ such that all its lattice points represent distinct k-tuples of lattice points that are in some parametric polyhedron $P_A(b) = \{x : Ax = b, x \geq 0\}$.

Theorem (Barvinok and Woods 2003)

Assume the dimension n is a fixed constant. Consider a rational polytope $P \subset \mathbb{R}^n$ and a linear map $T : \mathbb{Z}^n \to \mathbb{Z}^d$ such that $T(\mathbb{Z}^n) \subset \mathbb{Z}^d$. There is a polynomial time algorithm which computes a short representation of the generating function $f\left(T(P \cap \mathbb{Z}^n), x\right)$.

We apply a very simple linear map $T(X_1, X_2, \ldots, X_k) = AX_1$. This yields for each k-tuple the corresponding right-hand side vector $b = AX_1$ that has at least k-distinct solutions. The final generating expression will be

$$f = \sum_{b \in \text{projection of } Q(A,k,M) \text{: with at least } k\text{-representations}} t^b.$$

Main corollary

With some technical work we complete the proof and also obtain the following

Corollary

The k-Frobenius number can be computed in polynomial time for fixed k and n.

Thank you!