Cyclic Sieving Phenomenon

Donguk Rhee
University of Waterloo
durhee@uwaterloo.ca

Abstract: The cyclic sieving phenomenon is an interesting phenomenon with connections to enumeration and representation theory. We will study the canonical example of multisets and present two proofs that illustrate these connections. We conclude by looking at a few other examples of the cyclic sieving phenomenon. Much of this paper is based on Sagan's survey.

1 Introduction

1.1 Definition of the CSP

Suppose that we have a cyclic group C acting on a set X. In combinatorics, it is natural to ask the number of fixed points: $|X^g| = |\{x \in X : gx = x\}|$. In their 2004 paper Reiner, Stanton, and White describe a phenomenon where one polynomial encodes all numbers of fixed elements by cyclic actions [RSW04]. This is called the cyclic sieving phenomenon.

Definition 1.1. Let $C = \{1, c, c^2, \cdots, c^{n-1}\}$ be a finite cyclic group acting on a finite set X. Let $\zeta = e^{\frac{2\pi i}{n}} \in \mathbb{C}$ be a root of unity of order n and let $f(q)$ be a polynomial with non-negative integer coefficients. We say that the triple $(X, C, f(q))$ *exhibits the cyclic sieving phenomenon (CSP)* if for any non-negative integer d, we have that the fixed point set cardinality $|X^{c^d}|$ is equal to the polynomial evaluated at $f(\zeta^d)$.

Remark 1.1: A trivial remark one needs to make is that $f(1)$ is equal to the number of elements in X.

Remark 1.2: Having an action by $C = \{1, c\}$ is equivalent to having an involution on X (i.e. a bijection that is its own inverse). Then the CSP corresponds to the result given by Stembridge in 1993 [Ste94]. In fact, Stembridge's result was the motivation of the CSP.

Remark 1.3: It is easy to see that $f(q)$ is unique up to the polynomial $x^n - 1$. If $(X, C, f_1(q))$ and $(X, C, f_2(q))$ exhibit the CSP, then $f_1(q) - f_2(q)$ is a polynomial that has $1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$ as roots, so $x^n - 1$ divides $f_1(q) - f_2(q)$.

Remark 1.4: If $f(q) = \sum_{k=0}^{n-1} a_k q^k$ where a_k is the number of C-orbits in X with stabilizer order (i.e. the size of C divided by the size of the orbit) dividing k, then

$$f(q) = \sum_{k=0}^{n-1} a_k q^k = \sum_{\text{orbit } O} 1 + q^{|C|/|O|} + q^{2|C|/|O|} + \cdots + q^{(|O|-1)|C|/|O|}.$$

If $f(q)$ is evaluated at $q = \zeta^d$, $1 + q^{|C|/|O|} + q^{2|C|/|O|} + \cdots + q^{(|O|-1)|C|/|O|}$ is $|O|$ if the order of ζ^d divides $|C|/|O|$ and 0 otherwise. Therefore, $f(\zeta^d) = |X^{c^d}|$ and $(X, C, f(q))$ exhibits the CSP. Combined with the above remark, we now have existence and uniqueness of $f(q)$.

Note that in many situations, these polynomials are naturally associated to the combinatorial structure of the set X; $f(q)$ is often a generating function associated with X.

Before we present an example of the CSP, let us quickly introduce couple tools we will use.

1.2 Prerequisite: q-analogs

Define the the *q-analog of the number n* as $[n]_q = 1 + q + q^2 + \cdots + q^{n-1}$. Let $[n]_q! = [1]_q[2]_q \cdots [n]_q$ be the *q-analog of* $n!$ and $\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}$ be the *q-analog of* $\binom{n}{k}$. These q-analogs are polynomials in q and tend to our ordinary numbers, factorials, and binomial coefficients as q approaches 1.

The q-analog of a binomial coefficient adds extra information to each object the binomial coefficient is counting. For example, if $\binom{n}{k}$ counts the number of monotonic lattice path inside the $(n-k) \times k$ box, then its q-analog also takes the number of boxes that are above the path into account.

We remarked that $f(1) = |X|$ when $(X, C, f(q))$ exhibits the CSP. In many cases, f turns out to be the q-analog of the number of elements in X.

1.3 Prerequisite: representation theory

Let V be a complex vector space. The group of invertible linear maps from V to itself is denoted as $GL(V)$. A group homomorphism $[\cdot] : G \to GL(V)$ is called a *representation*. Representations provide a way to study group theory using linear algebra.

In this article, we will use representations when G acts on V. Then there is a natural choice of representation: $[g] : v \mapsto gv$.

Given a choice of basis B on V, $[g]$ can be written in a matrix form. Define the *character* of a representation to be $\chi : G \to \mathbb{C}$ such that $\chi(g) = \mathrm{tr}[g]$. Since the trace is independent of the choice of basis, $\chi(g)$ is well-defined.

Example 1.1. If $V = \mathbb{C}^3$ and $g = (1\ 2) \in S_3$ acts on V by switching the first two components, then the matrix form of g in the standard basis is

$$[g]_B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and $\chi(g)$ is 1.

2 Canonical Example

2.1 Example of multisets

The canonical example of a combinatorial structure exhibiting the CSP is the example of multisets. Let positive integers n and k be fixed. A k-multiset of $[n] = \{1, 2, 3, \cdots, n\}$ is an unordered family of k elements of $[n]$ where repetitions are allowed. For example, the set of 3-multisets of [3] is $\{111, 222, 333, 112, 113, 221, 223, 331, 332, 123\}$. Let X be the set of k-multisets of $[n]$.

Let C be the cyclic subgroup of S_n generated by the cycle $c = (1\ 2\ 3\ \cdots\ n)$. C acts naturally on X: if $M = m_1 m_2 \cdots m_k$ is a multiset, then $gM = g(m_1)g(m_2)\cdots g(m_k)$ where $g \in C$. For example, $(1\ 2\ 3)223 = 331$.

There are $\binom{n+k-1}{k}$ such multisets. For our polynomial, we take the q-analog. Define $f(q)$ as $\binom{n+k-1}{k}_q$.

Theorem 2.1. $(X, C, f(q))$ defined as above exhibits the cyclic sieving phenomenon.

Example 2.1. Let $n = 3$ and $k = 3$. $f(q)$ is

$$\binom{3+3-1}{3}_q = \frac{(1+q+q^2+q^3)(1+q+q^2+q^3+q^4)}{1(1+q)} = 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6.$$

$|X^{id}| = |X|$ is 10. $f(\zeta^0) = f(1) = 10$, so $|X^{id}| = f(\zeta^0)$. $|X^{(1\ 2\ 3)}|$ is 1 since 123 is the only fixed multiset. $f(\zeta^1) = 1 + \zeta + 2\zeta^2 + 2\zeta^3 + 2\zeta^4 + \zeta^5 + \zeta^6 = 4 + 3\zeta + 3\zeta^2 = 1$ since $\zeta^3 = 1$ and $1 + \zeta + \zeta^2 = 0$. Therefore, $|X^{(1\ 2\ 3)}| = f(\zeta)$.

2.2 Proof by direct evaluation

One can prove the above theorem by simply evaluating both $|X^{c^d}|$ and $f(\zeta^d)$ explicitly. The following two lemmas show the evaluation of these two sides.

Lemma 2.1. Let o be the order of c^d. Then $|X^{c^d}| = \binom{n/o+k/o-1}{k/o}$ if $o|k$ and 0 otherwise.

Proof. If $g = c_1 c_2 \cdots c_t \in C$ is the cycle decomposition of $g \in C$, then $x \in X$ is fixed under the action by g if and only if x can be written as disjoint union of the cycles c_i with repetition allowed. For example, if $g = c^2 = (1\,2\,3\,4\,5\,6)^2 = (1\,3\,5)(2\,4\,6)$, then the multisets fixed by g must have the form $1^a 3^a 5^a 2^b 4^b 6^b$. This claim is easy to check.

c^d decomposes into n/o cycles of size o, so no k-multiset is fixed if o does not divide k. If it does, then one must choose k/o cycles with repetition allowed to form a multiset of size k that is fixed under the action by c^d. Therefore, $|X^{c^d}| = \binom{n/o+k/o-1}{k/o}$. □

Lemma 2.2. Let o be the order of ζ^d. Then $f(\zeta^d) = \binom{n/o+k/o-1}{k/o}$ if $o|k$ and 0 otherwise.

Proof. Note that for any non-negative integer a and b, $\frac{[ao+k]_q}{[bo+k]_q}$ is $\frac{1+q+q^2+\cdots+q^{ao+k-1}}{1+q+q^2+\cdots+q^{bo+k-1}}$. When $q = \zeta^d$, this is equal to $\frac{1+q^o+q^{2o}+\cdots+q^{(a-1)o}}{1+q^o+q^{2o}+\cdots+q^{(b-1)o}} = \frac{a}{b}$ if $k = 0$. Otherwise, it is $\frac{1+q+q^2+\cdots+q^{k-1}}{1+q+q^2+\cdots+q^{k-1}} = 1$.

If o does not divide k, then $f(q) = \binom{n+k-1}{k}_q$ has more $[o]_q$ factors in the numerator than the denominator, so $f(\zeta^d) = 0$. Otherwise,

$$\begin{aligned}
f(\zeta^d) = \binom{n+k-1}{k}_{\zeta^d} &= \frac{[n]_{\zeta^d}}{[k]_{\zeta^d}} \frac{[n+1]_{\zeta^d}}{[1]_{\zeta^d}} \cdots \frac{[n+k-1]_{\zeta^d}}{[k-1]_{\zeta^d}} \\
&= \frac{n}{k} \cdot 1 \cdot 1 \cdots 1 \cdot \frac{n+o}{o} \cdot 1 \cdot 1 \cdots 1 \cdot \frac{n+2o}{2o} \cdots \\
&= \frac{n/o}{k/o} \cdot \frac{n/o+1}{1} \cdot \frac{n/o+2}{2} \cdots \\
&= \binom{n/o+k/o-1}{k/o},
\end{aligned}$$

which is what we wanted. □

By these two lemmas, we conclude that $|X^{c^d}| = f(\zeta^d)$. Therefore, $(X, C, f(q))$ exhibits the cyclic sieving phenomenon.

2.3 Proof by representation theory

The previous proof is elementary, but it does not tell us much about why the equality holds. We now present an another proof that uses representation theory and provides more insight into our situation.

The main idea of the proof is to evaluate a character using two different bases. In one basis, the character will be the number of fixed elements, which is combinatorial information. In another basis, the character will be algebraically realized as a polynomial.

Proof of Theorem 2.1. Given a set $S = \{s_1, s_2, \cdots, s_n\}$, we define a complex vector space

$$\mathbb{C}S = \{c_1 s_1 + c_2 s_2 + \cdots + c_n s_n | c_i \in \mathbb{C}\}.$$

An element $g \in S_n$ acts naturally on $\mathbb{C}[n]$: $g(c_1\mathbf{1} + c_2\mathbf{2} + \cdots + c_n\mathbf{n}) = c_1 g(\mathbf{1}) + c_2 g(\mathbf{2}) + \cdots + c_n g(\mathbf{n})$. Define $\mathrm{Sym}_k(n)$ as $\mathbb{C}X$ where X is the set of multisets of $[n]$ of size k.

Clearly, X is the standard basis of $\mathrm{Sym}_k(n)$. A diagonal entry of $[g]_X$ is 1 if the multiset $M \in X$ is fixed by g and 0 otherwise. Therefore, $\chi(g^d) = \mathrm{tr}[g^d]_X = |X^{g^d}|$.

Example 2.2. If $n = 3$ and $k = 3$ as before and $g = c^1 = (1\,2\,3)$, then

$$\begin{array}{lllll} g(111) = 222, & g(222) = 333, & g(333) = 111, & g(112) = 223, & g(113) = 221, \\ g(221) = 332, & g(223) = 331, & g(331) = 112, & g(332) = 113, & g(123) = 123. \end{array}$$

So $[g]_{\{111,222,333,112,113,221,223,331,332,123\}}$ is equal to

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Only one diagonal entry is 1 because only 123 is fixed under the action g. Therefore, $\chi(g) = 1$.

We want another way of evaluating this character $\chi(g)$, so that it yields $f(\zeta^d)$. Let $c = (1\,2\,3\,\cdots\,n) \in S_n$. c^n is the identity in S_n, so $[c]^n$ is also the identity in $GL(\mathbb{C}[n])$. Thus, the characteristic polynomial of $[c]$ is $x^n - 1$, which has n distinct roots: $x_1 = 1, x_2 = \zeta, x_3 = \zeta^2, \cdots, x_n = \zeta^{n-1}$. Therefore, there must be a basis $B = \{b_1, b_2, \cdots, b_n\}$ of $\mathbb{C}[n]$ such that $[c] \in GL(\mathbb{C}[n])$ is diagonalized with respect to B and has $x_1, x_2 \ldots, x_n$ on the diagonal. Note $[c^d]_B = \mathrm{diag}(x_1^d, x_2^d, \cdots, x_n^d)$. Let B' be the set of k-multisets of B, then B' is another basis for $\mathrm{Sym}_k(n)$ (this is a property of $\mathrm{Sym}_k(n)$).

We now evaluate the character of $g = c^d$ with the basis B'.

$$g(b_{i_1} b_{i_2} \cdots b_{i_k}) = g(b_{i_1}) g(b_{i_2}) \cdots g(b_{i_k}) = x_{i_1}^d x_{i_2}^d \cdots x_{i_k}^d b_{i_1} b_{i_2} \cdots b_{i_k}.$$

So it follows that the diagonal entries of $[g]_{B'}$ are $x_{i_1}^d x_{i_2}^d \cdots x_{i_k}^d$ and the trace of $[g]$ is $\sum_{1 \le i_1 \le i_2 \le \cdots \le i_k \le n} x_{i_1}^d x_{i_2}^d \cdots x_{i_k}^d$.

The polynomial $\sum_{1 \le i_1 \le i_2 \le \cdots \le i_k \le n} y_{i_1}^d y_{i_2}^d \cdots y_{i_k}^d$ is called the *complete homogeneous symmetric polynomial* in n variables of degree k and it is denoted by $h_k(y_1^d, y_2^d, \cdots, y_n^d)$.

It remains to show that $h_k(1, q, q^2, \cdots, q^{n-1})$ is equal to $\binom{n+k-1}{k}_q$. One can check that

$$h_k(1, q, q^2, \cdots, q^{n-1}) = h_k(1, q, q^2, \cdots, q^{n-2}) + q^{n-1} h_{k-1}(1, q, q^2, \cdots, q^{n-1})$$

and

$$\binom{n+k-1}{k}_q = \binom{n+k-2}{k}_q + q^{n-1} \binom{n+k-2}{k-1}_q.$$

Since the recursions are identical, the equality follows by induction. □

Example 2.3. Again picking $n = 3$, $k = 3$, and $g = c^1 = (1\,2\,3)$,

$$\begin{array}{rrr} g(b_1b_1b_1) = x_1^3b_1b_1b_1, & g(b_2b_2b_2) = x_2^3b_2b_2b_2, & g(b_3b_3b_3) = x_3^3b_3b_3b_3, \\ g(b_1b_1b_2) = x_1^2x_2b_1b_1b_2, & g(b_1b_1b_3) = x_1^2x_3b_1b_1b_3, & g(b_2b_2b_1) = x_2^2x_1b_2b_2b_1, \\ g(b_2b_2b_3) = x_2^2x_3b_2b_2b_3, & g(b_3b_3b_1) = x_3^2x_1b_3b_3b_1, & g(b_3b_3b_2) = x_3^2x_2b_3b_3b_2, \\ g(b_1b_2b_3) = x_1x_2x_3b_1b_2b_3. & & \end{array} .$$

So $[g]_{\{b_1b_1b_1, b_2b_2b_2, b_3b_3b_3, b_1b_1b_2, b_1b_1b_3, b_2b_2b_1, b_2b_2b_3, b_3b_3b_1, b_3b_3b_2, b_1b_2b_3\}}$ is equal to

$$\begin{bmatrix} x_1^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_2^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & x_3^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_1^2x_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x_1^2x_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x_2^2x_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x_2^2x_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_3^2x_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_3^2x_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_1x_2x_3 \end{bmatrix}.$$

Therefore, $\chi(g) = x_1^3 + x_2^3 + x_3^3 + x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 + x_1x_2x_3 = h_3(x_1, x_2, x_3)$.

3 Other Examples

3.1 Subsets of [n]

We have seen that multisets exhibit the csp. Subsets similarly exhibit the csp.

Theorem 3.1.

$$\left(\{S \subseteq [n] : |S| = k\}, \langle (1\,2\,\cdots\,n) \rangle, \binom{n}{k}_q \right)$$

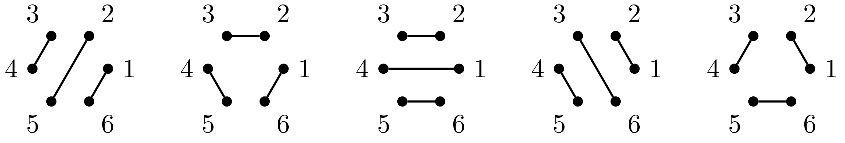
exhibits the cyclic sieving phenomenon.

Proof. The proof is similar to the proof of the multiset case, but it is more technical. □

3.2 Catalan numbers

A *matching* is a graph G with vertex set $[2n]$ and n edges, no two of which share a common vertex. The matching is *non-crossing* if it does not contain a pair of edges ab and cd such that $a < c < b < d$. It is equivalent to say that if the vertices are arranged in order around a circle, no two edges intersect. The nth Catalan number, $C_n = \frac{1}{n+1}\binom{2n}{n}$, is the number of non-crossing matchings of size $2n$.

Example 3.1. $C_3 = 5$.



Rotation by π/n is an action on non-crossing matchings.

Theorem 3.2. Let X be the set of non-crossing matchings of size $2n$ and let R be a rotation by π/n. Then

$$\left(X, \langle R\rangle, \frac{1}{[2n+1]_q}\binom{2n}{n}_q\right)$$

exhibits the cyclic sieving phenomenon.

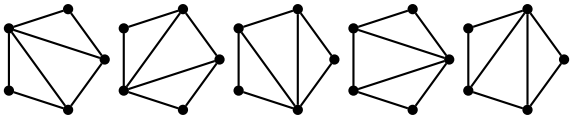
For readers who are familiar with Tableaux theory: this result is a special case of a csp result on rectangular tableaux, which says that if $X = \{\text{standard Young tableaux of shape } n \times d\}$ then

$$(X, \langle \text{jeu-de-taquin promotion}\rangle, \text{q-analog of hook length formula})$$

exhibits the csp. The Catalan case arises when $d = 2$. This result can be found in Rhoades' paper [Rho10].

There are other interesting cyclic actions one can consider on Catalan combinatorics. We end by showing one other cyclic action that exhibits the csp. It is well known that the number of triangulations of a regular $n+2$-gon is C_n.

Example 3.2. $C_3 = 5$



Rotation by $2\pi/(n+2)$ is an action on triangulations.

Theorem 3.3. Let X be the set of triangulations of a regular $n+2$-gon and R be a rotation by $2\pi/(n+2)$. Then

$$\left(X, \langle R\rangle, \frac{1}{[2n+1]_q}\binom{2n}{n}_q\right)$$

exhibits the cyclic sieving phenomenon.

References

[Rho10] Brendon Rhoades, *Cyclic sieving, promotion, and representation theory*, Journal of Combinatorial Theory Series A **117** (2010), 38–76.

[RSW04] V. Reiner, D. Stanton, and D. White, *The cyclic sieving phenomenon*, Journal of Combinatorial Theory Series A **108** (2004), 17–50.

[Ste94] John R. Stembridge, *On minuscule representations, plane partitions and involutions in complex lie groups*, Duke Mathematical Journal **73** (1994), 469–490.