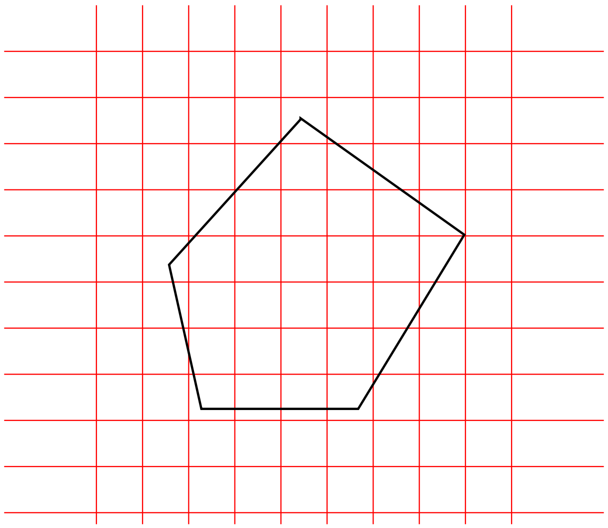
Generating Functions Algorithms for Lattice Point Problems

EPISODE I

Jesús Antonio De Loera
University of California, Davis



Lattice Point Problems

Given a subset X of $\mathbb{R}^d$, there are a number of basic problems about lattice points:

- Decide whether $X \cap \mathbb{Z}^d$ is non empty.
- If X is bounded, count how many lattice points are in X.
- Given a norm, such as the l_∞ or l_p norms, find the shortest lattice vector of X.
- Given a linear functional $c \cdot x$ we wish to optimize it over the lattice points of X, i.e. find the lattice point in X that maximizes (minimizes) cx.

- Given a polynomial $f(x) \in \mathbb{Z}[x_1, \ldots, x_d]$, find $y \in X \cap \mathbb{Z}^d$ which maximizes the value $f(y)$.

- How to generate a lattice point in X uniformly at random?

- Find a Hilbert bases for a polyhedral cone X.

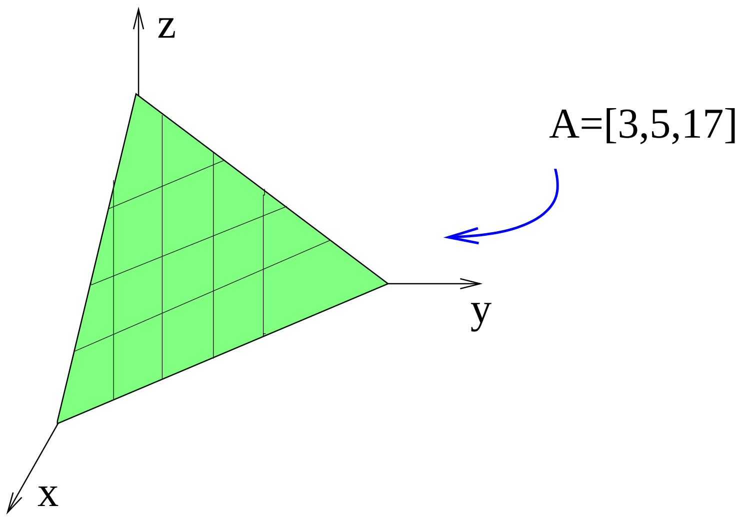
We present a non-traditional algebraic-analytic point of view:

GENERATING FUNCTIONS!!

Consider the problem of counting first...

Given a polytope, $P = \{x | Ax = b,\ x \geq 0\}$,

COUNT HOW MANY LATTICE POINTS are inside P.



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

More general...

Let

$$\phi_A(b) = \#\{x : Ax = b, x \geq 0, \quad x \quad \text{integral}\}.$$

It counts **the number of lattice points inside convex polyhedra with fix matrix** A.

1. (APPLIED MATHEMATICIAN) Fast exact evaluation of $\phi_A(b)$ for fixed values of b. or compute a "short" representation of $\phi_A(b)$.

2. (PURE MATHEMATICIAN) To compute explicit exact formulas in terms of the parameters b_i.

EXAMPLE When $A = [3, 5, 17]$, a short formula for $\phi_A(b)$ 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, you can see that $\phi_A(100) = 25, \phi_A(1110) = 2471$, etc...

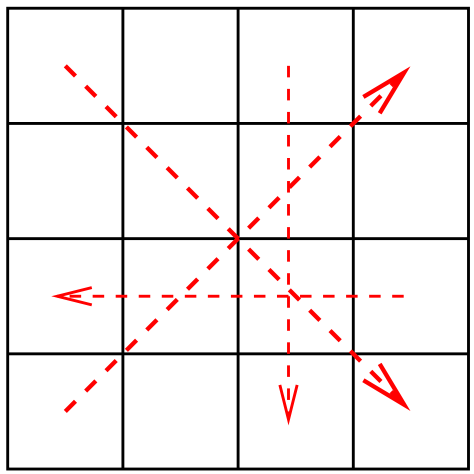
Disclaimers: Whenever I say counting, I mean **EXACT COUNTING**. There is a rich and exciting theory of estimation and approximation, but that is not us!

We really care to get this rational functions **In PRACTICE!!**

MOTIVATION

Combinatorics

Many discrete structures can be counted this way: e.g. matchings on graphs, Hamiltonian cycles, t-designs, linear extensions of posets, **MAGIC squares:**



12	0	5	7
0	12	7	5
7	5	0	12
5	7	12	0

5

QUESTION:**HOW MANY 4×4 magic squares with sum n are there?** Call this number $M_{4\times4}(n)$.

?	?	?	?	24
?	?	?	?	24
?	?	?	?	24
?	?	?	?	24
24	24	24	24	24

The possible tables are non-negative integer solutions of the system of equations: Four equations, one for each row sum and column sum. For example,

$x_{11} + x_{12} + x_{13} + x_{14} = 24,$ **first row**
$x_{13} + x_{23} + x_{33} + x_{43} = 24,$ **third column**

Generating Function Formulas

The problem we have is equivalent to determining a short expression for $\sum_{n=0}^{\infty} M_{4\times 4}(n)t^n$.

Because we are dilating a polytope, as we increase the magic sum n, one can prove the following theorem:

Theorem The number of 4×4 magic squares with magic sum n has a **toric rational generating function**:

$$\frac{t^8 + 4\,t^7 + 18\,t^6 + 36\,t^5 + 50\,t^4 + 36\,t^3 + 18\,t^2 + 4\,t + 1}{(-1+t)^4\,(-1+t^2)^4}$$

Optimization

Let G be a network with n nodes and m arcs, with integer-valued capacity and excess functions $c : arcs(G) \to \mathbf{Z}_{\geq 0}$ and $b : nodes(G) \to \mathbf{Z}$.

A *flow* is a function $f : arcs(G) \to \mathbf{Z}_{\geq 0}$ so that, for any node x, the sum of flow values in outgoing arcs minus the sum of values in incoming arcs equals $b(x)$, and $0 \leq f(i,j) \leq c(i,j)$.

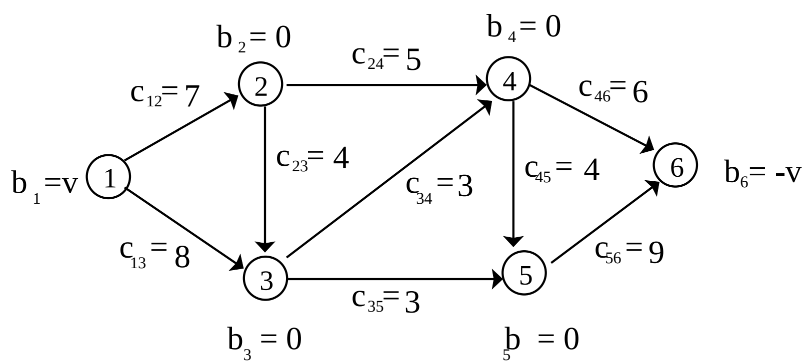


Figure 1: A simple example

How many Max-Flows are there?

From well-known theorems the max-flow value is 11, but how many max-flows are there?

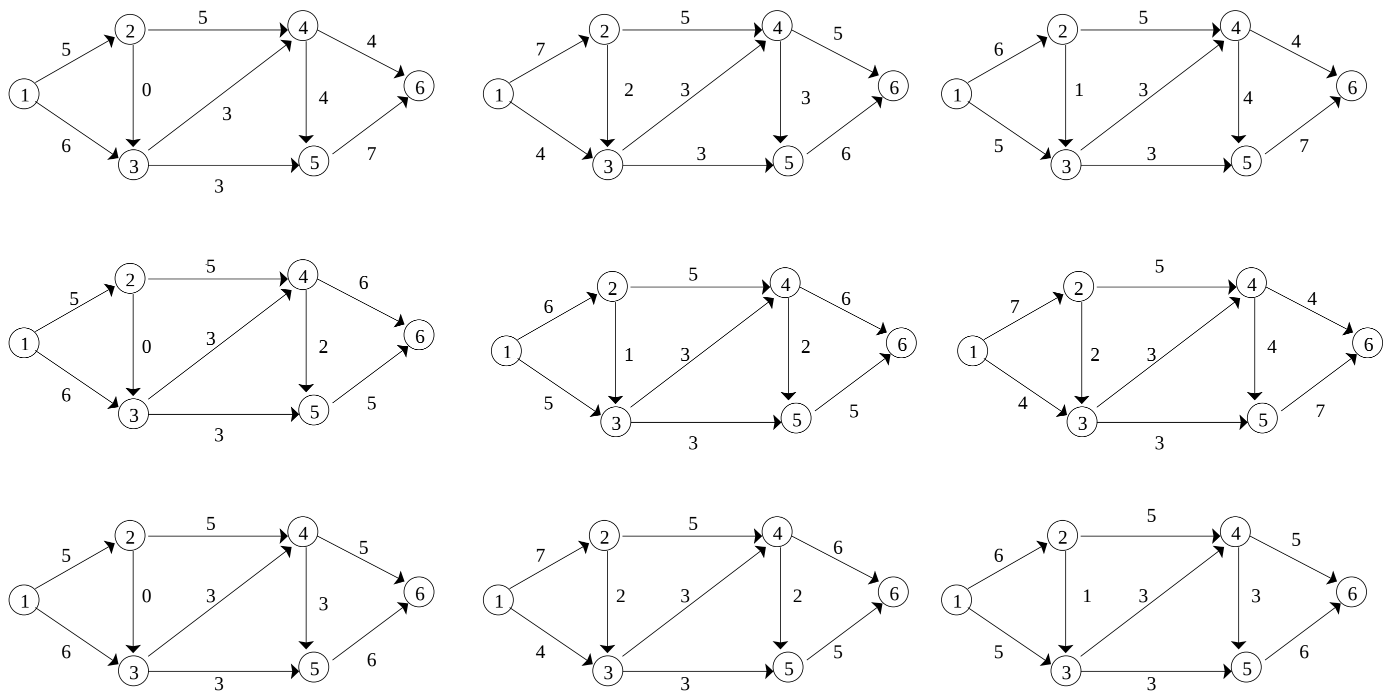


Figure 2: All max flows in the network.

- Solving linear integer programming problems can be reduced to a counting problem.

- There are VERY hard "small" instances, even commercial software (CPLEX) could not solve them! New ideas are necessary. See M. Cornuéjols et al. (1997,1998) and K. Aardal and A.K. Lenstra (1999,2002).

  For example:

$$\{(x, y, z, w, v) \in \mathbb{R}^5_+ | 12223x + 12224y + 36674z + 61119w + 85569v = 89643481\}.$$

Compiler Design

How often is a certain instruction I of the computer code executed?

Example:

```
void proc(int N, int M)
{
int i,j;
for (i=2N-M; i<= 4N+M-min(N,M), i++)
  for(j=0; j<N-2*i; j++)
    I;
}
```

$$\{(i,j) \in \mathbb{Z}^2 | i \geq 2N-M, i \leq 4N+M-min(N,M),\ j \geq 0, j-2i \leq N-1\}$$

Algebra and Number Theory

Number Theory Relations to the theory of partitions, Geometry of Numbers. For example, Frobenius problem: Given relatively prime $a_1, ..., a_n$ what is the highest value of N for which $a_1x_1 + \cdots + a_nx_n = N$, $x_i \geq 0$ is integral INFEASIBLE.

Representation Theory: The calculation of multiplicities and tensor product multiplicities for decomposition of representations into irreducible representations are given by Gelf'and-Tsetlin polytopes, Hive Polytopes (Knutson-Tao), Berenstein-Zelevinsky polytopes, Lattice-Path cones (Littelmann). Kostant's partition function for simple Lie algebras can be seen naturally as counting lattice points.

Commutative Algebra The Hilbert series of monomial algebras and Grobner bases of toric ideals can be seen as problems of counting lattice points in certains polytopes.

EHRHART's THEORY

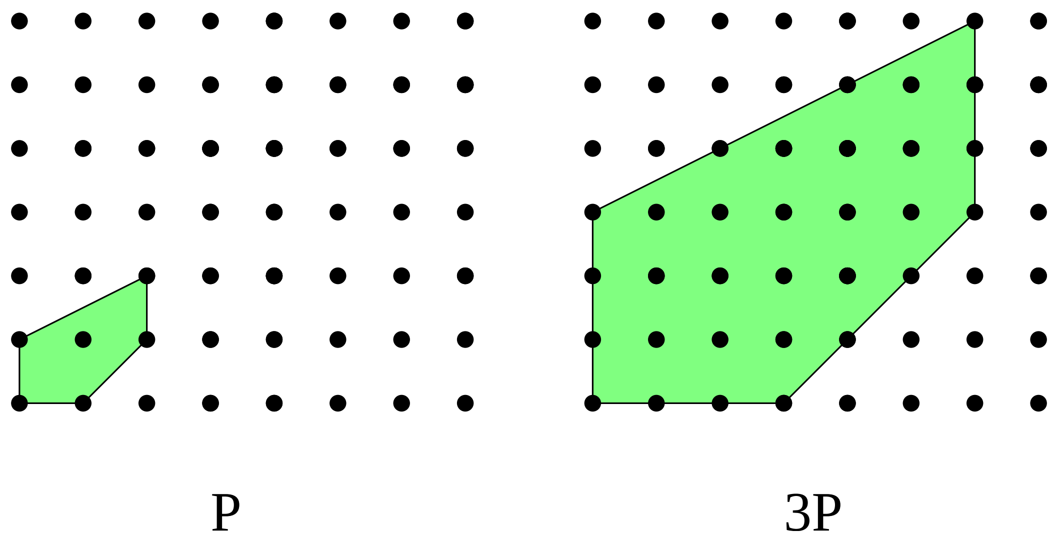
& THE DESCRIPTION OF

$$\phi_A(b)$$

Dilations of Polyhedra

Let P be a convex polytope in $\mathbb{R}^d$. For each integer $n \geq 1$, let

$$nP = \{nq | q \in P\}$$



Ehrhart Counting function

For P a d-polytope, let

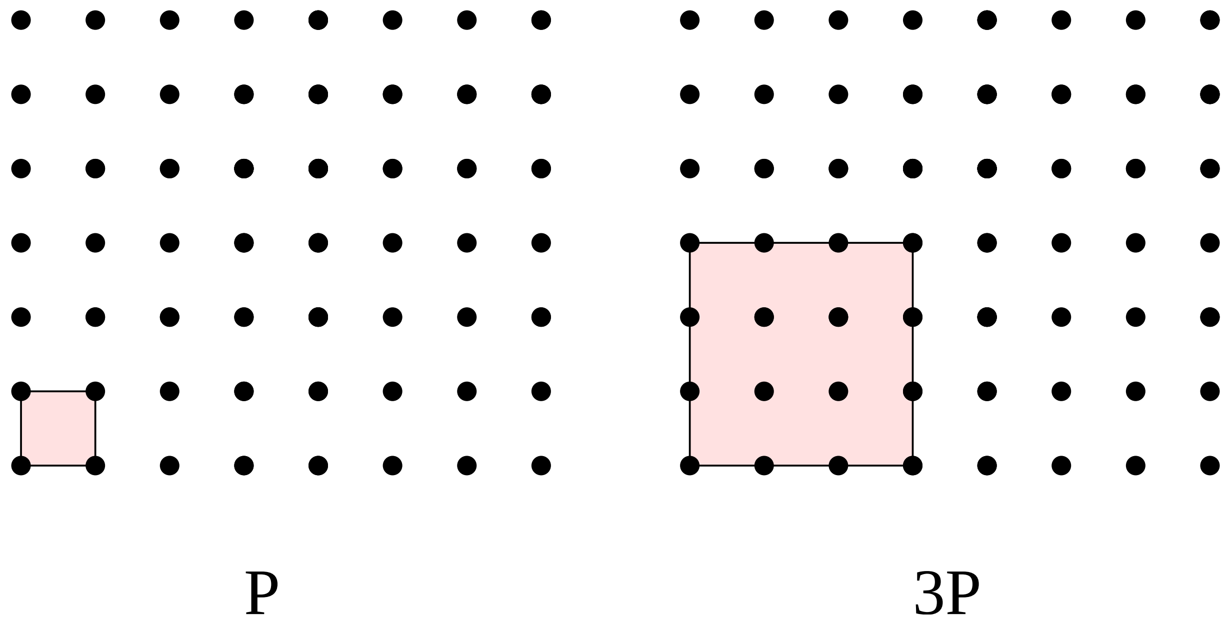
$$i(P, n) = \#(nP \cap \mathbb{Z}^d) = \#\{q \in P \ |nq \in \mathbb{Z}^d\}$$

This is the number of lattice points in the dilation nP.

Similarly if P° denotes the interior of P.

$$i(P^\circ, n) = \#\{q \in P - \partial P| \ nq \in \mathbb{Z}^d\}$$

Example 1: Cubes

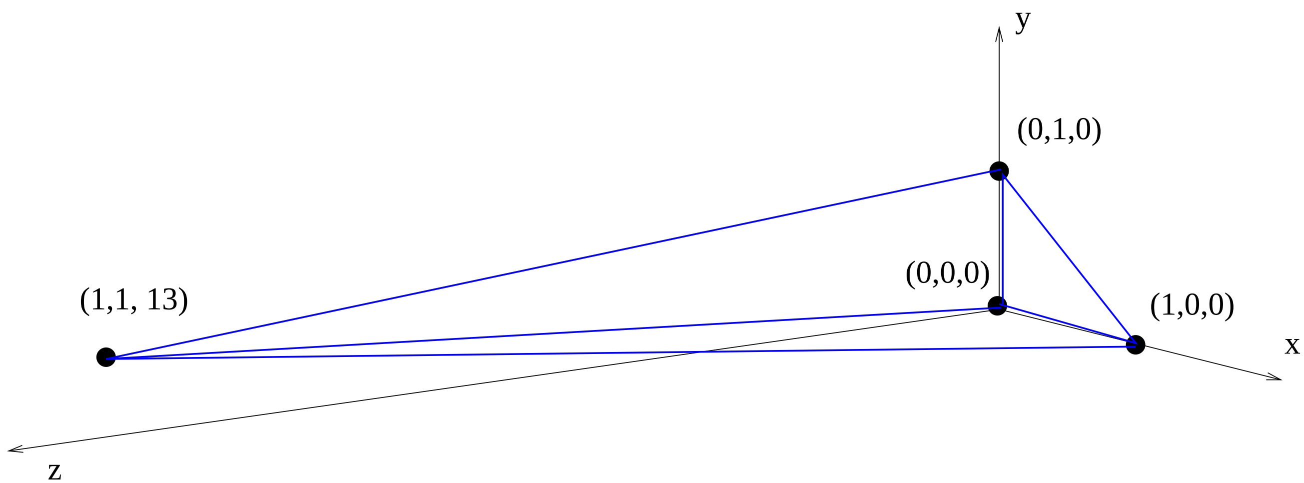


$$i(P,n) = (n+1)^2 \qquad i(P^\circ,n) = (n-1)^2$$

In general for a d-dimensional unit cube we have $i(P,n) = (n+1)^d$

Example 2

Let P be the tetrahedron



Then

$$i(P,n) = \frac{13}{6}n^3 + n^2 - \frac{1}{6}n + 1$$

WARNING: The coefficients of Ehrhart polynomials can be negative!

Example 3: MAGIC SQUARES polytopes

WARNING: The theory for polytopes with fractional vertices is more complicated.

We can consider the convex polytope inside $\mathbb{R}^{n^2}$ of magic $n \times n$ squares of magic sum 1. For example, for $n = 3$ the vertices are

1/3	0	2/3
2/3	1/3	0
0	2/3	1/3

2/3	0	1/3
0	1/3	2/3
1/3	2/3	0

0	2/3	1/3
2/3	1/3	0
1/3	0	2/3

1/3	2/3	0
0	1/3	2/3
2/3	0	1/3

In this case the Ehrhart counting function is not a polynomial, it is a *quasipolynomial!*

$$i(P, s) = \begin{cases} \frac{2}{9}s^2 + \frac{2}{3}s + 1 & \text{if } 3|s, \\ 0 & \text{otherwise,} \end{cases}$$

Ehrhart-Macdonald Theorem

Theorem (E. Ehrhart 1962, I. Macdonald 1963)

Let P be a full dimensional *rational polytope*. Then $i(P, n)$ is univariate quasipolynomial, the Ehrhart quasipolynomial of P, in the dilation variable n and of degree $dim(P)$ whose leading term on each quasipolynomial piece equals the volume of P.

Moreover, when the coordinates of the vertices of P are integers $i(P, n)$ is a polynomial.

BARVINOK's ENCODING

The Generating Function Encoding

Given $K \subset \mathbb{R}^d$ we **WANT** to compute the generating function

$$f(K) = \sum_{\alpha \in K \cap \mathbb{Z}^d} z_1^{\alpha_1} z_2^{\alpha_2} \dots z_n^{\alpha_n}.$$

Think of the lattice points as monomials!!! EXAMPLE: $(7, 4, -3)$ is $z_1^7 z_2^4 z_3^{-3}$.

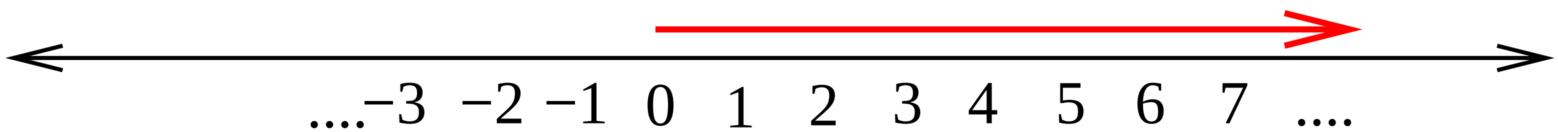
$f(K)$ has inside **all lattice points** of K. But it is too long! In fact, this is an infinite formal power series if K is not bounded, but if K is a polytope it is a (Laurent) polynomial.

We need a SHORT REPRESENTATION!!!

BARVINOK's ANSWER:

When K is a rational convex polyhedron, i.e. $K = \{x \in \mathbb{R}^n | Ax = b,\ Bx \leq b'\}$, where A, B are integral matrices and b, b' are integral vectors, The generating function $f(K)$, and thus ALL the lattice points of the polyhedron K, can be encoded in a "short" sum of rational functions!!!

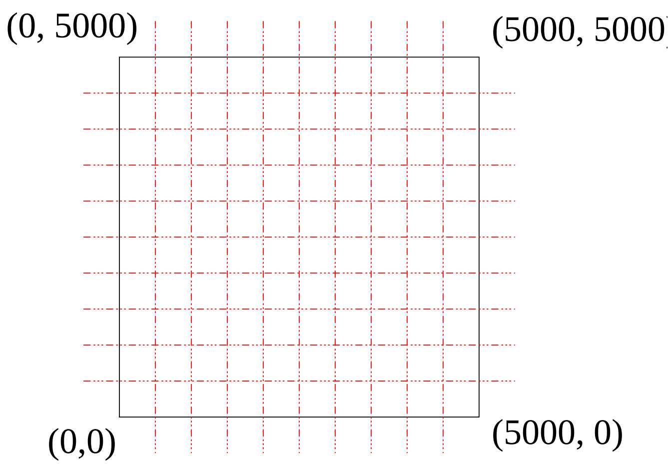
EXAMPLE 1: Suppose my polyhedron is the infinite half-line $P = \{x | x \geq 0\}$



$$f(P) = 1 + z + z^2 + z^3 + \ldots = \frac{1}{1-z}.$$

Example 2

Let P be the square with vertices $V_1 = (0,0)$, $V_2 = (5000,0)$, $V_3 = (5000,5000)$, and $V_4 = (0,5000)$.



The generating function $f(P)$ has over 25,000,000 monomials, $f(P) = 1 + z_1 + z_2 + z_1^1 z_2^2 + z_1^2 z_2 + \cdots + z_1^{5000} z_2^{5000}$, But it has only four rational functions in its Barvinok's encoding.

$$\frac{1}{(1-z_1)(1-z_2)}+\frac{{z_1}^{5000}}{(1-{z_1}^{-1})(1-z_2)}+\frac{{z_2}^{5000}}{(1-{z_2}^{-1})(1-z_1)}+\frac{{z_1}^{5000}{z_2}^{5000}}{(1-{z_1}^{-1})(1-{z_2}^{-1})}$$

Barvinok's Original Algorithm (1993 Barvinok)

Assume the dimension d is fixed. Let P be a rational convex d-dimensional polytope. Then, in polynomial time on the size of the input, we can write the generating function $f(P) = \sum_{\alpha \in P \cap \mathbb{Z}^d} z^\alpha$. as a polynomial-size sum of rational functions of the form:

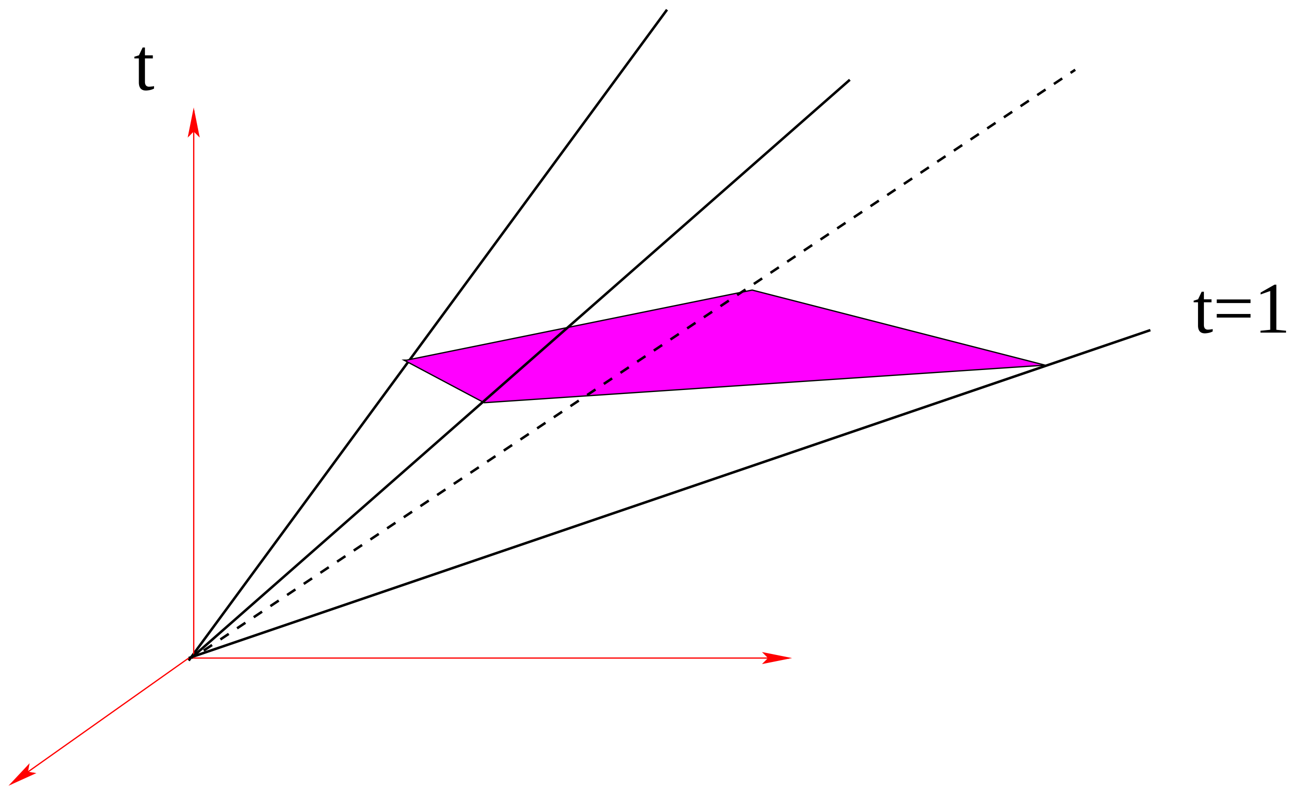
$$\sum_{i \in I} E_i \frac{z^{u_i}}{\prod_{j=1}^{d} (1 - z^{v_{ij}})}, \tag{1}$$

where I is a polynomial-size indexing set, and where $E_i \in \{1, -1\}$ and $u_i, v_{ij} \in \mathbb{Z}^d$ for all i and j.

We present an improved algorithm (2002 De Loera et al.)

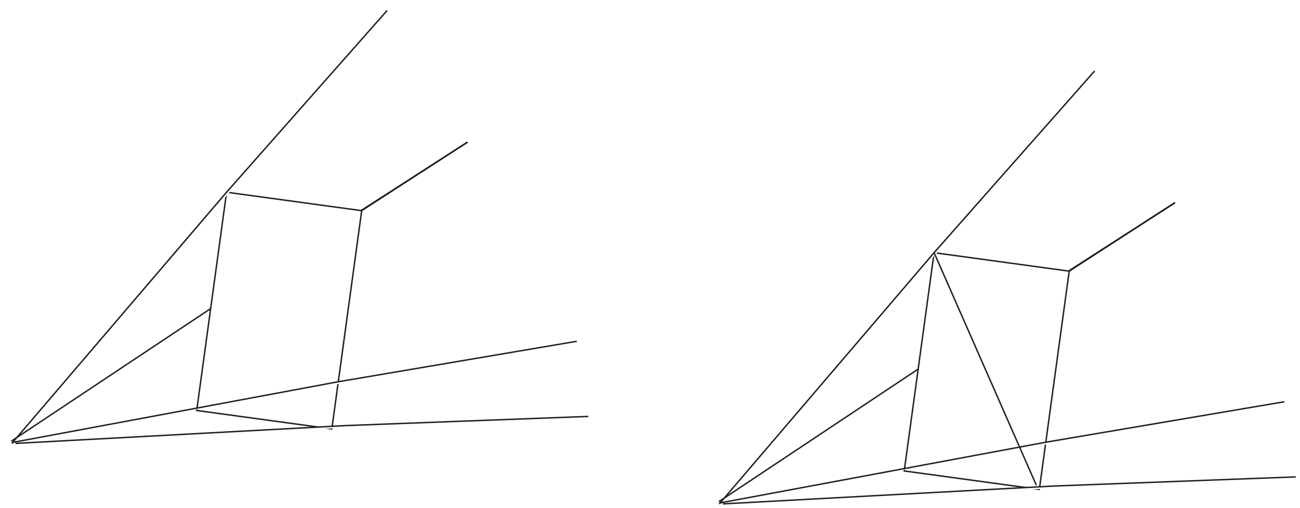
Enough to do it for CONES

Set your polytope P inside the hyperplane $t = 1$. What we want is the generating function of the lattice points in the cone.



Enough to do it for SIMPLE CONES

By the INCLUSION-EXCLUSION principle, we can just add the generating functions of the simplicial pieces!

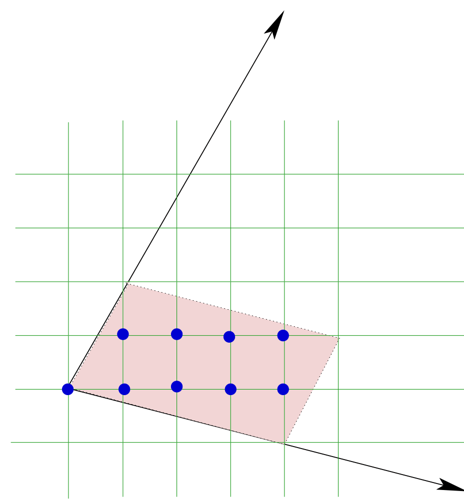


Simple Cones are Easy

For a simple cone $K \subset \mathbb{R}^d$,

$$f(K) = \frac{\sum_{u \in \Pi \cap \mathbb{Z}^d} z^u}{(1 - z^{c_1})(1 - z^{c_2}) \ldots (1 - z^{c_d})}$$

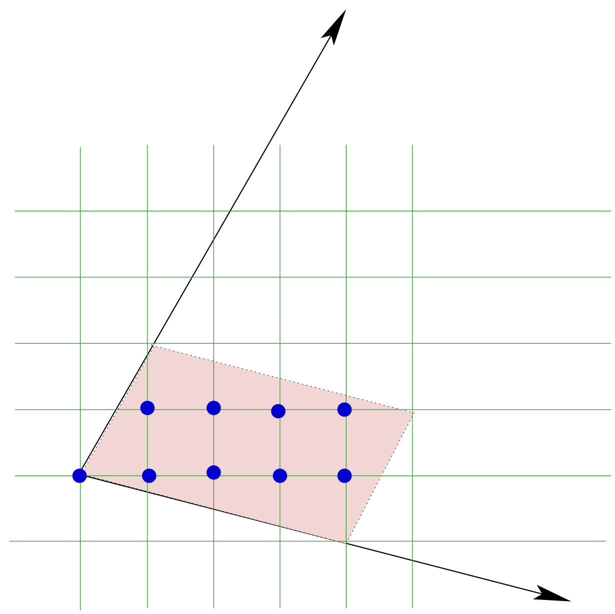
Π is the half open parallelepiped $\{x | x = \alpha_1 c_1 + \cdots + \alpha_d c_d,\ 0 \leq \alpha_i < 1\}$.



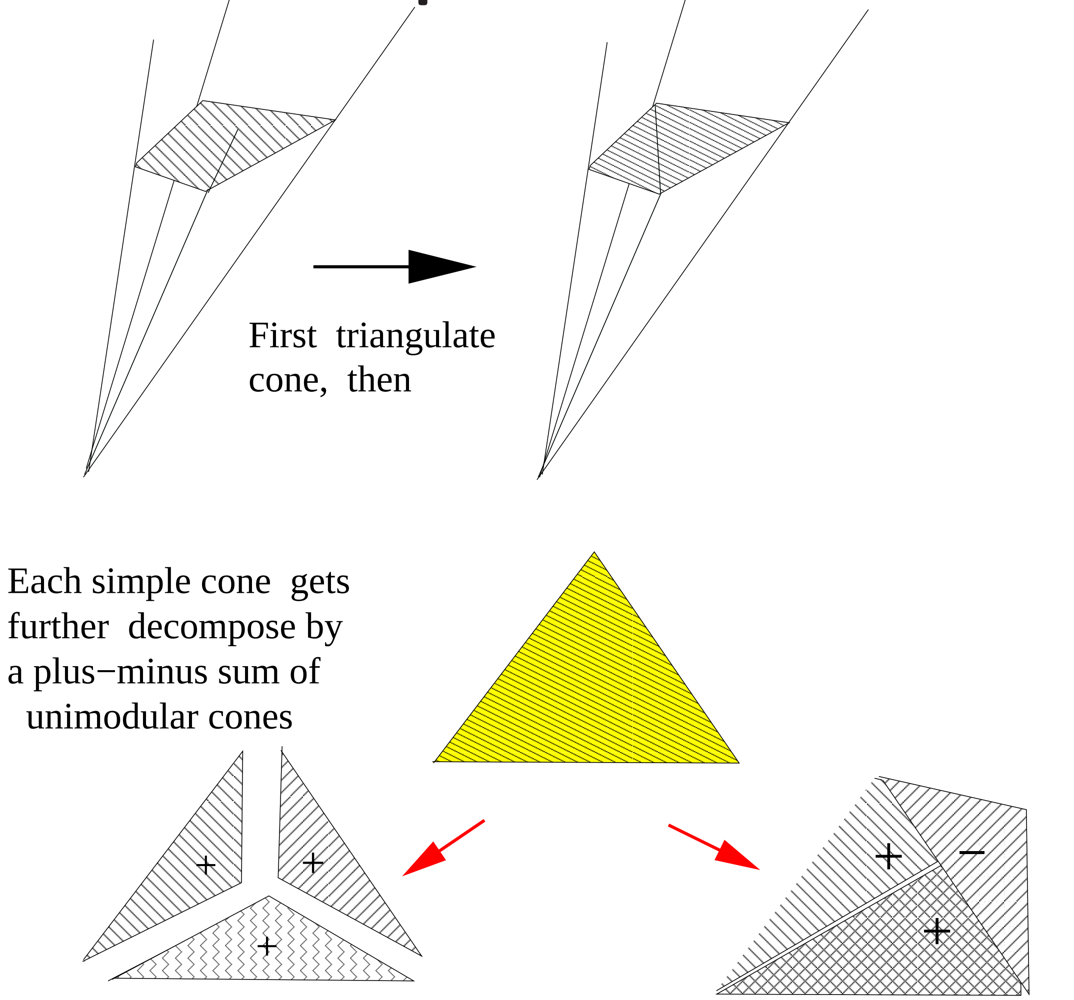
Example

In this case, we have $d = 2$ and $c_1 = (1, 2)$, $c_2 = (4, -1)$. We have:

$$f(K) = \frac{z_1^4 z_2 + z_1^3 z_2 + z_1^2 z_2 + z_1 z_2 + z_1^4 + z_1^3 + z_1^2 + z_1 + 1}{(1 - z_1 z_2^2)(1 - z_1^4 z_2^{-1})}.$$



If a cone K is not simple UNIMODULAR...break it



Barvinok's cone decomposition lemma

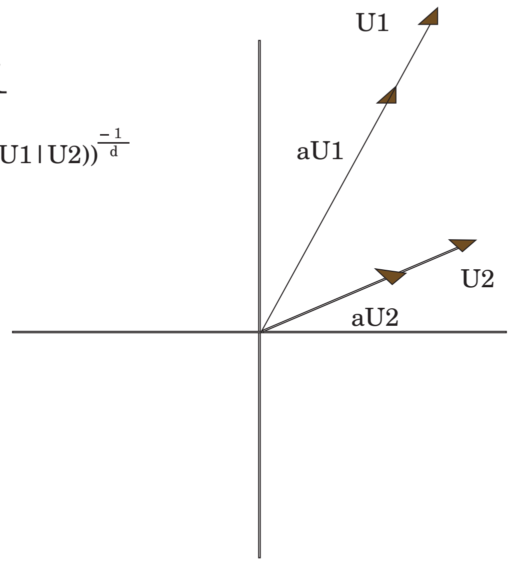
Theorem [Barvinok] Fix the dimension d. Then there exists a polynomial time algorithm which decomposes a rational polyhedral cone $K \subset \Re^d$ into unimodular cones K_i with numbers $\epsilon_i \in \{-1, 1\}$ such that

$$f(K) = \sum_{i \in I} \epsilon_i f(K_i), \ |I| < \infty.$$

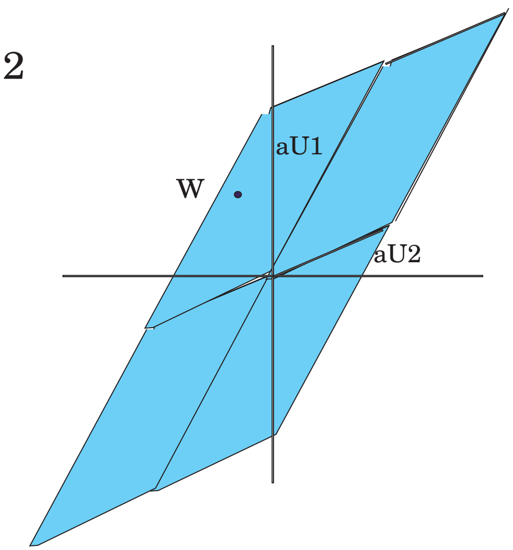
Main idea Triangulation is TOO expensive, allow simplicial cones's rays to be outside the original cone. Rays are short integer vectors inside a convex body, apply Minkowski's theorem!

Step 1

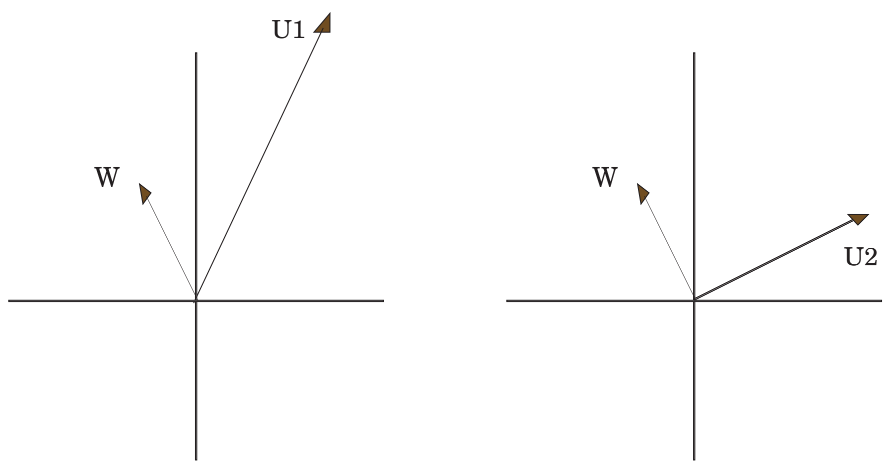
$a = (\det(U1 \mid U2))^{\frac{-1}{d}}$



Step 2



Step 3



SUMMARY of Homogenized Barvinok Algorithm.

Input is a full-dimensional convex rational convex polytope P in $\mathbb{R}^d$ specified by linear inequalities and linear equations.

1. Place the polytope P into the hyperplane defined by $x_{d+1} = 1$ in $\mathbb{R}^{d+1}$. Let K be the $d+1$-dimensional cone over P, that is, $K = cone(\{(p,1) : p \in P\})$.

2. We can triangulate K and reduce everything to simple cones $\sigma_1, \sigma_2, \ldots, \sigma_r$. Apply Barvinok's decomposition of σ_i into unimodular cones. We get a **signed** unimodular cone decomposition of K.

3. Retrieve a signed sum of multivariate rational functions, one per cone, which represents the series $\sum_{a \in K \cap \mathbb{Z}^n} x^a$.

4. If we call the variable $x_{d+1} = t$ then we obtain the expression of the generating function of $\sum_{n=0}^{\infty} \left(\sum_{\alpha \in nP \cap \mathbb{Z}^d} z^{\alpha}\right) \, t^n$,

EXAMPLE

For the triangle σ with vertices $V_0 = (-1,-1)$, $V_1 = (2,-1)$, and $V_2 = (-1,2)$ we have

$$(1-x)^{-1}(1-y)^{-1}\left(1-\frac{t}{xy}\right)^{-1} + \left(1-x^{-1}\right)^{-1}\left(1-\frac{y}{x}\right)^{-1}\left(1-\frac{x^2t}{y}\right)^{-1}$$

$$+\left(1-y^{-1}\right)^{-1}\left(1-\frac{x}{y}\right)^{-1}\left(1-\frac{y^2t}{x}\right)^{-1}$$

Counting Lattice Points FAST!

LEMMA: The number of lattice points in P is the limit when the vector $(x_1, \dots, x_n)$ goes to $(1, 1, \dots, 1)$.

TROUBLE: The vector $(1, 1, \dots, 1)$ is a pole in all the rational functions, a singularity, because the Barvinok rational functions are

$$\frac{z^a}{\prod_{i=1}^{k}(1 - z_i^v)}$$

HOW TO COMPUTE THIS LIMIT????

Shall I expand into monomials???

The singularity gets resolved that way...right?

NO WAY!

Never fully expand the rational

functions into ALL monomials!

USE NUMERICAL COMPLEX ANALYSIS 101

TO EVALUATE THE RATIONAL FUNCTIONS!!

Computation of Residues for rational functions

This reduces to computing a residue at a pole z_0.

If $f(z) = \sum_{k=-m}^{\infty} a_n (z - z_0)^k$, the residue is defined as

$$Res(f(z_0)) = a_{-1}.$$

Given a rational function $f(z) = \frac{p(z)}{q(z)}$, and a pole z_0 we use

THEOREM *Henrici's Algorithm for the residue:* If $p(z), q(z)$ have degree no more than d, then residue at z_0 can be computed in no more than $0(d^2)$ arithmetic operations.

Algorithm

(CASE 1) If z_0 is a simple pole is TRIVIAL, then $Resf(z_0) = \frac{p(z_0)}{q'(z_0)}$.

(CASE 2) Else z_0 is a pole of order $m > 1$,

(A) Write $f(z) = \frac{p(z)}{(z-z_0)^m q_1(z)}$.

(B) Expand p, q_1 in powers of $(z - z_0)$

$p(z) = a_0 + a_1(z - z_0) + a_2(z - z_0)^2 + \ldots$ $q_1(z) = b_0 + b_1(z - z_0) + b_2(z - z_0)^2 + \ldots$

(C) The Taylor expansion of $p(z)/q_1(z)$ at z_0 is $c_0 + c_1(z - z_0) + c_2(z - z_0)^2 + c_3(z - z_0)^3 + \ldots$ where

$c_0 = \frac{a_0}{b_0}$, and $c_k = \frac{1}{b_0}(a_k - b_1 c_{k-1} - b_2 c_{k-2} - \cdots - b_k c_0)$

(D) OUTPUT $Res(f(z_0)) = c_{m-1}$.

Monomial Substitution

Lemma: Let us fix k, the number of binomials in the denominator of a rational function. Given a rational function sum g of the form

$$g(x) = \sum_{i \in I} \alpha_i \frac{x^{u_i}}{\prod_{j=1}^{k} (1 - x^{v_{ij}})},$$

where u_i, v_{ij} are integral d-dimensional vectors, and a monomial map $\psi : \mathbb{C}^n \longrightarrow \mathbb{C}^d$ given by the variable change $x_i \rightarrow z_1^{l_{i1}} z_2^{l_{i2}} \dots z_n^{l_{in}}$ whose image does not lie entirely in the set of poles of $g(x)$, then there exists a polynomial time algorithm which, computes the function $g(\psi(z))$ as a sum of rational functions of the same shape as $g(z)$.

Corollary: Random Generation of Lattice Points

How to pick a random lattice point? Markov chain methods have been around for some time, but they work on some "roundness" assumptions!! Not working well for all polytopes! (work by Dyer, Frieze, Kannan, Lovasz, Simonovits and others)

THEOREM (Barvinok-Pak) Let P be a convex rational polytope in $\mathbb{R}^d$. Then using $O(d^2 \log(size(P)))$ calls to Barvinok's counting algorithm, one can in polynomial time can sample uniformly from set $P \cap \mathbb{Z}^d$.

LattE

- Our goal was to implement and develop algebraic-analytic algorithms. Members: J. De Loera, R. Hemmecke, R. Yoshida, D. Haws, P. Huggins, J. Tauzer.

- First implementation of Barvinok's encoding algorithm. Software implemented in C++.

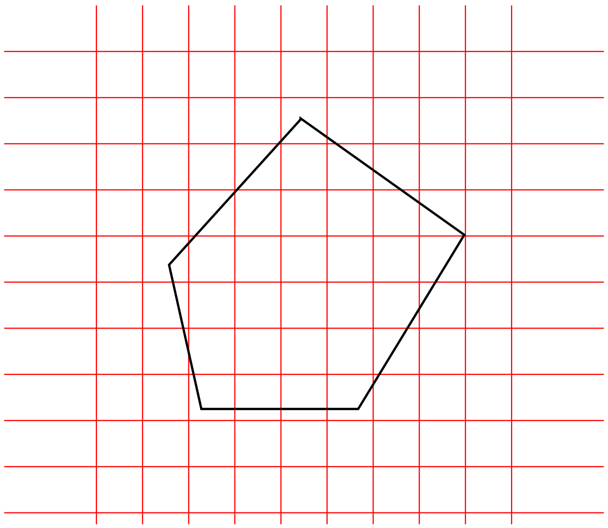
- We used also libraries from **CDD, NTL**.

- We use BOTH geometric computing AND symbolic-algebraic manipulations!!

Integer Polynomial Optimization in Fixed Dimension

EPISODE II

Jesús Antonio De Loera
University of California, Davis



Two Discrete Optimization Problems

Given the set $X = P \cap \mathbb{Z}^d$, we care about:

- Given a linear functional $c \cdot x$ we wish to optimize it over the lattice points of X, i.e. find the lattice point in X that maximizes (minimizes) cx.

- Given a polynomial $f(x) \in \mathbb{Z}[x_1, \ldots, x_d]$, find $y \in X \cap \mathbb{Z}^d$ which maximizes the value $f(y)$.

We take the point of view: GENERATING FUNCTIONS.

Recall: Barvinok's Theorem

Assume the dimension d is fixed. Let P be a rational convex d-dimensional polytope. Then, in polynomial time on the size of the input, we can write the generating function $f(P) = \sum_{\alpha \in P \cap \mathbb{Z}^d} z^\alpha$. as a polynomial-size sum of rational functions of the form:

$$\sum_{i \in I} E_i \frac{z^{u_i}}{\prod_{j=1}^{d} (1 - z^{v_{ij}})}, \tag{2}$$

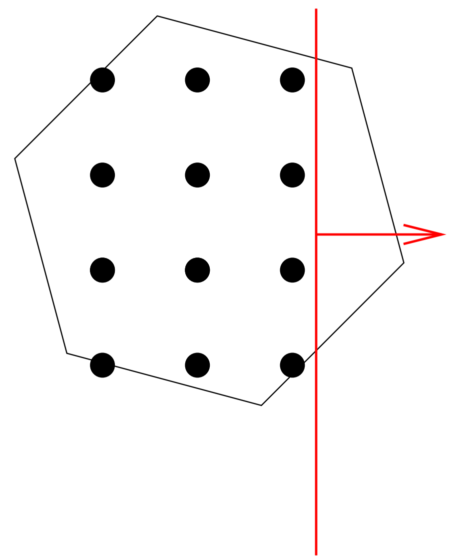
where I is a polynomial-size indexing set, and where $E_i \in \{1, -1\}$ and $u_i, v_{ij} \in \mathbb{Z}^d$ for all i and j.

INTEGER LINEAR PROGRAMS

ALGORITHM: Barvinok + Binary Search

Input: $A \in \mathbb{Z}^{m \times d}$, $b \in \mathbb{Z}^m$, $c \in \mathbb{Z}^d$.

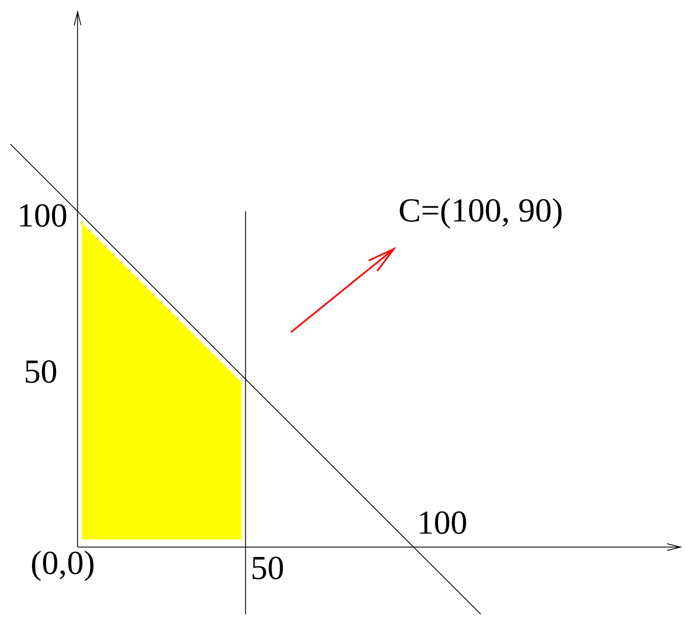
Output: The optimal value of maximize $\{c \cdot x : Ax \leq b, x \geq 0, x \in \mathbb{Z}^d\}$.



For fixed d, this algorithm runs in polynomial time (on the input size) by using the polynomiality of Barvinok's counting algorithm.

Toward More Direct Algorithms:

Barvinok's algorithm computes the function $f(P,z) = \sum_{\alpha \in P \cap \mathbb{Z}^d} z^\alpha$, in the form: $f(P,z) = \sum_{i \in I} \epsilon_i \frac{z^{u_i}}{\prod_{j=1}^{n}(1-z^{v_{ij}})}$.



$$f(P,z) = \frac{1}{(1-z_1)(1-z_2)} + \frac{z_1^{50}}{(1-z_1^{-1})(1-z_2)} + \frac{z_2^{100}}{(1-z_1^{-1})(1-z_2)} + \frac{z_1^{50} z_2^{50}}{(1-z_1^{-1})(1-z_1^{-1}z_2)}.$$

Changing Variables is IMPORTANT!!

$f(P, z) = \sum_{\alpha \in P \cap \mathbb{Z}^d} z^\alpha$, in the form:

$$f(P, z) = \sum_{i \in I} \epsilon_i \frac{z^{u_i}}{\prod_{j=1}^{n} (1 - z^{v_{ij}})}.$$

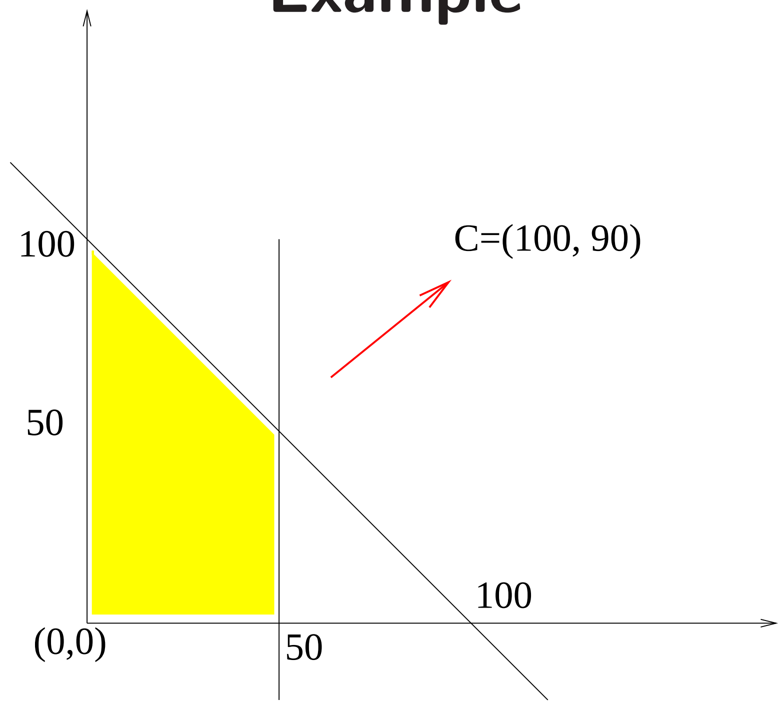
If we make the substitutions $z_i \rightarrow t^{c_i}$, then we have $z^\alpha \rightarrow t^{c \cdot \alpha}$,

$$f(P, z) \rightarrow \sum_{\alpha \in P \cap \mathbb{Z}^d} t^{c \cdot \alpha}$$

$$= t^M + (\text{lower degree terms in } t)$$

M is the optimal value of the integer linear programming problem!

Example



$$f(P,z) = \frac{1}{(1-z_1)(1-z_2)} + \frac{z_1^{50}}{(1-z_1^{-1})(1-z_2)} + \frac{z_2^{100}}{(1-z_1^{-1})(1-z_2)} + \frac{z_1^{50} z_2^{50}}{(1-z_1^{-1})(1-z_1^{-1} z_2)}.$$

Substitute $z_1 \to t^{100}$ and $z_2 \to t^{90}$, then we have t^{9500} + lower degree terms in t.

Monomial Substitution

Lemma: (Barvinok-Woods) Let us fix k, the number of binomials in the denominator of a rational function. Given a rational function sum g of the form

$$g(x) = \sum_{i \in I} \alpha_i \frac{x^{u_i}}{\prod_{j=1}^{k} (1 - x^{v_{ij}})},$$

where u_i, v_{ij} are integral d-dimensional vectors, and a monomial map $\psi : \mathbb{C}^n \longrightarrow \mathbb{C}^d$ given by the variable change $x_i \to z_1^{l_{i1}} z_2^{l_{i2}} \ldots z_n^{l_{in}}$ whose image does not lie entirely in the set of poles of $g(x)$, then there exists a polynomial time algorithm which, computes the function $g(\psi(z))$ as a sum of rational functions of the same shape as $g(z)$.

A Reformulation of Integer Linear Programming:

GOAL: Given $A \in \mathbb{Z}^{m \times d}$, $b \in \mathbb{Z}^m$, $c \in \mathbb{Z}^d$, and assume that number of variables d is fixed. Wish to solve the integer programming problem

maximize $(c \cdot x)$ subject to $x \in \{x | Ax \leq b, x \geq 0,\ x_i \in \mathbb{Z}\ \}$,

In our setting this is

DETECTING THE HIGHEST DEGREE COEFFICIENT OF A POLYNOMIAL!

THE POLYNOMIAL IS GIVEN AS A SUM OF RATIONAL FUNCTIONS.

Several different ways to do this!

Digging Algorithm: Laurent Series Expansion

Input: $A \in \mathbb{Z}^{m\times d}$, $b \in \mathbb{Z}^m$, $c \in \mathbb{Z}^d$.

Output: The optimal value of maximize $\{c\cdot x : Ax \le b, x \ge 0, x \in \mathbb{Z}^d\}$.

(A) Using Barvinok's algorithm and monomial substitution compute the rational function expression

$$\sum_{i\in I} E_i \frac{t^{c\cdot u_i}}{\prod_{j=1}^{d}(1-t^{c\cdot v_{ij}})}. \tag{3}$$

(B) Use the identity

$$\frac{1}{1-t^{c\cdot v_{ij}}} = \frac{-t^{-c\cdot v_{ij}}}{1-t^{-c\cdot v_{ij}}}$$

as necessary to enforce that all v_{ij} in (3) satisfy $c \cdot v_{ij} < 0$. So now the terms of the series are given in decreasing order with respect to the degree of t.

(3) For each of the rational functions in the sum compute a Laurent series expansion of the form

$$E_i \, t^{c \cdot u_i} \prod_{j=1}^{d} (1 + t^{c \cdot v_{ij}} + (t^{c \cdot v_{ij}})^2 + \ldots).$$

multiply out the factors and add the terms, group together those of the same degree in t. Thus we find a term expansion. Proceed in decreasing order with respect to the degree of t.

(4) Continue until a degree n of t is found such that for some the coefficient is non-zero in the expansion. Return n as the optimal value.

Boolean operations on rational functions

Lemma: Let S_1, S_2 be finite subsets of $\mathbb{Z}^n$ and let $f(S_1, x)$ and $f(S_2, x)$ be the corresponding generating functions, represented as short rational functions with at most k binomials in each denominator. Then there exist a polynomial time algorithm, which, given $f(S_i, x)$, computes

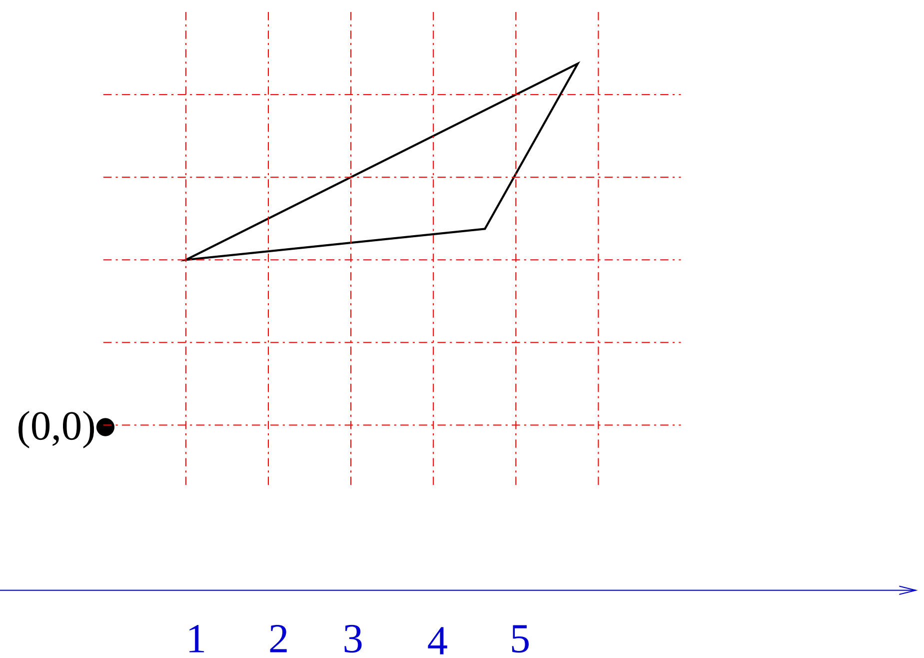
$$f(S_1 \cap S_2, x) \quad = \quad \sum_{i \in I} \gamma_i \frac{x^{u_i}}{(1 - x^{v_{i1}}) \ldots (1 - x^{v_{is}})}$$

with $s \leq 2k$ and γ_i rational numbers, u_i, v_{ij} nonzero integers.

Same with finite unions or complements!

The Projection Lemma

Lemma Consider a rational polytope $P \subset R^n$ and a linear map $T : \mathbb{Z}^n \to \mathbb{Z}^k$. There is a polynomial time algorithm which computes a short representation of the generating function $f\big(T(P \cap \mathbb{Z}^n), x\big)$.



$$z_1 z_2^2 + z_1^3 z_2^3 + z_1^4 z_2^3 + z_1^5 z_2^3 + z_1^5 z_2^4 \quad \text{projects to} \quad z_1 + z_1^3 + z_1^4 + z_1^5.$$

NON-LINEAR INTEGER OPTIMIZATION

Integer Polynomial Optimization

Problem: Let f, g_i are d-variate polynomials with integral coefficients.

$$\text{maximize } f(x_1, \ldots, x_d) \text{ subject to } g_i(x_1, \ldots, x_d) \geq 0, \; x \in \mathbb{Z}^d.$$

Also called **Integer Semialgebraic Optimization.**

Question: **What happens if we assume the number of variables is fixed?**

Positive Notes: problem contains *Integer Linear Programming*, Lenstra's Algorithm guarantees is solvable in polynomial time for fixed dimension. Also, *Integer Semidefinite Programming* runs in polynomial time in fixed dimension by Khachiyan and Porkolab's work.

Negative Notes: continuous polynomial optimization over polytopes, without fixed dimension, is NP-hard and no FPTAS is possible! the max-cut problem can be modeled as minimizing a quadratic form over the cube $[-1, 1]^d$.

The whole picture

Table 1: Computational complexity of polynomial integer problems in fixed dimension.

	Type of objective function				
Type of constraints	linear		convex polynomial		arbitrary polynomial
Linear constraints,	polytime $(*)$	$\Leftarrow$	polytime $(**)$		NP-hard (a)
	$\Uparrow$		$\Uparrow$		$\Downarrow$
Convex semialgebraic constraints,	polytime $(**)$	$\Leftarrow$	polytime $(**)$		NP-hard (c)
Arbitrary polynomial constraints,	undecidable (b)	$\Rightarrow$	undecidable (d)	$\Rightarrow$	undecidable (e)

Integer Polynomial Optimization over a Polytope

Problem: Let f be a d-variate polynomial with integral coefficients. Now the $g_i(x)$ are *linear inequalities.*

$$\boxed{\text{maximize } f(x_1,\ldots,x_d) \text{ subject to } g_i(x_1,\ldots,x_d) \geq 0,\ x \in \mathbb{Z}^d.}$$

Example: Consider this problem from *MINLPLIB* library

$$\begin{aligned} \max \quad & 100\left(\frac{1}{2} + i_2 - \left(\frac{3}{5} + i_1\right)^2\right)^2 + \left(\frac{2}{5} - i_1\right)^2 \\ \text{s.t.} \quad & i_1, i_2 \in [0, 200] \cap \mathbb{Z}. \end{aligned} \tag{4}$$

Its optimal solution is $i_1 = 1$, $i_2 = 2$ with an objective value of 0.72.

Integer Polynomial Optimization over a Polytope

Theorem (D,Hemmecke,Koeppe,Weismantel) Let the number of variables d be fixed. Let $f(x_1, \dots, x_d)$ be a polynomial of maximum total degree D with integer coefficients, and let P be a convex rational polytope defined by linear inequalities in d variables.

(1) We can construct an increasing sequence of lower bounds $\{L_k\}$ and a decreasing sequence of upper bounds $\{U_k\}$ to the optimal value

$$f^* = \text{maximize } f(x_1, x_2, \dots, x_d) \text{ subject to } x \in P \cap \mathbb{Z}^d. \tag{5}$$

The bounds L_k, U_k can be computed in time polynomial in k, the input size of P and f, and the maximum total degree D and they satisfy the inequality $U_k - L_k \le f^* \cdot (\sqrt[k]{|P \cap \mathbb{Z}^d|} - 1)$.

(2) Moreover, if f is positive semidefinite over the polytope (i.e. $f(x) \geq 0$ for all $x \in P$), there exists a fully polynomial-time approximation scheme (FPTAS) for the optimization problem (5).

The construction of the bounds and algorithm uses **Barvinok's rational functions.**

Polynomial Evaluation Lemma

Lemma: Given a Barvinok rational function $f(S)$, representing a finite set of lattice points S, and a polynomial g with integer coefficients we can compute, in time polynomial on the input size a Barvinok rational function for the generating function

$$f(S, g, z) = \sum_{a \in S} g(a) z^a.$$

NOTE: This is *independent* of the degree of g.

Differential Operators give the coefficients:

We can define the basic differential operator associated to $f(x) = x_r$

$$z_r \frac{\partial}{\partial z_r} \cdot \sum_{\alpha \in P \cap \mathbb{Z}^d} z^\alpha = \sum_{\alpha \in P \cap \mathbb{Z}^d} z_r \frac{\partial}{\partial z_r} z^\alpha = \sum_{\alpha \in P \cap \mathbb{Z}^d} \alpha_r z^\alpha.$$

Next if $f(z) = c \cdot z_1^{\beta_1} \cdot \ldots \cdot z_d^{\beta_d}$, then we can compute again a rational function representation of $g_{P,f}(z)$ by repeated application of basic differential operators:

$$c \left(z_1 \frac{\partial}{\partial z_1} \right)^{\beta_1} \cdot \ldots \cdot \left(z_d \frac{\partial}{\partial z_d} \right)^{\beta_d} \cdot g_P(z) = \sum_{\alpha \in P \cap \mathbb{Z}^d} c \cdot \alpha^\beta z^\alpha.$$

VISIT:

www.math.ucdavis.edu/~latte

with lots of nice stuff about lattice points on polytopes...

THANK YOU!