The Many Aspects of Counting Lattice Points in Polyhedra

Jesús Antonio De Loera
University of California, Davis

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

Le Menu

THE PROBLEM and WHY YOU SHOULD LISTEN!

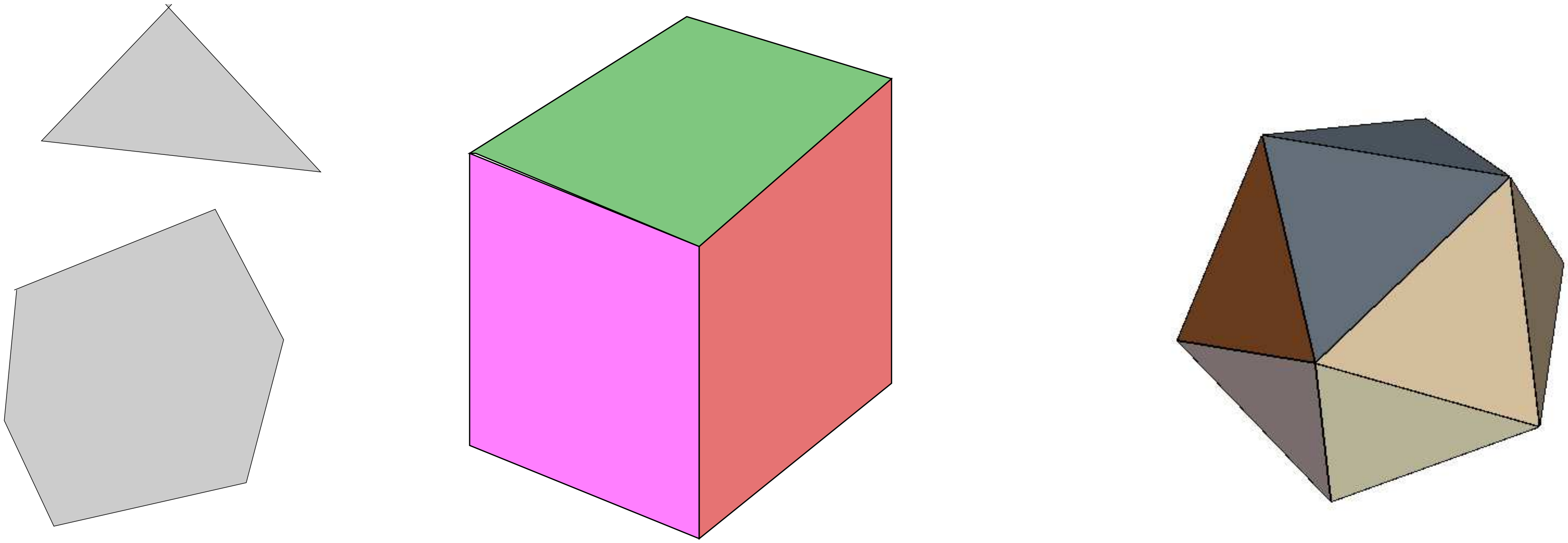
EHRHART's THEORY & THE MAIN STRUCTURE THEOREM

GENERALIZATIONS AND YOUR CREDIT CARD!

THE PROBLEM

The MAIN ACTORS OF THIS PLAY ARE...

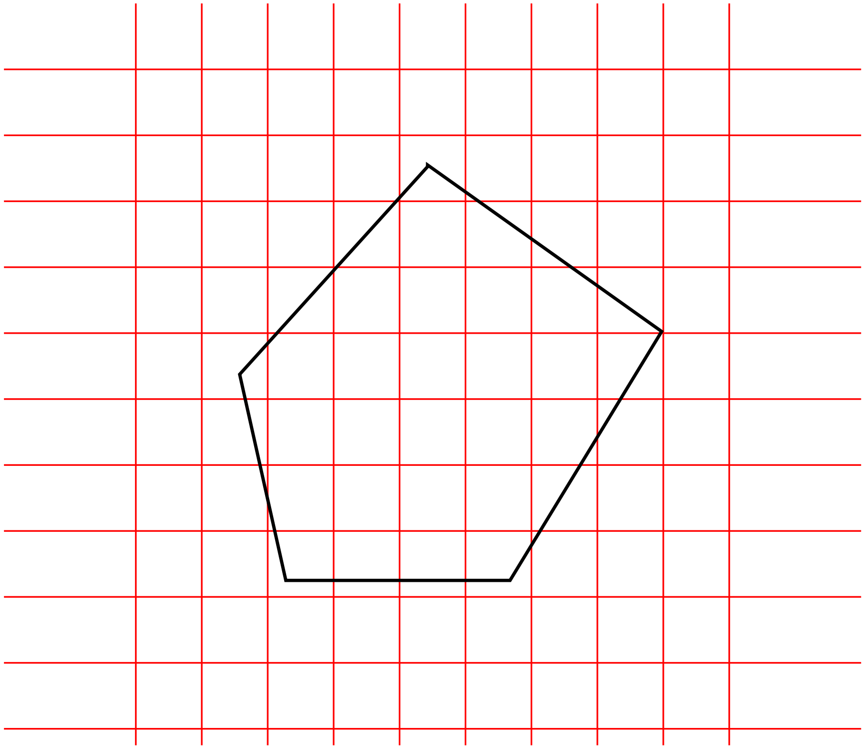
POLYHEDRA



Polyhedra represented by sets of the form $\{x|Ax = b,\ x \geq 0\}$, for suitable integral matrix A, and vector b.

...AND THE INTEGER LATTICE

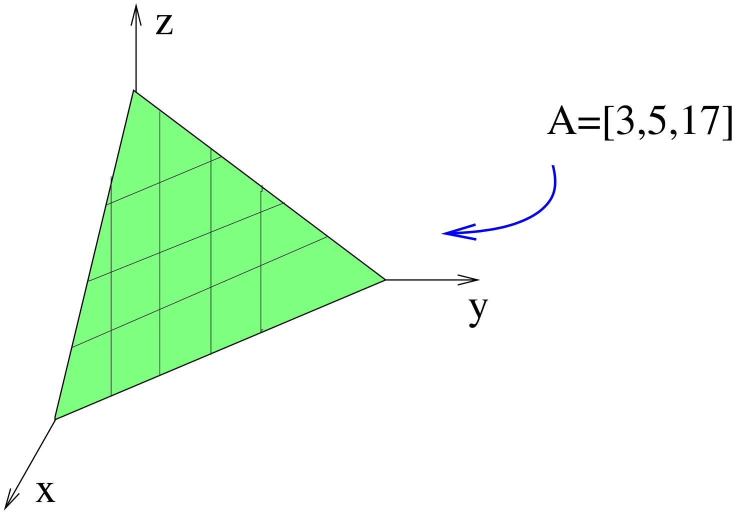
$$\mathbb{Z}^n = \{(x_1, x_2, \ldots, x_n) | x_i \text{ integer}\}$$



THE PROBLEM!!!

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...

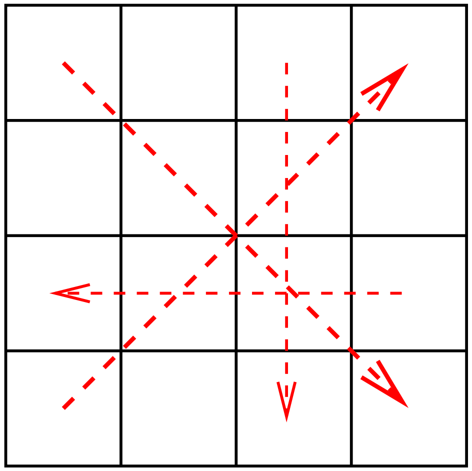
Disclaimers: Whenever I say counting, I mean **EXACT COUNTING**. There is a rich and exciting theory of estimation and approximation, but that is not us!

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,

$$x_{11} + x_{12} + x_{13} + x_{14} = 24, \text{ **first row**}$$

$$x_{13} + x_{23} + x_{33} + x_{43} = 24, \text{ **third column**}$$

Generating Function Formulas

The problem we have is equivalent to determining a short expression for $\sum_{n=0}^{\infty} M_{4\times4}(n)t^n$.

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**:

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

Optimization

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

A *flow* is a function $f : arcs(G) \to \mathbf{Z}_{\geq \mathbf{0}}$ 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 $0 \leq f(i,j) \leq c(i,j)$.

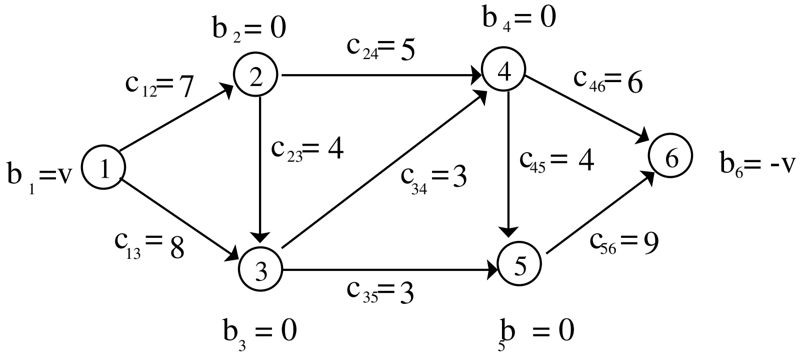


Figure 1: A simple example

How many Max-Flows are there?

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

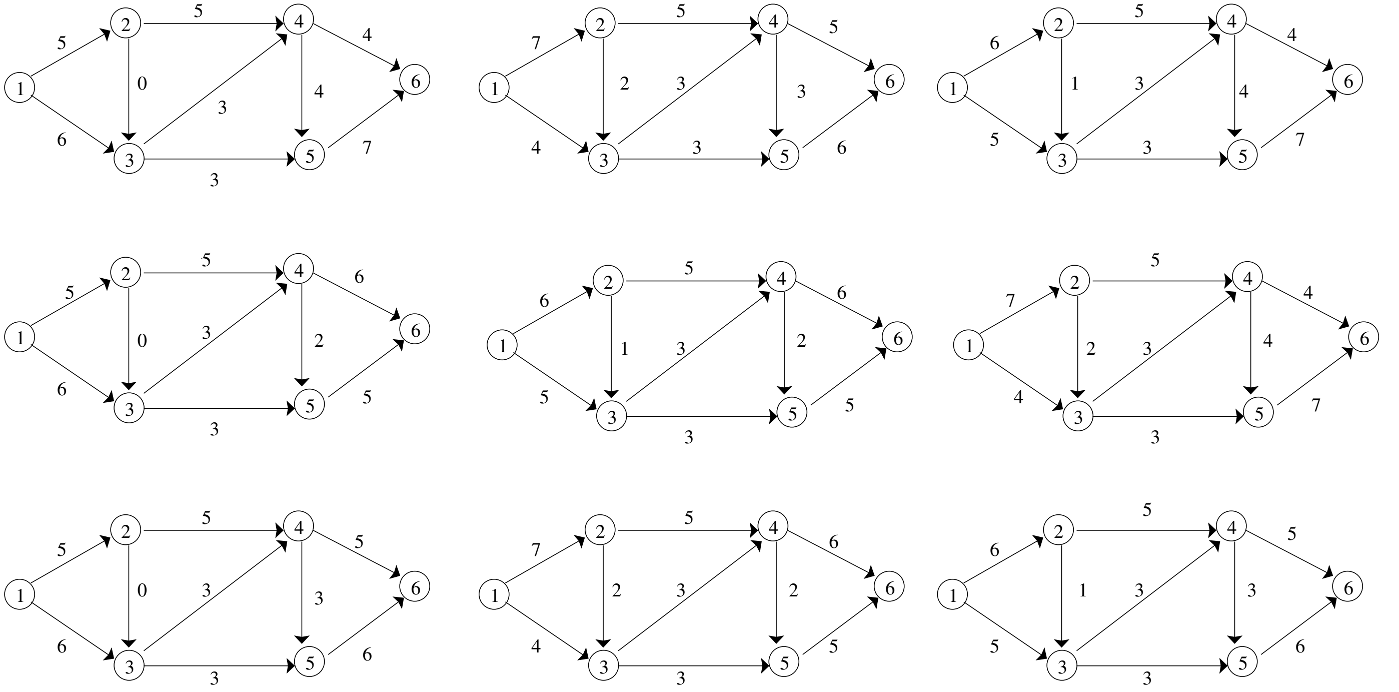


Figure 2: All max flows in the network.

- 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:

$$\{(x, y, z, w, v) \in \mathbb{R}^5_+ | 12223x + 12224y + 36674z + 61119w + 85569v = 89643$$

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

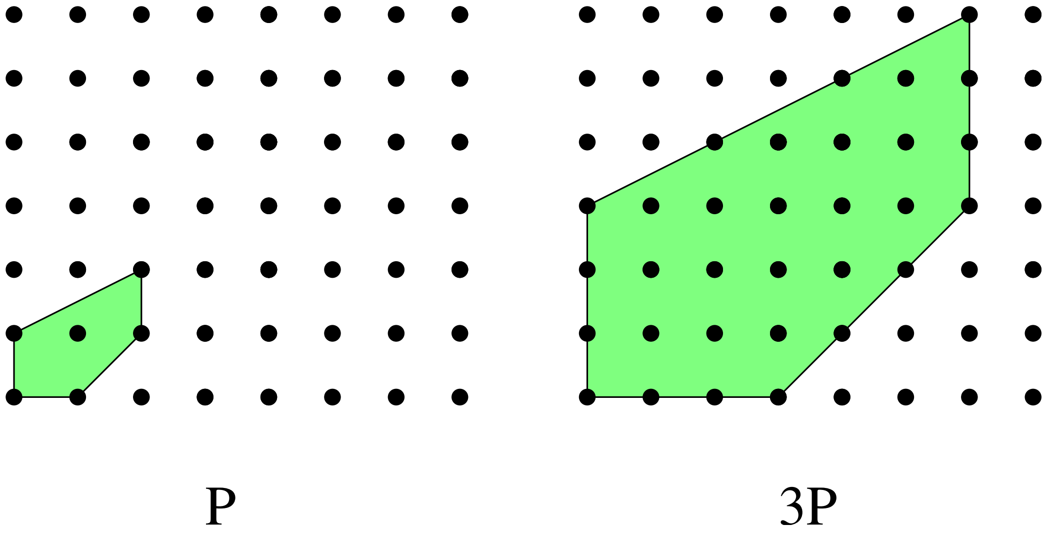
$$\phi_A(b)$$

Jesús De Loera

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

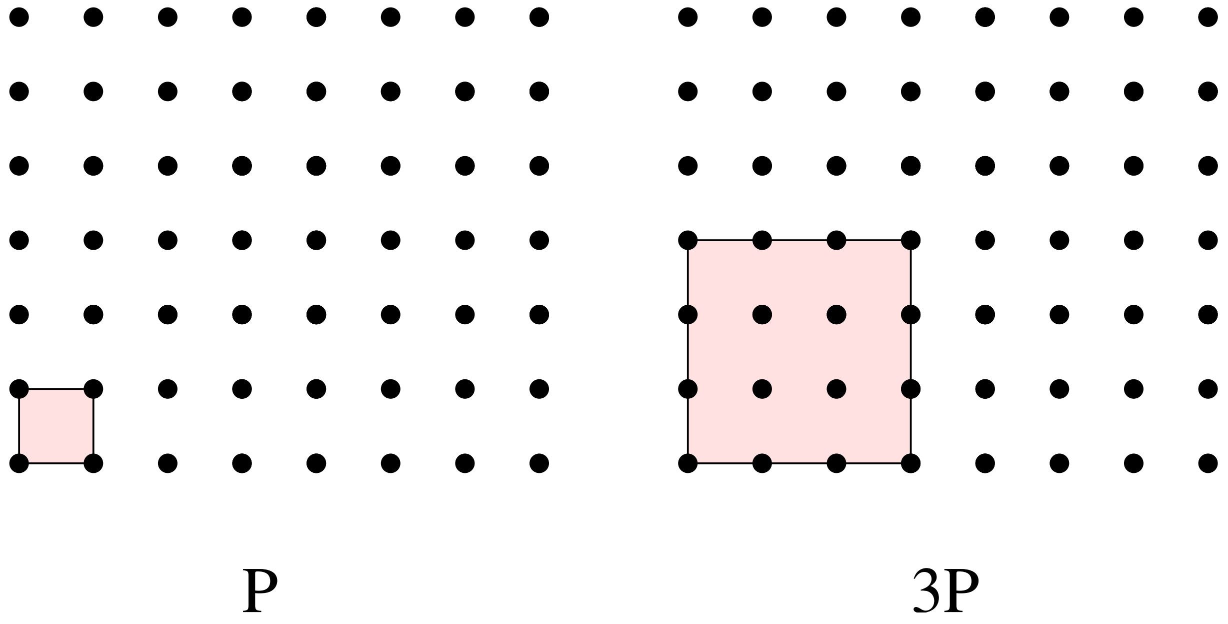
$$i(P,n) = \#(nP \cap \mathbb{Z}^d) = \#\{q \in P \ |nq \in \mathbb{Z}^d\}$$

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

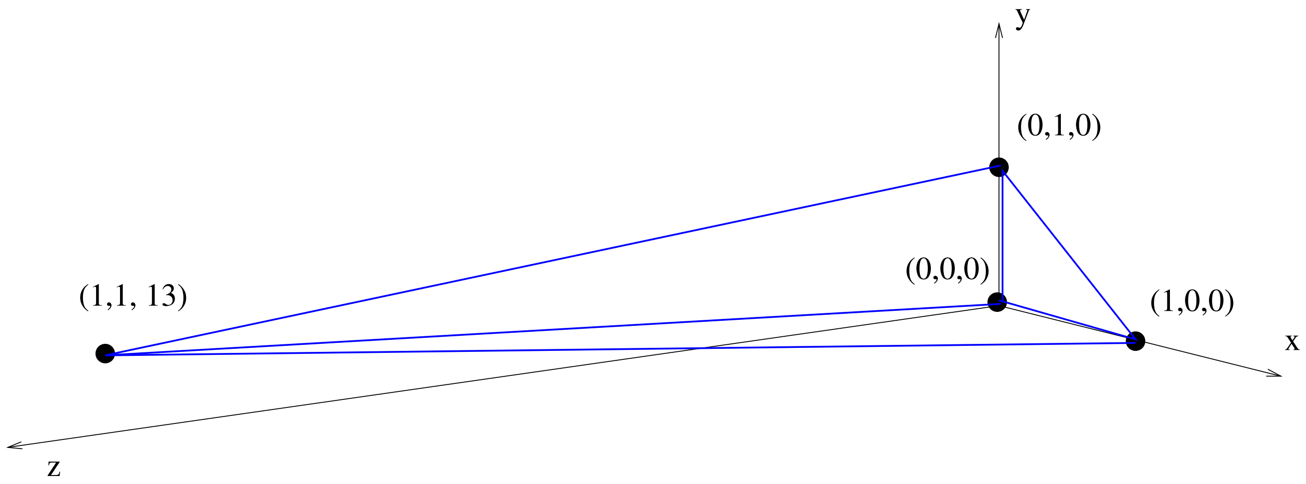


$$i(P,n) = (n+1)^2 \qquad i(P^\circ,n) = (n-1)^2$$

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.

Our Recent Generalization

Theorem (J. De Loera 2004). Let P be a convex rational d-polytope. Let f be any homogeneous polynomial function in $\mathbb{Z}[x_1, x_2, \ldots, x_d]$ and let a hyperplane arrangement H be given too. Then the counting function

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

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.

This generalizes results of Brion-Vergne and Beck-Pixton

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

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

A Key Structure Theorem.

Theorem. *For a $d \times n$ integral matrix A and a parameter vector $b \in cone(A)$,*

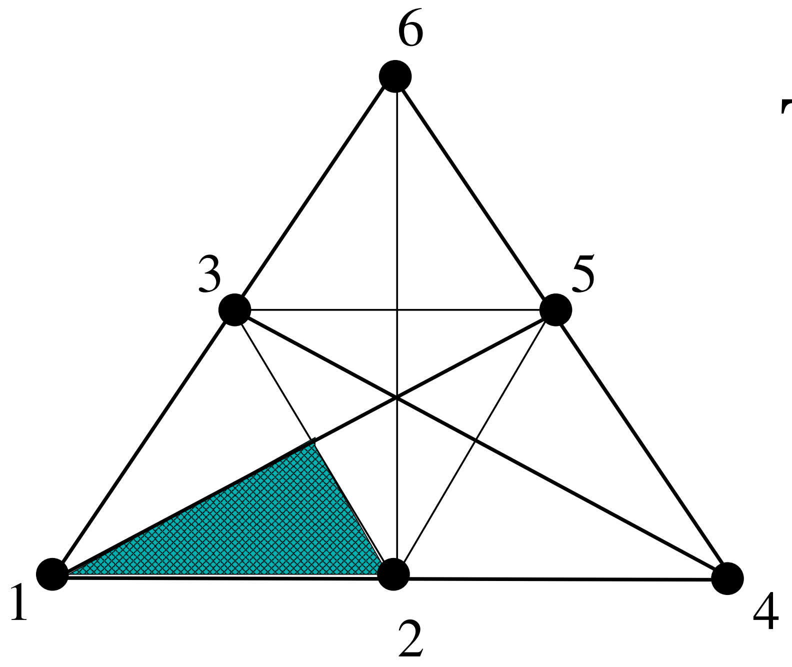
- *there exist a finite decomposition of $\mathbb{Z}^d \cap cone(A)$ such that ϕ_A is a multivariate polynomial of degree $n-d$ in each piece. The number $n-d$ is the dimension of the polytope $\{x | Ax = bx \geq 0\}$.*

- *More precisely, $cone(A)$ can be decomposed into pieces, called* chambers, *such that, for all integral vectors b inside a chamber the function $\phi_A(b)$ can be written as a fixed polynomial function of degree $n-d$ in the variables $b_1, \ldots, b_d$ plus a "correction polynomial" of smaller degree. The correction terms depend periodically on the values of $b_1, b_2, \ldots, b_d$.*

- *The chambers are convex polyhedral subcones of $cone(A)$, that subdivide its interior and their union equals $cone(A)$.*

Example

$$A = \begin{bmatrix} 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix}$$



Two dimensional slice of the cone Ax=b x>=0.

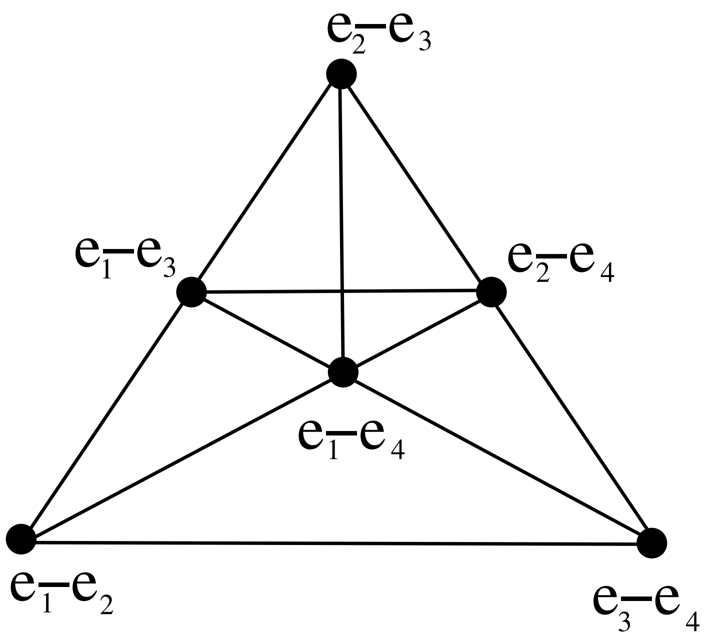
Here is the formula for the chamber marked in the picture.

$$\phi_A(b_1, b_2, b_3) = \frac{b_2 b_3}{2} + \frac{b_2 b_3^2}{8} - \frac{b_3^2}{24} + correction$$

$$correction = \begin{cases} 1 + \frac{b_2}{2} + \frac{2b_3}{3} & \text{if } b_1 = 0 \text{ and } b_2 = 0 \ mod 2 \\ \frac{1}{2} + \frac{b_2}{2} + \frac{5b_3}{12} & \text{if } b_1 = 1 \text{ and } b_2 = 1 \ mod 2 \\ \frac{1}{2} + \frac{3b_2}{8} + \frac{13b_3}{24} & otherwise. \end{cases}$$

Example:

$$A=\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & -1 & -1 \end{pmatrix}$$



Two dimensional slice of the cone Ax=b x>=0.

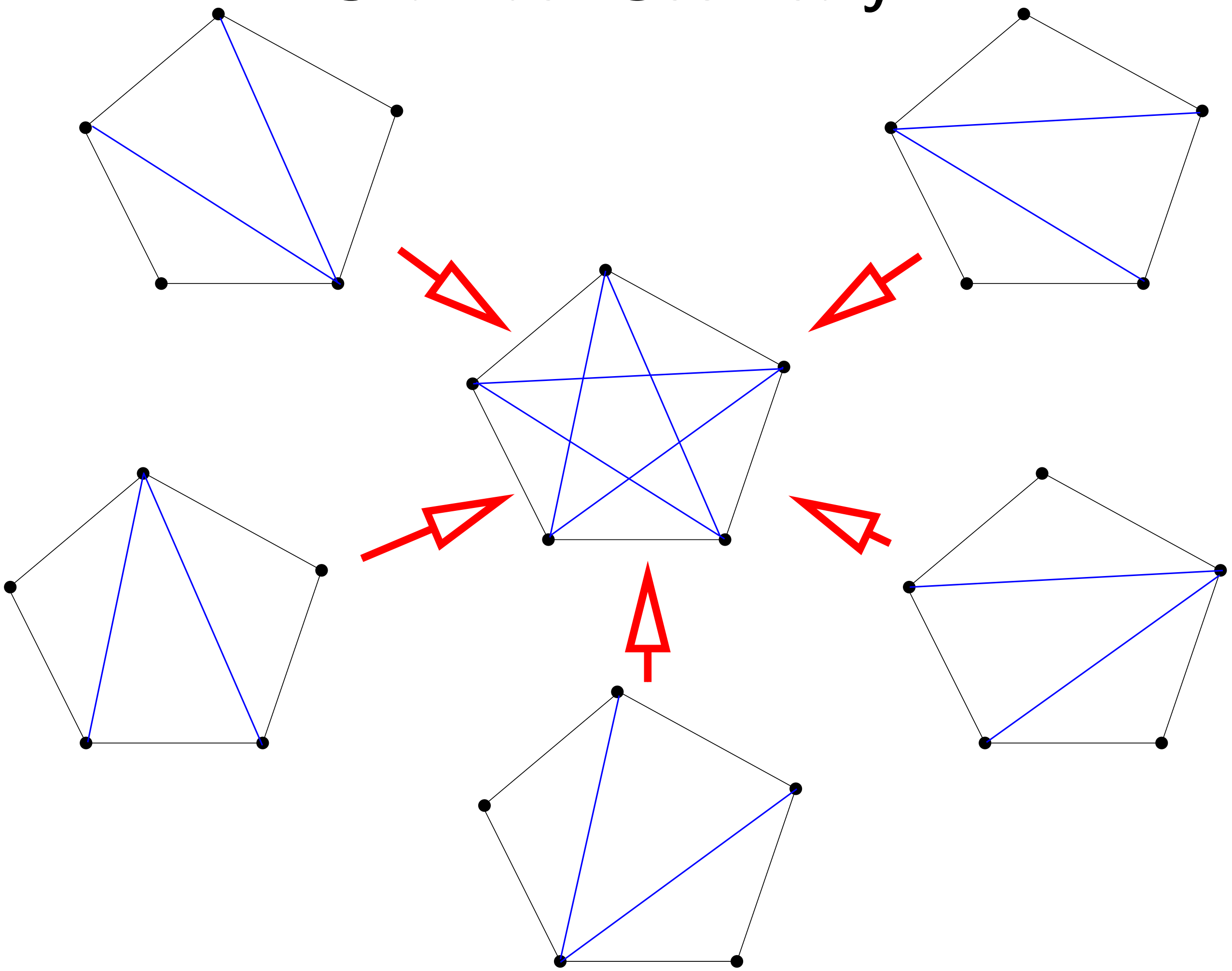
1. If $\min\{b_3, -b_2, b_1+b_2\} \geq 0$ then
$$\phi_{K_4}(b) \quad = \quad (b_1+b_2+3)(b_1+b_2+2)(b_1+b_2+1)/6.$$

2. If $\min\{b_1, b_2, b_3\} \geq 0$ then
$$\phi_{K_4}(b) \quad = \quad (b_1+1)(b_1+2)(b_1+3b_2+3)/6.$$

3. If $\min\{b_1, b_2, b_1+b_3, b_2+b_3, -b_3\} \geq 0$ then $\phi_{K_4}(b) \quad = \quad 1+\frac{11}{6}\, b_1 + 2/3\, b_3 + b_2 + 3/2\, b_1\, b_2 + {b_1}^2 + 1/6\, {b_1}^3 + 1/2\, {b_1}^2 b_2 - 1/6\, {b_3}^3 - 1/2\, b_1\, {b_3}^2 + 1/2\, b_1\, b_3 - 1/2\, {b_3}^2.$

4. If $\min\{b_1, b_2+b_3, -b_1-b_3\} \geq 0$ then $\phi_{K_4}(b) \quad = \quad (b_1+2)(b_1+1)(2b_1+3b_2+3+3b_3).$

Chamber Geometry.



COUNTING LATTICE POINTS INSIDE MORE COMPLICATED REGIONS, CAN WE?

Can one count inside other regions?

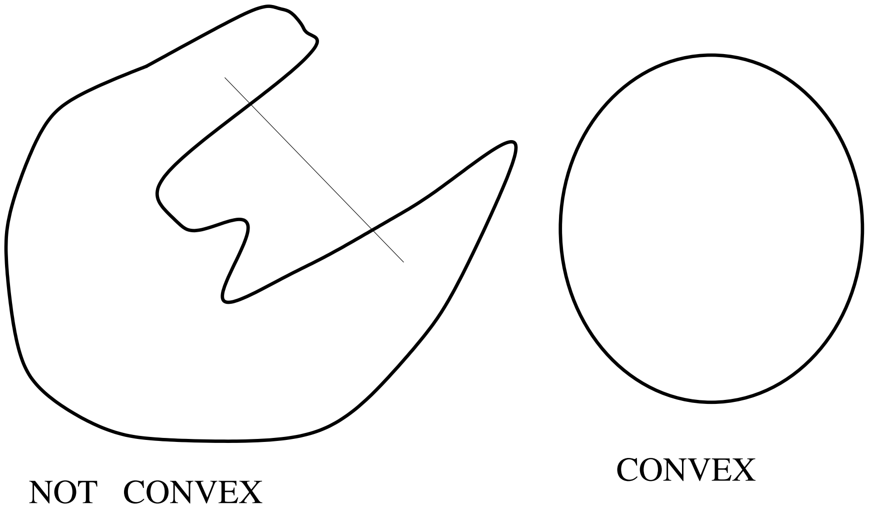
When the sets are arbitrary really bad things can happen, even in small fixed dimension!

- Given (a, b, c) positive integers, deciding whether there is a lattice point in the set $\{x|ax^2 + bx = c,\ x \geq 0\}$ is an NP-complete problem.
- Deciding whether there is a non-negative integer root for arbitrary polynomials in $\mathbb{Z}[x_1, \ldots, x_9]$ is undecidable.

Thus we clearly need to be less ambitious!

But convex sets must be tractable, right?

A convex set C is a set of Euclidean space such that for any pair of points in C the line segment joining x and y is completely inside C. Polyhedra are the simplest case.



CAN ONE EASILY COUNT THE LATTICE POINTS OF CONVEX SETS?

EARLIER WORKERS

CREDIT CARD CYBER-THIEVES CARE

For an integer number n consider the 4-dimensional convex body

$$B(n) = \{x \in R^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 \leq n\}$$

Jacobi proved that if $|B(n)|$ is the number of lattice points in $B(n)$, for n of the form $pq = n$, where p, q are primes, we have

$$|B(n)| - |B(n-1)| = 8(1 + p + q + n)$$

If we know that $n = pq$, then a factorization of n can be done fast if we know how to compute $|B(n)|$!!

RSA cryptosystems used in Internet transactions can be broken if you know how to count lattice points fast.

VISIT:

`www.math.ucdavis.edu/~latte`

`www.math.ucdavis.edu/~totalresidue`

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

THANK YOU!