Interdisciplinary Information Sciences Vol. 24, No. 1 (2018) 77–85

ISSN 1340-9050 print/1347-6157 online
DOI 10.4036/iis.2017.R.03

Some Restrictions on Weight Enumerators of Singly Even Self-Dual Codes II

Masaaki HARADA* and Akihiro MUNEMASA

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

In this note, we give some restrictions on the number of vectors of weight $d/2+1$ in the shadow of a singly even self-dual $[n, n/2, d]$ code. This eliminates some of the possible weight enumerators of singly even self-dual $[n, n/2, d]$ codes for $(n, d) = (62, 12)$, $(72, 14)$, $(82, 16)$, $(90, 16)$ and $(100, 18)$.

KEYWORDS: self-dual code, weight enumerator, shadow

1. Introduction

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 $C_0^{\perp} \setminus C$. Shadows for self-dual codes were introduced by Conway and Sloane [6] 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. The largest possible minimum weights of singly even self-dual codes of lengths $n \le 72$ were given in [6, Table I]. The work was extended to lengths $74 \le n \le 100$ in [9, Table VI]. We denote by $d(n)$ the largest possible minimum weight given in [6, Table I] and [9, Table VI] throughout this note. The possible weight enumerators of singly even self-dual codes having minimum weight $d(n)$ were also given in [6] for lengths $n \le 64$ and $n = 72$ (see also [9] for length 72), and the work was extended to lengths up to 100 in [9]. It is a fundamental problem to find which weight enumerators actually occur among the possible weight enumerators (see [6] and [11]).

Some restrictions on the number of vectors of weight $d/2$ in the shadow of a singly even self-dual $[n, n/2, d]$ code were given in [10]. Also, some restrictions on the number of vectors of weight $d/2+1$ in the shadow of a singly even self-dual $[n, n/2, d]$ code were given in [2] for $n \equiv 0 \pmod 4$. In this note, we improve the result in [2] about the restriction on the number of vectors of weight $d/2+1$ in the shadow of a singly even self-dual $[n, n/2, d]$ code for $n \equiv 0 \pmod 4$. We also give a restriction on the number of vectors of weight $d/2+1$ in the shadow of a singly even self-dual $[n, n/2, d]$ code for $n \equiv 2 \pmod 4$. These restrictions eliminate some of the possible weight enumerators determined in [6] and [9] for the parameters $(n, d) = (62, 12)$, $(72, 14)$, $(82, 16)$, $(90, 16)$ and $(100, 18)$.

2. Preliminaries

A (binary) $[n, k]$ *code* C is a k-dimensional vector subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ denotes the finite field of order 2. All codes in this note are binary. The parameter n is called the *length* of C. The *weight* $\mathrm{wt}(x)$ of a vector $x \in \mathbb{F}_2^n$ is the number of non-zero components of x. A vector of C is a *codeword* of C. The minimum non-zero weight of all codewords in C is called the *minimum weight* $d(C)$ of C and an $[n, k]$ code with minimum weight d is called an $[n, k, d]$ code. 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 exists at least one codeword of weight $\equiv 2 \pmod 4$. Rains [12] showed that the minimum weight d of a self-dual code C of length n is bounded by $d \le 4\lfloor \frac{n}{24} \rfloor + 6$ if $n \equiv 22 \pmod{24}$, $d \le 4\lfloor \frac{n}{24} \rfloor + 4$ otherwise. In addition, if $n \equiv 0 \pmod{24}$ and C is singly even, then $d \le 4\lfloor \frac{n}{24} \rfloor + 2$. A self-dual code meeting the bound is called *extremal*. Let A_i and B_i be the numbers of vectors of weight i in C and S, respectively. The weight enumerators of C and S are given by $\sum_{i=0}^{n} A_i y^i$ and $\sum_{i=d(S)}^{n-d(S)} B_i y^i$, respectively, where $d(S)$ denotes the minimum weight of S.

Let C be a singly even self-dual code of length n and let S be the shadow of C. Let C_0 denote the subcode of codewords having weight $\equiv 0 \pmod 4$. 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 $S = C_1 \cup C_3$.

Received June 12, 2017; Accepted December 18, 2017; J-STAGE Advance published January 18, 2018
2010 Mathematics Subject Classification: Primary 94B05.
*Corresponding author. E-mail: mharada@m.tohoku.ac.jp

Lemma 1 (Conway and Sloane [6]). *Let x_1, y_1 be vectors of C_1 and let x_3 be a vector of C_3. Then $x_1 + y_1 \in C_0$, $x_1 + x_3 \in C_2$ and* $\mathrm{wt}(x_1) \equiv \mathrm{wt}(x_3) \equiv \frac{n}{2} \pmod 4$.

Lemma 2 (Brualdi and Pless [5]). *Let x_1, y_1 be vectors of C_1 and let x_3 be a vector of C_3.*
1) *Suppose that $n \equiv 0 \pmod 4$. Then $x_1 \cdot y_1 = 0$ and $x_1 \cdot x_3 = 1$.*
2) *Suppose that $n \equiv 2 \pmod 4$. Then $x_1 \cdot y_1 = 1$ and $x_1 \cdot x_3 = 0$.*

3. $n \equiv 2 \pmod 4$ and $d(S) = \frac{d(C)}{2} + 1$

Recall that the Johnson graph $J(v, d)$ has the collection X of all d-subsets of $\{1, 2, \ldots, v\}$ as vertices, and two distinct vertices are adjacent whenever they share $d - 1$ elements in common. Assume $v \geq 2d$ and set

$$R_i = \{(x, y) \in X \times X \mid |x \cap y| = d - i\}.$$

Then $\{R_i\}_{i=0}^{d}$ is a partition of $X \times X$. The following lemma is known as Delsarte's inequalities since it is the basis of Delsarte's linear programming bound. We refer the reader to [7] for an explicit formula for the second eigenmatrix Q appearing in the lemma.

Lemma 3 ([4, Proposition 2.5.2]). *Let Y be a subset of vertices of $J(v, d)$, and set*

$$a_i = \frac{1}{|Y|} |(Y \times Y) \cap R_i| \quad (0 \leq i \leq d).$$

If we denote by $Q = (q_j^{(v)}(i))$ the second eigenmatrix of $J(v, d)$, then every entry of the vector $(a_0, \ldots, a_d)Q$ is nonnegative.

Suppose that Y is a subset of vertices of $J(v, d)$ such that two distinct members intersect at exactly one element. Then by Lemma 3, every entry of the vector

$$(1, 0, \ldots, 0, 0, |Y| - 1, 0)Q$$

is nonnegative, i.e.,

$$q_j^{(v)}(0) + (|Y| - 1) q_j^{(v)}(d - 1) \geq 0 \quad (1 \leq j \leq d).$$

Thus, we obtain

$$|Y| \leq M_{v,d}, \tag{3.1}$$

where

$$M_{v,d} = \min\left\{1 - \frac{q_j^{(v)}(0)}{q_j^{(v)}(d-1)} \mid 1 \leq j \leq d \text{ and } q_j^{(v)}(d-1) < 0\right\}.$$

If we define

$$M_{v,d} = \begin{cases} 2 & \text{if } v = 2d - 1, \\ 1 & \text{if } d \leq v \leq 2d - 2, \\ 0 & \text{if } 0 \leq v \leq d - 1, \end{cases}$$

then (3.1) also holds for all v, d.

Now, let C be a singly even self-dual code of length n and let S be the shadow of C. For the remainder of this section, we assume that

$$n \equiv 2 \pmod 4 \text{ and } d(S) = \frac{d(C)}{2} + 1. \tag{3.2}$$

By Lemma 1, $d(C) \equiv n - 2 \pmod 8$, and hence $d(S)$ is odd.

For each of $i = 1, 3$, let Y_i be the set of supports of vectors of weight $d(S)$ in C_i, and let S_i be the union of the members of Y_i. From Lemma 2 and (3.2), we have the following:

$$|x \cap y| = \begin{cases} 1 & \text{if } x, y \in Y_i,\ x \neq y, \\ 0 & \text{if } x \in Y_1,\ y \in Y_3. \end{cases} \tag{3.3}$$

Then by (3.1), we have

$$|Y_i| \leq M_{|S_i|, d(S)}.$$

It follows from (3.3) that $S_1 \cap S_3 = \emptyset$. Thus, we have

$$B_{d(S)} = |Y_1| + |Y_3| \leq \max\{M_{v,d(S)} + M_{n-v,d(S)} \mid 0 \leq v \leq n/2\}. \quad (3.4)$$

For $42 \leq n \leq 98$ and $d(C) = d(n)$, the parameters $(n, d(C), d(S))$ satisfying Condition (3.2) are listed in Table 1, where the values $d(n)$ are also listed in the table. For some lengths n, the existence of a singly even self-dual code of length n and minimum weight $d(n)$ is currently not known. In this case, we consider the case $d(C) = d(n) - 2$. We calculated the upper bound (3.4), where the results are listed in Table 1. This calculation was done by the program written in MAGMA [1], where the program is listed in Appendix A.

Table 1. Parameters satisfying (3.2).

n	$d(n)$	$d(C)$	$d(S)$	$B_{d(S)}$
42	8	8	5	≤ 42
62	12	12	7	≤ 48
70	14	12	7	≤ 52
82	16	16	9	≤ 74
90	16	16	9	≤ 76
98	18	16	9	≤ 78

We discuss the possible weight enumerators for the case $d(n) = d(C)$ in Table 1. The possible weight enumerators W_{42} and S_{42} of an extremal singly even self-dual $[42, 21, 8]$ code with $d(S) \geq 5$ and its shadow are as follows [6]:

$$W_{42} = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^{10} + \cdots,$$
$$S_{42} = \beta y^5 + (896 - 8\beta)y^9 + (48384 + 28\beta)y^{13} + \cdots,$$

respectively, where β is an integer. It was shown in [3] that $0 \leq \beta \leq 42$. Table 1 gives an alternative proof.

The possible weight enumerators W_{62} and S_{62} of an extremal singly even self-dual $[62, 31, 12]$ code with $d(S) \geq 7$ and its shadow are as follows [6] (see also [8]):

$$W_{62} = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots,$$
$$S_{62} = \beta y^7 + (1116 - 12\beta)y^{11} + (171368 + 66\beta)y^{15} + \cdots,$$

respectively, where β is an integer with $0 \leq \beta \leq 93$. Table 1 gives the following:

Proposition 4. *If there exists an extremal singly even self-dual* $[62, 31, 12]$ *code with weight enumerator* W_{62}*, then* $0 \leq \beta \leq 48$.

It is known that there exists an extremal singly even self-dual $[62, 31, 12]$ code with weight enumerator W_{62} for $\beta = 0, 2, 9, 10, 15, 16$ (see [13]).

The possible weight enumerators W_{82} and S_{82} of an extremal singly even self-dual $[82, 41, 16]$ code with $d(S) \geq 9$ and its shadow are as follows [9]:

$$W_{82} = 1 + (39524 + 128\alpha)y^{16} + (556985 - 896\alpha)y^{18} + \cdots,$$
$$S_{82} = \alpha y^9 + (1640 - \alpha)y^{13} + (281424 + 120\alpha)y^{17} + \cdots,$$

respectively, where α is an integer with $0 \leq \alpha \leq \lfloor \frac{556985}{896} \rfloor = 621$. Table 1 gives the following:

Proposition 5. *If there exists an extremal singly even self-dual* $[82, 41, 16]$ *code with weight enumerator* W_{82}*, then* $0 \leq \alpha \leq 74$.

It is unknown whether there exists an extremal singly even self-dual code for any of these cases.

The possible weight enumerators W_{90} and S_{90} of an extremal singly even self-dual $[90, 45, 16]$ code with $d(S) \geq 9$ and its shadow are as follows [9]:

$$W_{90} = 1 + (9180 + 8\beta)y^{16} + (-512\alpha - 24\beta + 224360)y^{18} + \cdots,$$
$$S_{90} = \alpha y^9 + (\beta - 18\alpha)y^{13} + (112320 + 153\alpha - 16\beta)y^{17} + \cdots,$$

respectively, where α and β are integers with $0 \leq \alpha \leq \frac{1}{18}\beta \leq \lfloor \frac{224360}{24} \rfloor = 9348$. Table 1 gives the following:

Proposition 6. *If there exists an extremal singly even self-dual* $[90, 45, 16]$ *code with weight enumerator* W_{90}*, then* $0 \leq \alpha \leq 76$.

It is unknown whether there exists an extremal singly even self-dual code for any of these cases.

4. $n \equiv 0 \pmod 4$ and $d(S) = \frac{d(C)}{2} + 1$

Let C be a singly even self-dual code of length n and let S be the shadow of C. In this section, we write $d(C) = d$ and $d(S) = s$ for short, and assume that

$$n \equiv 0 \pmod 4 \text{ and } s = \frac{d}{2} + 1. \tag{4.1}$$

By Lemma 1, $d \equiv n - 2 \pmod 8$, and hence s is even.

Proposition 7 ([2]). *Suppose that $n \equiv 0 \pmod 4$ and $s = \frac{d}{2} + 1$. Let B_s denote the number of vectors of weight s in S.*

(i) *If $2n > (d+2)^2$, then*

$$B_s \le \frac{2n}{d+2}.$$

(ii) *If $(d+2)^2 \le 4n \le 2(d+2)^2$, then*

$$B_s \le d+2, \quad B_s \ne d+1.$$

(iii) *If $4n < (d+2)^2$, then*

$$B_s \le 2\frac{2n-d-2}{d}.$$

The above proposition was essentially established by showing $B_s \le \max\{l_1, l_2\}$, where

$$l_1 = \frac{2n}{d+2},$$
$$l_2 = \min\left\{d+2, 2\frac{2n-d-2}{d}\right\}.$$

We recall part of the proof of Proposition 7 for later use. Denote the set of all vectors in C_i of weight s by $\mathcal{B}_i$ $(i = 1, 3)$. Denote by $v * w$ the entrywise product of two vectors v, w. If $v, w \in \mathcal{B}_i$, then $\mathrm{wt}(v * w) = 0$ and hence these vectors have disjoint supports. This implies

$$|\mathcal{B}_i| \le l_1 \quad (i = 1, 3). \tag{4.2}$$

If $v \in \mathcal{B}_1$ and $w \in \mathcal{B}_3$, then $\mathrm{wt}(v * w) = 1$. Thus, if $\mathcal{B}_1$ and $\mathcal{B}_3$ are both nonempty, then

$$|\mathcal{B}_i| \le s. \tag{4.3}$$

Using the following lemmas, we give an improvement of the upper bound by showing $B_s \le \max\{l'_1, l'_2\}$, where

$$l'_1 = \begin{cases} l_1 & \text{if } n \text{ is divisible by } 2s, \\ 2\left\lceil \frac{n-d+2}{d+2} \right\rceil - 1 & \text{otherwise,} \end{cases}$$

$$l'_2 = \begin{cases} d+2 - \left\lceil \sqrt{(d+2)^2 - 4n} \right\rceil & \text{if } 4n < (d+2)^2, \\ \min\left\{d+2, 4\left\lceil \frac{n-d+2}{d+2} \right\rceil - 2\right\} & \text{otherwise.} \end{cases}$$

Since

$$\left\lceil \frac{n-d+2}{d+2} \right\rceil = \left\lceil \frac{n/4 - (s/2 - 1)}{s/2} \right\rceil \le \frac{n}{2s}, \tag{4.4}$$

we have

$$l'_1 \le l_1, \tag{4.5}$$

and

$$4\left\lceil \frac{n-d+2}{d+2} \right\rceil - 2 \le \frac{2n}{s} - 2 < 2\frac{2n-d-2}{d}.$$

The latter implies $l'_2 \le l_2$ provided $4n \ge (d+2)^2$. If $4n < (d+2)^2$, then

$$\begin{aligned} &2\frac{2n-d-2}{d} - \left(d+2-\sqrt{(d+2)^2-4n}\right) \\ &= \frac{\sqrt{(d+2)^2-4n}}{d}\left(d-\sqrt{(d+2)^2-4n}\right) \\ &\geq 0. \end{aligned}$$

Thus $l'_2 \leq l_2$ holds in this case as well. Therefore, the bound $B_s \leq \max\{l'_1, l'_2\}$ which will be shown in Proposition 10 below is an improvement of the bound given in Proposition 7.

Lemma 8. *Let*

$$k = \left\lceil \frac{n-d+2}{2s} \right\rceil.$$

If n is not divisible by $2s$, then $|\mathcal{B}_i| \leq 2k-1$ for $i = 1, 3$.

Proof. Suppose, to the contrary, $|\mathcal{B}_i| \geq 2k$. Then the sum of the all-one vector and the $2k$ vectors of weight s belongs to C_0 and has weight $n - 2ks \leq d - 2$. This forces $n - 2ks = 0$, contradicting the assumption. □

Lemma 9. *Let n and s be positive integers with $n < s^2$. Then*

$$\max\{a+b \mid a, b \in \mathbb{Z},\ 0 \leq a, b \leq s,\ s(a+b) - ab \leq n\} = 2s - \left\lceil 2\sqrt{s^2-n} \right\rceil.$$

Proof. Since $n < s^2$, we have

$$\begin{aligned} &\max\{a+b \mid a, b \in \mathbb{R},\ 0 \leq a, b \leq s,\ s(a+b) - ab \leq n\} \\ &\quad = \max\{a+b \mid 0 \leq a, b \leq s,\ (s-a)b \leq n - sa\} \\ &\quad = \max\{a + \min\{(n-sa)/(s-a), s\} \mid 0 \leq a < s\} \\ &\quad = \max\{(n-a^2)/(s-a) \mid 0 \leq a < s\}. \end{aligned}$$

The function $f(x) = (n-x^2)/(s-x)$ defined on the interval $[0, s)$ has maximum $f(\alpha) = 2\alpha$, where $\alpha = s - \sqrt{s^2-n}$. Thus, we have

$$\begin{aligned} &\max\{a+b \mid a, b \in \mathbb{Z},\ 0 \leq a, b \leq s,\ s(a+b) - ab \leq n\} \\ &\quad \leq \lfloor \max\{a+b \mid a, b \in \mathbb{R},\ 0 \leq a, b \leq s,\ s(a+b) - ab \leq n\} \rfloor \\ &\quad = \lfloor 2\alpha \rfloor. \end{aligned}$$

Define $a, b \in \mathbb{Z}$ by $a = \lfloor \alpha \rfloor$ and

$$b = \begin{cases} \lfloor \alpha \rfloor & \text{if } \alpha - \lfloor \alpha \rfloor < \frac{1}{2}, \\ \lfloor \alpha \rfloor + 1 & \text{otherwise.} \end{cases}$$

Then $a + b = \lfloor 2\alpha \rfloor = 2s - \left\lceil 2\sqrt{s^2-n} \right\rceil$. Since $\alpha < s$, we have $b \leq s$. It remains to show $s(a+b) - ab \leq n$, or equivalently,

$$ab - s(a+b) + n \geq 0. \tag{4.6}$$

Observe

$$s - \lfloor \alpha \rfloor = \left\lceil \sqrt{s^2-n} \right\rceil.$$

If $\alpha - \lfloor \alpha \rfloor < \frac{1}{2}$, then

$$\begin{aligned} ab - s(a+b) + n &= \lfloor \alpha \rfloor^2 - 2s\lfloor \alpha \rfloor + n \\ &= (s - \lfloor \alpha \rfloor)^2 - (s^2 - n) \\ &= \left\lceil \sqrt{s^2-n} \right\rceil^2 - (s^2-n) \\ &\geq 0. \end{aligned}$$

Thus, (4.6) holds.

If $\alpha - \lfloor \alpha \rfloor \geq \frac{1}{2}$, then

$$s - \lfloor \alpha \rfloor \geq \sqrt{s^2-n} + \frac{1}{2}.$$

Thus

$$\begin{aligned} ab - s(a+b) + n &= \lfloor\alpha\rfloor(\lfloor\alpha\rfloor + 1) - s(2\lfloor\alpha\rfloor + 1) + n \\ &= (\lfloor\alpha\rfloor - s)(\lfloor\alpha\rfloor + 1 - s) - (s^2 - n) \\ &\geq \left(\sqrt{s^2 - n} + \frac{1}{2}\right)\left(\sqrt{s^2 - n} - \frac{1}{2}\right) - (s^2 - n) \\ &= -\frac{1}{4}. \end{aligned}$$

Since $ab - s(a+b) + n$ is an integer, (4.6) holds. □

Proposition 10. *Suppose that $n \equiv 0 \pmod 4$ and $s = \frac{d}{2} + 1$. Let B_s denote the number of vectors of weight s in S. Then*

$$B_s \leq \max\{l'_1, l'_2\}. \tag{4.7}$$

More precisely,

(i) *If $2n > d^2 + 6d$, then*

$$B_s \leq \begin{cases} \dfrac{2n}{d+2} & \text{if } n \text{ is divisible by } 2s, \\ 2\left\lceil \dfrac{n-d+2}{d+2} \right\rceil - 1 & \text{otherwise.} \end{cases}$$

(ii) *If $(d+2)^2 < 2n \leq d^2 + 6d$, then*

$$B_s \leq \begin{cases} \dfrac{2n}{d+2} & \text{if } n \text{ is divisible by } 2s, \\ d+2 & \text{otherwise.} \end{cases}$$

(iii) *If $d^2 + 8d - 4 < 4n \leq 2(d+2)^2$, then*

$$B_s \leq d+2, \quad B_s \neq d+1.$$

(iv) *If $(d+2)^2 \leq 4n \leq d^2 + 8d - 4$, then*

$$B_s \leq 4\left\lceil \frac{n-d+2}{d+2} \right\rceil - 2.$$

(v) *If $4n < (d+2)^2$, then*

$$B_s \leq d + 2 - \left\lceil \sqrt{(d+2)^2 - 4n} \right\rceil.$$

Proof. If one of $\mathcal{B}_1$ and $\mathcal{B}_3$ is empty, then (4.2) and Lemma 8 imply $B_s \leq l'_1$. If $\mathcal{B}_1$ and $\mathcal{B}_3$ are both nonempty, then by (4.3), we have $B_s \leq 2s = d+2$. Moreover, suppose $n < s^2$. Observe

$$\left| \bigcup_{x \in \mathcal{B}_1 \cup \mathcal{B}_3} \operatorname{supp}(x) \right| = s(|\mathcal{B}_1| + |\mathcal{B}_3|) - |\mathcal{B}_1||\mathcal{B}_3|,$$

and this is at most n. By (4.3), we can apply Lemma 9 to conclude

$$B_s \leq 2s - \left\lceil 2\sqrt{s^2 - n} \right\rceil.$$

Thus $B_s \leq l'_2$. Therefore, (4.7) holds.

Next, we determine $\max\{l'_1, l'_2\}$. If $2n > d^2 + 6d$, then

$$\frac{n-d+2}{d+2} > \frac{1}{2}(d+2) \in \mathbb{Z},$$

so

$$\begin{aligned} l'_1 &\geq 2\left\lceil \frac{n-d+2}{d+2} \right\rceil - 1 && \text{(by (4.4))} \\ &\geq 2\left(\frac{1}{2}(d+2) + 1\right) - 1 \\ &= d+3 \\ &\geq l'_2. \end{aligned}$$

Thus $\max\{l'_1, l'_2\} = l'_1$, and (i) holds.

Next suppose $(d+2)^2 < 2n \le d^2 + 6d$. Since

$$4\left\lceil \frac{n-d+2}{d+2} \right\rceil - 2 - (d+2) \ge 4\frac{n-d+2}{d+2} - 2 - (d+2) > \frac{d^2-2d+8}{d+2} > 0,$$

we have $l'_2 = d+2$. Since

$$\frac{n-d+2}{d+2} \le \frac{1}{2}(d+2) \in \mathbb{Z},$$

we have

$$2\left\lceil \frac{n-d+2}{d+2} \right\rceil - 1 < d+2 < l_1.$$

These imply

$$\max\{l'_1, l'_2\} = \begin{cases} l_1 & \text{if } n \text{ is divisible by } 2s, \\ l'_2 & \text{otherwise,} \end{cases}$$

and (ii) holds.

Next suppose $(d+2)^2 \le 4n \le 2(d+2)^2$. We claim

$$l'_2 = \begin{cases} d+2 & \text{if } 4n \le d^2+8d-4, \\ 4\left\lceil \frac{n-d+2}{d+2} \right\rceil - 2 & \text{otherwise.} \end{cases}$$

Indeed, since $(d+4)/4 = (s+1)/2 \notin \mathbb{Z}$, we have

$$d+2 > 4\left\lceil \frac{n-d+2}{d+2} \right\rceil - 2 \Longleftrightarrow \frac{s}{2} \ge \left\lceil \frac{n-d+2}{d+2} \right\rceil \Longleftrightarrow \frac{s}{2} \ge \frac{n-d+2}{d+2} \Longleftrightarrow 4n \le d^2+8d-4.$$

Since $4n \ge (d+2)^2$ and $d \ne 4$, we have $n \ge 3d-2$. Thus

$$4\left\lceil \frac{n-d+2}{d+2} \right\rceil - 2 \ge \frac{2n}{d+2}.$$

This, together with $2n \le (d+2)^2$ implies $l_1 \le l'_2$. Therefore, $\max\{l'_1, l'_2\} = l'_2$. Now (iii) and (iv) hold by Proposition 7 (ii).

Finally, suppose $4n < (d+2)^2$. Then it is easy to verify

$$\frac{2n}{d+2} \le d+2-\sqrt{(d+2)^2-4n},$$

hence $\max\{l'_1, l'_2\} = l'_2$ by (4.5). Thus (v) holds. □

Remark 11. In Proposition 10 (v), it is sometimes possible to draw a stronger conclusion

$$|\mathcal{B}_i| = \frac{1}{2}\left(d+2-\left\lceil \sqrt{(d+2)^2-4n} \right\rceil\right) \quad (i = 1, 3).$$

This is when a pair $\{a, b\}$ achieving the maximum in Lemma 9 is unique. For the parameters $(n, d, s) = (128, 22, 12)$, we necessarily have $|\mathcal{B}_i| = 8$ for $i = 1, 3$. In general, a pair $\{a, b\}$ achieving the maximum in Lemma 9 is not unique. For example, when $(n, d, s) = (120, 22, 12)$, both $\{6, 8\}$ and $\{7, 7\}$ achieve the maximum.

For only the parameters $(n, d, s) = (72, 14, 8)$ and $(100, 18, 10)$, Proposition 10 gives an improvement over Proposition 7, for $44 \le n \le 100$ and $d = d(n)$. The bounds on B_s obtained by Proposition 10 are listed in Table 2 for these parameters, together with the part of Proposition 10 used, where the bounds by Proposition 7 are listed in the last column. The values $d(n)$ are also listed in the table.

We discuss the possible weight enumerators for the case $d(n) = d$ in Table 2. The possible weight enumerators of an extremal singly even self-dual $[72, 36, 14]$ code with $s \ge 8$ and the shadow are as follows:

Table 2. Parameters satisfying (4.1).

n	$d(n)$	d	s	Proposition 10	Proposition 7
72	14	14	8	$B_s \le 14$ (iv)	$B_s \le 16, \neq 15$
100	18	18	10	$B_s \le 18$ (iv)	$B_s \le 20, \neq 19$
108	—	18	10	$B_s \le 18$ (iv)	$B_s \le 20, \neq 19$
116	—	18	10	$B_s \le 18$ (iv)	$B_s \le 20, \neq 19$
128	—	22	12	$B_s \le 16$ (v)	$B_s \le 21$

$$W_{72} = 1 + (8640 - 64\alpha)y^{14} + (124281 + 384\alpha)y^{16} + \cdots,$$
$$S_{72} = \alpha y^8 + (546 - 14\alpha)y^{12} + (244584 + 91\alpha)y^{16} + \cdots,$$

respectively, where α is an integer with $0 \le \alpha \le \lfloor \frac{546}{14} \rfloor = 39$ [9]. We remark that Conway and Sloane [6] give only two weight enumerators as the possible weight enumerators of an extremal singly even self-dual $[72, 36, 14]$ code with $s \ge 8$ without reason, namely $\alpha = 0, 1$ in W_{72}. Table 2 shows the following:

Proposition 12. *If there exists an extremal singly even self-dual* $[72, 36, 14]$ *code with weight enumerator* W_{72}*, then* $0 \le \alpha \le 14$.

It is unknown whether there exists an extremal singly even self-dual code for any of these cases.

The possible weight enumerators of a singly even self-dual $[100, 50, 18]$ code with $s \ge 10$ and the shadow are as follows:

$$W_{100} = 1 + (16\beta + 52250)y^{18} + (1024\alpha - 64\beta + 972180)y^{20} + \cdots,$$
$$S_{100} = \alpha y^{10} + (-20\alpha - \beta)y^{14} + (190\alpha + 104500 + 18\beta)y^{18} + \cdots,$$

respectively, where α, β are integers with $0 \le \alpha \le \frac{-1}{20}\beta \le \frac{5225}{32}$ [9]. Table 2 shows the following:

Proposition 13. *If there exists a singly even self-dual* $[100, 50, 18]$ *code with weight enumerator* W_{100}*, then* $0 \le \alpha \le 18$.

It is unknown whether there exists a singly even self-dual $[100, 50, 18]$ code for any of these cases.

We give more sets of parameters for which the bound on B_s obtained by Proposition 10 improves the bound obtained by Proposition 7:

$$(n, d, s) = (108, 18, 10), (116, 18, 10), (128, 22, 12).$$

These bounds are also listed in Table 2.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number 15H03633.

REFERENCES

[1] Bosma, W., Cannon, J., and Playoust, C., "The Magma algebra system I: The user language," *J. Symbolic Comput.*, **24**: 235–265 (1997).

[2] Bouyuklieva, S., Harada, M., and Munemasa, A., "Restrictions on the weight enumerators of binary self-dual codes of length 4*m*," In: *Proc. International Workshop Optimal Codes and Related Topics*, White Lagoon (2007) pp. 40–44.

[3] Bouyuklieva, S., Harada, M., and Munemasa, A., "Determination of weight enumerators of binary extremal self-dual $[42, 21, 8]$ codes," *Finite Fields Appl.*, **14**: 177–187 (2008).

[4] Brouwer, A. E., Cohen, A. M., and Neumaier, A., Distance-Regular Graphs, Springer-Verlag (1989).

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

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

[7] Delsarte, P., "An algebraic approach to the association schemes of coding theory," *Philips Research Reports Suppl.*, **10** (1973).

[8] Dontcheva, R., and Harada, M., "New extremal self-dual codes of length 62 and related extremal self-dual codes," *IEEE Trans. Inform. Theory*, **48**: 2060–2064 (2002).

[9] Dougherty, S. T., Gulliver, T. A., and Harada, M., "Extremal binary self-dual codes," *IEEE Trans. Inform. Theory*, **43**: 2036–2047 (1997).

[10] Harada, M., and Munemasa, A., "Some restrictions on weight enumerators of singly even self-dual codes," *IEEE Trans. Inform. Theory*, **52**: 1266–1269 (2006).

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

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

[13] Yankov, N., "Self-dual $[62, 31, 12]$ and $[64, 32, 12]$ codes with an automorphism of order 7," *Adv. Math. Commun.*, **8**: 73–81 (2014).

Appendix A

```
HahnPolynomial:=function(v,k,l,x)
  return (Binomial(v,l)-Binomial(v,l-1))*
      &+[ (-1)^i*Binomial(l,i)*Binomial(v+1-l,i)*
          Binomial(k,i)^(-1)*Binomial(v-k,i)^(-1)*
          Binomial(x,i) : i in [0..l] ];
end function;
Qmatrix:=function(v,k)
  return Matrix(Rationals(),k+1,k+1,
  [[HahnPolynomial(v,k,l,x) : l in [0..k] ]: x in [0..k]]);
end function;
boundM:=function(v,ds)
  if v le ds-1 then
    return 0;
  elif v le ds*2-2 then
    return 1;
  elif v eq ds*2-1 then
    return 2;
  else
  Q:=Qmatrix(v,ds);
  return Min( { 1-Q[1][i+1]/Q[ds][i+1] : i in [0..ds]
          | Q[ds][i+1] lt 0 } );
  end if;
end function;
res:=function(n,ds)
  bounds:=[ Floor(boundM(v,ds)+boundM(n-v,ds)):
          v in {0..(n div 2)} ];
  max:=Max(bounds);
  return max;
end function;

X:=[[42,5],[62,7],[70,7],[82,9],[90,9],[98,9]];
[res(x[1],x[2]): x in X] eq [42,48,52,74,76,78];
```