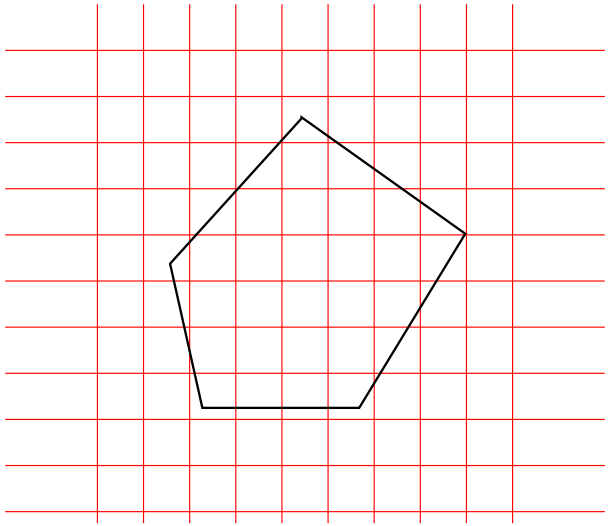
Polyhedra and Lattice Points

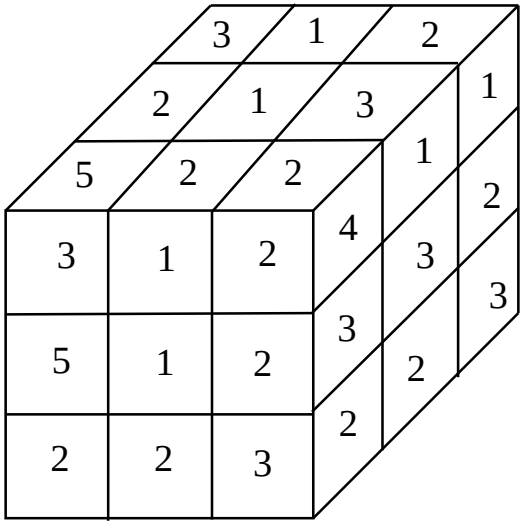
EPISODE I

Jesús Antonio De Loera
University of California, Davis



a Puzzle

Your friend claims to have a $3 \times 3 \times 3$ array of numbers, such that when adding 3 of the numbers along vertical lines or any horizontal row or column you get the numbers shown below:



We have a cubical array of 27 seven numbers and the 27 line sums are fixed. Is your friend telling the truth? How to tell?

Zen Meditation

- The answer will depend on the kind of numbers she is using!! This suggests three interesting variations of linear algebra.

- **Problem A:** Given a rational matrix $A \in \mathbb{Q}^{m \times n}$ and a rational vector $b \in \mathbb{Q}^m$. Is there a solution for the system $Ax = b,\ x \geq 0$, i.e. a solution with all non-negative entries? If yes, find one, otherwise give a proof of infeasibility.

- **Problem B:** Given an integral matrix $A \in \mathbb{Z}^{m \times n}$ and an integral vector $b \in \mathbb{Z}^m$. Is there a solution for the system $Ax = b,\ x \geq 0,\ x \in \mathbb{Z}^n$? i.e. a solution using only non-negative integer entries? If yes, find a solution, otherwise, find a proof of infeasibility.

- Which of the two problems is harder in practice?

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 an algebraic-analytic point of view:

GENERATING FUNCTIONS!!

COUNTING LATTICE POINTS: 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 $z_1^7 z_2^4 z_3^{-3}$.

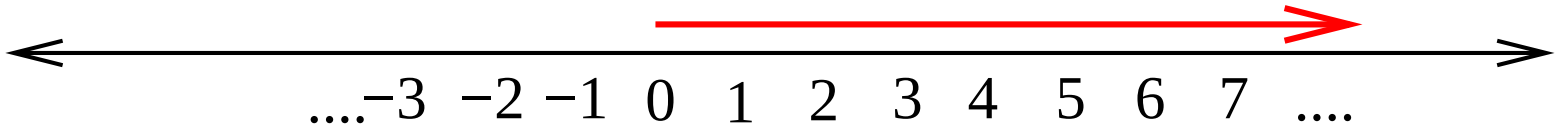
$f(K)$ has inside **all lattice points** of K. But it is too long! In fact, this is an infinite formal power series if K is not bounded, but if K is a polytope it is a (Laurent) polynomial.

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!!!

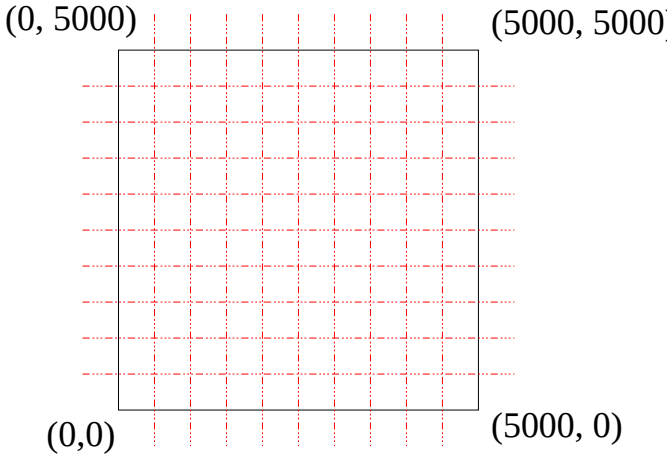
EXAMPLE 1: Suppose my polyhedron is the infinite half-line $P = \{x | x \geq 0\}$



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

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:

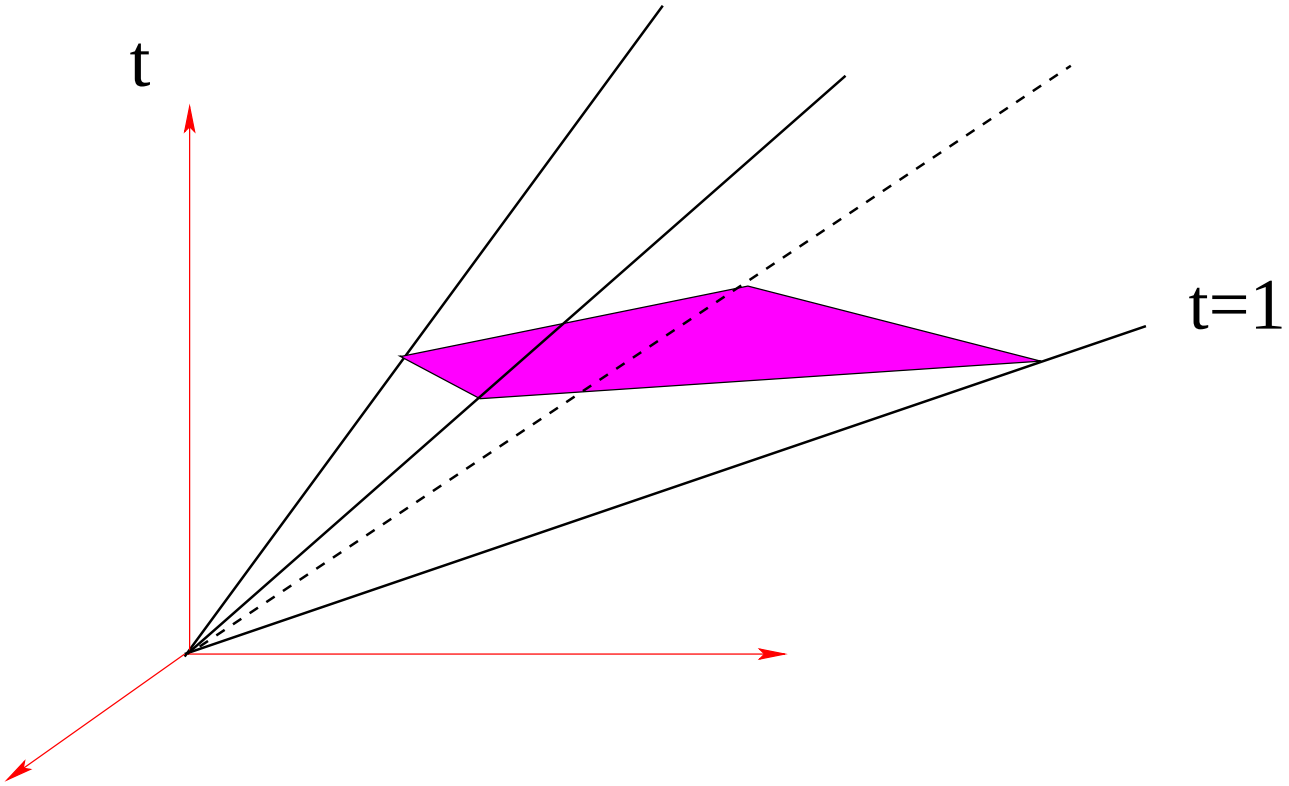
$$\sum_{i \in I} E_i \frac{z^{u_i}}{\prod_{j=1}^{d} (1 - z^{v_{ij}})}, \tag{1}$$

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 a version for cones because to count lattice points for polytopes is...

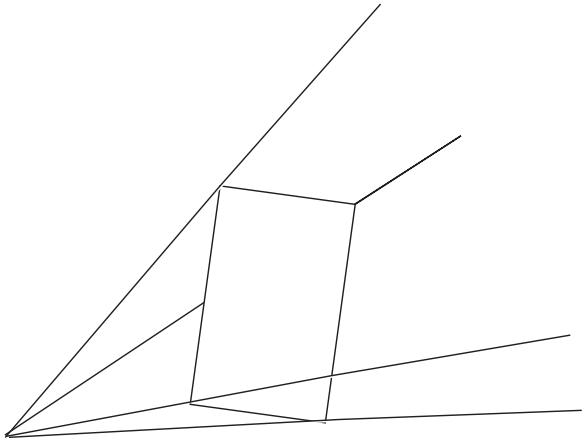
Enough to do it for CONES

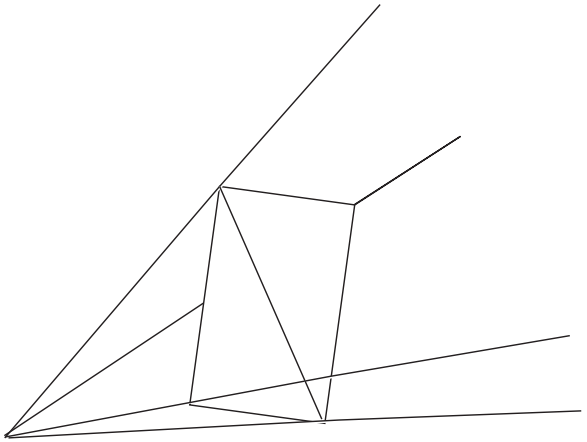
Set your polytope P inside the hyperplane $t = 1$. What we want is the generating function of the lattice points in the cone.



Enough to do it for SIMPLE CONES

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



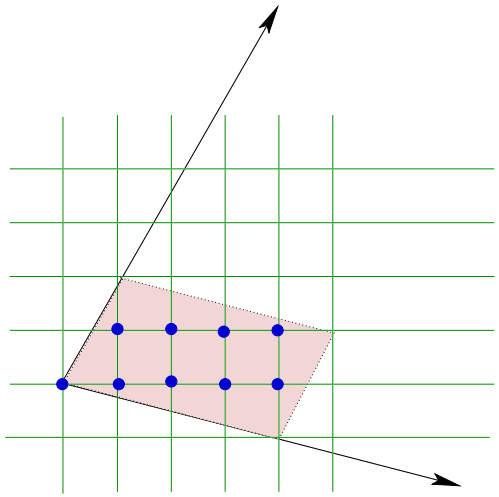


Simple Cones are Easy

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

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

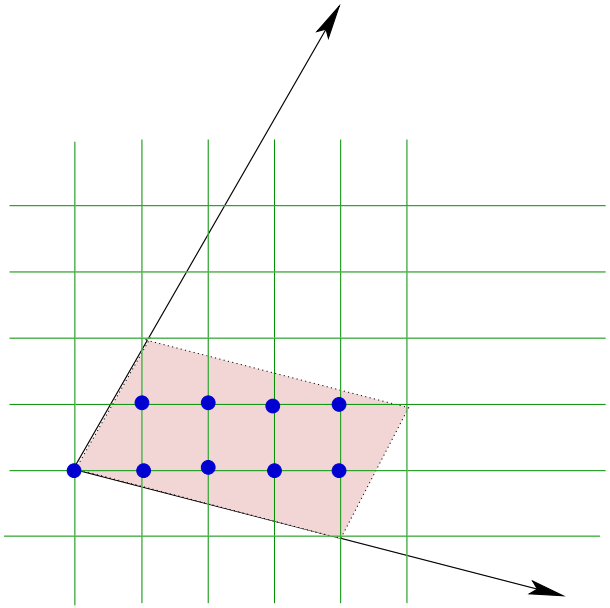
Π is the half open parallelepiped $\{x | x = \alpha_1 c_1 + \dots + \alpha_d c_d,\ 0 \leq \alpha_i < 1\}$.



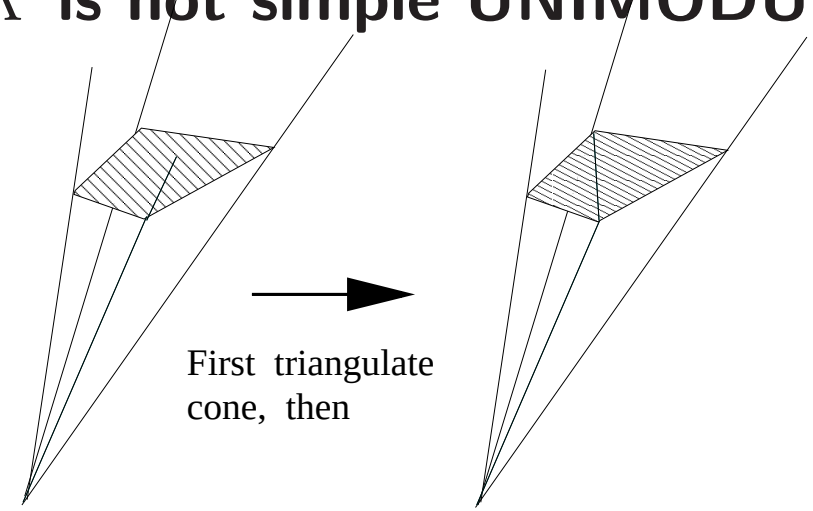
Example

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

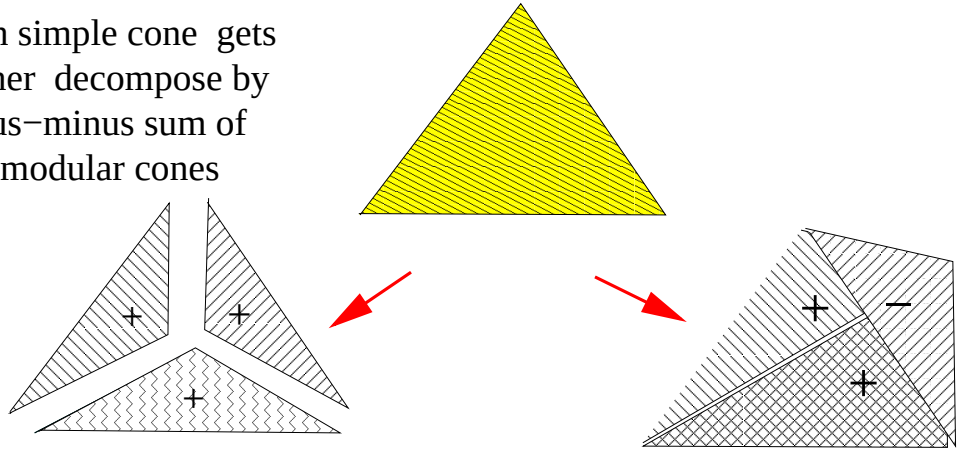
$$f(K) = \frac{z_1^4 z_2 + z_1^3 z_2 + z_1^2 z_2 + z_1 z_2 + z_1^4 + z_1^3 + z_1^2 + z_1 + 1}{(1 - z_1 z_2^2)(1 - z_1^4 z_2^{-1})}.$$



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



Each simple cone gets
further decompose by
a plus−minus sum of
unimodular cones



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

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

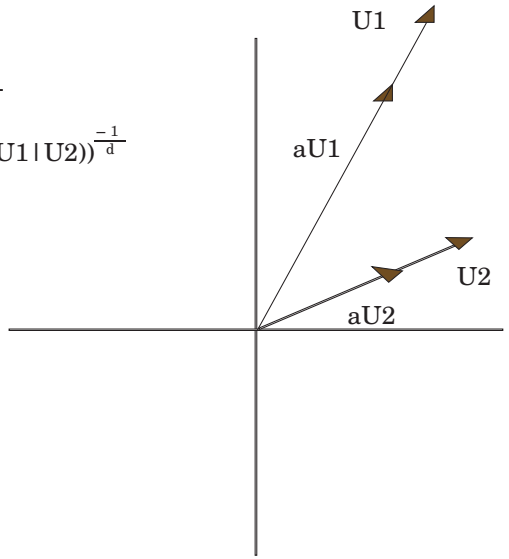
Main idea Triangulation is TOO expensive, allow simplicial cones's rays to be outside the original cone. Rays are short integer vectors inside a convex body, apply Minkowski's theorem!

Minkowski's Theorem

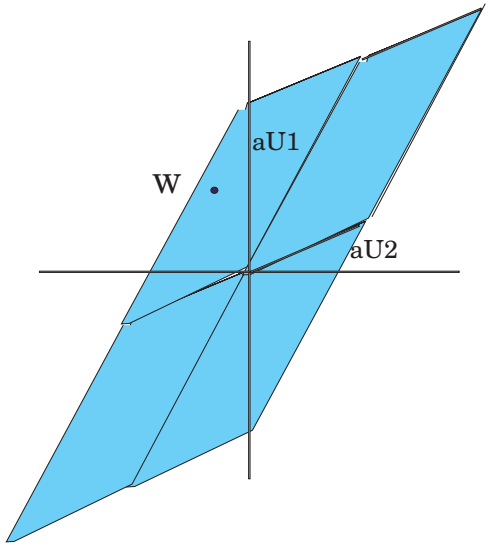
First Minkowski's Theorem: Let $\Lambda \subset \mathbb{R}^n$ be a lattice, $K \subset \mathbb{R}^n$ be a convex set compact centrally symmetric set (i.e., $x \in K \Rightarrow -x \in K$) with $vol(K) \geq 2^n \det(\Lambda)$. Then K must contain a non-zero lattice point $\mathbf{u}$.

Step 1

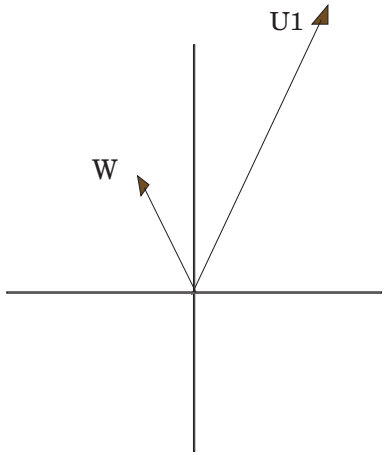
$a = (\det(U1 \mid U2))^{\frac{-1}{d}}$

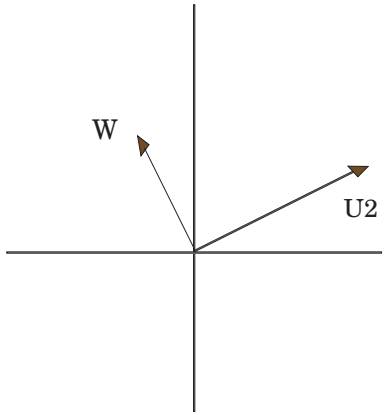


Step 2



Step 3





SUMMARY of Barvinok Algorithm for cones

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

1. We triangulate K and reduce everything to simple cones $\sigma_1, \sigma_2, \ldots, \sigma_r$. Polynomially many because of FIXED dimension.

2. 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 $\sum_{a \in K \cap \mathbb{Z}^n} x^a$.

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 $(x_1, \ldots, x_n)$ goes to $(1, 1, \ldots, 1)$.

TROUBLE: The vector $(1, 1, \ldots, 1)$ 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 $(z - z_0)$

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

(C) The Taylor expansion of $p(z)/q_1(z)$ at z_0 is $c_0 + c_1(z - z_0) + c_2(z - z_0)^2 + c_3(z - z_0)^3 +$ ... 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 $P \cap \mathbb{Z}^d$.

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

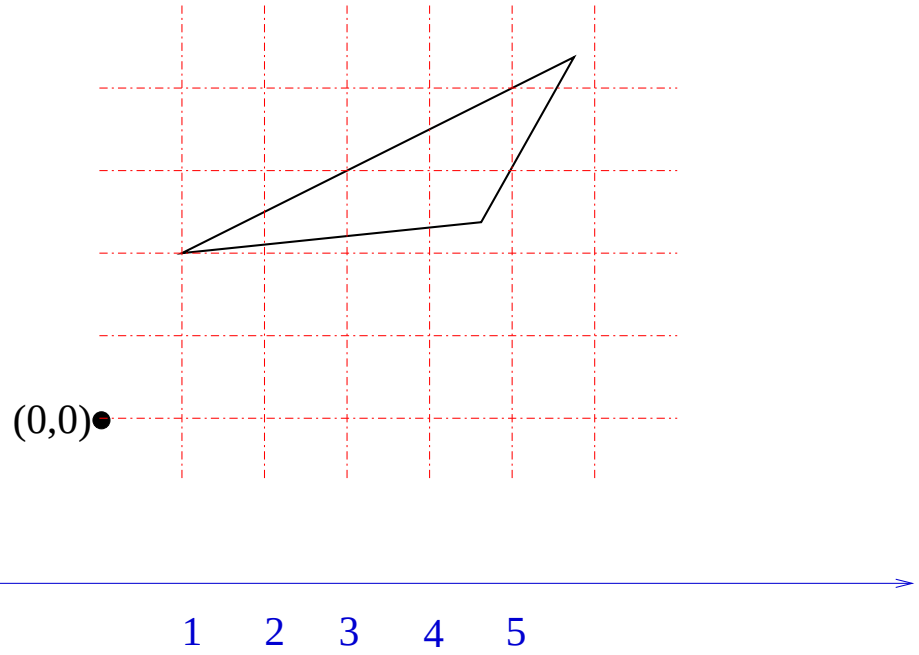
$$f(S_1 \cap S_2, x) \quad = \quad \sum_{i \in I} \gamma_i \frac{x^{u_i}}{(1 - x^{v_{i1}}) \dots (1 - x^{v_{is}})}$$

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 $f\big(T(P \cap \mathbb{Z}^n), x\big)$.



$z_1 z_2^2 + z_1^3 z_2^3 + z_1^4 z_2^3 + z_1^5 z_2^3 + z_1^5 z_2^4$ projects to $z_1 + z_1^3 + z_1^4 + z_1^5$.

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 $f(x) = x_r$

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

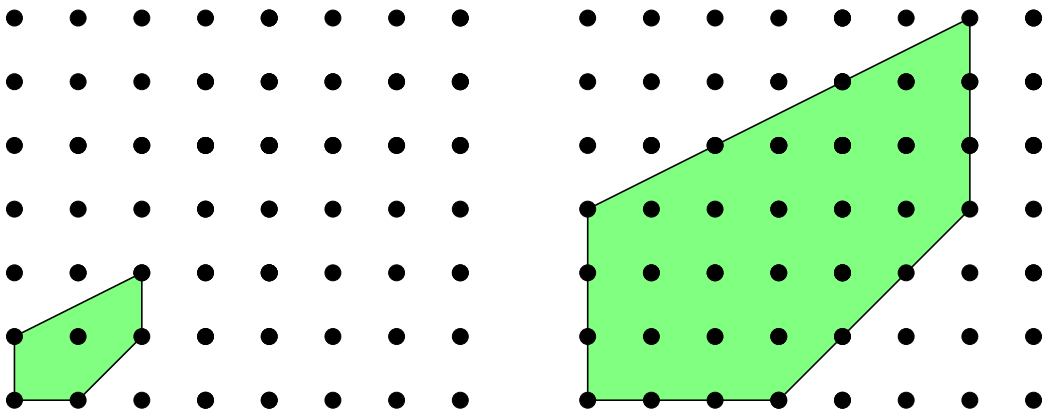
Next if $f(z) = c \cdot z_1^{\beta_1} \cdot \ldots \cdot z_d^{\beta_d}$, then we can compute again a rational function representation of $g_{P,f}(z)$ by repeated application of basic differential operators:

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

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

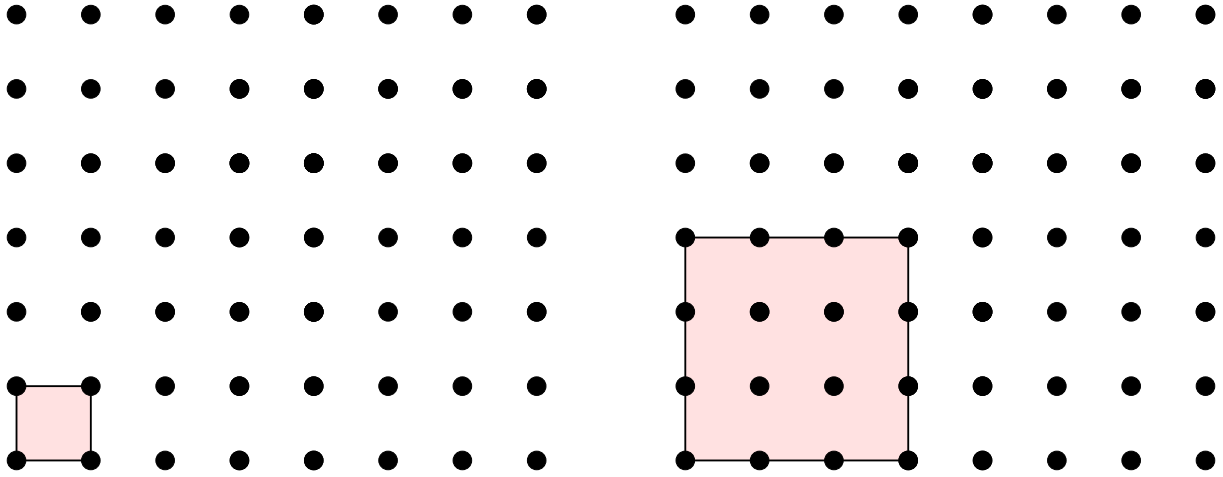
$$i(P,n) = \#(nP \cap \mathbb{Z}^d) = \#\{q \in P \mid nq \in \mathbb{Z}^d\}$$

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

Similarly if P° denotes the interior of P.

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

Example 1: Cubes



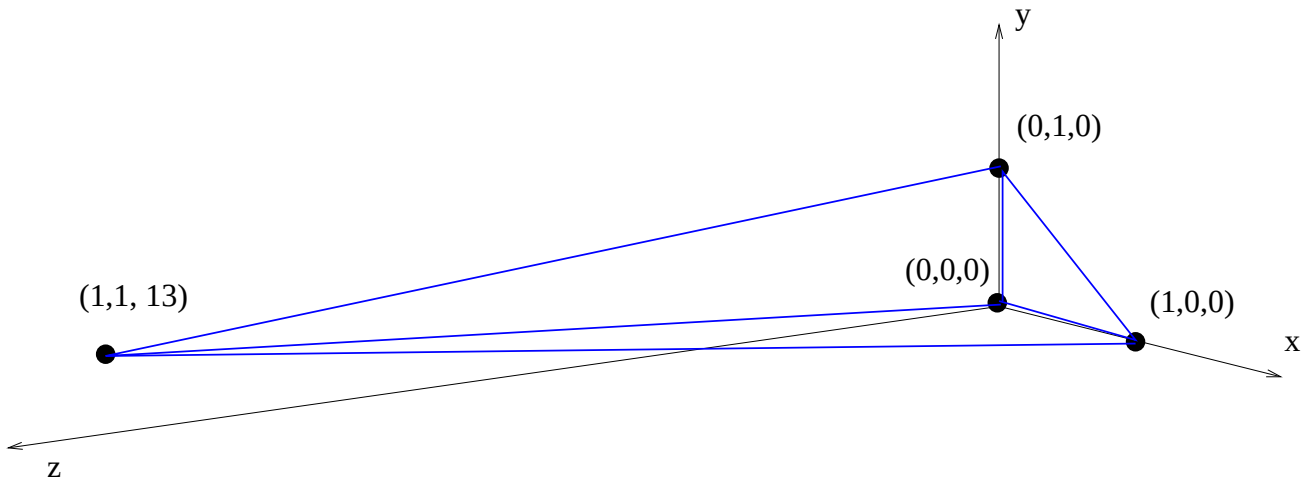
P 3P

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

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.

A Generalized version

Theorem Let P be a convex rational d-polytope. Let f be any homogeneous polynomial function in $\mathbb{Z}[x_1, x_2, \ldots, x_d]$ of degree D. Then the counting function

$$i_{P,f}(n) = \sum_{\alpha \in nP \cap \mathbb{Z}^d,} f(\alpha)$$

is a quasipolynomial of degree $d + D$ with rational coefficients on the variable n. Its leading coefficient equals the integral of f over the polytope P.

Example

Suppose the polytope P is the unit square $[0,1]^2$, and that $f(x,y)$ is of the form $x^k y^k$. Then

$$\begin{aligned}
i(P,n) =& n^2 + 2n + 1 = (n+1)^2 \\
i(P,xy,n) =& 1/4\, n^4 + 1/2\, n^3 + 1/4\, n^2 \\
i(P,x^2y^2,n) =& 1/9\, n^6 + 1/3\, n^5 + \frac{13}{36}\, n^4 + 1/6\, n^3 + 1/36\, n^2 \\
i(P,x^3y^3,n) =& 1/16\, n^8 + 1/4\, n^7 + 3/8\, n^6 + 1/4\, n^5 + 1/16\, n^4
\end{aligned}$$

LattE

- Our goal was to implement and develop algebraic-analytic algorithms. Current Members: JDL, M. Köppe, B. Dutra.
- 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!!

VISIT:
www.math.ucdavis.edu/~latte

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

THANK YOU!