Algebraic and Combinatorial Coding Theory

PROCEEDINGS

Fifth International Workshop

June 1-7,1996
Sozopol, Bulgaria

Contents

Page

On the Extremal Binary Codes of Lengths 36 and 38 with an Automorphism of Order 5*

Vassil Yorgov and Nikolay Yankov

Konstantin Preslavsky University
Shoumen 9712, Bulgaria

Abstract

All inequivalent binary self-dual [36,18,8] codes with automorphism of order 5 are obtained. It is proved that there does not exist a [38,19,8] self-dual binary code with automorphism of order 5.

1 Introduction

The weight enumerators of self-dual codes of length 36 and 38 with minimal weight 8 are known [1]. For length 36 we have two enumerators:

$$(1) \qquad 1 + 225y^8 + 2016y^{10} + 9555y^{12} + 28800y^{14} \cdots$$

*This work is partially supported by the Bulgarian National Science Fondation under Contract MM-503/95

and

$$(2) \qquad 1 + 289y^8 + 1632y^{10} + 10387y^{12} + 28288y^{14} \cdots$$

The codes R_2 and D_3 given in [1] have weight enumerators (1) and (2), respectively, and the two possible weight enumerators for length 38 are realized by the codes D_4 and R_3. In [6, 2] it is proved that D_3 and D_4 are unique double circulant extremal codes for these lengths. All possible odd prime factors of the order of the group of automorphisms of an extremal code of length 36 and 38 are 17, 7, 5, 3 and 19, 7, 5, 3 respectively [7, 8]. It is proved there that there are correspondsingly 3 and 7 extremal codes of length 36 and 38 which have automorphism of order 7. Here we consider codes with automorphism of order 5.

2 Codes of length 36

Let C be a [36,18,8] self-dual code with automorphism σ of order 5. It is known [6] that σ fixes exactly 6 points. We may assume that $\sigma = (1,2,3,4,5)(5,6,7,8,9,10)...(26,27,28,29,30)$. Let $E_\sigma(C)$ be the set of those vectors in C which have even weight in each cycle of σ and zeros in the fixed points. Denote $F_\sigma(C) = \{v \in C | v\sigma = v\}$. It is known that $C = F_\sigma(C) \oplus E_\sigma(C)$. For $v \in F_\sigma(C)$ let πv be the vector of length 12 obtained from v by choosing a coordinate from each cycle of v and from each of the last 6 points. It is known that $\pi(F_\sigma(C))$ is a self-dual binary code [3]. All such codes are enumerated in [4]. In the notation used there $\pi(F_\sigma(C))$ is equivalent to one of the codes C_2^6, $C_2^2 \oplus A_8$, and B_{12}. As $\pi(F_\sigma(C))$ does not have a weight two vector with two ones in the last 6 positions, it cannot be equivalent to C_2^6 or $C_2^2 \oplus A_8$.

Lemma 1 *Up to a permutation of the last 6 coordinates the code $\pi(F_\sigma(C))$ is generated by one of the matrices F_1, F_2:*

$$\begin{pmatrix} 1&0&0&0&0&0&0&1&1&1&1&1\\ 0&1&0&0&0&0&1&0&1&1&1&1\\ 0&0&1&0&0&0&1&1&0&1&1&1\\ 0&0&0&1&0&0&1&1&1&0&1&1\\ 0&0&0&0&1&0&1&1&1&1&0&1\\ 0&0&0&0&0&1&1&1&1&1&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&0&1&0&1&1&1&1\\ 0&1&0&0&0&0&0&1&1&1&1&1\\ 0&0&1&0&0&0&1&1&1&0&0&0\\ 0&0&0&1&0&0&1&1&0&1&0&0\\ 0&0&0&0&1&0&1&1&0&0&1&0\\ 0&0&0&0&0&1&1&1&0&0&0&1 \end{pmatrix}.$$

Proof. Call a duo any pair of coordinates. A cluster for a code is a set of disjoint duos such that the union of any two duos is a support of a weight 4 vector of the code. A d-set of a cluster is a set of coordinates such that its intersection with each duo of the cluster is an one element set. A defining set of a code consist of a cluster and a d-set provided that the weight 4 vectors arrising from the cluster and the vector with support the d-set generate the code. B_{12} has a defining set. Each permutation which is a product of transpositions in even number of duos of the defining set is an automorphism of B_{12}. Since the minimal weight of C is 8, two duos of the cluster cannot be in the last 6 positions of $\pi(F_\sigma(C))$. There are two cases.

In the first case we assume that there is not a duo in the last 6 positions. Clearly the d-set cannot be in the last 6 positions. Using an appropriate automorphism of the above mentioned type we obtain that 5 coordinates of the d-set are in the last 6 positions of $\pi(F_\sigma(C))$. This leads to the first matrix of Lemma 1.

Secondly we consider the case when only one duo of B_{12} is in the last 6 positions of $\pi(F_\sigma(C))$. Hence there is also a duo in the first 6 positions. This leads to the second matrix.

Let $E_\sigma(C)^*$ be $E_\sigma(C)$ with the last 6 points deleted. Every vector v from $E_\sigma(C)^*$ has even weight in each cycle of σ. All words of length 5 of even weight form an irreducible cyclic

code which we denote by P. The non zero elements of P are given in table 1. They can be considered as polynomials on x. P is a field with primitive element α. Denote by $\phi(v)$ the

Table 1: Nonzero elements of P

e	01111	α	11000	α^2	10100
α^3	11110	α^4	10001	α^5	01001
α^6	11101	α^7	00011	α^8	10010
α^9	11011	α^{10}	00110	α^{11}	00101
α^{12}	10111	α^{13}	01100	α^{14}	01010

vector v considered as a 6-tuple with elements from P. It is known [3] that $\phi(E_\sigma(C)^*)$ is a [6,3] code which is self-dual under the inner product

$$(3) \qquad (u,v) = u_1v_1^4 + u_2v_2^4 + \cdots + u_6v_6^4$$

and next lemma holds.

Lemma 2 *The following transformations applied to C lead to an equivalent code with automorphism σ:*
(a) a substitution $x \to x^t$ in $\phi(E_\sigma(C)^*)$, $1 \le t \le 4$;
(b) a multiplication of any coordinate of $\phi(E_\sigma(C)^*)$ by α^{12};
(c) a permutation of the first 6 cycles of σ;
(d) a permutation of the last 6 coordinates of C.

The proof of the next lemma is omitted.

Lemma 3 *Every $[6,3,d \ge 3]$ code over the field P which is self-dual under the inner product (3) is equivalent under the transformations (a), (b), and (c) to one of the two codes with generator matrices:*

$$E_1 = \begin{pmatrix} e & 0 & 0 & 0 & \alpha^5 & \alpha^{10} \\ 0 & e & 0 & \alpha^5 & \alpha^5 & e \\ 0 & 0 & e & \alpha^{10} & e & \alpha^{10} \end{pmatrix} \text{ and } E_2 = \begin{pmatrix} e & 0 & 0 & e & \alpha^5 & \alpha^5 \\ 0 & e & 0 & e & \alpha^2 & \alpha^8 \\ 0 & 0 & e & e & \alpha^6 & \alpha^9 \end{pmatrix}.$$

Denote by C_{ij}, $1 \leq i \leq 2$, $1 \leq j \leq 2$, the code determined by the matrices F_i and E_j. A computer check shows that these 4 codes are extremal. The codes C_{11} and C_{12} have enumerator (1) and the codes C_{21} and C_{22} have enumerator (2). Thus we obtain

Theorem 1 *Up to equivalence the codes C_{11}, C_{12}, C_{21}, and C_{22} are the only self-dual [36,18,8] codes having automorphism of order 5.*

Remark. The codes C_{11}, C_{12}, and C_{21} are inequivalent. It is an open problem whether C_{21}, and C_{22} are equivalent.

3 Codes of length 38

Theorem 2 *There does not exist a [38,19,8] self-dual code with automorphism of order 5.*

Proof. Assume C is such a code with automorphism σ of order 5. It is known that σ must fix 8 points. Now $\pi(F_\sigma(C))$ is a self-dual code of length 14. There are 4 inequivalent such codes : C_2^7, $C_2^3 \oplus A_8$, $C_2 \oplus B_{12}$, and D_{14} [4]. It is easy to be seen that $\pi(F_\sigma(C))$ is not equivalent to C_2^7, $C_2^3 \oplus A_8$, and $C_2 \oplus B_{12}$. It remains that $\pi(F_\sigma(C))$ is equivalent to D_{14}. Consder a generator matrix of $\pi(F_\sigma(C))$ of the form

$$\begin{array}{|c|c|}\hline A & 0 \\ \hline 0 & B \\ \hline D & E \\ \hline \end{array}$$

where the matrices A, B, D, and E are of types $k_a \times 6$, $k_b \times 8$, $k_d \times 6$, and $k_e \times 8$ with k_a, k_b, k_d, and k_e being the ranks of A, B, D, and E, respectively. It is known [5, p.175] that $k_d = k_e$, $2k_a + k_d = 6$, and $2k_b + k_e = 8$. Hence $k_b = k_a + 1$ and $k_b \geq 1$. As B must generate a code of minimal weight at

least 8 we conclude that $k_b = 1$. Hence $B = (11111111)$ and $k_a = 0$. As the all one vector belongs to $\pi(F_\sigma(C))$ the vector 111111000000000 must be in $\pi(F_\sigma(C))$ too. This is in conflict with $k_a = 0$. The theorem is proved.

References

[1] J.H.Conway and N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory, vol.36, 1990, pp.1319-1333.

[2] M.Harada, T.Gulliver, H.Kaneta, Classificassion of extremal double circulant self-dual codes of length up to 62, preprint.

[3] W.Cary Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, IEEE Trans. Inform. Theory, vol.28, 1982, pp.511-521.

[4] V.Pless, A classification of self-orthogonal codes over GF(2), Discr. Math., vol.3, 1972, pp.209-246.

[5] V.Pless, Introduction to the theory of error-correcting codes, John Wiley and sons: New York, 1990.

[6] R.P.Ruseva, Uniqueness of the [36,18,8] double circulant code, Proceedings of the Intern. workshop on Optimal Codes and Related Topics, May 26-June 1, 1995, Sozopol, 126-129.

[7] R.P.Russeva, New extremal self-dual codes of length 36, Proc. of Twenty Fifth Spring Conf. of the UBM, 1996, pp.150-153 (in Bulgarian).

[8] R.P.Ruseva, On the extremal self-dual binary codes of length 38 with an automorphism of order 7, preprint.