Ehrhart theory + cylic sieving =
true love forever?

Jim Propp (JamesPropp@gmail.com)

CCCC LIX, February 16, 2014

Ehrhart theory is about counting lattice points in dilations of polytopes.

Cyclic sieving is about counting fixed points of iterates of a map.

Can we combine them?

Given S finite and $\tau : S \to S$ invertible, with $\tau^n = \mathrm{Id}_S$, and given $p(t) \in \mathbb{Z}[t]$, say that (S, τ, n, p) exhibits cyclic sieving iff for all $k \geq 0$, the number of fixed points of τ^k equals $|p(\exp(2\pi i k)/n)|$. (This is slightly different from the standard definition.)

Primordial algebraic example: $S = \{z \in \mathbb{C} : \ z^n = 1\} = \{\zeta^k : 0 \leq k < n\}$ with ζ a primitive nth root of unity, $\tau : z \mapsto \zeta z$, $p(t) = 1 + t + \ldots + t^{n-1}$. (This is the basis of the discrete Fourier transform.)

There are many examples of cyclic sieving for which S is a set of combinatorial objects and $p(t) = \sum_{s \in S} t^{r(s)}$ where $r : S \mapsto \mathbb{N}$ is a combinatorially natural mapping having nothing obvious to do with τ. In particular, in many cases $r(s)$ is the rank of s under some natural poset structure on S. Example: Let S be the chain with m elements, τ be the involutory anti-automorphism $S \mapsto S$ (so that $n = 2$), and $p(t) = 1+t+\ldots+t^{m-1}$. Then $(S, \tau, 2, p)$ exhibits cyclic sieving.

Challenge: Construct a theory of cyclic sieving when S is the set of lattice points in a polytope with integer vertices and τ is some linear map of the ambient space carrying S to itself. The theory should be compatible with dilation of the polytope.

Example: Let Π be the polygon in $\mathbb{R}^s$ with vertices $(0, 0)$, $(1, 0)$, and $(0, 1)$; let S be the mth dilation of Π, let $n = 2$, and take the involution $\tau : (x, y) \mapsto (y, x)$ sending S to itself. If for all $s = (x, y)$ in S we define $r(s) = x + y$ and we take $p(t) = \sum_{s \in S} t^{r(s)} = 1 + 2t + 3t^2 + \ldots + (m + 1)t^m$, we find that $|p(-1)^k|$ equals the number of $s \in S$ with $\tau^k s = s$.