Some Extremal Self-Dual Codes and Unimodular Lattices in Dimension 40*

Stefka Bouyuklieva,† Iliya Bouyukliev‡and Masaaki Harada§

October 17, 2012

Abstract

In this paper, binary extremal singly even self-dual codes of length 40 and extremal odd unimodular lattices in dimension 40 are studied. We give a classification of extremal singly even self-dual codes of length 40. We also give a classification of extremal odd unimodular lattices in dimension 40 with shadows having 80 vectors of norm 2 through their relationships with extremal doubly even self-dual codes of length 40.

1 Introduction

Self-dual codes and unimodular lattices are studied from several viewpoints (see [16] for an extensive bibliography). Many relationships between self-dual codes and unimodular lattices are known and therefore these two objects have similar properties. In this paper, binary singly even self-dual codes of length 40 and odd unimodular lattices in dimension 40 are studied. Both binary self-dual codes and unimodular lattices are divided into two classes,

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

‡Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, P.O. Box 323, Veliko Tarnovo, Bulgaria

§Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan, and PRESTO, Japan Science and Technology Agency (JST), Kawaguchi, Saitama 332–0012, Japan. email: mharada@sci.kj.yamagata-u.ac.jp

namely, doubly even self-dual codes and singly even self-dual codes, and even unimodular lattices and odd unimodular lattices. In addition, a binary doubly even self-dual code of length n (as well as an even unimodular lattice in dimension n) exists if and only if $n \equiv 0 \pmod{8}$. This motivates us to study binary self-dual codes of length n and unimodular lattices in dimension n for $n \equiv 0 \pmod{8}$ simultaneously.

The classification of self-dual codes and unimodular lattices is a fundamental problem. Much work has been done towards classifying binary self-dual codes and unimodular lattices for modest lengths and dimensions (see [16]). A big progress has been realized recently in the classification of binary self-dual codes. All self-dual codes of length 36 were classified in [20]. All extremal codes among them, namely self-dual $[36, 18, 8]$ codes, had been previously classified in [1], so the result was approved in [20]. A classification of extremal self-dual $[38, 19, 8]$ codes was done by three groups independently. It was shown in [2] that there are exactly 2744 extremal self-dual $[38, 19, 8]$ codes, two s-extremal self-dual $[38, 19, 6]$ codes, and 1730 s-extremal self-dual $[38, 19, 8]$ codes, up to equivalence. Recently, a classification of doubly even self-dual codes of length 40 has been done in [6], namely there are 94343 doubly even self-dual codes, 16470 of which are extremal, up to equivalence. Using these codes, a classification of extremal self-dual $[38, 19, 8]$ codes was completed. In [9], an efficient algorithm for classification of binary self-dual codes was described and then applied to length 38. In this way, all binary self-dual codes of length 38 were classified. A lower bound on the number of inequivalent binary self-dual codes of length 40 is given in [9] by 4585657509.

The main aim of this paper is to give a classification of binary extremal singly even self-dual codes of length 40. Some part of the classification is done by considering a relationship with binary doubly even self-dual codes of the same length. In addition, the classification is completed using the algorithm presented in [9]. A partial classification of extremal odd unimodular lattices in dimension 40 is also established from the classification of binary extremal doubly even self-dual codes of length 40.

This paper is organized as follows. In Section 2, we give definitions and some basic properties of the self-dual codes and unimodular lattices. In Section 3, we study the binary extremal singly even self-dual codes of length 40. The number of vectors of weight 4 in the shadow of a binary extremal singly even self-dual code of length 40 is at most 10 [14]. We demonstrate that there are 19 inequivalent binary extremal singly even self-dual codes with shadows having 10 vectors of weight 4. This classification is done by con-

sidering a relationship with binary doubly even self-dual codes of length 40 satisfying the condition that the supports of all codewords of weight 4 form a T-decomposition. We mention a relationship between such binary doubly even self-dual codes and even self-dual additive $\mathbb{F}_4$-codes. By a method similar to the above, our classification is also extended to all cases that shadows have minimum weight 4. A classification of binary extremal (singly even) self-dual codes of length 40 is also completed by an approach which does not depend on the weight enumerators. As a consequence, we have a classification of binary extremal singly even self-dual codes with shadows of minimum weight 8, which is the remaining case. More precisely, combined with the above classification, we demonstrate that there are 10200655 inequivalent binary extremal singly even self-dual codes of length 40. In Section 4, for extremal odd unimodular lattices, we consider a situation which is similar to that for binary extremal singly even self-dual codes with 10 vectors of weight 4 in the shadows, given in Section 3. The number of vectors of norm 2 in the shadow of an extremal odd unimodular lattice in dimension 40 is at most 80. It is shown that there are 16470 non-isomorphic extremal odd unimodular lattices in dimension 40 with shadows having 80 vectors of norm 2. This classification is done by considering a relationship with binary extremal doubly even self-dual codes of length 40. Finally, in Section 5, we investigate theta series for which there is an extremal odd unimodular lattice in dimension 40. The existence of a number of extremal self-dual $\mathbb{Z}_4$-codes of length 40 is also given.

Generator matrices of all inequivalent binary extremal singly even self-dual codes of length 40 can be obtained electronically from [21]. Most of the computer calculations in this paper were done by MAGMA [8]. In Section 3.4, the package SELF-DUAL-BIN by the second author is also used, where it's main algorithm implemented in the program GEN-SELF-DUAL-BIN is described in [9].

2   Preliminaries

2.1   Binary self-dual codes

Let $\mathbb{F}_q$ denote the finite field of order q, where q is a prime power. Any subset of $\mathbb{F}_q^n$ is called an $\mathbb{F}_q$-*code* of length n. An $\mathbb{F}_q$-code is linear if it is a linear subspace of $\mathbb{F}_q^n$. An $\mathbb{F}_2$-code is called *binary* and all codes in this paper mean

binary linear codes unless otherwise noted.

A code is called *doubly even* if all codewords have weight $\equiv 0 \pmod 4$. The *dual code* $C^\perp$ of a code C of length n is defined as $C^\perp = \{x \in \mathbb{F}_2^n \mid x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y$ is the standard inner product. A code C is called *self-dual* if $C = C^\perp$. A self-dual code which is not doubly even is called *singly even*. A doubly even self-dual code of length n exists if and only if $n \equiv 0 \pmod 8$, while a singly even self-dual code of length n exists if and only if n is even. The minimum weight $d(C)$ of a self-dual code C of length n is bounded by $d(C) \leq 4\lfloor n/24 \rfloor + 4$ unless $n \equiv 22 \pmod{24}$ when $d(C) \leq 4\lfloor n/24 \rfloor + 6$ [31]. We say that a self-dual code meeting the upper bound is *extremal*.

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 $C_0^\perp \setminus C$. There are cosets C_1, C_2, C_3 of C_0 such that $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$, where $C = C_0 \cup C_2$ and $S = C_1 \cup C_3$. Shadows were introduced by Conway and Sloane [14], in order to provide restrictions on the weight enumerators of singly even self-dual codes. In fact, the above upper bound on the minimum weight was established by considering shadows (see [31]). Two self-dual codes C and C' of length n are said to be *neighbors* if $\dim(C \cap C') = n/2 - 1$. Since every self-dual code C of length n contains the all-one vector $\mathbf{1}$, C has $2^{n/2-1} - 1$ subcodes D of codimension 1 containing $\mathbf{1}$. Since $\dim(D^\perp/D) = 2$, there are two self-dual codes rather than C lying between $D^\perp$ and D. When C is doubly even, one of them is doubly even and the other is singly even for each subcode D. If C is a singly even self-dual code of length divisible by 8, then C has two doubly even self-dual neighbors, namely $C_0 \cup C_1$ and $C_0 \cup C_3$ (see [10]).

Two codes C and C' are *equivalent*, denoted $C \cong C'$, if one can be obtained from the other by permuting the coordinates. An *automorphism* of C is a permutation of the coordinates which preserves the code. The set consisting of all automorphisms of C forms a group called the *automorphism group* of this code and it is denoted by $\mathrm{Aut}(C)$. The number of the codes equivalent to C is $n!/\#\mathrm{Aut}(C)$, where n is the length of C. If we consider the action of the symmetric group S_n on the set Ω_n of all self-dual codes of length n, then two codes from this set are equivalent if they belong to the same orbit. This action induces an equivalence relation in Ω_n and the equivalence classes are the orbits with respect to the action of S_n. To classify the self-dual codes of length n means to find exactly one representative of each equivalence class.

2.2 Self-dual additive $\mathbb{F}_4$-codes and $\mathbb{Z}_4$-codes

In Section 3.2, we also consider additive $\mathbb{F}_4$-codes, where $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. Such a code is a k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_4^n$ and so has 2^k codewords. An additive $\mathbb{F}_4$-code is even if all its codewords have even Hamming weights. Two additive $\mathbb{F}_4$-codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if there is a map from $S_3^n \times S_n$ sending $\mathcal{C}_1$ onto $\mathcal{C}_2$, where S_n acts on the set of the n coordinates and S_3 permutes the elements $1, \omega, \omega^2$ of the field. The automorphism group of $\mathcal{C}$, denoted by $\mathrm{Aut}(\mathcal{C})$, consists of all elements of $S_3^n \times S_n$ which preserve the code.

An additive $\mathbb{F}_4$-code $\mathcal{C}$ is called self-dual if $\mathcal{C} = \mathcal{C}^*$, where the dual code $\mathcal{C}^*$ of $\mathcal{C}$ is defined as $\{x \in \mathbb{F}_4^n \mid x * y = 0 \text{ for all } y \in \mathcal{C}\}$ under

$$x * y = \sum_{i=1}^{n} (x_i y_i^2 + x_i^2 y_i) \text{ for } x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_4^n.$$

Even self-dual additive $\mathbb{F}_4$-codes exist only in even lengths. The minimum Hamming weight $d(\mathcal{C})$ of an even self-dual additive $\mathbb{F}_4$-code $\mathcal{C}$ of length n is bounded by $d(\mathcal{C}) \leq 2\lfloor n/6 \rfloor + 2$ [33, Theorem 33]. We say that an even self-dual additive $\mathbb{F}_4$-code meeting the upper bound is extremal.

The last family of self-dual codes which we consider is the set of self-dual $\mathbb{Z}_4$-codes, where $\mathbb{Z}_4$ denotes the ring of integers modulo 4. The self-dual $\mathbb{Z}_4$-codes are connected with unimodular lattices of a special form [7]. A $\mathbb{Z}_4$-code $\mathcal{C}$ of length n is a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$. A $\mathbb{Z}_4$-code $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^\perp$, where the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined as $\{x \in \mathbb{Z}_4^n \mid x \cdot y = 0 \text{ for all } y \in \mathcal{C}\}$ under the standard inner product $x \cdot y$. We say that two $\mathbb{Z}_4$-codes are equivalent if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates.

The Euclidean weight of a codeword $x = (x_1, \ldots, x_n)$ of $\mathcal{C}$ is $n_1(x) + 4n_2(x) + n_3(x)$, where $n_\alpha(x)$ denotes the number of components i with $x_i = \alpha$ ($\alpha = 1, 2, 3$). A $\mathbb{Z}_4$-code $\mathcal{C}$ is Type II if $\mathcal{C}$ is self-dual and the Euclidean weights of all codewords of $\mathcal{C}$ are divisible by 8 [7, 23]. A self-dual code which is not Type II is called Type I. A Type II $\mathbb{Z}_4$-code of length n exists if and only if $n \equiv 0 \pmod 8$, while a Type I $\mathbb{Z}_4$-code exists for every length. The minimum Euclidean weight $d_E(\mathcal{C})$ of a Type II $\mathbb{Z}_4$-code $\mathcal{C}$ of length n is bounded by $d_E(\mathcal{C}) \leq 8\lfloor n/24 \rfloor + 8$ [7]. It was also shown in [32] that the minimum Euclidean weight $d_E(\mathcal{C})$ of a Type I code $\mathcal{C}$ of length n is bounded by $d_E(\mathcal{C}) \leq 8\lfloor n/24 \rfloor + 8$ if $n \not\equiv 23 \pmod{24}$, and $d_E(\mathcal{C}) \leq 8\lfloor n/24 \rfloor + 12$ if

$n \equiv 23 \pmod{24}$. A self-dual $\mathbb{Z}_4$-code meeting the upper bound is called *extremal*.

2.3   Unimodular lattices

A (Euclidean) lattice $L \subset \mathbb{R}^n$ in dimension n is *integral* if $L \subset L^*$, where the dual lattice L^* of L is defined as $\{x \in \mathbb{R}^n \mid (x, y) \in \mathbb{Z} \text{ for all } y \in L\}$ under the standard inner product (x, y). An integral lattice is called *even* if the norm (x, x) of every vector x is even. A lattice $L = L^*$ is called *unimodular*. A unimodular lattice which is not even is called *odd*. An even unimodular lattice in dimension n exists if and only if $n \equiv 0 \pmod 8$, while an odd unimodular lattice exists for every dimension. Two lattices L and L' are *isomorphic*, denoted $L \cong L'$, if there exists an orthogonal matrix A with $L' = L \cdot A$. Rains and Sloane [32] showed that the minimum norm $\min(L)$ of a unimodular lattice L in dimension n is bounded by $\min(L) \leq 2\lfloor n/24 \rfloor + 2$ unless $n = 23$ when $\min(L) \leq 3$. We say that a unimodular lattice meeting the upper bound is *extremal*.

Let L be an odd unimodular lattice and let L_0 denote its sublattice of vectors of even norms. Then L_0 is a sublattice of L of index 2 [15]. The *shadow* S of L is defined to be $L_0^* \setminus L$. There are cosets L_1, L_2, L_3 of L_0 such that $L_0^* = L_0 \cup L_1 \cup L_2 \cup L_3$, where $L = L_0 \cup L_2$ and $S = L_1 \cup L_3$. Shadows for odd unimodular lattices appeared in [15] and also in [16, p. 440], in order to provide restrictions on the theta series of odd unimodular lattices. Two lattices L and L' are *neighbors* if both lattices contain a sublattice of index 2 in common. If L is an odd unimodular lattice in dimension divisible by 8, then L has two even unimodular neighbors of L, namely, $L_0 \cup L_1$ and $L_0 \cup L_3$.

3   Singly even self-dual codes of length 40

In this section, we give a classification of extremal singly even self-dual codes of length 40. For the case that the shadows have minimum weight 4, the classification was done in two different ways.

6

3.1 Weight enumerators

An extremal singly even self-dual code C of length 40 and its shadow S have the following weight enumerators

$$\begin{cases} W_{40,C,\beta} = & 1 + (125 + 16\beta)y^8 + (1664 - 64\beta)y^{10} + (10720 + 32\beta)y^{12} + \cdots, \\ W_{40,S,\beta} = & \beta y^4 + (320 - 8\beta)y^8 + (21120 + 28\beta)y^{12} + \cdots, \end{cases}$$

respectively, where β is an integer with $0 \leq \beta \leq 10$ [14]. It was shown in [19] that an extremal singly even self-dual code with weight enumerator $W_{40,C,\beta}$ exists if and only if $\beta = 0, 1, \ldots, 8, 10$.

Lemma 3.1 ([19, Section III]). *Let C be an extremal singly even self-dual code of length 40 with weight enumerator $W_{40,C,\beta}$. Then one of $C_0 \cup C_1$ and $C_0 \cup C_3$ is an extremal doubly even self-dual code of length 40 and the remaining one is a doubly even self-dual code of length 40 containing β codewords of weight 4.*

3.2 Weight enumerator $W_{40,C,10}$, T-decompositions and self-dual additive $\mathbb{F}_4$-codes

Let C be a code of length $n \equiv 0 \pmod 4$. A partition $\{T_1, T_2, \ldots, T_{\frac{n}{4}}\}$ of $\{1, 2, \ldots, n\}$ is called a T-*decomposition* of C if the following conditions hold

$$T_1 \cup T_2 \cup \cdots \cup T_{\frac{n}{4}} = \{1, 2, \ldots, n\}, \tag{1}$$

$$\#T_i = 4, \tag{2}$$

$$T_i \cup T_j \text{ is the support of a codeword of } C, \tag{3}$$

for $i, j = 1, 2, \ldots, \frac{n}{4}$ and $i \neq j$ [25]. In particular, when all T_i are the supports of codewords of C, we say that C contains the T-decomposition.

In this subsection, we assume that C is an extremal singly even self-dual code of length 40 with weight enumerator $W_{40,C,10}$. By Lemma 3.1, we may suppose without loss of generality that all 10 vectors of weight 4 in S are contained in C_1.

Lemma 3.2. *There is a T-decomposition for the self-dual codes C, $C_0 \cup C_1$ and $C_0 \cup C_3$. In particular, $C_0 \cup C_1$ contains a T-decomposition.*

Proof. Denote by S_4 the set of the 10 vectors of weight 4 in the shadow S of C. The supports of any two vectors of S_4 are disjoint. Thus, $\{\text{supp}(x) \mid x \in S_4\}$ is a T-decomposition for the codes C, $C_0 \cup C_1$ and $C_0 \cup C_3$. $\square$

By Lemmas 3.1 and 3.2, every extremal singly even self-dual code C of length 40 with weight enumerator $W_{40,C,10}$ is constructed as a neighbor of some doubly even self-dual code D satisfying the following condition

the supports of all codewords of weight 4 are a T-decomposition. (4)

It follows that $\dim(C \cap D) = 19$ and $\mathbf{1} \in C \cap D$. Since $\dim(C_0^\perp / C_0) = 2$, there are two doubly even self-dual codes lying between $C_0^\perp$ and C_0. In this case, one doubly even self-dual code $C_0 \cup C_1$ has minimum weight 4 and the other one $C_0 \cup C_3$ has minimum weight 8. Hence, C_0 is contained in a unique doubly even self-dual code satisfying the condition (4). This means that extremal singly even self-dual codes, constructed in this way from inequivalent doubly even self-dual codes satisfying (4), are inequivalent. In other words, it is sufficient to check equivalences only for the subcodes D with $\dim(D) = 19$, $d(D) = 8$ and $\mathbf{1} \in D$ contained in each doubly even self-dual code satisfying (4), in order to complete our classification. This observation substantially reduces the necessary calculations for equivalence tests in our classification.

We start the classification of extremal singly even self-dual codes with weight enumerator $W_{40,C,10}$ by investigating the doubly even self-dual codes of minimum weight 4. There are 1093 inequivalent doubly even self-dual codes with $A_4 = 10$, where A_i denotes the number of codewords of weight i [6]. We verified that 19 codes of them satisfy the condition (4). Note that every doubly even self-dual code of length 40 contains $2^{19} - 1$ subcodes of codimension 1 containing $\mathbf{1}$. For each of the 19 codes, we verified that all such subcodes are equivalent. The calculations took about 65 minutes using a single core of a PC Intel i7 6 core processor. By the above observation in the previous paragraph, we have the following:

Proposition 3.3. *There are* 19 *inequivalent extremal singly even self-dual codes of length* 40 *with weight enumerator* $W_{40,C,10}$.

Remark 3.4. A similar argument can be used for the classification of extremal singly even self-dual codes of length 32. The codes C67, C68 and C69 in [13, Table A] are the only doubly even self-dual codes of length 32 satisfying (4). Note that the shadow of an extremal singly even self-dual code has exactly 8 vectors of weight 4 for length 32.

Now we give some properties of the extremal singly even self-dual codes of length 40 with weight enumerator $W_{40,C,10}$. The *covering radius* of a code C of length n is the smallest integer R such that spheres of radius R around

codewords of C cover the space $\mathbb{F}_2^n$. The covering radius is a basic and important geometric parameter of a code. Let R_{40} be the covering radius of an extremal singly even self-dual code of length 40. Then, by the sphere-covering bound and the Delsarte bound (see [3]), $6 \leq R_{40} \leq 14$. In Table 1, we list the number $N(\# \operatorname{Aut}, R)$ of extremal singly even self-dual codes with automorphism groups of order $\# \operatorname{Aut}$ and covering radii R for $\beta = 10$.

Table 1: $(\# \operatorname{Aut}, R, N(\# \operatorname{Aut}, R))$ for $\beta = 10$

$(\# \operatorname{Aut}, R, N(\# \operatorname{Aut}, R))$				
$(12288, 8, 1)$	$(16384, 8, 1)$	$(18432, 8, 1)$	$(20480, 8, 1)$	$(32768, 8, 1)$
$(49152, 8, 3)$	$(65536, 8, 1)$	$(147456, 8, 1)$	$(245760, 8, 1)$	$(262144, 8, 1)$
$(327680, 8, 1)$	$(737280, 8, 1)$	$(786432, 8, 1)$	$(1179648, 8, 1)$	$(1474560, 8, 1)$
$(11796480, 8, 1)$	$(44236800, 7, 1)$			

From Table 1, for $\beta = 10$, there is a unique extremal singly even self-dual code with covering radius 7. This code must be equivalent to the extremal singly even self-dual code with covering radius 7 given in [22, Section 3]. The coset weight distribution of some extremal singly even self-dual code of length 40 with covering radius 7 was given in [28, Table IX], noting that the code was listed without giving its construction. It is claimed in [28, Table IX] that there are 40000 cosets with weight enumerator $4y^6 + 152y^8 + 1644y^{10} + 10608y^{12} + \cdots$. However, we verified that this is incorrect and there are only 14400 cosets with the weight enumerator and there are 25600 cosets with the following weight enumerator

$$4y^6 + 168y^8 + 1580y^{10} + 10640y^{12} + 44388y^{14}$$
$$+ 119768y^{16} + 216172y^{18} + 263136y^{20} + \cdots + 4y^{34}.$$

Now we study a relationship between the doubly even self-dual codes satisfying the condition (4) and the even self-dual additive $\mathbb{F}_4$-codes. Let $\mathcal{C}$ be an even self-dual additive $\mathbb{F}_4$-code of length n. From $\mathcal{C}$, the following code of length $4n$ is obtained

$$B(\mathcal{C}) = \rho(\mathcal{C}) + \{(0000), (1111)\}^n,$$

where ρ is the map $\mathbb{F}_4^n \to \mathbb{F}_2^{4n}$ induced from $\mathbb{F}_4 \to \mathbb{F}_2^4$, $0 \mapsto (0000)$, $1 \mapsto (1100)$, $\omega \mapsto (1010)$ and $\omega^2 \mapsto (0110)$. It is easy to see that if $\mathcal{C}$ is an even self-dual

additive $\mathbb{F}_4$-code of length n, then $B(\mathcal{C})$ is a doubly even self-dual code of length $4n$ and $A_4 \geq n$, containing a T-decomposition. Conversely, if a doubly even self-dual code C contains a T-decomposition, then $C \cong B(\mathcal{C})$ for some even self-dual additive $\mathbb{F}_4$-code $\mathcal{C}$ [34]. A classification of extremal even self-dual additive $\mathbb{F}_4$-codes of length 10 was given in [4]. There are 19 such codes, up to equivalence [4, Table 2]. We verified that, by a mapping $\mathcal{C} \mapsto B(\mathcal{C})$, the 19 inequivalent extremal even self-dual additive $\mathbb{F}_4$-codes of length 10 give the 19 inequivalent doubly even self-dual codes of length 40 satisfying (4).

Remark 3.5. Generator matrices of the 19 extremal even self-dual additive $\mathbb{F}_4$-codes of length 10 are listed in [4, Appendix], but the generator matrix for QC_10l is the same as that for QC_10b. Note that only QC_10l has automorphism group of order 16 [4, Table 2]. We found a code $\mathcal{C}_{10}$ with $\#\operatorname{Aut}(\mathcal{C}_{10}) = 16$ by [17, Theorem 6] from a graph on 10 vertices, where $\operatorname{Aut}(\mathcal{C}_{10})$ was determined using the method given in [12, p. 1373], by calculating the automorphism groups of some related binary codes of length 30. A generator matrix of $\mathcal{C}_{10}$ is listed in Figure 1.

$$\begin{pmatrix} \omega & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & \omega & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & \omega & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & \omega & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & \omega & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & \omega & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & \omega & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & \omega & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & \omega & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & \omega \end{pmatrix}$$

Figure 1: A generator matrix of $\mathcal{C}_{10}$

There is a unique extremal even self-dual additive $\mathbb{F}_4$-code of length 6 [24, Table 1], and the code F_{24} in [30, Table II] is a unique doubly even self-dual code of length 24 satisfying the condition (4). There are three inequivalent extremal even self-dual additive $\mathbb{F}_4$-codes of length 8 [24, Table 1]. These codes are No. 19, 20, 21 in [24, Table 1], and we denote them by $\mathcal{C}_{19}$, $\mathcal{C}_{20}$, $\mathcal{C}_{21}$, respectively. We verified that $B(\mathcal{C}_{19})$, $B(\mathcal{C}_{20})$ and $B(\mathcal{C}_{21})$ are equivalent to C67, C68 and C69 in [13, Table A], respectively (see Remark 3.4). Hence,

there is a one-to-one correspondence between the equivalence classes of doubly even self-dual codes of length $4n$ satisfying (4) and the equivalence classes of extremal even self-dual additive $\mathbb{F}_4$-codes of length n for $n = 6, 8, 10$.

3.3 Weight enumerators $W_{40,C,\beta}$ $(\beta = 1, 2, \ldots, 8)$

In this subsection, we continue the classification of extremal singly even self-dual codes by modifying the classification method for the case $\beta = 10$, which was given in the previous subsection.

Suppose that $1 \leq \beta \leq 8$. Let C be a doubly even self-dual code of length 40. By modifying the definition of T-decompositions, we consider a collection $\{T_1, T_2, \ldots, T_\beta\}$ satisfying the conditions (2), (3) and

$$T_i \cap T_j = \emptyset \tag{5}$$

for $i \neq j$. Denote by $N_{DE}^\beta(40)$ the number of the inequivalent doubly even self-dual codes with $A_4 = \beta$ and by $\overline{N}_{DE}^\beta(40)$ the number of those codes among them which satisfy (2), (3) and (5). It is trivial that $N_{DE}^\beta(40) = \overline{N}_{DE}^\beta(40)$ for $\beta = 1, 2$. The numbers $N_{DE}^\beta(40)$ and $\overline{N}_{DE}^\beta(40)$ for $\beta = 1, 2, \ldots, 8$ are obtained in [6], and the results are listed in Table 2.

Table 2: $N_{DE}^\beta(40)$, $\overline{N}_{DE}^\beta(40)$ and $N_{SE}^\beta(40)$ for $\beta = 1, 2, \ldots, 8$

β	$N_{DE}^\beta(40)$	$\overline{N}_{DE}^\beta(40)$	$N_{SE}^\beta(40)$
1	20034	20034	4674608
2	17276	17276	1511827
3	12168	11241	337565
4	8471	6645	64692
5	5552	3115	11009
6	3916	1380	2413
7	2610	405	405
8	1932	120	120

For $\beta = 1, 2, \ldots, 8$, a similar argument to that given in the previous subsection shows that every extremal singly even self-dual code with weight enumerator $W_{40,C,\beta}$ can be constructed from some doubly even self-dual code with $A_4 = \beta$ containing $\{T_1, T_2, \ldots, T_\beta\}$, which satisfies the conditions (2),

(3), (5). Moreover, the argument for equivalence tests given in the previous subsection is also applied to the cases $\beta = 1, 2, \ldots, 8$. Hence, for these cases, we were able to complete the classification of extremal singly even self-dual codes with weight enumerator $W_{40,C,\beta}$. For the case $\beta = 1$, the calculations took about 3 months using 6 cores of a PC Intel i7 6 core processor. The numbers $N_{SE}^{\beta}(40)$ of inequivalent extremal singly even self-dual codes of length 40 with weight enumerators $W_{40,C,\beta}$ are also listed in Table 2 for $\beta = 1, 2, \ldots, 8$. Combined with Proposition 3.3, we have the following:

Proposition 3.6. *There are* 6602658 *inequivalent extremal singly even self-dual codes of length* 40 *with shadows of minimum weight* 4.

In Table 3, we list the numbers $N(\#\operatorname{Aut}, R)$ of inequivalent extremal singly even self-dual codes with automorphism groups of order $\#\operatorname{Aut}$ and covering radii R for $\beta = 1, 2, \ldots, 8$.

3.4 Another approach and weight enumerator $W_{40,C,0}$

The classification of extremal self-dual codes of length 40 was also completed by an approach which does not depend on the weight enumerators. As a consequence, we have a classification of extremal singly even self-dual codes with weight enumerator $W_{40,C,0}$, which is the remaining case. Here we describe how such a classification was done.

From the self-dual codes of length 38 and minimum weights 6 and 8, we complete a classification of the extremal self-dual codes of length 40, using the algorithm presented in [9], noting that a classification of self-dual codes of length 38 was done in [9]. We emphasize that the used algorithm has a better way to deal with equivalence classes and it gives as output exactly one representative of every equivalence class. The constructive part of the algorithm is not different from the other recursive constructions of self-dual codes, which were listed in [2], but to take only one representative of any equivalence class, we used a completely different manner. Its special feature is that practically there is not equivalence test for the objects. Algorithms of this type are known as isomorph-free generation [26].

The algorithm for isomorph-free generation solves two main problems. The first one is to find only inequivalent objects (in our case extremal self-dual codes of length 40) using a basic object B from the previous step (in our case a self-dual code of length 38 and minimum weight 6 or 8). It is easy to solve this by defining an action of the automorphism group $\operatorname{Aut}(B)$ on

Table 3: $(\#\operatorname{Aut}, R, N(\#\operatorname{Aut}, R))$ for $\beta = 1, 2, \ldots, 8$

$(\#\operatorname{Aut}, R, N(\#\operatorname{Aut}, R))$					
$\beta = 1$					
$(1, 7, 370397)$	$(1, 8, 4235394)$	$(2, 7, 8663)$	$(2, 8, 53572)$	$(3, 7, 38)$	$(3, 8, 302)$
$(4, 7, 908)$	$(4, 8, 3965)$	$(6, 7, 21)$	$(6, 8, 75)$	$(8, 7, 153)$	$(8, 8, 645)$
$(12, 7, 4)$	$(12, 8, 51)$	$(14, 7, 1)$	$(16, 7, 98)$	$(16, 8, 160)$	$(18, 7, 1)$
$(18, 8, 2)$	$(21, 8, 1)$	$(24, 7, 5)$	$(24, 8, 25)$	$(32, 7, 47)$	$(32, 8, 45)$
$(36, 8, 4)$	$(48, 7, 4)$	$(48, 8, 4)$	$(64, 7, 3)$	$(64, 8, 3)$	$(72, 8, 4)$
$(96, 7, 2)$	$(96, 8, 3)$	$(128, 7, 3)$	$(192, 8, 2)$	$(1008, 8, 1)$	$(1728, 7, 1)$
$(4032, 8, 1)$					
$\beta = 2$					
$(1, 7, 96666)$	$(1, 8, 1359341)$	$(2, 7, 5464)$	$(2, 8, 39474)$	$(3, 7, 10)$	$(3, 8, 117)$
$(4, 7, 932)$	$(4, 8, 6042)$	$(6, 7, 5)$	$(6, 8, 76)$	$(8, 7, 167)$	$(8, 8, 1760)$
$(12, 7, 10)$	$(12, 8, 34)$	$(16, 7, 108)$	$(16, 8, 741)$	$(24, 7, 2)$	$(24, 8, 16)$
$(32, 7, 51)$	$(32, 8, 322)$	$(48, 8, 15)$	$(64, 7, 9)$	$(64, 8, 208)$	$(96, 7, 1)$
$(96, 8, 7)$	$(128, 7, 1)$	$(128, 8, 106)$	$(144, 8, 1)$	$(192, 8, 6)$	$(256, 7, 3)$
$(256, 8, 52)$	$(288, 8, 1)$	$(384, 8, 4)$	$(512, 8, 24)$	$(768, 7, 1)$	$(768, 8, 7)$
$(1024, 7, 1)$	$(1024, 8, 12)$	$(1536, 8, 2)$	$(2048, 7, 1)$	$(2048, 8, 12)$	$(4096, 8, 5)$
$(4608, 8, 1)$	$(6144, 8, 1)$	$(8192, 8, 1)$	$(12288, 8, 2)$	$(16384, 8, 2)$	$(98304, 7, 1)$
$(196608, 8, 2)$					
$\beta = 3$					
$(1, 7, 13222)$	$(1, 8, 300610)$	$(2, 7, 2014)$	$(2, 8, 16954)$	$(3, 7, 8)$	$(3, 8, 46)$
$(4, 7, 482)$	$(4, 8, 2923)$	$(6, 7, 8)$	$(6, 8, 51)$	$(8, 7, 123)$	$(8, 8, 643)$
$(12, 7, 6)$	$(12, 8, 48)$	$(16, 7, 56)$	$(16, 8, 214)$	$(24, 7, 4)$	$(24, 8, 11)$
$(32, 7, 23)$	$(32, 8, 84)$	$(48, 7, 1)$	$(48, 8, 12)$	$(64, 7, 3)$	$(64, 8, 13)$
$(96, 7, 1)$	$(128, 8, 2)$	$(144, 7, 1)$	$(192, 7, 1)$	$(384, 8, 1)$	
$\beta = 4$					
$(1, 7, 708)$	$(1, 8, 51223)$	$(2, 7, 349)$	$(2, 8, 7605)$	$(3, 7, 4)$	$(3, 8, 42)$
$(4, 7, 132)$	$(4, 8, 2309)$	$(6, 7, 6)$	$(6, 8, 32)$	$(8, 7, 58)$	$(8, 8, 943)$
$(12, 7, 5)$	$(12, 8, 29)$	$(16, 7, 24)$	$(16, 8, 454)$	$(18, 7, 1)$	$(18, 8, 2)$
$(24, 7, 3)$	$(24, 8, 18)$	$(32, 7, 14)$	$(32, 8, 284)$	$(36, 8, 2)$	$(48, 8, 7)$
$(64, 7, 1)$	$(64, 8, 162)$	$(72, 8, 2)$	$(96, 7, 4)$	$(96, 8, 7)$	$(128, 7, 2)$
$(128, 8, 108)$	$(144, 8, 1)$	$(192, 7, 1)$	$(192, 8, 4)$	$(256, 7, 2)$	$(256, 8, 36)$
$(288, 7, 1)$	$(288, 8, 1)$	$(384, 8, 9)$	$(512, 7, 1)$	$(512, 8, 29)$	$(576, 8, 2)$
$(768, 8, 4)$	$(1024, 8, 12)$	$(1536, 8, 11)$	$(1728, 8, 1)$	$(2048, 8, 14)$	$(3072, 8, 3)$
$(4096, 8, 3)$	$(6144, 8, 3)$	$(8192, 8, 6)$	$(9216, 8, 1)$	$(16384, 8, 1)$	$(20736, 7, 1)$
$(49152, 7, 1)$	$(98304, 8, 2)$	$(294912, 8, 2)$			

Table 3: $(\#\operatorname{Aut}, R, N(\#\operatorname{Aut}, R))$ for $\beta = 1, 2, \ldots, 8$ (continued)

$(\#\operatorname{Aut}, R, N(\#\operatorname{Aut}, R))$					
$\beta = 5$					
$(1,7,51)$	$(1,8,6723)$	$(2,7,75)$	$(2,8,2498)$	$(3,8,14)$	$(4,7,47)$
$(4,8,974)$	$(6,7,1)$	$(6,8,12)$	$(8,7,20)$	$(8,8,348)$	$(10,8,5)$
$(12,7,5)$	$(12,8,19)$	$(16,7,11)$	$(16,8,119)$	$(24,8,8)$	$(32,7,8)$
$(32,8,42)$	$(48,8,5)$	$(64,7,2)$	$(64,8,11)$	$(96,8,1)$	$(120,8,2)$
$(128,7,1)$	$(128,8,3)$	$(144,8,1)$	$(192,8,1)$	$(320,7,1)$	$(384,8,1)$
$\beta = 6$					
$(1,8,430)$	$(2,7,9)$	$(2,8,676)$	$(3,8,1)$	$(4,7,8)$	$(4,8,424)$
$(6,8,5)$	$(8,7,8)$	$(8,8,268)$	$(12,7,1)$	$(12,8,9)$	$(16,7,7)$
$(16,8,173)$	$(24,8,6)$	$(32,7,3)$	$(32,8,110)$	$(48,7,1)$	$(48,8,6)$
$(64,7,2)$	$(64,8,84)$	$(72,8,1)$	$(96,7,1)$	$(96,8,4)$	$(128,7,2)$
$(128,8,70)$	$(144,7,1)$	$(192,7,1)$	$(256,8,22)$	$(288,7,1)$	$(288,8,1)$
$(384,8,4)$	$(512,7,1)$	$(512,8,29)$	$(768,8,6)$	$(1024,8,8)$	$(1536,8,2)$
$(2048,8,9)$	$(3072,8,4)$	$(6144,7,1)$	$(6144,8,5)$	$(8192,8,5)$	$(24576,8,3)$
$(49152,8,1)$					
$\beta = 7$					
$(4,8,109)$	$(8,7,1)$	$(8,8,138)$	$(12,8,4)$	$(16,7,2)$	$(16,8,79)$
$(24,7,1)$	$(24,8,6)$	$(32,7,1)$	$(32,8,19)$	$(48,8,8)$	$(64,7,1)$
$(64,8,13)$	$(72,8,2)$	$(96,7,1)$	$(96,8,8)$	$(128,8,1)$	$(144,8,1)$
$(192,7,1)$	$(192,8,1)$	$(288,7,1)$	$(384,7,1)$	$(384,8,2)$	$(576,8,2)$
$(1728,7,1)$	$(5184,8,1)$				
$\beta = 8$					
$(32,8,6)$	$(64,8,21)$	$(96,8,1)$	$(128,8,26)$	$(192,8,3)$	$(256,8,11)$
$(384,8,4)$	$(512,8,17)$	$(768,7,1)$	$(1024,7,1)$	$(1024,8,4)$	$(1536,8,5)$
$(2048,8,5)$	$(3072,8,4)$	$(4096,8,2)$	$(5376,8,1)$	$(8192,8,3)$	$(12288,8,1)$
$(16384,8,2)$	$(36864,8,1)$	$(688128,7,1)$			

the set of the objects constructed from B. For this construction, we use the method described in [20].

The second main problem is how to take only the inequivalent objects among already constructed ones (after solving the first problem). This problem and our solution are explained in details in [9]. We give here only the general idea. We use the concept for a canonical labeling map and a canonical representative of an equivalence class. We consider here the action of the symmetric group S_n on the set of all self-dual codes of length n. We fix a so called *canonical representative* for any equivalence class which is selected on the base of some specific conditions. The canonical representative

is intended to make easily a distinction among the equivalence classes. The function which maps any code C to the canonical representative of its equivalence class is called a *canonical representative map*. This map is realized by a proper algorithm which uses invariants. Using the canonical representative, we define an ordering of the coordinates of the code C. This ordering is unique only if $\# \operatorname{Aut}(C) = 1$. In the other cases there are $\# \operatorname{Aut}(C)$ such orderings. To take only the inequivalent codes we use a parent test for each code obtained in the first part of the algorithm. An example for such test is the following: A code passes the test if the added two coordinates during the construction are the biggest (last) two coordinates in the defined ordering.

Using the above algorithm, all inequivalent extremal doubly even self-dual codes as well as extremal singly even self-dual codes of length 40 were obtained. The calculations took about two months using four cores of a PC Intel i5 4 core processor. We have the following:

Theorem 3.7. *There are* 10200655 *inequivalent extremal singly even self-dual codes of length* 40.

As a summary, we list in Table 4 the numbers $N_{SE}^{\beta}(40)$ of inequivalent extremal singly even self-dual codes with weight enumerators $W_{40,C,\beta}$.

Table 4: Extremal singly even self-dual codes of length 40

β	$N_{SE}^{\beta}(40)$	β	$N_{SE}^{\beta}(40)$
0	3597997	5	11009
1	4674608	6	2413
2	1511827	7	405
3	337565	8	120
4	64692	10	19

For $\beta = 0$, we list in Table 5 the numbers $N(\# \operatorname{Aut}, R)$ of inequivalent extremal singly even self-dual codes with automorphism groups of order $\# \operatorname{Aut}$ and covering radii R. Since the shadow of C is a coset of C having minimum weight 8, we have that $R \geq 8$. It follows from the classification that there is no extremal singly even self-dual code with $R \geq 9$.

Table 5: $(\#\operatorname{Aut}, R, N(\#\operatorname{Aut}, R))$ for $\beta = 0$

$(\#\operatorname{Aut}, R, N(\#\operatorname{Aut}, R))$					
$(1, 8, 3542831)$	$(2, 8, 48796)$	$(3, 8, 222)$	$(4, 8, 4273)$	$(5, 8, 4)$	$(6, 8, 133)$
$(8, 8, 904)$	$(10, 8, 5)$	$(12, 8, 59)$	$(16, 8, 379)$	$(20, 8, 4)$	$(24, 8, 29)$
$(32, 8, 113)$	$(40, 8, 2)$	$(48, 8, 19)$	$(64, 8, 103)$	$(96, 8, 3)$	$(120, 8, 5)$
$(128, 8, 35)$	$(160, 8, 1)$	$(192, 8, 6)$	$(256, 8, 22)$	$(384, 8, 2)$	$(512, 8, 14)$
$(640, 8, 1)$	$(768, 8, 3)$	$(1024, 8, 6)$	$(1536, 8, 4)$	$(2048, 8, 7)$	$(3072, 8, 2)$
$(4096, 8, 2)$	$(6144, 8, 1)$	$(8192, 8, 1)$	$(12288, 8, 1)$	$(16384, 8, 2)$	$(20480, 8, 1)$
$(24576, 8, 1)$	$(491520, 8, 1)$				

3.5 Automorphism groups

Here we consider automorphism groups of extremal self-dual codes of length
40. It can be shown without the classification that if a prime p divides the
order of the automorphism group of an extremal self-dual code of length
40 then $p \in \{2, 3, 5, 7, 19\}$ (see [11]). By [6] and Theorem 3.7, there are
10214125 extremal self-dual codes of length 40. Their automorphism groups
are divided into 91 different orders. We present the number of the codes in
respect to the order of their automorphism group in Table 6.

The 9972575 codes (more than 97% of 10214125 codes) have a trivial
automorphism group (group of order 1). This means that only 228849 codes
have nontrivial automorphism groups. There are 189449 codes with auto-
morphism group of order 2. So the codes with automorphism group of order
1 or 2 are more than 99.61% of all inequivalent codes. This calculation sub-
stantiates some conjectures from [9] and very small number of the codes have
bigger automorphism groups.

Extremal singly even self-dual codes of length 40 having automorphisms
of odd prime order $p \geq 5$ were considered in [11]. Here we give the current
knowledge on the existence of such codes for $p \geq 3$.

- $p = 19$: No such code exists for this case.

- $p = 7$: Unfortunately, there is a mistake in [11] because there are six in-
  equivalent extremal singly even self-dual codes of length 40 with an au-
  tomorphism of order 7 - two codes with weight enumerator $W_{40,C,8}$ and
  automorphism groups of orders $688128 = 2^{15} \cdot 21$ and $5376 = 2^8 \cdot 21$, and

four codes with weight enumerator $W_{40,C,1}$ and automorphism groups of orders $4032 = 2^6 \cdot 63$, $1008 = 2^4 \cdot 63$, 21 and 14. Bouyuklieva and Yorgov [11] missed four of the codes because they had to consider five different supports for the codeword of weight 2 in $\pi(F_\sigma(C))$, namely $\{1,6\}$, $\{2,6\}$, $\{3,6\}$, $\{4,6\}$ and $\{5,6\}$. So the codes with weight enumerator $W_{40,C,8}$ could be constructed as a combination of the matrix H_4 and $\pi(F_\sigma(C))$ with $\{2,6\}$ as a support of the weight 2 vector, and H_3 with $\{4,6\}$ as this support. The additional two codes with weight enumerator $W_{40,C,1}$ are obtained from H_1 with $\{2,6\}$ and H_2 with $\{3,6\}$ (see [11] for the details of the construction and for the matrices H_1, H_2, H_3, H_4).

- $p = 5$: Exactly 39 inequivalent singly even self-dual codes of length 40 have an automorphism of order 5 - two codes more than it is stated in [11]. The authors missed there two codes with weight enumerator $W_{40,C,0}$.

- $p = 3$: Exactly 1986 inequivalent extremal singly even self-dual codes of length 40 have an automorphism of order 3.

We formulate these corrections on the cases $p = 5$ and 7.

Corollary 3.8. *There are exactly* 6 *and* 39 *inequivalent extremal singly even self-dual codes of length* 40 *having an automorphism of order* 7 *and* 5*, respectively.*

3.6   Some observations

By the sphere-covering bound (see [3]), the covering radius of a self-dual code of length 40 is at least 6. From Tables 3 and 5, there are 501337 inequivalent extremal singly even self-dual codes of length 40 with covering radius 7, and there is no extremal singly even self-dual code with covering radius 6. Note that there are only two inequivalent extremal doubly even self-dual codes with covering radius 7, and there is no extremal doubly even self-dual code with covering radius 6 [6]. By the Delsarte bound (see [3]), the covering radius of an extremal doubly even self-dual code of length 40 is at most 8. It follows from the classification that the covering radius of an extremal singly even self-dual code of the same length is also at most 8.

Table 6: Automorphism groups of the extremal self-dual codes of length 40

# Aut(C)	singly even	doubly even	# Aut(C)	singly even	doubly even	# Aut(C)	singly even	doubly even
# Aut$(C) = 2^s$, $s = 0, 1, \ldots, 16, 18$								
1	9977596	10400	64	639	75	4096	12	1
2	186149	3538	128	360	46	8192	16	–
4	23528	1189	256	148	21	16384	8	1
8	6179	459	512	115	16	32768	1	1
16	2625	233	1024	44	3	65536	1	1
32	1172	70	2048	48	4	262144	1	–
# Aut$(C) = 2^s \cdot 3$, $s = 0, 1, \ldots, 16, 18$								
3	804	43	192	27	12	12288	5	2
6	425	68	384	28	12	24576	4	–
12	284	80	768	22	7	49152	5	3
24	134	41	1536	24	10	98304	3	–
48	82	34	3072	13	3	196608	2	–
96	44	12	6144	11	7	786432	1	1
# Aut$(C) = 2^s \cdot 3^m$, $s = 1, \ldots, 17$, $m = 2, 3, 4$								
18	6	1	1296	–	1	20736	1	1
36	6	1	1728	3	1	36864	1	–
72	9	4	4608	1	2	110592	–	1
144	6	4	5184	1	–	147456	1	1
288	6	4	9216	1	1	294912	2	–
576	4	3	18432	1	1	1179648	1	–
# Aut$(C) = 2^s \cdot 3^m \cdot 5$, $s = 0, 1, \ldots, 18$, $m = 0, 1, 2$								
5	4	2	240	–	2	245760	1	1
10	10	8	320	1	1	327680	1	–
20	4	4	640	1	–	491520	1	–
30	–	2	720	–	2	737280	1	1
40	2	5	1920	–	1	983040	–	1
60	–	2	3840	–	1	1474560	1	1
120	7	5	20480	2	1	11796480	1	–
160	1	1	61440	–	1			
# Aut$(C) = 2^s \cdot 3^m \cdot 7$, $s = 0, 1, \ldots, 18$, $m = 0, 1, 2$								
14	1	–	2688	–	1	688128	1	–
21	1	–	4032	1	–	5505024	–	1
1008	1	–	5376	1	1	8257536	–	1
# Aut$(C) = 19q$, $q = 2, 6, 360$								
38	–	1	114	–	1	6840	–	1
# Aut$(C) > 40000000$								
			44236800	1	1	82575360	–	1

Let $N_{DE}(n)$ and $N_{SE}(n)$ be the numbers of inequivalent extremal doubly even self-dual codes and singly even self-dual codes of length $n \equiv 0 \pmod 8$ and minimum weight $4\lfloor n/24 \rfloor + 4$, respectively. Then it holds that

$$(N_{DE}(8), N_{SE}(8)) = (1, 0),$$
$$(N_{DE}(16), N_{SE}(16)) = (2, 1),$$
$$(N_{DE}(24), N_{SE}(24)) = (1, 0),$$
$$(N_{DE}(32), N_{SE}(32)) = (5, 3),$$
$$(N_{DE}(40), N_{SE}(40)) = (16470, 10200655).$$

It follows that 40 is the smallest length n ($\equiv 0 \pmod 8$) with $N_{DE}(n) < N_{SE}(n)$.

4 Odd unimodular lattices in dimension 40

For odd unimodular lattices, we consider a situation which is similar to that for singly even self-dual codes given in Section 3.2. We show that the number of vectors of norm 2 in the shadow of an extremal odd unimodular lattice in dimension 40 is at most 80. We also give a classification of extremal odd unimodular lattices in dimension 40 with shadows having 80 vectors of norm 2.

4.1 Frames of Type A, B and C

Let L be an even integral lattice in dimension n. Let $e_1, e_2, \ldots, e_n$ be vectors of $\mathbb{R}^n$ satisfying

$$(e_i, e_j) = 2\delta_{ij} \text{ and } e_i \pm e_j \in L \ (1 \le i, j \le n), \tag{6}$$

where δ_{ij} is the Kronecker delta. If the vectors $e_1, e_2, \ldots, e_n$ satisfy the following condition

$$e_1, e_2, \ldots, e_n \in L, \tag{7}$$

$$e_1, e_2, \ldots, e_n \notin L \text{ but } \frac{1}{2}\sum_{i=1}^{n} \mathbb{Z}e_i \supset L, \tag{8}$$

$$\frac{1}{2}\sum_{i=1}^{n} \mathbb{Z}e_i \not\supset L, \tag{9}$$

then the set of these vectors is called *a frame* of Type A, B and C related to L, respectively [25].

Let D be a doubly even code of length $n \equiv 0 \pmod 8$. Let $e_1, e_2, \ldots, e_n$ be vectors of $\mathbb{R}^n$ satisfying $(e_i, e_j) = 2\delta_{ij}$ for $1 \le i, j \le n$. Set $\Lambda = \sum_{i=1}^{n} \mathbb{Z}e_i$, $\Lambda_\varepsilon = \{\sum_{i=1}^{n} x_i e_i \mid x_i \in \mathbb{Z}, \sum_{i=1}^{n} x_i \equiv \varepsilon \pmod 2\}$ $(\varepsilon = 0, 1)$. The following lattices are defined in [25]

$$L_A(D) = \bigcup_{x \in D} \left(\Lambda + \frac{1}{2}e_x\right),$$

$$L_B(D) = \bigcup_{x \in D} \left(\Lambda_0 + \frac{1}{2}e_x\right),$$

$$L_C(D) = \bigcup_{x \in D} \left\{\left(\Lambda_0 + \frac{1}{2}e_x\right) \bigcup \left(\Lambda_\varepsilon + \frac{1}{2}e_x + \frac{1}{4}e_{\mathbf{1}}\right)\right\} \quad (\varepsilon \equiv n/8 \pmod 2),$$

where $e_x = \sum_{i \in \mathrm{supp}(x)} e_i$ and $\mathrm{supp}(x)$ denotes the support of x. These lattices and their relationships with frames of Type A, B and C are investigated in [25]. For example, if D is a doubly even self-dual code of length 40 and minimum weight 4 (resp. 8), then $L_C(D)$ is an even unimodular lattice with minimum norm 2 (resp. 4) [25]. In addition, the following result is an important tool in this section.

Lemma 4.1 ([25, Theorem 3]). *For* U = A, B, C, *a mapping* $D \mapsto L_U(D)$ *gives a one-to-one correspondence between equivalence classes of doubly even codes D of length n and isomorphism classes of even lattices in dimension n with related frames of Type* U, *if $n > 16$ for* U = B *and if $n > 32$ for* U = C.

As an example of the above lemma, we directly have the following result from the classification of doubly even self-dual codes of length 40 in [6].

Remark 4.2. There are 94343 non-isomorphic extremal even unimodular lattices in dimension 40 with related frames of Type C, 16470 of which are extremal.

4.2 Theta series

Lemma 4.3. *Let L be an odd unimodular lattice in dimension $n \equiv 0 \pmod 4$. Suppose that L and its shadow S have minimum norms ≥ 4 and 2, respectively. Then all vectors of norm 2 in S are contained in one of L_1 and L_3.*

Proof. Suppose that $x \in L_1$. Since L_0^*/L_0 is isomorphic to the Klein 4-group (see e.g. [18, Lemma 1]), $-x \in L_1$. Hence, it is sufficient to consider the case that S contains at least 4 vectors of norm 2. Then there are vectors x, y of norm 2 in S such that $x \neq y$ and $x \neq -y$. Since $x - y \in L$,

$$(x - y, x - y) = 4 - 2(x, y) \geq 4. \tag{10}$$

We may assume without loss of generality that $(x, y) \geq 0$, since $-x \in L_1$ for $x \in L_1$. If $y \in L_3$, then, by [18, Lemma 2], $(x, y) \in \frac{1}{2} + \mathbb{Z}$. This contradicts (10). $\qquad\square$

By [15, (2) and (3)], one can determine the possible theta series $\theta_{40,L,\alpha}$ and $\theta_{40,S,\alpha}$ of an extremal odd unimodular lattice L and its shadow S

$$\begin{cases} \theta_{40,L,\alpha} = 1 + (19120 + 256\alpha)q^4 + (1376256 - 4096\alpha)q^5 + \cdots, \\ \theta_{40,S,\alpha} = \alpha q^2 + (40960 - 56\alpha)q^4 + (87818240 + 1500\alpha)q^6 + \cdots, \end{cases}$$

respectively, where α is an integer. Moreover, we have the following restriction on α.

Lemma 4.4. α *is even with* $0 \leq \alpha \leq 80$.

Proof. Denote by S_2 the set of all vectors of norm 2 in S. By the proof of Lemma 4.3, α is even and the set S_2 is written as

$$S_2 = T \cup (-T)$$

satisfying that $(x, y) = 0$ for $x, y \in T$ with $x \neq y$. Hence, $\#T \leq 40$, and L_1 has at most 80 vectors of norm 2. Therefore, $\alpha \leq 80$. $\qquad\square$

Lemma 4.5. *Let L be an extremal odd unimodular lattice in dimension* 40 *with theta series $\theta_{40,L,\alpha}$. Then one of $L_0 \cup L_1$ and $L_0 \cup L_3$ is an extremal even unimodular lattice and the remaining one is an even unimodular lattice containing α vectors of norm* 2.

Proof. Follows from Lemma 4.3 and $\theta_{40,S,\alpha}$. $\qquad\square$

4.3 Lattices with theta series $\theta_{40,L,80}$

Now we suppose that L is an extremal odd unimodular lattice in dimension 40 with shadow S having exactly 80 vectors of norm 2.

Lemma 4.6. *There is a frame of Type* B *related to the even sublattice L_0.*

Proof. By the proof of Lemma 4.4, the set of all vectors of norm 2 in S may be written as $T \cup (-T)$, where $T = \{e_1, e_2, \ldots, e_{40}\}$ satisfying the condition (6). Then

$$\left(\frac{1}{2} \sum_{i=1}^{40} \mathbb{Z}e_i \right)^* = \sum_{i=1}^{40} \mathbb{Z}e_i \subset L \cup S = L_0^*.$$

Hence, $e_1, e_2, \ldots, e_{40}$ satisfy the condition (8). $\qquad\qquad\square$

We are in a position to state and prove the main result of this section.

Theorem 4.7. *There are* 16470 *non-isomorphic extremal odd unimodular lattices in dimension* 40 *with theta series* $\theta_{40,L,80}$.

Proof. Let L be an extremal odd unimodular lattice in dimension 40 with theta series $\theta_{40,L,80}$. By Lemma 4.6, there is a frame of Type B related to the even sublattice L_0. Hence, by Theorem 1 in [25], there is a doubly even code C of length 40 such that $L_0 \cong L_B(C)$. Since $L_B(C)$ is a sublattice of index 2 of an even unimodular lattice $L_A(C)$, C must be self-dual. Since $L_B(C)$ has minimum norm 4, C has minimum weight 8, that is, extremal.

Moreover, by Lemma 4.1, a mapping $C \mapsto L_B(C)$ gives a one-to-one correspondence between equivalence classes of extremal doubly even self-dual codes C of length 40 and isomorphism classes of even sublattices of extremal odd unimodular lattices in dimension 40 with theta series $\theta_{40,L,80}$. There are 16470 inequivalent extremal doubly even self-dual codes of length 40 [6]. The result follows. $\qquad\qquad\square$

Remark 4.8. A similar argument can be found in [15] for dimension $n = 32$. There is a one-to-one correspondence between equivalence classes of extremal doubly even self-dual codes of length 32 and isomorphism classes of even sublattices of extremal odd unimodular lattices in dimension 32 with shadows having exactly 64 vectors of norm 2. In this dimension, the shadow of any extremal odd unimodular lattice has 64 vectors of norm 2. By Lemma 4.3, the 64 vectors of norm 2 of the shadow are contained in one of L_1 and L_3. It is incorrectly reported in [15, p. 360] that each L_i has 32 vectors of norm 2 $(i = 1, 3)$.

Now we give characterizations of the set of vectors of minimum norm in extremal odd unimodular lattices with theta series $\theta_{40,L,80}$. By the above theorem, the even sublattice of such a lattice is written by $L_B(C)$ using some extremal doubly even self-dual code C of length 40.

Proposition 4.9. *The set $L_B(C)_4$ of vectors of norm 4 in $L_B(C)$ is given by*

$$\{\pm e_i \pm e_j \mid i \neq j\} \cup \Big(\bigcup_{x \in C_8} \Big\{ \frac{1}{2} e_x - \sum_{y \in X} e_y \mid X \subset \mathrm{supp}(x), \#X \in 2\mathbb{Z} \Big\} \Big),$$

where C_8 is the set of codewords of weight 8 in C.

Proof. Since $\#C_8 = 285$ [27], it follows that $\#L_B(C)_4 = 2^2 \binom{40}{2} + 285 \cdot 2^7 = 39600$, which is the same as the number of vectors of norm 4 in $L_B(C)$. $\square$

By Lemmas 4.3 and 4.5, the even unimodular neighbor $L_0 \cup L_3$ is extremal. Then $L_0 \cup L_3$ is written as $L_C(C)$, where $L_0 = L_B(C)$ and C is some extremal doubly even self-dual code C of length 40 (see Remark 4.2). An extremal even unimodular lattice in dimension 40 has the following theta series $1 + 39600q^4 + 93043200q^6 + \cdots$. By the above proposition, the set of vectors of norm 4 in $L_C(C)$ is also given by $L_B(C)_4$. It is known that the set of vectors of each norm in an extremal even unimodular lattice in dimension 40 forms a spherical 3-design (see [5] for a recent survey on this subject). Hence, we have the following:

Proposition 4.10. *The set of vectors of minimum norm in an extremal odd unimodular lattice in dimension 40 with theta series $\theta_{40,L,80}$ forms a spherical 3-design.*

5 Extremal self-dual $\mathbb{Z}_4$-codes

Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code of length n and minimum Euclidean weight $d_E(\mathcal{C})$. Then the following lattice

$$A_4(\mathcal{C}) = \frac{1}{2}\{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid (x_1 \bmod 4, \ldots, x_n \bmod 4) \in \mathcal{C}\}$$

is a unimodular lattice in dimension n having minimum norm $\min\{4, d_E(\mathcal{C})/4\}$. In addition, $\mathcal{C}$ is Type II if and only if $A_4(\mathcal{C})$ is even [7]. A set $\{f_1, \ldots, f_n\}$ of n

vectors $f_1, \ldots, f_n$ of a unimodular lattice L in dimension n with $(f_i, f_j) = 4\delta_{ij}$ is called an *orthogonal frame of norm* 4 (a 4-frame for short) of L. It is known that L has an orthogonal frame of norm 4 if and only if there is a self-dual $\mathbb{Z}_4$-code $\mathcal{C}$ with $L \cong A_4(\mathcal{C})$.

Lemma 5.1. *Suppose that n is even. Let L be an even (resp. odd) unimodular lattice in dimension n such that there are vectors $e_1, e_2, \ldots, e_n$ satisfying the condition that $(e_i, e_j) = 2\delta_{ij}$ and $e_i \pm e_j \in L$ $(1 \le i, j \le n)$ which is the same condition as (6). Then L contains an orthogonal frame of norm 4 and there is a Type II (resp. Type I) $\mathbb{Z}_4$-code $\mathcal{C}$ of length n with $A_4(\mathcal{C}) \cong L$.*

Proof. Follows from that $\{e_{2i-1} + e_{2i}, e_{2i-1} - e_{2i} \mid i = 1, 2, \ldots, n/2\}$ is an orthogonal frame of norm 4 of L. $\qquad\square$

We consider the existence of extremal self-dual $\mathbb{Z}_4$-codes.

Proposition 5.2. *There are at least 16470 inequivalent extremal Type II $\mathbb{Z}_4$-codes of length 40. There are at least 16470 inequivalent extremal Type I $\mathbb{Z}_4$-codes of length 40.*

Proof. Since the two cases are similar, we give details only for Type I $\mathbb{Z}_4$-codes. By Theorem 4.7, there are 16470 non-isomorphic extremal odd unimodular lattices L_i $(i = 1, 2, \ldots, 16470)$ in dimension 40 containing $e_1, \ldots, e_{40}$ satisfying the condition of Lemma 5.1. Hence, there is an extremal Type I $\mathbb{Z}_4$-code $\mathcal{C}_i$ of length 40 with $A_4(\mathcal{C}_i) \cong L_i$. Since $L_1, \ldots, L_{16470}$ are non-isomorphic, $\mathcal{C}_1, \ldots, \mathcal{C}_{16470}$ are inequivalent. $\qquad\square$

Using the method given in [29], we found 16 new extremal Type I $\mathbb{Z}_4$-codes $\mathcal{D}_i$ $(i = 1, 2, \ldots, 16)$ of length 40, where the extremal odd unimodular lattices $A_4(\mathcal{D}_i)$ have theta series $\theta_{40,L,4k}$ $(k = 0, 1, \ldots, 14, 16)$. Then we have the following:

Proposition 5.3. *There is an extremal odd unimodular lattice with theta series $\theta_{40,L,4k}$ for $k \in \{0, 1, \ldots, 14, 16, 20\}$.*

Generator matrices for all codes $\mathcal{D}_i$ can be obtained electronically from "`http://sci.kj.yamagata-u.ac.jp/~mharada/Paper/z4-40.txt`".

References

[1] C. Aguilar-Melchor and P. Gaborit, On the classification of extremal $[36, 18, 8]$ binary self-dual codes, *IEEE Trans. Inform. Theory* **54** (2008), 4743–4750.

[2] C. Aguilar-Melchor, P. Gaborit, J.-L. Kim, L. Sok and P. Solé, Classification of extremal and *s*-extremal binary self-dual codes of length 38, *IEEE Trans. Inform. Theory* **58** (2012), 2253–2262.

[3] E.F. Assmus, Jr. and V. Pless, On the covering radius of extremal self-dual codes, *IEEE Trans. Inform. Theory* **29** (1983), 359–363.

[4] C. Bachoc and P. Gaborit, On extremal additive $\mathbb{F}_4$ codes of length 10 to 18, *J. Theór. Nombres Bordeaux* **12** (2000), 255–271.

[5] E. Bannai and Ets. Bannai, A survey on spherical designs and algebraic combinatorics on spheres, *European J. Combin.* **30** (2009), 1392–1425.

[6] K. Betsumiya, M. Harada and A. Munemasa, A complete classification of doubly even self-dual codes of length 40, *Electronic J. Combin.* **19** (2012), #P18 (12 pp.).

[7] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* **43** (1997), 969–976.

[8] W. Bosma, J.J. Cannon, C. Fieker and A. Steel, *Handbook of Magma Functions (Edition 2.17)*, 2010, 5117 pages.

[9] S. Bouyuklieva and I. Bouyukliev, An algorithm for classification of binary self-dual codes, *IEEE Trans. Inform. Theory* **58** (2012), 3933–3940.

[10] R. Brualdi and V. Pless, Weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **37** (1991), 1222–1225.

[11] S. Buyuklieva and V. Yorgov, Singly-even self-dual codes of length 40, *Des. Codes, Cryptogr.* **9** (1996), 131–141.

[12] A.R. Calderbank, E.R. Rains, P.W. Shor and N.J.A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory* **44** (1998), 1369–1387.

[13] J.H. Conway, V. Pless and N.J.A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *J. Combin. Theory Ser. A* **60** (1992), 183–195.

[14] 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.

[15] J.H. Conway and N.J.A. Sloane, A note on optimal unimodular lattices, *J. Number Theory* **72** (1998), 357–362.

[16] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups (3rd ed.)*, Springer-Verlag, New York, 1999.

[17] L.E. Danielsen and M.G. Parker, On the classification of all self-dual additive codes over GF(4) of length up to 12, *J. Combin. Theory Ser. A* **113** (2006), 1351–1367.

[18] S.T. Dougherty, M. Harada and P. Solé, Shadow lattices and shadow codes, *Disc. Math.* **219** (2000), 49–64.

[19] M. Harada and A. Munemasa, Some restrictions on weight enumerators of singly even self-dual codes, *IEEE Trans. Inform. Theory* **52** (2006), 1266–1269.

[20] M. Harada and A. Munemasa, Classification of self-dual codes of length 36, *Adv. Math. Commun.* **6** (2012), 229–235.

[21] M. Harada and A. Munemasa, Database of Self-Dual Codes, Available online at `http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm`.

[22] M. Harada and M. Ozeki, Extremal self-dual codes with the smallest covering radius, *Disc. Math.* **215** (2000), 271–281.

[23] M. Harada, P. Solé and P. Gaborit, Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey, Algebras and combinatorics (Hong Kong, 1997), 255–275, Springer, Singapore, 1999.

[24] G. Höhn, Self-dual codes over the Kleinian four group, *Math. Ann.* **327** (2003), 227–255.

[25] M. Kitazume, T. Kondo and I. Miyamoto, Even lattices and doubly even codes, *J. Math. Soc. Japan* **43** (1991), 67–87.

[26] B. D. McKay, Isomorph-free exhaustive generation, *J. Algorithms* **26** (1998), 306–324.

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

[28] M. Ozeki, Jacobi polynomials for singly even self-dual codes and the covering radius problems, *IEEE Trans. Inform. Theory* **48** (2002), 547–557.

[29] V. Pless, J. Leon and J. Fields, All $\mathbb{Z}_4$ codes of Type II and length 16 are known, *J. Combin. Theory Ser. A* **78** (1997), 32–50.

[30] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory Ser. A* **18** (1975), 313–335.

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

[32] E. Rains and N.J.A. Sloane, The shadow theory of modular and unimodular lattices, *J. Number Theory* **73** (1998), 359–389.

[33] E. Rains and N.J.A. Sloane, "Self-dual codes," Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 177–294.

[34] H. Shimakura, On isomorphism problems for vertex operator algebras associated with even lattices, *Proc. Amer. Math. Soc.* **140** (2012), 3333–3348.

[35] V.Y. Yorgov, Binary self-dual codes with automorphisms of odd order, *Problems Inform. Transmission* **19** (1983), 260–270; translated from *Probl. Peredachi Inf.* **19** (1983), 11–24 (Russian).