Weight enumerators of binary singly even self-dual codes

Akihiro Munemasa
Tohoku University
(joint work with Stefka Bouyuklieva and Masaaki Harada)

JCCA, August 18, 2017
Kumamoto University

Binary codes and their dual

A code C of length n is a vector subspace of $\mathbb{F}_2^n$.
The dual code $C^\perp$ of C is defined as

$$C^\perp = \{x \in \mathbb{F}_2^n \mid x \cdot y = 0 \text{ for all } y \in C\},$$

and C is self-dual if $C = C^\perp$.
A self-dual code C is

$$\begin{aligned} \text{doubly even} &\iff \mathrm{wt}(x) \equiv 0 \pmod 4 \quad (\forall x \in C), \\ \text{singly even} &\iff \text{otherwise} \\ &\iff C_0 = \{x \in C \mid \mathrm{wt}(x) \equiv 0 \pmod 4\} \\ &\qquad \subsetneq C \qquad \text{(codimension 1)} \end{aligned}$$

The minimum weight of C is

$$d(C) = \min\{\mathrm{wt}(x) \mid 0 \neq x \in C\}.$$

Upper bounds on minimum weight

Theorem (Mallows–Sloane (1973))

If C is a doubly even self-dual code of length n, then its minimum weight is at most

$$4\left\lfloor \frac{n}{24} \right\rfloor + 4.$$

Upper bounds on minimum weight

Theorem (Mallows–Sloane (1973))

If C is a doubly even self-dual code of length n, then its minimum weight is at most

$$4\left\lfloor \frac{n}{24} \right\rfloor + 4.$$

doubly even $\iff$ $\mathrm{wt}(x) \equiv 0 \pmod 4 \quad (\forall x \in C)$,

singly even $\iff$ otherwise

Upper bounds on minimum weight

Theorem (Mallows–Sloane (1973))

If C is a doubly even self-dual code of length n, then its minimum weight is at most

$$4\left\lfloor \frac{n}{24} \right\rfloor + 4.$$

Theorem (Rains (1999))

If C is a self-dual code of length n, then its minimum weight is at most

$$\begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 4 & \text{if } n \not\equiv 22 \pmod{24}, \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 6 & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

A self-dual code meeting this upper bound is called extremal.
Doubly even $\implies n \equiv 0 \pmod 8$.

Shadow

Let C be a singly even self-dual code of length n and let

$$C_0 = \{x \in C \mid \mathrm{wt}(x) \equiv 0 \pmod 4\} \subsetneq C.$$

The shadow S is defined to be

$$S = C_0^\perp \setminus C.$$

Then

$$\mathrm{wt}(x) \equiv n/2 \pmod 4 \quad (\forall x \in S),$$

so, letting $d(S) = \min\{\mathrm{wt}(x) \mid x \in S\}$, we say that C is a code with minimal shadow if

$$d(S) = \begin{cases} 1 & \text{if } n \equiv 2 \pmod 8, \\ 2 & \text{if } n \equiv 4 \pmod 8, \\ 3 & \text{if } n \equiv 6 \pmod 8, \\ 4 & \text{if } n \equiv 0 \pmod 8. \end{cases}$$

Shadow

Let C be a singly even self-dual code of length n and let

$$C_0 = \{x \in C \mid \mathrm{wt}(x) \equiv 0 \pmod 4\} \subsetneq C.$$

The shadow S is defined to be

$$S = C_0^{\perp} \setminus C.$$

Then

$$\mathrm{wt}(x) \equiv n/2 \pmod 4 \quad (\forall x \in S),$$

so, letting $d(S) = \min\{\mathrm{wt}(x) \mid x \in S\}$, we say that C is a code with minimal shadow if

$$d(S) = \begin{cases} 1 & \text{if } n \equiv 2 \pmod 8, \\ 2 & \text{if } n \equiv 4 \pmod 8, \\ 3 & \text{if } n \equiv 6 \pmod 8, \\ 4 & \text{if } n \equiv 0 \pmod 8. \end{cases}$$

Shadow

Let C be a singly even self-dual code of length n and let

$$C_0 = \{x \in C \mid \mathrm{wt}(x) \equiv 0 \pmod 4\} \subsetneq C.$$

The shadow S is defined to be

$$S = C_0^{\perp} \setminus C.$$

Then

$$\mathrm{wt}(x) \equiv n/2 \pmod 4 \quad (\forall x \in S),$$

so, letting $d(S) = \min\{\mathrm{wt}(x) \mid x \in S\}$, we say that C is a code with minimal shadow if

$$d(S) = \begin{cases} 1 & \text{if } n \equiv 2 \pmod 8, \\ 2 & \text{if } n \equiv 4 \pmod 8, \\ 3 & \text{if } n \equiv 6 \pmod 8, \\ 4 & \text{if } n \equiv 0 \pmod 8. \end{cases}$$

Singly even self-dual codes with minimal shadow

length n	$d = 4m + 4$ (extremal)	$d = 4m + 2$
$24m + 2$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 4$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 6$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !~~w~~.e.
$24m + 8$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 10$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 12$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 14$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 16$	$d(C) = 4m + 4$, ($\nexists$)	
$24m + 18$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 22$	$d(C) = 4m + 6$, $\nexists$	$d(C) = 4m + 4$, !~~w~~.e.

($\nexists$) means that nonexistence is shown for sufficiently large m.

Bouyuklieva and Varbanov (2011), by Bouyuklieva and Willems (2012),

Bouyuklieva, Harada and Munemasa (2017+)

Singly even self-dual codes with minimal shadow

length n	$d = 4m + 4$ (extremal)	$d = 4m + 2$
$24m + 2$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 4$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 6$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !~~w~~.e.
$24m + 8$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 10$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 12$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 14$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 16$	$d(C) = 4m + 4$, ($\nexists$)	
$24m + 18$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 22$	$d(C) = 4m + 6$, $\nexists$	$d(C) = 4m + 4$, !~~w~~.e.

($\nexists$) means that nonexistence is shown for sufficiently large m.

Bouyuklieva and Varbanov (2011), by Bouyuklieva and Willems (2012),

Bouyuklieva, Harada and Munemasa (2017+)

Singly even self-dual codes with minimal shadow

length n	$d = 4m + 4$ (extremal)	$d = 4m + 2$
$24m + 2$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 4$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 6$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !~~w~~.e.
$24m + 8$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 10$	$d(C) = 4m + 4$, $\nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 12$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 14$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 16$	$d(C) = 4m + 4$, ($\nexists$)	
$24m + 18$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 22$	$d(C) = 4m + 6$, $\nexists$	$d(C) = 4m + 4$, !~~w~~.e.

($\nexists$) means that nonexistence is shown for sufficiently large m.

Bouyuklieva and Varbanov (2011), by Bouyuklieva and Willems (2012),

Bouyuklieva, Harada and Munemasa (2017+)

Singly even self-dual codes with minimal shadow

length n	$d = 4m + 4$ (extremal)	$d = 4m + 2$
$24m + 2$	$d(C) = 4m + 4,\ \nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 4$	$d(C) = 4m + 4,\ \nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 6$	$d(C) = 4m + 4,\ \nexists$	$d(C) = 4m + 2$, !̸w.e.
$24m + 8$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 10$	$d(C) = 4m + 4,\ \nexists$	$d(C) = 4m + 2$, !w.e. ($\nexists$)
$24m + 12$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 14$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 16$	$d(C) = 4m + 4$, ($\nexists$)	
$24m + 18$	$d(C) = 4m + 4$, !w.e. ($\nexists$)	
$24m + 22$	$d(C) = 4m + 6,\ \nexists$	$d(C) = 4m + 4$, !̸w.e.

($\nexists$) means that nonexistence is shown for sufficiently large m.

Bouyuklieva and Varbanov (2011), by Bouyuklieva and Willems (2012),

Bouyuklieva, Harada and Munemasa (2017+)

$n = 24m + 4,\ d(C) = 4m + 2,\ d(S) = 2$

The weight enumerators of C and S:

$$W_C(y) = \sum_{i=0}^{12m+2} a_i y^{2i} \equiv \boldsymbol{a}\boldsymbol{y}^\top \pmod{y^{6m+1}},$$

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \equiv \boldsymbol{b}\boldsymbol{y}'^\top \pmod{y^{12m+3}},$$

where

$$\boldsymbol{y} = (1, y^2, y^4, \ldots, y^{6m}) \in \mathbb{Q}[y]^{3m+1},$$
$$\boldsymbol{y}' = (y^2, y^6, y^{10}, \ldots, y^{12m+2}) \in \mathbb{Q}[y]^{3m+1},$$
$$\boldsymbol{a} = (a_0, a_1, \ldots, a_{3m}) \in \mathbb{Z}^{3m+1},$$
$$\boldsymbol{b} = (b_0, b_1, \ldots, b_{3m}) \in \mathbb{Z}^{3m+1}.$$

$n = 24m + 4,\ d(C) = 4m + 2,\ d(S) = 2$

The weight enumerators of C and S:

$$W_C(y) = \sum_{i=0}^{12m+2} a_i y^{2i} \equiv \boldsymbol{a}\boldsymbol{y}^\top \pmod{y^{6m+1}},$$

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \equiv \boldsymbol{b}\boldsymbol{y}'^\top \pmod{y^{12m+3}},$$

where

$$\begin{aligned}
\boldsymbol{y} &= (1, y^2, y^4, \ldots, y^{6m}) \in \mathbb{Q}[y]^{3m+1}, \\
\boldsymbol{y}' &= (y^2, y^6, y^{10}, \ldots, y^{12m+2}) \in \mathbb{Q}[y]^{3m+1}, \\
\boldsymbol{a} &= (a_0, a_1, \ldots, a_{3m}) \in \mathbb{Z}^{3m+1}, \\
\boldsymbol{b} &= (b_0, b_1, \ldots, b_{3m}) \in \mathbb{Z}^{3m+1}.
\end{aligned}$$

$n = 24m+4,\ d(C) = 4m+2,\ d(S) = 2$

The weight enumerators of C and S:

$$W_C(y) = \sum_{i=0}^{12m+2} a_i y^{2i} \equiv \boldsymbol{a}\boldsymbol{y}^\top \pmod{y^{6m+1}},$$

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \equiv \boldsymbol{b}\boldsymbol{y}'^\top \pmod{y^{12m+3}},$$

where

$$\begin{aligned}
\boldsymbol{y} &= (1, y^2, y^4, \ldots, y^{6m}) \in \mathbb{Q}[y]^{3m+1}, \\
\boldsymbol{y}' &= (y^2, y^6, y^{10}, \ldots, y^{12m+2}) \in \mathbb{Q}[y]^{3m+1}, \\
\boldsymbol{a} &= (a_0, a_1, \ldots, a_{3m}) \in \mathbb{Z}^{3m+1}, \\
\boldsymbol{b} &= (b_0, b_1, \ldots, b_{3m}) \in \mathbb{Z}^{3m+1}.
\end{aligned}$$

$\boldsymbol{y} = (1, y^2, y^4, \dots, y^{6m})$, $\boldsymbol{y}' = (y^2, y^6, y^{10}, \dots, y^{12m+2})$

Rains (1999): Let

$$f_j = (1+y^2)^{12m+2-4j}(y^2(1-y^2)^2)^j \in \mathbb{Q}[y^2],$$
$$g_j = (-1)^j 2^{12m+2-6j} y^{12m+2-4j}(1-y^4)^{2j} \in y^2\mathbb{Q}[y^4].$$

Then

$$\mathbb{Q}[y]^{3m+1} \ni \boldsymbol{f} = (f_0, f_1, \dots, f_{3m+1}), \quad \boldsymbol{y} \equiv \boldsymbol{f}A \pmod{y^{6m+1}},$$
$$\ni \boldsymbol{g} = (g_0, g_1, \dots, g_{3m+1}), \quad \boldsymbol{y}' \equiv \boldsymbol{g}B \pmod{y^{12m+3}}.$$

$\exists \boldsymbol{c} \in \mathbb{Q}^{3m+1}$ such that

$$\boldsymbol{a}\boldsymbol{y}^\top \equiv W_C(y) = \boldsymbol{c}\boldsymbol{f}^\top \implies \boldsymbol{a}A^\top = \boldsymbol{c}$$
$$\boldsymbol{b}\boldsymbol{y}'^\top \equiv W_S(y) = \boldsymbol{c}\boldsymbol{g}^\top \implies \boldsymbol{b}B^\top = \boldsymbol{c}$$

$\boldsymbol{y} = (1, y^2, y^4, \dots, y^{6m}),$
$\boldsymbol{y}' = (y^2, y^6, y^{10}, \dots, y^{12m+2})$

Rains (1999): Let

$$f_j = (1+y^2)^{12m+2-4j}(y^2(1-y^2)^2)^j \in \mathbb{Q}[y^2],$$
$$g_j = (-1)^j 2^{12m+2-6j} y^{12m+2-4j}(1-y^4)^{2j} \in y^2\mathbb{Q}[y^4].$$

Then

$$\mathbb{Q}[y]^{3m+1} \ni \boldsymbol{f} = (f_0, f_1, \dots, f_{3m+1}), \quad \boldsymbol{y} \equiv \boldsymbol{f}A \pmod{y^{6m+1}},$$
$$\ni \boldsymbol{g} = (g_0, g_1, \dots, g_{3m+1}), \quad \boldsymbol{y}' \equiv \boldsymbol{g}B \pmod{y^{12m+3}}.$$

$\exists \boldsymbol{c} \in \mathbb{Q}^{3m+1}$ such that

$$\boldsymbol{a}\boldsymbol{y}^\top \equiv W_C(y) = \boldsymbol{c}\boldsymbol{f}^\top \implies \boldsymbol{a}A^\top = \boldsymbol{c}$$
$$\boldsymbol{b}\boldsymbol{y}'^\top \equiv W_S(y) = \boldsymbol{c}\boldsymbol{g}^\top \implies \boldsymbol{b}B^\top = \boldsymbol{c}$$

$\boldsymbol{y} = (1, y^2, y^4, \dots, y^{6m}),$
$\boldsymbol{y}' = (y^2, y^6, y^{10}, \dots, y^{12m+2})$

Rains (1999): Let

$$f_j = (1+y^2)^{12m+2-4j}(y^2(1-y^2)^2)^j \in \mathbb{Q}[y^2],$$
$$g_j = (-1)^j 2^{12m+2-6j} y^{12m+2-4j}(1-y^4)^{2j} \in y^2\mathbb{Q}[y^4].$$

Then

$$\mathbb{Q}[y]^{3m+1} \ni \boldsymbol{f} = (f_0, f_1, \dots, f_{3m+1}), \quad \boldsymbol{y} \equiv \boldsymbol{f}A \pmod{y^{6m+1}},$$
$$\ni \boldsymbol{g} = (g_0, g_1, \dots, g_{3m+1}), \quad \boldsymbol{y}' \equiv \boldsymbol{g}B \pmod{y^{12m+3}}.$$

$\exists \boldsymbol{c} \in \mathbb{Q}^{3m+1}$ such that

$$\boldsymbol{a}\boldsymbol{y}^\top \equiv W_C(y) = \boldsymbol{c}\boldsymbol{f}^\top \implies \boldsymbol{a}A^\top = \boldsymbol{c}$$
$$\boldsymbol{b}\boldsymbol{y}'^\top \equiv W_S(y) = \boldsymbol{c}\boldsymbol{g}^\top \implies \boldsymbol{b}B^\top = \boldsymbol{c}$$

$\boldsymbol{y} = (1, y^2, y^4, \dots, y^{6m}),$
$\boldsymbol{y}' = (y^2, y^6, y^{10}, \dots, y^{12m+2})$

Rains (1999): Let

$$f_j = (1+y^2)^{12m+2-4j}(y^2(1-y^2)^2)^j \in \mathbb{Q}[y^2],$$
$$g_j = (-1)^j 2^{12m+2-6j} y^{12m+2-4j}(1-y^4)^{2j} \in y^2\mathbb{Q}[y^4].$$

Then

$$\mathbb{Q}[y]^{3m+1} \ni \boldsymbol{f} = (f_0, f_1, \dots, f_{3m+1}), \quad \boldsymbol{y} \equiv \boldsymbol{f}A \pmod{y^{6m+1}},$$
$$\ni \boldsymbol{g} = (g_0, g_1, \dots, g_{3m+1}), \quad \boldsymbol{y}' \equiv \boldsymbol{g}B \pmod{y^{12m+3}}.$$

$\exists \boldsymbol{c} \in \mathbb{Q}^{3m+1}$ such that

$$\boldsymbol{a}\boldsymbol{y}^\top \equiv W_C(y) = \boldsymbol{c}\boldsymbol{f}^\top \implies \boldsymbol{a}A^\top = \boldsymbol{c}$$
$$\boldsymbol{b}\boldsymbol{y}'^\top \equiv W_S(y) = \boldsymbol{c}\boldsymbol{g}^\top \implies \boldsymbol{b}B^\top = \boldsymbol{c}$$

$\boldsymbol{y} = (1, y^2, y^4, \dots, y^{6m}),$
$\boldsymbol{y}' = (y^2, y^6, y^{10}, \dots, y^{12m+2})$

Rains (1999): Let

$$f_j = (1+y^2)^{12m+2-4j}(y^2(1-y^2)^2)^j \in \mathbb{Q}[y^2],$$
$$g_j = (-1)^j 2^{12m+2-6j} y^{12m+2-4j}(1-y^4)^{2j} \in y^2\mathbb{Q}[y^4].$$

Then

$$\mathbb{Q}[y]^{3m+1} \ni \boldsymbol{f} = (f_0, f_1, \dots, f_{3m+1}), \quad \boldsymbol{y} \equiv \boldsymbol{f}A \pmod{y^{6m+1}},$$
$$\ni \boldsymbol{g} = (g_0, g_1, \dots, g_{3m+1}), \quad \boldsymbol{y}' \equiv \boldsymbol{g}B \pmod{y^{12m+3}}.$$

$\exists \boldsymbol{c} \in \mathbb{Q}^{3m+1}$ such that

$$\boldsymbol{a}\boldsymbol{y}^\top \equiv W_C(y) = \boldsymbol{c}\boldsymbol{f}^\top \implies \boldsymbol{a}A^\top = \boldsymbol{c}$$
$$\boldsymbol{b}\boldsymbol{y}'^\top \equiv W_S(y) = \boldsymbol{c}\boldsymbol{g}^\top \implies \boldsymbol{b}B^\top = \boldsymbol{c}$$

$\boldsymbol{a}A^\top = \boldsymbol{b}B^\top$, $d(C) = 4m+2$, $d(S) = 2$

$$W_C(y) = \sum_{i=0}^{12m+2} a_i y^{2i} \equiv \boldsymbol{a}\boldsymbol{y}^\top \pmod{y^{6m+1}}$$

$$d(C) = 4m+2 \implies a_0 = 1, \quad a_1 = \cdots = a_{2m} = 0,$$

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \equiv \boldsymbol{b}\boldsymbol{y}'^\top \pmod{y^{12m+3}}$$

$$d(S) = 2 \implies b_0 = 1, \quad b_1 = \cdots = b_{m-1} = 0.$$

$\boldsymbol{a}A^\top = \boldsymbol{b}B^\top$ implies

$$(1, \underbrace{0, \ldots, 0}_{2m}, \underbrace{\boldsymbol{a}'}_{m}) \begin{pmatrix} * & * \\ 0 & A' \end{pmatrix} = (1, \underbrace{0, \ldots, 0}_{m-1}, *) \begin{pmatrix} * & B' \\ * & 0 \end{pmatrix}$$

$$\implies \boldsymbol{a}'A' \to \boldsymbol{a}' \to \boldsymbol{a} \to W_C(y).$$

$\boldsymbol{a}A^\top = \boldsymbol{b}B^\top$, $d(C) = 4m+2$, $d(S) = 2$

$$W_C(y) = \sum_{i=0}^{12m+2} a_i y^{2i} \equiv \boldsymbol{a}\boldsymbol{y}^\top \pmod{y^{6m+1}}$$

$$d(C) = 4m+2 \implies a_0 = 1, \quad a_1 = \cdots = a_{2m} = 0,$$

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \equiv \boldsymbol{b}\boldsymbol{y}'^\top \pmod{y^{12m+3}}$$

$$d(S) = 2 \implies b_0 = 1, \quad b_1 = \cdots = b_{m-1} = 0.$$

$\boldsymbol{a}A^\top = \boldsymbol{b}B^\top$ implies

$$(1, \underbrace{0, \ldots, 0}_{2m}, \underbrace{\boldsymbol{a}'}_{m}) \begin{pmatrix} * & * \\ 0 & A' \end{pmatrix} = (1, \underbrace{0, \ldots, 0}_{m-1}, *) \begin{pmatrix} * & B' \\ * & 0 \end{pmatrix}$$

$$\implies \boldsymbol{a}'A' \to \boldsymbol{a}' \to \boldsymbol{a} \to W_C(y).$$

$\boldsymbol{a}A^\top = \boldsymbol{b}B^\top$, $d(C) = 4m+2$, $d(S) = 2$

$$W_C(y) = \sum_{i=0}^{12m+2} a_i y^{2i} \equiv \boldsymbol{a}\boldsymbol{y}^\top \pmod{y^{6m+1}}$$

$$d(C) = 4m+2 \implies a_0 = 1, \quad a_1 = \cdots = a_{2m} = 0,$$

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \equiv \boldsymbol{b}\boldsymbol{y}'^\top \pmod{y^{12m+3}}$$

$$d(S) = 2 \implies b_0 = 1, \quad b_1 = \cdots = b_{m-1} = 0.$$

$\boldsymbol{a}A^\top = \boldsymbol{b}B^\top$ implies

$$(1, \underbrace{0, \ldots, 0}_{2m}, \underbrace{\boldsymbol{a}'}_{m}) \begin{pmatrix} * & * \\ 0 & A' \end{pmatrix} = (1, \underbrace{0, \ldots, 0}_{m-1}, *) \begin{pmatrix} * & B' \\ * & 0 \end{pmatrix}$$

$$\implies \boldsymbol{a}'A' \to \boldsymbol{a}' \to \boldsymbol{a} \to W_C(y).$$

Formula for b_m

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \quad (b_0 = 1,\ b_1 = \cdots = b_{m-1} = 0)$$

is also uniquely determined. In fact,

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

but incorrectly reported in Zhang–Michel–Feng–Ge (2015). Moreover,

$$b_{m+1} = -\frac{\text{polynomial in } m \text{ of positive leading coeff.}}{(5m-1)\prod_{i=2}^{6}(4m+i)} \binom{5m}{m-1}$$
$$< 0 \quad (\text{for } m \text{ sufficiently large}).$$

Formula for b_m

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \quad (b_0 = 1,\ b_1 = \cdots = b_{m-1} = 0)$$

is also uniquely determined. In fact,

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

but incorrectly reported in Zhang–Michel–Feng–Ge (2015).
Moreover,

$$b_{m+1} = -\frac{\text{polynomial in } m \text{ of positive leading coeff.}}{(5m-1)\prod_{i=2}^{6}(4m+i)} \binom{5m}{m-1}$$

$$< 0 \quad (\text{for } m \text{ sufficiently large}).$$

Formula for b_m

$$W_S(y) = \sum_{i=0}^{6m} b_i y^{4i+2} \quad (b_0 = 1,\ b_1 = \cdots = b_{m-1} = 0)$$

is also uniquely determined. In fact,

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

but incorrectly reported in Zhang–Michel–Feng–Ge (2015).
Moreover,

$$b_{m+1} = -\frac{\text{polynomial in } m \text{ of positive leading coeff.}}{(5m-1)\prod_{i=2}^{6}(4m+i)} \binom{5m}{m-1}$$
$$< 0 \quad (\text{for } m \text{ sufficiently large}).$$

Our results

Theorem (Bouyuklieva–Harada–M., arXiv:1707.04059)

The weight enumerators $W_C(y)$ and $W_S(y)$ of a singly even self-dual code C of length $24m+4$, minimum weight $4m+2$ and its shadow are uniquely determined by m. These uniquely determined polynomials have all coefficients nonnegative if and only if $0 \leq m \leq 155$.
In particular, for $m \geq 156$, there is no singly even self-dual code of length $24m+4$, minimum weight $4m+2$ with minimal shadow.

We have similar theorems for the lengths $24m+2$ and $24m+10$.

Our results

Theorem (Bouyuklieva–Harada–M., arXiv:1707.04059)

The weight enumerators $W_C(y)$ and $W_S(y)$ of a singly even self-dual code C of length $24m + 4$, minimum weight $4m + 2$ and its shadow are uniquely determined by m. These uniquely determined polynomials have all coefficients nonnegative if and only if $0 \leq m \leq 155$.
In particular, for $m \geq 156$, there is no singly even self-dual code of length $24m + 4$, minimum weight $4m + 2$ with minimal shadow.

We have similar theorems for the lengths $24m + 2$ and $24m + 10$.