AAECC **14**, 75–79 (2003)
Digital Object Identifier (DOI) 10.1007/s00200-003-0126-4

AAECC
Applicable Algebra in Engineering, Communication and Computing

Some Extremal Self-Dual Codes with an Automorphism of Order 7

Radinka Dontcheva[1], **Masaaki Harada**[2]

[1] Faculty of Information Technology and Systems, Delft University of Technology, Mekelweg 4, 2628 CD Delft, The Netherlands On leave from University of Shumen, Bulgaria
[2] Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan

Received: January 29, 2001; revised version: December 8, 2001

Abstract. In this note, some new extremal singly-even self-dual codes of lengths 60 and 64 are constructed using automorphisms of order 7. These codes have weight enumerators for which no extremal self-dual codes were previously known to exist.

Keywords: Self-dual codes, Automorphisms and weight enumerators.

1 Introduction

A binary $[n, k]$ code C is a k-dimensional vector subspace of $GF(2)^n$, where GF(2) is the field of two elements. The weight of a vector is the number of its nonzero coordinates. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. A code C is *self-dual* if $C = C^\perp$ where $C^\perp$ is the dual code of C under the standard inner product. A self-dual code C is *doubly-even* if all codewords of C have weight divisible by four, and *singly-even* if there is at least one codeword of weight $\equiv 2 \pmod 4$. An automorphism of C is a permutation of the coordinates of C which preserves C. The set consisting of all automorphisms of C is called the automorphism group of C.

A singly-even self-dual code is called *extremal* if it has the highest minimum weight for that length. Conway and Sloane [4] proved new upper bounds for the minimum weights of singly-even self-dual codes and gave a list of the possible weight enumerators of singly-even self-dual codes meeting the bounds with equality for lengths up to 64 and length 72. For example, the highest minimum weights of self-dual codes of lengths 60 and 64 are both equal to 12.

In this note, we study extremal singly-even self-dual codes of lengths 60 and 64 with an automorphism of order 7 using the theory developed by Huffman and Yorgov (cf. [9] and [15]). Extremal singly-even self-dual codes of lengths

42, 50, 52 and 54 with automorphisms of order 7 have been investigated in [17], [10], [11] and [13], respectively. In this note, their work is extended to lengths 60 and 64.

2 An Extremal Self-Dual [60, 30, 12] Code

The weight enumerators of extremal singly-even self-dual [60, 30, 12] codes are known from [4] and [6]:

$$W_{60,1} = 1 + (2555 + 64\beta)y^{12} + (33600 - 384\beta)y^{14} + \cdots \ (0 \le \beta \le 10),$$

$$W_{60,2} = 1 + 3451y^{12} + 24128y^{14} + \cdots ,$$

where β is a parameter. For the weight enumerator $W_{60,1}$, extremal self-dual codes with $\beta = 10$ were constructed in [6]. For the weight enumerator $W_{60,2}$, an extremal self-dual code was constructed in [4]. Recently, it was announced in [14] that an extremal self-dual code with $W_{60,1}$ for $\beta = 0$, exists. In this section, we construct an extremal singly-even self-dual [60, 30, 12] code with an automorphism of order 7. We make use of the theory developed in [9] and [15]. Recently many new extremal self-dual codes have been constructed having an automorphism of order 7, using the above theory (cf. [10], [11], [13] and [17]). Hence, we only give the results instead of describing our construction in detail.

Suppose that σ is an automorphism of order 7 of an extremal singly-even self-dual [60, 30, 12] code. As a consequence of [15, Theorem 1], σ has 8 independent 7-cycles and 4 fixed points. Hence we may assume that $\sigma = (1, 2, \ldots , 7)(8, 9, \ldots , 14) \cdots (50, 51, \ldots , 56)$. Using the theory in [9] and [15], we found an extremal singly-even self-dual [60, 30, 12] code C_{60}. The code C_{60} has the following generator matrix

$$G_{60} = \left(\begin{array}{cccccccc|cccc}
j & j & & & & & & & 1 & 1 & & \\
 & j & j & & & & & & & 1 & 1 & \\
 & & j & j & & & & & & & 1 & 1 \\
 & & & j & j & j & & & & & & 1 \\
 & & & & j & j & j & j & & & & \\
j & j & j & j & & j & & j & & & & \\
\hline
A_1 & & & & A_1 & A_1 & A_1 & A_1 & & & & \\
 & A_1 & & & A_1 & & & A_1 & & & & \\
 & & A_1 & & A_1 & & & A_2 & & & & \\
 & & & A_1 & A_1 & A_3 & A_2 & A_4 & & & & \\
B_1 & B_1 & B_1 & B_1 & B_1 & & & & & & & \\
B_1 & & & B_3 & & B_1 & & & & & & \\
B_1 & & & B_2 & & & B_1 & & & & & \\
B_1 & B_1 & B_2 & B_4 & & & & B_1 & & & &
\end{array}\right),$$

where j is the all-one vector of length 7, and $A_1, \ldots , A_4$, $B_1, \ldots , B_4$ are the right circulant 3×7 matrices with first rows (1110100), (0111010), (0011101), (1010011), (1001011), (1100101), (1110010), (0101110), respectively, and the blanks are filled up with zero's.

The code C_{60} corresponds to the weight enumerator $W_{60,1}$ where $\beta = 7$. Moreover, using Magma, we verified that the automorphism group of C_{60} is of order 14

Proposition 1. *There exists an extremal singly-even self-dual* [60, 30, 12] *code with weight enumerator* $W_{60,1}$ *for* $\beta = 7$.

3 Extremal Self-Dual [64, 32, 12] Codes

For length 64, two possible weight enumerators of extremal singly-even self-dual codes are given in [4]:

$$W_{64,1} = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \cdots (14 \le \beta \le 284) \text{ and}$$

$$W_{64,2} = 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \cdots (0 \le \beta \le 277),$$

where β is a parameter. For the weight enumerator $W_{64,1}$, extremal self-dual codes are known for $\beta = 18$ [12] and $\beta = 44$ [2]. For the weight enumerator $W_{64,2}$, extremal self-dual codes exist for $\beta = 32$ [4], $\beta = 40$ [3] and $\beta = 64$ [7]. Recently, an extremal self-dual code with $\beta = 14$ in $W_{64,1}$ has been constructed in [1]. An extremal self-dual code with weight enumerator $W_{64,2}$ where $\beta = 10$ has been also found in [8].

Similarly to the previous section, we consider an extremal singly-even self-dual [64, 32, 12] code with an automorphisms of order 7. Suppose that ϕ is an automorphism of order 7 of an extremal singly-even self-dual [64, 32, 12] code. By Lemma 5 in [16], ϕ has either 9 cycles of length 7 and 1 fixed point or 8 cycles of length 7 and 8 fixed points. Note that this also follows from Theorem 1 in [15]. In addition, by considering the decomposition structure, it is not hard to show that ϕ cannot be of the second type. Hence, we may assume that $\phi = (1, 2, \ldots, 7)(8, 9, \ldots, 14) \cdots (57, 58, \ldots, 63)$. By the method given in [15], we found a number of examples of extremal singly-even self-dual codes of length 64 with automorphism ϕ. We have found seven codes $C_{64,i}$, $1 \le i \le 7$ with weight enumerators $W_{64,2}$ for $\beta = 2, 9, 16, 23, 30, 37$ and 44, respectively. We verified by Magma that the automorphism groups of the codes are all of order 7.

Proposition 2. *There exist extremal singly-even self-dual* [64, 32, 12] *codes with weight enumerators* $W_{64,2}$ *for* $\beta = 2, 9, 16, 23, 30, 37$ *and* 44.

We now present generator matrices $G_{64,i}$ for these codes. Define the matrix A as

$$A = \left(\begin{array}{ccccccccc|c} j & j & & & & & & & & \\ & & j & j & j & j & & & & \\ & & & & j & j & j & j & & \\ & & & & & & j & j & j & 1 \\ & & j & & j & & j & & j & \end{array}\right).$$

Moreover, we define matrices D_i, $1 \le i \le 7$, respectively, as

$$\begin{pmatrix} E_1 & & & & & E_1 & E_1 & E_1 & E_1 \\ & E_1 & & & & E_1 & & & E_1 \\ & & E_1 & & & E_1 & & & E_2 \\ & & & E_1 & & E_1 & E_3 & E_7 & E_5 \\ & & & & E_1 & E_1 & E_3 & & E_6 \\ H_1 & H_1 & H_1 & H_1 & H_1 & H_1 & & & \\ H_1 & & & H_3 & H_3 & & H_1 & & \\ H_1 & & & H_7 & & & & H_1 & \\ H_1 & H_1 & H_2 & H_5 & H_6 & & & & H_1 \end{pmatrix}, \begin{pmatrix} E_1 & & & & & E_1 & E_1 & E_1 & E_1 \\ & E_1 & & & & E_1 & & & E_1 \\ & & E_1 & & & E_1 & & & E_2 \\ & & & E_1 & & E_1 & & E_1 & E_3 \\ & & & & E_1 & E_1 & E_2 & E_2 & \\ H_1 & H_1 & H_1 & H_1 & H_1 & H_1 & & & \\ H_1 & & & & H_2 & & H_1 & & \\ H_1 & & & H_1 & H_2 & & & H_1 & \\ H_1 & H_1 & H_2 & H_3 & & & & & H_1 \end{pmatrix},$$

$$\begin{pmatrix} E_1 & & & & & E_1 & E_1 & E_1 & E_1 \\ & E_1 & & & & E_1 & & & E_1 \\ & & E_1 & & & E_1 & & & E_2 \\ & & & E_1 & & E_1 & & E_7 & E_2 \\ & & & & E_1 & E_1 & E_6 & E_2 & E_7 \\ H_1 & H_1 & H_1 & H_1 & H_1 & H_1 & & & \\ H_1 & & & & H_6 & & H_1 & & \\ H_1 & & & H_7 & H_2 & & & H_1 & \\ H_1 & H_1 & H_2 & H_2 & H_7 & & & & H_1 \end{pmatrix}, \begin{pmatrix} E_1 & & & & & E_1 & E_1 & E_1 & E_1 \\ & E_1 & & & & E_1 & & & E_1 \\ & & E_1 & & & E_1 & & & E_2 \\ & & & E_1 & & E_1 & & E_6 & E_6 \\ & & & & E_1 & E_1 & E_5 & E_3 & E_5 \\ H_1 & H_1 & H_1 & H_1 & H_1 & H_1 & & & \\ H_1 & & & & H_5 & & H_1 & & \\ H_1 & & & H_6 & H_3 & & & H_1 & \\ H_1 & H_1 & H_2 & H_6 & H_5 & & & & H_1 \end{pmatrix},$$

$$\begin{pmatrix} E_1 & & & & & E_1 & E_1 & E_1 & E_1 \\ & E_1 & & & & E_1 & & & E_1 \\ & & E_1 & & & E_1 & & & E_2 \\ & & & E_1 & & E_1 & E_1 & E_2 & E_4 \\ & & & & E_1 & E_1 & E_3 & E_3 & \\ H_1 & H_1 & H_1 & H_1 & H_1 & H_1 & & & \\ H_1 & & & H_1 & H_3 & & H_1 & & \\ H_1 & & & H_2 & H_3 & & & H_1 & \\ H_1 & H_1 & H_2 & H_4 & & & & & H_1 \end{pmatrix}, \begin{pmatrix} E_1 & & & & & E_1 & E_1 & E_1 & E_1 \\ & E_1 & & & & E_1 & & & E_1 \\ & & E_1 & & & E_1 & & & E_2 \\ & & & E_1 & & E_1 & E_5 & E_5 & E_5 \\ & & & & E_1 & E_1 & E_4 & E_5 & \\ H_1 & H_1 & H_1 & H_1 & H_1 & H_1 & & & \\ H_1 & & & H_5 & H_4 & & H_1 & & \\ H_1 & & & H_5 & H_5 & & & H_1 & \\ H_1 & H_1 & H_2 & H_5 & & & & & H_1 \end{pmatrix},$$

$$\begin{pmatrix} E_1 & & & & & E_1 & E_1 & E_1 & E_1 \\ & E_1 & & & & E_1 & & & E_1 \\ & & E_1 & & & E_1 & & & E_2 \\ & & & E_1 & & E_1 & E_1 & E_2 & E_4 \\ & & & & E_1 & E_1 & E_7 & E_6 & E_7 \\ H_1 & H_1 & H_1 & H_1 & H_1 & H_1 & & & \\ H_1 & & & H_1 & H_7 & & H_1 & & \\ H_1 & & & H_2 & H_6 & & & H_1 & \\ H_1 & H_1 & H_2 & H_4 & H_7 & & & & H_1 \end{pmatrix},$$

where $E_1, E_2, \ldots, E_7, H_1, H_2, \ldots, H_7$ are the right circulant 3×7 matrices with first rows (1110100), (0111010), (0011101), (1001110), (0100111), (1010011), (1101001), (1001011), (1100101), (1110010), (0111001), (1011100), (0101110), (0010111), respectively. Then the generator matrix $G_{64,i}$ $(i = 1, 2, \ldots, 7)$ is defined as

$$G_{64,i} = \left(\begin{array}{c|c} \multicolumn{2}{c}{A} \\ \hline & 0 \\ D_i & \vdots \\ & 0 \end{array}\right).$$

References

1. Betsumiya, K., Gulliver, T.A., Harada, M., Munemasa, A.: On Type II codes over $\mathbb{F}_4$. IEEE Trans. Inform. Theory **47**, 2242–2248 (2001)
2. Buyuklieva, S.: On the binary self-dual codes with an automorphism of order 2. Designs, Codes and Cryptogr. **12**, 39–48 (1997)

3. Buyuklieva, S.: A method for constructing self-dual codes with applications to length 64. Proc. Alg. Combin. Coding Theory, Sozopol, Bulgaria, 1996
4. Conway, J.H., Sloane, N.J.A.: A new upper bound on the minimal distance of self-dual codes. IEEE Trans. Inform. Theory **36**, 1319–1333 (1990)
5. Dougherty, S.T., Gulliver, T.A., Harada, M.: Extremal binary self-dual codes. IEEE Trans. Inform. Theory **43**, 2036–2047 (1997)
6. Gulliver, T.A., Harada, M.: Weight enumerators of extremal singly-even [60, 30, 12] codes. IEEE Trans. Inform. Theory **42**, 658–659 (1996)
7. Gulliver, T.A., Harada, M.: Classification of extremal double circulant self-dual codes of lengths 64 to 72. Designs, Codes and Cryptogr. **13**, 257–269 (1998)
8. Gulliver, T.A., Harada, M., Kim, J.-L.: Construction of some extremal self-dual codes. Discrete Math. **263**, 81–91 (2003)
9. Huffman, W.C.: Automorphisms of codes with applications to extremal doubly even codes of length 48. IEEE Trans. Inform. Theory **28**, 511–521 (1982)
10. Huffman, W.C., Tonchev, V.D.: The existence of extremal self-dual [50, 25, 10] codes and quasi-symmetric 2-(49, 9, 6) designs. Designs, Codes and Cryptogr. **6**, 97–106 (1996)
11. Huffman, W.C., Tonchev, V.D.: The [52, 26, 10] binary self-dual codes with an automorphism of order 7. Finite Fields and Their Appl. **7**, 341–349 (2001)
12. Pless, V., Tonchev, V., Leon, J.: On the existence of a certain (64, 32, 12) extremal codes. IEEE Trans. Inform. Theory **39**, 214–215 (1993)
13. Tonchev, V.D., Yorgov, V.Y.: The existence of certain extremal [54, 27, 10] self-dual codes. IEEE Trans. Inform. Theory **42**, 1628–1631 (1996)
14. Tsai, H.-P., Jiang, Y.-J.: Some new extremal self-dual [58, 29, 10] codes. IEEE Trans. Inform. Theory **44**, 813–814 (1998)
15. Yorgov, V.Y.: Binary self-dual codes with automorphisms of odd order. (in Russian), Probl. Perda. Inform. **19**, 11–24 (1983); English translation in Probl. Inform. Transm. **19**, 260–270 (1983)
16. Yorgov, V.Y.: Doubly-even extremal codes of length 64. (in Russian), Probl. Perda. Inform. **22**, 35–42 (1986); English translation in Probl. Inform. Transm. **22**, 277–284 (1986)
17. Yorgov, V.Y.: The extremal codes of length 42 with automorphism of order 7. Discrete Math **190**, 201–213 (1998)