CYCLIC SIEVING FOR CYCLIC CODES

ALEX MASON, VICTOR REINER, AND SHRUTHI SRIDHAR

Abstract. Prompted by a question of Jim Propp, this paper examines the cyclic sieving phenomenon (CSP) in certain cyclic codes. For example, it is shown that, among dual Hamming codes over \( F_q \), the generating function for codedwords according to the major index statistic (resp. the inversion statistic) gives rise to a CSP when \( q = 2 \) or \( q = 3 \) (resp. when \( q = 2 \)). A byproduct is a curious characterization of the irreducible polynomials in \( F_2[x] \) and \( F_3[x] \) that are primitive.

1. Introduction

The Cyclic Sieving Phenomenon describes the following enumerative situation. One has a finite set \( X \) having the action of a cyclic group \( C = \langle c \rangle = \{1, c, c^2, \ldots, c^{n-1} \} \) of order \( n \), and a polynomial \( X(t) \) in \( \mathbb{Z}[t] \) that not only satisfies \( \#X = X(1) \), but furthermore every element \( c^d \) in \( C \) satisfies

\[
\# \{ x \in X : c^d(x) = x \} = [X(t)]_{t=(e^{2\pi i n})^d}.
\]

In this case, one says that the triple \( (X, X(t), C) \) exhibits the cyclic sieving phenomenon (CSP); see [8] for background and many examples. Frequently the polynomial \( X(t) \) is a generating function \( X_{\text{stat}}(t) := \sum_{x \in X} t^{\text{stat}(x)} \) for some combinatorial statistic \( X_{\text{stat}} \rightarrow \{0, 1, 2, \ldots\} \). Some of the first examples of CSPs (e.g., Theorem 3.1 below) arose for the cyclic \( n \)-fold rotation action on certain special collections \( X \) of words \( w = (w_1, \ldots, w_n) \) of length \( n \) in a linearly ordered alphabet, with \( X(q) = X_{\text{maj}}(t) \) or \( X_{\text{inv}}(t) \) being generating functions for the major index and inversion number statistics, defined as follows:

\[
\text{inv}(w) := \# \{(i, j) : 1 \leq i < j \leq n : w_i > w_j \},
\]

\[
\text{maj}(w) := \sum_{i : w_i > w_{i+1}} i.
\]

This prompted Jim Propp to ask the question [7] of whether there are such CSPs in which \( X \) is the set of codewords \( \mathcal{C} \) for a cyclic error-correcting code. He initially observed the following instances of CSP triples \( (X, X_{\text{stat}}(t), C) \) where \( X = \mathcal{C} \) is a cyclic code inside \( \mathbb{F}_q^n \), and \( C = \mathbb{Z}/n\mathbb{Z} \) acts as \( n \)-fold cyclic rotation of words, and either \( \text{stat} = \text{maj} \) or \( \text{stat} = \text{inv} \):

- all repetition codes (trivially),
- the full codes \( \mathcal{C} = \mathbb{F}_q^n \),
- all parity check codes, and
- all binary cyclic codes of length 7.
After a quick review of cyclic codes in Section 2, a few simple observations about CSPs for cyclic actions on words in Section 3 will explain all of the above CSPs, and a few more.

Section 4 addresses the more subtle examples of dual Hamming codes. Among other things, it shows that either $X^{maj}(t)$ or $X^{inv}(t)$ give rise to a CSP for all binary dual Hamming codes, while $X^{maj}(t)$ also works for all ternary Hamming codes. The analysis leads to a curious characterization (Theorem 4.5(ii)) of which irreducible polynomials in $\mathbb{F}_2[x]$ or $\mathbb{F}_3[x]$ are primitive polynomials.

2. Preliminaries

We briefly review here the notions of linear codes, cyclic codes, and the examples that we will consider; see, e.g., Garrett \cite{G} or Pless \cite{P} for more background. Recall an $\mathbb{F}_q$-linear code of length $n$ is an $\mathbb{F}_q$-linear subspace $C \subseteq \mathbb{F}_q^n$. One calls $C$ cyclic if it is also stable under the action of the 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

$$\begin{align*}
\mathbb{F}_q^n &\rightarrow \mathbb{F}_q[x]/(x^n - 1) \\
w = (w_1, \ldots, w_n) &\mapsto w_1 + w_2 x + w_3 x^2 + \cdots + w_n x^{n-1}.
\end{align*}$$

(2.1)

After identifying a code $C \subseteq \mathbb{F}_q^n$ with its image under the isomorphism in (2.1), the $\mathbb{F}_q$-linearity of $C$ together with cyclicity means that $C$ forms an ideal within the principal ideal ring $\mathbb{F}_q[x]/(x^n - 1)$. Hence $C$ is the set $(g(x))$ of all multiples of some generating polynomial $g(x)$. This means that

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

and therefore $k := \dim_{\mathbb{F}_q} C = n - \deg(g(x))$. The dual code $C^\perp$ of a linear code $C$ in $\mathbb{F}_q^n$ is defined as

$$C^\perp := \{v \in \mathbb{F}_q^n : 0 = v \cdot w = \sum_{i=1}^n v_i w_i\}.$$

One has that $C$ is cyclic with generator $g(x)$ if and only if $C^\perp$ is cyclic with generator $g^\perp(x) := \frac{x^{n-1}}{g(x)}$, called the parity check polynomial for the primal code $C$. This implies $k = \dim_{\mathbb{F}_q} C = \deg(g^\perp(x))$.

Example 2.1. The cyclic code $C$ 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 $C^\perp$ consisting of the scalar multiples of $g^\perp(x) = 1 + x + x^2 + \cdots + x^{n-1}$ is the repetition code. For example, the ternary ($q = 3$) repetition code $C^\perp$ and parity check code $C$ of length $n = 2$, and their respective generator polynomials $g^\perp(x), g(x)$ inside $\mathbb{F}_3[x]/(x^2 - 1)$, are

$$C^\perp = \{[0,0], [1,1], [2,2]\}, \quad \text{generated by} \quad g^\perp(x) = 1 + x,$n

$$C = \{[0,0], [1,2], [2,1]\}, \quad \text{generated by} \quad g(x) = \frac{x^2 - 1}{1+x} = 1 + 2x.$$

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 $\bar{x}$ 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 $C$ 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 $C^\perp$ generated by $\frac{x^{n-1}}{g(x)}$ is a dual Hamming code of length $n$ and dimension $k$. See Example 4.3 below for some examples with $q = 3$ (ternary codes) with $k = 2$ and length $n = 3^2 - 1 = 8$. 
Theorem 3.1. Let $C = \mathbb{F}_q^n$ or the parity check codes $C = \{w \in \mathbb{F}_q^n : \sum_{i=1}^n w_i = 0\}$, since both are $\mathfrak{S}_n$-stable inside $\mathbb{F}_q^n$. We first explain why the CSPs for full codes of length $n$ for every $\sigma$ in $\mathfrak{S}_n$. Then $(X, X^{\text{stat}}(t), C)$ exhibits the CSP, where either stat $= \text{maj}$ or stat $= \text{inv}$.

Note that Theorem 3.1 explains Propp’s observation of CSP triples involving either the full codes $C$ or the parity check codes $C = \{w \in \mathbb{F}_q^n : \sum_{i=1}^n w_i = 0\}$, since both are $\mathfrak{S}_n$-stable inside $\mathbb{F}_q^n$.

The next proposition analyzes how $\text{maj}(w)$ changes \footnote{A much more sophisticated analysis may be found in Ahlbach and Swanson \cite{2}.} when applying the cyclic shift $c$ to the word $w$, and similarly for $\text{inv}(w)$ if the alphabet $A$ is binary. In the latter case, we assume $A = \{0, 1\}$ has linear order $0 < 1$, and will refer to the Hamming weight $\text{wt}(w)$, as the number of ones in $w$. We also use another statistic on words $w$ in $A^n$, the number of cyclic descents

$$\text{cdes}(w) := \#\{i : 1 \leq i \leq n \text{ and } w_i > w_{i+1}\}$$

where we decree $w_{n+1} := w_1$ to understand the inequality $w_i > w_{i+1}$ when $i = n$. Lastly, define a $t$-analogue of the number $n$ by this geometric series: $[n]_t := 1 + t + t^2 + \cdots + t^{n-1} = \frac{t^n-1}{t-1}$. The following proposition is then straightforward to check from the definitions.

**Proposition 3.2.** Let $A$ be any linearly ordered alphabet, and $w$ a word in $A^n$.

(i) The statistic $\text{cdes}(w)$ is constant among all words within the $C$-orbit of $w$, and

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

(ii) In the binary case $A = \{0, 1\}$, one has

$$\text{inv}(c(w)) = \begin{cases} \text{inv}(w) + \text{wt}(w) & \text{if } w_n = 1, \\ \text{inv}(w) + \text{wt}(w) - n & \text{if } w_n = 0 \end{cases} \equiv \text{inv}(w) + \text{wt}(w) \mod n.$$  

The congruences modulo $n$ in Proposition 3.2 immediately imply the following.

**Proposition 3.3.** When $w$ in $A^n$ has free $C$-orbit, meaning that $\{w, c(w), c^2(w), \ldots, c^{n-1}(w)\}$ are all distinct, then one has the following congruence in $\mathbb{Z}[t]/(t^n - 1)$:

$$X^{\text{maj}}(t) \equiv t^{\text{maj}(w)} \cdot [n]_t^{\text{cdes}(w)} \mod t^n - 1.$$  

In the binary case, one has

$$X^{\text{inv}}(t) \equiv t^{\text{inv}(w)} \cdot [n]_t^{\text{wt}(w)} \mod t^n - 1.$$
The next corollary then explains Propp’s observation about CSPs for binary cyclic codes $X = C$ of length $n = 7$ using either $X^{\text{maj}}(t)$ or $X^{\text{inv}}(t)$. The key point is that 7 is prime. We will also frequently use the fact that the following three conditions are equivalent for positive integers $k, n$:

- $\gcd(k, n) = 1$.
- $t^k[n]_t ≡ [n]_t \mod t^n − 1$ for all nonnegative integers $\ell$.
- $t^k[n]_t$ vanishes upon evaluating $t$ at any $n$th root-of-unity that is not 1.

**Corollary 3.4.** When $n$ is prime, every $C$-stable subset $X \subset A^n$ gives rise to a CSP triple $(X, X^{\text{maj}}(t), C)$. If furthermore, $A = \{0, 1\}$, then one also has the CSP triple $(X, X^{\text{inv}}(t), C)$.

**Proof.** Since Proposition 3.3 implies the above sum is congruent modulo $t$, as in the proof of Corollary 3.4, for either statistic $\text{stat} = \text{maj}$ or $\text{stat} = \text{inv}$, the CSP holds if and only if $\gcd(n, \text{cdes}(w)) = 1$.

Remark 3.5. Note that Proposition 3.3 dashes any false hopes one might have that for binary words $w$ in $\{0, 1\}^n$, the distributions $\sum_{j=0}^{n-1} t^{\text{maj}(c^j(w))}$ and $\sum_{j=0}^{n-1} t^{\text{inv}(c^j(w))}$ are congruent modulo $t^n − 1$. This can fail for non-prime $n$ even when $w$ has a free $C$-orbit. For example, $w = (1, 0, 1, 1, 1, 1)$ has

$$\sum_{j=0}^{n-1} t^{\text{maj}(c^j(w))} \equiv t^5[6]_t \neq t^7[6]_t \equiv \sum_{j=0}^{n-1} t^{\text{inv}(c^j(w))} \mod t^6 − 1.$$ 

Our discussion of dual Hamming codes will use another consequence of Proposition 3.3.

**Corollary 3.6.** Suppose that a $C$-stable subset $X \subseteq A^n$ of words has all non-constant words in $X$ lying in a single free $C$-orbit, represented by the word $w$.

(i) Then $(X, X^{\text{maj}}(t), C)$ gives rise to a CSP triple if and only if $\gcd(n, \text{cdes}(w)) = 1$.

(ii) In the binary case, $(X, X^{\text{inv}}(t), C)$ gives rise to a CSP triple if and only if $\gcd(n, \text{wt}(w)) = 1$.

**Proof.** As in the proof of Corollary 3.3 for either statistic $\text{stat} = \text{maj}$ or $\text{stat} = \text{inv}$, the CSP holds if and only if $\sum_{j=0}^{n-1} t^{\text{stat}(c^j(w))}$ vanishes upon setting $t = \zeta_n^d$ for any $n$th root-of-unity $\zeta_n \neq 1$. Since Proposition 3.3 implies the above sum is congruent modulo $t^n − 1$ to $t^{\text{maj}(w)}[n]_{t^{\text{cdes}(w)}}$ when $\text{stat} = \text{maj}$, and to $t^{\text{inv}(w)}[n]_{t^{\text{wt}(w)}}$ in the binary case when $\text{stat} = \text{inv}$, the result follows. □
4. Dual Hamming codes

To understand when dual Hamming codes \( \mathcal{C} \) exhibit a CSP, it will help to have many ways to characterize them among cyclic codes. As a precursor step, it helps to first characterize the cyclic codes for which the cyclic action on nonzero codewords is free.

**Proposition 4.1.** A cyclic code \( \mathcal{C} \subset \mathbb{F}_q^n \) with parity check polynomial \( g^+(x) \) will have the \( C \)-action on \( \mathcal{C} \setminus \{0\} \) free if and only if \( \gcd(g^+(x), x^d - 1) = 1 \) for all proper divisors \( d \) of \( n \).

**Proof.** First note that, since \( C^n = 1 \), whenever a codeword \( w \) in \( \mathcal{C} \) is fixed by some element \( c^d \neq 1 \) in \( C \), without loss of generality, one may assume \( d \) is a proper divisor of \( n \); otherwise replace \( d \) by \( \gcd(d, n) \). When this happens, the polynomial \( h(x)g(x) \) representing \( w \) in \( \mathbb{F}_q[x]/(x^n - 1) \) has

\[
x^n h(x)g(x) \equiv h(x)g(x) \mod x^n - 1
\]

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 \((x^d - 1)h(x)\) being divisible by \( g^+(x) \) in \( \mathbb{F}_q[x] \). However, as discussed in Section 2, \( h(x) \) can be chosen with degree strictly less than \( k = \dim \mathcal{C} = \deg(g^+(x)) \), so the existence of such a nonzero \( h(x) \) is equivalent to \( g^+(x) \) sharing a common factor with \( x^d - 1 \). \( \square \)

The next result compiles various equivalent characterizations of the primitive polynomials within \( \mathbb{F}_q[x] \), or equivalently, the dual Hamming codes. Although many of the equivalences are well-known (see, e.g., Garrett [3] Chap. 21, [4] Chap. 16, Klein [5] Chap. 2 for some), we were unable to find a source for all of them in the literature, so we have included the proofs here. Some of the equivalences involve the linear feedback shift register (LFSR) associated to a monic polynomial \( f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} + x^k \), which is the \( \mathbb{F}_q \)-linear map

\[
\mathbb{F}_q^k \xrightarrow{T_f} \mathbb{F}_q^k \quad T_f(x) = (x_1, \ldots, x_{k-1}, x_k)
\]

where \( x_k : = -(a_0 x_{k-1} + a_1 x_{k-2} + \cdots + a_{k-1} x_0) \). Starting with a seed vector \( s = (s_0, s_1, \ldots, s_{k-1}) \), since \( s \) and \( T_f(s) \) overlap in a consecutive subsequence of length \( k - 1 \), it is possible to create an infinite pseudorandom sequence \( (s_0, s_1, \ldots, s_{k-1}, s_k, s_{k+1}, \ldots) \) containing as its length \( k \) consecutive subsequences all of the iterates \( T_f^n(s) = (s_{r+1}, s_{r+2}, \ldots, s_{r+k-1}) \).

**Proposition 4.2.** Let \( g^+(x) \) be any monic irreducible degree \( k \) polynomial in \( \mathbb{F}_q[x] \) that divides \( x^n - 1 \), where \( n := q^k - 1 \). Let \( \mathcal{C} \subset \mathbb{F}_q^n \) be the \( k \)-dimensional cyclic code generated by \( g(x) = \frac{x^n - 1}{g^+(x)} \). Then the following are equivalent:

(i) The \( C \)-action by \( n \)-fold cyclic shifts on \( \mathcal{C} \setminus \{0\} \) inside \( \mathbb{F}_q^n \) is simply transitive.

(ii) \( \gcd(g^+(x), x^d - 1) = 1 \) for all proper divisors \( d \) of \( n \).

(iii) \( g^+(x) \) is primitive, that is, \( \bar{x} \) has order \( n \) in \( \mathbb{F}_q[x]/(g^+(x)) \), so \( \mathcal{C} \) is dual Hamming.

(iv) The linear feedback shift register \( T_{g^+} : \mathbb{F}_q^k \to \mathbb{F}_q^k \) has order \( n \).

(v) With seed \( s := (0, \ldots, 0, 1) \) in \( \mathbb{F}_q^k \), the iterates \( \left\{ T_{g^+}^r(s) \right\}_{r=0,1,\ldots,n-1} \) exhaust \( \mathbb{F}_q^k \setminus \{0\} \).

(vi) The pseudorandom sequence generated by \( T_{g^+}(x) \) with seed \( s := (0, \ldots, 0, 1) \) is \( n \)-periodic, and each period contains each vector \( \mathbb{F}_q^k \setminus \{0\} \) as a consecutive subsequence exactly once.

(vii) The codeword \( w \) in \( \mathcal{C} \subset \mathbb{F}_q^n \) corresponding under \( T_{g^+} \) to \( g(x) \) in \( \mathbb{F}_q[x]/(x^n - 1) \), when repeated \( n \)-periodically, has each vector of \( \mathbb{F}_q^k \setminus \{0\} \) as a consecutive subsequence once per period.

**Example 4.3.** When \( q = 3 \) and \( k = 2 \), so \( n = 3^2 - 1 = 8 \), there are three degree two monic irreducibles \( g^+(x) \) in \( \mathbb{F}_3[x] \), each shown here with \( g(x) = \frac{x^n - 1}{g^+(x)} \) and its corresponding word \( w \) in \( \mathbb{F}_3^8 \).
The first choice is not primitive, while the second and third are primitive. The non-primitive first choice \( g^+(x) = x^2 + 1 \) has LFSR \( L_{g^+(x)} : (x_0, x_1) \mapsto (x_1, x_2) \) where \( x_2 = -(0 \cdot x_1 + 1 \cdot x_0) = -x_0 \). Starting with seed \((0, 1)\), it has only 4 different iterates

\[
(0, 1) \mapsto (1, 0) \mapsto (0, 2) \mapsto (2, 0) \mapsto (0, 1) \mapsto (1, 0) \mapsto (2, 0) \mapsto (0, 1) \mapsto \cdots
\]

and this pseudorandom sequence \((0, 1, 0, 2, 0, 1, 0, 2, 0, 1, 0, 2, 0, 1, \ldots)\), whose period is 4, not \( n = 8 \).

The primitive second choice \( g^+(x) = x^2 + x + 2 \) has LFSR \( L_{g^+(x)} : (x_0, x_1) \mapsto (x_1, x_2) \) where \( x_2 = -(1 \cdot x_1 + 2 \cdot x_0) = -x_1 + x_0 \). Starting with seed \((0, 1)\) it has 8 different iterates (all of \( \mathbb{F}_2^2 \setminus \{0\} \))

\[
(0, 1) \mapsto (1, 2) \mapsto (2, 2) \mapsto (2, 0) \mapsto (0, 2) \mapsto (2, 1) \mapsto (1, 1) \mapsto (1, 0) \mapsto (0, 1) \mapsto \cdots
\]

and pseudorandom sequence \((0, 1, 2, 2, 0, 2, 1, 1, 0, 1, 2, 2, 0, 2, 1, \ldots)\), whose period is \( n = 8 \).

**Proof.** (i) \( \iff \) (ii): Since both the cyclic group \( C \) and \( \mathbb{C} \setminus \{0\} \) have \( n = q^k - 1 \) elements, the \( C \)-action on \( \mathbb{C} \setminus \{0\} \) is simply transitive if and only if it is free. Proposition 4.1 then implies the equivalence.

(ii) \( \iff \) (iii): Since \( g^+(x) \) is an irreducible factor of \( x^n - 1 \), having \( \gcd(g^+(x), x^d - 1) \) for all proper divisors \( d \) of \( n \) is the same as saying \( g^+(x) \) does not divide \( x^d - 1 \) for any proper divisor \( d \) of \( n \). The latter is the same as saying \( \bar{x} \) has order \( n \) inside \( \mathbb{F}_q \langle x \rangle / (g^+(x)) \).

(iii) \( \iff \) (iv): The matrix for \( T_{g^+(x)} \) acting in the standard basis for \( \mathbb{F}_q^n \) is the transpose of the matrix for multiplication by \( \bar{x} \) acting in the ordered basis \((1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{k-1})\) for \( \mathbb{F}_q \langle x \rangle / (g^+(x)) \), that is, the usual companion matrix for \( g^+(x) \). Therefore they have the same multiplicative order.

(iv) \( \Rightarrow \) (v): Since \( T_{g^+(x)} \) has the same multiplicative order as multiplication by \( \bar{x} \) in \( \mathbb{F}_q \langle x \rangle / (g^+(x)) \), and since \( g^+(x) \) divides \( x^n - 1 \), the latter order divides \( n \). However, if the iterates \( \{T_{g^+(x)}(e_k)\}_{r=0,1,\ldots,n-1} \) exhaust \( \mathbb{F}_q^k \setminus \{0\} \), then there are \( n \) of them, so \( T_{g^+} \) has order at least \( n \), and hence exactly \( n \).

(ii) \( \Rightarrow \) (v): Assume (v) fails, that is, the \( n \) iterates \( \{T_{g^+(x)}(e_k)\}_{r=0,1,\ldots,n-1} \) do not exhaust the set \( \mathbb{F}_q^k \setminus \{0\} \) of cardinality \( n \), so two of them are equal. Since \( T_{g^+} \) is invertible, this means \( T_{g^+}^d(x) = x \) for some \( x \neq 0 \) and \( 1 \leq d < n \). Thus \( T_{g^+} \) has an eigenvalue \( \alpha \) in \( \mathbb{F}_q \) which is a \( d^\text{th} \) root-of-unity for some proper divisor \( d \) of \( n \), and hence its characteristic polynomial \( g^+(x) \) has \( \alpha \) as a root. But this would contradict (ii): primitivity of \( g^+(x) \) implies that any of its roots \( \alpha \) gives rise to an isomorphism \( \mathbb{F}_q \langle x \rangle / (g^+(x)) \cong \mathbb{F}_q[\alpha] \) sending \( \bar{x} \mapsto \alpha \), so \( \alpha \) should have order \( n \).

(v) \( \iff \) (vi): By construction the \( n \)-periodicity of the pseudorandom sequence comes from the fact that \( T_{g^+} \) had the same order \( n \) as \( \bar{x} \). The rest of (vi) is then a restatement of (v).

(vi) \( \iff \) (vii): We claim that the word \( w \) in (vii) is the reverse of the pseudorandom sequence in (vi). This is because the equation

\[
x^n - 1 = g^+(x)g(x) = \left(x^k + \sum_{i=0}^{k-1} a_i x^i\right) \left(\sum_{j=1}^{n} w_j x^{j-1}\right)
\]
defining \( g(x) \) via \( g^\pm(x) \) makes the coefficient of \( x^m \) vanish on both sides for \( 1 \leq m \leq n - 1 \), so

\[
w_{m-k+1} = -(a_{k-1}w_{m-k+2} + \cdots + a_1w_m + a_0w_{m+1}) = T_{g^+}(w_{m+1}, w_m, \ldots, w_{m-k+2}).
\]

Also, since \( g(x) \) is monic of degree \( n - k \), the reverse \( (w_n, w_{n-1}, \ldots, w_2, w_1) \) of \( w \) will start with its initial \( k \) terms being \( \langle w_n, w_{n-1}, \ldots, w_{n-k+2}, w_{n-k+1} \rangle = (0, 0, \ldots, 0, 1) \). In other words, this reverse of \( w \) is the pseudorandom sequence of length \( n \) generated by \( T_{g^+}(x) \) with seed \( (0, 0, \ldots, 0, 1) \).

**Proposition 4.4.** Let \( X = \mathbb{C} \subset \mathbb{F}_q^n \) be a \( k \)-dimensional dual Hamming code, so that \( n = q^k - 1 \), with generator \( g(x) \), and \( w \) in \( \mathbb{F}_q^n \) its corresponding word. Then

(i) \( (X, X^{ma}(t), C) \) exhibits the CSP if and only \( \gcd(n, \text{cdes}(w)) = 1 \).

(ii) In the binary case, \( (X, X^{inv}(t), C) \) exhibits the CSP if and only \( \gcd(n, \text{wt}(w)) = 1 \).

**Proof.** Combine the equivalence between Proposition 4.2 (i) and (iii) with Corollary 3.6.

This leads to the main result of this section, whose part (ii) we find surprising.

**Theorem 4.5.** Fix a positive integer \( k \) and prime power \( q \), and let \( n := q^k - 1 \).

(i) Any nonzero codeword \( w \) in a dual Hamming code in \( \mathbb{C} \subset \mathbb{F}_q^n \) has \( \text{cdes}(w) = \frac{q-1}{2} \cdot q^{k-1} \).

(ii) If \( q \in \{2, 3\} \), then a monic degree \( k \) irreducible \( g^\pm(x) \) in \( \mathbb{F}_q[x] \) is primitive if and only if the word \( w \) corresponding to \( \langle x = \frac{x-1}{g}(x) \rangle \) under the bijection (2.1) has \( \text{cdes}(w) = \frac{q-1}{2} \cdot q^{k-1} \).

(iii) If \( q \in \{2, 3\} \), then \( (X, X^{ma}(t), C) \) gives a CSP for \( X = \mathbb{C} \) any dual Hamming code.

(iv) If \( q = 2 \), then \( (X, X^{inv}(t), C) \) gives a CSP for \( X = \mathbb{C} \) any dual Hamming code.

**Proof.** For (i), note that part (i) of Proposition 4.2 shows that all nonzero words \( w \in \mathbb{C} \) lie in the same \( C \)-orbit, while part (iv) of the same proposition implies that the \( n \)-periodic extension of \( w \) contains every vector in \( \mathbb{F}_q^k \setminus \{0\} \) exactly once as a consecutive subsequence each period. Consequently, every possible pair \( (w_{i-1}, w_i) \) (with subscripts taken modulo \( n \)) contributing to \( \text{cdes}(w) \) has its location uniquely determined within an \( n \)-period once we

- choose the values \( w_{i-1} > w_i \) in \( \{\frac{q-k}{2}\} \) ways, and then
- complete the length \( k \) subsequence preceding it as \( \langle w_{i-k+1}, \ldots, w_{i-2}, w_{i-1}, w_i \rangle \) by choosing the preceding \( k - 2 \) entries arbitrarily in \( q^{k-2} \) ways; this is not \( 0 \) in \( \mathbb{F}_q \) since \( w_{i-1} > w_i \).

Thus \( \text{cdes}(w) = \left\{ \frac{q-k}{2} \right\} \cdot q^{k-2} = \frac{q-1}{2} \cdot q^{k-1} \).

For (ii), (iii), the crux is that if \( q \in \{2, 3\} \), then \( \frac{q-1}{2} q^{k-1} \) is a \( q \)-power, so \( \gcd\left(\frac{q-1}{2}, q^{k-1}, n\right) = 1 \).

To deduce (ii), assume \( q \in \{2, 3\} \) and \( \text{cdes}(w) = \frac{q-1}{2} q^{k-1} \). We know that in \( \mathbb{F}_q[x]/(g^\pm(x)) \), the element \( \tilde{x} \) has some multiplicative order \( d \) dividing \( n = q^k - 1 \), and want to show \( d = n \). Since the LFSR \( T_{g^+(x)} : \mathbb{F}_q^k \to \mathbb{F}_q^k \) also has order \( d \), the word \( w \) will be \( d \)-periodic, consisting of \( \frac{n}{d} \) repeats of some word of length \( d \). Hence \( \frac{n}{d} \) divides \( \text{cdes}(w) = \frac{q-1}{2} q^{k-1} \). Since \( \frac{n}{d} \) also divides \( n \), it divides \( \gcd\left(\frac{q-1}{2}, q^{k-1}, n\right) = 1 \). Hence \( d = n \) as desired.

To deduce (iv), Proposition 4.4 applies once we compute the Hamming weight \( \text{wt}(w) \). As the \( n \)-periodic extension of \( w \) has every binary sequence in \( \mathbb{F}_q^k \setminus \{0\} \) occurring exactly once consecutively in a period, this implies \( \text{wt}(w) = 2^{k-1} \), and hence \( \gcd(n, \text{wt}(w)) = \gcd(2^k - 1, 2^{k-1}) = 1 \), as desired.

**Example 4.6.** The assertion of Theorem 4.5 (ii) fails for \( q = 5 \) at \( k = 3 \). The cubic irreducible \( g^\pm(x) = 1 + x + x^3 \) in \( \mathbb{F}_5[x] \) is not primitive, since \( \tilde{x} \) has order \( d = 62 \) in \( \mathbb{F}_5[x]/(g^\pm(x)) \), rather than \( n = 5^3 - 1 = 124 \). However, one can check that the word \( w \) corresponding to \( g(x) = \frac{x^3 + 3x^2 + 1}{g^\pm(x)} \) still has \( \text{cdes}(w) = 50 = \frac{q-1}{2} \cdot 5^{k-1} \). Likewise the assertion fails for \( q = 7 \) at \( k = 2 \). The irreducible quadratic \( g^\pm(x) = 6 + x + x^2 \) in \( \mathbb{F}_7[x] \) is not primitive, as \( \tilde{x} \) has order 16 in \( \mathbb{F}_7[x]/(g^\pm(x)) \), not \( n = 7^2 - 1 = 48 \), but one can check that the word \( w \) corresponding to \( g(x) \) has \( \text{cdes}(w) = 21 = \frac{q-1}{2} \cdot 7^{k-1} \).
One can also check that the assertion of Theorem 4.5(iv) fails for \( q = 3 \) at \( k = 2 \), such as in Example 4.3 with the choice of primitive polynomial \( g^⊥(x) = x^2 + x + 2 \) as the parity check for a dual Hamming code \( X = C \): no matter how one orders the alphabet \( \mathbb{F}_3 = \{0, 1, 2\} \) to define inv in \( X^{\text{inv}}(t) \), the triple \((X, X^{\text{inv}}(t), C)\) does not exhibit the CSP.

5. Questions

We close with some questions that we have not seriously explored.

**Question 5.1.** Can one characterize the dual Hamming codes \( X = C \) for which \((X, X^{\text{maj}}(t), C)\) or \((X, X^{\text{inv}}(t), C)\) exhibits a CSP? To what extent does this depend upon the choice of primitive polynomial parity check polynomial \( g^⊥(x) \) and/or the linear ordering of \( \mathbb{F}_q \) used to define maj, inv?

**Question 5.2.** Do other cyclic codes (e.g., Reed-Solomon, BCH, Golay) exhibit interesting CSPs?

References

[1] C. Ahlbach and J.P. Swanson, Refined cyclic sieving on words for the major index statistic. *European J. Combin.* **73** (2018), 3760.
[2] A. Berget, S.-P. Eu, and V. Reiner, Constructions for cyclic sieving phenomena, *SIAM J. Discrete Math.* **25** (2011), 1297–1314.
[3] P. Garrett, Making, Breaking Codes: An Introduction to Cryptology, 2nd Edition. Prentice Hall, 2011.
[4] P. Garrett, The Mathematics of Coding: Information, Compression, Error Correction, and Finite Fields, [www-users.math.umn.edu/~garrett/coding/CodingNotes.pdf](http://www-users.math.umn.edu/~garrett/coding/CodingNotes.pdf).
[5] A. Klein, Stream ciphers. Springer, London, 2013.
[6] V. Pless, Introduction to the theory of error-correcting codes, 3rd edition. John Wiley & Sons, Inc., New York, 1998
[7] J. Propp, posting to the ”Dynamical Algebraic Combinatorics” list-server, dac@listserv.uml.edu, May 9, 2017.
[8] V. Reiner, D. Stanton, and D. White. The cyclic sieving phenomenon, *J. Combin. Theory Ser. A* **108** (2004), 17–50.