

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

Masaaki Harada*

March 18, 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 $m \in \{1, \dots, 6\}$, $k \in \{m + 1, \dots, 5m - 1\}$ 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

*Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan. email: mharada@m.tohoku.ac.jp. This work was partially carried out at Yamagata University.

n is bounded above by $d(C) \leq 4\lfloor n/24 \rfloor + 4$ [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 [13].

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 $\mathcal{D}$ is a self-orthogonal t -(v, k, λ) design with k even, then the code $C(\mathcal{D})$, which is generated by the rows of an incidence matrix of $\mathcal{D}$, is a self-orthogonal code. By the Assmus and Mattson theorem [2], the supports of the codewords of weight $4k$ ($\neq 0, 24m$) 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-($24m, 4k, \lambda_{24m,4k}$). Then, throughout this paper, we denote any self-orthogonal 5-($24m, 4k, \lambda_{24m,4k}$) design by $\mathcal{D}_{24m,4k}$. That is, $\mathcal{D}_{24m,4k}$ 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 $C(\mathcal{D}_{24m,4k})$ always an extremal doubly even self-dual code?

It is well known that $C(\mathcal{D}_{24,8})$ is the extended Golay code (see [1, Theorem 8.6.2]). It was shown that $C(\mathcal{D}_{24m,4m+4})$ ($m = 2, 3, 4$) 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-($24m, 4k, \lambda_{24m,4k}$) design, where $(4k, \lambda_{24m,4k}) = (8, 1), (12, 8), (16, 78)$ and $(20, 816)$, respectively. The powerful tool which is used in [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] is also similar to that in [7, 9] except that Gleason's theorem (see [10]) is employed to obtain stronger consequences.

In this paper, we study self-orthogonal 5-designs $C(\mathcal{D}_{24m,4k})$ for $k \in \{m+2, \dots, 5m-1\}$, which are related to codewords of weight other than the minimum weight. More precisely, we consider a problem whether $C(\mathcal{D}_{24m,4k})$ is an extremal doubly even self-dual code or not for $m \in \{1, \dots, 6\}$ and $k \in \{m+2, \dots, 5m-1\}$. In addition to the above approach done in [6, 7, 9], it is useful in this paper to observe weight enumerators of $C(\mathcal{D}_{24m,4k})$ and its dual codes, and singly even self-dual codes containing $C(\mathcal{D}_{24m,4k})$ and their

shadows. As a summary, in Table 1¹, we list some partial answers to the above problem for $m \in \{1, \dots, 6\}$ and $k \in \{m+1, \dots, 3m\}$. 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 $m \in \{1, \dots, 6\}$ and $k \in \{m+1, \dots, 3m-1\}$ (Proposition 9).

The main results of this paper are the following theorems.

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

$$\begin{aligned} &(72, 24, 1406405), (72, 32, 238957796), \\ &(96, 36, 28080500448), (96, 44, 1167789832440), \\ &(120, 56, 5156299310025435), (144, 68, 21788133027489299328). \end{aligned}$$

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 $m \in \{1, \dots, 6\}$ and $k \in \{m+1, \dots, 5m-1\}$. 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

¹See Sections 3 and 4 for the marks * in Table 1.

Table 1: Codes $C(\mathcal{D}_{24m,4k})$ ($m = 1, \dots, 6$, $k = m + 1, \dots, 3m$)

Parameters of $\mathcal{D}_{24m,4k}$	Self-dual	Extremal	Ref.
(24, 8, 1)	Yes	Yes	(see [1])
(24, 12, 48)	Yes	Yes	[14]
(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	[5]
(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, 261513764460)	Yes	12, 16, 20	[5]
(96, 44, 1167789832440)	Yes	Yes*	
(96, 48, 2561776811880)	Yes*	12, 16, 20	
(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, 8205989047403924124)	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 $d(C) \leq 4\lfloor n/24 \rfloor + 4$ [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 [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 [3], in order to provide restrictions on the weight enumerators of singly even self-dual codes (see [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 $\mathbf{1}$. 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 [11]).

2.2 Self-orthogonal designs and Mendelsohn equations

A t -(v, k, λ) design $\mathcal{D}$ 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 λ 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 λ_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, λ) design are the cardinalities of the intersections of any two distinct blocks. 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]). 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 $\mathcal{D}$ by $C(\mathcal{D})$. If $\mathcal{D}$ is a self-orthogonal t -(v, k, λ) design with k even, then $C(\mathcal{D})$ is a self-orthogonal code.

Let $\mathcal{D}$ be a t -(v, k, λ) design. Let $v \in C(\mathcal{D})^\perp$ be a vector of weight $w > 0$.

Denote by n_i the number of rows of an incidence matrix of $\mathcal{D}$ intersecting exactly i positions of the support of v in ones. Then we have the system of equations:

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

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 $\mathcal{D}$ be a self-orthogonal t -(v, k, λ) design with $k \equiv 0 \pmod{4}$.*

- (i) *If the system of equations (1) has no solution $(n_0, n_2, \dots)$ consisting of nonnegative integers for some w , then $C(\mathcal{D})^\perp$ contains no vector of weight w .*
- (ii) *If the system of equations (1) has no solution $(n_0, n_2, \dots)$ consisting of nonnegative integers for each w with $0 < w < v$, $w \not\equiv 0 \pmod{4}$, then $C(\mathcal{D})$ is doubly even self-dual.*

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

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

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

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 $C(\mathcal{D}_{72,28})$, $C(\mathcal{D}_{96,48})$, $C(\mathcal{D}_{120,60})$ and $C(\mathcal{D}_{120,52})$ are self-dual.*

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

Note that $\mathcal{D}_{72,28}$ has the following parameters:

$$\begin{aligned}\lambda_0 &= 4397342400, \lambda_1 = 1710077600, \lambda_2 = 650311200, \\ \lambda_3 &= 241544160, \lambda_4 = 87516000, \lambda_5 = 30888000.\end{aligned}$$

Let $v \in C(\mathcal{D}_{72,28})^\perp$ 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:

$$\begin{aligned}n_0 &= 41076475, n_2 = 1096595775, n_4 = 2375199750, \\ n_6 &= 834337350, n_8 = 50284575, n_{10} = -151525.\end{aligned}$$

Hence, there is no vector of weights 2, 4, 6, 8, 10 in $C(\mathcal{D}_{72,28})^\perp$. The number λ_0 of blocks satisfies that $2^{32} < \lambda_0 < 2^{33}$. Therefore, $C(\mathcal{D}_{72,28})^\perp$ 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 $\mathbf{1} \in D_{72}$. 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:

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

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:

$$\begin{aligned}2^\ell B_2 &= 2^6(\chi_{2,\ell} + 36a + 25b + 16c + 9d + 4e + f), \\ 2^\ell B_4 &= 2^6(\chi_{4,\ell} + 5640a + 2450b + 800c + 114d - 56e - 30f), \\ 2^\ell B_6 &= 2^6(\chi_{6,\ell} + 313060a + 77385b + 8976c - 1223d + 196e + 433f), \\ 2^\ell B_8 &= 2^6(\chi_{8,\ell} + 7582080a + 811360b - 43520c - 5280d + 1408e - 4000f), \\ 2^\ell B_{10} &= 2^6(\chi_{10,\ell} + 86892960a + 887656b - 372096c + 100584d - 17248e \\ &\quad + 26536f),\end{aligned}$$

where $(\chi_{2i,33}, \chi_{2i,34}, \chi_{2i,35})$ are as follows:

$$\begin{aligned} &(-4831838127, -9663676335, -19327352751), \\ &(84557200770, 169114369410, 338228706690), \\ &(-958309695231, -1916624273151, -3833253428991), \\ &(7906469297760, 15812564565600, 31624755101280), \\ &(-50582253079512, -101181262793688, -202379282222040), \end{aligned}$$

for $i = 1, 2, 3, 4, 5$, respectively.

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

$$b = \alpha_\ell - 12a, c = \beta_\ell + 66a, d = \gamma_\ell - 220a, e = \delta_\ell + 495a, f = \varepsilon_\ell - 792a,$$

where

$$\begin{aligned} (\alpha_\ell, \beta_\ell, \gamma_\ell, \delta_\ell, \varepsilon_\ell) = & (30105, 2273040, 57830955, 549766080, 2075173947), \\ & (61497, 4534992, 115706955, 1099419840, 4150537083), \\ & (124281, 9058896, 231458955, 2198727360, 8301263355), \end{aligned}$$

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

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

Proof. All cases are similar, and we only give the details for $C(\mathcal{D}_{120,40})$.

Note that $\mathcal{D}_{120,40}$ has the following parameters:

$$\begin{aligned} \lambda_0 &= 397450513031544, \lambda_1 = 132483504343848, \lambda_2 = 43418963608488, \\ \lambda_3 &= 13982378111208, \lambda_4 = 4421777693288, \lambda_5 = 1372275835848. \end{aligned}$$

Let $v \in C(\mathcal{D}_{120,40})^\perp$ 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. The number λ_0 of blocks satisfies that $2^{48} < \lambda_0 < 2^{49}$. Hence, $C(\mathcal{D}_{120,40})^\perp$ 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 $\ell \in \{49, \dots, 60\}$, D_{120} has minimum weight at least 12, $D_{120}^\perp$ has minimum weight at least 10 and $\mathbf{1} \in D_{120}$. We show that $\ell \neq 49, 50, \dots, 59$ in the following two steps.

The first step shows that $\ell \neq 49, \dots, 58$. The approach is similar to that given in Proposition 6. Suppose that $\ell \in \{49, \dots, 58\}$. Then, by considering the possible weight enumerators of D_{120} and $D_{120}^\perp$, one can obtain a contradiction for each ℓ . Since the situation is more complicated than that for $C(\mathcal{D}_{72,28})$ 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 $\mathbf{1}$, 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

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

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

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

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

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	$64b - 3d + 28e + 1009f + 19800g + 339180h + 26391755$
24	$4096a - 384b - 20c - 88d - 441e - 1218f + 25080g + 789840h$
26	$265912320 - 49152a - 64b - 102d - 1288e - 10717f - 35640g + 1096410h$
28	$2968094880 + 221184a + 4864b + 190c + 564d + 364e - 20424f - 238590g - 118980h$
30	$29559455744 - 311296a - 6720b + 1210d + 7800e + 7631f - 473880g - 4961862h$
32	$238259763105 - 946176a - 25984b - 1140c - 1944d + 9971e + 103766f - 182952g - 13088880h$

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	$6084129120 + 10626a + 1540b + 190c + 1152d + 4096e$
32	$475718702550 - 42504a - 7315b - 1140c - 9792d - 65536e - 262144f$
36	$18824260734240 + 134596a + 26334b + 4845c + 52224d + 491520e + 3670016f + 16777216g$

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

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

Proposition 9. *If $m \in \{1, \dots, 6\}$ and $k \in \{m+1, \dots, 3m-1\}$, then $C(\mathcal{D}_{24m,4k}) = C(\mathcal{D}_{24m,24m-4k})$.*

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

For $(24m, 4k) \in \{(72, 16), (72, 32), (120, 32), (144, 32), (144, 64)\}$, since the 5-design $\overline{\mathcal{D}_{24m,4k}}$ has odd r , $\mathbf{1} \in C(\overline{\mathcal{D}_{24m,4k}})$. Consider the remaining cases. The system of equations (1) has no solution $(n_0, n_2, \dots)$ consisting of non-negative integers for each odd w . By Lemma 4 (i), $\mathbf{1} \in C(\overline{\mathcal{D}_{24m,4k}})$. The result follows from Lemma 5. $\square$

By the above proposition, for $m \in \{1, \dots, 6\}$ and $k \in \{m+1, \dots, 3m-1\}$, $C(\mathcal{D}_{24m,4k})$ and $C(\mathcal{D}_{24m,24m-4k})$ are self-dual. In addition, $C(\mathcal{D}_{24m,12m})$ are self-dual for $m \in \{1, \dots, 5\}$. 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 $v \in C(\mathcal{D}_{72,4k})^\perp$ 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, $C(\mathcal{D}_{72,4k})$ is a doubly even self-dual code. By Lemma 4 (i), $C(\mathcal{D}_{72,4k})$ is a doubly even self-dual code of length 72 and minimum weight at least 12.

By Gleason's theorem (see [10]), the weight enumerator of a doubly even self-dual code of length n can be written as:

$$\sum_{i=0}^{\lfloor n/24 \rfloor} a_i (x^8 + 14x^4y^4 + y^8)^{n/8-3i} (x^4y^4(x^4 - y^4)^4)^i,$$

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

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

using a nonnegative integer α . 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 $\mathcal{D}_{72,24}$ (resp. $\mathcal{D}_{72,32}$). Hence, $\alpha = 0$. This means that $C(\mathcal{D}_{72,4k})$ must be extremal.

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 α, β , 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 $d(C(\mathcal{D}_{96,28})) \geq 16$.

Table 4: Weight enumerator of $C(\mathcal{D}_{96,4k})$

i	A_i
12	β
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	$91447669224080 + 12870\alpha + 1718068\beta$

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 (1) that the doubly even self-dual code $C(\mathcal{D}_{120,4k})$ has minimum weight at least 12. The weight enumerator $W_{120,12} = \sum_{i=0}^{120} A_i x^{120-i} y^i$ of $C(\mathcal{D}_{120,4k})$ can be written using integers α, β, γ , where A_i are listed in Table 5. If there is an integer $i \in \{12, 16, 20\}$ with $A_i > 0$, then

$$\begin{aligned} A_{56} = & 257257766776517715 - 1130786592A_{12} - 16300570A_{16} \\ & - 167960A_{20} < 257257766776517715, \end{aligned}$$

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

Table 5: Weight enumerator of $C(\mathcal{D}_{120,4k})$

i	A_i
12	γ
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	$397450513031544 - 15504\alpha - 613259\beta + 18650088\gamma$
44	$4630512364732800 + 38760\alpha + 2564432\beta + 37650159\gamma$
48	$30531599026535880 - 77520\alpha - 7035366\beta - 434682288\gamma$
52	$116023977311397120 + 125970\alpha + 13909076\beta + 1412322984\gamma$
56	$257257766776517715 - 167960\alpha - 20667530\beta - 2641019472\gamma$
60	$335200280030755776 + 184756\alpha + 23538216\beta + 3223090716\gamma$

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

The numbers of blocks of $\mathcal{D}_{144,36}$, $\mathcal{D}_{144,52}$, $\mathcal{D}_{144,60}$ and $\mathcal{D}_{144,68}$ are

$$\begin{aligned} & 9542972508784, 4686006803807297232, \\ & 170473729066542803616 \text{ and } 1005386522059285093728, \end{aligned}$$

respectively. If $4k \in \{36, 52, 60, 68\}$, then it follows from (1) that the doubly even self-dual code $C(\mathcal{D}_{144,4k})$ has minimum weight at least 12. The weight enumerator $W_{144,12} = \sum_{i=0}^{144} A_i x^{144-i} y^i$ of $C(\mathcal{D}_{144,4k})$ 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

$$\begin{aligned} A_{68} = & 1005386522059285093728 - 1215686694585A_{12} \\ & - 16397532256A_{16} - 246582076A_{20} - 2496144A_{24} \\ < & 1005386522059285093728, \end{aligned}$$

which gives a contradiction. Hence, $A_{12} = A_{16} = A_{20} = A_{24} = 0$, then $\alpha = \beta = \gamma = \delta = 0$. This means that $C(\mathcal{D}_{144,68})$ is extremal. Similarly, one can easily show that $C(\mathcal{D}_{144,60})$ is extremal, that $C(\mathcal{D}_{144,52})$ is extremal if $d(C(\mathcal{D}_{144,52})) \geq 20$, and that $C(\mathcal{D}_{144,36})$ is extremal if $d(C(\mathcal{D}_{144,36})) \geq 24$.

Table 6: Weight enumerator of $C(\mathcal{D}_{144,4k})$

i	A_i
12	δ
16	$\gamma + 114\delta$
20	$\beta + 68\gamma + 5619\delta$
24	$\alpha + 22\beta + 1722\gamma + 154820\delta$
28	$481008528 - 24\alpha - 59\beta + 17684\gamma + 2550861\delta$
32	$90184804281 + 276\alpha - 2152\beta + 11515\gamma + 24260742\delta$
36	$9542972508784 - 2024\alpha + 13286\beta - 881064\gamma + 102200559\delta$
40	$559456467836112 + 10626\alpha + 39788\beta - 982492\gamma - 215159832\delta$
44	$18950225255363376 - 42504\alpha - 861482\beta + 30439192\gamma - 3223863171\delta$
48	$381888573368657355 + 134596\alpha + 5423416\beta - 58206711\gamma + 568124866\delta$
52	$4686006803807297232 - 346104\alpha - 21252317\beta - 458108660\gamma + 55774876695\delta$
56	$35648745873701148864 + 735471\alpha + 59961226\beta + 3298378982\gamma - 82891353732\delta$
60	$170473729066542803616 - 1307504\alpha - 129387017\beta - 11030355684\gamma - 479267780119\delta$
64	$517692242136399518331 + 1961256\alpha + 220368688\beta + 24037485819\gamma + 2310638405958\delta$
68	$1005386522059285093728 - 2496144\alpha - 301497244\beta - 37463473392\gamma - 4857003070893\delta$
72	$1253789175212713133280 + 2704156\alpha + 334387688\beta + 43291346040\gamma + 6110981295024\delta$

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. Miezeki 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.