NOTES ON CSP FOR CYCLIC CODES

VICTOR REINER

ABSTRACT. These are notes on a preliminary follow-up to a question of Jim Propp, about cyclic sieving of cyclic codes.

1. JIM'S QUESTION

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?`

To explain, 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* 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 1.1. 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 $q = 2$). 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.*

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.

Example 1.2. 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 1.3. 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 2.1 below).
- All parity check codes (see Theorem 2.1 below).
- All cyclic codes over $\mathbb{F}_2$ of length 7 (empirically, seeking an explanation).

He 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.

2. Parity check codes

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 [3], as pointed out in [2, Prop. 17]:

Theorem 2.1. *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.

[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.

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

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

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 $x^d - 1$. $\square$

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. $\square$

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

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

and hence, in all cases, one has $\operatorname{maj}(c(w)) \equiv \operatorname{maj}(w) + \operatorname{cdes}(w) \bmod n$. 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

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

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

We come now to a remarkable conjecture.

Conjecture 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 $\operatorname{cdes}(w_0)$ depends only on k and q, not on the choice of $g^{\perp}(x)$.*
(b) *In fact, this value is*

$$\operatorname{cdes}(w_0) = \frac{p-1}{2} \cdot p^{k-1}$$

when q is a **prime** *p, not a prime power p^e with $e \geq 2$.*

Hence the triple $(X, X^{\operatorname{maj}}(t), C)$ always gives a CSP for dual Hamming codes $X = \mathcal{C}$ when $q = p = 2, 3$, but not always for primes $q = p \geq 5$.

(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 $\operatorname{cdes}(w_0) = \frac{p-1}{2} \cdot p^{k-1}$.*

Remark 3.5. When q is a prime power but not a prime, we haven't much tested the assertion of Conjecture 3.4(a) nor looked for a formula as in (b).

If Vic didn't make a computational error then when $q = 4$ and $k = 2$, *all* 6 of the irreducible quadratics $g^{\perp}(x)$ in $\mathbb{F}_4[x]$, even those that were not primitive, had the same $\operatorname{cdes}(w_0) = 5$ for w_0 corresponding to $g(x) = \frac{x^{15} - 1}{g(x)}$. On the other hand, this involved making a particular choice of a linear order on $\mathbb{F}_4$ to compute $\operatorname{cdes}(w_0)$..

Remark 3.6. The assertion of Conjecture 3.4(c) fails for $q = 5$ at $k = 3$, and fails for $q = 7$ at $k = 2$.

Here is another mystery that seems to occur just for $q = p = 2$.

Conjecture 3.7. *For $q = 2$, the triple $(X, X^{\operatorname{inv}}(t), C)$ also always gives a CSP for dual Hamming codes $X = \mathcal{C}$.*

Remark 3.8. The assertion of Conjecture 3.7 fails for $q = 3$.

Remark 3.9. 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 3.7 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 3.10. *What about other famous cyclic codes, such as Reed-Solomon, BCH, Golay?*

Question 3.11. *The cyclic descent statistic plays a role in the work of Ahlbach and Swanson* [1]*. Is their work relevant?*

References

[1] C. Ahlbach and J. Swanson, Refined cyclic sieving on words for the major index statistic, preprint 2017; poster at FPSAC 2017 forthcoming.

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

[3] 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