CYCLIC SIEVING FOR CYCLIC CODES

ALEX MASON, VICTOR REINER, SHRUTHI SRIDHAR

Abstract. These are notes on a preliminary follow-up to a question of Jim Propp, about cyclic sieving of cyclic codes. We show that two of the Mahonian polynomials are cyclic sieving polynomials for certain Dual Hamming Codes: X^{maj} and X^{inv} for $q = 2, 3$ and $q = 2$, respectively.

1. Introduction

The Cyclic Sieving Phenomenon has been observed in many cases where a cyclic group acts on a finite set. In particular, it gives a generating function that counts the number of fixed points of the action. This phenomenon been studied in detail in [1] and [2].

On May 9, 2017, Jim Propp asked the following question on the "Dynamic algebraic combinatorics" list-server:

`Has anyone tried applying cyclic sieving to cyclic codes?`

In section 2, we describe Jim's question in detail with necessary preliminaries. Our main theorem is prove in section 3. We show when the Mahonian polynomials X^{maj} and X^{inv} are cyclic sieving polynomials (CSP's) for Dual Hamming Codes.

2. Preliminaries

Recall an $\mathbb{F}_q$-linear code $\mathcal{C}$ of length n is a subspace of $\mathbb{F}_q^n$, and is *cyclic* if it is also[1] stable under the action of a cyclic group $C = \{e, c, c^2, \ldots, c^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$ whose generator c cyclically shifts codewords w as follows:

$$c(w_1, w_2, \ldots, w_n) = (w_2, w_3, \ldots, w_n, w_1).$$

It is convenient to rephrase this using the $\mathbb{F}_q$-vector space isomorphism

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

After identifying a code $\mathcal{C} \subset \mathbb{F}_q^n$ with its image under the above isomorphism, the $\mathbb{F}_q$-linearity of $\mathcal{C}$ together with the cyclic condition is equivalent to $\mathcal{C}$ forming an *ideal*

Date: May 18, 2017.

[1]In principle, one can consider subsets $\mathcal{C}$ of $\mathbb{F}_q^n$ that are not linear subspaces but stable under cyclic shifts as cyclic codes, but we will ignore these here.

within the ring $\mathbb{F}_q[x]/(x^n-1)$. Since this is a principal ideal ring, $\mathcal{C}$ is always the set $(g(x))$ of all multiples of some *generating polynomial* $g(x)$. This means that

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

and hence one has the relation

$$k := \dim_{\mathbb{F}_q} \mathcal{C} = n - \deg(g(x)).$$

In this setting, the *dual code* $\mathcal{C}^\perp$ inside $\mathbb{F}_q^n$ is also cyclic, with generating polynomial

$$g^\perp(x) := \frac{x^n-1}{g(x)}$$

sometimes called the *parity check polynomial* for the primal code $\mathcal{C}$. Thus one has

$$k := \dim_{\mathbb{F}_q} \mathcal{C} = \deg(g^\perp(x)).$$

Example 2.1. The cyclic code $\mathcal{C}$ having $g^\perp(x) = 1 + x + x^2 + \cdots + x^{n-1}$ is called the *parity check* code of length n (particularly when $q = 2$). As a vector space, it is the space of all vectors in $\mathbb{F}_q^n$ with coordinate sum 0. Its dual code $\mathcal{C}^\perp$ consisting of the scalar multiples of $g^\perp(x) = 1 + x + x^2 + \cdots + x^{n-1}$ is the *repetition code*.

Example 2.2. Recall that a degree k polynomial $f(x)$ in $\mathbb{F}_q[x]$ is called *primitive* if it is not only irreducible, but also has the property that the image of the variable x in the finite field $\mathbb{F}_q[x]/(f(x))$ has the maximal possible multiplicative order, namely $n := q^k - 1$. Equivalently, $f(x)$ is primitive when it is irreducible but divides none of the polynomials $x^d - 1$ for proper divisors d of n.

A cyclic code $\mathcal{C}$ generated by a primitive polynomial $g(x)$ in $\mathbb{F}_q[x]$ of degree k is called a *Hamming code* of length $n = q^k - 1$ and dimension $n - k$. Its dual $\mathcal{C}^\perp$ generated by $g^\perp(x) = \frac{x^n-1}{g(x)}$ is a *dual Hamming code* of length n and dimension k.

Definition 2.3. Recall that a triple $(X, X(t), C)$ X consisting of a finite set X, a cyclic group $C = \{e, c, c^2, \ldots, c^{n-1}\}$ permuting X, and 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 ζ is a primitive n^{th} root-of-unity.

Jim noted various CSP triples $(X, X(t), C)$ involving $X := \mathcal{C}$ a cyclic code in $\mathbb{F}_q^n$, with $C = \mathbb{Z}/n\mathbb{Z}$ acting as above, and $X(t)$ could be either generating function

$$X^{\mathrm{maj}}(t) := \sum_{w \in \mathcal{C}} t^{\mathrm{maj}(w)}, \text{ or}$$
$$X^{\mathrm{inv}}(t) := \sum_{w \in \mathcal{C}} t^{\mathrm{inv}(w)},$$

where the *inversion number* $\mathrm{inv}(w)$ and *major index* $\mathrm{maj}(w)$ are defined as follows[2]:

$$\mathrm{inv}(w) := \#\{(i,j) : 1 \leq i < j \leq n \text{ and } w_i > w_j\},$$
$$\mathrm{maj}(w) := \sum_{i : w_i > w_{i+1}} i.$$

Here are the codes mentioned by Jim as having such CSP's:

- All repetition codes $\mathcal{C}$ (trivially).
- All full codes $\mathcal{C} = \mathbb{F}_q^n$ (see Theorem 2.4 below).
- All parity check codes (see Theorem 2.4 below).
- All cyclic codes over $\mathbb{F}_2$ of length 7 (empirically, seeking an explanation).

The CSP for full and parity check codes turn out to be special cases of a general CSP for words, following from a result in [2], as pointed out in [1, Prop. 17]:

Theorem 2.4. *Let $\mathcal{C}$ be a collection of words of length n in a linearly ordered alphabet, stable under the symmetric group $\mathfrak{S}_n$ acting on the n positions.*

Then $(X, X(t), C)$ exhibits the CSP, where $X = \mathcal{C}$, with $X(t)$ the inv *or* maj *generating function for $\mathcal{C}$, and C the $\mathbb{Z}/n\mathbb{Z}$-action obtained by restriction from $\mathfrak{S}_n$.*

Note $\mathcal{C} = \mathbb{F}_q^n$ and parity check codes $\mathcal{C} = \{w \in \mathbb{F}_q^n : \sum_{i=1}^n w_i = 0\}$ are $\mathfrak{S}_n$-stable.

Jim Propp found that there was not always such a CSP, but wondered whether there are interesting examples, and suggested that perhaps the Hamming and dual Hamming codes might be good candidates.

3. Dual Hamming codes

Hamming codes do not always have the CSP, but conjecturally their duals do. Before stating a more precise conjecture, we first analyze for a cyclic code $\mathcal{C}$ the conditions under which $C = \mathbb{Z}/n\mathbb{Z}$ acts freely on $\mathcal{C} \setminus \{\mathbf{0}\}$, and when this action is simply transitive.

Proposition 3.1. *Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a cyclic code with parity check polynomial $g^\perp(x)$.*

Then the $\mathbb{Z}/n\mathbb{Z}$-action on $\mathcal{C} \setminus \{\mathbf{0}\}$ is free if and only if

$$\gcd(g^\perp(x), x^d - 1) = 1$$

for all proper divisors d of n.

Proof. First note that when a codeword w in $\mathcal{C}$ is fixed by some element $c^d \neq e$ in C, without loss of generality, d is a proper divisor of n. Note that this says the polynomial $h(x)g(x)$ representing w in $\mathbb{F}_q[x]/(x^n - 1)$ has the property that

$$x^d h(x)g(x) = h(x)g(x) \bmod x^n - 1$$

[2]Note that these definitions require a choice of a linear order on the alphabet $\mathbb{F}_q$, and it is not clear whether this choice should make a difference in the CSP.

or equivalently $(x^d-1)h(x)g(x)$ is divisible by x^n-1 in $\mathbb{F}_q[x]$. Canceling factors of $g(x)$, this is equivalent to saying $(x^d-1)h(x)$ is divisible by $g^\perp(x)$ in $\mathbb{F}_q[x]$. However, as discussed earlier, $h(x)$ can be chosen with degree strictly less than $k = \dim \mathcal{C} = \deg(g^\perp(x))$, so the existence of such a nonzero $h(x)$ would be equivalent to $g(x)$ sharing a common factor with x^d-1. □

Proposition 3.2. *Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a cyclic code of dimension k with parity check polynomial $g^\perp(x)$.*

Then the $\mathbb{Z}/n\mathbb{Z}$-action on $\mathcal{C} \setminus \{\mathbf{0}\}$ is simply transitive (that is, free and transitive) if and only if $\mathcal{C}$ is dual Hamming, that is, if and only if $n = q^k - 1$ and $g^\perp(x)$ is a primitive polynomial in $\mathbb{F}_q[x]$.

Proof. Since $k = \dim_{\mathbb{F}_q} \mathcal{C} = g^\perp(x)$, the cardinality $\#(\mathcal{C} \setminus \{\mathbf{0}\}) = q^k - 1$. Thus Proposition 3.1 implies $\mathcal{C} \setminus \{\mathbf{0}\}$ has free and transitive $\mathbb{Z}/n\mathbb{Z}$-action if and only if $n(= \#\mathbb{Z}/n\mathbb{Z}) = q^k - 1$ and $\gcd(g^\perp(x), x^d - 1) = 1$ for all proper divisors d of $q^k - 1$.

Now $g^\perp(x)$ divides into $x^{q^k-1}-1$, so it must factor as $g^\perp(x) = \prod_i f_i(x)$, where $f_i(x)$ are among the irreducible factors of $x^{q^k-1} - 1$. By definition of primitivity, the only such irreducible factors $f_i(x)$ which do not appear in any $x^d - 1$ for a proper divisor d of $q^k - 1$ are the primitive irreducible factors of degree k. But since $\deg(g^\perp(x)) = k$, this forces $g^\perp(x) = f_1(x)$ for one such primitive factor. □

Proposition 3.2 simplifies the analysis of a CSP for dual Hamming codes. When using the major index generating function $X^{\mathrm{maj}}(t)$, it turns out to hinge upon the behavior of the *cyclic descent* statistic

$$\mathrm{cdes}(w) := \#\{i \in \{1, 2, \ldots, n\} : w_i > w_{i+1}, \text{ where } w_{n+1} := w_1\},$$

applied to the word w_0 corresponding to its generator polynomial $g(x)$.

Proposition 3.3. *Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a k-dimensional dual Hamming code, so that one has $n = q^k - 1$, with generator $g(x)$, and w_0 in $\mathbb{F}_q^n$ its corresponding word. Then $(X, X^{\mathrm{maj}}(t), C)$ from before exhibits the CSP if and only* $\gcd(\mathrm{cdes}(w_0), n) = 1$.

Proof. Since the CSP involves evaluating $X(t)$ with t being various n^{th} roots-of-unity, one only cares about $X(t) \bmod t^n - 1$. Also, note that cyclically shifting w to $c(w)$ has a predictable effect on maj, namely

$$\mathrm{maj}(c(w)) = \begin{cases} \mathrm{maj}(w) + \mathrm{cdes}(w) & \text{if } w_n \leq w_1, \\ \mathrm{maj}(w) + \mathrm{cdes}(w) + n & \text{if } w_n > w_1, \end{cases}$$

and hence, in all cases, one has $\mathrm{maj}(c(w)) \equiv \mathrm{maj}(w) + \mathrm{cdes}(w) \bmod n$. Hence, as $\mathcal{C} \setminus \{\mathbf{0}\}$ is the free C-orbit of w_0, using $\equiv$ for equivalence modulo $t^n - 1$, one has

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

This gives a CSP if and only if $X^{\mathrm{maj}}(\zeta) = 1$ for all n^{th} roots-of-unity $\zeta \neq 1$. The above expression for $X^{\mathrm{maj}}(t) \bmod t^n - 1$ shows that this will occur if and only if all such ζ have $\zeta^{\mathrm{cdes}(w_0)} \neq 1$, that is, if and only if $\gcd(\mathrm{cdes}(w_0), n) = 1$. □

We come now to one of our main theorems.

Theorem 3.4. *Let $g^{\perp}(x)$ be a primitive irreducible polynomial of degree k in $\mathbb{F}_q[x]$, and let w_0 be the word in $\mathbb{F}_q^n$ corresponding to $g(x) = \frac{x^n-1}{g^{\perp}(x)}$, where $n := q^k - 1$.*

(a) *The value* $\mathrm{cdes}(w_0)$ *depends only on k and q, not on the choice of $g^{\perp}(x)$. In fact, this value is*
$$\mathrm{cdes}(w_0) = \frac{q-1}{2} \cdot q^{k-1}$$
(b) *The triple $(X, X^{\mathrm{maj}}(t), C)$ always gives a CSP for dual Hamming codes $X = \mathcal{C}$ when $q = p = 2, 3$, but not always for primes or prime powers $q > 3$.*
(c) *Furthermore, for $q = p = 2, 3$, an irreducible $f(x)$ in $\mathbb{F}_p[x]$ of degree k is primitive* **if and only if** *the word w_0 corresponding to $\frac{x^{p^k-1}-1}{f(x)}$ has* $\mathrm{cdes}(w_0) = \frac{p-1}{2} \cdot p^{k-1}$.

Before we prove the above theorem, we prove the following well known necessary and sufficient condition for primitive polynomials. Let $f(x) = x^k + c_{k-1}x^{k-1} + ... + c_0$ be an irreducible polynomial in $\mathbb{F}_q[x]$. Its associated Linear Feedback Shift Register (LFSR) is a linear map T from $(\mathbb{F}_q)^k \to (\mathbb{F}_q)^k$ that takes the vector $(x_0, x_1, ...x_{k-1}) \mapsto (x_1, ...x_{k-1}, x_k)$ where $x_k = -\sum_{i=0}^{k-1} c_i x_i$.

Lemma 3.5. *$f(x)$ is primitive $\iff$ LFSR has multiplicative order $q^k - 1$.*

Proof. The matrix for the transformation T is $M = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \dots & \dots & \\ & & \dots & \dots & \\ 0 & . & . & \dots & 1 \\ -c_0 & -c_1 & . & \dots & -c_{k-1} \end{bmatrix}$.
It is easy to see by induction on the degree of $f(x)$ that the characteristic polynomial is $(-1)^k f(\lambda)$. This is irreducible, hence the minimal polynomial is $f(T)$. We know $f(x) \Big| x^{q^k-1} - 1$, hence $T^{q^k-1} - I = 0$. Since $f(x)$ is primitive, there is no smaller d

such that $T^d = I$, hence T has order $q^k - 1$. The above statements are reversible giving us the converse.

□

Corollary 3.6. *Let* $\mathbf{x} \in (\mathbb{F}_q)^k \setminus \{\mathbf{0}\}$*, then the set* $\{\mathbf{x}, T\mathbf{x}...T^{n-2}\mathbf{x}\} = (\mathbb{F}_q)^k \setminus \{\mathbf{0}\}$*, where* T *is the LFSR associated to any primitive polynomial.*

Proof. Assume the contrary, that $\{\mathbf{x}, T\mathbf{x}...T^{n-2}\mathbf{x}\}$ is some proper subset of $(\mathbb{F}_q)^k \setminus \{\mathbf{0}\}$, so that $T^d\mathbf{x} = \mathbf{x}$ for some $d < n-1$. This would mean that T has an eigenvalue that is a d^{th} root of unity. However, all eigenvalues of T are roots of the primitive polynomial which have order $p^k - 1$ which is larger than d giving rise to a contradiction. □

Now we can prove the main theorem.

Proof. (of Theorem 3.4)

(a) Let $g^{\perp}(x) = c_0 + c_1x + ... + c_{k-1}x^{k-1} + x^k$. Let $\frac{x^n-1}{g^{\perp}(x)} = a_{n-1}x^{n-1} + ... + a_1x + a_0$, where $a_i \in \mathbb{F}_q = \{b_0, b_1, ..b_{q-1}\}$. Here, we implicitly assign some linear order on $\mathbb{F}_q$ and label the elements such that $b_i < b_{i+1}$. If $g^{\perp}(x)$ is primitive, then we want the number of cyclic **ascents** in the sequence $\rho = (a_{n-1}, .., a_1, a_0)$ to equal $\frac{(q-1)}{2}q^{k-1}$. (We are looking for cyclic ascents instead of cyclic descents because this word is the reverse of the word that gives the cyclic code.)

Let $(x_0, x_1, ...x_{k-1}) = (0, 0, ..., 1)$. We have $T(\mathbf{x}) = (x_1, ...x_{k-1}, x_k)$. Using this process, we obtain a sequence of length n: $(x_0, x_1, ...x_{n-1})$. When considered cyclically, every sequence of length k occurs as a subsequence by Corollary 3.6. We calculate the number of cyclic ascents in such a sequence by checking how many non-zero sequences of length end in an ascent. There are q^{k-2} ways to fill the first $k-2$ spots. Then the number of ascending pairs is $\frac{q(q-1)}{2}$, giving us a total of $\frac{(q-1)}{2}q^{k-1}$ sequences that end with an ascent.

Now we will show that this sequence $(x_0, x_1, ...x_{n-1})$ is the same as $\rho = (a_{n-1}, .., a_1, a_0)$. We need to check that $(x_0t^{n-1} + ... + x_{n-2}t + x_{n-1})(g^{\perp}(t)) = t^n - 1$. When $(q^{k-1} - 1) > m > k$ the coefficient of t^m is $x_{n-m-1}c_0 + x_{n-m}c_1 + ... + x_{n-m+k-2}c_{k-1} + x_{n-m+k-1}$. This is zero because $x_{n-m+k-1} = -(x_{n-m-1}c_0 + x_{n-m}c_1 + ... + x_{n-m+k-2}c_{k-1})$. For $k \geq m > 0$, the coefficient is $x_{n-m-1}c_0 + x_{n-m}c_1 + ... + x_{n-m+k-2}c_{m-1} + x_{n-1}c_m$. This is also 0, inductively, since it is equal to $-x_{n+k-m-1} = -x_{k-m-1} = 0$, since the LFSR sequence repeats with period n. This also gives us that the constant coefficient is -1.

(b) In the case that $p = 2, 3$, $\mathrm{cdes}(w_0) = \frac{(p-1)}{2}p^{k-1}$ is a power of p, and thus relatively prime to $n = p^k - 1$. By Proposition 3.3, X^{maj} is a CSP for the Dual Hamming Code.

(c) Suppose $f^{\perp}(x)$ has $\frac{(p-1)}{2}p^{k-1}$ descents and is not primitive, then, $f(x)\Big|x^d - 1$ for some proper divisor d of $p^k - 1$. This results in, $T^d = I$ making the sequence obtained from the LFSR repeat with a repeating part of length d. Thus the number

of descents is a multiple of $n = \frac{p^k-1}{d}$. This would mean n divides both $p^k - 1$ and $\frac{(p-1)}{2}p^{k-1}$ which is not possible for $p = 2, 3$. □

Remark 3.7. The assertion of Conjecture 3.4(c) fails for $q = 5$ at $k = 3$, and fails for $q = 7$ at $k = 2$.

However, the following holds for dual Hamming codes over $\mathbb{F}_2$.

Proposition 3.8. *For $q = 2$, the triple $(X, X^{\mathrm{inv}}(t), C)$ also always gives a CSP for dual Hamming codes $X = \mathcal{C}$.*

Proof. Let the dual Hamming code be generated by $g(x) = \frac{x^{p^k-1}-1}{g^{\perp}(x)}$ and $g^{\perp}(x)$, a primitive polynomial of degree k over $\mathbb{F}_p$. Then, by theorem () the sequence of coefficients of $g(x)$ have every possible non zero sequence of length k as a subsequence. This means there are $p^{k-1} - 1$ zeros and p^{k-1} ones. Let w be any non zero code in $\mathcal{C}$. We look at the number of inversions of c(w) for $p = 2$. We get:

$$\mathrm{inv}(c(w)) = \begin{cases} \mathrm{inv}(w) + 2^{k-1} - 1 & \text{if } w \text{ ends with 1} \\ \mathrm{inv}(w) - 2^{k-1} & \text{if } w \text{ ends with 0} \end{cases}$$

However, $2^{k-1} - 1$ and -2^{k-1} are equal mod $n = 2^k - 1$ and are coprime to n. Hence the set $\{\ \mathrm{inv}(c^i(w)) \ \big|\ i = 0, ...n-1\}$ is all of $\{0, 1, ...n-1\}$ making $X^{\mathrm{inv}}(t) = 1$ which thus has CSP. □

Remark 3.9. The assertion of Conjecture 3.8 fails for $q = 3$.

Remark 3.10. One might optimistically hope that any binary word w_0 in $\mathbb{F}_2^n$ has

$$\sum_{\text{cyclic shifts } w \text{ of } w_0} t^{\mathrm{maj}(w)} \equiv \sum_{\text{cyclic shifts } w \text{ of } w_0} t^{\mathrm{inv}(w)} \bmod t^n - 1.$$

Sadly, this is not always true. It even fails for some words with no cyclic symmetry. Of course, Conjecture 3.4(a,b) together with Conjecture 3.8 would show that it is true whenever w_0 corresponds to $\frac{x^{2^k-1}-1}{f(x)}$ with $f(x)$ primitive of degree k.

Question 3.11. *What about other famous cyclic codes, such as Reed-Solomon, BCH, Golay?*

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.

School of Mathematics, University of Minnesota, Minneapolis, MN 55455, USA
E-mail address: reiner@math.umn.edu