Des. Codes Cryptogr. (2018) 86:1085–1094
https://doi.org/10.1007/s10623-017-0380-2

Binary extremal self-dual codes of length 60 and related codes

Masaaki Harada[1]

Received: 19 April 2017 / Revised: 9 June 2017 / Accepted: 17 June 2017 /
Published online: 24 June 2017

Abstract We give a classification of four-circulant singly even self-dual $[60, 30, d]$ codes for $d = 10$ and 12. These codes are used to construct extremal singly even self-dual $[60, 30, 12]$ codes with weight enumerator for which no extremal singly even self-dual code was previously known to exist. From extremal singly even self-dual $[60, 30, 12]$ codes, we also construct optimal singly even self-dual $[58, 29, 10]$ codes with weight enumerator for which no optimal singly even self-dual code was previously known to exist. Finally, we give some restriction on the possible weight enumerators of certain singly even self-dual codes with shadow of minimum weight 1.

Keywords Extremal self-dual code · Weight enumerator · Neighbor

Mathematics Subject Classification 94B05

1 Introduction

Let C be a (binary) singly even self-dual code. All codes in this note are binary. Let C_0 denote the subcode of C consisting of codewords having weight $\equiv 0 \pmod 4$. The *shadow* S of C is defined to be $C_0^{\perp} \setminus C$. Shadows for self-dual codes were introduced by Conway and Sloane [3] in order to derive new upper bounds for the minimum weight of singly even self-dual codes, and to provide restrictions on the weight enumerators of singly even self-dual codes. In addition, Rains [11] showed that the minimum weight d of a self-dual code C of length n is bounded by $d \leq 4\lfloor n/24 \rfloor + 4$ unless $n \equiv 22 \pmod{24}$ when $d \leq 4\lfloor n/24 \rfloor + 6$ by considering the shadows. A self-dual code meeting the upper bound is called *extremal*. We

Communicated by P. Charpin.

✉ Masaaki Harada
mharada@m.tohoku.ac.jp

1 Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan

say that a self-dual code is *optimal* if it has the largest minimum weight among all self-dual codes of that length.

The possible weight enumerators of singly even self-dual codes with the largest possible minimum weights given in [3, Table I] are given in [3] for lengths up to 64 and length 72 (see also [7] for length 60). It is a fundamental problem to find which weight enumerators actually occur for the possible weight enumerators (see [3]). The possible weight enumerators of extremal singly even self-dual [60, 30, 12] codes are known as follows:

$$\begin{aligned} W_{60,1} &= 1 + (2555 + 64\beta)y^{12} + (33600 - 384\beta)y^{14} + \cdots, \\ W_{60,2} &= 1 + 3451y^{12} + 24128y^{14} + \cdots, \end{aligned}$$

where β is an integer. If there is an extremal singly even self-dual [60, 30, 12] code with weight enumerator $W_{60,1}$, then $\beta \in \{0, 1, 2, \dots, 8, 10\}$ [8]. For $\beta = 0, 1, 5, 7$ and 10, an extremal singly even self-dual code with weight enumerator $W_{60,1}$ was found in [13,2,14,5] and [7], respectively. An extremal singly even self-dual code with weight enumerator $W_{60,2}$ was found in [3].

One of the main aims of this note is to show the following:

Proposition 1 *There is an extremal singly even self-dual* [60, 30, 12] *code with weight enumerator* $W_{60,1}$ *for* $\beta = 2, 6$.

These codes are constructed from four-circulant singly even self-dual $[60, 30, d]$ codes for $d = 10$ and 12 by considering self-dual neighbors. It remains to determine whether there is an extremal singly even self-dual [60, 30, 12] code with weight enumerator $W_{60,1}$ for $\beta = 3, 4, 8$.

The largest minimum weight among singly even self-dual codes of length 58 is 10 [3]. The possible weight enumerators of optimal singly even self-dual [58, 29, 10] codes are known as follows:

$$\begin{aligned} W_{58,1} &= 1 + (165 - 2\gamma)y^{10} + (5078 + 2\gamma)y^{12} + \cdots, \\ W_{58,2} &= 1 + (319 - 24\beta - 2\gamma)y^{10} + (3132 + 152\beta + 2\gamma)y^{12} + \cdots, \end{aligned}$$

where β, γ are integers [3]. If there is an optimal singly even self-dual [58, 29, 10] code with weight enumerator $W_{58,2}$, then $\beta \in \{0, 1, 2\}$ [8]. An optimal singly even self-dual code with weight enumerator $W_{58,1}$ is known for $\gamma = 55$ [12]. An optimal singly even self-dual code with weight enumerator $W_{58,2}$ is known for

$$\begin{aligned} &\beta = 0 \text{ and } \gamma \in \{2m \mid m = 0, 1, 5, 6, 8, 9, 10, 11, 13, \dots, 65, 68, 71, 79\}, \\ &\beta = 1 \text{ and } \gamma \in \{2m \mid m = 13, 14, 16, \dots, 58, 63\}, \\ &\beta = 2 \text{ and } \gamma \in \{2m \mid m = 0, 16, \dots, 50, 55\} \end{aligned}$$

(see [9,10,14]).

The following proposition is one of the main results of this note.

Proposition 2 *There is an optimal singly even self-dual* [58, 29, 10] *code with weight enumerator* $W_{58,2}$ *for*

$$\begin{aligned} &\beta = 0 \text{ and } \gamma \in \{2m \mid m = 2, 3, 4, 7, 12\}, \\ &\beta = 1 \text{ and } \gamma \in \{2m \mid m = 8, 9, 10, 11, 12, 15\}, \\ &\beta = 2 \text{ and } \gamma \in \{2m \mid m = 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 51, 52, 53, 54\}. \end{aligned}$$

These codes are constructed from extremal singly even self-dual [60, 30, 12] codes constructed in this note by subtracting and their self-dual neighbors. Finally, we give some restriction on the possible weight enumerators of certain singly even self-dual codes with shadow of minimum weight 1 (Proposition 5). As a consequence, it is shown that $\gamma = 55$ for the possible weight enumerator $W_{58,1}$ (Corollary 6). All self-dual codes in this note are singly even. From now on, we omit the term singly even.

All computer calculations in this note were done with the help of MAGMA [1].

2 Extremal four-circulant self-dual [60, 30, 12] codes

An $n \times n$ circulant matrix has the following form:

$$\begin{pmatrix} r_0 & r_1 & r_2 & \cdots & r_{n-1} \\ r_{n-1} & r_0 & r_1 & \cdots & r_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{pmatrix},$$

so that each successive row is a cyclic shift of the previous one. Let A and B be $n \times n$ circulant matrices. Let C be a $[4n, 2n]$ code with generator matrix of the following form:

$$\begin{pmatrix} I_{2n} & \begin{matrix} A & B \\ B^T & A^T \end{matrix} \end{pmatrix}, \tag{1}$$

where I_n denotes the identity matrix of order n and A^T denotes the transpose of A. It is easy to see that C is self-dual if $AA^T + BB^T = I_n$. The codes with generator matrices of the form (1) are called *four-circulant*.

In this section, we give a classification of extremal four-circulant self-dual [60, 30, 12] codes. Two codes are *equivalent* if one can be obtained from the other by a permutation of coordinates. Our exhaustive search found all distinct extremal four-circulant self-dual [60, 30, 12] codes, which must be checked further for equivalence to complete the classification. This was done by considering all pairs of 15×15 circulant matrices A and B satisfying the condition that $AA^T + BB^T = I_{15}$, the sum of the weights of the first rows of A and B is congruent to $1 \pmod 4$ and the sum of the weights is greater than or equal to 13. Since a cyclic shift of the first rows gives an equivalent code, we may assume without loss of generality that the last entry of the first row of B is 1. Then our computer search shows that the above distinct extremal four-circulant self-dual [60, 30, 12] codes are divided into 13 inequivalent codes.

Proposition 3 *Up to equivalence, there are* 13 *extremal four-circulant self-dual* [60, 30, 12] *codes.*

We denote the 13 codes by $C_{60,i}$ $(i = 1, 2, \dots, 13)$. For the 13 codes $C_{60,i}$ $(i = 1, 2, \dots, 13)$, the first rows r_A (resp. r_B) of the circulant matrices A (resp. B) in generator matrices (1) are listed in Table 1. We verified that the codes $C_{60,i}$ have weight enumerator $W_{60,1}$, where β are also listed in Table 1.

3 Extremal self-dual [60, 30, 12] neighbors

Two self-dual codes C and C' of length n are said to be *neighbors* if $\dim(C \cap C') = n/2 - 1$. Any self-dual code of length n can be reached from any other by taking successive neighbors

Table 1 Extremal four-circulant self-dual [60, 30, 12] codes $C_{60,i}$

Code	r_A	r_B	β
$C_{60,1}$	(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)	(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)	0
$C_{60,2}$	(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)	(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)	0
$C_{60,3}$	(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)	(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)	0
$C_{60,4}$	(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)	(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)	0
$C_{60,5}$	(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)	(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)	0
$C_{60,6}$	(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)	(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)	0
$C_{60,7}$	(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)	(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)	0
$C_{60,8}$	(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)	(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)	0
$C_{60,9}$	(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)	(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)	10
$C_{60,10}$	(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)	(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)	10
$C_{60,11}$	(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)	(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)	10
$C_{60,12}$	(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)	(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)	10
$C_{60,13}$	(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)	(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)	10

(see [3]). It is known that a self-dual code C of length n has $2(2^{n/2-1}-1)$ self-dual neighbors. These neighbors are constructed by finding $2^{n/2-1}-1$ subcodes of codimension 1 in C containing the all-one vector. A computer program written in Magma, which was used to find self-dual neighbors, can be obtained electronically from http://www.math.is.tohoku.ac.jp/~mharada/Paper/neighbor.txt. In this section, we construct extremal self-dual [60, 30, 12] codes by considering self-dual neighbors.

For $i = 1, 2, \dots, 13$, by finding all $2(2^{29}-1)$ self-dual neighbors of $C_{60,i}$, we determined the equivalence classes among extremal self-dual neighbors of $C_{60,i}$. Our computer search shows that the code $C_{60,i}$ has n_i inequivalent extremal self-dual neighbors, which are equivalent to none of the 13 codes $C_{60,j}$, where n_i are given by

$$n_i = \begin{cases} 3 & \text{if} \quad i = 1, \\ 1 & \text{if} \quad i = 2, 4, 10, 12, \\ 0 & \text{otherwise.} \end{cases}$$

We denote the 7 extremal self-dual codes by $D_{60,i}$ $(i = 1, 2, \dots, 7)$. These codes $C = D_{60,i}$ are constructed as

$$\langle (D \cap \langle x \rangle^{\perp}), x \rangle,$$

where D and the support $\mathrm{supp}(x)$ of x are listed in Table 2. We verified that the codes $D_{60,i}$ have weight enumerator $W_{60,1}$, where W in Table 2 indicates the values β in the weight enumerator $W_{60,1}$. The code $D_{60,3}$ has the following weight enumerator:

$$\begin{aligned} &1 + 2683y^{12} + 32832y^{14} + 280017y^{16} + 1719808y^{18} + 7800120y^{20} \\ &+ 26380032y^{22} + 67167368y^{24} + 130134528y^{26} + 193185267y^{28} \\ &+ 220336512y^{30} + \cdots + y^{60}. \end{aligned}$$

We verified that there is no pair of equivalent codes among the 13 codes $C_{60,i}$ and the 7 codes $D_{60,i}$.

Table 2 Extremal self-dual [60, 30, 12] neighbors $D_{60,i}$

C	D	supp(x)	W
$D_{60,1}$	$C_{60,1}$	{1, 31, 32, 38, 42, 43, 46, 47, 48, 50, 51, 55}	$\beta = 0$
$D_{60,2}$	$C_{60,1}$	{2, 3, 8, 33, 35, 39, 40, 41, 46, 50, 54, 59}	$\beta = 0$
$D_{60,3}$	$C_{60,1}$	{4, 8, 9, 32, 42, 43, 48, 51, 53, 54, 56, 60}	$\beta = 2$
$D_{60,4}$	$C_{60,2}$	{2, 32, 34, 38, 40, 43, 49, 52, 54, 55, 57, 59}	$\beta = 0$
$D_{60,5}$	$C_{60,4}$	{1, 31, 35, 39, 40, 41, 42, 43, 50, 52, 54, 55}	$\beta = 0$
$D_{60,6}$	$C_{60,10}$	{2, 32, 38, 41, 43, 49, 51, 52, 54, 55, 56, 60}	$\beta = 10$
$D_{60,7}$	$C_{60,12}$	{3, 7, 10, 32, 35, 36, 38, 46, 53, 55, 58, 60}	$\beta = 10$

Table 3 Extremal self-dual [60, 30, 12] neighbors $E_{60,i}$ and F_{60}

C	D	supp(x)	W
$E_{60,1}$	$D_{60,2}$	{2, 3, 6, 31, 32, 37, 39, 40, 46, 47, 54, 57}	$\beta = 0$
$E_{60,2}$	$D_{60,6}$	{1, 2, 5, 7, 8, 40, 43, 46, 47, 50, 51, 60}	$\beta = 10$
$E_{60,3}$	$D_{60,6}$	{1, 4, 5, 8, 36, 38, 39, 40, 48, 53, 55, 60}	$\beta = 10$
$E_{60,4}$	$D_{60,6}$	{3, 32, 33, 34, 37, 46, 48, 52, 56, 57, 58, 60}	$\beta = 10$
F_{60}	$E_{60,3}$	{1, 2, 5, 35, 37, 40, 45, 49, 50, 55, 57, 59}	$\beta = 10$

We continue the search to find extremal self-dual codes by considering self-dual neighbors. We found all inequivalent extremal self-dual neighbors E_{60,i_1} of D_{60,i_2}, which are equivalent to none of the extremal self-dual codes previously obtained in this note. For the codes $E_{60,i_1} = \langle (D \cap \langle x \rangle^{\perp}), x \rangle$, D and supp(x) are listed in Table 3. In the table, W indicates the values β in the weight enumerator $W_{60,1}$. By continuing this process, we found all inequivalent extremal self-dual neighbors of $E_{60,i}$, which are equivalent to none of the extremal self-dual codes previously obtained in this note. Finally, we verified that there is no extremal self-dual neighbor of F_{60}, which are equivalent to none of the extremal self-dual codes previously obtained in this note.

4 Extremal four-circulant self-dual [60, 30, 10] codes and self-dual neighbors

Using an approach similar to that given in Sect. 2, our exhaustive search found all distinct four-circulant self-dual [60, 30, 10] codes. Then our computer search shows that the distinct four-circulant self-dual [60, 30, 10] codes are divided into 113 inequivalent codes.

Proposition 4 *Up to equivalence, there are* 113 *four-circulant self-dual* [60, 30, 10] *codes.*

We denote the 113 codes by $G_{60,i}$ $(i = 1, 2, \ldots, 113)$. For the 13 codes $G_{60,i}$ $(i = 1, 2, \ldots, 13)$, the first rows r_A (resp. r_B) of the circulant matrices A (resp. B) in generator matrices (1) are listed in Table 4. The first rows for the all codes can be obtained from http://www.math.is.tohoku.ac.jp/~mharada/Paper/60-4cir-d10.txt.

In addition, we found extremal self-dual [60, 30, 12] codes by considering self-dual neighbors of $G_{62,i}$ $(i = 1, 2, \ldots, 113)$. Using a method similar to that given in [4], we completed

Table 4 Four-circulant self-dual [60, 30, 10] codes $G_{60,i}$

Code	r_A	r_B
$G_{60,1}$	(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)	(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)
$G_{60,2}$	(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)	(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)
$G_{60,3}$	(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)	(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)
$G_{60,4}$	(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)	(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)
$G_{60,5}$	(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)	(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)
$G_{60,6}$	(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)	(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)
$G_{60,7}$	(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)	(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)
$G_{60,8}$	(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)	(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)
$G_{60,9}$	(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)	(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)
$G_{60,10}$	(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)	(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)
$G_{60,11}$	(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)	(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)
$G_{60,12}$	(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)	(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)
$G_{60,13}$	(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)	(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)

the classification of extremal self-dual [60, 30, 12] neighbors of $G_{62,i}$ $(i = 1, 2, \dots, 113)$. Our computer search shows that there is an extremal self-dual [60, 30, 12] neighbor $H_{60,i}$ for $i = 1, 2, \dots, 13$ and that there is no extremal self-dual [60, 30, 12] neighbor for $i = 14, 15, \dots, 113$. The codes $H_{60,i}$ are constructed as $\langle (D \cap \langle x \rangle^{\perp}), x \rangle$, where D and supp(x) are listed in Table 5 and W indicates the values β in the weight enumerator $W_{60,1}$. We verified that there are the following equivalent codes among C_{60,i_1}, D_{60,i_2}, E_{60,i_3}, F_{60}, H_{60,i_4}:

$$H_{60,2} \cong C_{60,4}, \quad H_{60,5} \cong C_{60,1}, \quad H_{60,6} \cong C_{60,3}, \quad H_{60,7} \cong C_{60,8}, \quad H_{60,8} \cong C_{60,7},$$
$$H_{60,9} \cong C_{60,2}, \quad H_{60,11} \cong H_{60,3}, \quad H_{60,12} \cong H_{60,10}, \quad H_{60,13} \cong H_{60,4}, \quad H_{60,10} \cong D_{60,2},$$

where $C \cong D$ means that C and D are equivalent.

Similar to Sect. 3, by continuing this process, we completed a classification of extremal self-dual neighbors $J_{60,i}$ (resp. $K_{60,i}$, $L_{60,i}$), which are equivalent to none of the extremal self-dual codes previously obtained in this note, of $H_{60,j}$ (resp. $J_{60,j}$, $K_{60,j}$). Finally, we verified that there is no extremal self-dual neighbor of $L_{60,i}$ $(i = 1, 2)$, which are equivalent to none of the 37 codes in Tables 1, 2, 3 and 5. We remark that there is no pair of equivalent codes among the following 37 codes:

$$C_{60,i}\ (i = 1, 2, \dots, 13), \quad D_{60,i}\ (i = 1, 2, \dots, 7), \quad E_{60,i}\ (i = 1, 2, 3, 4), F_{60},$$
$$H_{60,i}\ (i = 1, 3, 4), \quad J_{60,i}\ (i = 1, 2, 3, 4, 5), \quad K_{60,i}\ (i = 1, 2), \quad L_{60,i}\ (i = 1, 2).$$

The codes $D_{60,3}$ and $J_{60,5}$ (see Tables 2, 5) establish Proposition 1. The code $J_{60,5}$ has the following weight enumerator:

$$\begin{aligned} &1 + 2939y^{12} + 31296y^{14} + 282321y^{16} + 1723904y^{18} + 7784760y^{20} \\ &+ 26386176y^{22} + 67197064y^{24} + 130097664y^{26} + 193168371y^{28} \\ &+ 220392832y^{30} + \cdots + y^{60}. \end{aligned}$$

Table 5 Extremal self-dual [60, 30, 12] neighbors $H_{60,i}$, $J_{60,i}$, $K_{60,i}$ and $L_{60,i}$

C	D	supp(x)	W
$H_{60,1}$	$G_{60,1}$	{4, 30, 32, 36, 37, 40, 42, 43, 47, 51, 52, 54, 57, 58}	$\beta = 10$
$H_{60,2}$	$G_{60,2}$	{1, 2, 4, 32, 36, 39, 40, 42, 49, 50, 55, 56, 57, 58}	$\beta = 0$
$H_{60,3}$	$G_{60,3}$	{1, 2, 32, 33, 34, 35, 37, 44, 45, 48, 51, 54, 55, 59}	$\beta = 0$
$H_{60,4}$	$G_{60,4}$	{2, 30, 32, 34, 36, 37, 40, 44, 48, 52, 55, 56, 58, 60}	$\beta = 0$
$H_{60,5}$	$G_{60,5}$	{1, 31, 32, 33, 35, 36, 37, 42, 43, 44, 46, 49, 56, 58}	$\beta = 0$
$H_{60,6}$	$G_{60,6}$	{1, 31, 32, 35, 38, 40, 41, 43, 44, 45, 51, 56, 58, 59}	$\beta = 0$
$H_{60,7}$	$G_{60,7}$	{1, 3, 5, 32, 37, 38, 41, 42, 50, 51, 53, 56, 57, 59}	$\beta = 0$
$H_{60,8}$	$G_{60,8}$	{1, 2, 3, 5, 6, 33, 34, 35, 36, 38, 42, 55, 56, 57}	$\beta = 0$
$H_{60,9}$	$G_{60,9}$	{1, 2, 6, 33, 35, 39, 41, 42, 43, 44, 46, 47, 55, 56}	$\beta = 0$
$H_{60,10}$	$G_{60,10}$	{2, 30, 32, 33, 36, 41, 43, 44, 48, 49, 51, 56, 59, 60}	$\beta = 0$
$H_{60,11}$	$G_{60,11}$	{2, 3, 32, 39, 40, 42, 43, 44, 45, 48, 51, 52, 56, 60}	$\beta = 0$
$H_{60,12}$	$G_{60,12}$	{2, 3, 32, 33, 34, 35, 36, 38, 45, 47, 51, 55, 56, 60}	$\beta = 0$
$H_{60,13}$	$G_{60,13}$	{1, 30, 35, 37, 41, 43, 44, 45, 46, 47, 48, 50, 54, 56}	$\beta = 0$
$J_{60,1}$	$H_{60,1}$	{4, 6, 36, 41, 43, 48, 49, 51, 53, 55, 56, 59}	$\beta = 10$
$J_{60,2}$	$H_{60,3}$	{1, 3, 4, 30, 32, 36, 37, 38, 51, 52, 55, 56}	$\beta = 0$
$J_{60,3}$	$H_{60,3}$	{1, 31, 34, 36, 39, 40, 41, 44, 45, 55, 56, 59}	$\beta = 0$
$J_{60,4}$	$H_{60,4}$	{2, 5, 33, 34, 37, 38, 39, 42, 44, 50, 57, 59}	$\beta = 0$
$J_{60,5}$	$H_{60,4}$	{3, 6, 7, 30, 34, 36, 39, 42, 48, 50, 53, 58}	$\beta = 6$
$K_{60,1}$	$J_{60,1}$	{1, 3, 4, 6, 36, 40, 41, 46, 47, 51, 54, 57}	$\beta = 10$
$K_{60,2}$	$J_{60,4}$	{5, 7, 34, 36, 37, 40, 41, 42, 47, 49, 50, 60}	$\beta = 6$
$L_{60,1}$	$K_{60,1}$	{2, 3, 32, 33, 37, 38, 41, 46, 51, 52, 57, 58}	$\beta = 10$
$L_{60,2}$	$K_{60,2}$	{2, 3, 32, 34, 37, 38, 41, 44, 47, 51, 53, 58}	$\beta = 6$

5 Optimal self-dual [58, 29, 10] codes

An extremal self-dual [60, 30, 12] code gives an optimal self-dual [58, 29, 10] code by subtracting two coordinates. We found all the optimal self-dual [58, 29, 10] codes by subtracting from the 37 inequivalent extremal self-dual [60, 30, 12] codes given in Sects. 2, 3 and 4. The only extremal self-dual [60, 30, 12] code $D_{60,3}$ gives 18 optimal self-dual [58, 29, 10] codes $C_{58,i}$ $(i = 1, 2, \dots, 18)$ with weight enumerator for which no optimal self-dual code was previously known to exist. More precisely, the codes by subtracting i and j have weight enumerator $W_{58,2}$ for $\beta = 2$ and $\gamma = 104$, where (i, j) are listed in Table 6. We verified that there are the following equivalent codes:

$$C_{58,1} \cong C_{58,i} \ (i = 2, 4, 5, 7, 8, 11, 12, 14, 15, 17, 18),$$
$$C_{58,3} \cong C_{58,i} \ (i = 6, 9, 10, 13, 16),$$

where $C_{58,1}$ and $C_{58,3}$ are inequivalent.

Similar to Sects. 3 and 4, we continue the search to find optimal self-dual [58, 29, 10] codes with weight enumerator for which no optimal self-dual code was previously known to exist, by considering self-dual neighbors of $C_{58,i}$ $(i = 1, 3)$. These codes $C = D_{58,i}$ are constructed as

$$\langle (D \cap \langle x \rangle^{\perp}), x \rangle,$$

Table 6 Optimal self-dual [58, 29, 10] codes $C_{58,i}$

Code	(i, j)	Code	(i, j)	Code	(i, j)
$C_{58,1}$	(2, 36)	$C_{58,7}$	(12, 31)	$C_{58,13}$	(22, 41)
$C_{58,2}$	(2, 41)	$C_{58,8}$	(12, 36)	$C_{58,14}$	(22, 48)
$C_{58,3}$	(2, 58)	$C_{58,9}$	(12, 53)	$C_{58,15}$	(22, 58)
$C_{58,4}$	(7, 31)	$C_{58,10}$	(17, 36)	$C_{58,16}$	(27, 31)
$C_{58,5}$	(7, 41)	$C_{58,11}$	(17, 53)	$C_{58,17}$	(27, 48)
$C_{58,6}$	(7, 48)	$C_{58,12}$	(17, 58)	$C_{58,18}$	(27, 53)

Table 7 Optimal self-dual [58, 29, 10] neighbors

C	D	supp(x)	W
$D_{58,1}$	$C_{58,1}$	{3, 4, 28, 30, 33, 41, 43, 44, 52, 53, 55, 56}	(2, 102)
$D_{58,2}$	$C_{58,1}$	{2, 3, 5, 28, 33, 34, 35, 41, 42, 44, 45, 50}	(2, 108)
$D_{58,3}$	$C_{58,3}$	{1, 4, 6, 7, 8, 39, 40, 41, 42, 43, 47, 52}	(2, 28)
$E_{58,1}$	$D_{58,2}$	{1, 3, 6, 7, 34, 35, 40, 47, 49, 51}	(2, 106)
$E_{58,2}$	$D_{58,3}$	{1, 6, 10, 28, 31, 32, 33, 40, 53, 54}	(0, 24)
$E_{58,3}$	$D_{58,3}$	{2, 6, 7, 8, 31, 34, 38, 45, 51, 57}	(1, 24)
$E_{58,4}$	$D_{58,3}$	{6, 8, 28, 30, 39, 40, 41, 46, 57, 58}	(1, 30)
$E_{58,5}$	$D_{58,3}$	{6, 32, 33, 38, 41, 42, 44, 46, 47, 57}	(2, 16)
$E_{58,6}$	$D_{58,3}$	{2, 5, 6, 33, 36, 39, 42, 52, 53, 56}	(2, 20)
$E_{58,7}$	$D_{58,3}$	{5, 6, 8, 36, 38, 41, 48, 51, 52, 55}	(2, 24)
$E_{58,8}$	$D_{58,3}$	{3, 6, 7, 12, 32, 33, 34, 43, 47, 54}	(2, 26)
$E_{58,9}$	$D_{58,3}$	{1, 8, 13, 35, 36, 44, 47, 50, 53, 55}	(2, 30)
$F_{58,1}$	$E_{58,6}$	{1, 4, 36, 38, 39, 41, 43, 45, 49, 58}	(0, 14)
$F_{58,2}$	$E_{58,5}$	{1, 5, 6, 7, 8, 11, 29, 31, 44, 46}	(1, 16)
$F_{58,3}$	$E_{58,5}$	{1, 2, 30, 32, 35, 44, 46, 47, 53, 58}	(1, 18)
$F_{58,4}$	$E_{58,5}$	{4, 6, 9, 34, 41, 42, 45, 50, 51, 56}	(1, 20)
$F_{58,5}$	$E_{58,5}$	{4, 5, 37, 41, 47, 49, 50, 55, 56, 58}	(1, 22)
$F_{58,6}$	$E_{58,5}$	{1, 4, 6, 7, 8, 35, 39, 41, 42, 43}	(2, 8)
$F_{58,7}$	$E_{58,5}$	{6, 7, 12, 15, 41, 43, 46, 47, 49, 56}	(2, 12)
$F_{58,8}$	$E_{58,5}$	{1, 6, 8, 29, 34, 39, 47, 50, 54, 55}	(2, 18)
$F_{58,9}$	$E_{58,5}$	{3, 35, 36, 38, 39, 42, 47, 49, 50, 56}	(2, 22)
$G_{58,1}$	$F_{58,1}$	{2, 7, 11, 29, 31, 32, 33, 48, 49, 52}	(0, 8)
$G_{58,2}$	$F_{58,7}$	{3, 9, 32, 38, 47, 48, 49, 51, 52, 55}	(0, 4)
$G_{58,3}$	$F_{58,7}$	{1, 8, 12, 30, 33, 40, 42, 49, 50, 55}	(2, 14)
H_{58}	$G_{58,2}$	{5, 6, 7, 9, 32, 44, 46, 47, 49, 58}	(0, 6)

where D and supp(x) are listed in Table 7. We verified that the codes $D_{58,i}$ have weight enumerator $W_{58,2}$, where W in Table 7 indicates the values (β, γ) in the weight enumerator $W_{58,2}$. By continuing this process, we found more optimal self-dual [58, 29, 10] codes with weight enumerator for which no optimal self-dual code was previously known to exist. The results are listed in Table 7. From Tables 6 and 7, we have Proposition 2.

6 Weight enumerator $W_{58,1}$

In this section, we give a remark on the possible weight enumerator $W_{58,1}$. First, we discuss a general case including $W_{58,1}$.

Proposition 5 *Let C be a self-dual $[n, n/2, d]$ code with shadow S of minimum weight* 1. *Let A_i and B_i denote the numbers of vectors of weight i in C and S, respectively. Suppose that $n \equiv 2 \pmod 8$ and $d \equiv 2 \pmod 4$. Then $B_{d-1} = A_d$.*

Proof Let x be the vector of weight 1 and let y be a vector of weight $d-1$ in S. Since $x + y \in C$, $x + y$ has weight d. Thus, $B_{d-1} \leq A_d$.

Now let c be a codeword of weight d in C and let x be the vector of weight 1 in S. Then we have $x + c \in S$. From the assumption that $n \equiv 2 \pmod 8$, the weight of $x + c$ is congruent to $1 \pmod 4$ by Theorem 5 in [3]. Hence, from the assumption that $d \equiv 2 \pmod 4$, $x + c$ has weight $d - 1$. Thus, $B_{d-1} \geq A_d$. The result follows. □

For example, Proposition 5 can be applied to the following parameters:

$$(n, d) = (58, 10), (74, 14) \text{ and } (98, 18).$$

- $(n, d) = (58, 10)$:
  The possible weight enumerator of the shadow of an optimal self-dual [58, 29, 10] code with weight enumerator $W_{58,1}$ is as follows [3]:

  $$y + \gamma y^9 + (23918 - 10\gamma)y^{13} + \cdots .$$

  By Proposition 5, we have

  $$165 - 2\gamma = \gamma.$$

  Since there is an optimal self-dual [58, 29, 10] code with weight enumerator $W_{58,1}$ for $\gamma = 55$ [12], we have the following:

Corollary 6 *There is an optimal self-dual* [58, 29, 10] *code with weight enumerator $W_{58,1}$ if and only if $\gamma = 55$.*

- $(n, d) = (74, 14)$:
  The largest minimum weight among self-dual codes of length 74 is at most 14 [6]. The weight enumerator W_2 in [6, p. 2039] is the possible weight enumerator of a self-dual [74, 37, 14] code with shadow of minimum weight 1. By Proposition 5, we have $\alpha = -135$ for W_2 in [6, p. 2039]. The weight enumerators of such a code and its shadow are as follows:

  $$1 + 2044y^{14} + 159067y^{16} + 520782y^{18} + \cdots ,$$
  $$y + 2044y^{13} + 679849y^{17} + 44010824y^{21} + \cdots ,$$

  respectively. It is still unknown whether there is a self-dual [74, 37, 14] code (with shadow of minimum weight 1).
- $(n, d) = (98, 18)$:
  The largest minimum weight among self-dual codes of length 98 is at most 18 [6]. The weight enumerator W_3 in [6, p. 2041] is the unique weight enumerator for a self-dual [98, 49, 18] code with shadow of minimum weight 1. The weight enumerators of such a code and its shadow are as follows:

$$1 + 22116y^{18} + 2016048y^{20} + 7181104y^{22} + \cdots,$$
$$y + 22116y^{17} + 9197152y^{21} + 964758896y^{25} + \cdots,$$

respectively. It is still unknown whether there is a self-dual [98, 49, 18] code (with shadow of minimum weight 1).

Acknowledgements This work was supported by JSPS KAKENHI Grant Number 15H03633. The author would like to thank the anonymous reviewers for the useful comments.

References

1. Bosma W., Cannon J., Playoust C.: The Magma algebra system I: The user language. J. Symb. Comput. **24**, 235–265 (1997).
2. Bouyuklieva S., Russeva R., Yankov N.: On the structure of binary self-dual codes having an automorphism of order a square of an odd prime. IEEE Trans. Inf. Theory **51**, 3678–3686 (2005).
3. Conway J.H., Sloane N.J.A.: A new upper bound on the minimal distance of self-dual codes. IEEE Trans. Inf. Theory **36**, 1319–1333 (1990).
4. Chigira N., Harada M., Kitazume M.: Extremal self-dual codes of length 64 through neighbors and covering radii. Des. Codes Cryptogr. **42**, 93–101 (2007).
5. Dontcheva R., Harada M.: Some extremal self-dual codes with an automorphism of order 7. Appl. Algebra Eng. Commun. Comput. **14**, 75–79 (2003).
6. Dougherty S.T., Gulliver T.A., Harada M.: Extremal binary self-dual codes. IEEE Trans. Inf. Theory **43**, 2036–2047 (1997).
7. Gulliver T.A., Harada M.: Weight enumerators of extremal singly-even [60, 30, 12] codes. IEEE Trans. Inf. Theory **42**, 658–659 (1996).
8. Harada M., Munemasa A.: Some restrictions on weight enumerators of singly even self-dual codes. IEEE Trans. Inf. Theory **52**, 1266–1269 (2006).
9. Karadeniz S., Aksoy R.: Self-dual R_k lifts of binary self-dual codes. Finite Fields Appl. **34**, 317–326 (2015).
10. Kaya A., Yildiz B., Siap I.: New extremal binary self-dual codes from $\mathbb{F}_4 + u\mathbb{F}_4$-lifts of quadratic circulant codes over $\mathbb{F}_4$. Finite Fields Appl. **35**, 318–329 (2015).
11. Rains E.M.: Shadow bounds for self-dual codes. IEEE Trans. Inf. Theory **44**, 134–139 (1998).
12. Tsai H.-P.: Existence of certain extremal self-dual codes. IEEE Trans. Inf. Theory **38**, 501–504 (1992).
13. Tsai H.-P., Jiang Y.J.: Some new extremal self-dual [58, 29, 10] codes. IEEE Trans. Inf. Theory **44**, 813–814 (1998).
14. Yankov N., Lee M.H.: New binary self-dual codes of lengths 50–60. Des. Codes Cryptogr. **73**, 983–996 (2014).