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

$$\begin{bmatrix} 10 & \cdots & 010 & \cdots & 0 \\ 01 & \cdots & 001 & \cdots & 0 \\ & \cdots & & \cdots & \\ 00 & \cdots & 100 & \cdots & 1 \end{bmatrix}$$

(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 $n = 2^a \cdot b$, $a \geqslant 1$, $b \geqslant 1$ 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^a. Then C contains codewords of weight congruent to 2 modulo 4.

(For any undefined terms from coding theory or group theory see [8] or [13], respectively.) Note that G need not be the full automorphism group of the code.

Corollary 2: No binary cyclic self-dual code has all its weights divisible by four.

II. Proofs of Theorem 1 and Corollary 2

Let $\mathbb{F}_2^n$ denote the vector space of all binary n-tuples. If $C \subseteq \mathbb{F}_2^n$ is a code (i.e., a subspace of $\mathbb{F}_2^n$), the dual $C^\perp$ is the subspace

$$\{v \in \mathbb{F}_2^n \colon u \cdot v = 0, \text{ for all } u \in C\}.$$

Then C is self-dual if $C = C^\perp$.

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

$$(\mathbb{F}_2^n)_0 = \{v \in \mathbb{F}_2^n \colon vh = v, \text{ for all } h \in H\},$$
$$C_0 = C \cap (\mathbb{F}_2^n)_0.$$

Then

$$\dim (\mathbb{F}_2^n)_0 = 2 \dim C_0.$$

Proof of Theorem 1: Let P be the cyclic 2-Sylow subgroup of G, with generator π. Since $|P| = 2^a$, $|G| = 2^a \cdot e$, 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 $G|H \cong P$, $|H| = e$.

Let $C_0 = \{u \in C \colon uh = u, \text{ for all } h \in H\}$. 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 π must be transitive on the blocks, so $m \leqslant 2^a$, i.e., $m = 2^a$. Thus the orbits of H consist of 2^a blocks of length b.

Therefore the fixed subspace $(\mathbb{F}_2^n)_0$ has dimension 2^a, with one generator for each block. If the n coordinates are labeled appropriately, $(\mathbb{F}_2^n)_0$ has the generator matrix shown in Fig. 1. From Theorem 3, C_0 has dimension 2^{a-1}. Furthermore the action of π *on the blocks* (i.e., on $\mathbb{F}_2^{2^a}$) is represented by the $2^a \times 2^a$ matrix

$$A = \begin{bmatrix} 010 & \cdots & 0 \\ 001 & \cdots & 0 \\ & \cdots & \\ 000 & \cdots & 1 \\ 100 & \cdots & 0 \end{bmatrix}.$$

Manuscript received October 31, 1982.

N. J. A. Sloane is with the Mathematics and Statistics Research Center, Bell Laboratories, Murray Hill, NJ 07974.

J. G. Thompson is with the Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge, CB2 1SB England.

0018-9448/83/0500-0364$01.00 ©1983 IEEE

$$\begin{array}{cc} & \xleftrightarrow{\;b\;} \\ \updownarrow 2^a & \left[\begin{array}{cccc} 111 & 000 & \cdots & 000 \\ 000 & 111 & \cdots & 000 \\ & \cdots & \cdots & \\ 000 & 000 & \cdots & 111 \end{array}\right] \end{array}.$$

Fig. 1. Generator matrix for $(\mathbb{F}_2^n)_0$.

$$\begin{array}{cc} & \xleftrightarrow{\;b\;} \\ \updownarrow 2^{a-1} & \left[\begin{array}{cccccccc} 111 & 000 & \cdots & 000 & 111 & 000 & \cdots & 000 \\ 000 & 111 & \cdots & 000 & 000 & 111 & \cdots & 000 \\ & \cdots & \cdots & & \cdots & & & \cdots \\ 000 & 000 & \cdots & 111 & 000 & 000 & \cdots & 111 \end{array}\right] \end{array}$$

Fig. 2. Generator matrix for C_0.

The characteristic polynomial of A is

$$\det(\lambda I - A) = \lambda^{2^a} - 1 = (\lambda - 1)^{2^a},$$

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

$$B = \begin{bmatrix} 100 & \cdots & 000 \\ 110 & \cdots & 000 \\ 011 & \cdots & 000 \\ \cdots & \cdots & \cdots \\ 000 & \cdots & 110 \\ 000 & \cdots & 011 \end{bmatrix}.$$

From this it follows that there is a unique subspace X of $\mathbb{F}_2^{2^a}$ of every dimension k, $1 \leqslant k \leqslant 2^a$, that is fixed (setwise) by π. For with respect to the basis $v_1, \cdots, v_{2^a}$, π must be represented on X by the $k \times k$ matrix

$$\begin{bmatrix} 100 & \cdots & 00 \\ 110 & \cdots & 00 \\ 011 & \cdots & 00 \\ \cdots & \cdots & \\ 000 & \cdots & 10 \\ 000 & \cdots & 11 \end{bmatrix}.$$

Thus X is spanned by $v_1, \cdots, v_k$. In particular there is a unique subcode C_0 of dimension 2^{a-1}.

We can see directly (in terms of the old basis for $\mathbb{F}_2^n$) 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 σ 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 $\overleftarrow{f(x)} = x^{\deg f} f(1/x)$ denote the reciprocal polynomial. Then the dual code $C^{\perp}$ has generator polynomial $\overleftarrow{h(x)} = (x^n + 1)/\overleftarrow{g(x)}$, and we conclude that C is a cyclic self-dual code if and only if its generator polynomial satisfies

$$g(x)\overleftarrow{g(x)} = x^n + 1. \tag{1}$$

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

$$x^n + 1 = \Big\{ \prod_s M_s^{(b)}(x) \Big\}^{2^a}, \tag{2}$$

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

$$C_s^{(b)} = \{s, 2s, 4s, 8s, \cdots \pmod b\},$$

and

$$M_s^{(b)}(x) = \prod_{i \in C_s^{(b)}} (x - \xi^i),$$

where ξ is a primitive bth root of unity in some field containing GF(2) (see [8, ch. 7, §7]).

Let us call a cyclotomic coset $C_s^{(b)}$ *symmetric* if $-s \in C_s^{(b)}$, and otherwise *asymmetric*. The asymmetric cosets come in pairs $C_s^{(b)}$, $C_{-s}^{(b)}$, and we let $\delta(b)$ denote the number of such pairs. If $C_s^{(b)}$ is symmetric,

$$\overleftarrow{M_s^{(b)}(x)} = M_s^{(b)}(x),$$

while if $C_s^{(b)}$, $C_{-s}^{(b)}$ are an asymmetric pair,

$$\overleftarrow{M_s^{(b)}(x)} = M_{-s}^{(b)}(x).$$

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

$$g(x) = \prod_{\text{symmetric}} M_s^{(b)}(x)^{2^{a-1}} \cdot \prod_{\text{asymmetric}} M_s^{(b)}(x)^{i_s} M_{-s}^{(b)}(x)^{2^a - i_s}, \tag{3}$$

where in the first product there is one term for each symmetric coset $C_s^{(b)}$, in the second product there is one term for each asymmetric pair $C_s^{(b)}$, $C_{-s}^{(b)}$, and i_s is any number in the range $0 \leqslant i_s \leqslant 2^a$. 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 $i_s = 2^{a-1}$ in (3). The nontrivial codes, if any, fall into pairs of equivalent codes (for replacing all i_s by $2^a - i_s$ 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

$$\tfrac{1}{2}\{(2^a + 1)^{\delta(b)} - 1\}.$$

Examples: Since $\delta(b) = 0$ for $b = 1, 3, 5, 9, 11, 13, 17, \cdots$, for these values of b there are no nontrivial codes of length $2^a \cdot b$.

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

$$\begin{aligned} g(x) &= (x + 1)(x^3 + x + 1)^2 \\ &= x^7 + x^6 + x^3 + x^2 + x + 1. \end{aligned}$$

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

$$\begin{aligned} &(x + 1)^2(x^3 + x + 1)^4, \\ &(x + 1)^2(x^3 + x + 1)^3(x^3 + x^2 + 1). \end{aligned}$$

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

$$\begin{aligned} &(x + 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1) \\ &(x^4 + x + 1)^2 \\ &= x^{15} + x^{14} + x^{13} + x^{10} + x^6 + x^5 + x^4 + x^3 + x + 1. \end{aligned}$$

This is equivalent to the $[30, 15, 6]$ code r_{30} 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

[1] R. P. Anstee, M. Hall, Jr., and J. G. Thompson, "Planes of order 10 do not have a collineation of order 5," *J. Comb. Theory*, vol. 29A, pp. 39–58, 1980.
[2] S. D. Berman, "On the theory of group codes," *Cybern.*, vol. 3, no. 1, pp. 25–31, 1967.
[3] J. H. Conway and V. Pless, "On the enumeration of self-dual codes," *J. Comb. Theory*, vol. 28A, pp. 26–53, 1980.
[4] C. Hering, "On codes and projective designs," Kyoto University Math. Research Inst. Seminar Notes, 344, pp. 26–60, 1979.
[5] K. Hoffman and R. Kunze, *Linear Algebra*. Englewood Cliffs, NJ: Prentice-Hall, 1961, p. 187.
[6] B. Huppert, "Endliche Gruppen I," New York: Springer-Verlag, 1967.
[7] J. S. Leon, "Computing automorphism groups of error correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-28, no. 3, pp. 496–511, May 1982.
[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
[9] Mathlab Group, *MACSYMA Reference Manual*. Cambridge, MA: MIT, Version 9, 1977.
[10] V. Pless, "A classification of self-orthogonal codes over GF(2)," *Discrete Math.*, vol. 3, pp. 209–246, 1972.
[11] V. Pless, "The children of the (32, 16) doubly even codes," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 738–746, 1978.
[12] V. Pless and N. J. A. Sloane, "On the classification and enumeration of self-dual codes," *J. Comb. Theory*, vol. 18A, pp. 313–335, 1975.
[13] J. J. Rotman, *The Theory of Groups*, 2nd ed. Boston: Allyn and Bacon, 1973.
[14] N. J. A. Sloane, "Self-dual codes and lattices," in *Relations Between Combinatorics and Other Parts of Mathematics, Proc. Symp. Pure Math.*, vol. XXXIV, *Amer. Math. Soc.*, Providence, RI, 1979, pp. 273–308.
[15] H. Wielandt, *Finite Permutation Groups*. New York: Academic Press, 1964.