Let's count points!

Han-Bom Moon

School of Mathematics
Institute for Advanced Study

September 12, 2017

Question

Question

What is your favorite mathematical theorem, result, or formula?

Part I

Introduction - integral points and integral polytopes

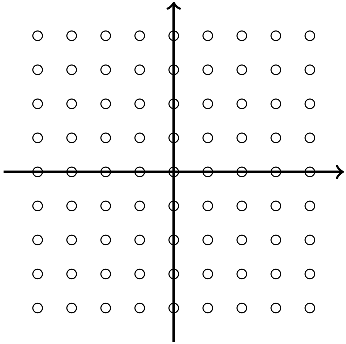
Integral points

An integral point of $\mathbb{R}^n$ is a point $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ such that each coordinate x_i is an integer.

Examples:

- $(2, -1, 5)$: an integral point in $\mathbb{R}^3$
- $(-2, \frac{2}{5})$: not an integral point in $\mathbb{R}^2$

$\mathbb{Z}^n$: set of n-dimensional integral points.

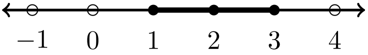


Integral polytope

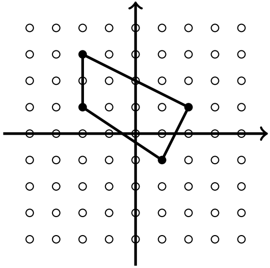
In $\mathbb{R}^n$, an integral polytope is a figure (convex set) generated by finitely many integral points.

Examples:

- One-dimensional integral polytope in $\mathbb{R}^1$: finite interval with integer endpoints.



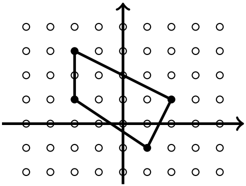
- Two-dimensional integral polytope in $\mathbb{R}^2$: polygon whose vertices are all integral points.



Main question

Question

For an integral polytope P, count the number of integral points on P.



Two related questions:

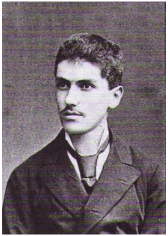
Question (Computational aspect)

Find a fast way counting the number of integral points on P.

Question (Theoretical aspect)

Describe the number of integral points on P in terms of some geometric properties/quantities of P.

Pick's theorem



Georg Alexander Pick, 1859 - 1942

Theorem (Pick, 1899)

Let P be a two-dimensional integral polytope in $\mathbb{R}^2$.

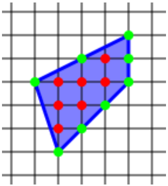
- i: *number of integral points in the interior of P.*
- b: *number of integral points on the boundary of P.*

Then

$$\text{Area}(P) = i + \frac{b}{2} - 1.$$

Pick's theorem

$$\text{Area}(P) = i + \frac{b}{2} - 1$$



For instance, in the picture above, $i = 7$, $b = 8$. So

$$\text{Area} = 7 + \frac{8}{2} - 1 = 10.$$

Corollary

Every two-dimensional integral polytope has a half-integer area.

Goal

I will present and prove an interesting formula which counts the number of integral points (indeed, describes the set of integral points completely) on a given integral polytope P.

- The result is true for arbitrary dimension.
- I will give a proof for two-dimensional case, for notational simplicity.
- The same proof works for every dimension.

Part II

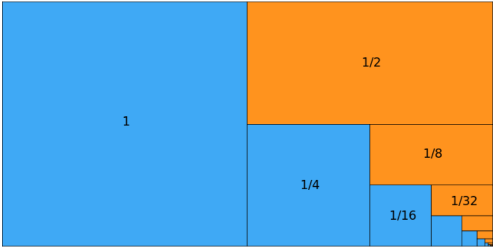
Preliminary - Geometric series

Geometric series

A geometric series is an infinite sum with constant ratio between successive terms.

$$a + ar + ar^2 + ar^3 + ar^4 + \cdots = \sum_{n=0}^{\infty} ar^n$$

It appears in many different geometric contexts. For instance:



This picture shows us that

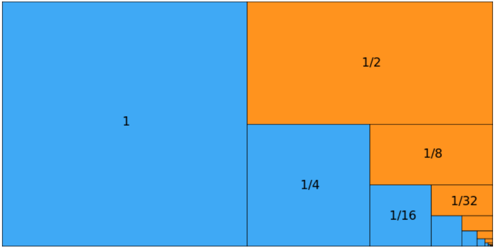
$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^3 + \cdots =$$

Geometric series

A geometric series is an infinite sum with constant ratio between successive terms.

$$a + ar + ar^2 + ar^3 + ar^4 + \cdots = \sum_{n=0}^{\infty} ar^n$$

It appears in many different geometric contexts. For instance:



This picture shows us that

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^3 + \cdots = 2.$$

Geometric series

$$a + ar + ar^2 + ar^3 + ar^4 + \cdots = \sum_{n=0}^{\infty} ar^n$$

Indeed, if $|r| < 1$, we can evaluate this sum by using a very simple formula.

First of all, consider the sum of first $n+1$ terms:

$$S_n := a + ar + ar^2 + \cdots + ar^n$$

$$rS_n = ar + ar^2 + ar^3 + \cdots + ar^{n+1}$$

$$(1-r)S_n = S_n - rS_n = (a + ar + \cdots + ar^n) - (ar + ar^2 + \cdots + ar^{n+1})$$

$$= a - ar^{n+1} = a(1 - r^{n+1})$$

$$\Rightarrow S_n = \frac{a(1-r^{n+1})}{1-r}$$

$$a + ar + ar^2 + ar^3 + \cdots = \lim_{n\to\infty} S_n = \lim_{n\to\infty} \frac{a(1-r^{n+1})}{1-r} = \frac{a}{1-r}$$

Geometric series

$$a + ar + ar^2 + ar^3 + ar^4 + \cdots = \sum_{n=0}^{\infty} ar^n = \frac{a}{1-r}$$

Here are some explicit examples we will consider later:

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x} \; (a = 1, r = x)$$

$$x^3 + x^4 + x^5 + \cdots = \frac{x^3}{1-x} \; (a = x^3, r = x)$$

$1+x^{-1}+x^{-2}+x^{-3}+\cdots =$

Geometric series

$$a + ar + ar^2 + ar^3 + ar^4 + \cdots = \sum_{n=0}^{\infty} ar^n = \frac{a}{1-r}$$

Here are some explicit examples we will consider later:

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x} \ (a = 1, r = x)$$

$$x^3 + x^4 + x^5 + \cdots = \frac{x^3}{1-x} \ (a = x^3, r = x)$$

$$1+x^{-1}+x^{-2}+x^{-3}+\cdots = 1+x^{-1}+(x^{-1})^2+(x^{-1})^3+\cdots = \frac{1}{1-x^{-1}} = \frac{x}{x-1}$$

$$1 + xy^{-1} + x^2y^{-2} + x^3y^{-3} + \cdots \quad =$$

Geometric series

$$a + ar + ar^2 + ar^3 + ar^4 + \cdots = \sum_{n=0}^{\infty} ar^n = \frac{a}{1-r}$$

Here are some explicit examples we will consider later:

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x} \ (a = 1, r = x)$$

$$x^3 + x^4 + x^5 + \cdots = \frac{x^3}{1-x} \ (a = x^3, r = x)$$

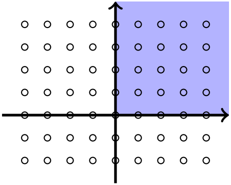
$$1+x^{-1}+x^{-2}+x^{-3}+\cdots = 1+x^{-1}+(x^{-1})^2+(x^{-1})^3+\cdots = \frac{1}{1-x^{-1}} = \frac{x}{x-1}$$

$$\begin{aligned} 1 + xy^{-1} + x^2y^{-2} + x^3y^{-3} + \cdots &= 1 + xy^{-1} + (xy^{-1})^2 + (xy^{-1})^3 + \cdots \\ &= \frac{1}{1-xy^{-1}} = \frac{y}{y-x} \end{aligned}$$

Some variations

Exercise: Compute the sum of all monomials $x^i y^j$ on the first quadrant, that is, $x^i y^j$ with $i, j \geq 0$.

$$1 + x + y + x^2 + xy + y^2 + x^3 + x^2y + xy^2 + y^3 + \cdots = ?$$



If we change the order of terms with respect to the degree of x:

$$\begin{aligned}
&1 + x + y + x^2 + xy + y^2 + x^3 + x^2y + xy^2 + y^3 + \cdots \\
&= (1 + y + y^2 + \cdots) + (x + xy + xy^2 + \cdots) + (x^2 + x^2y + x^2y^2 + \cdots) + \cdots \\
&= \frac{1}{1-y} + \frac{x}{1-y} + \frac{x^2}{1-y} + \cdots = \frac{1}{1-y} + \frac{1}{1-y} \cdot x + \frac{1}{1-y} \cdot x^2 + \cdots \\
&= \frac{\frac{1}{1-y}}{1-x} = \frac{1}{(1-x)(1-y)}.
\end{aligned}$$

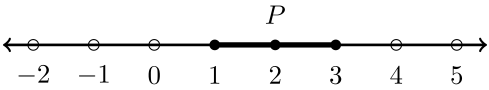
Part III

Main theorem

First example

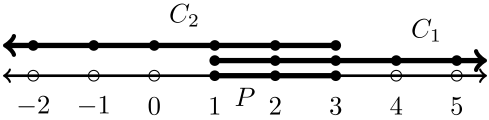
Before stating the main theorem, let's compute some simple examples.

Consider an interval $P = [1, 3]$.



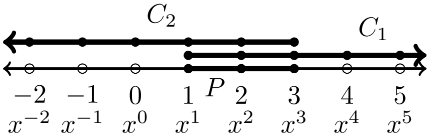
There are three integral points on it, 1, 2, and 3.

For each endpoint, we can draw a ray.



The overlap of these two rays is precisely P.

First example



For each C_i, we can make a geometric series $[C_i]$ by adding all x^i's where i is an integer on the ray.

$$[C_1] = x + x^2 + x^3 + x^4 + \cdots = \frac{x}{1-x}$$

$$[C_2] = x^3 + x^2 + x + 1 + x^{-1} + \cdots = \frac{x^3}{1-x^{-1}} = \frac{x^4}{x-1}$$

Let's add them. Then we have:

$$[C_1] + [C_2] = \frac{x}{1-x} + \frac{x^4}{x-1} = \frac{x}{1-x} - \frac{x^4}{1-x}$$

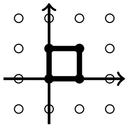
$$= \frac{x - x^4}{1-x} = \frac{x(1-x^3)}{1-x} = \frac{x(1-x)(1+x+x^2)}{1-x} = x(1+x+x^2) = x+x^2+x^3$$

This is precisely the sum of x^i for i on the interval P!

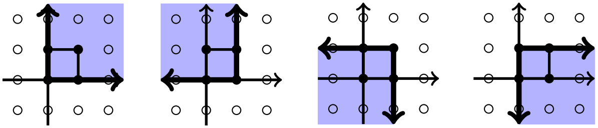
Second example

Let's look at a two-dimensional example.

Consider a unit square S on the plane:



For each vertex v_k, we can make an internal angle C_k.

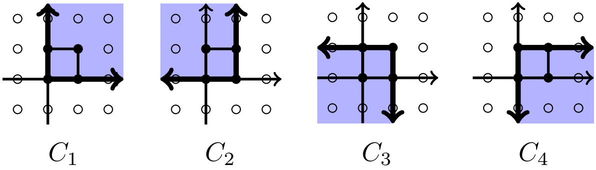


C_1 C_2 C_3 C_4

As we have done before, by adding all $x^i y^j$ on C_k, we can make an infinite sum $[C_k]$. For instance,

$$[C_1] = 1+x+y+x^2+xy+y^2+x^3+x^2y+xy^2+y^3+\cdots = \frac{1}{(1-x)(1-y)}.$$

Second example



By similar computations, we obtain:

$$[C_1] = \frac{1}{(1-x)(1-y)}$$

$$[C_2] = x+1+xy+x^{-1}+y+xy^2+\cdots = \sum_{i\le 1, j\ge 0} x^i y^j = \frac{x}{(1-x^{-1})(1-y)} = \frac{x^2}{(x-1)(1-y)}$$

$$[C_3] = \sum_{i\le 1, j\le 1} x^i y^j = \frac{xy}{(1-x^{-1})(1-y^{-1})} = \frac{x^2y^2}{(x-1)(y-1)}$$

$$[C_4] = \sum_{i\ge 0, j\le 1} x^i y^j = \frac{y}{(1-x)(1-y^{-1})} = \frac{y^2}{(1-x)(y-1)}$$

Second example

$$[C_1] = \frac{1}{(1-x)(1-y)}, \quad [C_2] = \frac{x^2}{(x-1)(1-y)},$$
$$[C_3] = \frac{x^2y^2}{(x-1)(y-1)}, \quad [C_4] = \frac{y^2}{(1-x)(y-1)}$$

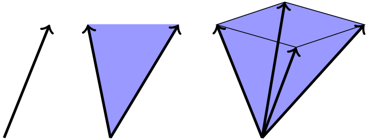
If we add them together, we have:

$$\frac{1}{(1-x)(1-y)} + \frac{x^2}{(x-1)(1-y)} + \frac{x^2y^2}{(x-1)(1-y)} + \frac{y^2}{(1-x)(y-1)}$$
$$= \frac{1-x^2+x^2y^2-y^2}{(1-x)(1-y)} = \frac{(1-x)(1-y)(1+x)(1+y)}{(1-x)(1-y)}$$
$$= (1+x)(1+y) = 1+x+y+xy$$

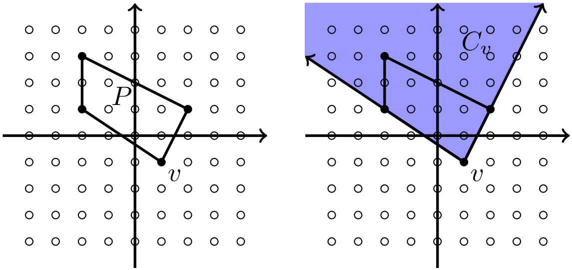
which is exactly, the sum of x^iy^j on the square S.

Some terminologies

A cone is a figure generated by several rays starting from a point.

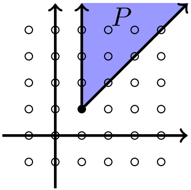


The inner tangent cone C_v to P at v is the internal angle we've described before.



Some teminologies

For any polytope or cone P, let $[[P]]$ be the (possibly infinite) sum of all $x^i y^j$'s where (i,j) is in P.



$$[[P]] = xy + xy^2 + x^2y^2 + xy^3 + x^2y^3 + x^3y^3 + \cdots$$

Let $[P]$ be a representation of $[[P]]$ as a rational function.

$$\begin{aligned}[P] &= (xy + x^2y^2 + x^3y^3 + \cdots) + (xy^2 + x^2y^3 + x^3y^4 + \cdots) + \cdots \\ &= \frac{xy}{1-xy} + \frac{xy^2}{1-xy} + \cdots = \frac{\frac{xy}{1-xy}}{1-y} = \frac{xy}{(1-xy)(1-y)}\end{aligned}$$

If P is an integral polytope, $[[P]] = [P]$ is a finite sum.

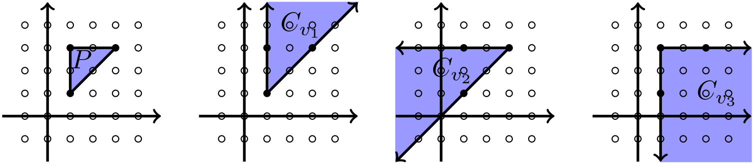
One can generalize them to n-dimensional polytopes.

Main theorem

Theorem (Brion, 1988)

Let P be an integral polytope with vertices $v_1, v_2, \cdots, v_k$. Then

$$[P] = \sum_{i=1}^{k} [C_{v_i}].$$



$$\begin{aligned}[C_{v_1}] + [C_{v_2}] + [C_{v_3}] &= \frac{xy}{(1-y)(1-xy)} + \frac{x^5y^4}{(x-1)(xy-1)} + \frac{xy^4}{(1-x)(y-1)} \\ &= xy + xy^2 + x^2y^2 + xy^3 + x^2y^3 + x^3y^3 = [P]\end{aligned}$$

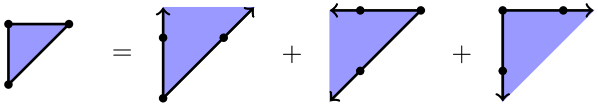
Main theorem

Theorem (Brion, 1988)

Let P be an integral polytope with vertices $v_1, v_2, \cdots, v_k$. Then

$$[P] = \sum_{i=1}^{k} [C_{v_i}].$$

Schematically, we can say:



Part IV

The proof

First reduction - Induction on dimension

Theorem

Let P be an integral polytope with vertices $v_1, v_2, \cdots, v_k$. Then

$$[P] = \sum_{i=1}^{k} [C_{v_i}].$$

The theorem is saying that “for every n-dimensional integral polytope, a certain equation holds”.

It is a nice idea to use mathematical induction on the dimension of integral polytopes.

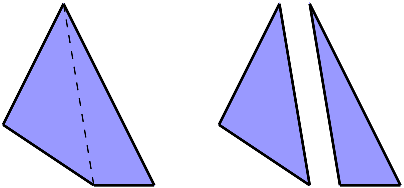
For $n = 1$, integral polytopes are finite intervals. We can check it directly.

So we'll assume that $n = 1$ case is true. I'll give a proof for 2-dimensional case.

Second reduction - Divide and conquer

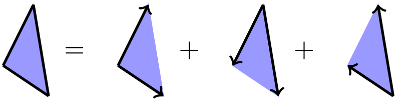
A great idea to solve a mathematical problem is to reduce it into simpler problems.

Every polygon can be decomposed into triangles. For instance, consider the following quadrilateral.

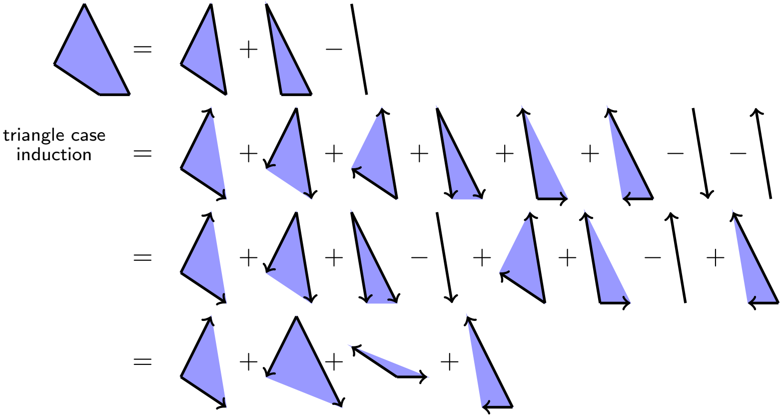


Second reduction - Divide and conquer

Suppose that we can prove the triangle case, that is,

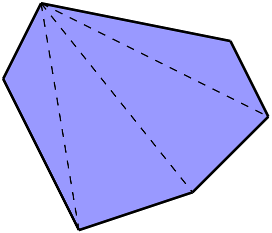


Then it is also true for the quadrilateral case, because:



Second reduction - Divide and conquer

By applying the same idea several times, we can conclude that it is sufficient to prove the theorem for triangles.



Let's prove the theorem for triangles.

Some algebraic definitions

1. $\mathbb{Q}[x, y]$: set of polynomials with two variables x and y.
   $x + y^2$, xy, $x + 4x^3$
2. $\mathbb{Q}[x^{\pm}, y^{\pm}]$: set of Laurent polynomials.
   $x + y^2$, xy, xy^{-1}, $x^3y^{-2} + 5y^4$
3. $\mathbb{Q}[[x, y]]$: set of formal power series.
   $1 + x + y + x^2 + xy + y^2 + \cdots, 1 + x + x^2 + x^3 + \cdots$.
4. $\mathbb{Q}[[x^{\pm}, y^{\pm}]]$: set of formal Laurent series.
   $\cdots + x^{-2} + x^{-1} + 1 + x + x^2 + \cdots,$
5. $\mathbb{Q}(x, y)$: set of rational functions.
   $\frac{x^2+y}{1+x+y^2}, 1 + x + x^2 + \cdots = \frac{1}{1-x}$

$$\begin{array}{ccccc} & & \mathbb{Q}[x,y] & \subset & \mathbb{Q}[[x,y]] \\ & & \cap & & \cap \\ \mathbb{Q}(x,y) & \supset & \mathbb{Q}[x^{\pm},y^{\pm}] & \subset & \mathbb{Q}[[x^{\pm},y^{\pm}]] \end{array}$$

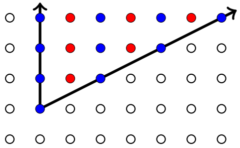
Some formal Laurent series cannot be written as rational functions.

Infinite sum associated to a cone

For any polytope or cone C,

$[[C]]$: infinite sum of all monomials on C. $[[C]] \in \mathbb{Q}[[x^{\pm}, y^{\pm}]]$.

$[C]$: its realization as a rational function. $[C] \in \mathbb{Q}(x, y)$.



sum of blue terms $= 1+y+x^2y+y^2+x^2y^2+x^4y^2+\cdots = \dfrac{1}{(1-x^2y)(1-y)}$

sum of red terms $= x+xy+x^3y+xy^2+x^3y^2+x^5y^2+\cdots = \dfrac{x}{(1-x^2y)(1-y)}$

$$\text{total sum} = \frac{1+x}{(1-x^2y)(1-y)}$$

Infinite sum associated to a cone

Let PL be the subspace of $\mathbb{Q}[[x^{\pm}, y^{\pm}]]$ generated by $[[C]]$ for some cone C (space of polyhedral Laurent series).

There is a map

$$\begin{aligned} p : PL &\to \mathbb{Q}(x, y) \\ [[C]] &\mapsto [C]. \end{aligned}$$

It preserves the addition, subtraction and polynomial multiplication.

$$p([[C]] \pm [[D]]) = [C] \pm [D] = p([[C]]) \pm p([[D]])$$

For any $h \in \mathbb{Q}[x^{\pm}, y^{\pm}]$, then

$$p(h \cdot [[C]]) = h \cdot [C] = h \cdot p([[C]]).$$

In abstract algebra, we say p is an $\mathbb{Q}[x^{\pm}, y^{\pm}]$-module homomorphism.

Key observation

An half-plane H is a union of two cones. So $[[H]] \in PL$.

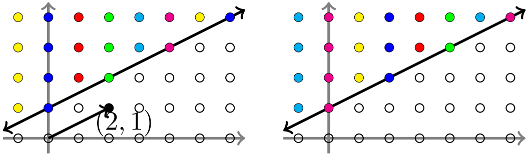
We want to compute $[H] := p([[H]])$.

Lemma

For a half-plane H, $[H] = 0$.

Proof.

Let (a, b) be an integral vector parallel to the boundary of H.
Then $x^a y^b [[H]] = [[H]]$.
Apply p. $[H] = p([[H]]) = p(x^a y^b [[H]]) = x^a y^b p([[H]]) = x^a y^b [H]$.
We have $(1 - x^a y^b)[H] = 0$.
Divide $1 - x^a y^b$. Then we obtain $[H] = 0$. □



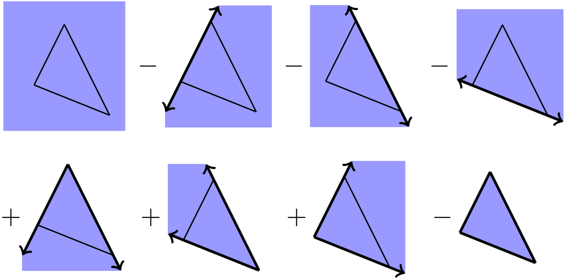
Final step of the proof

For any triangle T, let C_1, C_2, C_3 be three inner tangent cones, H_1, H_2, H_3 be three half-planes generated by three edges.

Consider the following alternating sum:

$$[[\mathbb{R}^2]] - [[H_1]] - [[H_2]] - [[H_3]] + [[C_1]] + [[C_2]] + [[C_3]] - [[T]]$$

Schematically,



This sum is 0. (Why?)

Final step of the proof

$$[[\mathbb{R}^2]] - [[H_1]] - [[H_2]] - [[H_3]] + [[C_1]] + [[C_2]] + [[C_3]] - [[T]] = 0$$

Apply the map p here. Then $[H_1] = [H_2] = [H_3] = 0$.

$[\mathbb{R}^2] = 0$ because $\mathbb{R}^2$ is the union of two half-planes.

So we have $[C_1] + [C_2] + [C_3] - [T] = 0$, or equivalently,

$$[T] = [C_1] + [C_2] + [C_3].$$

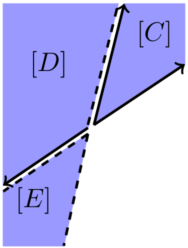
Part V

Final remarks

Ehrhart-MacDonald reciprocity

Recall that for any half-plane H, $[H] = 0$.

We can make an interesting consequence. Consider the following figure:



1. $[C] + [D] = 0$
2. $[D] + [E] = 0$
3. By adding 1 and 2, we have $[C] = [E]$. In other words, any closed cone is equal to the opposite open cone.

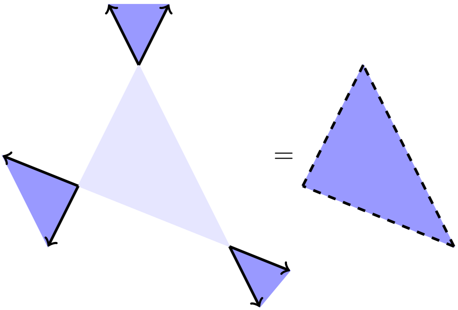
Ehrhart-MacDonald reciprocity

Let T be any triangle. Let E_1, E_2, E_3 be three outer tangent cones, and let C_1, C_2, C_3 be three open inner tangent cones.

Then

$$[E_1] + [E_2] + [E_3] = [C_1] + [C_2] + [C_3] = [T]_{int}$$

where $[T]_{int}$ be the sum of all monomials on the interior of T.



Ehrhart-MacDonald reciprocity

Eugène Ehrhart, 1906 - 2000

Of course, we can generalize it to arbitrary n-dimensional integral polytopes.

Theorem (Ehrhart-MacDonald reciprocity)

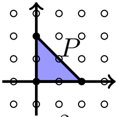
Let P be an integral polytope with vertices $v_1, v_2, \cdots, v_k$. Let E_i be the outer tangent cone to P at v_i. Then

$$[P]_{int} = (-1)^n \sum_{i=1}^{k} [E_i].$$

So... how can we count points?

$$[P] = \sum_{i=1}^{k} [C_{v_i}]$$

The left hand side is the sum of monomials on P.



$$[P] = 1 + x + x^2 + y + xy + y^2$$

The number of integral points on P is $[P](1,1) = 6$.

On the other hand, the right hand side

$$[C_{v_1}]+[C_{v_2}]+[C_{v_3}] = \frac{1}{(1-x)(1-y)} + \frac{y^4}{(y-1)(y-x)} + \frac{x^4}{(x-1)(x-y)}$$

is not defined at $(x,y) = (1,1)$. But we can compute its limit

$$\lim_{(x,y)\to(1,1)} \frac{1}{(1-x)(1-y)} + \frac{y^4}{(y-1)(y-x)} + \frac{x^4}{(x-1)(x-y)} = 6.$$

Original proof

Michel Brion, 1958 -

Brion's original proof uses the well-known correspondence

$$\text{integral polytope } P \Longleftrightarrow \text{projective polarized toric variety } (X, L)$$

So we may interpret the result in a purely geometric context.

Keywords: T-equivariant Grothendieck group, localization.

Thank you!