Hadamard Matrices of Orders 60 and 64 with Automorphisms of Orders 29 and 31

Makoto Araya[a] Masaaki Harada[b] Vladimir D. Tonchev[c]

Submitted: Jul 25, 2023; Accepted: Feb 10, 2024; Published: Feb 23, 2024

Abstract

A classification of Hadamard matrices of order $2p + 2$ with an automorphism of order p is given for $p = 29$ and 31. The ternary self-dual codes spanned by the newly found Hadamard matrices of order 60 with an automorphism of order 29 are computed, as well as the binary doubly even self-dual codes of length 120 with generator matrices defined by related Hadamard designs. Several new ternary near-extremal self-dual codes, as well as binary near-extremal doubly even self-dual codes with previously unknown weight enumerators are found.

Mathematics Subject Classifications: 05B05, 05B20, 94B05

1 Introduction

We assume familiarity with basic notions from error-correcting codes, combinatorial designs and Hadamard matrices [5], [8], [17] and [32]. Hadamard matrices appear in many research areas of mathematics and practical applications (see e.g., [16] and [28]).

It is known that for every odd prime p there exists a Hadamard matrix of order $2p+2$ with an automorphism of order p, found by Paley [26], and known in the combinatorial literature as the Paley-Hadamard matrix of type II. If p is an odd prime such that $p \equiv -1 \pmod 3$ then the Paley-Hadamard matrix of type II of order $2p+2$ is a generator matrix of a Pless symmetry code [27], being a ternary self-dual code of length $2p + 2$. In the context of ternary codes, we consider the elements $0, 1, -1$ of $\mathbb{Z}$ as the elements $0, 1, 2$ of the finite field $\mathbb{F}_3$ of order 3. By the Assmus–Mattson theorem [4], the Pless symmetry codes of length $2p+2$ for $p = 5, 11, 17, 23$ and 29 are ternary extremal self-dual codes that support 5-designs [27]. The ternary extended quadratic residue codes of length $2p + 2$

[a] Department of Computer Science, Shizuoka University, Hamamatsu 432–8011, Japan (araya@inf.shizuoka.ac.jp).

[b] Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan (mharada@tohoku.ac.jp).

[b] Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, U.S.A. (tonchev@mtu.edu).

https://doi.org/10.37236/12249

are ternary extremal self-dual codes that support 5-designs for $p = 5, 11, 23$ and 29, and these codes have generator matrices, being Hadamard matrices of order $2p + 2$ with an automorphism of order p [33]. In 2013, Nebe and Villar [25] gave a series of ternary self-dual codes of length $2p + 2$ for a prime $p \equiv 5 \pmod 8$. The self-dual codes are also ternary extremal self-dual codes that support 5-designs for $p = 5$ and 29 [25]. Recently, it was shown in [2] that these codes found by Nebe and Villar [25] also have generator matrices, being Hadamard matrices of order $2p+2$ for $p \equiv 5 \pmod{24}$. In addition, it was also shown that there are at least two inequivalent Hadamard matrices in a third ternary extremal self-dual code of length 60. This implies that there are at least four inequivalent Hadamard matrices of order 60 formed by codewords of weight 60 in the known three ternary extremal self-dual codes of length 60. In addition, each of these four Hadamard matrices has an automorphism of order 29. This motivates us to classify the Hadamard matrices of order 60 with an automorphism of order 29.

The Paley-Hadamard matrices of type II for $p = 3$ and $p = 5$ coincide with the unique, up to equivalence, Hadamard matrices of orders 8 and 12, respectively. The Hadamard matrices of order $2p + 2$ with an automorphism of orders $p = 7, 11, 13, 17, 19$ and 23 have been previously classified up to equivalence. A short summary on these matrices is given in Section 5, along with relevant references.

In this paper, we present the classification of Hadamard matrices of order $2p + 2$ with an automorphism of order p for the next two odd primes, $p = 29$ and 31. As an application, we compute the ternary self-dual codes and self-dual codes over the finite field $\mathbb{F}_5$ of order 5 spanned by the newly found Hadamard matrices of order 60 with an automorphism of order 29, as well as some binary doubly even self-dual codes of length 120 with generator matrices defined by related Hadamard designs. In addition, we study the binary self-dual codes defined by Hadamard designs arising from Hadamard matrices of order 64 with an automorphism of order 31.

This paper is organized as follows. In Section 2, we give definitions and some known results about Hadamard matrices, designs and codes used in this paper. We also review a method from [10], [29] and [31] for classifying Hadamard matrices of order $2p + 2$ with an automorphism of order p, where p is an odd prime.

In Section 3, we give the classification of Hadamard 2-$(59, 29, 14)$ designs with an automorphism of order 29 having one fixed point, and show that there are exactly 531 nonisomorphic such designs. Using these designs, we classify up to equivalence the Hadamard matrices of order 60 with an automorphism of order 29 and show that the total number of inequivalent Hadamard matrices with this property is 266. The ternary code and the code over $\mathbb{F}_5$ spanned by the rows of a Hadamard matrix of order 60 are self-dual. A computation of the minimum weights of the ternary codes spanned by the 266 inequivalent Hadamard matrices of order 60 with an automorphism of order 29 shows that only four of these matrices span a ternary extremal self-dual code, and these four matrices appear in the three known inequivalent ternary extremal self-dual codes. Among the remaining codes, several new ternary near-extremal self-dual codes with previously unknown weight enumerators are found. Self-dual codes over $\mathbb{F}_5$ spanned by the newly found Hadamard matrices of order 60 with an automorphism of order 29 are also computed. In addition, new binary near-extremal doubly even self-dual codes of length 120 with previously unknown weight enumerators are constructed from some of the Hadamard 2-$(59, 29, 14)$ designs with an automorphism of order 29.

In Section 4, we give the classification of Hadamard 2-$(63, 31, 15)$ designs with an automorphism of order 31 having one fixed point. There are exactly 826 non-isomorphic designs with this property. Using these designs, we classify the Hadamard matrices of order 64 with an automorphism of order 31, and show that there are 414 inequivalent matrices with this property. The extended code of a binary code of length 63 spanned by the incidence matrix of a Hadamard 2-$(63, 31, 15)$ design is doubly even. Among the extended codes of the 826 non-isomorphic 2-$(63, 31, 15)$ designs with an automorphism of order 31, there are 794 self-dual codes, and among these codes there are 28 inequivalent extremal doubly even self-dual codes of length 64 with an automorphism of order 31.

In Section 5, we give a summary of the classification of Hadamard 2-$(2p+1, p, (p-1)/2)$ designs with an automorphism of order p having one fixed point and Hadamard matrices of order $2p + 2$ with an automorphism of order p, where $p \leqslant 31$ is an odd prime.

All computer calculations in this paper were done by programs in the language C and programs in Magma [6].

2 Preliminaries

In this section, we give some definitions and known results about Hadamard matrices, designs and codes used in this paper. We also review a method from [10], [29] and [31] for classifying Hadamard matrices of order $2p + 2$ with an automorphism of order p, where p is an odd prime.

2.1 Hadamard matrices, designs and codes

Throughout this paper, I_n denotes the identity matrix of order n, A^T denotes the transpose of a matrix A, and J denotes the all-one matrix of appropriate size.

A *Hadamard* matrix H of order n is an $n \times n$ matrix whose entries are from $\{1, -1\}$ such that $HH^T = nI_n$. It is known that the order n is necessarily $1, 2$, or a multiple of 4. Two Hadamard matrices H and K are *equivalent* if there are $(1, -1, 0)$-monomial matrices P and Q with $K = PHQ^T$. An *automorphism* of a Hadamard matrix H is an equivalence of H to itself. The set of all automorphisms of H forms a group under composition called the *automorphism group* $\mathrm{Aut}(H)$ of H. For orders up to 32, all inequivalent Hadamard matrices are known (see [19] for order 32).

A t-(v, k, λ) *design* $\mathcal{D}$ is a pair of a set $\mathcal{P}$ of v points and a collection $\mathcal{B}$ of k-element subsets of $\mathcal{P}$ (called blocks) such that every t-element subset of $\mathcal{P}$ is contained in exactly λ blocks. Often a t-(v, k, λ) design is simply called a t-design. Two t-(v, k, λ) designs are *isomorphic* if there is a bijection between their point sets that maps the blocks of the first design into the blocks of the second design. An *automorphism* of a t-(v, k, λ) design $\mathcal{D}$ is any isomorphism of the design with itself and the set consisting of all automorphisms of $\mathcal{D}$ is called the *automorphism group* $\mathrm{Aut}(\mathcal{D})$ of $\mathcal{D}$. A t-design can be represented by its (block by point) *incidence matrix* $A = (a_{ij})$, where $a_{ij} = 1$ if the i-th block contains the j-th point and $a_{ij} = 0$ otherwise. The *complementary* (resp. *dual*) design of a t-design with incidence matrix A is the design with incidence matrix $J - A$ (resp. A^T). The blocks of a t-(v, k, λ) design $\mathcal{D}$ which contain a given point form a $(t-1)$-$(v-1, k-1, \lambda)$ design called a *derived* design of $\mathcal{D}$. A 2-design is called *symmetric* if the numbers of points and blocks are the same. A symmetric 2-$(4t+3, 2t+1, t)$ design is called a *Hadamard* 2-design.

Let $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ denote the finite field of order p, where p is a prime. An $[n, k]$ *code* C over $\mathbb{F}_p$ is a k-dimensional vector subspace of $\mathbb{F}_p^n$. In this paper, we consider codes over $\mathbb{F}_p$ ($p = 2, 3, 5$) only. A code over $\mathbb{F}_2$ and $\mathbb{F}_3$ are called *binary* and *ternary*, respectively. The parameters n and k are called the *length* and *dimension* of C, respectively. The *weight* $\mathrm{wt}(x)$ of a vector $x \in \mathbb{F}_p^n$ is the number of non-zero components of x. A vector of C is called a *codeword*. The minimum non-zero weight of all codewords in C is called the *minimum weight* of C. The *weight enumerator* of C is defined as the polynomial $\sum_{c \in C} y^{\mathrm{wt}(c)}$. Two codes C and C' over $\mathbb{F}_p$ are *equivalent* if there is a monomial matrix P over $\mathbb{F}_p$ with $C' = C \cdot P$, where $C \cdot P = \{xP \mid x \in C\}$.

The *dual* code $C^\perp$ of a code C of length n is defined as $C^\perp = \{x \in \mathbb{F}_p^n \mid x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y$ is the standard inner product. A code C is *self-dual* if $C = C^\perp$. A binary code C is *doubly even* if $\mathrm{wt}(x) \equiv 0 \pmod 4$ for all codewords $x \in C$. A binary doubly even self-dual code of length n exists if and only if n is divisible by eight. A ternary self-dual code of length n exists if and only if n is divisible by four. It was shown in [22] that the minimum weight d of a binary doubly even self-dual code (resp. ternary self-dual code) of length n is bounded by $d \leqslant 4\lfloor n/24 \rfloor + 4$ (resp. $d \leqslant 3\lfloor n/12 \rfloor + 3$). If $d = 4\lfloor n/24 \rfloor + 4$ (resp. $d = 4\lfloor n/24 \rfloor$), then the binary doubly even self-dual code is called *extremal* (resp. *near-extremal*). If $d = 3\lfloor n/12 \rfloor + 3$ (resp. $d = 3\lfloor n/12 \rfloor$), then the ternary self-dual code is called *extremal* (resp. *near-extremal*).

2.2 Hadamard matrices of order $2p+2$ with an automorphism of order p

A method for classifying Hadamard matrices of order $2p+2$ with an automorphism of order p, where p is an odd prime with $p > 3$, is given in [10], [29] and [31]. Using this method, a classification of Hadamard matrices of order $2p+2$ with an automorphism of order p was completed in [10], [29] and [31] for $p = 13, 17, 19, 23$. Here we review the method.

Let $p > 3$ be an odd prime. If a Hadamard matrix H of order $2p+2$ has an automorphism of order p, then H is constructed from a Hadamard 2-$(2p+1, p, (p-1)/2)$ design with an automorphism of order p having one fixed point. Note that this follows from a well-known connection between Hadamard matrices and symmetric designs, together with a bound on the number of fixed points [11, p. 82]. Let $\mathcal{D}$ be a Hadamard 2-$(2p+1, p, (p-1)/2)$ design with an automorphism of order p having one fixed point. Then $\mathcal{D}$ has an incidence matrix of the form:

$$A = \begin{pmatrix} M & N & \mathbf{1}^T \\ P & J - Q & \mathbf{0}^T \\ \mathbf{1} & \mathbf{0} & 0 \end{pmatrix}, \tag{1}$$

where M, N, P and Q are $p \times p$ circulant matrices satisfying

$$MJ = NJ = PJ = QJ = \frac{p-1}{2}J, \tag{2}$$

and $\mathbf{1}$ and $\mathbf{0}$ denote the all-one's vector and the zero vector, respectively. If the circulant matrices M, N, P and Q satisfy (2), the matrix A in (1) is an incidence matrix of a Hadamard 2-$(2p+1, p, (p-1)/2)$ design if and only if the following equalities hold:

$$MM^T + NN^T = \frac{p+1}{2}I_p + \frac{p-3}{2}J, \tag{3}$$

$$PP^T + QQ^T = \frac{p+1}{2}I_p + \frac{p-3}{2}J, \tag{4}$$

$$MM^T + PP^T = \frac{p+1}{2}I_p + \frac{p-3}{2}J, \tag{5}$$

$$NN^T + QQ^T = \frac{p+1}{2}I_p + \frac{p-3}{2}J, \tag{6}$$

$$MP^T = NQ^T. \tag{7}$$

Define a $(2p+2) \times (2p+2)$ $(1, -1)$-matrix

$$H = ((-1)^{b_{ij}}), \tag{8}$$

where

$$(b_{ij}) = \begin{pmatrix} 1 & \mathbf{1} & \mathbf{1} & 1 \\ \mathbf{1}^T & M & N & \mathbf{1}^T \\ \mathbf{1}^T & P & J-Q & \mathbf{0}^T \\ 1 & \mathbf{1} & \mathbf{0} & 0 \end{pmatrix}. \tag{9}$$

Then H is a Hadamard matrix of order $2p+2$ with an automorphism of order p.

In the next two sections, we use the above method to extend the classification of Hadamard matrices of order $2p+2$ with an automorphism of order $p = 29$ and $p = 31$.

3 Hadamard matrices of order 60 with an automorphism of order 29

Using the method given in Section 2.2, in this section, we give the classification of Hadamard 2-$(59, 29, 14)$ designs with an automorphism of order 29 having one fixed point. Using this classification, we give the classification of Hadamard matrices of order 60 with an automorphism of order 29. We construct ternary self-dual codes and self-dual codes over $\mathbb{F}_5$ from the Hadamard matrices of order 60. We also construct binary doubly even self-dual codes from the Hadamard 2-$(59, 29, 14)$ designs.

3.1 Hadamard 2-$(59, 29, 14)$ designs $D_{59,i}$ and Hadamard matrices $H_{60,i}$ of order 60

As a first step, we completed the classification of Hadamard 2-$(59, 29, 14)$ designs with an automorphism of order 29 having one fixed point. In order to classify such 2-designs, we consider incidence matrices of the form (1). By a program implemented in the language C using functions from the GNU Scientific Library (GSL), our exhaustive computer search found all circulant matrices M, N, P and Q satisfying the conditions (2)–(7). In this calculation, we identify 14-element subsets S_M, S_N, S_P and S_Q of $\{1, 2, \dots, 29\}$ with the supports of the first rows of M, N, P and Q, respectively. In this way, we found all Hadamard 2-$(59, 29, 14)$ designs with an automorphism of order 29 which need to be checked further for isomorphism. To test an isomorphism of Hadamard 2-$(59, 29, 14)$ designs, we employed the algorithm given in [24, p. 15, Theorem 1 (b)]. This algorithm considers coloured graphs corresponding to Hadamard 2-$(59, 29, 14)$ designs. In this calculation, we used NAUTY software library [23] for coloured graphs isomorphism testing. After isomorphism testing, we completed the classification of Hadamard 2-$(59, 29, 14)$ designs with an automorphism of order 29 having one fixed point.

Using this classification, all Hadamard matrices of order 60 with an automorphism of order 29 are obtained as matrices of the form (8) and (9), which need be checked further for equivalence. After equivalence testing, we completed the classification of Hadamard matrices of order 60 with an automorphism of order 29. This was done by using the MAGMA function `IsHadamardEquivalent`. Then we have the following:

Proposition 1. *There are* 531 *non-isomorphic Hadamard* 2-$(59, 29, 14)$ *designs with an automorphism of order* 29 *having one fixed point. There are* 266 *inequivalent Hadamard matrices of order* 60 *with an automorphism of order* 29*.*

The incidence matrices of the above 531 non-isomorphic Hadamard 2-$(59, 29, 14)$ designs $D_{59,i}$ $(i = 1, 2, \dots, 531)$ and the above 266 inequivalent Hadamard matrices $H_{60,i}$ $(i = 1, 2, \dots, 266)$ of order 60 can be obtained electronically from [3].

The automorphism group orders $|\operatorname{Aut}(D_{59,i})|$ of $D_{59,i}$ were computed with the MAGMA function `AutomorphismGroup`, and are listed in Table 1.

Table 1: Orders of the automorphism groups of $D_{59,i}$

$\lvert\operatorname{Aut}(D_{59,i})\rvert$	i
$29 \cdot 59$	24
$2 \cdot 7 \cdot 29$	531
$7 \cdot 29$	$527, 528, 529, 530$
29	others

The automorphism group orders $|\operatorname{Aut}(H_{60,i})|$ of $H_{60,i}$ were computed with the MAGMA function `HadamardAutomorphismGroup`, and are listed in Table 2.

3.2 Ternary self-dual codes $C_3(H_{60,i})$

Let H be a Hadamard matrix of order 60. We denote by $C_3(H)$ the ternary code generated by the rows of H. In the context of ternary codes, we consider the elements $0, 1, -1$ of $\mathbb{Z}$ as the elements $0, 1, 2$ of $\mathbb{F}_3$, respectively. It is trivial that if H and H' are equivalent Hadamard matrices of order 60 then $C_3(H) \cong C_3(H')$. Since 3 divides 60 and 3^2 does

Table 2: Orders of the automorphism groups of $H_{60,i}$

$\lvert \mathrm{Aut}(H_{60,i}) \rvert$	i
$2^3 \cdot 3 \cdot 5 \cdot 29 \cdot 59$	21
$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	266
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	264
$2^2 \cdot 7 \cdot 29$	265
$2^2 \cdot 29$	others

not divide 60, by considering the elementary divisors of $H_{60,i}$, it follows that the codes $C_3(H_{60,i})$ $(i = 1, 2, \dots, 266)$ are self-dual (see [20, Section IV]). The minimum weights d of $C_3(H_{60,i})$ were computed with the Magma function `MinimumWeight`, and are listed in Table 3. Using the Magma function `IsIsomorphic`, we found the following pairs (i, j) of equivalent codes $C_3(H_{60,i}) \cong C_3(H_{60,j})$:

$$\begin{aligned}(i,j) = &(20,146),(57,179),(75,103),(95,114),(96,190),\\ &(129,194),(132,140),(167,221),(223,241),(264,265),\end{aligned} \tag{10}$$

and there is no other pair of equivalent codes among $C_3(H_{60,i})$.

Table 3: Minimum weights of ternary self-dual codes $C_3(H_{60,i})$

d	i
9	$239, 256$
12	$2, 6, 7, 11, 12, 16, 20, 25, 26, 30, 31, 32, 33, 34, 36, 37, 40, 44, 45, 53, 54, 55, 56, 59, 62, 68, 75, 79, 81, 85, 87, 88, 93, 95, 96, 101, 103, 104, 105, 106, 111, 112, 113, 114, 115, 117, 120, 123, 125, 127, 129, 130, 132, 134, 135, 137, 140, 143, 144, 146, 148, 152, 154, 155, 160, 164, 165, 168, 172, 176, 180, 181, 182, 184, 186, 188, 189, 190, 191, 192, 194, 198, 200, 202, 203, 206, 212, 216, 217, 218, 219, 222, 223, 226, 227, 230, 234, 235, 241$ $244, 245, 250, 252, 261, 262, 263$
15	others
18	$21, 264, 265, 266$

It is trivial that an automorphism of order 29 of $H_{60,i}$ induces an automorphism of order 29 of $C_3(H_{60,i})$. There are three inequivalent ternary extremal self-dual codes of length 60 with an automorphism of order 29 [7]. The three codes are the extended quadratic residue code QR_{60}, the Pless symmetry code P_{60} and the code NV_{60} found by Nebe and Villar [25]. The codes QR_{60} and P_{60} contain a type I Paley-Hadamard matrix H_{P_I} and a type II Paley-Hadamard matrix $H_{P_{II}}$, respectively (see [33]). The code NV_{60} contains two inequivalent Hadamard matrices H_{NV_1} and H_{NV_2} of order 60 [2]. From Table 3, we have the following:

Proposition 2. *Let H be a Hadamard matrix H of order 60 with an automorphism of order 29 such that $C_3(H)$ generates a ternary extremal self-dual code. Then H is equivalent to one of the four inequivalent Hadamard matrices H_{P_I}, $H_{P_{II}}$, H_{NV_1} and H_{NV_2}.*

Table 4: Ternary near-extremal self-dual codes of length 60

β	i
2552	13
2668	$167, 221$
2697	$52, 138$
2726	$51, 100, 248$
2755	$243, 260$
2784	4
2813	$163, 201, 257$
2842	$61, 86, 92, 153, 254$
2871	$28, 39, 83, 108, 229$
2900	$38, 84, 118, 122, 142, 177, 224$
2929	$14, 23, 43, 76, 102, 170, 242, 255$
2958	$5, 42, 58, 73, 82, 91, 174, 211, 215$
2987	$24, 57, 77, 107, 133, 139, 179, 197, 208, 210, 238$
3016	$49, 69, 141, 171, 175, 231$
3045	$17, 78, 119, 157, 185, 251$
3074	$8, 15, 35, 67, 90, 116, 128, 145, 193, 195, 213, 228, 236, 246, 253$
3103	$18, 46, 74, 89, 98, 150, 158, 196, 204, 209, 214, 258$
3132	$29, 48, 64, 66, 80, 94, 131, 147, 156, 187, 207, 237, 240$
3161	$3, 9, 47, 70, 259$
3190	$41, 50, 65, 161, 162, 166, 169, 173, 199, 233$
3219	$27, 60, 97, 136, 178, 220$
3248	$63, 99, 121, 149, 159, 247, 249$
3277	$1, 19, 71, 72, 183, 205$
3306	$124, 126, 225$
3335	$109, 110, 232$
3364	22
3393	151
3422	10

Recently, some restrictions on the weight enumerators of ternary near-extremal self-dual codes of length divisible by 12 were proved in [1], namely, the weight enumerator of a ternary near-extremal self-dual code of length 60 is of the form:

$$W_{3,60} = 1 + \alpha y^{15} + (3901080 - 15\alpha)y^{18} + (241456320 + 105\alpha)y^{21} + \cdots ,$$

where $\alpha = 8\beta$ with $\beta \in \{1, 2, \ldots, 5148\}$ [1]. It is known that there is a ternary near-extremal self-dual code of length 60 having weight enumerator $W_{3,60}$ for

$$\alpha \in \{24\beta \mid \beta \in \Gamma_{60,1}\} \cup \{8\beta \mid \beta \in \Gamma_{60,2}\},$$

where $\Gamma_{60,1}$ and $\Gamma_{60,2}$ are listed in [1, Tables 22 and 27]. It follows from Table 3 that 154 of the codes $C_3(H_{60,i})$ are near-extremal. The values $\alpha = 8\beta$ in the weight enumerators $W_{3,60}$ for the 154 near-extremal self-dual codes $C_3(H_{60,i})$ are listed in Table 4. This was calculated by the Magma function `NumberOfWords`. From Table 4, we have the following:

Proposition 3. *There is a ternary near-extremal self-dual code of length* 60 *having weight enumerator* $W_{3,60}$ *for* $\alpha \in \{8\beta \mid \beta \in \Gamma_{60,3}\}$*, where*

$$\Gamma_{60,3} = \left\{ \begin{array}{l} 2552, 2668, 2697, 2726, 2755, 2784, 2813, 2842, 2871, \\ 2900, 2929, 2987, 3016, 3074, 3103, 3132, 3161, 3190, \\ 3219, 3248, 3277, 3306, 3335, 3364, 3422 \end{array} \right\}.$$

We note that no ternary near-extremal codes with weight enumerators given in Proposition 3 were previously known.

3.3 Binary doubly even self-dual codes $C_2(D_{59,i})$

Let $A_{59,i}$ be the incidence matrix of a Hadamard 2-$(59, 29, 14)$ design $D_{59,i}$ and let $C_2(D_{59,i})$ be the binary $[120, 60]$ code generated by the rows of the following matrix:

$$\left(\begin{array}{ccccc} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I_{60} & \vdots & & B_{59,i} & \\ & 1 & & & \end{array} \right),$$

where $B_{59,i} = J - A_{59,i}$ is the incidence matrix of the complementary design of $D_{59,i}$. In the context of binary codes, we consider the elements $0, 1$ of $\mathbb{Z}$ as the elements $0, 1$ of $\mathbb{F}_2$, respectively. It is trivial that if D and D' are isomorphic Hadamard 2-$(59, 29, 14)$ designs then $C_2(D) \cong C_2(D')$. The binary codes $C_2(D_{59,i})$ are doubly even self-dual codes [30]. The minimum weights d of $C_2(D_{59,i})$ were computed with the Magma function `MinimumWeight`, and are listed in Table 5. It is trivial that an automorphism of order 29 of $D_{59,i}$ induces an automorphism of order 29 of $C_2(D_{59,i})$. Note that there is no binary extremal doubly even self-dual code of length 120 with an automorphism of order 29 [9]. Also, it is currently not known whether there is a binary extremal doubly even self-dual code of length 120.

Table 5: Minimum weights of binary doubly even self-dual codes $C_2(D_{59,i})$

d	i
8	531
12	$7, 8, 19, 20, 123, 124, 125, 126, 131, 132, 133, 134, 167, 168, 185, 186,$ $197, 198, 217, 218, 221, 222, 251, 252, 281, 282, 285, 286, 337, 338,$ $371, 372, 397, 398, 407, 408, 417, 418, 421, 422, 497, 498, 511, 512$
16	others
20	$21, 24, 209, 210, 529, 530$

From Table 5, the codes $C_2(D_{59,i})$ $(i = 21, 24, 209, 210, 529, 530)$ are binary near-extremal doubly even self-dual codes of length 120. We verified with the Magma function `NumberOfWords` that the numbers of codewords of weight 20 in these codes are 71862, 71862, 98484, 98484, 104052 and 104052, respectively. If $D_{59,i}$ and $D_{59,j}$ are Hadamard

2-$(59, 29, 14)$ designs which are derived designs of isomorphic 3-$(60, 30, 14)$ designs, then $C_2(D_{59,i})$ and $C_2(D_{59,j})$ are equivalent [30, Theorem 2]. For $(i, j) \in \{(21, 24), (209, 210), (529, 530)\}$, we verified with the Magma function `IsIsomorphic` that $D_{59,i}$ and $D_{59,j}$ are derived designs of isomorphic 3-$(60, 30, 14)$ designs. This implies that $C_2(D_{59,i})$ and $C_2(D_{59,j})$ are equivalent.

The weight enumerator of a binary near-extremal doubly even self-dual code of length 120 is of the form:

$$\begin{aligned} W_{2,120} =& 1 + \alpha y^{20} + (39703755 - 20\alpha)y^{24} + (6101289120 + 190\alpha)y^{28} \\ &+ (475644139425 - 1140\alpha)y^{32} + (18824510698240 + 4845\alpha)y^{36} \\ &+ (397450513031544 - 15504\alpha)y^{40} + \cdots , \end{aligned}$$

(see [15, Section 4]). The existence of 528 inequivalent binary near-extremal doubly even self-dual codes of length 120 is known (see [15, Proposition 2] and [35, Table 1]). These codes have difference weight enumerators $W_{2,120}$, where α are given in [15, Table 3] and [35, Table 1].

Remark 4. The number of inequivalent binary near-extremal doubly even self-dual codes of length 120 constructed in [15] was incorrectly reported as 500. We point out that the correct number is 502. Hence, 528 inequivalent binary near-extremal doubly even self-dual codes of length 120 were previously known.

Proposition 5. (i) *There is a binary near-extremal doubly even self-dual code of length* 120 *with weight enumerator* $W_{2,120}$ *for* $\alpha = 98484$ *and* 104052.

(ii) *There are at least* 530 *inequivalent binary near-extremal doubly even self-dual codes of length* 120.

We note that no binary near-extremal codes with weight enumerators given in Proposition 5 (i) were previously known.

3.4 Self-dual codes $C_5(H_{60,i})$ over $\mathbb{F}_5$

Let H be a Hadamard matrix of order 60. We denote by $C_5(H)$ the code over $\mathbb{F}_5$ generated by the rows of H. In the context of codes over $\mathbb{F}_5$, we consider the elements $0, 1, -1$ of $\mathbb{Z}$ as the elements $0, 1, 4$ of $\mathbb{F}_5$, respectively. It is trivial that if H and H' are equivalent Hadamard matrices of order 60 then $C_5(H) \cong C_5(H')$. In addition, $C_5(H)$ is self-dual [21]. The minimum weights d of $C_5(H_{60,i})$ $(i = 1, 2, \dots, 266)$ were computed with the Magma function `MinimumWeight`, and are listed in Table 6. Let $d(C_5(H_{60,i}))$ and $N(C_5(H_{60,i}))$ denote the minimum weight and the number of codewords of minimum weight in $C_5(H_{60,i})$, respectively. For the pair (i, j) such that $d(C_5(H_{60,i})) = d(C_5(H_{60,j}))$ and $N(C_5(H_{60,i})) = N(C_5(H_{60,j}))$, using the Magma function `IsIsomorphic`, we determined whether $C_5(H_{60,i}) \cong C_5(H_{60,j})$ or not, where the numbers $N(C_5(H_{60,i}))$ were computed with the Magma function `NumberOfWords`. Then we found equivalent codes $C_5(H_{60,238}) \cong C_5(H_{60,257})$ and there is no other pair of equivalent codes among $C_5(H_{60,i})$.

Note that the extended quadratic residue code QR_{60} of length 60 is a self-dual code having minimum weight 18. The largest minimum weight among self-dual codes of length 60 is between 18 and 24 [12, Table 9]. From Table 6, $C_5(H_{60,21})$ and $C_5(H_{60,266})$ have the largest minimum weight among currently known self-dual codes of length 60. We verified with the Magma function `NumberOfWords` that the numbers of codewords of minimum weight in QR_{60}, $C_5(H_{60,21})$ and $C_5(H_{60,266})$ are 410640, 410640 and 288840, respectively. Therefore, there are at least two inequivalent self-dual codes over $\mathbb{F}_5$ of length 60 and minimum weight 18.

Table 6: Minimum weights of self-dual codes $C_5(H_{60,i})$ over $\mathbb{F}_5$

d	i
12	$66, 103, 129, 142, 170, 198, 209, 248, 259$
14	$1, 3, 4, 11, 19, 25, 28, 33, 35, 36, 38, 47, 49, 51, 52, 54, 58, 59, 64, 68, 72, 76, 78, 79, 81, 84, 85, 87, 89, 90, 91, 94, 96, 97, 105, 108, 109, 111, 113, 114, 115, 116, 118, 119, 120, 122, 123, 128, 132, 133, 135, 139, 149, 150, 152, 155, 157, 161, 162, 164, 165, 169, 172, 176, 178, 181, 183, 185, 188, 189, 194, 195, 196, 199, 200, 202, 206, 208, 211, 212, 218, 221, 222, 223, 224, 225, 226, 228, 233, 235, 236, 238, 240, 244, 245, 246, 252, 253, 256, 257, 260$
15	$7, 45, 48, 50, 53, 60, 61, 62, 65, 70, 92, 95, 101, 102, 107, 121, 127, 136, 144, 146, 159, 160, 171, 174, 177, 186, 192, 193, 210, 215, 219, 220, 230, 239, 243, 247, 255, 263$
16	others
18	$21, 266$

4 Hadamard matrices of order 64 with an automorphism of order 31

Using the method described in Section 2.2, we give in this section the classification of Hadamard 2-$(63, 31, 15)$ designs with an automorphism of order 31 having one fixed point. Using this classification, we give a complete classification of Hadamard matrices of order 64 with an automorphism of order 31. We construct binary doubly even codes from the Hadamard 2-$(63, 31, 15)$ designs.

4.1 Hadamard 2-$(63, 31, 15)$ designs $D_{63,i}$ and Hadamard matrices $H_{64,i}$ of order 64

The approach used in the classification is similar to that given in the previous section, so in this section, only results are given.

Proposition 6. *There are* 826 *non-isomorphic Hadamard* 2-$(63, 31, 15)$ *designs with an automorphism of order* 31 *having one fixed point. There are* 414 *inequivalent Hadamard matrices of order* 64 *with an automorphism of order* 31*.*

Remark 7. If p is an odd prime dividing the order of the automorphism group of a Hadamard matrix of order $n \geqslant 4$, then either p divides n or $n-1$, or $p \leqslant n/2-1$ [29]. Hence, the largest prime which can divide the order of the automorphism group of a Hadamard matrix of order 64 is 31.

The incidence matrices of the above 826 non-isomorphic Hadamard 2-$(63,31,15)$ designs $D_{63,i}$ ($i = 1,2,\dots,826$) and the above 414 inequivalent Hadamard matrices $H_{64,i}$ ($i = 1,2,\dots,414$) from Proposition 6 can be obtained electronically from [3].

The automorphism group orders $|\operatorname{Aut}(D_{63,i})|$ of $D_{63,i}$ and the automorphism group orders $|\operatorname{Aut}(H_{64,i})|$ of $H_{64,i}$ are listed in Tables 7 and 8, respectively.

Table 7: Orders of the automorphism groups of $D_{63,i}$

$\|\operatorname{Aut}(D_{63,i})\|$	i
$2^{15} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$	805
$2^5 \cdot 5 \cdot 31$	$790, 791, 793, 797, 806, 807, 808, 809, 810, 812, 813, 816, 820, 823$
$3 \cdot 5 \cdot 31$	$789, 792, 799$
$5 \cdot 31$	$794, 795, 796, 798, 800, 801, 802, 803, 804, 811, 814, 815, 817, 818, 819, 821, 822, 824, 825, 826$
$3 \cdot 31$	$765, 766, 767, 768, 769, 770, 771, 772, 779, 780, 781, 782, 783, 784, 785, 786$
31	others

Table 8: Orders of the automorphism groups of $H_{64,i}$

$\|\operatorname{Aut}(H_{64,i})\|$	i
$2^{28} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$	406
$2^{13} \cdot 5 \cdot 31$	$407, 410$
$2^{12} \cdot 5 \cdot 31$	$408, 409, 411, 413$
$2^8 \cdot 3 \cdot 5 \cdot 31$	$395, 398, 405$
$2^7 \cdot 5 \cdot 31$	$396, 397, 399, 403$
$2^2 \cdot 5 \cdot 31$	$400, 404, 412, 414$
$2^2 \cdot 3 \cdot 31$	$387, 388, 389, 390, 391, 392, 393, 394$
$2 \cdot 5 \cdot 31$	$401, 402$
$2^2 \cdot 31$	others

4.2 Binary doubly even codes $C_2'(D_{63,i})$

Let $A_{63,i}$ be the incidence matrix of a Hadamard 2-$(63,31,15)$ design $D_{63,i}$ and let $C_2'(D_{63,i})$ be the binary code generated by the rows of the following matrix:

$$\left(\begin{array}{cc} & 1 \\ A_{63,i} & \vdots \\ & 1 \end{array}\right).$$

It is trivial that if D and D' are isomorphic Hadamard 2-$(63, 31, 15)$ designs then we have $C_2'(D) \cong C_2'(D')$. In addition, it is trivial that $C_2'(D_{63,i})$ are doubly even. The dimensions $\dim(C_2'(D_{63,i}))$ were computed with the Magma function `Dimension`, and are listed in Table 9. The minimum weights d of the 794 doubly even self-dual codes $C_2'(D_{63,i})$ were computed with the Magma function `MinimumWeight`, and are listed in Table 10. In addition, we verified that the 520 extremal doubly even self-dual codes $C_2'(D_{63,i})$ are divided into 28 equivalence classes. More precisely, each of the 520 codes is equivalent to one of the 28 inequivalent extremal doubly even self-dual codes $C_2'(D_{63,i})$, where

$$i \in \left\{ \begin{array}{l} 1,2,3,4,6,8,9,10,11,14,15,17,18,20,24, \\ 25,30,35,36,47,54,55,59,67,69,87,150,195 \end{array} \right\}.$$

This was calculated with the Magma function `IsIsomorphic`. It is trivial that an automorphism of order 31 of $D_{63,i}$ induces an automorphism of order 31 of $C_2'(D_{63,i})$. Note that there are 38 inequivalent extremal doubly even self-dual codes of length 64 with an automorphism of order 31 [34].

Table 9: Dimensions of $C_2'(D_{63,i})$

$\dim(C_2'(D_{63,i}))$	i
7	805
12	806, 807, 808, 809, 810, 812, 813, 816, 820, 823
17	789, 790, 793, 800, 804
22	791, 795, 796, 797, 801, 802, 811, 814, 815, 817, 818, 819, 821, 822, 824, 826
32	others

5 Summary

We end this paper by listing a summary of the classification of Hadamard 2-$(2p+1, p, (p-1)/2)$ designs with an automorphism of order p having one fixed point and the classification of Hadamard matrices of order $2p+2$ with an automorphism of order p for $p \leqslant 31$. The number $N(\mathcal{D}_{2p+1})$ of non-isomorphic Hadamard 2-$(2p+1, p, (p-1)/2)$ designs with an automorphism of order p having one fixed point and the number $N(H_{2p+2})$ of inequivalent Hadamard matrices of order $2p+2$ with an automorphism of order p are listed in Table 11, along with relevant references.

Acknowledgements

This work was supported by JSPS KAKENHI Grant Numbers 19H01802, 21K03350 and 23H01087.

Table 10: Minimum weights of doubly even self-dual codes $C_2'(D_{63,i})$

d	i
4	792
8	$5, 14, 16, 17, 19, 21, 28, 30, 32, 34, 35, 36, 37, 41, 43, 49, 51, 53, 54, 59, 60, 61, 64, 66, 67, 70, 73, 75, 78, 82, 85, 92, 93, 103, 107, 113, 114, 118, 120, 123, 124, 135, 136, 138, 140, 141, 142, 143, 146, 153, 155, 156, 162, 166, 171, 172, 173, 180, 182, 185, 186, 188, 189, 200, 205, 206, 208, 211, 212, 213, 214, 229, 231, 232, 237, 242, 243, 244, 246, 248, 250, 251, 254, 257, 259, 263, 264, 265, 266, 267, 270, 271, 272, 274, 275, 279, 280, 281, 285, 287, 295, 297, 298, 300, 305, 309, 310, 313, 316, 319, 322, 323, 325, 333, 337, 338, 341, 342, 343, 347, 354, 357, 358, 359, 369, 370, 381, 382, 383, 390, 403, 407, 412, 413, 418, 420, 423, 425, 430, 432, 434, 441, 442, 444, 446, 456, 458, 468, 471, 476, 477, 478, 483, 484, 485, 490, 497, 500, 504, 505, 507, 509, 510, 515, 516, 519, 521, 527, 536, 537, 538, 546, 547, 548, 553, 555, 558, 559, 565, 572, 575, 587, 588, 591, 594, 596, 598, 599, 600, 601, 604, 606, 609, 610, 611, 612, 614, 617, 628, 634, 635, 636, 637, 639, 642, 643, 645, 646, 647, 648, 651, 653, 654, 656, 657, 658, 659, 661, 662, 663, 669, 672, 673, 674, 682, 686, 688, 689, 690, 697, 707, 711, 712, 713, 715, 717, 718, 728, 730, 739, 743, 748, 752, 753, 756, 757, 758, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 775, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 798, 799, 825$
12	others

Table 11: Summary

p	$N(\mathcal{D}_{2p+1})$	$N(H_{2p+2})$	References
3	1	1	[26]
5	1	1	[26] (see [14])
7	3	3	[13]
11	5	4	[18]
13	7	4	[29]
17	21	11	[31]
19	33	18	[10]
23	109	56	[10]
29	531	266	Section 3
31	826	414	Section 4

References

[1] M. Araya and M. Harada, Some restrictions on the weight enumerators of near-extremal ternary self-dual codes and quaternary Hermitian self-dual codes, *Des. Codes Cryptogr.* **91** (2023), 1813–1843.

[2] M. Araya, M. Harada and K. Momihara, Hadamard matrices related to a certain series of ternary self-dual codes, *Des. Codes Cryptogr.* **91** (2023), 795–805.

[3] M. Araya, M. Harada and V. D. Tonchev, Hadamard matrices of orders 60 and 64 with automorphisms of orders 29 and 31, https://www.math.is.tohoku.ac.jp/~mharada/H60/.

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

[5] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Second Edition, Cambridge University Press, Cambridge, 1999.

[6] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[7] S. Bouyuklieva, J. de la Cruz and D. Villar, Extremal binary and ternary codes of length 60 with an automorphism of order 29 and a generalization, *Mathematics* **10** (2022), 748.

[8] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, Second Edition, Chapman & Hall/CRC, New York, 2007.

[9] J. de la Cruz, M. Kiermaier and A. Wassermann, The automorphism group of an extremal $[120, 60, 24]$ code does not contain elements of order 29, *Des. Codes Cryptogr.* **78** (2016), 693–702.

[10] D. B. Dalan, M. Harada and A. Munemasa, On Hadamard matrices of order $2(p+1)$ with an automorphism of odd prime order p, *J. Combin. Designs* **11** (2003), 367–380.

[11] P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin-Heidelberg-New York, 1968.

[12] M. Grassl and T. A. Gulliver, On circulant self-dual codes over small fields, *Des. Codes Cryptogr.* **52** (2009), 57–81.

[13] M. Hall, Jr., Hadamard matrices of order 16, *Jet Propultion Laboratory Research Summary* No. 36-10, **1** (1961), 21–26.

[14] M. Hall, Jr., *Combinatorial Theory*, Second Edition, John Wiley & Sons, New York, 1986.

[15] M. Harada, New doubly even self-dual codes having minimum weight 20, *Adv. Math. Commun.* **14** (2020), 89–96.

[16] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, NJ, 2007.

[17] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[18] N. Ito, J. S. Leon and J. Q. Longyear, Classification of 3-$(24, 12, 5)$ designs and 24-dimensional Hadamard matrices, *J. Combin. Theory Ser. A* **31** (1981), 66–93.

[19] H. Kharaghani and B. Tayfeh-Rezaie, Hadamard matrices of order 32, *J. Combin. Designs* **21** (2013), 212–221.

[20] J. S. Leon, V. Pless and N. J. A. Sloane, On ternary self-dual codes of length 24, *IEEE Trans. Inform. Theory* **27** (1981), 176–180.

[21] J. S. Leon, V. Pless and N. J. A. Sloane, Self-dual codes over $GF(5)$, *J. Combin. Theory Ser. A* **32** (1982), 178–194.

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

[23] B. D. McKay and A. Piperno, Practical graph isomorphism, II, *J. Symbolic Comput.* **60** (2014), 94–112.

[24] B. D. McKay and A. Piperno, Nauty and Traces User's Guide (Version 2.8.6), http://pallini.di.uniroma1.it/Guide.html (2022).

[25] G. Nebe and D. Villar, An analogue of the Pless symmetry codes, Seventh International Workshop on Optimal Codes and Related Topics, Bulgaria, pp. 158–163, (2013).

[26] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.

[27] V. Pless, Symmetry codes over $GF(3)$ and new five-designs, *J. Combin. Theory Ser. A* **12** (1972), 119–142.

[28] J. Seberry, *Orthogonal Designs: Hadamard Matrices, Quadratic Forms and Algebras*, Springer, Cham, 2017.

[29] V. D. Tonchev, Hadamard matrices of order 28 with automorphisms of order 13, *J. Combin. Theory Ser. A* **35** (1983), 43–57.

[30] V. D. Tonchev, Block designs of Hadamard type and self-dual codes (in Russian), *Probl. Perda. Inform.* **19** (1983), 25–30. English translation in *Probl. Inform. Transm.* **19** (1983), 270–275.

[31] V. D. Tonchev, Hadamard matrices of order 36 with automorphisms of order 17, *Nagoya Math. J.* **104** (1986), 163–174.

[32] V. D. Tonchev, *Combinatorial Configurations*, John Wiley & Sons, New York, 1988.

[33] V. D. Tonchev, On Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs, *Des. Codes Cryptogr.* **90** (2022), 2753–2762.

[34] V. Y. Yorgov, Doubly-even extremal codes of length 64 (in Russian), *Probl. Perda. Inform.* **22** (1986), 35–42. English translation in *Probl. Inform. Transm.* **22** (1986), 277–284.

[35] R. Yorgova and A. Wassermann, Binary self-dual codes with automorphisms of order 23, *Des. Codes Cryptogr.* **48** (2008), 155–164.