# CYCLIC SIEVING LECTURE NOTES, UW SEMINAR, 11/05/2015

JOSH SWANSON

Basic references:

- Reiner, Stanton, White (2004), "The Cyclic Sieving Phenomenon": the original paper.
- Sagan (2011), "The cyclic sieving phenomenon: a survey": nicely written survey as of a few years ago. We'll more or less go through the first 15 pages.

**Outline.**

(1) Motivational example
(2) Test case—direct proof paradigm
(3) Representation theory paradigm and example
(4) Further directions

**Example 1.** Suppose one day you were playing with a generating function for a statistic on combinatorial objects, say words of content $\{1^2, 2^2\}$ using inversions. These are

| | | | | | | |
|---|---|---|---|---|---|---|
| 1122 | 1212 | 2112 | $\Rightarrow$ # inversions: | 0 | 1 | 2 |
| 1221 | 2121 | | | 2 | 3 | |
| 2211 | | | | 4 | | |

The generating function is $1 + q + 2q^2 + q^3 + q^4$. At $q = 1$ this counts the number of such words. At $q = -1$? Gives 2. At $q = \pm i$? Gives 0. These are all non-negative integers. Are they counting something?

Cyclic sieving is a remarkably general "explanation scheme":

**Definition 2.** Let $f(q) \in \mathbb{N}[q]$ and suppose $X$ is a set of size $f(1)$. Let $C_n$ be a cyclic group of order $n$, and suppose $C_n$ acts on $X$. Write $\omega_d$ for a primitive $d$th root of unity. If

$$f(\omega_d) = \#\{x \in G : \alpha \cdot x = x\}$$

whenever $\alpha \in C_n$ has order $d$, then $(X, C_n, f(q))$ *exhibits the cyclic sieving phenomenon (CSP).*

Note that $f \in \mathbb{N}[q]$ means $f$ is constant on different primitive $d$th roots of unity.

**Example 3.** Let $\langle(1234)\rangle \leq S_4$ act on words of content $\{1^2, 2^2\}$ by permuting indexes. Then $(1234)$ has order 4 and fixes no element, and $(13)(24)$ fixes only 2121 and 1212. The identity fixes all six. Hence by direct computation, the above generating function with this action exhibits the cyclic sieving phenomenon.

Our main example is a little different from the motivational one in part because the representation theoretic argument ends up being nicer.

**Definition 4.** Let

$$[n]_q := 1 + q + \cdots + q^{n-1}$$
$$[n]_q! := [n]_q [n-1]_q \cdots [1]_q$$
$$\binom{n}{k}_q := \frac{[n]_q!}{[k]_q! [n-k]_q!} \in \mathbb{N}[q]$$

*Date*: November 7, 2015.

(where the $q$-binomial coefficient is in $\mathbb{N}[q]$ since it satisfies a Pascal's triangle-like recurrence; at $q = 1$ it counts the number of $k$-element subsets of $[n]$, and at prime powers it counts the number of $k$-dimensional subspaces of $\mathbb{F}_q^n$). Set

$$\left(\!\!\binom{[n]}{k}\!\!\right) := \{M : M \text{ is a } k\text{-element multiset on } [n]\}.$$

For instance, at $n = 3, k = 2$, this is the set $\{11, 12, 13, 22, 23, 33\}$. By "stars and bars",

$$\#\left(\!\!\binom{[n]}{k}\!\!\right) = \binom{n+k-1}{k}.$$

Let $\langle \sigma_n := (12 \cdots n)\rangle \subset S_n$ act on this set by permuting values: $(123) \cdot 33 = 11$. As it turns out,

$$\left(\!\!\binom{3+2-1}{2}\!\!\right)_q = 1 + q + 2q^2 + q^3 + q^4.$$

(Here $n = 3$, not 4.) (123) has fixes no element of $\left(\!\binom{[3]}{2}\!\right)$, and indeed the polynomial is zero at $\omega_3$, so we again have the CSP.

**Theorem 5.** *The triple*

$$\left(\left(\!\!\binom{[n]}{k}\!\!\right), \langle 12 \cdots n\rangle, \binom{n+k-1}{k}_q\right)$$

*exhibits the CSP.*

We first give a direct, elementary proof, which does not explain why we might expect such behavior to exist in the first place.

*Proof.* One idea is to explicitly compute both the fixed point set sizes and evaluations of the $q$-binomial coefficient. For the first, we have:

**Lemma 6.** *Let $g \in S_n$ have disjoint cycle decomposition $g = c_1 \cdots c_t$. Then for $M \in \left(\!\binom{[n]}{k}\!\right)$, $g \cdot M = M$ if and only if*

$$M = c_{r_1} \coprod \cdots \coprod c_{r_s},$$

*where here we view cycles as (multi)sets and the disjoint union adds multiplicities of multisets.*

*Proof.* ...by example: what does (124)(35) fix in $\left(\!\binom{[5]}{4}\!\right)$? Only 3355. In general we need multiplicities to be constant on cycles. ☐

**Corollary 7.** *Let $\alpha = \sigma_n^{n/d}$, which has order $d \mid n$. Then*

$$\#\left(\!\!\binom{[n]}{k}\!\!\right)^\alpha = \begin{cases} \binom{n/d+k/d-1}{k/d} & \text{if } d \mid k \\ 0 & \text{otherwise} \end{cases}.$$

Having identified half of the required equation, what is $\binom{n+k-1}{k}_{q=\omega_d}$? An example is illuminating:

$$\begin{aligned}\binom{4}{2}_{q=\omega_2} &= \left.\frac{[4]_q[3]_q}{[2]_q}\right|_{q=-1} \\ &= \frac{0 \cdot 1}{0}\end{aligned}$$

so consider

$$\lim_{q \to -1} \frac{[4]_q}{[2]_q} = \lim_{q \to -1} \frac{(1+q) + q^2(1+q)}{1+q} = 2 = \frac{4}{2}.$$

Hence $\binom{4}{2}_{q=\omega_2} = 4/2$. Generalizing this computation quickly yields the same formula as before,

$$\binom{n+k-1}{k}_{q=\omega_d} = \begin{cases} \binom{n/d+k/d-1}{k/d} & \text{if } d \mid k \\ 0 & \text{otherwise} \end{cases}.$$

□

This is nice, but a bit messy and unenlightening. Why should we even expect fixed point sets to be counted by evaluations of a polynomial at roots of unity?

**Definition 8.** Let $G$ be a finite group acting on a set $X$. Let $\mathbb{C}X$ denote the $\mathbb{C}$-vector space with basis $X$; $G$ acts on $\mathbb{C}X$ by linear automorphisms. The *character* of this action is $\chi\colon G \to \mathbb{C}$ given by

$$\chi(g) := \mathrm{Tr}([g] \in \mathrm{GL}(\mathbb{C}X)).$$

**Remark 9.** Viewing $[g]$ in the $X$ basis, $[g]$ is a permutation matrix with fixed points on the main diagonal. Hence

$$\chi(g) = \#X^g,$$

so cyclic sieving really says that our polynomial is encoding these character values at its evaluations.

On the other hand, let $G = C_n$ be a cyclic group. (Now we'll assume some basic representation theory of finite dimensional $G$-modules over $\mathbb{C}$.) What are the irreducible $C_n$-modules? It's abelian, so it has as many 1-dimensional representations as elements, which must be all of them. What are they? We can declare 1 to act as $\omega_n^j$ for $j = 0, 1, \ldots, n-1$ on $\mathbb{C} = \mathbb{C}[1]$, written $C^{(j)}$. These are inequivalent since their traces ($\omega_n^j$) are distinct. Hence $C_n$ acting on $\mathbb{C}X$ decomposes as $C_n$ acting on

$$m_0 C^{(0)} \oplus \cdots \oplus m_n C^{(n)}$$

for $m_j \in \mathbb{N}$. A generator in this basis has matrix

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & \omega_n^{n-1} & & \\ & & & & & \ddots & \\ & & & & & & \omega_n^{n-1} \end{pmatrix}$$

where $\omega_n^j$ appears $m_j$ times. It follows that a general element of $\alpha$ of order $d$ has trace

$$\chi(\alpha) = \sum_j m_j \omega_n^{jn/d} = \left( \sum_j m_j q^j \right) \Bigg|_{q=\omega_d}$$

**Remark 10.** Hence the CSP happens literally every time we have a cyclic group acting on a finite set if we use $f(q) := \sum_{j=0}^{n-1} m_j q^j$. This $f$ has degree at most $n-1$, making it in some sense uninteresting—for instance, our motivational example already has degree $4 > 3 = n$.

Note that all such $f$'s are equivalent mod $(q^n - 1)$. The "interesting" part of CSP is finding a polynomial which has some intrinsic interest that also happens to exhibit CSP.

It is a fact that the character of a finite dimensional representation of a finite group over $\mathbb{C}$ determines the representation up to equivalence. Hence each CSP has a unique $C_n$-module giving rise to its polynomial.

Our next goal is to give a representation-theoretic proof of the previous result. We will identify an appropriate $C_n$-module and evaluate the character cleverly, without ever deriving the explicit formulas above.

*Proof.* Consider $\mathbb{C}[n]^{\otimes k}$, the $k$-fold tensor product of the $n$-dimensional $\mathbb{C}$-vector space $\mathbb{C}[n]$, which has basis

$$\{i_1 \otimes \cdots \otimes i_k : i_j \in [n]\}.$$

Let $\mathrm{Sym}_k(n)$ denote the $k$-th symmetric power of $\mathbb{C}[n]$, namely

$$\mathrm{Sym}_k(n) := \frac{\mathbb{C}[n]^{\otimes k}}{i_1 \otimes \cdots \otimes i_k = i_{u(1)} \otimes \cdots \otimes i_{u(k)}} \qquad \forall u \in S_k$$

which has basis

$$\{[i_1 \otimes \cdots \otimes i_k] : 1 \leq i_1 \leq \cdots \leq i_k \leq n\},$$

which is naturally indexed by $\left(\!\binom{[n]}{k}\!\right)$. (We'll now write $i_1 \cdots i_k$ instead of $[i_1 \otimes \cdots \otimes i_k]$.) Now, $\langle (12 \cdots n) \rangle$ acts on $\mathbb{C}[n]$ on values, so it acts on $\mathbb{C}[n]^{\otimes k}$ and $\mathrm{Sym}_k(n)$. Indeed, we have an isomorphism of $\langle \sigma_n \rangle$-modules

$$\mathrm{Sym}_k(n) \cong \mathbb{C}\left(\!\binom{[n]}{k}\!\right),$$

so it suffices to consider the character of $\mathrm{Sym}_k(n)$ and in particular to show the character of $\alpha$ of order $d$ is $\binom{n+k-1}{k}_{q=\omega_n^d}$.

Evidently $\alpha^n = \mathrm{id}$, so the minimal polynomial of $\alpha \in \mathrm{GL}(\mathbb{C}[n])$ divides $x^n - 1$, which has distinct roots, so $\alpha$ is diagonalizable, say with basis $\{b_1, \ldots, b_n\}$. This yields a basis

$$\{b_{i_1} \cdots b_{i_k} : 1 \leq i_1 \leq \cdots \leq i_k \leq n\}$$

for $\mathrm{Sym}_k(n)$, where $b_i$ has some eigenvalue $x_i$. Indeed, this yields a basis in which $\alpha \in \mathrm{GL}(\mathrm{Sym}_k(n))$ is diagonal:

$$\alpha \cdot (b_{i_1} \cdots b_{i_k}) = (\alpha \cdot b_{i_1}) \cdots (\alpha \cdot b_{i_k}) = x_{i_1} \cdots x_{i_k} (b_{i_1} \cdots b_{i_k}).$$

Indeed, this shows

$$\chi(\alpha) = \sum_{1 \leq i_1 \leq \cdots \leq i_k \leq n} x_{i_1} \cdots x_{i_k} =: h_k(x_1, \ldots, x_n).$$

(Incidentally, we used multisets instead of subsets since subsets use the $k$th exterior power and $e_k(x_1, \ldots, x_n)$, which involves keeping track of some negatives.) Indeed, it's easy to see that we may take $(x_1, \ldots, x_n) = (1, q, \ldots, q^{n-1})$ where $q = \omega_d$. Hence the result follows from the following principal specialization:

**Lemma 11.** *If $n \geq 1$ and $k \geq 0$, then*

$$h_k(1, q, \ldots, q^{n-1}) = \binom{n+k-1}{k}_q.$$

*Proof.* One can show both sides satisfy a Pascal's triangle-like recurrence. □

□

We now turn to some more advanced and general examples. We certainly won't have time to define all the terms involved.

**Definition 12.** Let $(W, S)$ be a finite Coxeter system, let $J \subset S$, take $W_J$ to be the parabolic subgroup generated by $S$, and let $W^J$ denote the set of minimal length coset representatives of $W/W_J$. Define

$$W^J(q) := \sum_{w \in W^J} q^{\ell(w)}.$$

(For example, $S_n^{[n-1]-\{k\}}(q) = \binom{n}{k}_q$ and $S_n^{\varnothing}(q) = \sum_{w \in S_n} q^{\ell(w)} = [n]_q! = \sum_{w \in S_n} q^{\mathrm{maj}\, w}$.)

**Theorem 13** (Reiner-Stanton-White)**.** *The triple*

$$(W/W_J, C, W^J(q))$$

*exhibits the CSP (where $C \leq W$ is cyclically generated by a "regular" element, meaning one which, as an element of $W$ viewed as a complex reflection group, contains an eigenvector which is not in any of the reflecting hyperplanes).*

Using maximal parabolic subgroups in type $A$ and ignoring the multiset-subset distinction, this is essentially a vast generalization of the theorem we proved above. It has a further complex reflection group generalization:

**Definition 14.** Let $W$ be a finite complex reflection group with subgroup $W'$. Let $A = S/S_+^W$ be the coinvariant algebra of $W$ and let $A^{W'}$ denote the $W'$-invariants of the coinvariant algebra of $W$. Write $\mathrm{Hilb}(A^{W'}; q)$ for the Hilbert series of $A^{W'}$, namely the dimension generating function of the homogeneous components of the graded algebra $A^{W'}$.

**Theorem 15** (Springer, 1974)**.** *$\mathbb{C}[W]$ and $A$ have natural, isomorphic $W \times C$-actions, where $C$ is cyclically generated by a regular element.*

Ignoring the $C$ piece in the theorem gives a classic result of Borel: the coinvariant algebra is often thought of as a graded analogue of the regular representation. As for the promised generalization, we have:

**Theorem 16** (Reiner-Stanton-White)**.** *The triple*

$$(W/W', C, \mathrm{Hilb}(A^{W'}; q))$$

*exhibits the CSP.*

For an example of the CSP of a very different flavor, Rhoades proved that the "promotion" action on $\mathrm{SYT}((n^m))$ using a $q$-analogue of the hook length formula,

$$f^\lambda(q) := \frac{[n]_q!}{\prod_{(i,j)\in\lambda}[h_{i,j}]_q},$$

exhibits the CSP. In another vein, Sagan-Shareshian-Wachs showed that $\langle(12\cdots n)\rangle$ acting by conjugation on the subset of $S_n$ consisting of permutations with cycle type $\lambda$ using the $\mathrm{maj} - \mathrm{exc}$ generating function exhibits the CSP. In one more direction, one may generalize the notion of cyclic sieving from cyclic groups to abelian groups ($\equiv$ products of cyclic groups) by keeping track of multiple statistics.

(Notes to self: this was maybe 75 minutes; cut out direct proof paradigm.)