Cyclic Sieving of Dual Hamming Codes

Alex Mason[1] Shruthi Sridhar [2]

[1]Washington University, St. Louis *masona@wustl.edu*

[2]Cornell University *ss2945@cornell.edu*

Research work from UMN Twin Cities REU 2017

July 31, 2017

Definition

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:

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

Example

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

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

Cyclic Codes

One has the following isomorphism: $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/(x^n - 1)$

$$w = (w_1, \ldots, w_n) \longmapsto \sum_{i=1}^{n} w_i x^{i-1}$$

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* $g(x)$.

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

The repetition code is generated by $1 + x + ... + x^{n-1}$.
Hamming codes are those generated by primitive polynomials.

Cyclic Codes

One has the following isomorphism: $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/(x^n - 1)$

$$w = (w_1, \ldots, w_n) \longmapsto \sum_{i=1}^{n} w_i x^{i-1}$$

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* $g(x)$.

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

The repetition code is generated by $1 + x + \ldots + x^{n-1}$.
Hamming codes are those generated by primitive polynomials.

Definition

The Dual Code, $\mathcal{C}^\perp$ of a cyclic code $\mathcal{C}$ generated by $g(x)$ is the cyclic code generated by $g^\perp(x) = \frac{x^n - 1}{g(x)}$

The parity check code and the repetition code are duals.
Dual Hamming codes are the duals of Hamming Codes.

Cyclic Sieving

Definition

Given any set $\mathcal{C}$ acted upon by the cyclic group $\mathbb{Z}_n$, a polynomial $X(t)$ is a *cyclic sieving polynomial* for $\mathcal{C}$ if $\forall m, X(\zeta_n^m) = |\{w \in \mathcal{C} : c^m w = w\}|$, where ζ_n is a primitive nth root of 1.

Constants are cyclic sieving polynomials for repetition codes.

Question

When do dual Hamming codes exhibit Cyclic sieving?

Some candidates are Mahonian polynomials:

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

where

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

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

These are two particular types of Mahonian statistics.

Primitive Polynomials

Definition

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

Note: Any irreducible polynomial $f(x)$ of degree k will divide $x^{q^k-1} - 1$ because $\mathbb{F}_{q^k} \cong \mathbb{F}_q[x]/(f(x))$ and $\mathbb{F}_{q^k} \setminus \{0\} \cong \mathbb{Z}/(q^k - 1)\mathbb{Z}$

Primitive polynomials over $\mathbb{F}_2$ of degree 3:

$$x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$$

$x^3 + x + 1$ and $x^3 + x^2 + 1$ are primitive.

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

$$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

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

Linear Feedback Shift Register

Let $f(x) = x^k + c_{k-1}x^{k-1} + \dots c_1 x + c_0$ be an irreducible polynomial. The *Linear Feedback Shift Register* (LFSR) of $f(x)$ is a linear map $T : \mathbb{F}_q^k \longmapsto \mathbb{F}_q^k$ defined as

$$T(x_0, x_1, \dots x_{k-1}) = (x_1, \dots, x_{k-1}, x_k) \qquad \text{where } x_k = -\sum_{i=0}^{k-1} c_i x_i$$

Property

f(x) is primitive $\iff$ LFSR has multiplicative order $n = q^k - 1$

Proof Sketch.
The characteristic polynomial of the matrix of the transformation is $(-1)^k f(x)$ which is irreducible. Hence the minimal polynomial of T is $f(T)$. The minimum n such that $f(x) \mid x^n - 1$ is $n = q^k - 1$.

The **LFSR sequence** of $f(x)$: $(x_0, x_1, \dots, x_{k-1}, x_k, x_{k+1}, \dots, x_{n-1})$.

Primitive Polynomials

Example: q=2, k=3

We start with $\mathbf{x} = (0,0,1)$ and $f(x) = x^3 + x^2 + 1$.
Thus $c_0 = 1, c_1 = 0, c_2 = 1$

$$\begin{pmatrix}0\\0\\1\end{pmatrix} \mapsto \begin{pmatrix}0\\1\\1\end{pmatrix} \mapsto \begin{pmatrix}1\\1\\1\end{pmatrix} \mapsto \begin{pmatrix}1\\1\\0\end{pmatrix} \mapsto \begin{pmatrix}1\\0\\1\end{pmatrix} \mapsto \begin{pmatrix}0\\1\\0\end{pmatrix} \mapsto \begin{pmatrix}1\\0\\0\end{pmatrix} \mapsto \begin{pmatrix}0\\0\\1\end{pmatrix}$$

The LFSR sequence is (0,0,1,1,1,0,1)

Corollary

f(x) is primitive $\iff$ *the set* $\{\mathbf{x}, T\mathbf{x} \dots T^{n-2}\mathbf{x}\} = (\mathbb{F}_q)^k \setminus \{\mathbf{0}\}$ *for some* $\mathbf{x} \neq \mathbf{0}$ *where* T *is the LFSR of* $f(x)$

By the Corollary, the LFSR sequence has **every** possible sequence of length k as a subsequence exactly once.

Primitive Polynomials

One of our main results:

Theorem

The coefficient sequence of $\frac{x^n-1}{f(x)}$ is the LFSR sequence reversed, where the sequence is defined to begin at (0,0...1).

Example: q=2, k=3

We use $f(x) = x^3 + x^2 + 1$. The LFSR sequence was (0,0,1,1,1,0,1).

$$\frac{x^7 - 1}{x^3 + x^2 + 1} = 1 + x^2 + x^3 + x^4$$
$$= 1 + 0x + 1x^2 + 1x^3 + 1x^4 + 0x^5 + 0x^6$$

Cyclic Descents

Definition

If $w = (w_1, w_2, ..., w_n)$, a *cyclic descent* is a pair of consecutive terms (w_i, w_{i+1}) with $w_i > w_{i+1}$, including possibly the pair (w_n, w_1). The *cyclic descent number* of w, $\text{cdes}(w)$, is the number of cyclic descents.

Cyclic descents play in important role in understanding $\text{maj}(w)$.

In any LFSR sequence for a primitive polynomial, all possible subsequences of length k except the 0 subsequence are present, there are $(q-1)q^{k-1}$ subsequences where the last two elements are different, exactly half of which end in descents.

Example: q=2, k=3

If $w = (0, 0, 1, 1, 1, 0, 1)$, then $\text{cdes}(w) = 2$, as expected.

Cyclic Descents

The coefficient sequence w of generating polynomial $g(x)$ of the dual Hamming code, is the reverse of the LFSR sequence.

Thus every k-subsequence except the zero sequence appears in the coefficient sequence, and $\mathrm{cdes}(w) = \frac{q-1}{2} q^{k-1}$.

Corollary

When $p = 2, 3$, the converse is also true: if $\mathrm{cdes}(w) = \frac{q-1}{2} q^{k-1}$, f is primitive.

This is true because if $\gcd(\mathrm{cdes}(w), n) = 1$, no k-subsequence can repeat. This is not true in general: it fails at $q = 5, k = 3$ and $q = 7, k = 2$.

Back to Cyclic Sieving

Definition

Hamming codes: codes whose generating polynomial is primitive.
Dual Hamming codes: dual of Hamming codes.

Our first goal is to find when the polynomial $X^{\text{maj}}(t)$ is a cyclic sieving polynomial for dual Hamming codes.

Since (aside from the zero code) all elements of dual Hamming codes are fixed by only the identity, any CSP must evaluate to 1 for all n^{th} roots of unity except 1. Also, it should evaluate to $n+1$ at $t=1$. Thus the CSP should have the form $1+\sum_{m=0}^{n-1} t^m$.

X^{maj} as a CSP

Proposition

Suppose X is a dual Hamming code over $\mathbb{F}_2$ or $\mathbb{F}_3$. Then, $X^{\mathrm{maj}}(t)$ is a cyclic sieving polynomial for X.

Proof.

The main observation is:

$$\mathrm{maj}(c(w)) = \begin{cases} \mathrm{maj}(w) + \mathrm{cdes}(w) - n & \text{if } w \text{ ends in a descent} \\ \mathrm{maj}(w) + \mathrm{cdes}(w) & \text{if } w \text{ does not end in a descent} \end{cases}$$

$$\text{Hence, } X^{\mathrm{maj}}(t) = 1 + \sum_{m=0}^{n-1} t^{\mathrm{maj}(c^m w)} = 1 + \sum_{m=0}^{n-1} t^{\mathrm{maj}(w)+m(\mathrm{cdes}(w))}$$

When $q = 2, 3$, $\mathrm{cdes}(w) = \frac{q-1}{2} q^{k-1}$ is relatively prime to n, it is a primitive additive element of $\mathbb{Z}_n$. So,

$$X^{\mathrm{maj}}(t) = 1 + \sum_{m=0}^{n-1} t^{\mathrm{maj}(w)+m(\mathrm{cdes}(w))} = 1 + \sum_{m=0}^{n-1} t^m$$

. □

X^{inv} as a CSP

Proposition

Suppose X is a dual Hamming code over $\mathbb{F}_2$. Then, $X^{\text{inv}}(t)$ is a cyclic sieving polynomial for X.

Proof.

This time, the main observation is

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

As before, $2^{k-1} - 1$ and -2^{k-1} are equal mod $n = 2^k - 1$ and are coprime to n. Hence,

$$X^{\text{maj}}(t) = 1 + \sum_{m=0}^{n-1} t^{\text{inv}(c^m w)} = 1 + \sum_{m=0}^{n-1} t^{\text{inv}(w)+m(2^{k-1}-1)} = 1 + \sum_{m=0}^{n-1} t^m$$

. $\square$

Summary of results

- For $q = 2, 3$, the triple $(X, X^{\text{maj}}(t), C)$ always gives a CSP for dual Hamming codes $X = \mathcal{C}$.
- For $q = 2, 3$, an irreducible polynomial $f(x)$ is primitive iff the cyclic descents in the coefficient sequence of $\frac{x^{q^k-1}-1}{f(x)}$ is exactly $\frac{(q-1)}{2}q^{k-1}$.
- For $q = 2$, the triple $(X, X^{\text{inv}}(t), C)$ always gives a CSP for dual Hamming codes $X = \mathcal{C}$.

Acknowledgements

This research was supported by NSF RTG grant DMS-1148634 and by NSF grant DMS-1351590. We would like to thank the mathematics department at the University of Minnesota, Twin Cities. In particular, we would like to thank Victor Reiner, Pasha Pylyavskyy, and Craig Corsi for their mentorship, and support.

References

- A. Berget, S.-P. Eu, and V. Reiner, Constructions for cyclic sieving phenomena, *SIAM J. Discrete Math.* **25** (2011), 1297–1314.
- V. Reiner, D. Stanton, and D. White. The cyclic sieving phenomenon, *J. Combin. Theory Ser. A* **108** (2004), 17–50.