Cyclic Self-Dual Codes

N. J. A. SLOANE, FELLOW, IEEE, AND J. G. THOMPSON

DEDICATED TO JESSIE MACWILLIAMS ON THE OCCASION OF HER RETIREMENT FROM BELL LABORATORIES

Abstract—It is shown that if the automorphism group of a binary self-dual code satisfies a certain condition then the code contains words of weight congruent to 2 modulo 4. In particular, no cyclic binary self-dual code can have all its weights divisible by four. The number of cyclic binary self-dual codes of length \( n \) is determined, and the shortest nontrivial code in this class is shown to have length 14.

I. INTRODUCTION

ALTHOUGH self-dual codes have been extensively studied ([3], [8], [10]–[12], [14]), cyclic self-dual codes do not seem to have received much attention. The simplest self-dual code \([00, 11]\) is cyclic, as are all the trivial codes with generator matrices of the form

\[
\begin{bmatrix}
1 & \cdots & 1 \\
0 & \cdots & 0 \\
\vdots & & \vdots \\
0 & \cdots & 1
\end{bmatrix}
\]

(in this paper all codes are binary and linear). But, as we shall see in Section III, these exist nontrivial cyclic self-dual codes, the shortest of which has length 14. On the other hand there do not exist doubly even cyclic self-dual codes, i.e., codes in which all weights are divisible by four. This is a consequence of Theorem 1.

Theorem 1: Suppose \( C \) is a binary self-dual code of length \( n \), where \( n = 2^a \cdot b \), \( a > 1 \), \( b \geq 1 \) and \( b \) is odd, that is fixed (setwise) by a permutation group \( G \) satisfying the conditions a) \( G \) is transitive on the \( n \) coordinate positions and b) \( G \) has a 2-Sylow subgroup which is cyclic of order \( 2^b \). Then \( C \) contains codewords of weight congruent to 2 modulo 4.

For the proof of Theorem 1 we quote the following theorem from Hering [4] and Anstee-Hall-Thompson [1] (the result given in [1] and [4] is more general than this, but the binary version is sufficient for our purpose).

Theorem 3: Suppose \( C \subseteq \mathbb{F}_2^n \) is self-dual and is fixed (setwise) by a group of permutations \( H \) with \( |H| \) odd. Let

\[
(F_2^n)_o = \{ v \in \mathbb{F}_2^n : vh = v, \text{ for all } h \in H \}.
\]

Then \( \dim (F_2^n)_o = 2 \dim C_0 \).

Proof of Theorem 1: Let \( P \) be the cyclic 2-Sylow subgroup of \( G \), with generator \( \pi \). Since \( |P| = 2^a \cdot 2^{b-e} \), where \( e \) is odd and divisible by \( b \). Because \( P \) is cyclic, by [6, p. 420, th. 2.8] \( G \) contains a normal subgroup \( H \) with \( G/H \cong P \), \( |H| = 2^e \).

Let \( C_0 = \{ u \in C : uh = u, \text{ for all } h \in H \} \). The key to the proof is the rather surprising fact that \( C_0 \) can be found explicitly.

We shall determine the orbits of \( H \) on the \( n \) coordinates. \( H \) is not transitive, since \( |H| \) is odd and \( n \) is even. By Proposition 7.1 of [15], \( G \) is imprimitive, and the orbits of \( H \) form a complete block system of \( G \). In particular all the blocks have the same length, \( l \) say. Suppose there are \( m \) blocks, where \( lm = n = 2^a b \). Since \( H \) is transitive on each block, \( l \) divides \( |H| \), and therefore \( l \) is odd and \( 2^a \) divides \( m \). But \( \pi \) must be transitive on the blocks, so \( m \leq 2^a \), i.e., \( m = 2^a \). Thus the orbits of \( H \) consist of \( 2^a \times 2^a \) blocks of length \( b \).

Therefore the fixed subspace \((F_2^n)_o \) has dimension \( 2^a \), with one generator for each block. If the \( n \) coordinates are labeled appropriately, \((F_2^n)_o \) has the generator matrix shown in Fig. 1. From Theorem 3, \( C_0 \) has dimension \( 2^{a-1} \). Furthermore the action of \( \pi \) on the blocks (i.e., on \( F_2^a \)) is represented by the \( 2^a \times 2^a \) matrix

\[
A = \begin{bmatrix}
010 & \cdots & 0 \\
001 & \cdots & 0 \\
\vdots & & \vdots \\
000 & \cdots & 1 \\
100 & \cdots & 0
\end{bmatrix}
\]
The characteristic polynomial of \( A \) is

\[
\det(\lambda I - A) = \lambda^{2n} - 1 = (\lambda - 1)^{2^n},
\]

and all the eigenvalues are 1. Therefore there is a basis \( v_1, \ldots, v_{2^n} \) for \( \mathbb{F}_2^{2^n} \) with respect to which \( \pi \) is represented by its Jordan normal form [5, p. 209], which is the \( 2^n \times 2^n \) matrix

\[
B = \begin{bmatrix}
100 & \cdots & 000 \\
110 & \cdots & 000 \\
011 & \cdots & 000 \\
\vdots & \cdots & \vdots \\
000 & \cdots & 110 \\
000 & \cdots & 011 \\
\end{bmatrix}
\]

From this it follows that there is a unique subspace \( X \) of \( \mathbb{F}_2^{2^n} \) of every dimension \( k, 1 \leq k \leq 2^n \), that is fixed (set-wise) by \( \pi \). For with respect to the basis \( v_1, \ldots, v_{2^n} \), \( \pi \) must be represented on \( X \) by the \( k \times k \) matrix

\[
B = \begin{bmatrix}
100 & \cdots & 000 \\
110 & \cdots & 000 \\
011 & \cdots & 000 \\
\vdots & \cdots & \vdots \\
000 & \cdots & 110 \\
000 & \cdots & 011 \\
\end{bmatrix}
\]

Thus \( X \) is spanned by \( v_1, \ldots, v_k \). In particular there is a unique subspace \( C_0 \) of dimension \( 2^n - 1 \).

We can see directly (in terms of the old basis for \( \mathbb{F}_2^{2^n} \)) what \( C_0 \) must be: it is the code spanned by vectors having two blocks of \( b \) ones, as shown in Fig. 2. Since \( b \) is odd, \( C_0 \) contains words of weight congruent to 2 (modulo 4).

Proof of Corollary 2: Let \( \sigma \) be a cyclic permutation fixing \( C \), and set \( G = \langle \sigma \rangle \). Then \( P = \langle \sigma^b \rangle \) is a cyclic 2-Sylow subgroup of \( G \), of order \( 2^a \), and the result follows from Theorem 1.

III. THE ENUMERATION OF CYCLIC SELF-DUAL CODES

If \( C \) is a cyclic self-dual code of length \( n \) then a standard argument (see [2], [8, ch. 7]) shows that \( C \) has a generator polynomial \( g(x) \) which is a divisor of \( x^n + 1 \), and a check polynomial \( h(x) = (x^n + 1)/g(x) \). If \( f(x) \) is any polynomial, let \( f(1/x) \) denote the reciprocal polynomial. Then the dual code \( C^\perp \) has generator polynomial \( h(x) = (x^n + 1)/g(x) \), and we conclude that \( C \) is a cyclic self-dual code if and only if its generator polynomial satisfies

\[
g(x)g(x) = x^n + 1. \tag{1}
\]

If \( n = 2^a \cdot b \) with \( b \) odd then \( x^n + 1 \) factors over \( \mathbb{GF}(2) \) into

\[
x^n + 1 = \left( \prod_i M^{(b)}_i(x)^{2^{a_i}} \right), \tag{2}
\]

where there is one term in the product for each cyclotomic coset modulo \( b \):

\[
C^{(b)}_s = \{ s, 2s, 4s, 8s, \ldots \ (\text{mod } b) \},
\]

and

\[
M^{(b)}_i(x) = \prod_{\xi \in C^{(b)}_i} (x - \xi^i).
\]

The general solution of (1) and (2) is therefore

\[
g(x) = \prod_{\text{symmetric}} M^{(b)}_i(x)^{2^{a_i}} \prod_{\text{asymmetric}} M^{(b)}_i(x)^{i_i} M^{(b)}_{s_i}(x)^{2^{a_i - i_i}}, \tag{3}
\]

where in the first product there is one term for each symmetric coset \( C^{(b)}_s \), in the second product there is one term for each asymmetric pair \( C^{(b)}_s, C^{(b)}_{s_i} \), and \( i_i \) is any number in the range \( 0 < i_i < 2^a \). Thus we have proved the following result.

Theorem 4: The number of distinct cyclic self-dual codes of length \( n = 2^a \cdot b \), \( b \) odd, is \( (2^a + 1)^{\delta(b)} \), where \( \delta(b) \) is the number of pairs of asymmetric cyclotomic cosets modulo \( b \).

There is always one cyclic self-dual code, the trivial code with generator polynomial \( x^{n/2} + 1 \), obtained by taking all \( i_i = 2^{a_i - 1} \) in (3). The nontrivial codes, if any, fall into pairs of equivalent codes (for replacing all \( i_i \) by \( 2^a - i_i \) produces an equivalent code). There may be further equivalences, but the number of inequivalent, nontrivial, cyclic self-dual codes of length \( n \) is at most

\[
\frac{1}{2} \left( (2^a + 1)^{\delta(b)} - 1 \right).
\]
Examples: Since $\delta(b) = 0$ for $b = 1, 3, 5, 9, 11, 13, 17, \ldots$, for these values of $b$ there are no nontrivial codes of length $2^s \cdot b$.

For $b = 7$ we have

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

and $\delta(7) = 1$. Thus the first example of a nontrivial cyclic self-dual code is the $[14, 7, 4]$ code with

$$g(x) = (x + 1)(x^3 + x + 1)^2$$

$$= x^7 + x^6 + x^3 + x^2 + x + 1.$$ 

It is unique up to equivalence, and furthermore is equivalent to the code $D_{14}$ (or $e_7^2$) found by Pless in [10], although there it is not identified as a cyclic code. Similarly for $n = 28$ there are two inequivalent nontrivial codes, both with minimum distance four, and having generator polynomials

$$(x + 1)^2(x^3 + x + 1)^4,$$

$$(x + 1)^2(x^3 + x + 1)^3(x^3 + x^2 + 1).$$

Their group orders are $2^{15} \cdot 3^4 \cdot 7^4$ and $2^{18} \cdot 3 \cdot 7$, respectively.

Next, $\delta(15) = 1$, and there is a unique nontrivial self-dual code of length 30, with generator polynomial

$$(x + 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

$$(x^4 + x + 1)^2$$

$$= x^{15} + x^{14} + x^{12} + x^{10} + x^9 + x^8 + x^4 + x^3 + x + 1.$$ 

This is equivalent to the $[30, 15, 6]$ code $r_{10}$ described by Pless in [11], and is a shortened Reed–Muller code.

Continuing in this way, we find that for length less than or equal to 54 the only nontrivial cyclic self-dual codes are one of length 14, two of length 28, one of length 30, at most four of length 42, and one of length 46.

ACKNOWLEDGMENT

The symbolic manipulation program MACSYMA [8] was used to find some of the generator polynomials in Theorem 4. We also thank J. S. Leon for allowing us to use his code automorphism program [7] to determine the groups of the codes in Section III.

REFERENCES