Nonexistence of certain singly even self-dual codes with minimal shadow

Stefka Bouyuklieva

Faculty of Mathematics and Informatics
Veliko Tarnovo University
5000 Veliko Tarnovo, Bulgaria

stefka@uni-vt.bg

Masaaki Harada Akihiro Munemasa

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

mharada@m.tohoku.ac.jp, munemasa@math.is.tohoku.ac.jp

Submitted: Jul 12, 2017; Accepted: Dec 28, 2017; Published: Jan 25, 2018
Mathematics Subject Classifications: 94B05

Abstract

It is known that there is no extremal singly even self-dual $[n, n/2, d]$ code with minimal shadow for $(n, d) = (24m+2, 4m+4)$, $(24m+4, 4m+4)$, $(24m+6, 4m+4)$, $(24m + 10, 4m + 4)$ and $(24m + 22, 4m + 6)$. In this paper, we study singly even self-dual codes with minimal shadow having minimum weight $d - 2$ for these (n, d). For $n = 24m + 2$, $24m + 4$ and $24m + 10$, we show that the weight enumerator of a singly even self-dual $[n, n/2, 4m + 2]$ code with minimal shadow is uniquely determined and we also show that there is no singly even self-dual $[n, n/2, 4m + 2]$ code with minimal shadow for $m \geqslant 155$, $m \geqslant 156$ and $m \geqslant 160$, respectively. We demonstrate that the weight enumerator of a singly even self-dual code with minimal shadow is not uniquely determined for parameters $[24m + 6, 12m + 3, 4m + 2]$ and $[24m + 22, 12m + 11, 4m + 4]$.

Keywords: self-dual code, shadow, weight enumerator

1 Introduction

A (binary) code C of length n is a vector subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ denotes the finite field of order 2. The *dual* code $C^\perp$ of C 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 $C = C^{\perp}$. Self-dual codes are divided into two classes. 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 $\equiv 2 \pmod 4$. 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 [5] in order to derive new upper bounds for the minimum weight of singly even self-dual codes. By considering shadows, Rains [9] showed that the minimum weight d of a self-dual code of length n is bounded by $d \leqslant 4\lfloor \frac{n}{24} \rfloor + 6$ if $n \equiv 22 \pmod{24}$, $d \leqslant 4\lfloor \frac{n}{24} \rfloor + 4$ otherwise. A self-dual code meeting the bound is called *extremal*.

Let C be a singly even self-dual code of length n with shadow S. Let $d(S)$ denote the minimum weight of S. We say that C is a code with *minimal shadow* if $r = d(S)$, where $r = 4, 1, 2$ and 3 if $n \equiv 0, 2, 4$ and $6 \pmod 8$, respectively. The concept of self-dual codes with minimal shadow was introduced in [2]. In that paper, different types of self-dual codes with the same parameters were compared with regard to the decoding error probability. In [3], the connection between singly even self-dual codes with minimal shadow of some lengths, combinatorial designs and secret sharing schemes was considered. It was shown in [4] that there is no extremal singly even self-dual code with minimal shadow for lengths $24m + 2$, $24m + 4$, $24m + 6$, $24m + 10$ and $24m + 22$. In [3], it was shown that the weight enumerator of a (non-extremal) singly even self-dual $[24m+2, 12m+1, 4m+2]$ code with minimal shadow is uniquely determined for each positive integer m. These motivate us to study singly even self-dual codes with minimal shadow having minimum weight two less than the hypothetical extremal case.

The main aim of this paper is to investigate singly even self-dual codes with minimal shadow having minimum weight $4m + 2$ for the lengths $24m + 2$, $24m + 4$ and $24m + 10$. We show that the weight enumerator of a singly even self-dual code with minimal shadow having minimum weight $4m+2$ is uniquely determined for lengths $24m+4$ and $24m+10$. For lengths $24m + 2$, $24m + 4$ and $24m + 10$, nonnegativity of the coefficients of weight enumerators shows that there is no such code for m sufficiently large. We also show that the uniqueness of the weight enumerator fails for the parameters $[24m+6, 12m+3, 4m+2]$ and $[24m + 22, 12m + 11, 4m + 4]$.

The paper is organized as follows. In Section 2, we review the results given by Rains [9]. In Section 3, we show that there is no singly even self-dual $[24m + 2, 12m + 1, 4m + 2]$ code with minimal shadow for $m \geqslant 155$. In Sections 4 and 5, for parameters $[24m + 4, 12m + 2, 4m + 2]$ and $[24m + 10, 12m + 5, 4m + 2]$, we show that there is no singly even self-dual code with minimal shadow for $m \geqslant 156$ and for $m \geqslant 160$, respectively. Finally, in Section 6, we demonstrate that the weight enumerator of a singly even self-dual code with minimal shadow is not uniquely determined for parameters $[24m+6, 12m+3, 4m+2]$ and $[24m + 22, 12m + 11, 4m + 4]$.

All computer calculations in this paper were done with the help of the algebra software Magma [1] and the mathematical software Maple and Mathematica.

2 Preliminaries

Let C be a singly even self-dual code of length n with shadow S. Write $n = 24m+8l+2r$, where m is an integer, $l \in \{0,1,2\}$ and $r \in \{0,1,2,3\}$. The weight enumerators $W_C(y)$ and $W_S(y)$ of C and S are given by ([5, (10), (11)])

$$W_C(y) = \sum_{i=0}^{12m+4l+r} a_i y^{2i} = \sum_{j=0}^{3m+l} c_j (1+y^2)^{12m+4l+r-4j}(y^2(1-y^2)^2)^j, \tag{1}$$

$$W_S(y) = \sum_{i=0}^{6m+2l} b_i y^{4i+r} = \sum_{j=0}^{3m+l} (-1)^j c_j 2^{12m+4l+r-6j} y^{12m+4l+r-4j}(1-y^4)^{2j}, \tag{2}$$

respectively, for suitable integers c_j. Let

$$(1+y^2)^{n/2-4j}(y^2(1-y^2)^2)^j = \sum_{i=0}^{12m+4l+r} \alpha'_{i,j} y^{2i} \quad (0 \leqslant j \leqslant 3m+l). \tag{3}$$

Then

$$\alpha'_{i,j} = \begin{cases} 0 & \text{if } 0 \leqslant i < j \leqslant 3m+l, \\ 1 & \text{if } 0 \leqslant i = j \leqslant 3m+l. \end{cases} \tag{4}$$

This implies that the $(3m+l+1) \times (3m+l+1)$ matrix $[\alpha'_{i,j}]$ is invertible, since it is unitriangular. Let $[\alpha_{i,j}]$ be its inverse matrix. Then by (4), we have

$$\alpha_{i,j} = \begin{cases} 0 & \text{if } 0 \leqslant i < j \leqslant 3m+l, \\ 1 & \text{if } 0 \leqslant i = j \leqslant 3m+l, \end{cases} \tag{5}$$

and

$$y^{2i} = \sum_{j=0}^{3m+l} \alpha_{j,i} (1+y^2)^{n/2-4j}(y^2(1-y^2)^2)^j \quad (0 \leqslant i \leqslant 3m+l) \tag{6}$$

by (3). By (1), (5) and (6), we obtain

$$c_i = \sum_{j=0}^{i} \alpha_{i,j} a_j. \tag{7}$$

Lemma 1. *For $1 \leqslant i \leqslant 3m+l$, we have*

$$\alpha_{i,0} = -\frac{n}{2i} \sum_{\substack{0 \leqslant t \leqslant n/2+1-6i \\ t+i \text{ is odd}}} (-1)^t \binom{\frac{n}{2}+1-6i}{t} \binom{\frac{n-7i-t-1}{2}}{\frac{i-t-1}{2}}. \tag{8}$$

Proof. For $1 \leqslant i$,

$$\alpha_{i,0} = -\frac{n}{2i} [\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n/2-1+4i}(1-y)^{-2i}],$$

[9]. Since

$$\begin{aligned}
&(1+y)^{-n/2-1+4i}(1-y)^{-2i}\\
&=(1-y^2)^{-n/2-1+4i}(1-y)^{n/2+1-6i}\\
&=(1-y^2)^{-n/2-1+4i}\sum_{t=0}^{n/2+1-6i}(-1)^t\binom{\frac{n}{2}+1-6i}{t}y^t,
\end{aligned}$$

we have

$$\begin{aligned}
\alpha_{i,0}&=-\frac{n}{2i}\sum_{t=0}^{n/2+1-6i}(-1)^t\binom{\frac{n}{2}+1-6i}{t}[\text{coeff. of } y^{i-1} \text{ in } (1-y^2)^{-n/2-1+4i}y^t]\\
&=-\frac{n}{2i}\sum_{\substack{0\leqslant t\leqslant n/2+1-6i\\ t+i \text{ is odd}}}(-1)^t\binom{\frac{n}{2}+1-6i}{t}(-1)^{(i-t-1)/2}\binom{-\frac{n}{2}-1+4i}{\frac{i-t-1}{2}}.
\end{aligned}$$

The result follows by applying the formula

$$(-1)^j\binom{-n}{j}=\binom{n+j-1}{j}.$$

□

Write

$$(-1)^j 2^{n/2-6j}y^{n/2-4j}(1-y^4)^{2j}=\sum_{i=0}^{6m+2l}\beta'_{i,j}y^{4i+r}\quad(0\leqslant j\leqslant 3m+l).$$

Since $n/2-4j=4(3m+l-j)+r$, we have

$$\beta'_{i,j}=\begin{cases}0 & \text{if } i<3m+l-j,\\ (-1)^j 2^{n/2-6j} & \text{if } i=3m+l-j.\end{cases}$$

This implies that the $(3m+l+1)\times(3m+l+1)$ matrix $[\beta'_{i,3m+l-j}]$ is invertible, since it is lower triangular such that the diagonal elements are not zeros. Thus, the matrix $[\beta'_{i,j}]$ is also invertible. Let $[\beta_{i,j}]$ be its inverse matrix. Then

$$y^{4i+r}=\sum_{j=0}^{3m+l}\beta_{j,i}(-1)^j 2^{n/2-6j}y^{n/2-4j}(1-y^4)^{2j}\quad(0\leqslant i\leqslant 3m+l). \tag{9}$$

Moreover, $[\beta_{3m+l-i,j}]$ is the inverse of the lower triangular matrix $[\beta'_{i,3m+l-j}]$, and so lower triangular as well, and

$$\beta_{3m+l-j,j}=\beta'^{-1}_{j,3m+l-j}.$$

Thus

$$\beta_{i,j}=\begin{cases}0 & \text{if } i>3m+l-j,\\ (-1)^{3m+l-j}2^{6(3m+l-j)-n/2} & \text{if } i=3m+l-j.\end{cases} \tag{10}$$

By (2), (9) and (10), we obtain

$$c_i = \sum_{j=0}^{3m+l-i} \beta_{i,j} b_j. \tag{11}$$

Lemma 2 (Rains [9]). *For $1 \leqslant i \leqslant 3m+l$ and $0 \leqslant j \leqslant 3m+l$ with $i+j \leqslant 3m+l$, we have*

$$\beta_{i,j} = (-1)^i 2^{-n/2+6i} \frac{3m+l-j}{i} \binom{3m+l+i-j-1}{3m+l-i-j}. \tag{12}$$

From (7) and (11), we have

$$c_i = \sum_{j=0}^{i} \alpha_{i,j} a_j = \sum_{j=0}^{3m+l-i} \beta_{i,j} b_j. \tag{13}$$

Now let C be a singly even self-dual $[24m+8l+2r, 12m+4l+r, 4m+2]$ code with minimal shadow. Suppose that $(l,r) \in \{(0,1),(0,2),(1,1)\}$. Since the minimum weight of C is $4m+2$, we have

$$a_0 = 1, a_1 = a_2 = \cdots = a_{2m} = 0. \tag{14}$$

Since the minimum weight of the shadow is 1 or 2, we have

$$\begin{cases} b_0 = 1 & \text{if } m = 1, \\ b_0 = 1, b_1 = b_2 = \cdots = b_{m-1} = 0 & \text{if } m \geqslant 2. \end{cases} \tag{15}$$

From (13), (14) and (15), we have

$$c_i = \begin{cases} \alpha_{i,0} & \text{if } i = 0,1,\ldots,2m, \\ \beta_{i,0} & \text{if } i = 2m+l+1, 2m+l+2, \ldots, 3m+l. \end{cases} \tag{16}$$

Suppose that $l = 0$. From (13), (14), (15) and (16), we obtain

$$c_{2m} = \alpha_{2m,0} = \beta_{2m,0} + \beta_{2m,m} b_m, \tag{17}$$

$$c_{2m-1} = \alpha_{2m-1,0} = \beta_{2m-1,0} + \beta_{2m-1,m} b_m + \beta_{2m-1,m+1} b_{m+1}. \tag{18}$$

Suppose that $l = 1$. From (13), (14), (15) and (16), we obtain

$$c_{2m} = \alpha_{2m,0} = \beta_{2m,0} + \beta_{2m,m} b_m + \beta_{2m,m+1} b_{m+1}, \tag{19}$$

$$c_{2m+1} = \alpha_{2m+1,0} + \alpha_{2m+1,2m+1} a_{2m+1} = \beta_{2m+1,0} + \beta_{2m+1,m} b_m. \tag{20}$$

3 Singly even self-dual $[24m + 2, 12m + 1, 4m + 2]$ codes with minimal shadow

It was shown in [3] that the weight enumerator of a singly even self-dual $[24m+2, 12m+1, 4m+2]$ code with minimal shadow is uniquely determined for each length. In this section, we show that there is no singly even self-dual $[24m + 2, 12m + 1, 4m + 2]$ code with minimal shadow for $m \geqslant 155$.

Suppose that $m \geqslant 1$. Let C be a singly even self-dual $[24m + 2, 12m + 1, 4m + 2]$ code with minimal shadow. The weight enumerators of C and its shadow S are written as in (1) and (2), respectively.

From (8),

$$\alpha_{2m,0} = \frac{12m+1}{m}\binom{5m}{m-1}.$$

From (10),

$$\beta_{2m,m} = \frac{1}{2}.$$

From (12),

$$\beta_{2m,0} = \frac{3}{2^2}\binom{5m-1}{m} = \frac{3(4m+1)}{5m}\binom{5m}{m-1}.$$

From (17),

$$b_m = \frac{\alpha_{2m,0} - \beta_{2m,0}}{\beta_{2m,m}} = \frac{4(24m+1)}{5m}\binom{5m}{m-1}.$$

Remark 3. Unfortunately, b_m was incorrectly reported in [12]. The correct formula for b_m is given in [13]. We showed that b_m is always a positive integer (see [13]).

From (8),

$$\begin{aligned}\alpha_{2m-1,0} = &-\frac{12m+1}{2m-1}\left(\binom{5m+4}{m-1} + 28\binom{5m+3}{m-2} + 70\binom{5m+2}{m-3}\right.\\ &\left.+28\binom{5m+1}{m-4} + \binom{5m}{m-5}\right)\\ = &-\frac{8(12m+1)(376m^3-4m^2+5m+1)}{(4m+2)(4m+3)(4m+4)(4m+5)}\binom{5m}{m-1}.\end{aligned}$$

From (10),

$$\beta_{2m-1,m+1} = -\frac{1}{2^7}.$$

From (12),

$$\begin{aligned}\beta_{2m-1,0} &= -\frac{1}{2^7}\frac{3m}{2m-1}\binom{5m-2}{m+1} = -\frac{1}{2^4}\frac{3(4m-1)(4m+1)}{5(5m-1)(m+1)}\binom{5m}{m-1},\\ \beta_{2m-1,m} &= -\frac{m}{2^5}.\end{aligned}$$

From (18),

$$\begin{aligned} b_{m+1} =& \frac{\alpha_{2m-1,0} - \beta_{2m-1,0} - \beta_{2m-1,m} b_m}{\beta_{2m-1,m+1}} \\ =& - \frac{64(24m+1)f(m)}{(5m-1)(4m+2)(4m+3)(4m+4)(4m+5)} \binom{5m}{m-1}, \end{aligned}$$

where

$$f(m) = 64m^5 - 14816m^4 + 2812m^3 + 46m^2 - 14m + 1.$$

Theorem 4. *All coefficients in the weight enumerators of a singly even self-dual* $[24m+2, 12m+1, 4m+2]$ *code with minimal shadow and its shadow are nonnegative integers if and only if* $1 \leqslant m \leqslant 154$. *In particular, for* $m \geqslant 155$, *there is no singly even self-dual* $[24m+2, 12m+1, 4m+2]$ *code with minimal shadow.*

Proof. We verified that the equation $f(m) = 0$ has three solutions consisting of real numbers and the largest solution is in the interval $(231, 232)$. Thus, b_{m+1} is negative for $m \geqslant 232$. Using (1) and (2), we determined numerically the weight enumerators of a singly even self-dual $[24m+2, 12m+1, 4m+2]$ code with minimal shadow and its shadow for $m \leqslant 231$. The theorem follows from this calculation. □

4 Singly even self-dual $[24m+4, 12m+2, 4m+2]$ codes with minimal shadow

Proposition 5. *The weight enumerator of a singly even self-dual* $[24m+4, 12m+2, 4m+2]$ *code with minimal shadow is uniquely determined for each length.*

Proof. The weight enumerator of a singly even self-dual $[4, 2, 2]$ code is uniquely determined. Suppose that $m \geqslant 1$. Let C be a singly even self-dual $[24m+4, 12m+2, 4m+2]$ code with minimal shadow. The weight enumerators of C and its shadow S are written as using (1) and (2). Since $\alpha_{i,0}$ $(i = 0, 1, \dots, 2m)$ and $\beta_{i,0}$ $(i = 2m+1, 2m+2, \dots, 3m)$ are calculated by (8) and (12), respectively, from (16), c_i $(i = 0, 1, \dots, 3m)$ depends only on m. This means that the weight enumerator of C is uniquely determined for each length. □

From (8),

$$\begin{aligned} \alpha_{2m,0} =& \frac{6m+1}{m} \left(3\binom{5m+1}{m-1} + \binom{5m}{m-2} \right) \\ =& \frac{(6m+1)(8m+1)}{m(2m+1)} \binom{5m}{m-1}. \end{aligned}$$

From (10),

$$\beta_{2m,m} = \frac{1}{2^2}.$$

From (12),

$$\beta_{2m,0} = \frac{1}{2^2}\frac{3}{2}\binom{5m-1}{m} = \frac{3(4m+1)}{10m}\binom{5m}{m-1}.$$

From (17),

$$b_m = \frac{\alpha_{2m,0} - \beta_{2m,0}}{\beta_{2m,m}} = \frac{2(12m+1)(38m+7)}{5m(2m+1)}\binom{5m}{m-1}.$$

Remark 6. Unfortunately, b_m was incorrectly reported in [12]. The correct formula for b_m is given in [13]. We showed that b_m is always a positive integer (see [13]).

From (8),

$$\begin{aligned}\alpha_{2m-1,0} = &-\frac{12m+2}{2m-1}\left(\binom{5m+5}{m-1} + 36\binom{5m+4}{m-2} + 126\binom{5m+3}{m-3}\right. \\ &\left. +84\binom{5m+2}{m-4} + 9\binom{5m+1}{m-5}\right) \\ = &-\frac{16(5m+1)(6m+1)(8m+1)(68m^2-m+3)}{(4m+2)(4m+3)(4m+4)(4m+5)(4m+6)}\binom{5m}{m-1}.\end{aligned}$$

From (10),

$$\beta_{2m-1,m+1} = -\frac{1}{2^8}.$$

From (12),

$$\begin{aligned}\beta_{2m-1,0} &= -\frac{1}{2^8}\frac{3m}{2m-1}\binom{5m-2}{m+1} = -\frac{1}{2^5}\frac{3(4m-1)(4m+1)}{5(5m-1)(m+1)}\binom{5m}{m-1}, \\ \beta_{2m-1,m} &= -\frac{m}{2^6}.\end{aligned}$$

From (18),

$$\begin{aligned}b_{m+1} = &\frac{\alpha_{2m-1,0} - \beta_{2m-1,0} - \beta_{2m-1,m}b_m}{\beta_{2m-1,m+1}} \\ = &-\frac{128(12m+1)f(m)}{(5m-1)(4m+2)(4m+3)(4m+4)(4m+5)(4m+6)}\binom{5m}{m-1},\end{aligned}$$

where

$$f(m) = 1216m^6 - 212096m^5 - 33020m^4 + 5440m^3 + 1171m^2 + 88m + 6.$$

Theorem 7. *All coefficients in the weight enumerators of a singly even self-dual $[24m+4, 12m+2, 4m+2]$ code with minimal shadow and its shadow are nonnegative integers if and only if $1 \leqslant m \leqslant 155$. In particular, for $m \geqslant 156$, there is no singly even self-dual $[24m+4, 12m+2, 4m+2]$ code with minimal shadow.*

Proof. We verified that the equation $f(m) = 0$ has two solutions consisting of real numbers and the largest solution is in the interval $(174, 175)$. Thus, b_{m+1} is negative for $m \geqslant 175$. Using (1) and (2), we determined numerically the weight enumerators of a singly even self-dual $[24m+4, 12m+2, 4m+2]$ code with minimal shadow and its shadow for $m \leqslant 174$. The theorem follows from this calculation. □

5 Singly even self-dual $[24m + 10, 12m + 5, 4m + 2]$ codes with minimal shadow

Lemma 8 (Harada [7]). *Suppose that* $n \equiv 2 \pmod 8$. *Let* C *be a singly even self-dual* $[n, n/2, d]$ *code with minimal shadow. If* $d \equiv 2 \pmod 4$, *then* $a_{d/2} = b_{(d-2)/4}$.

As a consequence, the weight enumerator of a singly even self-dual $[58, 29, 10]$ code with minimal shadow was uniquely determined in [7].

Proposition 9. *The weight enumerator of a singly even self-dual* $[24m+10, 12m+5, 4m+2]$ *code with minimal shadow is uniquely determined for each length.*

Proof. The weight enumerator of a singly even self-dual $[10, 5, 2]$ code with minimal shadow is uniquely determined. Suppose that $m \geqslant 1$. Let C be a singly even self-dual $[24m + 10, 12m + 5, 4m + 2]$ code with minimal shadow. The weight enumerators of C and its shadow S are written as in (1) and (2), respectively. Since $\alpha_{i,0}$ $(i = 0, 1, \dots, 2m)$ and $\beta_{i,0}$ $(i = 2m + 2, 2m + 3, \dots, 3m + 1)$ are calculated by (8) and (12), respectively, from (16), c_i $(i = 0, 1, \dots, 2m, 2m + 2, \dots, 3m + 1)$ depends only on m.

From (5) and (10), we have

$$\alpha_{2m+1,2m+1} = 1 \text{ and } \beta_{2m+1,m} = -2,$$

respectively. By Lemma 8, it holds that $a_{2m+1} = b_m$. From (20), we obtain

$$a_{2m+1} = \frac{\beta_{2m+1,0} - \alpha_{2m+1,0}}{3}. \tag{21}$$

Therefore, from (20), c_{2m+1} depends only on m. This means that the weight enumerator of C is uniquely determined for each length. □

From (8), we have

$$\alpha_{2m+1,0} = -\frac{12m + 5}{2m + 1}\binom{5m + 1}{m}.$$

From (12), we have

$$\beta_{2m+1,0} = -2\frac{3m + 1}{2m + 1}\binom{5m + 1}{m}.$$

Since $a_{2m+1} = b_m$, from (21), we have

$$b_m = \binom{5m+1}{m} = \frac{5m+1}{4m+1}\binom{5m}{m}.$$

From (8),

$$\begin{aligned}\alpha_{2m,0} =& \frac{12m+5}{2m}\left(6\binom{5m+4}{m-1} + 20\binom{5m+3}{m-2} + 6\binom{5m+2}{m-3}\right)\\ =& \frac{4(12m+5)(5m+1)(5m+2)(32m^2+19m+3)}{(4m+1)(4m+2)(4m+3)(4m+4)(4m+5)}\binom{5m}{m}.\end{aligned}$$

From (10),

$$\beta_{2m,m+1} = \frac{1}{2^5}.$$

From (12),

$$\begin{aligned}\beta_{2m,0} =& \frac{1}{2^5}\frac{3m+1}{2m}\binom{5m}{m+1} = \frac{1}{2^4}\frac{3m+1}{m+1}\binom{5m}{m},\\ \beta_{2m,m} =& \frac{1}{2^5}\frac{2m+1}{2m}4m = \frac{2m+1}{2^4}.\end{aligned}$$

From (19),

$$\begin{aligned}b_{m+1} =& \frac{\alpha_{2m,0} - \beta_{2m,0} - \beta_{2m,m}b_m}{\beta_{2m,m+1}}\\ =& -\frac{16(5m+2)f(m)}{(4m+1)(4m+2)(4m+3)(4m+4)(4m+5)}\binom{5m}{m},\end{aligned}$$

where

$$f(m) = 64m^5 - 15040m^4 - 18036m^3 - 7924m^2 - 1511m - 105.$$

Theorem 10. *All coefficients in the weight enumerators of a singly even self-dual* $[24m+10, 12m+5, 4m+2]$ *code with minimal shadow and its shadow are nonnegative integers if and only if* $1 \leqslant m \leqslant 159$. *In particular, for* $m \geqslant 160$, *there is no singly even self-dual* $[24m+10, 12m+5, 4m+2]$ *code with minimal shadow.*

Proof. We verified that the equation $f(m) = 0$ has three solutions consisting of real numbers and the largest solution is in the interval $(236, 237)$. Thus, b_{m+1} is negative for $m \geqslant 237$. Using (1) and (2), we determined numerically the weight enumerators of a singly even self-dual $[24m+10, 12m+5, 4m+2]$ code with minimal shadow and its shadow for $m \leqslant 236$. The theorem follows from this calculation. □

6 Remaining cases

For the remaining cases, we demonstrate that the weight enumerator of a singly even self-dual code with minimal shadow is not uniquely determined.

6.1 Singly even self-dual $[24m + 6, 12m + 3, 4m + 2]$ codes with minimal shadow

Using (1) and (2), the possible weight enumerators of a singly even self-dual $[30, 15, 6]$ code with minimal shadow and its shadow are given by

$$1 + (35 - 8\beta)y^6 + (345 + 24\beta)y^8 + 1848y^{10} + \cdots,$$
$$\beta y^3 + (240 - 6\beta)y^7 + (6720 + 15\beta)y^{11} + \cdots,$$

respectively, where β is an integer with $1 \leqslant \beta \leqslant 4$. It is known that there is a singly even self-dual $[30, 15, 6]$ code with minimal shadow for $\beta \in \{1, 2\}$ (see [5]).

Using (1) and (2), the possible weight enumerators of a singly even self-dual $[54, 27, 10]$ code with minimal shadow and its shadow are given by

$$1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + (43884 + 32\beta)y^{14} + \cdots,$$
$$y^3 + (-12 + \beta)y^7 + (2874 - 10\beta)y^{11} + (258404 + 45\beta)y^{15} + \cdots,$$

respectively, where β is an integer with $12 \leqslant \beta \leqslant 43$. It is known that there is a singly even self-dual $[54, 27, 10]$ code with minimal shadow for $\beta \in \{12, 13, \dots, 20, 21, 22, 24, 26\}$ (see [10]).

6.2 Singly even self-dual $[24m + 22, 12m + 11, 4m + 4]$ codes with minimal shadow

Using (1) and (2), the possible weight enumerators of a singly even self-dual $[22, 11, 4]$ code with minimal shadow and its shadow are given by

$$1 + 2\beta y^4 + (77 - 2\beta)y^6 + (330 - 6\beta)y^8 + (616 + 6\beta)y^{10} + \cdots,$$
$$\beta y^3 + (352 - 4\beta)y^7 + (1344 + 6\beta)y^{11} + \cdots,$$

respectively, where β is an integer with $1 \leqslant \beta \leqslant 38$. It is known that there is a singly even self-dual $[22, 11, 4]$ code with minimal shadow for $\beta \in \{2, 4, 6, 8, 10, 14\}$ (see [8]).

Using (1) and (2), the possible weight enumerators of a singly even self-dual $[46, 23, 8]$ code with minimal shadow and its shadow are given by

$$1 + 2\beta y^8 + (884 - 2\beta)y^{10} + (10556 - 14\beta)y^{12} + (54621 + 14\beta)y^{14} + \cdots,$$
$$y^3 + (-10 + \beta)y^7 + (6669 - 8\beta)y^{11} + (242760 + 28\beta)y^{15} + \cdots,$$

respectively, where β is an integer with $10 \leqslant \beta \leqslant 442$. Let C_{46} be the code with generator matrix $\begin{bmatrix} I_{23} & R \end{bmatrix}$, where I_{23} denotes the identity matrix of order 23 and R is the 23×23 circulant matrix with first row

$$(01011101011100000111110).$$

We verified that C_{46} is a singly even self-dual $[46, 23, 8]$ code. By considering self-dual neighbors of C_{46}, we found singly even self-dual $[46, 23, 8]$ codes $N_{46,i}$ with minimal shadow

Codes	supp(x)	β
$N_{46,1}$	$\{1, 24, 26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 42, 43, 45, 46\}$	36
$N_{46,2}$	$\{1, 27, 28, 31, 33, 35, 36, 37, 42, 43, 45, 46\}$	42
$N_{46,3}$	$\{10, 11, 20, 27, 29, 34, 38, 41, 42, 45\}$	44
$N_{46,4}$	$\{5, 6, 25, 29, 30, 32, 33, 36, 40, 41, 44, 45\}$	46
$N_{46,5}$	$\{1, 23, 28, 29, 30, 31, 32, 37, 40, 41, 44, 45\}$	48
$N_{46,6}$	$\{1, 26, 27, 28, 30, 32, 35, 36, 37, 42, 43, 45\}$	50
$N_{46,7}$	$\{2, 3, 24, 25, 26, 28, 29, 33, 34, 36, 37, 41, 42, 44\}$	52
$N_{46,8}$	$\{1, 25, 28, 29, 32, 33, 34, 36, 38, 42, 43, 45\}$	54
$N_{46,9}$	$\{1, 23, 24, 27, 30, 36, 40, 41, 44, 45\}$	56
$N_{46,10}$	$\{1, 2, 25, 29, 30, 33, 35, 38, 44, 46\}$	58

Table 1: Singly even self-dual $[46, 23, 8]$ codes $N_{46,i}$ with minimal shadows.

($i = 1, 2, \dots, 10$). These codes are constructed as $\langle C_{46} \cap \langle x\rangle^{\perp}, x\rangle$, where the supports supp(x) of x are listed in Table 1. The values β in the weight enumerators of $N_{46,i}$ are also listed in the table.

The possible weight enumerators of a singly even self-dual $[70, 35, 12]$ code with minimal shadow and its shadow are given by

$$1 + 2\beta y^{12} + (9682 - 2\beta)y^{14} + (173063 - 22\beta)y^{16} + \cdots,$$
$$y^3 + (-104 + \beta)y^{11} + (88480 - 12\beta)y^{15} + \cdots,$$

respectively, where β is an integer $104 \leqslant \beta \leqslant 4841$ [6]. It is known that there is a singly even self-dual $[70, 35, 12]$ code with minimal shadow for many different β [11, p. 1191].

Acknowledgements

The first author is supported by Grant DN 02/2/13.12.2016 of the Bulgarian National Science Fund. The second author is supported by JSPS KAKENHI Grant Number 15H03633.

References

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

[2] S. Bouyuklieva, A. Malevich, and W. Willems. On the performance of binary extremal self-dual codes. *Adv. Math. Commun.*, 5:267–274, 2011.

[3] S. Bouyuklieva and Z. Varbanov. Some connections between self-dual codes, combinatorial designs and secret sharing schemes. *Adv. Math. Commun.*, 5:191–198, 2011.

[4] S. Bouyuklieva and W. Willems. Singly even self-dual codes with minimal shadow. *IEEE Trans. Inform. Theory*, 58:3856–3860, 2012.

[5] 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.

[6] M. Harada. The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes. *Finite Fields Appl.*, 3:131–139, 1997.

[7] M. Harada. Binary extremal self-dual codes of length 60 and related codes. *Des. Codes Cryptogr.*, (to appear), arXiv:1706.01694.

[8] 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.

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

[10] N. Yankov and M. H. Lee. New binary self-dual codes of lengths 50–60. *Des. Codes Cryptogr.*, 73:983–996, 2014.

[11] N. Yankov, M. H. Lee, Gürel, and M. Ivanova. Self-dual codes with an automorphism of order 11. *IEEE Trans. Inform. Theory*, 61:1188–1193, 2015.

[12] T. Zhang, J. Michel, T. Feng, and G. Ge. On the existence of certain optimal self-dual codes with lengths between 74 and 116. *Electron. J. Combin.*, 22:#P4.33, 2015.

[13] T. Zhang, J. Michel, T. Feng, and G. Ge. Erratum to "On the existence of certain optimal self-dual codes with lengths between 74 and 116". (submitted).