

# A Complete Classification of Doubly Even Self-Dual Codes of Length 40\*

Masaaki Harada<sup>†</sup>

April 19, 2011

## Abstract

A complete classification of binary doubly even self-dual codes of length 40 is given. As a consequence, a classification of binary extremal self-dual codes of length 38 is also given.

## 1 Introduction

As described in [18], self-dual codes are an important class of linear codes for both theoretical and practical reasons. It is a fundamental problem to classify self-dual codes of modest lengths and much work has been done towards classifying self-dual codes over  $\mathbb{F}_q$  for  $q = 2$  and  $3$ , where  $\mathbb{F}_q$  denotes the finite field of order  $q$  and  $q$  is a prime power (see [18]).

Codes over  $\mathbb{F}_2$  are called *binary* and all codes in this paper are binary. The *dual code*  $C^\perp$  of a code  $C$  of length  $n$  is defined as  $C^\perp = \{x \in \mathbb{F}_2^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ , where  $x \cdot y$  is the standard inner product. A code  $C$  is called *self-dual* if  $C = C^\perp$ . 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  $\equiv 2 \pmod{4}$ . It is known that a self-dual code of length  $n$  exists if and only if  $n$  is even, and a doubly even self-dual code of length  $n$  exists if and only if  $n$  is divisible by eight. The minimum weight  $d$  of

---

\*This work was supported by JST PRESTO program.

<sup>†</sup>Department of Mathematical Sciences, Yamagata University, Yamagata 990-8560, Japan, and PRESTO, Japan Science and Technology Agency (JST), Kawaguchi, Saitama 332-0012, Japan. email: mharada@sci.kj.yamagata-u.ac.jp.

a self-dual code of length  $n$  is bounded by  $d \leq 4\lfloor \frac{n}{24} \rfloor + 6$  if  $n \equiv 22 \pmod{24}$ ,  $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$  otherwise [13] and [17]. A self-dual code meeting the bound is called *extremal*.

Two codes are *equivalent* if one can be obtained from the other by permuting the coordinates. 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  $C$  and it is denoted by  $\text{Aut}(C)$ .

A classification of doubly even self-dual codes was done for lengths 8, 16 in [15], for length 24 in [16] and for length 32 in [6]. The main aim of this paper is to give a classification of doubly even self-dual codes of length 40.

**Theorem 1.** *There are 94343 inequivalent doubly even self-dual codes of length 40, 16470 of which are extremal.*

*Remark 2.* A classification of extremal doubly even self-dual codes of length 40 was recently obtained in [1] by somewhat different techniques. This was indicated by Akihiro Munemasa in a private communication [14].

As a summary, we list in Table 1 the total number  $N_T(n)$  of inequivalent doubly even self-dual codes of length  $n$  and the number  $N_d(n)$  of inequivalent doubly even self-dual codes of length  $n$  ( $n = 8, 16, \dots, 40$ ) and minimum weight  $d$  ( $d = 4, 8$ ).

Table 1: Number of doubly even self-dual codes

Length $n$	$N_T(n)$	$N_4(n)$	$N_8(n)$
8	1	1	-
16	2	2	-
24	9	8	1
32	85	80	5
40	94343	77873	16470

A classification of singly even self-dual codes of lengths up to 36 is known [2], [3], [6], [9], [15], [16]. As a consequence of Theorem 1, we give a classification of extremal singly even self-dual codes of length 38.

Generator matrices of all inequivalent doubly even self-dual codes of length 40 and extremal self-dual codes of length 38 can be obtained electronically from [10]. All computer calculations in this paper were done by MAGMA [4].

## 2 Classification method

In this section, we describe how to complete a classification of doubly even self-dual codes of length 40.

The number of distinct doubly even self-dual codes of length  $n$  is given [12] by the formula:

$$\prod_{i=0}^{n/2-2} (2^i + 1). \quad (1)$$

King [11] determined the number of distinct extremal doubly even self-dual codes of length 40. Let  $N(40, d)$  denote the number of distinct doubly even self-dual codes of length 40 and minimum weight  $d$  ( $d = 4, 8$ ). Then we have

$$\begin{aligned} N(40, 4) &= 4009357722800739726876619952910304312989584368968750, \\ N(40, 8) &= 10263335567003567415076803513287627980544163840000000. \end{aligned}$$

Let  $C$  be a singly even self-dual code and let  $C_0$  denote the subcode of codewords having weight  $\equiv 0 \pmod{4}$ . Then  $C_0$  is a subcode of codimension 1. The *shadow*  $S$  of  $C$  is defined to be  $C_0^\perp \setminus C$  [7]. There are cosets  $C_1, C_2, C_3$  of  $C_0$  such that  $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ , where  $C = C_0 \cup C_2$  and  $S = C_1 \cup C_3$ .

**Proposition 3** (Brualdi and Pless [5]). *Let  $C$  be a self-dual code of length  $n \equiv 6 \pmod{8}$ . Let  $C_0, C_1, C_2$  and  $C_3$  be as above. Then*

$$\begin{aligned} C^* &= \{(v, 0, 0) \mid v \in C_0\} \cup \{(v, 1, 1) \mid v \in C_2\} \\ &\quad \cup \{(v, 1, 0) \mid v \in C_1\} \cup \{(v, 0, 1) \mid v \in C_3\} \end{aligned}$$

*is a doubly even self-dual code of length  $n + 2$ .*

There are 519492 inequivalent self-dual codes of length 36 [9]. By considering the direct sum of the unique self-dual code of length 2 and each of these codes, we have 519492 self-dual codes of length 38 and minimum weight 2. By Proposition 3, 519492 doubly even self-dual codes of length 40 and minimum weight 4 are constructed.

We examine the equivalence or inequivalence of codes as follows. Let  $C$  be a doubly even self-dual code of length 40 and minimum weight  $d$  ( $d = 4, 8$ ). Let  $M(C)$  be the  $A_8 \times 40$  matrix with rows composed of the codewords of

weight 8 in  $C$ , where the  $(1, 0)$ -matrix  $M(C)$  is regarded as a matrix over  $\mathbb{Z}$ , and  $A_w$  denotes the number of codewords of weight  $w$ . We define

$$N(C) = \begin{cases} \{n_{ij} \mid 1 \leq i, j \leq 40\} \setminus \{57\} & \text{if } C \text{ is extremal} \\ \{n_{ij} \mid 1 \leq i, j \leq 40\} & \text{otherwise,} \end{cases}$$

where  $n_{ij}$  is the  $(i, j)$ -entry of  $M(C)^T M(C)$ , and  $M(C)^T$  denotes the transpose of  $M(C)$ . The codewords of weight  $w$  in  $C$  are calculated by the MAGMA function `Words`. Note that the codewords of weight 8 in  $C$  form a  $1$ -(40, 8, 57) design when  $C$  is extremal. This means that  $n_{ii} = 57$  for any  $i$  ( $i = 1, 2, \dots, 40$ ) and  $\max\{n_{ij} \mid 1 \leq i, j \leq 40\} = 57$  when  $C$  is extremal. Then we consider the following:

$$\alpha(C) = (\#\text{Aut}(C), A_4, \max N(C), \min N(C), \#N(C)).$$

The automorphism group  $\text{Aut}(C)$  is calculated by the MAGMA function `AutomorphismGroup`. Of course,  $C$  and  $C'$  are inequivalent if  $\alpha(C) \neq \alpha(C')$ . For a given set of codes, we divided into classes where each class contains codes  $C$  with identical  $\alpha(C)$ . Then we divided the codes in each class into equivalence classes. This was done by the MAGMA function `IsIsomorphic`.

In this way, we checked equivalences among the above 519492 doubly even self-dual codes of length 40 and minimum weight 4 constructed by Proposition 3. Then we obtained the set  $\mathcal{C}_{40,4}$  of 77873 inequivalent doubly even self-dual codes with minimum weight 4 satisfying

$$\sum_{C \in \mathcal{C}_{40,4}} \frac{40!}{\#\text{Aut}(C)} = N(40, 4). \quad (2)$$

This shows that there is no other doubly even self-dual code of length 40 and minimum weight 4.

For constructing extremal doubly even self-dual codes of length 40, we employ the following method, together with Proposition 3.

**Proposition 4** (Kimura and Harada [8]). *Let  $A$  be a  $4n \times 4n$  matrix satisfying that  $\text{wt}(a_i) \equiv 3 \pmod{4}$  and  $AA^T = I_{4n}$ , where  $a_i$  is the  $i$ -th row of  $A$ ,  $\text{wt}(x)$  denotes the weight of a vector  $x$ ,  $I_m$  is the identity matrix of order  $m$ . Let  $t$  be a vector of length  $4n$  and even weight. Let  $B$  be the  $4n \times 4n$  matrix with  $i$ -th row*

$$b_i = \begin{cases} a_i + t, & \text{if } \text{wt}(a_i + t) \equiv 3 \pmod{4} \\ a_i + t + \mathbf{1}, & \text{otherwise,} \end{cases}$$

where  $\mathbf{1}$  is the all-one vector. Then the matrix  $( I_{4n} , B )$  generates a doubly even self-dual code of length  $8n$ .

Many extremal doubly even self-dual codes of length 40 are known (see e.g. [18]). From some known extremal doubly even self-dual codes and new extremal doubly even self-dual codes found by Propositions 3 and 4, we obtained the set  $\mathcal{C}_{40,8}$  of 16470 inequivalent extremal doubly even self-dual codes satisfying

$$\sum_{C \in \mathcal{C}_{40,8}} \frac{40!}{\# \text{Aut}(C)} = N(40, 8). \quad (3)$$

From (2) and (3), it follows that there is no other doubly even self-dual code of length 40. Therefore, we have Theorem 1.

The weight enumerator of a doubly even self-dual code of length 40 can be written as:

$$1 + A_4 y^4 + (285 + 24A_4) y^8 + (21280 + 92A_4) y^{12} \\ + (239970 - 600A_4) y^{16} + (525504 + 966A_4) y^{20} + \cdots + y^{40},$$

(see e.g. [13]). The numbers  $N(A_4)$  of doubly even self-dual codes of length 40 containing  $A_4$  codewords of weight 4 are listed in Table 2.

At the end of this section, we give some properties of extremal doubly even self-dual codes of length 40. In Table 3, we list the numbers  $N(\# \text{Aut})$  of extremal doubly even self-dual codes with automorphism groups of order  $\# \text{Aut}$ . In Table 4, we list the numbers  $N(\text{dim})$  of extremal doubly even self-dual codes such that subcodes generated by codewords of weight 8 have dimension  $\text{dim}$ . The dimension is the same as the 2-rank of the 1-(40, 8, 57) design formed by the codewords of weight 8.

### 3 Extremal self-dual codes of length 38

Let  $D$  be a doubly even self-dual code of length 40. Let  $C$  be the code obtained from  $D$  for which some particular pair of coordinates  $i, j$  are 00 and 11 and deleting these coordinates. Then  $C$  is a self-dual code of length 38. Here we say that  $C$  is obtained from  $D$  by subtracting coordinates  $i, j$ . In addition, any self-dual code of length 38 is obtained from some doubly even self-dual code of length 40 by subtracting some two coordinates (see [6]). Due to the computational complexity, we only completed a classification of

Table 2: Number of doubly even self-dual codes of length 40

$(A_4, N(A_4))$				
(0, 16470)	(13, 382)	(26, 47)	(40, 12)	(64, 3)
(1, 20034)	(14, 374)	(27, 16)	(41, 1)	(66, 1)
(2, 17276)	(15, 231)	(28, 38)	(42, 9)	(70, 3)
(3, 12168)	(16, 236)	(29, 13)	(43, 3)	(72, 1)
(4, 8471)	(17, 143)	(30, 29)	(44, 7)	(74, 1)
(5, 5552)	(18, 160)	(31, 7)	(46, 7)	(78, 1)
(6, 3916)	(19, 100)	(32, 22)	(48, 4)	(90, 1)
(7, 2610)	(20, 104)	(33, 3)	(50, 4)	(92, 1)
(8, 1932)	(21, 54)	(34, 25)	(52, 6)	(94, 2)
(9, 1243)	(22, 90)	(35, 3)	(54, 2)	(106, 1)
(10, 1093)	(23, 37)	(36, 11)	(56, 1)	(134, 1)
(11, 669)	(24, 59)	(37, 4)	(58, 4)	(190, 1)
(12, 605)	(25, 26)	(38, 11)	(62, 2)	

extremal self-dual codes of length 38. Note that there are at least 13644433 inequivalent self-dual codes of length 38 [9].

Any extremal self-dual code  $C$  of length 38 and its shadow  $S$  have one of the following weight enumerators [7]:

$$\begin{cases} W_C = 1 + 171y^8 + 1862y^{10} + 10374y^{12} + 36765y^{14} + 84759y^{16} \\ \quad + 128212y^{18} + \dots, \\ W_S = 114y^7 + 9044y^{11} + 118446y^{15} + 269080y^{19} + \dots, \end{cases} \quad (4)$$

$$\begin{cases} W_C = 1 + 203y^8 + 1702y^{10} + 10598y^{12} + 36925y^{14} + 84055y^{16} \\ \quad + 128660y^{18} + \dots, \\ W_S = y^3 + 106y^7 + 9072y^{11} + 118390y^{15} + 269150y^{19} + \dots. \end{cases} \quad (5)$$

Although the following two lemmas are somewhat trivial, it is useful in finding extremal self-dual codes of length 38.

**Lemma 5.** *Any extremal self-dual code of length 38 with weight enumerator (4) (resp. (5)) is obtained from some extremal doubly even self-dual code of length 40 (resp. some doubly even self-dual code of length 40 containing one codeword of weight 4) by subtracting some two coordinates.*

*Proof.* Let  $C$  be an extremal self-dual code of length 38 with weight enumerator (4) (resp. (5)). By Proposition 3, a doubly even self-dual code  $C^*$  of

Table 3: Orders of automorphism groups

(# Aut, $N(\# \text{Aut})$ )				
(1, 10400)	(36, 1)	(256, 21)	(3072, 3)	(61440, 1)
(2, 3538)	(38, 1)	(288, 4)	(3840, 1)	(65536, 1)
(3, 43)	(40, 5)	(320, 1)	(4096, 1)	(110592, 1)
(4, 1189)	(48, 34)	(384, 12)	(4608, 2)	(147456, 1)
(5, 2)	(60, 2)	(512, 16)	(5376, 1)	(245760, 1)
(6, 68)	(64, 75)	(576, 3)	(6144, 7)	(737280, 1)
(8, 459)	(72, 4)	(720, 2)	(6840, 1)	(786432, 1)
(10, 8)	(96, 12)	(768, 7)	(9216, 1)	(983040, 1)
(12, 80)	(114, 1)	(1024, 3)	(12288, 2)	(1474560, 1)
(16, 233)	(120, 5)	(1296, 1)	(16384, 1)	(5505024, 1)
(18, 1)	(128, 46)	(1536, 10)	(18432, 1)	(8257536, 1)
(20, 4)	(144, 4)	(1728, 1)	(20480, 1)	(44236800, 1)
(24, 41)	(160, 1)	(1920, 1)	(20736, 1)	(82575360, 1)
(30, 2)	(192, 12)	(2048, 4)	(32768, 1)	
(32, 70)	(240, 2)	(2688, 1)	(49152, 3)	

Table 4: Dimensions of subcodes generated by codewords of weight 8

dim	17	18	19	20
$N(\text{dim})$	5	1	14	16450

length 40 is constructed. In addition, by (4) (resp. (5)),  $C^*$  is extremal (resp.  $C^*$  contains one codeword of weight 4). The code  $C$  is obtained from  $C^*$  by subtracting the last two coordinates. The result follows.  $\square$

For the remainder of this section, we suppose that  $D$  is either an extremal doubly even self-dual code of length 40 or a doubly even self-dual code of length 40 containing one codeword of weight 4. Also, let  $D_{i,j}$  denote the self-dual code of length 38 obtained from  $D$  by subtracting two coordinates  $i, j$ .

**Lemma 6.** *Let  $M(D)$  be the matrix with rows composed of the codewords of weight 8 in  $D$ , where the  $(1, 0)$ -matrix  $M(D)$  is regarded as a matrix over  $\mathbb{Z}$ .*

- (1) Suppose that  $D$  is extremal. Then the  $(i, j)$ -entry of  $M(D)^T M(D)$  is zero if and only if  $D_{i,j}$  is extremal.
- (2) Suppose that  $D$  has one codeword  $x$  of weight 4. Then the  $(i, j)$ -entry of  $M(D)^T M(D)$  is zero and the pair of coordinates  $i, j$  in  $x$  are 10 or 01 if and only if  $D_{i,j}$  is extremal.

*Proof.* There is a codeword of weight 8 in  $D$  for which the coordinates  $i, j$  are 11 if and only if  $D_{i,j}$  contains a codeword of weight 6. Suppose that  $D$  contains one codeword  $x$  of weight 4. The coordinates  $i, j$  in  $x$  are 11 (resp. 00) if and only if  $D_{i,j}$  contains a codeword of weight 2 (resp. 4).  $\square$

By Lemma 6, from all inequivalent extremal doubly even self-dual codes and all inequivalent doubly even self-dual codes containing one codeword of weight 4, we constructed extremal self-dual codes of length 38 which need be checked further for equivalences. Then we checked equivalences among these codes using the method similar to that given in Section 2. Finally we have the following:

**Proposition 7.** *There are 2744 inequivalent extremal self-dual codes of length 38. Of these 1730 have weight enumerator (4) and 1014 have weight enumerator (5).*

In Table 5, we list the numbers  $N(\# \text{Aut})$  of extremal self-dual codes with automorphism groups of order  $\# \text{Aut}$  for both weight enumerators (4) and (5).

Table 5: Number of extremal self-dual codes of length 38

( $\# \text{Aut}, N(\# \text{Aut})$ )				
Weight enumerator (4)				
(1, 1480)	(4, 30)	(9, 1)	(24, 4)	(342, 1)
(2, 177)	(6, 7)	(12, 5)	(36, 1)	
(3, 15)	(8, 7)	(18, 1)	(168, 1)	
Weight enumerator (5)				
(1, 773)	(4, 38)	(12, 3)	(24, 10)	(216, 1)
(2, 145)	(6, 10)	(14, 1)	(144, 1)	(504, 1)
(3, 21)	(8, 8)	(21, 1)	(168, 1)	

**Acknowledgment.** The author would like to thank Akihiro Munemasa for providing information on [1].

## References

- [1] K. Betsumiya and A. Munemasa, Classification of extremal doubly even self-dual codes of length 40, (in preparation).
- [2] R.T. Bilous, Enumeration of the binary self-dual codes of length 34, *J. Combin. Math. Combin. Comput.* **59** (2006), 173–211.
- [3] R.T. Bilous and G.H.J. van Rees, An enumeration of self-dual codes of length 32, *Des. Codes, Cryptogr.* **26** (2002), 61–86.
- [4] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at <http://magma.maths.usyd.edu.au/magma/>.
- [5] R. Brualdi and V. Pless, Weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **37** (1991), 1222–1225.
- [6] J.H. Conway, V. Pless and N.J.A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *J. Combin. Theory Ser. A* **60** (1992), 183–195.
- [7] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.
- [8] M. Harada and H. Kimura, New extremal doubly-even  $[64, 32, 12]$  codes, *Des. Codes Cryptogr.* **6** (1995), 91–96.
- [9] M. Harada and A. Munemasa, Classification of self-dual codes of length 36, (submitted).
- [10] M. Harada and A. Munemasa, Database of Self-Dual Codes, Available online at <http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm>.
- [11] O.D. King, The mass of extremal doubly-even self-dual codes of length 40, *IEEE Trans. Inform. Theory* **47** (2001), 2558–2560.

- [12] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, Good self dual codes exist, *Discrete Math.* **3** (1972), 153–162.
- [13] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.
- [14] A. Munemasa, private communication, January 5, 2011.
- [15] V. Pless, A classification of self-orthogonal codes over  $GF(2)$ , *Discrete Math.* **3** (1972), 209–246.
- [16] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory Ser. A* **18** (1975), 313–335.
- [17] E.M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Inform. Theory* **44** (1998), 134–139.
- [18] E. Rains and N.J.A. Sloane, “Self-dual codes,” *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 177–294.