A note on Assmus–Mattson type theorems

Tsuyoshi Miezaki[1] · Akihiro Munemasa[2] · Hiroyuki Nakasora[3]

Abstract

In the present paper, we give Assmus–Mattson type theorems for codes and lattices. We show that a binary doubly even self-dual code of length $24m$ with minimum weight $4m$ provides a combinatorial 1-design and an even unimodular lattice of rank $24m$ with minimum norm $2m$ provides a spherical 3-design. We remark that some of such codes and lattices give t-designs for higher t. As a corollary, we give some restrictions on the weight enumerators of binary doubly even self-dual codes of length $24m$ with minimum weight $4m$. Ternary and quaternary analogues are also given.

1 Introduction

Let C be a code over $\mathbb{F}_q$ and $C_\ell := \{c \in C \mid \mathrm{wt}(c) = \ell\}$. Let $L \subset \mathbb{R}^n$ be a lattice and $L_\ell := \{x \in L \mid (x, x) = \ell\}$. In this paper, we call C_ℓ (resp. L_ℓ) a shell of the code C (resp. lattice L) whenever it is non-empty.

Shells of extremal self-dual codes are known to support combinatorial designs by the Assmus–Mattson theorem. More precisely, the set $\mathcal{B}(C_\ell) := \{\mathrm{supp}(x) \mid x \in C_\ell\}$ forms the

---

Communicated by V. D. Tonchev.

✉ Tsuyoshi Miezaki
  miezaki@edu.u-ryukyu.ac.jp

  Akihiro Munemasa
  munemasa@math.is.tohoku.ac.jp

  Hiroyuki Nakasora
  nakasora@ge.kobegakuin.ac.jp

[1] Faculty of Education, University of the Ryukyus, Okinawa 903–0213, Japan

[2] Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan

[3] Institute for Promotion of Higher Education, Kobe Gakuin University, Kobe 651–2180, Japan

set of blocks of a combinatorial design. Note that $\mathcal{B}(C_\ell)$ is not a multiset, so combinatorial designs in this papers are always without repeated blocks. Similarly, shells of extremal even unimodular lattices are known to give spherical designs by a theorem of Venkov. In the present paper, we give analogues of these theorems with relaxed assumptions; the minimum weight of a self-dual code is allowed to be slightly smaller than the extremal case, the minimum norm of an even unimodular lattice is allowed to be smaller by 2 than the extremal case. The conclusions we obtain are necessarily weaker than the extremal cases, but still they are nontrivial, and give a restriction on weight enumerators for the binary case.

To explain our results, we review some results on codes and lattices. Let C be a binary doubly even self-dual code of length n. Then we have the following bound on the minimum weight of C [21]:

$$\min(C) \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4. \tag{1.1}$$

We say that C meeting the bound (1.1) with equality is extremal. Let C be an extremal code of length n. Identifying codewords with their support, C_ℓ forms a combinatorial t-design, where

$$t = \begin{cases} 5 & \text{if } n \equiv 0 \pmod{24}, \\ 3 & \text{if } n \equiv 8 \pmod{24}, \\ 1 & \text{if } n \equiv 16 \pmod{24}, \end{cases}$$

provided $C_\ell \neq \emptyset$ [1]. Ternary and quaternary analogues of this fact were also given in [1]. Let C be a ternary or quaternary self-dual code of length n. Then we have the following bound on the minimum weight of C [19,21]:

$$\min(C) \leq \begin{cases} 3 \left\lfloor \frac{n}{12} \right\rfloor + 3 & \text{if } C \text{ is ternary}, \\ 2 \left\lfloor \frac{n}{6} \right\rfloor + 2 & \text{if } C \text{ is quaternary}. \end{cases} \tag{1.2}$$

We say that C meeting the bound (1.2) with equality is extremal. Let C be an extremal code of length n and w be the largest integer satisfying

$$w - \left\lfloor \frac{w + q - 2}{q - 1} \right\rfloor < d.$$

Then for $\ell \leq w$, C_ℓ forms a combinatorial t-design, where

$$t = \begin{cases} 5 & \text{if } n \equiv 0 \pmod{12}, \\ 3 & \text{if } n \equiv 4 \pmod{12}, \\ 1 & \text{if } n \equiv 8 \pmod{12}, \end{cases}$$

if C is ternary, and

$$t = \begin{cases} 5 & \text{if } n \equiv 0 \pmod{6}, \\ 3 & \text{if } n \equiv 2 \pmod{6}, \\ 1 & \text{if } n \equiv 4 \pmod{6}, \end{cases}$$

if C is quaternary, provided $C_\ell \neq \emptyset$ [1].

Let L be an even unimodular lattices of rank n. Then we have the following bound on the minimum norm of L [20]:

$$\min(L) \leq 2 \left\lfloor \frac{n}{24} \right\rfloor + 2. \tag{1.3}$$

We say that L meeting the bound (1.3) with equality is extremal. Let L be an extremal lattice of length n. After normalization, L_ℓ forms a spherical t-design, where

$$t = \begin{cases} 11 & \text{if } n \equiv 0 \pmod{24}, \\ 7 & \text{if } n \equiv 8 \pmod{24}, \\ 3 & \text{if } n \equiv 16 \pmod{24}, \end{cases}$$

provided $L_\ell \neq \emptyset$ [27,28] (see also [24]).

The main results of the present paper is to give an analogue of these results for non-extremal codes and lattices, as follows:

Theorem 1.1 (1) *Let C be a binary doubly even self-dual code of length $24m$ with minimum weight $4m$. Then every shell of C is a combinatorial 1-design.*

(2) *Let C be a ternary self-dual code of length $12m$ with minimum weight $3m$. Then for $\ell \leq 6m - 3$, C_ℓ is a combinatorial 1-design.*

(3) *Let C be a quaternary self-dual code of length $6m$ with minimum weight $2m$. Then for $\ell \leq 3m - 1$, C_ℓ is a combinatorial 1-design.*

(4) *Let L be an even unimodular lattice of rank $24m$ with minimum norm $2m$. Then every shell of L supports a spherical 3-design.*

Remark 1.1 Theorem 1.1 (1) and (4) were firstly obtained by B. Venkov and the second named author using modular forms. We remark that the proof of Theorem 1.1 (1) in the present paper is different from their original proof.

As an application of Theorem 1.1, we give some restrictions on the weight enumerators of self-dual codes.

Corollary 1.2 (1) *Let C be a binary doubly even self-dual code of length $24m$ with minimum weight $4m$. Then the coefficient of $x^{24m-4m}y^{4m}$ in the weight enumerator of C is divisible by 6.*

(2) *Let C be a ternary self-dual code of length $12m$ with minimum weight $3m$. Then the coefficient of $x^{12m-3m}y^{3m}$ in the weight enumerator of C is divisible by 4.*

(3) *Let C be a quaternary self-dual code of length $6m$ with minimum weight $2m$. Then the coefficient of $x^{6m-2m}y^{2m}$ in the weight enumerator of C is divisible by 3.*

The following theorem gives a strengthening of Theorem 1.1 (1) and (4) for some particular cases.

Theorem 1.3 (1) *Let C be a binary doubly even self-dual code of length 96 with minimum weight 16. Then C_{20} (also C_{76}) is a combinatorial 2-design.*

(2) *Let L be an even unimodular lattice of rank 240 with minimum norm 20. Then L_{22} supports a spherical 5-design.*

On the other hand, we give an upper bound on the value t of combinatorial t-designs formed by a shell of a binary doubly even self-dual code of length 96 with minimum weight 16. For convenience, let

$$\mathcal{L} = \{\ell \in \mathbb{Z} \mid 16 \leq \ell \leq 80, \ \ell \equiv 0 \pmod 4\}. \tag{1.4}$$

Theorem 1.4 *Let C be a binary doubly even self-dual code of length 96 with minimum weight 16, and let $\ell \in \mathcal{L}$. Assume that C_ℓ is a combinatorial t-design. Then the following statements hold:*

(1) *If $t = 2$ and $\ell \neq 20, 76$, then every shell of C is a combinatorial 2-design.*
(2) *If $t \geq 3$ and $\ell \neq 20, 48, 76$, then every shell of C is a combinatorial t-design.*
(3) *We have*

$$t \leq \begin{cases} 7 & \textit{if } \ell = 48, \\ 5 & \textit{if } \ell = 20, 76. \\ 4 & \textit{otherwise.} \end{cases}$$

This paper is organized as follows. In Sect. 2, we give definitions and some basic properties of self-dual codes, unimodular lattices, combinatorial t-designs and spherical t-designs used in this paper. In Sects. 3 and 4, we give proofs of Theorem 1.1 and 1.3, respectively. In Sect. 5, we give a proof of Theorem 1.4, give the known examples of binary doubly even self-dual codes of length 96 with minimum weight 16 and investigate their designs. Finally, in Sect. 6, we give concluding remarks.

All computer calculations in this paper were done with the help of Magma [5] and Mathematica [29].

2 Preliminaries

2.1 Codes and combinatorial *t*-designs

A linear code C of length n is a linear subspace of $\mathbb{F}_q^n$. For $q = 2$ and $q = 3$, an inner product (x, y) on $\mathbb{F}_q^n$ is given by

$$(x, y) = \sum_{i=1}^{n} x_i y_i,$$

where $x, y \in \mathbb{F}_q^n$ with $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$. The Hermitian inner product $(x, y)_H$ on $\mathbb{F}_4^n$ is given by

$$(x, y)_H = \sum_{i=1}^{n} x_i y_i^2,$$

where $x, y \in \mathbb{F}_4^n$ with $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$. The dual of a linear code C is defined as follows: for $q = 2$ and $q = 3$,

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

for $q = 4$,

$$C^{\perp, H} = \{y \in \mathbb{F}_q^n \mid (x, y)_H = 0 \text{ for all } x \in C\}.$$

A linear code C is called self-dual if $C = C^\perp$ for $q = 2$ and $q = 3$ and if $C = C^{\perp, H}$ for $q = 4$. For $x \in \mathbb{F}_q^n$, the weight $\mathrm{wt}(x)$ is the number of its nonzero components. In this paper, we consider the following self-dual codes [7]:

Doubly even: A code is defined over $\mathbb{F}_2^n$ with all weights divisible by 4,
Ternary: A code is defined over $\mathbb{F}_3^n$ with all weights divisible by 3,
Quaternary: A code is defined over $\mathbb{F}_4^n$ with all weights divisible by 2.

A combinatorial t-design is a pair $\mathcal{D} = (\Omega, \mathcal{B})$, where Ω is a set of points of cardinality v, and $\mathcal{B}$ a collection of k-element subsets of Ω called blocks, with the property that any t points are contained in precisely λ blocks.

The support of a vector $x := (x_1, \ldots, x_n)$, $x_i \in \mathbb{F}_q$ is the set of indices of its nonzero coordinates: $\mathrm{supp}(x) = \{i \mid x_i \neq 0\}$. Let $\Omega := \{1, \ldots, n\}$ and $\mathcal{B}(C_\ell) := \{\mathrm{supp}(x) \mid x \in C_\ell\}$. Then for a code C of length n, we say that C_ℓ is a combinatorial t-design if $(\Omega, \mathcal{B}(C_\ell))$ is a combinatorial t-design.

2.2 Harmonic weight enumerators

In this section, we extend the method of harmonic weight enumerators which were used by Bachoc [2] and Bannai et al. [4]. For the readers convenience we quote from [2,8] the definitions and properties of discrete harmonic functions (for more information the reader is referred to [2,8]).

Let $\Omega = \{1, 2, \ldots, n\}$ be a finite set (which will be the set of coordinates of the code) and let X be the set of its subsets, while, for all $k = 0, 1, \ldots, n$, X_k is the set of its k-subsets. We denote by $\mathbb{R}X$ and $\mathbb{R}X_k$ the real vector spaces spanned by the elements of X and X_k, respectively. An element of $\mathbb{R}X_k$ is denoted by

$$f = \sum_{z \in X_k} f(z)z$$

and is identified with the real-valued function on X_k given by $z \mapsto f(z)$.

An element $f \in \mathbb{R}X_k$ can be extended to an element $\widetilde{f} \in \mathbb{R}X$ by setting, for all $u \in X$,

$$\widetilde{f}(u) = \sum_{z \in X_k, z \subset u} f(z).$$

If an element $g \in \mathbb{R}X$ is equal to $\widetilde{f}$ for some $f \in \mathbb{R}X_k$, then we say that g has degree k. The differentiation γ is the operator defined by linearity from

$$\gamma(z) = \sum_{y \in X_{k-1}, y \subset z} y$$

for all $z \in X_k$ and for all $k = 0, 1, \ldots, n$, and Harm_k is the kernel of γ:

$$\mathrm{Harm}_k = \ker(\gamma|_{\mathbb{R}X_k}).$$

Lemma 2.1 ([8, Theorem 7], [25, Lemma 2.5]) *Let C be a code of length n with minimum weight d. Let w_0 be the largest integer satisfying*

$$w_0 - \left\lfloor \frac{w_0 + q - 2}{q - 1} \right\rfloor < d,$$

where, if $q = 2$, we take $w_0 := n$. Let i be a weight of C such that $d \leq i \leq w_0$. Then the subset of $\{1, 2, \ldots, n\}$ which support codewords of weight i in C form a t-design if and only if

$$\sum_{u \in C, \mathrm{wt}(u) = i} \widetilde{f}(u) = 0,$$

for all $f \in \mathrm{Harm}_k$, $1 \leq k \leq t$.

In [2], the harmonic weight enumerator associated to a linear code C was defined as follows:

Definition 2.2 ([2, Definition 2.1], [3, Definition 4.1]) Let C be a linear code of length n and let $f \in \mathrm{Harm}_k$. The harmonic weight enumerator associated to C and f is

$$W_{C,f}(x, y) = \sum_{c \in C} \widetilde{f}(c) x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)}.$$

Then the submodules of harmonic weight enumerators are described as follows:

Theorem 2.3 ([2, Lemma 3.1], [3, Lemma 6.1 and 6.2]) *Let C be a linear code of length n, and let $f \in \mathrm{Harm}_k$.*

(1) *Suppose C is a binary doubly even self-dual code. Then*

$$W_{C,f}(x, y) \in \begin{cases} (xy)^k \mathbb{C}[P_8, P_{24}] & \text{if } k \equiv 0 \pmod 4, \\ (xy)^k P_{12} \mathbb{C}[P_8, P_{24}] & \text{if } k \equiv 2 \pmod 4, \\ (xy)^k P_{18} \mathbb{C}[P_8, P_{24}] & \text{if } k \equiv 3 \pmod 4, \\ (xy)^k P_{30} \mathbb{C}[P_8, P_{24}] & \text{if } k \equiv 1 \pmod 4, \end{cases}$$

where

$$\begin{aligned} P_8 &= x^8 + 14x^4 y^4 + y^8, \\ P_{12} &= x^2 y^2 (x^4 - y^4)^2, \\ P_{18} &= xy(x^8 - y^8)(x^8 - 34x^4 y^4 + y^8), \\ P_{24} &= P_{12}^2, \\ P_{30} &= P_{12} P_{18}. \end{aligned}$$

(2) *Suppose C is a ternary self-dual code. Then*

$$W_{C,f} \in \begin{cases} xy p_{14} \mathbb{C}[g_4, g_{12}], & \text{if } k = 1, \\ (xy)^2 p_4 \mathbb{C}[g_4, g_{12}], & \text{if } k = 2, \end{cases}$$

where

$$\begin{aligned} p_4 &= y(x^3 - y^3), \\ p_{14} &= y^2 (x^3 - y^3)^2 (x^6 - 20x^3 y^3 - 8y^6), \\ g_4 &= x^4 + 8xy^3, \\ g_{12} &= y^3 (x^3 - y^3)^3. \end{aligned}$$

(3) *Suppose C is a quaternary self-dual code. Then*

$$W_{C,f} \in \begin{cases} xy q_6 \mathbb{C}[h_2, h_6], & \text{if } k = 1, \\ (xy)^2 \mathbb{C}[h_2, h_6], & \text{if } k = 2, \end{cases}$$

where

$$\begin{aligned} h_2 &= x^2 + 3y^2, \\ h_6 &= y^2 (x^2 - y^2)^2, \\ q_6 &= y(x^2 - y^2)(x^3 - 9xy^2). \end{aligned}$$

Remark 2.4 In [2, Lemma 3.1] and [3, Lemma 6.1 and 6.2], explicit sets of generators of the submodules for general k were given. We omit listing them here, since we do not need them.

2.3 Lattices and spherical t-designs

A lattice in $\mathbb{R}^n$ is a subgroup $L \subset \mathbb{R}^n$ with the property that there exists a basis $\{e_1, \ldots, e_n\}$ of $\mathbb{R}^n$ such that $L = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$. The dual lattice of L is the lattice

$$L^{\sharp} := \{y \in \mathbb{R}^n \mid (y, x) \in \mathbb{Z}, \ \forall x \in L\},$$

where (x, y) is the standard inner product. In this paper, we assume that the lattice L is integral, that is, $(x, y) \in \mathbb{Z}$ for all $x, y \in L$. An integral lattice L is called even if $(x, x) \in 2\mathbb{Z}$ for all $x \in L$. An integral lattice L is called unimodular if $L^{\sharp} = L$.

The concept of a spherical t-design is due to Delsarte–Goethals–Seidel [9]. For a positive integer t, a finite nonempty set X in the unit sphere

$$S^{n-1} = \{x = (x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_1^2 + \cdots + x_n^2 = 1\}$$

is called a spherical t-design in S^{n-1} if the following condition is satisfied:

$$\frac{1}{|X|} \sum_{x \in X} f(x) = \frac{1}{|S^{n-1}|} \int_{S^{n-1}} f(x) d\sigma(x),$$

for all polynomials $f(x) = f(x_1, \ldots, x_n)$ of degree not exceeding t. A finite subset X in $S^{n-1}(r)$, the sphere of radius r centered at the origin, is also called a spherical t-design if $(1/r)X$ is a spherical t-design in the unit sphere S^{n-1}. Then we say that L_ℓ is a spherical t-design if $(1/\sqrt{\ell})L_\ell$ is a spherical t-design.

Let $\mathrm{Harm}_j(\mathbb{R}^n)$ denote the set of homogeneous harmonic polynomials of degree j:

$$\mathrm{Harm}_j(\mathbb{R}^n) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid \deg(f) = j \text{ and } \sum_{i=1}^{n} \frac{\partial^2}{\partial^2 x_i} f = 0\}.$$

It is well known that X is a spherical t-design if and only if the condition

$$\sum_{x \in X} P(x) = 0$$

holds for all $P \in \mathrm{Harm}_j(\mathbb{R}^n)$ with $1 \le j \le t$. If the set X is antipodal, that is $-X = X$, and j is odd, then the above condition is fulfilled automatically. So we reformulate the condition of spherical t-design for antipodal sets as follows:

Proposition 2.5 *A nonempty finite antipodal subset $X \subset S_m^{n-1}$ is a spherical $(2s+1)$-design if and only if the condition*

$$\sum_{x \in X} P(x) = 0$$

holds for all $P \in \mathrm{Harm}_{2j}(\mathbb{R}^n)$ with $1 \le j \le s$.

2.4 Spherical theta series

Let $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ be the upper half-plane.

Definition 2.6 Let L be an integral lattice in $\mathbb{R}^n$. For a polynomial P, the function on $\mathbb{H}$ defined by

$$\vartheta_{L,P}(z) := \sum_{x \in L} P(x) e^{\pi i z (x,x)}$$

is called the theta series of L weighted by P.

Remark 2.7 (i) When $P = 1$, we get the classical theta series

$$\vartheta_L(z) = \vartheta_{L,1}(z) = \sum_{m \geq 0} |L_m| q^m, \quad \text{where } q = e^{\pi i z}.$$

(ii) The weighted theta series can be written as

$$\vartheta_{L,P}(z) = \sum_{m \geq 0} a_m^{(P)} q^m, \text{ where } a_m^{(P)} := \sum_{x \in L_m} P(x). \tag{2.1}$$

Lemma 2.8 ([24, Lemma 5],[27,28]) *Let L be an integral lattice in $\mathbb{R}^n$. Then, for $m > 0$, the non-empty shell L_m is a spherical $(2s + 1)$-design if and only if*

$$a_m^{(P)} = 0 \text{ for every } P \in \text{Harm}_{2j}(\mathbb{R}^n) \text{ and } 1 \leq j \leq s,$$

where $a_m^{(P)}$ is the Fourier coefficient of the weighted theta series (2.1).

For example, we consider an even unimodular lattice L. Then the weighted theta series $\vartheta_{L,P}(z)$ of L weighted by a harmonic polynomial P, is a modular form with respect to $SL_2(\mathbb{Z})$. In general, we have the following:

Lemma 2.9 ([24, Theorem 12, Proposition 16]) *Let $L \subset \mathbb{R}^n$ be an even unimodular lattice of of rank $n = 8N$ and of minimum norm $2M$. Let*

$$E_4(z) := 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n},$$

$$E_6(z) := 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^{2n},$$

$$\Delta(z) := \frac{E_4(z)^3 - E_6(z)^2}{1728}$$
$$= q^2 - 24q^4 + \cdots,$$

where $\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$, and $q = e^{\pi i z}$. Then we have for $P \in \text{Harm}_{2j}(\mathbb{R}_n)$,

$$\vartheta_{L,P} \in \begin{cases} \mathbb{C}[E_4, \Delta] & \text{if } j \text{ is even,} \\ E_6 \mathbb{C}[E_4, \Delta] & \text{if } j \text{ is odd.} \end{cases}$$

More precisely, there exist $c_i \in \mathbb{C}$ such that

$$\vartheta_{L,P} = \begin{cases} \displaystyle\sum_{i=M}^{[(N+j/2)/3]} c_i \Delta^i E_4^{N+j/2-3i} & \text{if } j \text{ is even,} \\ \displaystyle\sum_{i=M}^{[(N+j/2)/3]} c_i E_6 \Delta^i E_4^{N+(j-3)/2-3i} & \text{if } j \text{ is odd.} \end{cases}$$

In particular, $\vartheta_{L,P} = 0$ if j is even and $3M > N + j/2$, or j is odd and $3M > N + (j-3)/2$.

3 Proof of Theorem 1.1 and Corollary 1.2

In this section, we give proofs of Theorem 1.1 and Corollary 1.2.

3.1 Proof of Theorem 1.1 (1)

Let C be a binary doubly even self-dual code of length $n = 24m$, and let $f \in \mathrm{Harm}_1$. It is enough to show that $W_{C,f}(x, y) = 0$ by Theorem 2.1. By Theorem 2.3 (1) we have

$$W_{C,f}(x, y) = xy P_{30} Q,$$

where $Q \in \mathbb{C}[P_8, P_{24}]$. Because of $\min(C) = 4m$, $W_{C,f}(x, y)$ is divisible by y^{4m}. This implies that Q is divisible by y^{4m-4}, and hence $Q = P_{24}^{m-1} Q'$ for some $Q' \in \mathbb{C}[P_8, P_{24}]$. If this polynomial is nonzero, then

$$24m = \deg W_{C,f}(x, y) = 32 + \deg Q \geq 32 + 24(m - 1).$$

This contradiction proves $Q = 0$, and hence $W_{C,f}(x, y) = 0$.

3.2 Proof of Theorem 1.1 (2)

Let C be a ternary self-dual code of length $n = 12m$, and let $f \in \mathrm{Harm}_1$. It is enough to show that $W_{C,f}(x, y) = 0$ by Lemma 2.1. By Theorem 2.3 (2) we have

$$W_{C,f}(x, y) = xy p_{14} Q,$$

where $Q \in \mathbb{C}[g_4, g_{12}]$. Because of $\min(C) = 3m$, $W_{C,f}(x, y)$ is divisible by y^{3m}. This implies that Q is divisible by y^{3m-3}, and hence $Q = g_{12}^{m-1} Q'$ for some $Q' \in \mathbb{C}[g_4, g_{12}]$. If this polynomial is nonzero, then

$$12m = \deg W_{C,f}(x, y) = 16 + \deg Q \geq 16 + 12(m - 1).$$

This contradiction proves $Q = 0$, and hence $W_{C,f}(x, y) = 0$.

3.3 Proof of Theorem 1.1 (3)

Let C be a quaternary self-dual code of length $n = 6m$, and let $f \in \mathrm{Harm}_1$. It is enough to show that $W_{C,f}(x, y) = 0$ by Lemma 2.1. By Theorem 2.3 (3) we have

$$W_{C,f}(x, y) = xy q_6 Q,$$

where $Q \in \mathbb{C}[h_2, h_6]$. Because of $\min(C) = 2m$, $W_{C,f}(x, y)$ is divisible by y^{2m}. This implies that Q is divisible by y^{2m-1}, and hence $Q = h_6^{m-1} Q'$ for some $Q' \in \mathbb{C}[h_2, h_6]$. If this polynomial is nonzero, then

$$6m = \deg W_{C,f}(x, y) = 8 + \deg Q \geq 8 + 6(m - 1).$$

This contradiction proves $Q = 0$, and hence $W_{C,f}(x, y) = 0$.

3.4 Proof of Theorem 1.1 (4)

Let L be an even unimodular lattice of rank $24m$ with minimum norm $2m$. Let us assume that $P \in \mathrm{Harm}_2(\mathbb{R}^{24m})$. Then by Lemma 2.9 we have $\vartheta_{L,P}(z) = 0$. Thus, the result follows from Lemma 2.8.

3.5 Proof of Corollary 1.2

The following lemma is easily seen.

Lemma 3.1 ([6, Page 3, Proposition 1.4]) *Let $\lambda(S)$ be the number of blocks containing a given set S of s points in a combinatorial t-(v, k, λ) design, where $0 \leq s \leq t$. Then*

$$\lambda(S)\binom{k-s}{t-s} = \lambda\binom{v-s}{t-s}.$$

In particular, the number of blocks is

$$\frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}\lambda.$$

We give the proof of Corollary 1.2 (1). The other cases can be proved similarly.

Let C be a binary doubly even self-dual code of length $24m$ with minimum weight $4m$. By Theorem 1.1 (1), C_{4m} is a combinatorial 1-design. Then by Lemma 3.1, $|C_{4m}|$ is divisible by 6. This means that the coefficient of $x^{24m-4m}y^{4m}$ in the weight enumerator of C is divisible by 6. This completes the proof of Corollary 1.2 (1).

4 Proof of Theorem 1.3

In this section, we give a proof of Theorem 1.3.

4.1 Proof of Theorem 1.3 (1)

Let C be a binary doubly even self-dual code of length $n = 24m$, and let $f \in \mathrm{Harm}_2$. Then by Theorem 2.3 (1) we have $W_{C,f}(x, y) = (xy)^2 P_{12} Q$ for some $Q \in \mathbb{C}[P_8, P_{24}]$. Because of $\min(C) = 4m$, $W_{C,f}$ is divisible by y^{4m}. This implies that Q is divisible by y^{4m-4}, and hence Q is divisible by P_{24}^{m-1}. Since Q has degree $24m - 16$, this forces $W_{C,f}$ to be a constant multiple of $(xy)^2 P_8 P_{12}^{2m-1}$. The coefficient of y^{4m+4} in $(xy)^2 P_8 P_{12}^{2m-1}$ is equal to the coefficient of y^4 in

$$(x^8 + 14x^4y^4 + y^8)(x^4 - y^4)^{4m-2} \tag{4.1}$$

which is $16 - 4m$. This vanishes when $m = 4$. Therefore, $C_{4m+4} = C_{20}$ is a 2-design by Lemma 2.1.

4.2 Proof of Theorem 1.3 (2)

Let L be an even unimodular lattice of rank $24m$ with minimum norm $2m$. Let us assume that $P \in \mathrm{Harm}_4(\mathbb{R}^{24m})$. Then by the Lemma 2.9 we have $\vartheta_{L,P}(z) \in \mathbb{C}[E_4, \Delta]$. Since L has

minimum norm $2m$, $\vartheta_{L,P}(z)$ is a constant multiple of $\Delta^m E_4$. The coefficient of q^{2m+2} in $\Delta^m E_4$ is equal to the coefficient of q^2 in

$$(1 - 24q^2)^m (1 + 240q^2),$$

which is $240 - 24m$. This vanishes when $m = 10$. Therefore, L_{22} supports a spherical 5-design by Lemma 2.8.

5 Binary doubly even self-dual codes of length 96

In order to prove Theorem 1.4, let us introduce the fundamental equation for combinatorial designs in [18]. Let $\Omega = \{1, \ldots, n\}$, and suppose that $(\Omega, \mathcal{B})$ is a combinatorial t-(n, k, λ) design. Let $c' \in \mathbb{F}_2^n$ and

$$u_j(c') := |\{x \in \mathcal{B} \mid |\mathrm{supp}(c') \cap x| = j\}|.$$

Then the following holds:

$$\sum_{j=\mu}^{\mathrm{wt}(c')} \binom{j}{\mu} u_j(c') = \lambda_\mu \binom{\mathrm{wt}(c')}{\mu}, \quad \mu = 1, \ldots, t, \tag{5.1}$$

where we denote by λ_μ the number of blocks which contain a given set of μ points. Here we note that

$$\lambda_\mu = \frac{k(k-1)\cdots(k-\mu+1)}{n(n-1)\cdots(n-\mu+1)} |\mathcal{B}|$$

by Lemma 3.1. Another consequence of Lemma 3.1 is the following.

Lemma 5.1 *If $(\Omega, \mathcal{B})$ is a combinatorial t-(n, k, λ) design, then $|\mathcal{B}|$ is divisible by the numerator of*

$$\frac{n(n-1)\cdots(n-s+1)}{k(k-1)\cdots(k-s+1)} \quad (s = 1, \ldots, t)$$

as an irreducible fraction.

For the remainder of this section, we let C be a binary doubly even self-dual code of length 96 with minimum weight 16. In [11], the weight enumerator of C is determined to be

$$
\begin{aligned}
W_C&(x, y) \\
&= 1 + (-28086 + a)y^{16} + (3666432 - 16a)y^{20} \\
&\quad + (366474560 + 120a)y^{24} + (18658567680 - 560a)y^{28} \\
&\quad + (422018863695 + 1820a)y^{32} + (4552989336064 - 4368a)y^{36} \\
&\quad + (24292464652992 + 8008a)y^{40} + (65727332943360 - 11440a)y^{44} \\
&\quad + (91447307757260 + 12870a)y^{48} + \cdots,
\end{aligned}
\tag{5.2}
$$

where

$$28086 < a \leq 229152. \tag{5.3}$$

Since C has minimum weight 16, $W_{C,f}(x,y)$ is divisible by y^{16} for $f \in \mathrm{Harm}_k$ with $k \geq 1$. By Theorem 2.3 (1), this implies

$$W_{C,f}(x,y) \in \begin{cases} \mathbb{C}x^2y^2P_8P_{12}^7 & \text{if } f \in \mathrm{Harm}_2, \\ \mathbb{C}x^3y^3P_{12}^6P_{18} & \text{if } f \in \mathrm{Harm}_3, \\ \mathbb{C}x^4y^4P_8^2P_{12}^6 & \text{if } f \in \mathrm{Harm}_4, \\ \mathbb{C}x^5y^5P_8P_{12}^5P_{18} & \text{if } f \in \mathrm{Harm}_5. \end{cases} \tag{5.4}$$

We first investigate the coefficients of the polynomials appearing above. Note that the coefficient of $x^{96-\ell}y^\ell$ in the harmonic weight enumerator (5.4) is 0 unless $\ell \in \mathcal{L}$, where the set $\mathcal{L}$ is defined in (1.4).

Lemma 5.2 (1) *Let* $x^2y^2P_8P_{12}^7 = \sum c_\ell x^{96-\ell}y^\ell$. *Then* $c_\ell \neq 0$ *for* $\ell \in \mathcal{L} \setminus \{20, 76\}$.
(2) *Let* $x^3y^3P_{12}^6P_{18} = \sum c_\ell x^{96-\ell}y^\ell$. *Then* $c_\ell \neq 0$ *for* $\ell \in \mathcal{L} \setminus \{48\}$.
(3) *Let* $x^4y^4P_8^2P_{12}^6 = \sum c_\ell x^{96-\ell}y^\ell$. *Then* $c_\ell \neq 0$ *for* $\ell \in \mathcal{L}$.
(4) *Let* $x^5y^5P_8P_{12}^5P_{18} = \sum c_\ell x^{96-\ell}y^\ell$. *Then* $c_\ell \neq 0$ *for* $\ell \in \mathcal{L} \setminus \{48\}$.

Proof We can check directly that $c_\ell \neq 0$ for ℓ in the range specified in (1)–(4). □

Proof of Theorem 1.4 (1) By Lemma 5.2 (1) and (5.4), we have $W_{C,f}(x,y) = 0$ for $f \in \mathrm{Harm}_2$. Since every shell of C is a combinatorial 1-design by Theorem 1.1 (1), it is also a combinatorial 2-design by Lemma 2.1.

(2) By Lemma 5.2 (2) and (5.4), we have $W_{C,f}(x,y) = 0$ for $f \in \mathrm{Harm}_3$. Thus, every shell of C is a combinatorial 3-design by Lemma 2.1. Similarly, if $t = 4, 5$, every shell of C is a combinatorial t-design. The proof is complete if we show $t \leq 4$ which, at the same time proves the inequality in (3) for the case $\ell \neq 20, 48, 76$. If $t \geq 5$, then, in particular, C_{16} is a combinatorial 5-design. Since

$$\frac{96 \cdot 95 \cdot 94 \cdot 93 \cdot 92}{16 \cdot 15 \cdot 14 \cdot 13 \cdot 12} = \frac{2 \cdot 19 \cdot 23 \cdot 31 \cdot 47}{7 \cdot 13},$$

Lemma 5.1 implies that $|C_{16}| = a - 28086$ is divisible by $2 \cdot 19 \cdot 23 \cdot 31 \cdot 47 = 1273418$. Then we have $a \geq 1301504$, contrary to (5.3).

(3) First, we give the proof for the case $\ell = 48$. Suppose $t \geq 8$. We use the fundamental equation (5.1). Take $c' \in C_{16}$ and write $x_j := u_j(c')$ for simplicity. Note that $x_j = 0$ if $j > 16$ or $j = $ odd. Note also that $|C_{48}| = 91447307757260 + 12870a$. Solving the system of equations

$$\binom{16}{i}\lambda_i = \sum_{j=0}^{8} \binom{2j}{i}x_{2j} \quad (i = 0, 1, \ldots, 8),$$

we obtain the solution $x_0 = 8112261172015/13528 + 70785a/838736$, and $x_0 \notin \mathbb{Z}$ for all integers $a \in \mathbb{Z}$ in the range (5.3). This is a contradiction.

Next, we give the proof for the cases $\ell = 20, 76$. Suppose $t \geq 6$. Then C_{20} is a combinatorial 6-design. Since

$$\frac{96 \cdot 95 \cdot 94 \cdot 93 \cdot 92 \cdot 91}{20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15} = \frac{2 \cdot 7 \cdot 13 \cdot 23 \cdot 31 \cdot 47}{3 \cdot 5 \cdot 17},$$

Lemma 5.1 implies that $|C_{20}|$ is divisible by $2 \cdot 7 \cdot 13 \cdot 23 \cdot 31 \cdot 47 = 6099002$. Since $6099002 > 3666432 - 16a = |C_{20}|$, this is a contradiction.

The inequality for the case $\ell \neq 20, 48, 76$ has already been proved in part (2). □

Recall that C is a binary doubly even self-dual code of length 96 with minimum weight 16. For each $\ell \in \mathcal{L}$, we denote by $t_\ell(C)$ the largest integer t such that C_ℓ is a combinatorial t-design. Let

$$\delta(C) = \min\{t_\ell(C) \mid \ell \in \mathcal{L}\},$$
$$s(C) = \max\{t_\ell(C) \mid \ell \in \mathcal{L}\}.$$

In [22,23], the first and third authors considered the possible occurrence of $\delta(C) < s(C)$. By Theorems 1.1 (1) and 1.4, we have

$$1 \leq \delta(C) \leq 4, \ 2 \leq s(C) \leq 7.$$

We will show in Example 5.4 that, for all the known codes C, $\delta(C) = 1 < 2 = s(C)$ holds. More precisely,

$$t_\ell(C) = \begin{cases} 2 & \text{if } \ell \in \{20, 76\}, \\ 1 & \text{if } \ell \in \mathcal{L} \setminus \{20, 76\}. \end{cases} \tag{5.5}$$

To do this, let us begin with the following lemma:

Lemma 5.3 (1) *If* $t_{20}(C) \geq 3$, *then* $a = 141k + 28086$ *for some integer k with* $1 \leq k \leq 1426$.
(2) *If* $t_\ell(C) \geq 2$ *for some* $\ell \in \mathcal{L} \setminus \{20, 76\}$, *then* $a = 114k + 28086$ *for some integer k with* $1 \leq k \leq 1763$.

Proof (1) Since

$$\frac{96 \cdot 95 \cdot 94}{20 \cdot 19 \cdot 18} = \frac{8 \cdot 47}{3}, \quad \frac{96 \cdot 95}{20 \cdot 19} = 8 \cdot 3,$$

Lemma 5.1 implies that $|C_{20}| = 3666432 - 16a$ is divisible by $8 \cdot 3 \cdot 47 = 1128$. Thus $a \equiv 27 \pmod{141}$. The result then follows from (5.3).
(2) By Theorem 1.4 (1), we have $t_{16}(C) \geq 2$. Since

$$\frac{96 \cdot 95}{16 \cdot 15} = 2 \cdot 19, \quad \frac{96}{16} = 6,$$

Lemma 5.1 implies that $|C_{16}| = a - 28086$ is divisible by $2 \cdot 3 \cdot 19 = 114$. The result then follows from (5.3). □

The known examples of a binary doubly even self-dual code of length 96 with minimum weight 16 are as follows:

Example 5.4 (a) Feit [13]: $a = 37722$.
(b) Dougherty, Gulliver and Harada [11]: $a \in \{37584, 37500, 37524, 37596\}$.
(c) Dontcheva [10]: $a \in \{36918, 37884, 37332\}$.
(d) Harada, Kiermaier, Wassermann and Yorgova [16]: $a = 37194$.
(e) Gulliver and Harada [14, Table 5, 6]: there are 639 values of a.

It is claimed in [11] that there exists a code with $a = 37598$. However, this value is incorrect, as it contradicts Corollary 1.2. We verified that the correct value is $a = 37596$.

If C is one of the codes in Example 5.4 (a)–(d), Lemma 5.3 implies immediately that (5.5) holds.

For some codes in Example 5.4 (e), Lemma 5.3 (1) does not rule out larger values of $t_{20}(C)$. In fact, all the 1532 bordered double circulant codes in [14, Table 6], and 117 codes out of 4565 in [14, Table 5] satisfy the condition of Lemma 5.3 (1). We have checked, however, by Magma that none of these codes C satisfies $t_{20}(C) \geq 3$.

Some codes given in [14] satisfies the condition of Lemma 5.3 (2). More precisely, 92 bordered double circulant codes in [14, Table 6], and 246 codes out of 4565 in [14, Table 5] satisfy the condition of Lemma 5.3 (2). We have checked, however, by Magma that none of these codes C satisfies $t_{16}(C) \geq 2$. Therefore, for codes in (e), (5.5) holds as well.

We note that there is no known example C with $C_{20} = \emptyset$.

6 Concluding remarks

Remark 6.1 A code or lattice satisfying the assumption of Theorem 1.1 is called near-extremal. In [20], it is shown that for sufficiently large n, there is no extremal or near-extremal codes (resp. lattices) with length n (resp. rank n).

More precisely, it is shown in [30] that there is no extremal code with length n for

$$\text{Doubly even:} \quad n = 24i \ (i \geq 154), \ 24i + 8 \ (i \geq 159), \ 24i + 16 \ (i \geq 164),$$
$$\text{Ternary:} \quad n = 12i \ (i \geq 70), \ 12i + 4 \ (i \geq 75), \ 12i + 8 \ (i \geq 78),$$
$$\text{Quaternary:} \quad n = 6i \ (i \geq 17), \ 6i + 2 \ (i \geq 20), \ 6i + 4 \ (i \geq 22),$$

and it is shown in [15] that there is no near-extremal code with length n for

$$\text{Doubly even:} \quad n = 24i \ (i \geq 315), \ 24i + 8 \ (i \geq 320), \ 24i + 16 \ (i \geq 325),$$
$$\text{Ternary:} \quad n = 12i \ (i \geq 147), \ 12i + 4 \ (i \geq 150), \ 12i + 8 \ (i \geq 154),$$
$$\text{Quaternary:} \quad n = 6i \ (i \geq 38), \ 6i + 2 \ (i \geq 41), \ 6i + 4 \ (i \geq 43).$$

Moreover, it is shown in [17] that there is no extremal lattice with rank $n > 163264$. We do not know whether it can be proved that there is no near-extremal lattice with sufficiently large rank.

Remark 6.2 Our proof of Theorem 1.3 actually shows that, $m = 4$ is the only case where we can show that $t_{4m+4}(C) \geq 2$. In fact, it can be easily verified by computer that nontrivial vanishing of coefficients of the polynomial (4.1) for $1 \leq m \leq 314$ (see Remark 6.1) occurs only for the case mentioned in our proof.

Remark 6.3 Ternary and quaternary analogues of Theorem 1.3 do not exist. Let C be a ternary (resp. quaternary) self-dual code of length $12m$ (resp. $6m$) with minimum weight $3m$ (resp. $2m$). By Theorem 2.3, for $f \in \text{Harm}_2$, the harmonic weight enumerator is written as follows:

$$W_{C,f} \in \begin{cases} \mathbb{C}x^2y^2 p_4 g_4 g_{12}^{m-1} & \text{if } C \text{ is ternary,} \\ \mathbb{C}x^2y^2 h_2 h_6^{m-1} & \text{if } C \text{ is quaternary.} \end{cases}$$

By Lemma 2.1, if the coefficient of $x^{12m-3\ell}y^{3\ell}$ (resp. $x^{6m-2\ell}y^{2\ell}$) in $W_{C,f}$ is zero for $3m \leq 3\ell \leq 12m$ (resp. $2m \leq 2\ell \leq 6m$), then $C_{3\ell}$ (resp. $C_{2\ell}$) is a combinatorial 2-design. However, no such coefficient vanishes.

Remark 6.4 An analogue of Theorem 1.4, parts (1) and (2) seems to hold. That is, for an even unimodular lattice L of rank 240, and $t = 5, 7$, if $L_{2\ell}$ supports a spherical t-design for some $\ell \neq 11$, then $L_{2\ell}$ supports a spherical t-design for all nonzero ℓ with $L_{2\ell} \neq \emptyset$. The proof would require non-vanishing of coefficients of the modular forms $\Delta^{10}E_4$ and $\Delta^{10}E_6$ as formal power series.

Remark 6.5 The case $m = 1$ in Theorem 1.1 (4) was essentially used in the proof of the classification of even unimodular lattices of rank 24 [26] (see also [12, Proposition 3.3 and Corollary 3.5]).

References

1. Assmus Jr. E.F., Mattson Jr. H.F.: New 5-designs. J. Comb. Theory **6**, 122–151 (1969).
2. Bachoc C.: On harmonic weight enumerators of binary codes. Des. Codes Cryptogr. **18**(1–3), 11–28 (1999).
3. Bachoc C.: Harmonic weight enumerators of nonbinary codes and MacWilliams identities. In: Codes and Association Schemes (Piscataway, NJ, 1999), pp. 1–23, DIMACS Ser. Discrete. Math. Theoret. Comput. Sci., vol. 56. Amer. Math. Soc., Providence, RI (2001).
4. Bannai E., Koike M., Shinohara M., Tagami M.: Spherical designs attached to extremal lattices and the modulo p property of Fourier coefficients of extremal modular forms. Mosc. Math. J. **6**, 225–264 (2006).
5. Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997).
6. Cameron P.J., van Lint J.H.: Designs, Graphs, Codes and Their Links, London Mathematical Society Student Texts, vol. 22. Cambridge University Press, Cambridge (1991).
7. Conway J.H., Sloane N.J.A.: Sphere Packings Lattices and Groups, 3rd edn. Springer, New York (1999).
8. Delsarte P.: Hahn polynomials, discrete harmonics, and t-designs. SIAM J. Appl. Math. **34**(1), 157–166 (1978).
9. Delsarte P., Goethals J.-M., Seidel J.J.: Spherical codes and designs. Geom. Dedicata **6**, 363–388 (1977).
10. Dontcheva R.: Doubly-even self-dual code of length 96. IEEE Trans. Inf. Theory **48**, 557–561 (2002).
11. Dougherty S.T., Gulliver T.A., Harada M.: Extremal binary self-dual codes. IEEE Trans. Inf. Theory **43**, 2036–2047 (1997).
12. Ebeling W.: Lattices and Codes, A Course Partially Based on Lectures by Friedrich Hirzebruch, Third edition, Advanced Lectures in Mathematics, Springer Spektrum, Wiesbaden (2013).
13. Feit W.: A self-dual even (96, 48, 16) code. IEEE Trans. Inf. Theory **20**, 136–138 (1974).
14. Gulliver T.A., Harada M.: On extremal double circulant self-dual codes of lengths 90–96, Applicable Algebra in Eng. Commun. Comput. First online, 1–13 (2019).
15. Han S., Kim J.-L.: The nonexistence of near-extremal formally self-dual codes. Des. Codes Cryptogr. **51**(1), 69–77 (2009).
16. Harada M., Kiermaier M., Wassermann A., Yorgova R.: New binary singly even self-dual codes. IEEE Trans. Inf. Theory **56**, 1612–1617 (2010).
17. Jenkins P., Rouse J.: Bounds for coefficients of cusp forms and extremal lattices. Bull. Lond. Math. Soc. **43**(5), 927–938 (2011).
18. Koch H.: On self-dual doubly-even extremal codes. Discret. Math. **83**(2–3), 291–300 (1990).
19. MacWilliams F.J., Odlyzko A.M., Sloane N.J.A., Ward H.N.: Self-dual codes over GF(4). J. Comb. Theory Ser. A **25**(3), 288–318 (1978).
20. Mallows C.L., Odlyzko A.M., Sloane N.J.A.: Upper bounds for modular forms, lattices, and codes. J. Algebra **36**, 68–76 (1975).
21. Mallows C.L., Sloane N.J.A.: An upper bound for self-dual codes. Inf. Control **22**, 188–200 (1973).
22. Miezaki T., Nakasora H.: An upper bound of the value of t of the support t-designs of extremal binary doubly even self-dual codes. Des. Codes Cryptogr. **79**, 37–46 (2016).
23. Miezaki T., Nakasora H.: The support designs of the triply even binary codes of length 48. J. Comb. Des. **27**, 673–681 (2019).
24. Pache C.: Shells of selfdual lattices viewed as spherical designs. Int. J. Algebra Comput. **15**(5–6), 1085–1127 (2005).
25. Tanabe K.: A new proof of the Assmus-Mattson theorem for non-binary codes. Des. Codes Cryptogr. **22**(2), 149–155 (2001).
26. Venkov B.B.: On the classification of integral even unimodular 24-dimensional quadratic forms. (Russian) Algebra, number theory and their applications. Trudy Mat. Inst. Steklov. **148**, 65–76 (1978). 273.
27. Venkov B.B.: Even unimodular extremal lattices. (Russian) Algebraic geometry and its applications. Trudy Mat. Inst. Steklov. **165**, 43–48 (1984); translation in Proc. Steklov Inst. Math. **165**, 47–52 (1985).

28. Venkov B.B.: Réseaux et designs sphériques, (French) [Lattices and spherical designs] Réseaux euclidiens, designs sphériques et formes modulaires, pp. 10–86, Monogr. Enseign. Math., vol. 37, Enseignement Math. Geneva (2001).
29. Wolfram Research, Inc., Mathematica, Version 11.2, Champaign, IL (2017).
30. Zhang S.: On the nonexistence of extremal self-dual codes. Discret. Appl. Math. **91**, 277–286 (1999).