counting lattice points in polytopes

federico ardila

san francisco state university  
san francisco california usa

universidad de los andes  
bogotá colombia

sacnas national meeting
san jose . oct 26 . 2011
2-D: Polygons

Let's focus on convex polygons:

$P$ is convex if:

If $p, q \in P$, then the whole line segment $pq$ is in $P$. 
2-D: Polygons

Combinatorially, polygons are very simple:

- One “combinatorial" type of $n$-gon for each $n$.
- One “regular" $n$-gon for each $n$.
3-D: Polyhedra

The combinatorial types in 3-D are much more complicated (and interesting)

Combinatorial type doesn’t depend just on number of vertices. Keep track of numbers $V, E, F$ of vertices, edges, and faces.
3-D: Polyhedra

Keep track of numbers $V, E, F$ of vertices, edges, and faces. But even that is not enough! Two combinatorially different polytopes can have the same numbers $(V, E, F)$.

Also, not every combinatorial type has a “regular" polytope. Only regular polytopes:
tetrahedron, cube, octahedron, dodecahedron, icosahedron.
Theorem. (Euler 1752) \( V - E + F = 2 \).

Klee: “first landmark in the theory of polytopes"
Alexandroff-Hopf: “first important event in topology"
3-D: Polyhedra

**Question.**
Given numbers $V, E, F$, can you construct a polytope with $V$ vertices, $E$ edges, and $F$ faces?

**Theorem.** (Steinitz, 1906)
There exists a polytope with $V$ vertices, $E$ edges, and $F$ faces if and only if

$$V - E + F = 2, \quad V \leq 2F - 4, \quad F \leq 2V - 4.$$
4-D: Polychora

In 4-D, things are even more complicated (and interesting).

Euler’s theorem?
\[ V - E + F - S = 0. \]

Steinitz’s theorem?
Not yet. But Ziegler et. al. have made significant progress.

Regular polychora?
simplex, cube, crosspolytope, 24-cell, 120-cell, 600-cell
Discovered by Ludwig Schläfli and by Alicia Boole Stott.
(She coined the term “polytope”.)

But what are we even talking about? What is a polytope?
What is a polytope? (First answer.)

In 1-D: “polytope" = segment

\[ \overline{xy} = \text{“convex hull" of } x \text{ and } y \]
\[ = \{ \lambda x + \mu y : \lambda, \mu \geq 0, \lambda + \mu = 1 \} \]
**n-D: Polytopes**

What is a polytope? (First answer.)

In 2-D:

\[ \triangle xyz = \text{"convex hull" of } x, y, \text{ and } z \]
\[ = \text{conv}(x, y, z) \]
\[ = \{\lambda x + \mu y + \nu z : \lambda, \mu, \nu \geq 0, \lambda + \mu + \nu = 1\} \]
**n-D: Polytopes**

**What is a polytope?** (First answer.)

**Definition.** A polytope is the convex hull of $m$ points in $\mathbb{R}^d$:

$$P = \text{conv}(v_1, \ldots, v_m) := \left\{ \sum_{i=1}^m \lambda_i v_i : \lambda_i \geq 0, \sum_{i=1}^m \lambda_i = 1 \right\}$$

**Trouble:** Hard to tell whether a point is in the polytope or not.
What is a polytope? (Second answer.)

**Definition.** A polytope is the solution to a system of linear inequalities in $\mathbb{R}^d$:

$$ P = \left\{ \mathbf{x} \in \mathbb{R}^d : A\mathbf{x} \leq \mathbf{b} \right\} $$

(Trouble: Hard to tell what are the vertices.)
n-D: Polytopes

What is a polytope? (Both answers are the same.)

Theorem. A subset of $\mathbb{R}^d$ is the convex hull of a finite number of points if and only if it is the bounded set of solutions to a system of linear inequalities.

Note. It is tricky, but possible, to go from the V-description to the H-description of a polytope. The software polymake does it.
Examples of polytopes

1. Simplices

(point, segment, triangle, tetrahedron, \ldots)

Let \( \mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{R}^d \). (1 in \( i \)th position)

The standard \((d - 1)\)-simplex is

\[
\Delta_{d-1} := \text{conv}(\mathbf{e}_1, \ldots, \mathbf{e}_d)
\]

\[
= \left\{ \mathbf{x} \in \mathbb{R}^d : x_i \geq 0, \sum_{i=1}^{d} x_i = 1 \right\}
\]
Examples of polytopes

2. Cubes

(point, segment, square, cube, . . .)

The standard $d$-cube is

$$\square_d := \text{conv}(b : \text{all } b_i \text{ equal } 0 \text{ or } 1)$$

$$= \left\{ x \in \mathbb{R}^d : 0 \leq x_i \leq 1 \right\}$$
Examples of polytopes

3. Crosspolytopes

(point, segment, square, octahedron, ...)

The $d$-crosspolytope is

$$
\diamond_d := \text{conv}( -e_1, e_1, \ldots, -e_d, e_d )
$$

$$
= \left\{ x \in \mathbb{R}^d : \sum_{i=1}^{d} a_i x_i \leq 1 \text{ whenever all } a_i \text{ are } -1 \text{ or } 1 \right\}
$$
Two very nice facts about polytopes. *(Schläfli, 1850)*

- **Euler’s theorem:**
  If $f_i$ is the number of $i$-dimensional faces, then
  
  $$f_1 - f_2 + \cdots \pm f_{d-1} = \begin{cases} 
  0 & \text{if } d \text{ is even,} \\
  2 & \text{if } d \text{ is odd.} 
  \end{cases}$$

  *(Roots of algebraic topology.)*

- **Classification of regular polytopes:**
  The only regular polytopes are:
  - the $d$-simplices (all $d$),
  - the $d$-cubes (all $d$),
  - the $d$-crosspolytopes (all $d$),
  - the icosahedron and dodecahedron ($d = 3$),
  - the 24-cell, the 120-cell, and the 600-cell ($d = 4$).

  *(Roots of Coxeter group theory.)*
Corte de comerciales.

For more information about

• polytopes
• Coxeter groups,
• matroids, and
• combinatorial commutative algebra,

please visit

http://math.sfsu.edu/federico/

where you will find links to the (150+) lecture videos and notes of my courses at San Francisco State University and the Universidad de Los Andes.

(Also exercises, discussion forum, research projects, etc.)

(San Francisco State University – Colombia Combinatorics Initiative)
Polygons

**Question.** How does the combinatorialist measure a polytope?

**Answer.** By counting! (Counting what?)

Continuous measure: area
Discrete measure: number of lattice points

area: $3\frac{1}{2}$

lattice points: 8 total, 1 interior.
Polygons

Continuous measure: area
Discrete measure: number of lattice points

From discrete to continuous:

**Theorem. (Pick, 1899)**
Let $P$ be a polygon with integer vertices. If $I = \text{number of interior points of } P$ and $B = \text{number of boundary points of } P$, then

$$\text{Area}(P) = I + \frac{B}{2} - 1$$

In the example,

$$\text{Area}(P) = \frac{7}{2}, \quad I = 1, \quad B = 7.$$
Polytopes

To extend to $n$ dimensions, we need to count more things.

Continuous measure: volume = $\int_P dV$
Discrete measure: number of lattice points
A richer discrete measure:

Let $L_P(n) =$ number of lattice points in $nP$.
Let $L_{P^o}(n) =$ number of interior lattice points in $nP$.

In example,

$$L_P(n) = \frac{7}{2}n^2 + \frac{7}{2}n + 1,$$
$$L_{P^o}(n) = \frac{7}{2}n^2 - \frac{7}{2}n + 1.$$
Examples

2. Cube

In 3-D, \( L_{\square_3}(n) = (n + 1)^3 \) (a cubical grid of size \( n + 1 \))

\( L_{\square_3^o}(n) = (n - 1)^3 \) (a cubical grid of size \( n - 1 \))
Examples

2. Cube
In dimension 3, \( L_{\square_3}(n) = (n + 1)^3 \), \( L_{\square_3^o}(n) = (n - 1)^3 \).
In dimension \( d \), we need to count lattice points in
\[
 n_{\square_d} = \left\{ \mathbf{x} \in \mathbb{R}^d : 0 \leq x_i \leq n \right\}.
\]

Lattice points:
\((y_1, \ldots, y_d) \in \mathbb{Z}^d\) with \(0 \leq y_i \leq n\). \((n + 1\) options for each \(y_i)\)
Interior lattice points:
\((y_1, \ldots, y_d) \in \mathbb{Z}^d\) with \(0 < y_i < n\). \((n - 1\) options for each \(y_i)\)

\[
 L_{\square_d}(n) = (n + 1)^d, \quad L_{\square_d^o}(n) = (n - 1)^d.
\]
Examples

1. Simplex

Count points in

\[ n\Delta_{d-1} = \left\{ x \in \mathbb{R}^d : x_i \geq 0, \sum_{i=1}^{d} x_i = n \right\}. \]

Interior points:

\((y_1, \ldots, y_d) \in \mathbb{Z}^d \text{ with } y_i > 0, \sum_{i=1}^{d} y_i = n.\)

\[ L_{\Delta_d^o}(n) = \binom{n - 1}{d - 1}. \]

Lattice points:

\((y_1, \ldots, y_d) \in \mathbb{Z}^d \text{ with } y_i \geq 0, \sum_{i=1}^{d} y_i = n.\)

\[ z_i = y_i + 1 \leftrightarrow (z_1, \ldots, z_d) \in \mathbb{Z}^d \text{ with } z_i > 0, \sum_{i=1}^{d} z_i = n + d.\]

\[ L_{\Delta_d}(n) = \binom{n + d - 1}{d - 1}. \]
Examples

3. Crosspolytope: Skip.

4. The “coin polytope"

Let $f(N) =$ number of ways to make change for $N$ cents using (an unlimited supply of) quarters, dimes, nickels, and pennies.

Notice: $f(N)$ is the number of lattice points in the polytope

$\text{Coin}(N) = \{(q, d, n, p) \in \mathbb{R}^4 : q, d, n, p \geq 0, 25q + 10d + 5n + p = N\}$

Now, $\text{Coin}(N) = N\text{Coin}(1)$, so

$$L_{\text{Coin}(1)}(N) = f(N), \quad L_{\text{Coin}(1)^o}(N) = f(N - 41).$$

Warning: Coin(1) does not have integer vertices.
Ehrhart’s theorem

Theorem. (Ehrhart, 1962)

Let \( P \) be a \( d \)-polytope with integer vertices in \( \mathbb{R}^d \). Then

\[
L_P(n) = c_d n^d + c_{d-1} n^{d-1} + \cdots + c_1 n + c_0
\]

is a polynomial in \( n \) of degree \( d \). Also,

\[
c_d = \text{Vol}(P), \quad c_{d-1} = \text{“Surface Vol”}(P), \quad c_0 = 1.
\]

So (discrete) counting gives us the (continuous) volume of \( P \).

This is called the \textbf{Ehrhart polynomial} of \( P \).
Ehrhart’s theorem

Theorem. (Ehrhart, 1962) For a $d$-polytope $P$,

$$L_P(n) = c_d n^d + c_{d-1} n^{d-1} + \cdots + c_1 n + c_0$$

is the Ehrhart polynomial of $P$.

Define the Ehrhart series of $P$ to be

$$Ehr_P(z) = \sum_{n \geq 0} L_P(n) z^n = L_P(0) z^0 + L_P(1) z^1 + L_P(2) z^2 + \cdots$$

In our first example,

$$Ehr_P(z) = \sum_{n \geq 0} \left( \frac{7}{2} n^2 + \frac{7}{2} n + 1 \right) z^n = \cdots = \frac{1 + 5z + z^2}{(1 - z)^3}$$

for $|z| < 1$. 
Examples

1. Simplex. We computed the Ehrhart polynomial:

\[ L_{\Delta_d}(n) = \binom{n+d-1}{d-1} = \binom{n+d-1}{n} = \frac{(n+d-1)(n+d-2)\cdots(d+1)d}{d!}. \]

Notice that:

\[ \binom{-d}{n} = \frac{(-d)(-d-1)\cdots(-n-d+2)(-n-d+1)}{d!} = (-1)^n \binom{n+d-1}{d-1} \]

so

\[ Ehr_{\Delta_d}(z) = \sum_{n \geq 0} L_{\Delta_d}(n)z^n = \sum_{n \geq 0} (-1)^n \binom{-d}{n}z^n = (1 - z)^{-d}. \]

In conclusion,

\[ Ehr_{\Delta_d}(z) = \frac{1}{(1 - z)^d} \]
Examples

2. Cube. We computed the Ehrhart polynomial:

\[ L_{\square_d}(n) = (n + 1)^d \]  
so  
\[ Ehr_{\square_d}(z) = \sum_{n \geq 0} (n + 1)^d z^n. \]

\[ Ehr_{\square_0}(z) = \frac{1}{1-z}, \quad Ehr_{\square_1}(z) = \frac{1}{(1-z)^2}, \quad Ehr_{\square_2}(z) = \frac{1+z}{(1-z)^3} \]

\[ Ehr_{\square_3}(z) = \frac{1+4z+z^2}{(1-z)^4}, \quad Ehr_{\square_4}(z) = \frac{1+11z+11z^2+z^3}{(1-z)^5}, \ldots \]

To compute these use  
\[ Ehr_{\square_{d+1}}(z) = Ehr_{\square_d}(z) + z \frac{d}{dz} Ehr_{\square_d}(z) \]

We are led to guess that

\[ Ehr_{\square_d}(z) = \frac{a_0 z^0 + a_1 z^1 + \cdots + a_d z^d}{(1 - z)^{d+1}} \]

where \( a_i \) is a positive integer. What does it count?
Examples

2. Cube. The Ehrhart series of the $d$-cube is:

$$Ehr_{\square_d}(z) = \sum_{n \geq 0} (n + 1)^d z^n = \frac{a_0 z^0 + a_1 z^1 + \cdots + z_d z^d}{(1 - z)^{d+1}}$$

**Theorem.** (Euler 1755 / Carlitz, 1953) The number $a_i$ equals the number of permutations of $[n]$ having exactly $i$ descents.

Example: The permutations of $\{1, 2, 3\}$ and their descents:

$$123, 132, 213, 231, 312, 321$$

So

$$Ehr_{\square_3}(z) = \frac{1 + 4z + 1z^2}{(1 - z)^3}.$$
Examples

3. Crosspolytope The Ehrhart series of the $d$-crosspolytope is:

$$Ehr_{\diamond,d}(z) = \frac{(1 + z)^d}{(1 - z)^{d+1}}.$$ 

4. Coin polytope The Ehrhart series of the coin polytope is:

$$Ehr_{Coin}(z) = (1 + z^1 + z^{1\cdot2} + z^{1\cdot3} + \cdots)(1 + z^5 + z^{5\cdot2} + z^{5\cdot3} + \cdots) \cdot (1 + z^{10} + z^{10\cdot2} + z^{10\cdot3} + \cdots)(1 + z^{25} + z^{25\cdot2} + z^{25\cdot3} + \cdots)$$

so

$$Ehr_{Coin}(z) = \frac{1}{(1 - z)(1 - z^5)(1 - z^{10})(1 - z^{25})}.$$ 

One of these is not like the others. Why?
Stanley’s theorem

Theorem. (Stanley 1980) For any $d$-polytope with integer vertices, the Ehrhart series is of the form

$$Ehr_P(z) = \frac{a_0 z^0 + a_1 z^1 + \cdots + a_d z^d}{(1 - z)^{d+1}}$$

where $a_0, \ldots, a_d$ are non-negative integers.

- If the vertices are rational, then for some integers $n_1, \ldots, n_{d+1} > 0$:

$$Ehr_P(z) = \frac{a_0 z^0 + a_1 z^1 + \cdots + a_d z^d}{(1 - z^{n_1}) \cdots (1 - z^{n_{d+1}})}$$

- If the vertices are irrational, nobody knows.

Strategy of proof: Prove it for simplices, then “triangulate".
Ehrhart reciprocity

If we plug \( n \in \mathbb{N} \) into the Ehrhart polynomial, we get

\[ L_P(n) = \text{number of lattice points in } nP \]

A strange idea: What if we plug in a negative integer \(-n\)?

\[ L_P(-n) = ?? \]

Something amazing happens:

**Theorem.** (Macdonald 1971) For any \( d \)-polytope with integer vertices,

\[ L_P(-n) = (-1)^d L_P^o(n). \]

We get the number of interior points in \( nP \)!
Ehrhart reciprocity v2

Put differently,

**Theorem. (Macdonald 1971)** If the Ehrhart polynomial of $P$ is

$$L_P(n) = c_d n^d + c_{d-1} n^{d-1} + \cdots + c_1 n + c_0$$

then the interior Ehrhart polynomial is

$$L_{P^o}(n) = c_d n^d - c_{d-1} n^{d-1} + \cdots \pm c_1 n \mp c_0.$$ 

For instance, recall that in our example:

$$L_P(n) = \frac{7}{2} n^2 + \frac{7}{2} n + 1, \quad L_{P^o}(n) = \frac{7}{2} n^2 - \frac{7}{2} n + 1.$$
Back to Pick’s theorem

**Theorem.** (Pick, 1899)

Let $P$ be a polygon with integer vertices. If

- $I =$ number of interior points of $P$ and
- $B =$ number of boundary points of $P$, then

\[
\text{Area}(P) = I + \frac{B}{2} - 1
\]

**Proof:** We have

\[
L_P(n) = an^2 + bn + c, \quad L_{P^o}(n) = an^2 - bn + c.
\]

Therefore

\[
I = a - b + c, \quad B = 2b \quad \longrightarrow \quad I + \frac{B}{2} - 1 = a + c - 1.
\]

But we saw that $a = \text{Area}(P)$ and $c = 1$. \(\square\)
Thank you very much.

Muchas gracias.
Corte de comerciales.

For more information about

- polytopes
- Coxeter groups,
- matroids, and
- combinatorial commutative algebra,

please visit

http://math.sfsu.edu/federico/

where you will find links to the (150+) lecture videos and notes of my courses at San Francisco State University and the Universidad de Los Andes.

(Also exercises, discussion forum, research projects, etc.)

(San Francisco State University – Colombia Combinatorics Initiative)