

A Mass Formula for Cyclic Self-Orthogonal Codes

Chekad Sarami

Department of Mathematics & Computer Science
Fayetteville State University
Fayetteville, North Carolina, U.S.A.

Abstract - We give an algorithm for generating cyclic self-orthogonal (CSO) codes for an arbitrary positive integer n with $\gcd(n, q) = 1$. Given a cyclic q -ary code of length n , we determine how many codes isomorphic to the given code are cyclic. We introduce a mass formula for $\text{CSO}(n, q)$ codes of maximum dimension. Using the mass formula we classify $\text{CSO}(63, 2)$ codes. This mass formula works for any cyclic incidence structure on n points. At the end, We conjecture that there are at least two $\text{CSO}(127, 2)$ codes of dimension 63 up to isomorphism.

Keywords: cyclic codes, self-orthogonal codes, mass formula.

1 Introduction

We assume that the reader is familiar with the basic definitions and facts of the theory of error-correcting codes. Our notation and terminology for error-correcting codes will be standard and can be found in [3], for instance. A polynomial $p(x) \in F_q[x]$ is said to be irreducible over F_q if $p(x)$ has positive degree and $p(x) = a(x)b(x)$, with $a(x), b(x) \in F_q[x]$ implies that either $a(x)$ or $b(x)$ is a constant polynomial. For every finite field F_q and $n \in \mathbb{N}$, the product of all monic irreducible polynomials over F_q whose degrees divide n is equal to $x^{q^n} - x$.

The code C is cyclic if it is linear and is closed under the shift of the codewords. In other words, (c_0, \dots, c_{n-1}) is a codeword whenever $(c_1, \dots, c_{n-1}, c_0)$ is also a codeword. We associate the codeword (c_0, \dots, c_{n-1}) in F_q^n with the polynomial $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in F_q[x]$. A cyclic code of length n is an ideal of the quotient ring $R_n = F_q[x]/(x^n - 1)$. The generator polynomial of $C = \langle g(x) \rangle$ is a unique monic polynomial $g(x)$ of minimum degree. The generator polynomial $g(x)$ divides $x^n - 1$. If $\deg(g(x)) = r$, then C has dimension $n - r$. The

check polynomial of C is $h(x) = (x^n - 1)/g(x)$. The dual code C^\perp is also cyclic and has generator polynomial $g^\perp(x) = x^{\deg(h(x))}h(x^{-1})$.

The formula for the total number of maximal self-orthogonal codes ([3], Theorem 9.5.3) implies that the number of self-orthogonal codes of length 63 and dimension 31 is larger than 4.8×10^{149} . Classification of self-orthogonal codes of large lengths is infeasible. In this paper, we consider classification of cyclic self-orthogonal codes.

The enumeration and classification of all cyclic binary self-orthogonal codes of length 63 of maximum dimension have been carried out in [8]. The classification of the aforementioned codes has been done using the isomorphism of the incidence structures derived from codewords of particular weights. It is very helpful to have a mass formula to classify these codes. We present a mass formula for cyclic self-orthogonal codes of maximum dimension in Theorem 7. Using this formula, we classify $\text{CSO}(63, 2)$ codes of maximum dimension 27 and give the order of their automorphism groups.

2 Generating CSO codes

We shall denote the set of all cyclic self-orthogonal codes of length n over \mathbb{F}_q by $\text{CSO}(n, q)$. We give an algorithm for generating $\text{CSO}(n, q)$ codes for an arbitrary positive integer n with $\gcd(n, q) = 1$. The algorithm can be revised to generate $\text{CSO}(n, q)$ codes of any given dimension.

The *reciprocal* of a non-zero polynomial $f(x) \in \mathbb{F}_q[x]$ is defined by

$$\text{rec}(f(x)) := x^{\deg(p(x))}f(x^{-1}) \in \mathbb{F}_q[x]. \quad (1)$$

For non-zero polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ we say $f(x)$ is reciprocal of $g(x)$ if $f(x)$ is a non-zero multi-

ple of reciprocal of $g(x)$; i.e. $rec(f(x)) = ag(x)$ for some $a \in \mathbb{F}_q^*$ and $f(x)$ is **self-reciprocal** if $f(x)$ is reciprocal of itself.

Lemma 1 [3] *Let $x^n - 1 = g(x)h(x)$ over \mathbb{F}_q . Then a cyclic code C with generator polynomial $g(x)$ is self-orthogonal if and only if the reciprocal of $h(x)$ divides $g(x)$.*

If C is a self-orthogonal cyclic q -ary code with a generator polynomial $g(x)$, we have $\deg(g(x)) \geq \lfloor \frac{n}{2} \rfloor$. Let $x^n - 1 = f_1(x) \dots f_l(x)$ be the factorization of $x^n - 1$ in $F_q[x]$. According to Lemma 1, we can find all generator polynomials of $CSO(n, q)$ codes by inspecting the factors of $x^n - 1$ of degree $\geq \lfloor \frac{n}{2} \rfloor$.

Theorem 2 [3, page 148] *Suppose the following is a factorization of $x^n - 1$ into monic irreducible polynomials*

$$x^n - 1 = f_1(x) \cdots f_s(x) a_1(x) \cdots a_l(x) b_1(x) \cdots b_l(x),$$

where for $1 \leq i \leq s$, $f_i(x)$ is self-reciprocal and for $1 \leq i \leq l$, $b_i(x)$ is reciprocal of $a_i(x)$.

Let C be a cyclic code of length n over F_q with generator polynomial $g(x)$. Then C is self-orthogonal if and only if $g(x)$ has factors $f_1(x) \cdots f_s(x)$ and at least one of $a_i(x)$ or $b_i(x)$ for $1 \leq i \leq l$.

From above theorem we conclude that $|CSO(n, q)| = 3^l$ and every cyclic self-orthogonal code is contained in some maximal $CSO(n, q)$ code of dimension

$$k_{\max} = n - \sum_{i=1}^s \deg f_i(x) - \sum_{i=1}^l \deg a_i(x). \quad (2)$$

Moreover, the number of $CSO(n, q)$ codes of maximum dimension is 2^l [7].

Remark 3 *For $n = q^m - 1$, the irreducible polynomials and the number of self-reciprocal irreducible polynomials have been enumerated [6], [4]. We can find explicit formulas for the number of $CSO(q^m - 1, q)$ codes, the number of $CSO(q^m - 1, q)$ codes of a given dimension, and a dimension formula for such codes in terms of q and m .*

Using the following algorithm we can systematically generate $CSO(n, q)$ codes:

Algorithm 4 Generator Polynomials of $CSO(n, q)$

Input parameters: n, q

Output: ε : list of all generator polynomials of $CSO(n, q)$ codes.

$$S_1 \leftarrow \emptyset, S_2 \leftarrow \emptyset, \varepsilon \leftarrow \emptyset$$

$$S \leftarrow \{ \text{set of all irreducible factors of } x^n - 1 \}.$$

For $p(x) \in S$

If $f(x) = rec(f(x))$ **then** $S_1 \leftarrow S_1 \cup \{f(x)\}$

else $S_2 \leftarrow S_2 \cup \{f(x)\}$

$$g_1(x) \leftarrow \prod_{f(x) \in S_1} f(x)$$

$$s \leftarrow |S_2| / 2$$

$U \leftarrow \cup_{i=1}^s \{ \{g_{i_1}(x), h_{i_1}(x)\} \}$ ($\{g_{i_1}(x), h_{i_1}(x)\}$ are the reciprocal pairs introduced in Theorem 2)

$$V \leftarrow \cup_{i=1}^s \{ \{g_{i_1}(x), h_{i_1}(x), g_{i_1}(x)h_{i_1}(x)\} \}$$

$$G_2 \leftarrow \times_{v \in V} v \text{ (Cartesian product)}$$

For $g = (v_1(x), \dots, v_s(x)) \in G_2$

$$\varepsilon \leftarrow \varepsilon \cup \{g_1(x) \cdot \prod_{i=1}^s v_i(x)\}$$

Return(ε).

Remark 5 *Changing*

$$V \leftarrow \cup_{i=1}^s \{ \{g_{i_1}(x), h_{i_1}(x), g_{i_1}(x)h_{i_1}(x)\} \}$$

in the above algorithm to $V \leftarrow \cup_{i=1}^s \{ \{g_{i_1}(x), h_{i_1}(x)\} \}$ will result the generator polynomials of all $CSO(n, q)$ codes of maximum dimension.

Factorization of $x^{63} - 1$ over $F_2[x]$ shows that there are exactly 32 $CSO(63, 2)$ codes of maximum dimension 27. The polynomial $x^{127} - 1$ has a unique self-reciprocal factor $x + 1$ and 18 non-self-reciprocal factor over F_2 . Therefore there are 512 $CSO(127, 2)$ codes of maximum dimension 63.

3 Mass Formula for Maximal CSO Codes

So far we have enumerated the number of CSO(n, q) codes and maximal CSO(n, q) codes. Having a mass formula can be helpful to classify these codes. We know if C is an arbitrary q -ary code of length n then the number of codes equivalent to C is

$$\frac{n!}{|\text{PAut}(C)|}, \quad (3)$$

where $\text{PAut}(C)$, called the permutation automorphism group of C , is subgroup of the symmetric group S_n consists of all coordinate permutations that map C to itself. We call elements of $\text{PAut}(C)$ permutation automorphism.

Two linear codes C_1 and C_2 are isomorphic (permutation equivalent) if there is a permutation of coordinates which sends C_1 to C_2 . Here we are interested in cyclic codes. Given a cyclic q -ary code of length n we want to know how many codes isomorphic to C are cyclic. Of course this number is not always $n!/|\text{PAut}(C)|$ since not every permutation in S_n preserves the property of cyclicity. We have formulated this number in the following Lemma.

Lemma 6 *Let C be a cyclic q -ary code of length n and let $\text{PAut}_{\text{cyc}}(C)$ be the set of n -cycles of $\text{PAut}(C)$. Then $P_{\text{cyc}}(C)$, the number of cyclic codes isomorphic to C is*

$$P_{\text{cyc}}(C) = \frac{n|\text{PAut}_{\text{cyc}}(C)|}{|\text{PAut}(C)|} \quad (4)$$

Assume C is a cyclic q -ary code of length n with permutation automorphism $\text{PAut}(C)$. Take

$$U := \{g \in S_n : Cg \text{ is cyclic}\}. \quad (5)$$

Suppose $\{C_1, \dots, C_m\}$ with $m = P_{\text{cyc}}(C)$ is the set of all distinct cyclic codes isomorphic to C . Therefore, there are permutations $\sigma_1, \dots, \sigma_m \in U$ such that $C_i = C_{\sigma_i}$. Clearly, the coset $\text{PAut}(C)\sigma_i \subseteq U$ for every i . Hence $\cup_{i=1}^m \text{PAut}(C)\sigma_i \subseteq U$. Conversely, let $g \in U$ so C_g be a cyclic code isomorphic to C . Therefore, $C_g = C_i$ for some $i \in \{1, \dots, m\}$. This implies $C_g = C\sigma_i$ or $g\sigma_i^{-1} \in \text{PAut}(C)$. So $g \in \text{PAut}(C)\sigma_i$. Hence $U = \cup_{i=1}^m \text{PAut}(C)\sigma_i$ and we have

$$|U| = P_{\text{cyc}}(C)|\text{PAut}(C)| \quad (6)$$

Assume z is the n -cyclic $(1, 2, \dots, n)$. If $g \in U$ then $z \in \text{PAut}(Cg)$. This is the same as saying the conjugate of z in S_n is in $\text{Aut}(C)$. Suppose

$$\text{PAut}_{\text{cyc}}(C) := \{\alpha_1, \dots, \alpha_c\} \quad (7)$$

is the set of all n -cycle automorphisms of C where $c = |\text{PAut}_{\text{cyc}}(C)|$. Since any two n -cycles in S_n are conjugate in S_n , we have

$$|U| = \sum_{i=1}^c |\{g \in S_n : gzg^{-1} = \alpha_i\}| \quad (8)$$

From $gzg^{-1} = (g(1), g(2), \dots, g(n))$ it follows that $|\{g \in S_n : gzg^{-1} = \alpha_i\}| = n$. Hence

$$|U| = n|\text{PAut}_{\text{cyc}}(C)| \quad (9)$$

Comparing the equations (2) and (5) gives the equality in Lemma 6.

The mass formula for maximal CSO(n, q) codes follows from Theorem 2 and Lemma 6 as follows:

Theorem 7 *Let*

$$x^n - 1 = f_1(x) \dots f_s(x) a_1(x) \dots a_l(x) b_1(x) \dots b_l(x)$$

be the factorization of $x^n - 1$ over F_q given in Theorem 2. Assume $\sum_{i=1}^s \deg f_i(x) + \sum_{i=1}^l \deg a_i(x) = t$. Then the mass formula for cyclically-maximal CSO(n, q) is as follows:

$$\sum_i \frac{n|\text{PAut}_{\text{cyc}}(C_i)|}{|\text{PAut}(C_i)|} = 2^t \quad (10)$$

where the sum runs over all i , where $\{C_i\}$ is a complete set of representatives of non-isomorphic maximal CSO(n, q) codes. $\text{PAut}_{\text{cyc}}(C)$ is defined as in Lemma 6.

There are exactly 32 CSO(63,2) codes of maximum dimension 27 and there are precisely eight inequivalent classes of CSO(63, 2) codes [8]. These codes have been classified using isomorphism of incidence structures derived from codewords of certain weights. In fact, these codes could be classified easier using above Mass Formula (see Table 1). The coefficient list of the generator polynomials of the inequivalent codes are given in a decimal representation. For example, the binary representation of 41 is 101001 and the corresponding binary polynomial $1 + x^2 + x^5$ is the generator polynomial of the code.

Code #	Generator Poly.Coefficients	Min. Weight	$ \text{Aut}(C) $	$P_{\text{cyc}}(C)$
1	128336401643	8	$27216 = 2^4 3^5 7$	2
2	130251012467	8	$7620480 = 2^7 3^5 5^1 7^2$	2
3	123521236283	12	$378 = 2^1 3^3 7$	6
4	134246910755	16	$10584 = 2^3 3^3 7^2$	6
5	126538148171	16	$10584 = 2^3 3^3 7^2$	6
6	78517404169	8	$2^{22} 3^{10} 5^3 7^3$	2
7	68853956609	4	$2^{34} 3^{13} 5^1 7^{10}$	2
8	106916043935	12	$10584 = 2^3 3^3 7^2$	6
				Total= 32

Table 1: Classification of maximal CSO(63,2) codes and their group orders.

Remark 8 We have used Magma [1] to compute automorphism groups and n -cycles of automorphism groups of the codes using the following command:

```
> #[ u : u in G | CycleStructure(u)
eq [<n,1> ] ;
```

Example 9 $x^{127} - 1$ has a unique self-reciprocal irreducible factor $x + 1$ and 18 non-self-reciprocal irreducible factors over F_2 . Therefore there are 512 CSO(127, 2) codes of maximum dimension 63. Using the Magma Calculator (Total time: 14.160 seconds, [7]), we can verify that the polynomial

$$x^{64} + x^{56} + x^{55} + x^{54} + x^{53} + x^{52} + x^{51} + x^{50} + x^{49} + x^{40} + x^{37} + x^{36} + x^{33} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^8 + x + 1$$

is generator polynomial of C , a CSO(127, 2) code of dimension 63. We have $P\text{Aut}(C) = 7 \times 127$, so $P\text{Aut}_{\text{cyc}}(C) = 126$. There are precisely

$$\frac{n|P\text{Aut}_{\text{cyc}}(C)|}{|P\text{Aut}(C)|} = 18$$

CSO(127, 2) codes isomorphic to C . Algorithm 4 lists all 512 CSO(127, 2) codes of dimension 63. Using the mass formula, It seems to be feasible to classify these codes up to isomorphism.

It is known that there are exactly two CSO(31, 2) codes of maximum dimension 15 up to isomorphism. Existence of these two codes shows that the "only if" part of the Hamada's conjecture is not true in general [9].

Sarami and Tonchev [8] have used the classification of binary cyclic self-orthogonal codes of length 63 to

prove that any cyclic quasi-symmetric 2-(63, 15, 35) design with block intersection numbers $x = 3$ and $y = 7$ is isomorphic to the geometric design having as blocks the 3-dimensional subspaces in PG(5, 2). Now the question is whether there is a cyclic quasi-symmetric 2-(127, 31, 155) design non-isomorphic to the geometric quasi-symmetric 2-(127, 31, 155) design. Extended binary code of a geometric quasi-symmetric design is a cyclic self-orthogonal code. We conjecture that there are at least two CSO(127, 2) codes of dimension 63 up to isomorphism. Classification of CSO(127, 2) codes may provide another counterexample for Hamada's conjecture [5].

References

- [1] W. Bosma and J.J. Cannon. Magma. Sydney: School of Mathematics and Statistics, University of Sydney, 1995.
- [2] J.H. Conway and V. Pless. On the enumeration of self-dual codes. J. Combin Theory Ser. A, 28:26–53, 1980.
- [3] W.C. Huffman and V. Pless. Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003.
- [4] W. Götz and H. Meyn. Self-reciprocal polynomials over finite fields. In Séminaire Lotharingien de Combinatoire, pages 82–90. I.R.M.A. Strasbourg, 1990.
- [5] N. Hamada. On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes. Hiroshima Math.J., 3:153–226, 1973.

- [6] R. Lidl and H. Niederreiter. Introduction to Finite Fields and Their Applications. Cambridge University Press, 1986.
- [7] Magma: <http://magma.maths.usyd.edu.au/calc/>
- [8] C. Sarami and V.D. Tonchev, Cyclic quasi-symmetric designs and self-orthogonal codes of length 63, J. Statist. Planning and Inference, to appear.
- [9] V.D. Tonchev. Quasi-symmetric 2 - $(31,7,7)$ designs and a revision of Hamada's conjecture. J. Combin. Theory, A 42:104—110, 1986.
- [10] V.D. Tonchev. Codes and designs. in: "Handbook of Coding Theory", V.S. Pless and W.C. Huffman eds., Chapter 15, pages 1229–1267, 1998.