On a 5-design related to a putative extremal doubly even self-dual code of length a multiple of 24

Masaaki Harada*

March 20, 2014

Abstract

By the Assmus and Mattson theorem, the codewords of each non-trivial weight in an extremal doubly even self-dual code of length $24m$ form a self-orthogonal 5-design. In this paper, we study the codes constructed from self-orthogonal 5-designs with the same parameters as the above 5-designs. We give some parameters of a self-orthogonal 5-design whose existence is equivalent to that of an extremal doubly even self-dual code of length $24m$ for $m = 3, 4, 5, 6$. If $m \in \{1, \ldots, 6\}$, $k \in \{m + 1, \ldots, 5m - 1\}$ and $(m, k) \neq (6, 18)$, then it is shown that an extremal doubly even self-dual code of length $24m$ is generated by codewords of weight $4k$.

Keywords self-orthogonal $t$-design, extremal doubly even self-dual code, weight enumerator

Mathematics Subject Classification 94B05, 05B30

1 Introduction

A doubly even self-dual code of length $n$ exists if and only if $n$ is divisible by 8. The minimum weight $d(C)$ of a doubly even self-dual code $C$ of length...
A t-(v, k, λ) design is called self-orthogonal if the block intersection numbers have the same parity as the block size k (see [14]). If D is a self-orthogonal t-(v, k, λ) design with k even, then the code C(D), which is generated by the rows of an incidence matrix of D, is a self-orthogonal code. By the Assmus and Mattson theorem [2], the supports of the codewords of weight 4k (≠ 0, 24m) in an extremal doubly even self-dual code of length 24m form a self-orthogonal 5-design. We denote the parameters of the design by 5-(24m, 4k, λ24m, 4k). Then, throughout this paper, we denote any self-orthogonal 5-(24m, 4k, λ24m, 4k) design by D24m, 4k. That is, D24m, 4k is a self-orthogonal 5-design with the same parameters as the self-orthogonal 5-design formed from the supports of the codewords of weight 4k in an extremal doubly even self-dual code of length 24m. This gives rise to a natural question, namely, is the code C(D24m, 4k) always an extremal doubly even self-dual code?

It is well known that C(D24, 8) is the extended Golay code (see [1, Theorem 8.6.2]). It was shown that C(D24m, 4m+4) (m = 2, 3, 4) is an extremal doubly even self-dual code [9, 7, 6], respectively. This means that the existence of an extremal doubly even self-dual code of length 24m (m = 1, 2, 3, 4) is equivalent to that of a self-orthogonal 5-(24m, 4k, λ24m, 4k) design, where (4k, λ24m, 4k) = (8, 1), (12, 8), (16, 78) and (20, 816), respectively. The powerful tool which is used in [6, 7, 9] is the use of fundamental equations, sometimes called the Mendelsohn equations [12] (see also e.g., [14]), obtained by counting the number of blocks that meet S in i points for some subset S of the point set. The approach in [6, 7, 9, 10] except that in [7, 9] and Gleason’s theorem (see [10]) is employed to obtain stronger consequences.

In this paper, we study self-orthogonal 5-designs C(D24m, 4k) for k ∈ {m + 2, . . . , 5m − 1}, which are related to codewords of weight other than the minimum weight. More precisely, we consider a problem whether C(D24m, 4k) is an extremal doubly even self-dual code or not for m ∈ {1, . . . , 6} and k ∈ {m + 2, . . . , 5m − 1}. In addition to the above approach done in [6, 7, 9], it is useful in this paper to observe weight enumerators of C(D24m, 4k) and its dual codes, and singly even self-dual codes containing C(D24m, 4k) and their
shadows. As a summary, in Table 1, we list some partial answers to the above problem for \( m \in \{1, \ldots, 6\} \) and \( k \in \{m + 1, \ldots, 3m\} \). For the cases \((24m, 4k)\) that \( C(\mathcal{D}_{24m,4k}) \) is self-dual, we list “Yes” in the second column of Table 1. When \( C(\mathcal{D}_{24m,4k}) \) is self-dual, we list “Yes” in the third column in case that \( C(\mathcal{D}_{24m,4k}) \) is extremal. We also list the possible minimum weights, when \( C(\mathcal{D}_{24m,4k}) \) is self-dual but not extremal. It is shown that \( C(\mathcal{D}_{24m,4k}) = C(\mathcal{D}_{24m,24m-4k}) \) for \( m \in \{1, \ldots, 6\} \) and \( k \in \{m+1, \ldots, 3m-1\} \) (Proposition 9).

The main results of this paper are the following theorems.

**Theorem 1.** Suppose that \((24m, k, \lambda)\) is each of the following:

- \((72, 24, 1406405)\), \((72, 32, 238957796)\),
- \((96, 36, 2808050448)\), \((96, 44, 1167789832440)\),
- \((120, 56, 5156299310025435)\), \((144, 68, 21788133027489299328)\).

Then the existence of a self-orthogonal 5-(24m, k, \lambda) design is equivalent to that of an extremal doubly even self-dual code of length 24m.

**Theorem 2.** Suppose that \( m \in \{1, \ldots, 6\} \) and \( k \in \{m + 1, \ldots, 5m - 1\} \). If \((m, k) \neq (6, 18)\), then an extremal doubly even self-dual code of length 24m is generated by codewords of weight 4k.

**Remark 3.** For some cases \((m, k)\), the above theorem is already known (see Table 1). It is still unknown whether \( C(\mathcal{D}_{144,72}) \) is self-dual or not (see Remark 8).

## 2 Preliminaries

### 2.1 Self-dual codes and shadows

In this paper, codes mean binary codes. A code is called **doubly even** if every codeword has weight a multiple of 4. A code \( C \) is called **self-orthogonal** if \( C \subset C^\perp \), and \( C \) is called **self-dual** if \( C = C^\perp \), where \( C^\perp \) is the dual code of \( C \) under the standard inner product. A self-dual code which is not doubly even is called **singly even**, namely, a singly even self-dual code contains a codeword of weight \( \equiv 2 \pmod{4} \). It is known that a self-dual code of length \( n \) exists

\[ \text{See Sections 8 and 1 for the marks * in Table 1.} \]
Table 1: Codes $\mathcal{C}(\mathcal{D}_{24m,4k})$ ($m = 1, \ldots, 6$, $k = m + 1, \ldots, 3m$)

| Parameters of $\mathcal{D}_{24m,4k}$ | Self-dual | Extremal | Ref. |
|--------------------------------------|-----------|----------|------|
| $(24, 8, 1)$                         | Yes       | Yes      | (see [1]) |
| $(24, 12, 48)$                       | Yes       | Yes      | [11] |
| $(48, 12, 8)$                        | Yes       | Yes      | [9]  |
| $(48, 16, 1365)$                     | Yes       | Yes      | [5]  |
| $(48, 20, 36176)$                    | Yes       | Yes      | [5]  |
| $(48, 24, 190680)$                   | Yes       | 8, 12    |
| $(72, 16, 78)$                       | Yes       | Yes      | [7]  |
| $(72, 20, 20064)$                    | Yes       | 12, 16   | [5]  |
| $(72, 24, 1406405)$                  | Yes       | Yes*     |       |
| $(72, 28, 30888000)$                 | Yes*      | 12, 16   |       |
| $(72, 32, 238957796)$                | Yes       | Yes*     |       |
| $(72, 36, 693996160)$                | Yes       | 12, 16   |      |
| $(96, 20, 816)$                      | Yes       | Yes      | [6]  |
| $(96, 24, 257180)$                   | Yes       | 16, 20   | [5]  |
| $(96, 28, 29975400)$                 | Yes       | 12, 20*  |       |
| $(96, 32, 1390528685)$               | Yes       | 12, 16, 20 | [5] |
| $(96, 36, 28080500448)$              | Yes       | Yes*     |       |
| $(96, 40, 26151376460)$              | Yes       | 12, 16, 20 | [5] |
| $(96, 44, 1167789832440)$            | Yes       | Yes*     |       |
| $(96, 48, 2561776811880)$            | Yes*      | 12, 16, 20 | [5] |
| $(120, 24, 8855)$                    | Yes       | 16, 24   | [4]  |
| $(120, 28, 3146400)$                 | Yes       | 16, 20, 24 |     |
| $(120, 32, 502593700)$               | Yes       | 12, 16, 24* |   |
| $(120, 36, 37237713920)$             | Yes*      | 12–24    |       |
| $(120, 40, 1372275835848)$           | Yes*      | 12, 24*  |       |
| $(120, 44, 26386953577600)$          | Yes*      | 12–24    |       |
| $(120, 48, 274320081834480)$         | Yes*      | 12, 24*  |       |
| $(120, 52, 1582247888524800)$        | Yes*      | 12–24    |       |
| $(120, 56, 5156299310025435)$        | Yes       | Yes*     |       |
| $(120, 60, 9606041207517888)$        | Yes*      | 12–24    |       |
| $(144, 28, 98280)$                   | Yes       | 16, 20, 28 | [8] |
| $(144, 32, 37756202)$                | Yes       | 16–28    |       |
| $(144, 36, 7479335776)$              | Yes       | 16, 20, 28* |   |
| $(144, 40, 765322879032)$            | Yes       | 12–28    |       |
| $(144, 44, 42785304274536)$          | Yes       | 12, 16, 20, 28* |   |
| $(144, 48, 1359454757387265)$        | Yes       | 12–28    |       |
| $(144, 52, 25319185698144240)$       | Yes       | 12, 16, 28* |    |
| $(144, 56, 283096123959568608)$      | Yes*      | 12–28    |       |
| $(144, 60, 1935608752827917264)$     | Yes       | 12, 28*  |       |
| $(144, 64, 820589047403924124)$      | Yes       | 12–28    |       |
| $(144, 68, 21788133027489299328)$    | Yes       | Yes*     |       |
| $(144, 72, 36470135955078919440)$    | ?         | –        |       |
if and only if $n$ is even, and a doubly even self-dual code of length $n$ exists if and only if $n$ is divisible by eight. The minimum weight $d(C)$ of a doubly even self-dual code $C$ of length $n$ is bounded by $d(C) \leq 4\lfloor n/24 \rfloor + 4$ \cite{10}. A doubly even self-dual code meeting the bound is called extremal. In case that $n \equiv 0 \pmod{24}$, the only known extremal doubly even self-dual codes are the extended Golay code and the extended quadratic residue code of length 48. The existence of an extremal doubly even self-dual code of length 72 is a long-standing open question \cite{13}.

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 were introduced by Conway and Sloane \cite{3}, in order to provide restrictions on the weight enumerators of singly even self-dual codes (see \cite{3} for fundamental results on shadows). Let $D$ be a doubly even code of length $n \equiv 0 \pmod{8}$. Suppose that $D$ has dimension $n/2 - 1$ and $D$ contains the all-one vector $1$. Then there are three self-dual codes lying between $D^\perp$ and $D$, one of which is singly even and the others are doubly even (see \cite{11}).

2.2 Self-orthogonal designs and Mendelsohn equations

A $t$-$(v, k, \lambda)$ design $D$ is a set $X$ of $v$ points together with a collection of $k$-subsets of $X$ (called blocks) such that every $t$-subset of $X$ is contained in exactly $\lambda$ blocks. A $t$-design with no repeated block is called simple. In this paper, designs mean simple designs. It follows that every $i$-subset of points ($i \leq t$) is contained in exactly $\lambda_i = \lambda \binom{v-i}{t-i} / \binom{k-i}{t-i}$ blocks. The number $\lambda_1$ is traditionally denoted by $r$, and the total number of blocks is $b = \lambda_0$. A $t$-design can be represented by its (block-point) incidence matrix $A = (a_{ij})$, where $a_{ij} = 1$ if the $j$th point is contained in the $i$th block and $a_{ij} = 0$ otherwise.

The block intersection numbers of a $t$-$(v, k, \lambda)$ design are the cardinalities of the intersections of any two distinct blocks. A $t$-$(v, k, \lambda)$ design is called self-orthogonal if the block intersection numbers have the same parity as the block size $k$ (see \cite{14}). The term self-orthogonal is due to a natural connection between such designs and self-orthogonal codes. Throughout this paper, we denote the code generated by the rows of an incidence matrix of $D$ by $C(D)$. If $D$ is a self-orthogonal $t$-$(v, k, \lambda)$ design with $k$ even, then $C(D)$ is a self-orthogonal code.

Let $D$ be a $t$-$(v, k, \lambda)$ design. Let $v \in C(D)^\perp$ be a vector of weight $w > 0.$
Denote by \( n_i \) the number of rows of an incidence matrix of \( D \) intersecting exactly \( i \) positions of the support of \( v \) in ones. Then we have the system of equations:

\[
\min\{k,w\} \sum_{i=0}^{\min\{k,w\}} \binom{i}{j} n_i = \lambda_j \binom{w}{j} \quad (j = 0, 1, \ldots, t).
\]

These fundamental equations, which are sometimes called Mendelsohn equations \([12]\) (see also \([14]\)), are the powerful tool in the study of this paper. We note that \( n_i = 0 \) if \( i \) is odd, \( i > k \) or \( i > w \).

The following lemma follows immediately.

**Lemma 4.** Let \( D \) be a self-orthogonal \( t-(v,k,\lambda) \) design with \( k \equiv 0 \pmod{4} \).

(i) If the system of equations (1) has no solution \((n_0,n_2,\ldots)\) consisting of nonnegative integers for some \( w \), then \( C(D)^\perp \) contains no vector of weight \( w \).

(ii) If the system of equations (1) has no solution \((n_0,n_2,\ldots)\) consisting of nonnegative integers for each \( w \) with \( 0 < w < v \), \( w \not\equiv 0 \pmod{4} \), then \( C(D) \) is doubly even self-dual.

The complementary design \( \overline{D} \) of a design \( D \) is obtained by replacing each block of \( D \) by its complement. The following lemma is used in Section 4 to show that \( C(D_{24m,4k}) = C(D_{24m,24m-4k}) \) for \( m \in \{1, \ldots, 6\} \) and \( k \in \{m+1, \ldots, 3m-1\} \).

**Lemma 5.** Let \( D \) be a self-orthogonal \( t-(v,k,\lambda) \) design with \( k \) even. Suppose that \( C(D) \) is self-dual. Then \( C(D) = C(\overline{D}) \) if \( 1 \in C(\overline{D}) \), and \( C(\overline{D}) \subset C(D) \) with \( |C(D) : C(\overline{D})| = 2 \) otherwise.

**Proof.** Since \( C(D) \) is self-dual, \( 1 \in C(D) \). It turns out that \( C(\overline{D}) \subset C(D) \) and \( \langle C(\overline{D}), 1 \rangle = C(D) \). The result follows.

### 3 On the self-duality

In this section, we describe how to determine the self-duality given in the second column of Table 1 for the cases denoted by \(*\) in Table 1. For the other cases, the self-duality is determined by Lemma 4(ii) only.
Proposition 6. The codes $C(D_{72,28})$, $C(D_{96,48})$, $C(D_{120,60})$ and $C(D_{120,52})$ are self-dual.

Proof. All cases are similar, and we only give the details for $C(D_{72,28})$.

Note that $D_{72,28}$ has the following parameters:

\[
\lambda_0 = 4397342400, \lambda_1 = 1710077600, \lambda_2 = 650311200,
\lambda_3 = 241544160, \lambda_4 = 87516000, \lambda_5 = 30888000.
\]

Let $v \in C(D_{72,28})^\perp$ be a vector of weight $w > 0$. For each $w$ of the cases with $w \equiv 1 \pmod{2}$ and $w \leq 8$, the system of equations \((1)\) has no solution. In addition, for $w = 10$, \((1)\) has the following unique solution:

\[
\begin{align*}
n_0 &= 41076475, n_2 = 1096595775, n_4 = 2375199750, \\
n_6 &= 834337350, n_8 = 50284575, n_{10} = -151525.
\end{align*}
\]

Hence, there is no vector of weights $2, 4, 6, 8, 10$ in $C(D_{72,28})^\perp$. The number $\lambda_0$ of blocks satisfies that $2^{32} < \lambda_0 < 2^{33}$. Therefore, $C(D_{72,28})^\perp$ is an even code such that the minimum weight is at least 12 and the dimension is at most 39.

Let $D_{72}$ be a doubly even code of length 72 satisfying the conditions that $D_{72}$ has dimension $\ell \in \{33, 34, 35, 36\}$, both $D_{72}$ and $D_{72}^\perp$ have minimum weights at least 12 and $1 \in D_{72}$. We denote the weight enumerators of $D_{72}$ and $D_{72}^\perp$ by $W_{D_{72}}$ and $W_{D_{72}^\perp}$, respectively. In this case, $W_{D_{72}}$ can be written as:

\[
x^{72} + ax^{60}y^{12} + bx^{56}y^{16} + cx^{52}y^{20} + dx^{48}y^{24} + ex^{44}y^{28} + fx^{40}y^{32} + (2^\ell - 2 - 2a - 2b - 2c - 2d - 2e - 2f)x^{36}y^{36} + \cdots + y^{72},
\]

using nonnegative integers $a, b, c, d, e, f$. Set $W_{D_{72}^\perp} = \sum_{i=0}^{72} B_i x^{72-i} y^i$. By the MacWilliams identity, we have:

\[
\begin{align*}
2^\ell B_2 &= 2^\ell (\chi_{2,\ell} + 36a + 25b + 16c + 9d + 4e + f), \\
2^\ell B_4 &= 2^\ell (\chi_{4,\ell} + 5640a + 2450b + 800c + 114d + 56e - 30f), \\
2^\ell B_6 &= 2^\ell (\chi_{6,\ell} + 313060a + 77385b + 8976c - 1223d + 196e + 433f), \\
2^\ell B_8 &= 2^\ell (\chi_{8,\ell} + 7582080a + 811360b - 43520c - 5280d + 1408e - 4000f), \\
2^\ell B_{10} &= 2^\ell (\chi_{10,\ell} + 86892960a + 887656b - 372096c + 100584d - 17248e + 26536f),
\end{align*}
\]
where \((\chi_{2i,33}, \chi_{2i,34}, \chi_{2i,35})\) are as follows:

\[
(-4831838127, -9663676335, -19327352751),
(84557200770, 169114369410, 338228706690),
(-958309695231, -1916624273151, -3833253428991),
(790649297760, 15812564565600, 31624755101280),
(-50582253079512, -101181262793688, -202379282222040),
\]

for \(i = 1, 2, 3, 4, 5\), respectively.

The assumptions \(B_{2i} = 0\) \((i = 1, 2, 3, 4, 5)\) yield the following:

\[
\begin{align*}
\mathbf{b} &= \alpha \ell - 12a, \\
\mathbf{c} &= \beta \ell + 66a, \\
\mathbf{d} &= \gamma \ell - 220a, \\
\mathbf{e} &= \delta \ell + 495a, \\
\mathbf{f} &= \varepsilon \ell - 792a,
\end{align*}
\]

where

\[
(\alpha \ell, \beta \ell, \gamma \ell, \delta \ell, \varepsilon \ell) = (30105, 2273040, 57830955, 549766080, 2075173947),
(61497, 4534992, 115706955, 1099419840, 4150537083),
(124281, 9058896, 231458955, 2198727360, 8301263355),
\]

for \(\ell = 33, 34, 35\), respectively. For \(\ell = 33, 34, 35\), it follows from \(b \geq 0\) that

\[
e = \delta \ell + 495a \leq \delta \ell + \frac{165}{4}\alpha \ell < 4397342400 = \lambda_0.
\]

Since \(C(D_{72,28})\) contains at least \(4397342400\) codewords of weight 28, we obtain a contradiction. Therefore, \(C(D_{72,28})\) must be self-dual. \(\square\)

**Proposition 7.** The codes \(C(D_{120,36}), C(D_{120,40}), C(D_{120,44}), C(D_{120,48})\) and \(C(D_{144,56})\) are self-dual.

**Proof.** All cases are similar, and we only give the details for \(C(D_{120,40})\).

Note that \(D_{120,40}\) has the following parameters:

\[
\lambda_0 = 397450513031544, \lambda_1 = 132483504343848, \lambda_2 = 43418963608488, \\
\lambda_3 = 13982378111208, \lambda_4 = 4421777693288, \lambda_5 = 1372275835848.
\]

Let \(v \in C(D_{120,40})^\perp\) be a vector of weight \(w > 0\). For each \(w\) of the cases with \(w \equiv 1\) (mod 2) and \(w \leq 8\), the system of equations has no solution. The number \(\lambda_0\) of blocks satisfies that \(2^{48} < \lambda_0 < 2^{49}\). Hence, \(C(D_{120,40})^\perp\) is
an even code such that the minimum weight is at least 10 and the dimension is at most 71.

Let $D_{120}$ be a doubly even code of length 120 satisfying the conditions that $D_{120}$ has dimension $\ell \in \{49, \ldots , 60\}$, $D_{120}$ has minimum weight at least 12, $D_{120}^\perp$ has minimum weight at least 10 and $1 \in D_{120}$. We show that $\ell \neq 49, 50, \ldots , 59$ in the following two steps.

The first step shows that $\ell \neq 49, \ldots , 58$. The approach is similar to that given in Proposition 6. Suppose that $\ell \in \{49, \ldots , 58\}$. Then, by considering the possible weight enumerators of $D_{120}$ and $D_{120}^\perp$, one can obtain a contradiction for each $\ell$. Since the situation is more complicated than that for $C(D_{72,28})$ considered in Proposition 6, we omit the details to save space.

We remark that this argument does not work to show that $\ell \neq 59$.

The second step shows that $\ell \neq 59$. The approach is to consider singly even self-dual codes containing $D_{120}$. Suppose that $\ell = 59$. Since $D_{120}$ contains $1$, there are three self-dual codes lying between $D_{120}^\perp$ and $D_{120}$, one of which is singly even and the others are doubly even (see [11]). We denote the singly even code by $C_{120}$, noting that $D_{120}$ is the subcode $(C_{120})_0$ consisting of codewords of weight $\equiv 0 \pmod{4}$ of $C_{120}$. Let $S_{120}$ be the shadow of $C_{120}$. Since the weight of a vector in $S_{120}$ is divisible by four [3] and $D_{120}^\perp$ has minimum weight at least 10, $C_{120}$ and $S_{120}$ have minimum weights at least 10 and 12, respectively. Using [3] (10) and (11), from the condition on the minimum weights, one can determine the possible weight enumerators $\sum_{i=0}^{120} A_i x^{120-i} y^i$ and $\sum_{i=0}^{120} B_i x^{120-i} y^i$ of $C_{120}$ and $S_{120}$, respectively. In this case, the possible weight enumerators can be written using integers $a, b, c, d, e, f, g, h$.

We investigate the number of codewords of weight 40. In this case, we have that

$$A_{40} = 198725556937080 + 32980992a - 28160b - 15504c + 4896d + 161525e - 599494f - 4385880g + 91345008h.$$  

Using the mathematical software MATHEMATICA, we have verified that $A_{2i} \geq 0 \ (i = 5, \ldots , 16)$ and $B_{4i} \geq 0 \ (i = 3, \ldots , 9)$ yield

$$A_{40} < 397450513031544 = \lambda_0,$$

where $A_{2i} \ (i = 5, \ldots , 16)$ and $B_{4i} \ (i = 3, \ldots , 9)$ are listed in Tables 2 and 3, respectively. Since $C(D_{120,40})$ contains at least 397450513031544 codewords of weight 40, we obtain a contradiction. Therefore, $C(D_{120,40})$ must be self-dual. This completes the proof. 

\[\Box\]
Table 2: Weight enumerator of $C_{120}$

| $i$ | $A_i$ |
|-----|-------|
| 10  | $h$   |
| 12  | $g+30h$ |
| 14  | $f+24g+425h$ |
| 16  | $e+18f+264g+3760h$ |
| 18  | $d+12e+139f+1736g+23100h$ |
| 20  | $c+6d+50e+564f+7380g+103256h$ |
| 22  | $64b-3d+28c+1009f+19800g+339180h+26391755$ |
| 24  | $4096a-384b-20c-88d-441e-1218f+25080g+789840h$ |
| 26  | $265912320-49152a-64b-102d-128e-10717f-35640g+1096410h$ |
| 28  | $2968094880+221184a+4864b+190c+564d+364e-20424f-238590g-118980h$ |
| 30  | $2955945744-31296a-6720b+1210d+7600e+763f-473880g-4961862h$ |
| 32  | $23825963105-946176a-25984b-1140c-1944d+9971e+103766f-182952g-13088880h$ |

Table 3: Weight enumerator of $S_{120}$

| $i$ | $B_i$ |
|-----|-------|
| 12  | $a$   |
| 16  | $17250-24a-b$ |
| 20  | $-315744+276a+22b+c$ |
| 24  | $42581630-2024a-231b-20c-64d$ |
| 28  | $6084129120+10626a+15406+190c+1152d+4096e$ |
| 32  | $473718702550-42504a-7315b-1140c-9792d-65536e-62144f$ |
| 36  | $18824260734240+1345906a+26334b+4845c+52224d+491520e+3670016f+16777216g$ |

Remark 8. If $C(D_{144,72}^\perp)$ has minimum weight at least 10, then one can show that $C(D_{144,72})$ is self-dual by an argument similar to that described in above.

For $m \in \{1, \ldots, 6\}$ and $k \in \{m+1, \ldots, 3m-1\}$, the self-duality of $C(D_{24m,4k})$ has been verified above. As a consequence, we have the following:

Proposition 9. If $m \in \{1, \ldots, 6\}$ and $k \in \{m+1, \ldots, 3m-1\}$, then $C(D_{24m,4k}) = C(D_{24m,24m-4k})$.

Proof. It is trivial that $D_{24m,24m-4k} = \overline{D_{24m,4k}}$. For $m \in \{1, \ldots, 6\}$ and $k \in \{m+1, \ldots, 3m-1\}$, the codes $C(D_{24m,4k})$ are self-dual (see Table 1).

For $(24m, 4k) \in \{(72, 16), (72, 32), (120, 32), (144, 32), (144, 64)\}$, since the 5-design $\overline{D_{24m,4k}}$ has odd $r$, $1 \in C(\overline{D_{24m,4k}})$. Consider the remaining cases. The system of equations (11) has no solution $(n_0, n_2, \ldots)$ consisting of non-negative integers for each odd $w$. By Lemma 4 (i), $1 \in C(\overline{D_{24m,4k}})$. The result follows from Lemma 5. □
By the above proposition, for \( m \in \{1, \ldots, 6\} \) and \( k \in \{m+1, \ldots, 3m-1\} \), \( C(D_{24m,4k}) \) and \( C(D_{24m,24m-4k}) \) are self-dual. In addition, \( C(D_{24m,12m}) \) are self-dual for \( m \in \{1, \ldots, 5\} \). This completes the proof of Theorem 2.

4 On the minimum weights

In this section, we describe how to determine the minimum weights given in the third column of Table 1 for the cases denoted by * in Table 1. For the other cases, the minimum weights are determined by Lemma 4 (i) only. The result in this section completes the proof of Theorem 1.

4.1 \((24m, 4k) = (72, 24), (72, 32)\)

Suppose that \( 4k \in \{24, 32\} \). Let \( v \in C(D_{72,4k})^\perp \) be a vector of weight \( w > 0 \). For each \( w \in \{4, 8\} \), the system of equations (1) has no solution. From the result in the previous section, \( C(D_{72,4k}) \) is a doubly even self-dual code. By Lemma 4 (i), \( C(D_{72,4k}) \) is a doubly even self-dual code of length 72 and minimum weight at least 12.

By Gleason’s theorem (see [11]), the weight enumerator of a doubly even self-dual code of length \( n \) can be written as:

\[
|n/24| \sum_{i=0}^{n/8-3i} a_i (x^8 + 14x^4y^4 + y^8)^{n/8-3i}(x^4y^4(x^4 - y^4)^4)^i,
\]

using integers \( a_i \). Hence, the weight enumerator of \( C(D_{72,4k}) \) can be written as:

\[
x^{72} + \alpha x^{60}y^{12} + (249849 - 12\alpha)x^{56}y^{16} + (18106704 + 66\alpha)x^{52}y^{20} + (462962955 - 220\alpha)x^{48}y^{24} + (4397342400 + 495\alpha)x^{44}y^{28} + (16602715899 - 792\alpha)x^{40}y^{32} + (25756721120 + 924\alpha)x^{36}y^{36} + \cdots,
\]

using a nonnegative integer \( \alpha \). If \( \alpha > 0 \), then the number of codewords of weight \( 4k = 24 \) (resp. 32) is less than 462962955 (resp. 16602715899), which is the number of blocks of \( D_{72,24} \) (resp. \( D_{72,32} \)). Hence, \( \alpha = 0 \). This means that \( C(D_{72,4k}) \) must be extremal.
\subsection*{4.2 \ (24m, 4k) = (96, 28), (96, 36), (96, 44)}

The numbers of blocks of $\mathcal{D}_{96,28}, \mathcal{D}_{96,36}$ and $\mathcal{D}_{96,44}$ are

\[ 18642839520, 4552866656416 \text{ and } 65727011639520, \]

respectively. If $4k \in \{28, 36, 44\}$, then it follows from (1) that the doubly even self-dual code $C(\mathcal{D}_{96,4k})$ has minimum weight at least 12. The weight enumerator $\sum_{i=0}^{96} A_i x^{96-i} y^i$ of $C(\mathcal{D}_{96,4k})$ can be written using integers $\alpha, \beta$, where $A_i$ are listed in Table 4. If there is an integer $i \in \{12, 16\}$ with $A_i > 0$, then

\[ A_{36} = 4552866656416 - 4368A_{12} - 192412A_{16} < 4552866656416, \]

which is the number of the blocks of $\mathcal{D}_{96,36}$. This gives a contradiction. Hence, $A_{12} = A_{16} = 0$, then $\alpha = \beta = 0$. This means that $C(\mathcal{D}_{96,36})$ is extremal. Similarly, one can easily show that $C(\mathcal{D}_{96,44})$ is extremal, and that $C(\mathcal{D}_{96,28})$ is extremal if $d(C(\mathcal{D}_{96,28})) \geq 16$.

\begin{table}[h]
\centering
\caption{Weight enumerator of $C(\mathcal{D}_{96,4k})$}
\begin{tabular}{|c|c|}
\hline
$i$ & $A_i$ \\
\hline
12 & $\beta$ \\
16 & $\alpha + 30\beta$ \\
20 & $3217056 - 16\alpha + 153\beta$ \\
24 & $369844880 + 120\alpha - 1712\beta$ \\
28 & $18642839520 - 560\alpha - 3084\beta$ \\
32 & $422069980215 + 1820\alpha + 69576\beta$ \\
36 & $4552866656416 - 4368\alpha - 323452\beta$ \\
40 & $24292689565680 + 8008\alpha + 842544\beta$ \\
44 & $65727011639520 - 11440\alpha - 1443090\beta$ \\
48 & $91447669224080 + 12870\alpha + 1718068\beta$ \\
\hline
\end{tabular}
\end{table}

\subsection*{4.3 \ (24m, 4k) = (120, 32), (120, 40), (120, 48), (120, 56)}

The numbers of blocks of $\mathcal{D}_{120,32}, \mathcal{D}_{120,40}, \mathcal{D}_{120,48}$ and $\mathcal{D}_{120,56}$ are

\[ 475644139425, 397450513031544, 30531599026535880 \text{ and } 257257766776517715, \]
respectively. If $4k \in \{32, 40, 48, 56\}$, then it follows from (11) that the doubly even self-dual code $C(D_{120, 4k})$ has minimum weight at least 12. The weight enumerator $W_{120, 12} = \sum_{i=0}^{120} A_i x^{120-i} y^i$ of $C(D_{120, 4k})$ can be written using integers $\alpha, \beta, \gamma$, where $A_i$ are listed in Table 5. If there is an integer $i \in \{12, 16, 20\}$ with $A_i > 0$, then

$$A_{56} = 257257766776517715 - 167960 A_{20} < 257257766776517715,$$

which gives a contradiction. Hence, $A_{12} = A_{16} = A_{20} = 0$, then $\alpha = \beta = \gamma = 0$. This means that $C(D_{120, 56})$ is extremal. Similarly, one can easily show that $C(D_{120, 4k})$ is extremal for $4k = 40, 48$, and that $C(D_{120, 32})$ is extremal if $d(C(D_{120, 32}) \geq 20$.

| $i$ | $A_i$ |
|-----|-------|
| 12  | $\gamma$ |
| 16  | $\beta + 72 \gamma$ |
| 20  | $\alpha + 26 \beta + 2004 \gamma$ |
| 24  | $39703755 - 20 \alpha + 39 \beta + 25272 \gamma$ |
| 28  | $6101289120 + 190 \alpha - 2148 \beta + 100866 \gamma$ |
| 32  | $475644139425 - 1140 \alpha + 4563 \beta - 621288 \gamma$ |
| 36  | $18824510698240 + 4845 \alpha + 71058 \beta - 3973756 \gamma$ |
| 40  | $39745051301544 - 15504 \alpha - 613259 \beta + 18650088 \gamma$ |
| 44  | $4630512363728000 + 38760 \alpha + 2564432 \beta + 37650159 \gamma$ |
| 48  | $30531599026535880 - 77520 \alpha - 7035366 \beta - 434682288 \gamma$ |
| 52  | $11602397631397120 + 1259700 \alpha + 13909076 \beta + 1412322984 \gamma$ |
| 56  | $257257766776517715 - 167960 \alpha - 20667530 \beta - 2641019472 \gamma$ |
| 60  | $335200280030755776 + 184756 \alpha + 23538216 \beta + 3223090716 \gamma$ |

**Table 5: Weight enumerator of $C(D_{120, 4k})$**

**4.4** $(24m, 4k) = (144, 36), (144, 52), (144, 60), (144, 68)$

The numbers of blocks of $D_{144, 36}, D_{144, 52}, D_{144, 60}$ and $D_{144, 68}$ are

9542972508784, 4686006803807297232,

170473729066542803616 and 1005386522059285093728,
respectively. If $4k \in \{36, 52, 60, 68\}$, then it follows from (11) that the doubly even self-dual code $C(D_{144,4k})$ has minimum weight at least 12. The weight enumerator $W_{144,12} = \sum_{i=0}^{4k} A_i x^{144-i} y^i$ of $C(D_{144,4k})$ can be written using integers $\alpha, \beta, \gamma, \delta$, where $A_i$ are listed in Table 6. If there is an integer $i \in \{12, 16, 20, 24\}$ with $A_i > 0$, then

$$A_{68} = 1005386522059285093728 - 1215686694585 A_{12} - 16397532256 A_{16} - 246582076 A_{20} - 2496144 A_{24}$$

$$< 1005386522059285093728,$$

which gives a contradiction. Hence, $A_{12} = A_{16} = A_{20} = A_{24} = 0$, then $\alpha = \beta = \gamma = \delta = 0$. This means that $C(D_{144,68})$ is extremal. Similarly, one can easily show that $C(D_{144,4k})$ is extremal if $d(C(D_{144,52})) \geq 20$, and that $C(D_{144,36})$ is extremal if $d(C(D_{144,36})) \geq 24$.

Table 6: Weight enumerator of $C(D_{144,4k})$

| $i$  | $A_i$                                      |
|------|-------------------------------------------|
| 12   | $\gamma + 1145\delta$                    |
| 16   | $\beta + 68\gamma + 5619\delta$          |
| 20   | $\alpha + 22\beta + 1722\gamma + 154820\delta$ |
| 24   | $481008528 - 24\alpha - 59\beta + 17684\gamma + 2550861\delta$ |
| 28   | $9018480421 + 276\alpha - 2152\beta + 11515\gamma + 24260742\delta$ |
| 32   | $9542972508784 - 2024\alpha + 13286\beta - 881064\gamma + 102200559\delta$ |
| 36   | $559456467836112 + 106260\alpha + 39788\beta - 982492\gamma - 215159832\delta$ |
| 40   | $1895022525539376 - 42504\alpha - 861482\beta + 30439192\gamma - 3223863171\delta$ |
| 44   | $381888573368657355 + 1345960\alpha + 5423416\beta - 58206711\gamma + 5681248668\delta$ |
| 48   | $486006803807297232 - 346104\alpha - 21252317\beta - 548108660\gamma + 557748766954\delta$ |
| 52   | $53648745873701148864 + 75471\alpha + 59961226\beta + 3298378982\gamma - 82891353732\delta$ |
| 56   | $170473729066542803616 - 1307504\alpha - 129387017\beta - 110303535684\gamma - 479267780119\delta$ |
| 60   | $517692242416399518331 + 1961256\alpha + 220368688\beta + 24037485819\gamma + 2310638405958\delta$ |
| 64   | $1005386522059285093728 - 246144\alpha - 301497244\beta - 37463473392\gamma - 4857003070893\delta$ |
| 68   | $468600683087297232 - 346104\alpha - 21252317\beta - 548108660\gamma + 557748766954\delta$ |
| 72   | $12537891752121731333280 + 2704156\alpha + 334387688\beta + 43291346040\gamma + 6110981295024\delta$ |

Acknowledgments. The author would like to thank Tsuyoshi Miezaki for verifying the calculations in the proofs of Propositions 6 and 7, independently. This work is supported by JSPS KAKENHI Grant Number 23340021.
References

[1] E.F. Assmus, Jr. and J.D. Key, Designs and Their Codes, Cambridge Tracts in Mathematics, 103. Cambridge University Press, Cambridge, 1992.

[2] E.F. Assmus, Jr. and H.F. Mattson, Jr., New 5-designs, J. Combin. Theory 6 (1969), 122–151.

[3] 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 (1990), 1319–1333.

[4] J. Cruz and W. Willems, 5-designs related to binary extremal self-dual codes of length $24m$, Theory and applications of finite fields, 75–80, Contemp. Math., 579, Amer. Math. Soc., Providence, RI, 2012.

[5] S.T. Dougherty, private communication, July 2005.

[6] M. Harada, Remark on a 5-design related to a putative extremal doubly-even self-dual [96, 48, 20] code, Des. Codes Cryptogr. 37 (2005), 355–358.

[7] M. Harada, M. Kitazume and A. Munemasa, On a 5-design related to an extremal doubly even self-dual code of length 72, J. Combin. Theory Ser. A 107 (2004), 143–146.

[8] M. Harada, T. Miezaki and A. Munemasa, On $t$-designs supported by self-orthogonal codes, (in preparation).

[9] M. Harada, A. Munemasa and V.D. Tonchev, A characterization of designs related to an extremal doubly-even self-dual code of length 48, Ann. Comb. 5 (2005), 189–198.

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

[11] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, Good self dual codes exist, Discrete Math. 3 (1972), 153–162.

[12] N.S. Mendelsohn, Intersection numbers of $t$-designs, In: Studies in Pure Mathematics (presented to Richard Rado), Academic Press, London, 1971, 145–150.
[13] N.J.A. Sloane, Is there a $(72,36)$ $d = 16$ self-dual code? *IEEE Trans. Inform. Theory* **19** (1973), 251.

[14] V.D. Tonchev, A characterization of designs related to the Witt system $S(5,8,24)$, *Math. Z.* **191** (1986), 225–230.