Affine Semigroups and Parametric Polyhedra with Prescribed Number of Lattice Points

Jesús A. De Loera, UC Davis

Joint work with Iskander Aliev and Quentin Louveaux

IMS-National University of Singapore

December 16, 2013

What is the problem?

Why do you care?

Coin exchange Problems

We wish to know, using USA coins (pennies, nickels, dimes and quarters)

1. **How many ways** are there to give change for b cents?
2. What is **the smallest number of coins necessary** to do so?
3. What is **largest quantity** b which cannot be expressed using these coins?

Holes Gaps and the Frobenius Problem

- Let $a = (a_1, \ldots, a_n)^T \in \mathbb{Z}^n_{>0}$ with $\gcd(a_i) = 1$. The values of coins!
- We study $\mathrm{sg}_a := \{b : b = a_1x_1 + a_2x_2 + \ldots a_nx_n, x_i \in \mathbb{Z}_+\}$
- Deciding whether $b \in \mathrm{sg}_a$ is an NP-complete problem. Counting solutions is #P-complete.
- We say b is a **gap** or a **hole** cannot be represented as a non-negative integral combination of the a_i's.
- *Classical Frobenius problem*: Find the largest number b which is a hole.
- When n is not fixed this is an NP-hard problem Ramirez Alfonsin (1996).
- For fixed n the Frobenius number can be computed in polynomial time Kannan (1992) Barvinok and Woods (2003).

Generalization!!

- **M. Beck and S. Robins (2004):** introduced the $< k$-**Frobenius number**: The largest right-hand number b representable in *no more than* $k - 1$ ways as a non-linear combination of the entries $a_1, a_2, \ldots, a_n$.
- They gave formulas for $n = 2$ of the $< k$-Frobenius number, but for general n and k only bounds on the $< k$-Frobenius number are available (**work by Aliev, Henk, Fushansky, etc**).
- For $\text{sg}_a := \{b : b = a_1x_1 + a_2x_2 + \ldots a_nx_n, x_i \in \mathbb{Z}_+\}$ we can ask
- For which b is there a **unique** way to give change?
- For which b are there **at most k ways** to give change?
- For which b are there **at least k ways** to give change?
- **Observation:** If one knows the solution of the $\geq k$ problem one can also solve the $< k$ problem and vice versa!!

The Question for General Semigroups

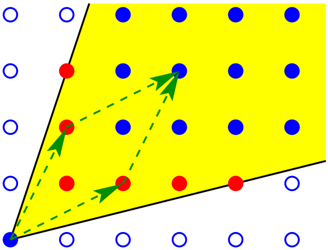
- Let $A \in \mathbb{Z}^{d \times n}$ and $b \in \mathbb{Z}^d$. Tthink of A as fixed and b is a parameter.
- We study **parametric family** of linear Diophantine problems $Ax = b$, $x \geq 0$, $x \in \mathbb{Z}^n$ (*).
- Let $P_A(b) = \{x : x \in \mathbb{R},\ Ax = b,\ x \geq 0\}$ be the convex polyhedron of *real solutions* of Problem (*)
- Let $IP_A(b) = P_A(b) \cap \mathbb{Z}^n$.
- Let $\mathrm{sg}(A)$ be the finitely generated semigroup all non-negative integer combinations of the columns of A,

$$\mathrm{sg}(A) = \{b : Ax = b, \text{for some } x \in \mathbb{Z}^n, x_i \geq 0\}.$$

- Let $\mathrm{cone}(A)$ the *cone generated by* A, i.e., the set of all non-negative real combinations of columns of A.

Finite generation of lattice points in Cones

(Gordan's lemma) Given a matrix A, let cone(A) and sg(A) be the cone and affine semigroup generated by A.
Moreover cone(A) $\cap \mathbb{Z}^d$ is finitely generated in terms of sg(A) in the sense that there exist finitely many $z_1, \ldots, z_u \in \Pi_A \cap \mathbb{Z}^d_+$ such that cone(A) $= \bigcup_{i=1}^{u} z_i + \text{sg}(A)$;
Those elements $z_1, \ldots, z_u$ are the famous *Hilbert bases*



- **Fact** $\mathrm{sg}(A)$ is not always equal to $\mathrm{cone}(A) \cap \mathbb{Z}^d$, but it is always contained in it.
- A **hole** a lattice point that is in $\mathrm{cone}(A)$ but not in $\mathrm{sg}(A)$!
- Surprisingly, the set of holes may be finite or infinite.
- There is a finite description of the holes in terms of finitely many generators.

Theorem (Hemmecke-Takemura-Yoshida)

There exists an algorithm that computes for an integral matrix A a finite explicit representation for the set H of holes of the semigroup Q generated by the columns of A, that is, the algorithm computes (finitely many) vectors $h_i \in \mathbb{Z}^n$ and monoids M_i, each given by a finite set of generators in $\mathbb{Z}^n$, $i \in I$, such that

$$H = \bigcup_{i \in I} \left(\{h_i\} + M_i \right).$$

Example of holes

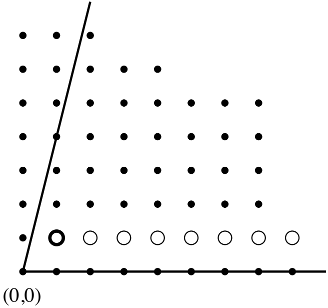
Let

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 3 & 4 \end{pmatrix}$$

The cone has infinitely many holes H, but it is a finitely generated set!!

$$H = \{(1,1)^\intercal + \alpha \cdot (1,0)^\intercal : \alpha \in \mathbb{Z}_+\},$$

where $\mathbb{Z}_+$ denote the set of nonnegative integers.



QUESTIONS!!! *the fundamental problems of k-feasibility*

Let $IP_A(b) = \{x : Ax = b,\ x \geq 0,\ x \in \mathbb{Z}^n\}$ and $k \geq 1$ an integer.

- 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*.
- Let $\text{sg}_{\geq k}(A)$ (respectively $\text{sg}_{=k}(A)$ and $\text{sg}_{<k}(A)$) be the set of right-hand side vectors $b \in \text{cone}(A) \cap \mathbb{Z}^d$ that make $IP_A(b)$ $\geq$ k-feasible (respectively $=$ k-feasible, $<$ k-feasible).
- **Note:** $\text{sg}(A) = \text{sg}_{\geq 1}(A)$, the holes of cone(A) are $\text{sg}_{<1}(A)$.

RESULTS

Structure of $\mathrm{sg}_{\geq k}(A)$ and $\mathrm{sg}_{<k}(A)$: Finite Generation

Theorem

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

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

where $E(A)$ *is the set of exponents of monomials of* $I(A)$.

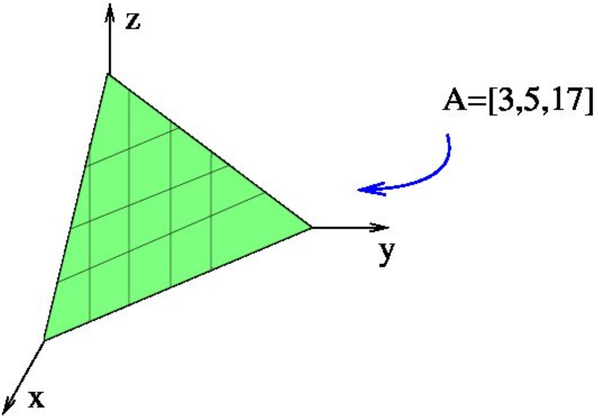
(ii) *We can compute (finitely many) vectors* $h_i \in \mathbb{Z}^n$ *and monoids* M_i*, each given by a finite set of generators in* $\mathbb{Z}^n$*,* $i \in I$*, such that*

$$\mathrm{sg}_{\geq k}(A) = \bigcup_{i \in I} (\{h_i\} + M_i).$$

(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* $\mathbb{Z}^n_{\geq 0}$ *union with the holes.*

Representation of Lattice Points via Generating Functions

Given the parametric convex polytopes,
$P(b) = \{x | Ax = b,\ x \geq 0\}$,
GOAL: COUNT HOW MANY LATTICE POINTS are inside $P(b)$.



$\phi_A(b) = \#\{(x, y, z) | 3x + 5y + 17z = b,\ x \geq 0, y \geq 0, z \geq 0\}$

When $A = [3, 5, 17]$, a short formula for $\phi_A(n)$ would be a **generating function**

$$\sum_{n=0}^{\infty} \phi_A(n) t^n = \frac{1}{(1-t^{17})(1-t^5)(1-t^3)}.$$

From that, one can see that $\phi_A(100) = 25, \phi_A(1110) = 2471$, etc...

Theorem For a knapsack problem $A = [a_1, a_2, \dots, a_M]$, the generating function for $\phi_A(n)$ is

$$\sum_{n=0}^{\infty} \phi_A(n) t^n = \frac{1}{(1-t^{a_1})(1-t^{a_2})\dots(1-t^{a_M})}.$$

We can use it to count solutions for the coin problem!!

Computational Complexity

Theorem

Let $A \in \mathbb{Z}^{d \times n}$. Assuming that n and k are fixed, there is a polynomial time algorithm to compute a short sum of rational function $G(t)$ which efficiently represents the formal sum $\sum_{k-feasible} t^b$.
Here by k-feasible we mean that such precise description is possible for those b which are $=$ k-feasible, $\geq$ k-feasible, or $<$ k-feasible. Moreover, from the algebraic formula, one can perform the following tasks in polynomial time:

1. *Count the number of k-feasible vectors (if finite).*
2. *Extract the lexicographic-smallest b, k-feasible vector.*
3. *Find the k-feasible vector b that maximizes the dot product $c^T b$.*

- In 1993 A. Barvinok gave an algorithm for counting the lattice points in 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 $f(P) = \sum_{a \in P \cap \mathbb{Z}^n} x^a$ 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 many monomials is encoded as a much shorter sum of rational functions of the form

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

- Barvinok and Woods developed a set of manipulation rules for using these short rational functions in **Boolean constructions** on various sets of lattice points.
- They also recover the lattice points inside the image a **linear projection** of a convex polytope.

- **Remark** From the results of Barvinok for fixed n, but not necessarily fixed k, one can decide whether a particular b is k-feasible in polynomial time, but more strongly

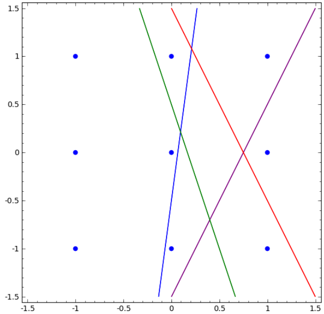
Corollary

Consider the knapsack problem $a^T x = b$ associated with $a = (a_1, \ldots, a_n)^T \in \mathbb{Z}^n_{>0}$ with $\gcd(a_1, \ldots, a_n) = 1$. For a fixed positive integer k and fixed n the k-Frobenius number can be computed in polynomial time.

- Identical results hold for the problem of the form $\{x : Ax \leq b, x \in \mathbb{Z}^n\}$.

A theorem of Doignon (reproved by Bell and Scarf)

- **Theorem** [Doignon 1973] Let A be a $d \times n$ matrix and b a vector of $\mathbb{R}^d$. If the problem $IP_A(\leq, b)$ is infeasible, then there is a subset S of the rows of A of cardinality no more than 2^n, with the property that the smaller integer program $IP_S(\leq, b)$ is also infeasible.



- This theorem has many applications, including Clarkson's probabilistic algorithm for integer linear programming.

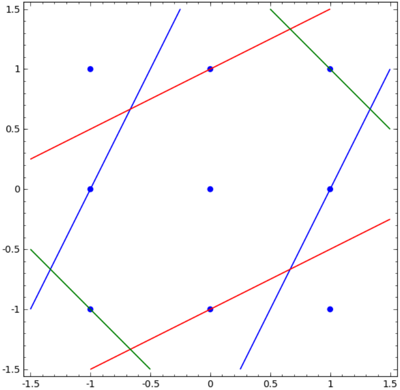
We proved a $=k$-feasibility version of Doignon's theorem:

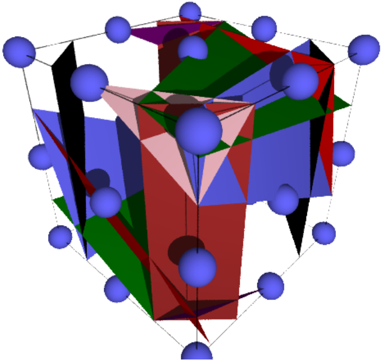
Theorem

Given n, k two non-negative integers there exists a universal constant $c(k,n)$, depending only on k and n, such that for any $d \times n$ integral matrix A, and d-vector b if $P_A(b)\{x : Ax \leq b\}$ has exactly k integral solutions, then there is a subset S of the rows of A of cardinality no more than $c(k,n)$, with the property that the smaller integer program $IP_S(\leq, b)$ has exactly the same k solutions as $P_A(b)$.

Our initial estimation of the constant $c(k,n)$ is $2^n 2^k$ but it appears to be loose!

Better values for dimension $c(2,1), c(3,1)$





Thank you!