A complete classification of doubly even self-dual codes of length 40*

Koichi Betsumiya

Graduate School of Science and Technology
Hirosaki University
Hirosaki 036–8561, Japan

betsumi@cc.hirosaki-u.ac.jp

Masaaki Harada

Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan, and
PRESTO, Japan Science and Technology Agency (JST)
Saitama 332–0012, Japan
mharada@sci.kj.yamagata-u.ac.jp

Akihiro Munemasa

Graduate School of Information Sciences
Tohoku University
Sendai 980–8579, Japan

munemasa@math.is.tohoku.ac.jp

November 13, 2012

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.

*This work was supported by JST PRESTO program.

1 Introduction

As described in [26], 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 [26]).

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 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 [20] and [25]. A self-dual code meeting the bound is called *extremal*.

Two codes C and C' are *equivalent*, denoted $C \cong C'$, 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 $\mathrm{Aut}(C)$.

A classification of doubly even self-dual codes was done for lengths $8, 16$ in [23], for length 24 in [24] and for length 32 in [9]. For length 40, only some partial classifications have been done by various authors. Extremal doubly even self-dual codes of length 40 with automorphism of a prime order p having c cycles have been classified for $(p, c) = (19, 2), (7, 5), (5, 4)$ in [28], $(p, c) = (3, 6)$ in [6], $(p, c) = (3, 8)$ in [16], and $(p, c) = (5, 8)$ in [29]. 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.*

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 ($n = 8, 16, \ldots, 40$) 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 [3], [4], [9], [11], [23], [24]. 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 [12]. All computer calculations in this paper were done by Magma [5].

2 Classification method

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

2.1 Preliminaries

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

$$1 + A_4y^4 + (285 + 24A_4)y^8 + (21280 + 92A_4)y^{12} \\ + (239970 - 600A_4)y^{16} + (525504 + 966A_4)y^{20} + \cdots + y^{40}, \quad (1)$$

where A_w denotes the number of codewords of weight w (see e.g. [20]).

The number of distinct doubly even self-dual codes of length n is given [19] by the formula:

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

King [18] 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

$$N(40, 4) = 4009357722800739726876619952910304312989584368968750,$$
$$N(40, 8) = 10263335567003567415076803513287627980544163840000000.$$

2.2 Minimum weight 4

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 $C_0^{\perp} \setminus C$ [10]. 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 2 (Brualdi and Pless [8])**.** *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*

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

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

There are 519492 inequivalent self-dual codes of length 36 [11]. 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 2, 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 $\mathbb{Z}$. We define

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

where n_{ij} is the (i, j)-entry of $M(C)^T M(C)$, and $M(C)^T$ denotes the transposed matrix 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 $(i = 1, 2, \ldots, 40)$ and $\max\{n_{ij} \mid 1 \leq i, j \leq 40\} = 57$ when C is extremal. Then we consider the following:

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

The automorphism group $\operatorname{Aut}(C)$ of the code 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. Then we obtained the set $\mathcal{C}_{40,4}$ of 77873 inequivalent doubly even self-dual codes with minimum weight 4 satisfying

$$\sum_{C \in \mathcal{C}_{40,4}} \frac{40!}{\#\operatorname{Aut}(C)} = N(40, 4). \tag{3}$$

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

2.3 Minimum weight 8

For a set of coordinates $I \subset \{1, 2, \ldots, n\}$, let $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^t$, $\pi' : \mathbb{F}_2^n \to \mathbb{F}_2^{n-t}$ be the projection to the set of coordinates I, I', respectively, where $I' = \{1, \ldots, n\} \setminus I$ and $\#I = t$. For a code C of length n, the *punctured code* and the *shortened code* of C on the set of coordinates I are the codes $\pi'(C)$ and $\{\pi'(c) \mid c \in C,\ \pi(c) = \mathbf{0}\}$, respectively, where $\mathbf{0}$ denotes the zero vector.

If C is a doubly even code containing the all-one vector $\mathbf{1}$, then we denote by $q_C : C^\perp/C \to \mathbb{F}_2$ the map defined by $q_C(x+C) = \frac{\operatorname{wt}(x)}{2} \bmod 2$, where $\operatorname{wt}(x)$ denotes the weight of x. It is easy to verify that the map q_C is well-defined.

Let C_i be a doubly even code of length n_i containing $\mathbf{1}$, for $i = 1, 2$. A bijective linear map

$$f : C_1^\perp/C_1 \to C_2^\perp/C_2 \tag{4}$$

is called an *isometry* if $q_{C_1} = q_{C_2} \circ f$. The set of isometries (4) is denoted by $\Phi(C_1, C_2)$. Note that an isometry exists only if $n_1 - n_2 = 2(\dim C_1 - \dim C_2)$ and $n_1 \equiv n_2 \pmod 8$. For an isometry $f \in \Phi(C_1, C_2)$, we define a code

$$D(C_1, C_2, f) = \{(x_1, x_2) \mid x_1 \in C_1^\perp,\ x_2 \in f(x_1 + C_1)\} \subset \mathbb{F}_2^{n_1+n_2}, \tag{5}$$

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

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

It is easy to see that $D(C_1, C_2, f)$ is a doubly even self-dual code. Conversely, every doubly even self-dual code of length $n_1 + n_2$ containing a codeword of weight n_1 can be constructed by this method. Indeed, let x be a codeword of weight n_1 in a doubly even self-dual code C of length $n_1 + n_2$. Let C_2 (resp. C_1) be the shortened code of C on the support (resp. the complement of the support) of x. Then C_1 and C_2 are doubly even codes. Moreover, $C_2^{\perp}$ (resp. $C_1^{\perp}$) is the punctured code of C on the support (resp. the complement of the support) of x. Let π and π' denote the projections onto the support of x and the complement of the support of x, respectively. We define $f : C_1^{\perp}/C_1 \to C_2^{\perp}/C_2$ by $f(x_1 + C_1) = \pi'(x) + C_2$, where x is a codeword of C satisfying $\pi(x) = x_1$. Then $D(C_1, C_2, f)$ is equivalent to C.

For fixed codes C_1, C_2, the resulting code $D(C_1, C_2, f)$ depends on the choice of an isometry f. However, some of these codes are equivalent to each other. We will give a sufficient condition for two resulting codes to be equivalent. We need this criterion to reduce the amount of calculation to be reasonable.

First, we define some groups. For a doubly even code C containing $\mathbf{1}$, we denote by $\mathcal{G}_0(C)$ the subgroup of $\mathrm{GL}(C^{\perp}/C)$ induced by the action of $\mathrm{Aut}(C)$ on the linear space $C^{\perp}/C$ and denote by $\mathcal{G}_1(C)$ the subgroup $\Phi(C, C)$ of $\mathrm{GL}(C^{\perp}/C)$. By the definition, the group $\mathcal{G}_0(C)$ is a subgroup of $\mathcal{G}_1(C)$. If

we replace f by $\sigma_2 \circ f \circ \sigma_1$, where $\sigma_i \in \mathcal{G}_0(C_i)$, then the resulting codes are equivalent, that is,

$$D(C_1, C_2, f) \cong D(C_1, C_2, \sigma_2 \circ f \circ \sigma_1).$$

This means that, in order to enumerate the set of codes $\{D(C_1, C_2, h) \mid h \in \Phi(C_1, C_2)\}$ up to equivalence, we first fix $f \in \Phi(C_1, C_2)$, and it suffices to enumerate the codes $D(C_1, C_2, f \circ g)$, where g runs through a set of representatives for the double cosets

$$(f^{-1} \circ \mathcal{G}_0(C_2) \circ f) \backslash \mathcal{G}_1(C_1) / \mathcal{G}_0(C_1).$$

We now apply this method with $(n_1, n_2) = (16, 24)$ in order to classify extremal doubly even self-dual codes of length 40. Note that from the weight enumerator (1), such a code has a codeword of weight 16. This means that every extremal doubly even self-dual code of length 40 is equivalent to $D(C_1, C_2, f)$ for some doubly even code C_1 of length 16 containing $\mathbf{1}$, some doubly even code C_2 of length 24 containing $\mathbf{1}$, and $f \in \Phi(C_1, C_2)$. All doubly even codes of lengths 16 and 24 can be found in [21].

However, if $\dim C_1 \leq 2$, then the degree of $\mathcal{G}_1(C_1) \subset \mathrm{GL}(C_1^{\perp}/C_1)$ as a permutation group is too large to perform the double coset enumeration, so we only enumerated codes $D(C_1, C_2, f)$, where C_1 is a doubly even code of length 16 with $\dim C_1 \geq 3$. Here, the group $\mathcal{G}_1(C_1)$ was constructed by the MAGMA function `GOPlus`, and the double coset enumeration was performed using the MAGMA function `DoubleCosetRepresentatives`. Then we classified the resulting codes using the method described in the previous subsection. In this way, we obtained a set of pairwise inequivalent 16468 extremal doubly even self-dual codes of length 40. It turns out that there are two other codes. One is the code with automorphism group of order 6840 constructed in [28]. The other is the code $H^{(1234)}B_6'$ in the notation of [29] and this code has automorphism group of order 120.

In this way, we obtained the set $\mathcal{C}_{40,8}$ of 16470 inequivalent extremal doubly even self-dual codes satisfying

$$\sum_{C \in \mathcal{C}_{40,8}} \frac{40!}{\#\operatorname{Aut}(C)} = N(40, 8). \tag{6}$$

From (3) and (6), it follows that there is no other doubly even self-dual code of length 40. This explains the number $N(0)$ of extremal doubly even self-dual codes of length 40 listed in Table 2. Therefore, we have Theorem 1.

3 Some properties

In this section, we give some properties of doubly even self-dual codes of length 40.

The covering radius of a code C of length n is the smallest integer R such that spheres of radius R around codewords of C cover the space $\mathbb{F}_2^n$. It is known that the covering radius is the same as the largest value among weights of cosets. Here, the weight of a coset is the smallest weight of a vector in the coset. The covering radius is a basic and important geometric parameter of a code. Assmus and Pless [2] began the study of the covering radii of (extremal) doubly even self-dual codes.

Let $R_{40,d}$ be the covering radius of a doubly even self-dual code of length 40 and minimum weight d ($d = 4, 8$). Then, by the sphere-covering bound and the Delsarte bound (see [2]), $6 \leq R_{40,8} \leq 8$ and $6 \leq R_{40,4} \leq 10$. In Table 3, we list the numbers $N(d, R)$ of doubly even self-dual codes with minimum weight d and covering radius R. This was calculated by the MAGMA function `CoveringRadius`. From the above calculation, we have the following:

Proposition 3. *There is no doubly even self-dual code of length* 40 *with covering radius* 6.

Remark 4. In [14], based on a preprint by Michio Ozeki, the non-existence of an extremal doubly even self-dual code with covering radius 6 was announced. However, unfortunately, his preprint contained an error and, in his paper [22] he withdrew the above announcement. From the above calculation, the non-existence of an extremal doubly even self-dual code with covering radius 6 was verified.

Remark 5. The two extremal doubly even self-dual codes with covering radius 7 can be found in [13] and [14].

Now we give some properties of extremal doubly even self-dual codes of length 40. Let σ be an automorphism of odd prime order p. If σ has c independent p-cycles and f fixed points, then σ is said to be of type p-(c, f). All extremal doubly even self-dual codes of length 40 with automorphism of type p-(c, f) are known for $p \geq 5$ (see [15, Table 3]). The cases with $(p, c) = (3, 6)$ and $(3, 8)$ were considered in [6] and [16], respectively. The numbers $N(p, c)$ of inequivalent extremal doubly even self-dual codes with automorphism of type p-(c, f) are listed in Table 4 for $(p, c) = (3, 6), (3, 10)$ and $(3, 12)$. It is claimed in [6, Theorem 12] that $N(3, 6) = 16$. However, we

Table 3: Covering radii of doubly even self-dual codes

R	$N(4,R)$	$N(8,R)$
6	0	0
7	23	2
8	76768	16468
9	954	-
10	128	-

verified that $N(3,6) = 17$. Since the list of the 16 codes is not available, we are unable to compare the result with ours.

Proposition 6. *There are* 17, 70 *and* 322 *inequivalent extremal doubly even self-dual codes of length* 40 *with automorphism of types* 3-$(6,22)$, 3-$(10,10)$ *and* 3-$(12,4)$, *respectively.*

Table 4: $N(p,c)$ for $(p,c) = (3,6), (3,10)$ and $(3,12)$

(p,c)	$(3,6)$	$(3,10)$	$(3,12)$
$N(p,c)$	17	70	322

In Table 5, we list the numbers $N(\#\,\mathrm{Aut})$ of extremal doubly even self-dual codes with automorphism groups of order $\#\,\mathrm{Aut}$.

As we mentioned at the end of Subsection 2.3, we have the following:

Proposition 7. *Let C_x denote the shortened code of C on the complement of the support of a codeword x. Then there are two inequivalent extremal doubly even self-dual codes C of length* 40 *such that* $\dim C_x \leq 2$ *for all* $x \in C$ *with* $\mathrm{wt}(x) = 16$.

Although the condition given in Proposition 7 can be characterized by the vanishing of a coefficient in the weight enumerator of genus 3 (see [27]), we have not been able to prove Proposition 7 directly, without classifying all extremal doubly even self-dual codes of length 40.

In Table 6, we list the numbers $N(\dim)$ of extremal doubly even self-dual codes such that subcodes generated by codewords of weight 8 have

Table 5: Orders of automorphism groups

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

dimension dim. The dimension is the same as the 2-rank of the 1-$(40, 8, 57)$ design formed by the codewords of weight 8.

Table 6: Dimensions of subcodes generated by codewords of weight 8

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

4 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 [9]). Due to the computational complexity, we only completed a classification of extremal self-dual codes of length 38. Note that there are at least 13644433 inequivalent self-dual codes of length 38 [11].

Any extremal self-dual code C of length 38 and its shadow S have one of the following weight enumerators [10]:

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

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

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

Lemma 8. *Any extremal self-dual code of length* 38 *with weight enumerator (7) (resp. (8)) 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 (7) (resp. (8)). By Proposition 2, a doubly even self-dual code C^* of length 40 is constructed. In addition, by (7) (resp. (8)), 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. □

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 9. *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 contains 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). □

By Lemma 9, 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 10. *There are* 2744 *inequivalent extremal self-dual codes of length* 38*. Of these* 1730 *have weight enumerator (7) and* 1014 *have weight enumerator (8).*

Remark 11. A classification of extremal self-dual codes of length 38 was very recently obtained in [1] by somewhat different techniques. This was indicated by Jon-Lark Kim in a private communication [17].

In Table 7, we list the numbers $N(\#\,\mathrm{Aut})$ of extremal self-dual codes with automorphism groups of order $\#\,\mathrm{Aut}$ for both weight enumerators (7) and (8).

Some historical comments (July 27, 2012). A classification of extremal self-dual codes of length 38 was completed in [1], and a classification of all self-dual codes of length 38 was completed in [7]. The paper [1] was submitted before this paper was submitted, and the paper [7] was submitted after this paper was submitted.

Acknowledgements

The authors would like to thank Jon-Lark Kim for providing information on [1].

Table 7: Number of extremal self-dual codes of length 38

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

References

[1] C. Aguilar-Melchor, P. Gaborit, J.-L. Kim, L. Sok and P. Solé. Classification of extremal and s-extremal binary self-dual codes of length 38. *IEEE Trans. Inform. Theory*, 58:2253–2262, 2012.

[2] E. F. Assmus, Jr. and V. Pless. On the covering radius of extremal self-dual codes. *IEEE Trans. Inform. Theory*, 29:359–363, 1983.

[3] R. T. Bilous. Enumeration of the binary self-dual codes of length 34. *J. Combin. Math. Combin. Comput.*, 59:173–211, 2006.

[4] R. T. Bilous and G. H. J. van Rees. An enumeration of self-dual codes of length 32. *Des. Codes, Cryptogr.*, 26:61–86, 2002.

[5] 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/`.

[6] S. Bouyuklieva. Some optimal self-orthogonal and self-dual codes. *Disc. Math.*, 287:1–10, 2004.

[7] S. Bouyuklieva and I. Bouyukliev. An algorithm for classification of binary self-dual codes. *IEEE Trans. Inform. Theory*, 58:3933–3940, 2012.

[8] R. Brualdi and V. Pless. Weight enumerators of self-dual codes. *IEEE Trans. Inform. Theory*, 37:1222–1225, 1991.

[9] 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*, 60:183–195, 1992.

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

[11] M. Harada and A. Munemasa. Classification of self-dual codes of length 36. *Advances Math. Communications*, 6:229–235, 2012.

[12] M. Harada and A. Munemasa. Database of Self-Dual Codes. Available online at `http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm`.

[13] M. Harada, A. Munemasa and K. Tanabe. Extremal self-dual $[40, 20, 8]$ codes with covering radius 7. *Finite Fields Appl.*, 10:183–197, 2004.

[14] M. Harada and M. Ozeki. Extremal self-dual codes with the smallest covering radius. *Disc. Math.*, 215:271–281, 2000.

[15] W. C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, 11:451–490, 2005.

[16] H. J. Kim. Self-dual codes with automorphism of order 3 having 8 cycles. *Des. Codes Cryptogr.*, 57:329–346, 2010.

[17] J.-L. Kim. private communication. April 25, 2011.

[18] O. D. King. The mass of extremal doubly-even self-dual codes of length 40. *IEEE Trans. Inform. Theory*, 47:2558–2560, 2001.

[19] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson. Good self dual codes exist. *Disc. Math.*, 3:153–162, 1972.

[20] C. L. Mallows and N. J. A. Sloane. An upper bound for self-dual codes. *Inform. Control*, 22:188–200, 1973.

[21] R. L. Miller. Doubly Even Codes. Available online at `http://www.rlmiller.org/de_codes/`.

[22] M. Ozeki. Jacobi polynomials for singly even self-dual codes and the covering radius problems. *IEEE Trans. Inform. Theory*, 48:547–557, 2002.

[23] V. Pless. A classification of self-orthogonal codes over GF(2). *Disc. Math.*, 3:209–246, 1972.

[24] V. Pless and N. J. A. Sloane. On the classification and enumeration of self-dual codes. *J. Combin. Theory Ser. A*, 18:313–335, 1975.

[25] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory*, 44:134–139, 1998.

[26] E. Rains and N. J. A. Sloane. Self-dual codes. In *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman (Editors), pages 177–294, Elsevier, Amsterdam, 1998.

[27] B. Runge. Codes and Siegel modular forms. *Disc. Math.*, 148:175–204, 1996.

[28] V. Y. Yorgov. Binary self-dual codes with automorphisms of odd order. *Problems Inform. Transmission*, 19:260–270, 1984. translated from *Problemy Peredachi Informatsii*, 19:11–24, 1983 (Russian).

[29] V. Y. Yorgov and N. Zyapkov. Doubly even self-dual $[40, 20, 8]$-codes with an automorphism of odd order. *Problems Inform. Transmission*, 32:253–257, 1997. translated from *Problemy Peredachi Informatsii*, 32:41–46, 1996 (Russian).