Serdica

Mathematical Journal

Сердика

Математическо списание

Serdica Math. J. **25** (1999), 185-190

Serdica
Mathematical Journal

Institute of Mathematics
and Informatics, Bulgarian
Academy of Sciences

NEW BINARY EXTREMAL SELF-DUAL CODES OF LENGTHS 50 AND 52

Stefka Buyuklieva*

Communicated by R. Hill

Abstract. New extremal binary self-dual codes of lengths 50 and 52 are constructed. Some of them are the first known codes with such weight enumerators. The structure of their automorphisms groups are shown.

1. Introduction. A binary linear $[n, k]$ code C is a k-dimensional subspace of F_2^n where F_2^n is the n-dimensional vector space over the binary field F_2. The number of the non-zero coordinates of a vector in F_2^n is called its weight. An $[n, k, d]$ code is an $[n, k]$ linear code with minimum non-zero weight d. An automorphism of the code C is a permutation of the coordinates of C which preserves C.

Let $(u, v) = \sum_{i=1}^{n} u_i v_i \in F_2$ for $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in F_2^n$ be the inner product in F_2^n. Then if C is an $[n, k]$ code over F_2, $C^\perp = \{u \in F_2^n : (u, v) = 0 \text{ for all } v \in C\}$. If $C \subseteq C^\perp$, C is termed self-orthogonal and if $C = C^\perp$, C is self-dual. Self-dual codes with the largest minimum weight for a given length

1991 *Mathematics Subject Classification:* 05A05

Key words: Self-dual codes

This work was partially supported by the Bulgarian National Science Fund under Contract No. MM – 503/1995.

are called extremal. A list of possible weight enumerators of extremal self-dual codes of length up to 72 was given by Conway and Sloane in [3]. However, the existence of some extremal sef-dual codes is still unknown.

For length 50 these weight enumerators are

$$W(y) = 1 + 196y^{10} + 11368y^{12} + 31752y^{14} + \cdots \tag{1}$$

$$W(y) = 1 + (580 - 32\beta)y^{10} + (7400 + 160\beta)y^{12} + \cdots \tag{2}$$

where β is an integer parameter, $0 \le \beta \le 18$.

Self-dual codes with weight enumerator (1) are obtained by Huffman and Tonchev [6]. A code with weight enumerator (2) for $\beta = 0$ is shown in [3], and a code with weight enumerator (2) for $\beta = 1$ is found in [2]. We construct a binary self-dual [50,25,10] code with this weight enumerator for $\beta = 2$.

The possible weight enumerators for length 52 are

$$W(y) = 1 + 250y^{10} + 7980y^{12} + 4800y^{14} + \cdots \tag{3}$$

$$W(y) = 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + 53040y^{14} + \cdots \tag{4}$$

for $0 \le \beta \le 27$.

A self-dual [52,26,10] code with weight enumerator (3) is shown in [3]. Tsai constructed a code with weight enumerator (4) for $\beta = 0$ [8]. Harada obtained self-dual codes with weight enumerator (4) for $\beta = 1$ and 2 [4]. We construct self-dual [52,26,10] codes with weight enumerator (4) for $\beta = 0, 1, 2, 3, 4, 5, 6$.

2. Construction Methods. We use two construction methods.

A method for constructing binary self-dual codes with an automorphism of order 2 without fixed points is given in [1]. The basis of this method is the following theorem.

Theorem 1. *Let C' be a self-orthogonal $[k, s, d']$ code, C'' be its dual code and $\psi : C'' \to F_2^{2k}$ be the map defined by $\psi(v) = (\alpha_1, \alpha_1, \ldots, \alpha_k, \alpha_k)$ for $v = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in C''$. Let $M = \{(j_1, j_2), (j_3, j_4), \ldots, (j_{2r-1}, j_{2r})\}$ be a set of r pairs of different coordinates of the code C', $0 \le 2r \le k$, and $\tau : C' \to F_2^{2k}$ be the map defined by $\tau(v) = (\alpha'_1, \alpha''_1, \ldots, \alpha'_k, \alpha''_k)$ for $v = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in C'$, where $(\alpha'_i, \alpha''_i) = (\alpha_i, 0)$ for $i \ne j_l, l = 1, 2, \ldots, 2r$, and $(\alpha'_{j_{2i-1}}, \alpha''_{j_{2i-1}}, \alpha'_{j_{2i}}, \alpha''_{j_{2i}})$ is given in Table 1. Then $C = \tau(C') + \psi(C'')$ is a self-dual $[2k, k, d]$ code with $min\{d', 2d''\} \le d \le 2d''$, and $\sigma = (1, 2)(3, 4) \ldots (2k - 1, 2k)$ is an automorphism of C.*

Table 1.

$(\alpha_{j_{2i-1}}, \alpha_{j_{2i}})$	$(\alpha'_{j_{2i-1}}, \alpha''_{j_{2i-1}}, \alpha'_{j_{2i}}, \alpha''_{j_{2i}})$
(0,0)	(0,0,0,0)
(1,0)	(1,0,1,1)
(0,1)	(1,1,1,0)
(1,1)	(0,1,0,1)

The second construction was given by Harada in [5].

Theorem 2. *Let $x = (x_1, x_2, \ldots, x_n)$ be a vector in F_2^n such that $wt(x) \equiv n + 1 (\mathrm{mod}\ 2)$, and $G_0 = (I_n, A)$ be a generator matrix of a self-dual code C_0 of length $2n$ where I_n is the identity matrix of order n. Then the following matrix*

$$G = \begin{pmatrix} 1 & 0 & x_1 \ \ldots \ x_n & 1 \ \ldots \ 1 \\ y_1 & y_1 & & \\ \multicolumn{2}{c}{\ldots} & I_n & A \\ y_n & y_n & & \end{pmatrix}$$

where $y_i = x_i + 1 (\mathrm{mod}\ 2)$ $(1 \leq i \leq n)$, generates a self-dual code C of length $2n + 2$.

3. Results. We construct two binary self-dual [50,25,10] codes with automorphism $\sigma = (1, 2)(3, 4) \ldots (49, 50)$. We use a self-orthogonal [25,12,6] code with a generator matrix $G_{25} = (I_{12}\ B)$ where I_{12} is the identity matrix, and B is the 12×13 circulant matrix with first row 1100101111101.

$$G_{25} = \begin{pmatrix} 1000000000001100101111101 \\ 0100000000001110010111110 \\ 0010000000000111001011111 \\ 0001000000001011100101111 \\ 0000100000001101110010111 \\ 0000010000001110111001011 \\ 0000001000001111011100101 \\ 0000000100001111101110010 \\ 0000000010000111110111001 \\ 0000000001001011111011100 \\ 0000000000100101111101110 \\ 0000000000010010111110111 \end{pmatrix}$$

We get $r = 11$.
If the set $M = \{(1, 18), (2, 25), (3, 6), (5, 9), (7, 13), (10, 21), (11, 14), (12, 17),$

$(15,24), (16,23), (20,22)\}$ we obtain a self-dual [50,25,10] code $C_{50,1}$ with weight enumerator (2) for $\beta = 0$. If the set $M = \{(2,7), (3,5), (4,20), (6,12), (8,11), (9,18), (10,25), (13,23), (15,19), (16,22), (17,24)\}$ we obtain an extremal self-dual [50,25,10] code $C_{50,2}$ with generator matrix $G_{50,2}$ and with weight enumerator (2) for $\beta = 2$. This code is the first known code with this weight enumerator. Using a computer program we obtain that the order of its automorphism group is 2. Hence σ is the unique nontrivial automorphism of this code.

Using the code $C_{50,2}$ and the construction method from Theorem 2 we obtain extremal self-dual codes of length 52 with weight enumerators (4) for $\beta = 2, 3, 4, 5, 6$. All these codes have trivial automorphism groups. They are listed in Table 3.

Table 2. Extremal self-dual [52,26,10] codes.

vector x	β
000110100111101101111010	2
001111100001101110000101	3
000101000000100001111011	4
000000001101001001010000	5
000001110101101111101101	6

There exists a unique self-dual [26,13,6] code [7]. The matrix $G_{26} = (I_{13}\ D)$ where D is a circulant matrix with first row 0010111110111 generates this code.

$$G_{26} = \begin{pmatrix} 10000000000000010111110111 \\ 01000000000000101111101110 \\ 00100000000001011111011100 \\ 00010000000000111110111001 \\ 00001000000001111101110010 \\ 00000100000001111011100101 \\ 00000010000001110111001011 \\ 00000001000001101110010111 \\ 00000000100001011100101111 \\ 00000000010000111001011111 \\ 00000000001001110010111110 \\ 00000000000101100101111101 \\ 00000000000011001011111011 \end{pmatrix}$$

We use it to construct the self-dual [52,26,10] codes listed in Table 3. All these codes have groups of automorphisms of order 2. Hence they are not equivalent to the codes from Table 2.

Table 3. Extremal self-dual [52,26,10] codes.

r	set M	weight enumerator
12	(1,21)(2,4)(3,10)(5,26)(6,24)(7,12) (8,18)(9,14)(11,15)(16,20)(17,19)(23,25)	(4) for $\beta = 0$
11	(1,9)(3,25)(4,23)(5,7)(6,26)(8,22) (10,12)(11,21)(14,18)(16,20)(17,19)	(4) for $\beta = 1$
13	(1,11)(2,8)(3,18)(4,17)(5,6)(7,25)(9,10) (12,13)(14,24)(15,26)(16,22)(19,21) (20,23)	(4) for $\beta = 2$
12	(1,19)(2,22)(3,6)(5,13)(7,10)(9,17) (11,12)(14,18)(15,20)(16,21)(23,26)(24,25)	(4) for $\beta = 3$
11	(1,17)(2,18)(3,15)(4,22)(5,24)(6,11) (8,10)(9,12)(16,25)(19,20)(21,23)	(4) for $\beta = 4$
12	(1,14)(2,6)(3,12)(4,8)(5,19)(7,16)(9,25) (10,24)(11,23)(13,20)(15,17)(21,26)	(4) for $\beta = 5$
11	(1,7)(3,13)(4,17)(5,9)(6,23)(8,19) (10,21)(11,16)(12,25)(15,18)(20,24)	(3)

$$
G_{50,2} = \begin{pmatrix}
11110011111111110011000011000000000000000000000000 \\
11111100111111111100110000110000000000000000000000 \\
00111111001111111111001100001100000000000000000000 \\
00001111110011111111110000000011000000000000000000 \\
11000011111100111111111100000000110000000000000000 \\
00110000111111001111111100000000001100000000000000 \\
11001100001111110011111100000000000011000000000000 \\
11110011000011111100111100000000000000110000000000 \\
11111100110000111111001100000000000000001100000000 \\
11111111001100001111110000000000000000000011000000 \\
11111111110011000011111100000000000000000000110000 \\
00111111111100110000111100000000000000000000001100 \\
11001111111111001100001100000000000000000000000011 \\
00000011001100001111001011000100011001101000100110 \\
00000011000000111100100011101101011010100001100100 \\
00000000000000001110000001000101101001001001011111 \\
00000011000000000111000000101001100111101001001110 \\
00000011000000100000110010100110010001101011110100 \\
00110011000010001111000001100110001001100011010010 \\
00000000001000001111001110100111011001000010110110 \\
00001100100000001111000001100010011000001011010110 \\
00000001000000000011000001001001010011010001010110 \\
00001000110000000011000011100101110001001001101010 \\
00100011000011001100000001101011111011101010011000 \\
10000011000000000011000001101111100010101010011110
\end{pmatrix}
$$

Acknowledgment. The author wishes to thank Dr.Kapralov for his help in calculating the order of the automorphism groups of the codes.

REFERENCES

[1] S. Buyuklieva, I. Boukliev. Extremal self-dual codes with an automorphism of order 2. *IEEE Trans. Inform. Theory* January (1998), to appear.

[2] I. Boukliev, S. Buyuklieva. Some New Extremal Self-Dual Codes with Lengths 44, 50, 54 and 58. *IEEE Trans. Inform. Theory* March (1998), to appear.

[3] J. H. Conway, N. J. A. Sloane. A New Upper Bound on the Minimal Distance of Self-Dual Codes. *IEEE Trans. Inform. Theory* **36** (1991), 1319-1333.

[4] M. Harada. Existence of new extremal double-even codes and extremal singly-even codes. *Designs, Codes and Cryptography* **8** (1996), 1-12.

[5] M. Harada. The existence of a self-dual [70,35,12] code and formally self-dual codes, *Finite Fields and Their Appl.* **3** (1997), 131-139.

[6] W. C. Huffman, V. D. Tonchev. The existence of extremal [50,25,10] codes and quasi-symmetric 2-(49,9,6) designs. *Designs, Codes and Cryptography* **6** (1995), 97-106.

[7] V. Pless. The children of the [32,16] doubly even codes. *IEEE Trans. Inform. Theory* **24** (1982), 738-746.

[8] H. P. Tsai. Existence of some extremal self-dual codes. *IEEE Trans. Inform. Theory* **38** (1992), 1829-1833.

Stefka Buyuklieva
Faculty of Mathematics and Informatics
Veliko Tarnovo University
5000 Veliko Tarnovo
Bulgaria

Received December 19, 1997