Cyclic Sieving On Cyclic Codes

Alex Mason
University of Washington, Seattle

Shruthi Sridhar
Princeton University

Advisor: Dr. Victor Reiner
University of Minnesota, Twin Cities

Abstract

The *Cyclic Sieving Phenomenon (CSP)* has been observed in many cases where a cyclic group C_n acts on a finite set. In particular, it gives a generating function that counts the number of fixed points of the action.

James Propp proposed the question: Do Cyclic Codes exhibit CSP? We show that, for Dual Hamming codes over $\mathbb{F}_2, \mathbb{F}_3$, two important Mahonian polynomials are cyclic sieving polynomials.

Cyclic Sieving Phenomenon

A triple $(X, X(t), C)$ consisting of

- a finite set X
- a cyclic group $C = \{1, c \dots c^{n-1}\}$ permuting X
- a polynomial $X(t)$ in $\mathbb{Z}[t]$

is said to exhibit the *Cyclic Sieving Phenomenon* (or CSP) if for every c^d in C, the number of x in X having $c^d(x) = x$ is given by the substitution $[X(t)]_{t=\zeta^d}$ where $\zeta = e^{2\pi i/n}$, or any primitive n^{th} root of unity.

Example:
X is the set of triangulations of an $n+2$-gon, C has order $n+2$ acting by cyclic rotation on $\{1, 2, \dots n+2\}$ inducing an action on X. Then, $X(q) = C_n(q)$, the q-analog of the n^{th} Catalan number.

Suppose $n = 4$. We have $X(q) = 1+q^2+q^3+2q^4+q^5+2q^6+q^7+2q^8+q^9+q^{10}+q^{12}$. When we plug in $q = 1$, we get 14, which is all the triangulations of a $6-gon$ (fixed by 1). When we plug in $q = \zeta_6^2$ we get 2 triangulations fixed by $e^{2\pi i/3}$ as below:

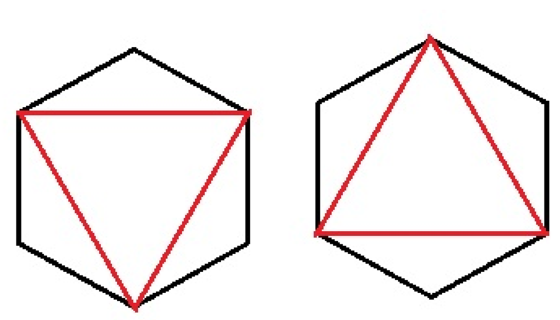

Fig. 1: Triangulations fixed by 120° rotation

Cyclic Codes

A cyclic code $\mathcal{C}$ of length n is a linear subspace of $\mathbb{F}_q^n$ stable under the action of the cyclic group $C =< c >\cong \mathbb{Z}/n\mathbb{Z}$ which acts by cyclically shifting codewords w as follows:

$$c(w_1, w_2, \dots, w_n) = (w_2, w_3, \dots, w_n, w_1)$$

The repetition code: $\mathcal{C} = \{(k, k, \dots k) : k \in \mathbb{F}_q\}$

The parity check code: $\mathcal{C} = \{(w_1, w_2, \dots, w_n) \in \mathbb{F}_q^n : \sum w_i = 0\}$

Generating Polynomials

One has the following isomorphism:

$$\begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x]/(x^n-1) \\ w = (w_1, \dots, w_n) & \longmapsto & \sum_{i=1}^n w_i x^{i-1} \end{array}$$

Any cyclic code $\mathcal{C}$ will be an ideal of this ring, which is a Principal Ideal Ring. Thus, the ideal has a single *generating polynomial* $g(x)$.

$$\mathcal{C} \cong \{h(x)g(x) \in \mathbb{F}_q[x]/(x^n-1)\}$$

where $\deg(h(x)) < n - \deg(g(x))$

The repetition code is generated by $1+x+\dots+x^{n-1}$

Hamming codes are those generated by primitive polynomials $g(x)$.

Dual Hamming Codes are generated by $\dfrac{x^n-1}{g(x)}$

Primitive Polynomials

An irreducible polynomial $g(x)$ of degree k over $\mathbb{F}_q$ is *primitive* if the smallest integer n such that $g(x) \mid x^n - 1$ is $n = q^k - 1$.

Note: Any irreducible polynomial $f(x)$ of degree k will divide $x^{q^k-1} - 1$.

Primitive polynomials over $\mathbb{F}_2$ of degree 4:

$$\begin{aligned} x^{15} - 1 = &(x+1)(x^2+x+1)(x^4+x+1) \\ &(x^4+x^3+1)(x^4+x^3+x^2+x+1) \end{aligned}$$

x^4+x+1 and x^4+x^3+1 are primitive while $x^4+x^3+x^2+x+1$ is not because it divides x^5-1.

Question

Which special polynomials are cyclic sieving polynomials for Dual Hamming Codes?

Mahonian polynomials

Two important Mahonian polynomials:

$$X^{\mathrm{maj}}(t) = \sum_{w\in\mathcal{C}} t^{\mathrm{maj}(w)} \quad \text{and} \quad X^{\mathrm{inv}}(t) = \sum_{w\in\mathcal{C}} t^{\mathrm{inv}(w)}$$

where

$$\mathrm{maj}(w) := \sum_{i: w_i > w_{i+1}} i$$

$$\mathrm{inv}(w) := \#\{(i,j) : 1 \le i < j \le n \text{ and } w_i > w_j\}$$

Theorem 1

For $q = 2, 3$, the triple $(X, X^{\mathrm{maj}}(t), C)$ always gives a CSP for dual Hamming codes X over $\mathbb{F}_q$.

Theorem 2

For $q = 2$, the triple $(X, X^{\mathrm{inv}}(t), C)$ always gives a CSP for dual Hamming codes X over $\mathbb{F}_q$.

Proof sketch

We show that the cyclic group action on non zero Dual Hamming Codes is free and transitive. Thus, the cyclic sieving polynomial is 1 for all non trivial roots of unity.

We make the observation that:

$$\mathrm{maj}(c(w)) \equiv \mathrm{maj}(w) + \mathrm{cdes}\,(w) \pmod n$$

where $\mathrm{cdes}(w)$ is the number of cyclic descents of w.

$$\begin{aligned} X^{\mathrm{maj}}(t) &= t^{\mathrm{maj}(0)} + \sum_{w\in\mathcal{C}\setminus\{0\}} t^{\mathrm{maj}(w)} \\ &= 1 + t^{\mathrm{maj}(w_0)} \sum_{i=0}^{n-1} (t^{\mathrm{cdes}(w_0)})^i \end{aligned}$$

Proof Sketch (contd..)

Thus we need gcd(n,cdes(w_0)) = 1.
We then use the following lemma, proved by studying the *Linear Feedback Shift Register* (LFSR) operator for the primitive polynomial $g(x)$

Lemma

For any primitive polynomial $g(x)$ over $\mathbb{F}_q$, the cyclic descents in the coefficient sequence of $\frac{x^{q^k-1}-1}{g(x)}$ is exactly $\frac{(q-1)}{2} q^{k-1}$.

Future Directions

- Which other Cyclic Codes exhibit the Cyclic Sieving Phenomenon?
- For what other cyclic actions are the Mahonian polynomials the cyclic sieving polynomial?

References

[1] A. Berget, S.-P. Eu, and V. Reiner, Constructions for cyclic sieving phenomena, *SIAM J. Discrete Math.* **25** (2011), 1297–1314.

[2] V. Reiner, D. Stanton, and D. White. The cyclic sieving phenomenon, *J. Combin. Theory Ser. A* **108** (2004), 17–50.

Acknowledgements

This research was performed as a part of the 2017 University of Minnesota, Twin Cities Combinatorics REU, and was supported by NSF RTG grant DMS-1148634 and by NSF grant DMS-1351590. We would like to thank Victor Reiner for his mentorship and Craig Corsi for his helpful advice.