Lattice-point counting and cyclic sieving,

or,

Ehrhart theory and cyclic sieving: two great tastes that taste great together?

James Propp

June 24, 2014

Slides at http://jamespropp.org/polytope-csp.pdf

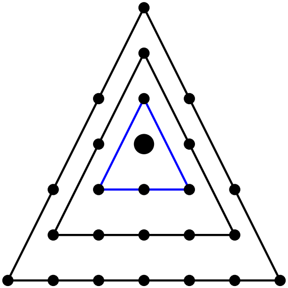
Ehrhart theory

Given a polytope Π in $\mathbb{R}^d$ with vertices in $\mathbb{Z}^d$, there is a polynomial P such that the number of lattice points in the dilated polytope $N\Pi$ is $P(N)$ for all non-negative integers N.

Ehrhart theory

Given a polytope Π in $\mathbb{R}^d$ with vertices in $\mathbb{Z}^d$, there is a polynomial P such that the number of lattice points in the dilated polytope $N\Pi$ is $P(N)$ for all non-negative integers N.

E.g., for Π in $\mathbb{R}^2$ with vertices $(-1,-1)$, $(0,1)$, and $(1,-1)$, we have $\#(N\Pi \cap \mathbb{Z}^2) = 2N^2 + 2N + 1$ for all $N \geq 0$:



What if the vertices aren't lattice points?

For polytopes with vertices in $\mathbb{Q}^d$, we need quasipolynomials; that is, powers of roots of unity get involved.

E.g., if Π is the polytope in $\mathbb{R}^1$ with vertices $-\frac{1}{2}$ and $\frac{1}{2}$, we have $\#(N\Pi \cap \mathbb{Z}^2) = N + \frac{1}{2} + \frac{1}{2}(-1)^N$ for all $N \geq 0$.

Cyclic sieving

Given a set S and a map $L : S \to S$ satisfying $L^n = \mathrm{Id}_S$ giving rise to an action of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ on S, there is (in many cases) a "natural" polynomial $p(\cdot)$ such that the number of fixed-points of L^k is $|p(\zeta^k)|$ for all integers k (where ζ is a primitive nth root of unity).

Cyclic sieving

Given a set S and a map $L : S \to S$ satisfying $L^n = \mathrm{Id}_S$ giving rise to an action of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ on S, there is (in many cases) a "natural" polynomial $p(\cdot)$ such that the number of fixed-points of L^k is $|p(\zeta^k)|$ for all integers k (where ζ is a primitive nth root of unity).

More specifically, we often have $\#\mathrm{Fix}(L^k) = |p(\zeta^k)|$ with

$$p(t) = \sum_{s \in S} t^{f(s)},$$

where $f : S \to \mathbb{Z}$ is some function that reflects the structure of S and L.

Why does this make sense?

A polynomial of the form $p(t) = \sum_{s \in S} t^{f(s)}$ is a good candidate for satisfying $\#\mathrm{Fix}(L^k) = |p(\zeta^k)|$ for all integers k:

Why does this make sense?

A polynomial of the form $p(t) = \sum_{s \in S} t^{f(s)}$ is a good candidate for satisfying $\#\mathrm{Fix}(L^k) = |p(\zeta^k)|$ for all integers k:

For k a multiple of n, we get

$$|p(\zeta^k)| = |p(1)| = |\sum_{s \in S} 1^{f(s)}| = |S|,$$

the number of fixed points of L^k.

Why does this make sense?

A polynomial of the form $p(t) = \sum_{s \in S} t^{f(s)}$ is a good candidate for satisfying $\#\mathrm{Fix}(L^k) = |p(\zeta^k)|$ for all integers k:

For k a multiple of n, we get

$$|p(\zeta^k)| = |p(1)| = |\sum_{s \in S} 1^{f(s)}| = |S|,$$

the number of fixed points of L^k.

For general k, we have

$$|p(\zeta^k)| = |\sum_{s \in S} \zeta^{kf(s)}| \leq \sum_{s \in S} |\zeta^{kf(s)}| = |S|.$$

What am I trying to do?

I've been trying to combine Ehrhart Theory and cyclic sieving, letting S be $N\Pi$ with L some linear map from $\mathbb{R}^d$ to itself (restricted to $N\Pi \cap \mathbb{Z}^d$).

What am I trying to do?

I've been trying to combine Ehrhart Theory and cyclic sieving, letting S be $N\Pi$ with L some linear map from $\mathbb{R}^d$ to itself (restricted to $N\Pi \cap \mathbb{Z}^d$).

Motivation: Let's see what kind of geometrical situations lead to cyclic sieving.

Then we can go back to combinatorial contexts and see if that kind of geometry is latent there.

Why bring this up here?

Why bring this up here?

Richard's role in Ehrhart theory: e.g., his work on enumerating semimagic squares, viewing semimagic squares as lattice points in a suitable polytope

Why bring this up here?

Richard's role in Ehrhart theory: e.g., his work on enumerating semimagic squares, viewing semimagic squares as lattice points in a suitable polytope

Richard's role in the theory of cyclic sieving:
symmetries of plane partitions and the complementation map

Why bring this up here?

Richard's role in Ehrhart theory: e.g., his work on enumerating semimagic squares, viewing semimagic squares as lattice points in a suitable polytope

Richard's role in the theory of cyclic sieving:
symmetries of plane partitions and the complementation map
$\rightarrow$ Stembridge's discovery of the $q = -1$ phenomenon

Why bring this up here?

Richard's role in Ehrhart theory: e.g., his work on enumerating semimagic squares, viewing semimagic squares as lattice points in a suitable polytope

Richard's role in the theory of cyclic sieving:
symmetries of plane partitions and the complementation map
$\rightarrow$ Stembridge's discovery of the $q = -1$ phenomenon
$\rightarrow$ Reiner, Stanton, and White's discovery of the cyclic sieving phenomenon

Why bring this up here?

Richard's role in Ehrhart theory: e.g., his work on enumerating semimagic squares, viewing semimagic squares as lattice points in a suitable polytope

Richard's role in the theory of cyclic sieving:
   symmetries of plane partitions and the complementation map
$\rightarrow$ Stembridge's discovery of the $q = -1$ phenomenon
$\rightarrow$ Reiner, Stanton, and White's discovery of the cyclic sieving phenomenon

Richard's role in founding the Cambridge Combinatorics Coffee Club

What went wrong

My first attempt to marry Ehrhart theory and cyclic sieving failed.

What went wrong

My first attempt to marry Ehrhart theory and cyclic sieving failed.

My mistake, I think, was to imagine that the center of dilation has to be in the same space as the polytope itself.

What went wrong

My first attempt to marry Ehrhart theory and cyclic sieving failed.

My mistake, I think, was to imagine that the center of dilation has to be in the same space as the polytope itself.

Here as in many other Ehrhart-ish situations, one should instead STACK the dilated polytopes to form a polyhedral cone in a space with 1 extra dimension.

The new setup

Given:

The new setup

Given:
a polyhedral cone C generated by lattice vectors $v_1, \ldots, v_k$ in $\mathbb{Z}^d$,
not generated by any proper subset;

The new setup

Given:
a polyhedral cone C generated by lattice vectors $v_1, \ldots, v_k$ in $\mathbb{Z}^d$, not generated by any proper subset;
a linear map L from $\mathbb{R}^d$ to $\mathbb{R}^d$ that takes $C_{\mathbb{Z}} = C \cap \mathbb{Z}^d$ to itself and has $L^n = I$; and

The new setup

Given:
a polyhedral cone C generated by lattice vectors $v_1, \ldots, v_k$ in $\mathbb{Z}^d$, not generated by any proper subset;
a linear map L from $\mathbb{R}^d$ to $\mathbb{R}^d$ that takes $C_{\mathbb{Z}} = C \cap \mathbb{Z}^d$ to itself and has $L^n = I$; and
a linear function r from $\mathbb{Z}^d$ to $\mathbb{Z}$ (a "rank function") whose level sets $\{x : x \in C_{\mathbb{Z}},\ r(x) = N\}$ are empty when $N < 0$ and finite otherwise;

The new setup

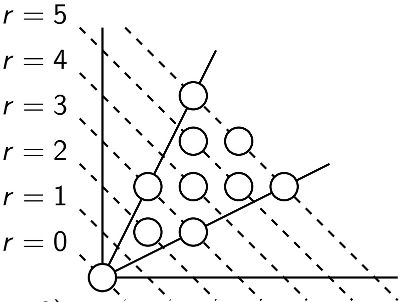
Given:
a polyhedral cone C generated by lattice vectors $v_1, \ldots, v_k$ in $\mathbb{Z}^d$, not generated by any proper subset;
a linear map L from $\mathbb{R}^d$ to $\mathbb{R}^d$ that takes $C_{\mathbb{Z}} = C \cap \mathbb{Z}^d$ to itself and has $L^n = I$; and
a linear function r from $\mathbb{Z}^d$ to $\mathbb{Z}$ (a "rank function") whose level sets $\{x : x \in C_{\mathbb{Z}},\ r(x) = N\}$ are empty when $N < 0$ and finite otherwise;
we say a function f from $C_{\mathbb{Z}}$ to $\mathbb{Z}$ is <u>sieving</u>

The new setup

Given:
a polyhedral cone C generated by lattice vectors $v_1, \ldots, v_k$ in $\mathbb{Z}^d$, not generated by any proper subset;
a linear map L from $\mathbb{R}^d$ to $\mathbb{R}^d$ that takes $C_{\mathbb{Z}} = C \cap \mathbb{Z}^d$ to itself and has $L^n = I$; and
a linear function r from $\mathbb{Z}^d$ to $\mathbb{Z}$ (a "rank function") whose level sets $\{x : x \in C_{\mathbb{Z}},\ r(x) = N\}$ are empty when $N < 0$ and finite otherwise;
we say a function f from $C_{\mathbb{Z}}$ to $\mathbb{Z}$ is sieving when for all integers k and for all non-negative integers N, the number of $x \in C_{\mathbb{Z}}$ with $r(x) = N$ and $L^k x = x$ equals $\left|\sum_{x \in C_{\mathbb{Z}},\ r(x)=N} \zeta^{kf(s)}\right|$, where ζ is a primitive nth root of 1.

A two-dimensional example

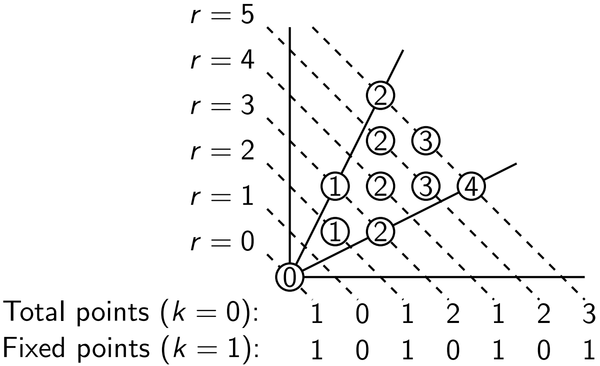
Example 1: Take $C = \langle (2,1),(1,2) \rangle$, $L : (x,y) \mapsto (y,x)$, $n = 2$, $r(i,j) = i + j$.



Total points ($k = 0$):	1	0	1	2	1	2	3
Fixed points ($k = 1$):	1	0	1	0	1	0	1

A two-dimensional example

Example 1: Take $C = \langle (2,1),(1,2) \rangle$, $L : (x,y) \mapsto (y,x)$, $n = 2$, $r(i,j) = i + j$.



Then $f(i,j) = i$ is sieving.

Some higher-dimensional examples you can try at home

Example 2: Take $C = \langle (1,0,0),(0,1,0),(0,0,1) \rangle$, $L : (x,y,z) \mapsto (y,z,x)$, $n = 3$, $r(i,j,k) = i + j + k$.

Then $f(i,j,k) = j + 2k$ is sieving. (To generalize to higher dimensions, write this as $0i + 1j + 2k$. This example encodes the prototypical CSP for the $\mathbb{Z}/(a+b)\mathbb{Z}$ rotation action on a-element subsets of an $a+b$-element set.)

Some higher-dimensional examples you can try at home

Example 2: Take $C = \langle (1,0,0),(0,1,0),(0,0,1) \rangle$,
$L : (x,y,z) \mapsto (y,z,x)$, $n = 3$, $r(i,j,k) = i + j + k$.

Then $f(i,j,k) = j + 2k$ is sieving. (To generalize to higher dimensions, write this as $0i + 1j + 2k$. This example encodes the prototypical CSP for the $\mathbb{Z}/(a+b)\mathbb{Z}$ rotation action on a-element subsets of an $a+b$-element set.)

Example 3: Take $C = \langle (1,0,1),(-1,0,1),(0,1,1),(0,-1,1) \rangle$,
$L : (x,y,z) \mapsto (y,-x,z)$, $n = 4$, $r(i,j,k) = k$.

Then $f(i,j,k) = i + 2j$ is sieving.

My old conjecture

I conjectured that we can always find a sieving function f that is linear on $\mathbb{R}^d$ (as is the case for the three preceding Examples).

My old conjecture

I conjectured that we can always find a sieving function f that is linear on $\mathbb{R}^d$ (as is the case for the three preceding Examples).

I found a counterexample: Let $C_{\text{bad}} \subset \mathbb{R}^3$ be the cone generated by lattice vectors $(2, 1, 1)$, $(-1, 2, 1)$, $(-2, -1, 1)$, and $(1, -2, 1)$, with rank function $r(i, j, k) = k$, and let L be 90-degree rotation counterclockwise about the z-axis.

Case analysis shows that no linear sieving function f exists.

My old conjecture

I conjectured that we can always find a sieving function f that is linear on $\mathbb{R}^d$ (as is the case for the three preceding Examples).

I found a counterexample: Let $C_{\mathrm{bad}} \subset \mathbb{R}^3$ be the cone generated by lattice vectors $(2,1,1)$, $(-1,2,1)$, $(-2,-1,1)$, and $(1,-2,1)$, with rank function $r(i,j,k) = k$, and let L be 90-degree rotation counterclockwise about the z-axis.

Case analysis shows that no linear sieving function f exists.

But: We can find a sieving function f that, while not linear, comes close.

My new conjecture

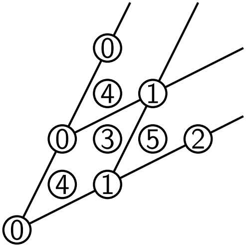
Conjecture: Given C, L, and r as above, there exists a sieving function f such that for each generating vector v_i, there is a constant c_i such that $f(x + v_i) - f(x) = c_i$ for all x in $C_{\mathbb{Z}}$.

E.g., returning to Example 1 (with $v_1 = (2, 1)$ and $v_2 = (1, 2)$) the following f would qualify (with $c_1 = 1$ and $c_2 = 0$):

My new conjecture

Conjecture: Given C, L, and r as above, there exists a sieving function f such that for each generating vector v_i, there is a constant c_i such that $f(x + v_i) - f(x) = c_i$ for all x in $C_{\mathbb{Z}}$.

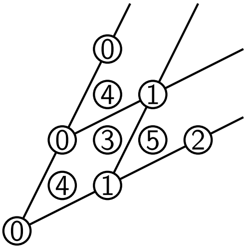
E.g., returning to Example 1 (with $v_1 = (2, 1)$ and $v_2 = (1, 2)$) the following f would qualify (with $c_1 = 1$ and $c_2 = 0$):



My new conjecture

Conjecture: Given C, L, and r as above, there exists a sieving function f such that for each generating vector v_i, there is a constant c_i such that $f(x + v_i) - f(x) = c_i$ for all x in $C_{\mathbb{Z}}$.

E.g., returning to Example 1 (with $v_1 = (2, 1)$ and $v_2 = (1, 2)$) the following f would qualify (with $c_1 = 1$ and $c_2 = 0$):



C_{bad} is not a counterexample to my new conjecture; computer search finds many suitable f's (too many!).

Final remarks

A better question: What constraints on C and L make this new conjecture (or my old conjecture) true in some systematic way?

Final remarks

A better question: What constraints on C and L make this new conjecture (or my old conjecture) true in some systematic way?

Even if the conjecture as phrased fails, it may become true if we restrict to polytopes Π and/or actions L with some special properties.

Final remarks

A better question: What constraints on C and L make this new conjecture (or my old conjecture) true in some systematic way?

Even if the conjecture as phrased fails, it may become true if we restrict to polytopes Π and/or actions L with some special properties.

Slides at http://jamespropp.org/polytope-csp.pdf