Hadamard Matrices of Order 32 and Extremal Ternary Self-Dual Codes

Koichi Betsumiya*, Masaaki Harada† and Hiroshi Kimura‡

April 12, 2010

Abstract

A ternary self-dual code can be constructed from a Hadamard matrix of order congruent to 8 modulo 12. In this paper, we show that the Paley-Hadamard matrix is the only Hadamard matrix of order 32 which gives an extremal self-dual code of length 64. This gives a coding theoretic characterization of the Paley-Hadamard matrix of order 32.

Keywords: Hadamard matrix, Paley-Hadamard matrix, extremal self-dual code, ternary code

1 Introduction

As described in [7], self-dual codes are an important class of linear codes for both theoretical and practical reasons. It is a fundamental problem to classify self-dual codes of modest length and determine the largest minimum weight among self-dual codes of that length (see [7]). By the Gleason–Pierce theorem, there are nontrivial divisible self-dual codes over $\mathbb{F}_q$ for $q = 2, 3$ and 4 only, where $\mathbb{F}_q$ denotes the finite field of order q (see [7, Theorem 5]), and

*Graduate School of Science and Technology, Hirosaki University, Hirosaki 036–8561, Japan. email: betsumi@cc.hirosaki-u.ac.jp

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

‡2900–2 Oka, Fukaya 369–0201, Japan. email: kimurafuka@kind.ocn.ne.jp

this is one of the reasons why much work has been done concerning self-dual codes over these fields.

A code C over $\mathbb{F}_3$ is called *ternary*. All codes in this paper are ternary linear codes. A matrix whose rows are linearly independent and generate the code C is called a generator matrix of C. A code C of length n is said to be *self-dual* if $C = C^{\perp}$, where the dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in \mathbb{F}_3^n |\ x \cdot y = 0 \text{ for all } y \in C\}$ under the standard Euclidean inner product $x \cdot y$. A self-dual code of length n exists if and only if $n \equiv 0 \pmod 4$. It was shown in [6] that the minimum weight d of a self-dual code of length n is bounded by $d \leq 3[n/12] + 3$. If $d = 3[n/12] + 3$, then the code is called *extremal*. Two codes C and C' are *equivalent* if there exists a monomial matrix P over $\mathbb{F}_3$ with $C' = CP = \{xP \mid x \in C\}$.

A *Hadamard* matrix H of order n is an $n \times n$ matrix whose entries are from $\{1, -1\}$ such that $HH^T = nI$, where H^T is the transpose of H and I is the identity matrix. It is known that the order n is necessarily $1, 2$, or a multiple of 4. A Hadamard matrix is *normalized* if its first row and column consist entirely of 1's. Two Hadamard matrices H and H' are said to be *equivalent* if there exist $(0, \pm 1)$-signed permutation matrices P, Q with $H' = PHQ$. All Hadamard matrices of orders up to 28 have been classified (see [5]), and there are at least $13, 708, 126$ inequivalent Hadamard matrices of order 32 (see [4]).

Let H_n be a Hadamard matrix of order n. Let $C(H_n)$ be the ternary code with generator matrix $(\ I\ ,\ H_n\ )$, where entries of the matrix are regarded as elements of $\mathbb{F}_3$. It is known that if $n \equiv 8 \pmod{12}$, then $C(H_n)$ is self-dual [2]. Moreover, it was shown that if H is the Paley-Hadamard matrix of order 32, then $C(H)$ is an extremal self-dual code of length 64 [2]. The goal of this paper is to give the following coding theoretic characterization of the Paley-Hadamard matrix of order 32.

Theorem 1. *Let H be a Hadamard matrix of order* 32*. Let $C(H)$ be the ternary self-dual code of length* 64 *with generator matrix $(\ I\ ,\ H\ )$. The code $C(H)$ is extremal if and only if H is equivalent to the Paley-Hadamard matrix.*

Remark 2. Only the above code is a currently known extremal self-dual code of length 64 (see [7, Table XII]).

In the process of proving the above theorem, we have the following partial classification of Hadamard matrices of order 32 (see Section 3 for the definition of type 3).

Proposition 3. *Let H be a Hadamard matrix of order* 32*. If both H and H^T are of type* 3*, then H is equivalent to the Paley-Hadamard matrix.*

2 Self-dual codes constructed from Hadamard matrices

Let H be a Hadamard matrix of order n. Let $C(H)$ be the ternary code with generator matrix $(\ I\ ,\ H\ )$, where entries of the matrix are regarded as elements of $\mathbb{F}_3$.

Lemma 4 (Dawson [2])**.** *If $n \equiv 8 \pmod{12}$, then $C(H)$ is self-dual.*

The following lemmas are somewhat trivial, but useful for our approach.

Lemma 5. *Let H and H' be Hadamard matrices of order n. If H and H' are equivalent, then $C(H)$ and $C(H')$ are equivalent.*

Proof. See e.g., [3, Lemma 3.1]. □

Thus, for the remainder of this paper, we assume that a Hadamard matrix is normalized, unless specified otherwise.

Lemma 6. *If $n \equiv 8 \pmod{12}$, then $C(H)$ and $C(H^T)$ are equivalent.*

Proof. Since the dual code of $C(H)$ has generator matrix $(\ -H^T\ ,\ I\ )$, $C(H)^\perp$ and $C(H^T)$ are equivalent. Since $C(H)$ is self-dual, $C(H)$ and $C(H^T)$ are equivalent. □

The unique Hadamard matrix of order 8 constructs an extremal self-dual code of length 16 denoted by $2f_8$ in [1]. The three inequivalent Hadamard matrices of order 20 construct three inequivalent extremal self-dual codes of length 40 [3]. For order 32, if H is the Paley-Hadamard matrix, then $C(H)$ is an extremal self-dual code of length 64 [2].

3 Hadamard matrices of order 32

3.1 Types of Hadamard matrices

By permuting and negating rows and columns, any four rows of a Hadamard matrix of order n can be converted to the following form:

$$
\begin{pmatrix}
\mathbf{1}_a & \mathbf{1}_a & \mathbf{1}_a & \mathbf{1}_a & \mathbf{1}_b & \mathbf{1}_b & \mathbf{1}_b & \mathbf{1}_b \\
\mathbf{1}_a & \mathbf{1}_a & -\mathbf{1}_a & -\mathbf{1}_a & \mathbf{1}_b & \mathbf{1}_b & -\mathbf{1}_b & -\mathbf{1}_b \\
\mathbf{1}_a & -\mathbf{1}_a & \mathbf{1}_a & -\mathbf{1}_a & \mathbf{1}_b & -\mathbf{1}_b & \mathbf{1}_b & -\mathbf{1}_b \\
\mathbf{1}_a & -\mathbf{1}_a & -\mathbf{1}_a & \mathbf{1}_a & -\mathbf{1}_b & \mathbf{1}_b & \mathbf{1}_b & -\mathbf{1}_b
\end{pmatrix}, \tag{1}
$$

where $\mathbf{1}_m$ denotes the all-one vector of length m, $a + b = n/4$ and $0 \le a \le [n/8]$. The set of four rows, which has the above form, is called *type* a, due to [5]. A Hadamard matrix is of *type* a if it has a set of four rows of type a and no set of four rows of type $a' < a$. For order 32, there are five types of sets of four rows, namely types $0, 1, 2, 3$ and 4.

We remark that types of Hadamard matrices given in [4] were defined for sets of four columns, and it has been shown that there are $13, 680, 757$ inequivalent Hadamard matrices of order 32 which are of type 0 and there is no Hadamard matrix of order 32 which is of type 4. Hence, there are $13, 680, 757$ inequivalent Hadamard matrices H of order 32 such that H^T are of type 0, and there is no Hadamard matrix of type 4 in our sense [4]. In the next subsection, we give a proof of the latter result for the sake of completeness.

In the next subsections, we consider Hadamard matrices of each type. In the remaining part of the paper, H denotes $(K + J)/2$, where K is a normalized Hadamard matrix of order 32 and J is the matrix with all one entries.

3.2 Type 4

Lemma 7 ([4]). *For order* 32, *there is no Hadamard matrix of type* 4.

Proof. Let H be a Hadamard matrix of type 4. We may assume that H has the following form:

$$\left(\begin{array}{c|c|c|c|c|c|c|c}
1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\
1111 & 1111 & 0000 & 0000 & 1111 & 1111 & 0000 & 0000 \\
1111 & 0000 & 1111 & 0000 & 1111 & 0000 & 1111 & 0000 \\
1111 & 0000 & 0000 & 1111 & 0000 & 1111 & 1111 & 0000 \\
v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7
\end{array}\right),$$

where v_i $(i = 0, 1, \ldots, 7)$ are vectors of length 4. Let n_i denote the number of 1's in v_i. From the orthogonality of the 5-th row to each of the other rows, we have the following:

$$\begin{aligned}
n_0 + n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 &= 16, \\
n_0 + n_1 - n_2 - n_3 + n_4 + n_5 - n_6 - n_7 &= 0, \\
n_0 - n_1 + n_2 - n_3 + n_4 - n_5 + n_6 - n_7 &= 0, \\
n_0 - n_1 - n_2 + n_3 - n_4 + n_5 + n_6 - n_7 &= 0.
\end{aligned}$$

Moreover, since the following fours set of four rows

$$\{r_1, r_2, r_3, r_5\}, \{r_1, r_2, r_4, r_5\}, \{r_1, r_3, r_4, r_5\}, \{r_2, r_3, r_4, r_5\},$$

are also of type 4, where r_i denotes the i-th row in the above matrix, we also have the following:

$$\begin{aligned}
n_0 + n_4 = n_1 + n_5 = n_2 + n_6 = n_3 + n_7 &= 4, \\
n_0 + n_5 = n_1 + n_4 = n_2 + n_7 = n_3 + n_6 &= 4, \\
n_0 + n_6 = n_1 + n_7 = n_2 + n_4 = n_3 + n_5 &= 4, \\
n_0 + (4 - n_7) = n_1 + (4 - n_6) = (4 - n_2) + n_5 = (4 - n_3) + n_4 &= 4,
\end{aligned}$$

respectively. This system of the equations has the following unique solution:

$$n_0 = n_1 = n_2 = n_3 = n_4 = n_5 = n_6 = n_7 = 2.$$

Hence, the i-th row of H has $n_0 = 2$ for $i = 5, 6, \ldots, 32$. This gives the nonexistence of a Hadamard matrix of type 4. □

3.3 Types 0 and 1

Lemma 8. *Let H be a Hadamard matrix of order 32. If H has a set of four rows of type 1, then H^T is of type 0.*

Proof. We may assume that H contains the following five rows:

$$\left(\begin{array}{c|ccc|c|c|c|c} 1 & 1 & 1 & 1 & 1111111 & 1111111 & 1111111 & 1111111 \\ 1 & 1 & 0 & 0 & 1111111 & 1111111 & 0000000 & 0000000 \\ 1 & 0 & 1 & 0 & 1111111 & 0000000 & 1111111 & 0000000 \\ 1 & 0 & 0 & 1 & 0000000 & 1111111 & 1111111 & 0000000 \\ 1 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \end{array}\right),$$

where v_i $(i = 1, 2, 3)$ are vectors of length 1 and v_i $(i = 4, 5, 6, 7)$ are vectors of length 7. Let n_i denote the number of 1's in v_i $(i = 1, 2, \ldots, 7)$. From the orthogonality of the 5-th row to each of the other rows, we have the following:

$$\begin{aligned} n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 &= 15, \\ n_1 - n_2 - n_3 + n_4 + n_5 - n_6 - n_7 &= -1, \\ -n_1 + n_2 - n_3 + n_4 - n_5 + n_6 - n_7 &= -1, \\ -n_1 - n_2 + n_3 - n_4 + n_5 + n_6 - n_7 &= -1. \end{aligned}$$

This implies that

$$n_1 = 1 + n_6 - n_7, n_2 = 1 + n_5 - n_7, n_3 = 7 - n_5 - n_6, n_4 = 6 - n_5 - n_6 + n_7,$$

then $n_1 + n_2 + n_3 = 9 - 2n_7 \equiv 1 \pmod 2$. Therefore, we have the following:

$$(n_1, n_2, n_3) = (1, 0, 0), (0, 1, 0), (0, 0, 1) \text{ or } (1, 1, 1).$$

Let $r_i = (1, v_1, v_2, v_3, v_4, v_5, v_6, v_7)$ denote the i-th row of H. Let s, t, u and v be the numbers of i $(i = 5, 6, \ldots, 32)$ with

$$(v_1, v_2, v_3) = (1, 1, 1), (1, 0, 0), (0, 1, 0) \text{ and } (0, 0, 1),$$

respectively. Note that $s + t + u + v = 28$. From the orthogonality of among i-th columns $(i = 2, 3, 4)$,

$$s + v - t - u = 0, s + u - t - v = 0, s + t - u - v = 0.$$

Therefore, $s = t = u = v = 7$, and the set of the first four rows of H^T is of type 0. □

Lemma 9. *If H is of type 0 or 1, then $C(H)$ is not extremal.*

Proof. There is a codeword of weight 12 corresponding to some linear combination of the four rows of type 0. For a Hadamard matrix H of type 1, by Lemma 8, H^T is of type 0. Hence, $C(H^T)$ contains a codeword of weight 12. Since $C(H)$ is self-dual, $C(H)$ and $C(H^T)$ are equivalent, by Lemma 6. Hence, if H is of type 0 or 1, then $C(H)$ contains a codeword of weight 12, that is, $C(H)$ is not extremal. $\square$

Remark 10. By Lemmas 6 and 9, the $13,680,757$ inequivalent Hadamard matrices found in [4] give no extremal self-dual code.

3.4 Type 2

Suppose that H is of type 2. By Lemma 6, $C(H)$ and $C(H^T)$ are equivalent. By Lemma 9, if H^T is of type 0 or 1, then $C(H)$ is not extremal. Hence, we may assume that H^T has no set of four rows of type 0 or 1. Moreover, we may assume that H has the following form:

$$\left(\begin{array}{c|c|c|c|c|c|c|c}
11 & 11 & 11 & 11 & 111111 & 111111 & 111111 & 111111 \\
11 & 11 & 00 & 00 & 111111 & 111111 & 000000 & 000000 \\
11 & 00 & 11 & 00 & 111111 & 000000 & 111111 & 000000 \\
11 & 00 & 00 & 11 & 000000 & 111111 & 111111 & 000000 \\
v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7
\end{array}\right),$$

where v_i $(i = 0, 1, 2, 3)$ are vectors of length 2 and v_i $(i = 4, 5, 6, 7)$ are vectors of length 6. Let n_i denote the number of 1's in v_i. From the orthogonality of the 5-th row to each of the other rows, we have the following:

$$\begin{aligned}
n_0 + n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 &= 16, \\
n_0 + n_1 - n_2 - n_3 + n_4 + n_5 - n_6 - n_7 &= 0, \\
n_0 - n_1 + n_2 - n_3 + n_4 - n_5 + n_6 - n_7 &= 0, \\
n_0 - n_1 - n_2 + n_3 - n_4 + n_5 + n_6 - n_7 &= 0.
\end{aligned}$$

We remark that this gives

$$\begin{aligned}
n_4 = 4 + \frac{1}{2}(-n_0 - n_1 - n_2 + n_3), n_5 = 4 + \frac{1}{2}(-n_0 - n_1 + n_2 - n_3), \\
n_6 = 4 + \frac{1}{2}(-n_0 + n_1 - n_2 - n_3), n_7 = 4 + \frac{1}{2}(n_0 - n_1 - n_2 - n_3).
\end{aligned}$$

Table 1: (n_0, n_1, n_2, n_3) for the solutions s_i

s_i	n_0	n_1	n_2	n_3	s_i	n_0	n_1	n_2	n_3	s_i	n_0	n_1	n_2	n_3
s_1	2	2	2	2	s_{10}	2	0	2	2	s_{19}	1	1	2	2
s_2	2	2	2	0	s_{11}	2	0	2	0	s_{20}	1	1	2	0
s_3	2	2	1	1	s_{12}	2	0	1	1	s_{21}	1	1	1	1
s_4	2	2	0	2	s_{13}	2	0	0	2	s_{22}	1	1	0	2
s_5	2	2	0	0	s_{14}	2	0	0	0	s_{23}	1	1	0	0
s_6	2	1	2	1	s_{15}	1	2	2	1	s_{24}	1	0	2	1
s_7	2	1	1	2	s_{16}	1	2	1	2	s_{25}	1	0	1	2
s_8	2	1	1	0	s_{17}	1	2	1	0	s_{26}	1	0	1	0
s_9	2	1	0	1	s_{18}	1	2	0	1	s_{27}	1	0	0	1

Since H is normalized, $v_0 = (11)$ or (10). Hence, $n_0 = 2$ or 1. Under this condition, this system of equations has 27 solutions s_i $(i = 1, 2, \dots, 27)$, where (n_0, n_1, n_2, n_3) are listed in Table 1 for each solution s_i.

By considering the orthogonality of columns, types of sets of four columns among the first eight columns, and the condition that $C(H^T)$ is extremal, we determined the sets of the possible solutions $s_{i_5}, s_{i_6}, \dots, s_{i_{32}}$ corresponding to the rows $r_5, r_6, \dots, r_{32}$, respectively, where r_j denotes the j-th row of H. By permuting rows, it is sufficient to consider the possible solutions under the following conditions:

1. $i_5, i_6, \dots, i_{16} \in \{1, 2, \dots, 14\}$,
2. $i_{17}, i_{18}, \dots, i_{32} \in \{15, 16, \dots, 27\}$,
3. $i_j \le i_{j+1}$ for $j = 5, 6, \dots, 31$.

Then there are 43 such sets, and the solutions $(i_5, i_6, \dots, i_{32})$ are listed in Table 2. By considering the possible solutions in Table 2, we constructed 32×8 submatrices in Figure 1, column by column. Then we found 1045 12×6 matrices A_1 in Figure 1. For each of the 1045 matrices A_1, based on the possible solutions in Table 2, we tried to construct Hadamard matrices, row by row under the assumption that H is of type 2, H^T has no set of four rows of type 0 and 1, and $C(H)$ is extremal. However, no Hadamard matrix is obtained under the above assumption. Therefore, we have the following:

Lemma 11. *If H is of type 2, then $C(H)$ is not extremal.*

Table 2: Possible solutions for each row r_j ($j = 5, 6, \ldots, 32$)

(1, 3, 3, 3, 6, 8, 8, 9, 12, 12, 12, 13, 16, 17, 19, 20, 21, 21, 21, 21, 21, 21, 22, 22, 23, 23, 24, 24)
(1, 3, 3, 3, 6, 8, 8, 9, 12, 12, 12, 13, 16, 18, 19, 20, 20, 21, 21, 21, 21, 21, 21, 22, 23, 23, 24, 25)
(1, 3, 3, 3, 6, 8, 9, 9, 11, 12, 12, 13, 16, 17, 19, 20, 21, 21, 21, 21, 21, 21, 21, 22, 23, 23, 24, 25)
(1, 3, 3, 3, 6, 8, 9, 9, 11, 12, 12, 13, 16, 18, 19, 20, 20, 21, 21, 21, 21, 21, 21, 21, 23, 23, 25, 25)
(1, 3, 3, 3, 6, 8, 9, 9, 12, 12, 12, 12, 16, 17, 19, 20, 20, 21, 21, 21, 21, 21, 22, 22, 23, 23, 24, 25)
(1, 3, 3, 3, 6, 8, 9, 9, 12, 12, 12, 12, 16, 18, 19, 20, 20, 20, 21, 21, 21, 21, 21, 22, 23, 23, 25, 25)
(1, 3, 3, 3, 6, 9, 9, 9, 11, 12, 12, 12, 16, 17, 19, 20, 20, 21, 21, 21, 21, 21, 21, 22, 23, 23, 25, 25)
(1, 3, 3, 5, 6, 6, 9, 9, 11, 12, 12, 13, 16, 16, 20, 20, 21, 21, 21, 21, 21, 21, 21, 21, 23, 23, 25, 25)
(1, 3, 3, 5, 6, 6, 9, 9, 11, 12, 12, 13, 16, 17, 19, 20, 21, 21, 21, 21, 21, 21, 21, 21, 22, 23, 25, 26)
(1, 3, 3, 5, 6, 6, 9, 9, 12, 12, 12, 12, 16, 16, 20, 20, 20, 21, 21, 21, 21, 21, 21, 22, 23, 23, 25, 25)
(1, 3, 3, 5, 6, 6, 9, 9, 12, 12, 12, 12, 16, 17, 19, 20, 20, 21, 21, 21, 21, 21, 21, 22, 22, 23, 25, 26)
(1, 3, 3, 5, 6, 7, 8, 9, 11, 12, 12, 13, 15, 16, 20, 21, 21, 21, 21, 21, 21, 21, 21, 22, 23, 23, 24, 25)
(1, 3, 3, 5, 6, 7, 8, 9, 11, 12, 12, 13, 15, 18, 19, 20, 21, 21, 21, 21, 21, 21, 21, 21, 22, 23, 25, 26)
(1, 3, 3, 5, 6, 7, 8, 9, 12, 12, 12, 12, 15, 16, 20, 20, 21, 21, 21, 21, 21, 21, 22, 22, 23, 23, 24, 25)
(1, 3, 3, 5, 6, 7, 8, 9, 12, 12, 12, 12, 15, 17, 19, 20, 21, 21, 21, 21, 21, 21, 22, 22, 22, 23, 24, 26)
(1, 3, 3, 5, 6, 7, 8, 9, 12, 12, 12, 12, 15, 18, 19, 20, 20, 21, 21, 21, 21, 21, 21, 22, 22, 23, 25, 26)
(1, 3, 3, 6, 6, 8, 8, 9, 9, 12, 12, 13, 16, 16, 17, 20, 21, 21, 21, 21, 21, 21, 22, 23, 23, 24, 24, 25)
(1, 3, 3, 6, 6, 8, 8, 9, 9, 12, 12, 13, 16, 16, 18, 20, 20, 21, 21, 21, 21, 21, 21, 23, 23, 24, 25, 25)
(1, 3, 3, 6, 6, 8, 8, 9, 9, 12, 12, 13, 16, 17, 18, 19, 20, 21, 21, 21, 21, 21, 21, 22, 23, 24, 25, 26)
(1, 3, 3, 6, 6, 8, 9, 9, 9, 12, 12, 12, 16, 16, 17, 20, 20, 21, 21, 21, 21, 21, 22, 23, 23, 24, 25, 25)
(1, 3, 3, 6, 6, 8, 9, 9, 9, 12, 12, 12, 16, 16, 18, 20, 20, 20, 21, 21, 21, 21, 21, 23, 23, 25, 25, 25)
(1, 3, 3, 6, 6, 8, 9, 9, 9, 12, 12, 12, 16, 17, 17, 19, 20, 21, 21, 21, 21, 21, 22, 22, 23, 24, 25, 26)
(1, 3, 3, 6, 7, 8, 8, 8, 9, 12, 12, 13, 15, 16, 17, 21, 21, 21, 21, 21, 21, 22, 22, 23, 23, 24, 24, 24)
(1, 3, 3, 6, 7, 8, 8, 8, 9, 12, 12, 13, 15, 16, 18, 20, 21, 21, 21, 21, 21, 21, 22, 23, 23, 24, 24, 25)
(1, 3, 3, 6, 7, 8, 8, 8, 9, 12, 12, 13, 15, 18, 18, 19, 20, 21, 21, 21, 21, 21, 21, 22, 23, 24, 25, 26)
(1, 3, 3, 6, 7, 8, 8, 9, 9, 11, 12, 13, 15, 16, 17, 21, 21, 21, 21, 21, 21, 21, 22, 23, 23, 24, 24, 25)
(1, 3, 3, 6, 7, 8, 8, 9, 9, 11, 12, 13, 15, 17, 18, 19, 21, 21, 21, 21, 21, 21, 21, 22, 23, 24, 25, 26)
(1, 3, 3, 6, 7, 8, 8, 9, 9, 12, 12, 12, 15, 16, 17, 20, 21, 21, 21, 21, 21, 22, 22, 23, 23, 24, 24, 25)
(1, 3, 3, 6, 7, 8, 8, 9, 9, 12, 12, 12, 15, 17, 17, 19, 21, 21, 21, 21, 21, 22, 22, 22, 23, 24, 24, 26)
(1, 3, 3, 6, 7, 8, 8, 9, 9, 12, 12, 12, 15, 17, 18, 19, 20, 21, 21, 21, 21, 21, 22, 22, 23, 24, 25, 26)
(1, 3, 3, 6, 7, 8, 8, 9, 9, 12, 12, 12, 15, 18, 18, 19, 20, 20, 21, 21, 21, 21, 21, 22, 23, 25, 25, 26)
(3, 3, 3, 3, 6, 6, 9, 9, 12, 12, 12, 12, 16, 16, 19, 20, 20, 20, 21, 21, 21, 21, 22, 23, 23, 23, 25, 25)
(3, 3, 3, 3, 6, 6, 9, 9, 12, 12, 12, 12, 16, 17, 19, 19, 20, 20, 21, 21, 21, 21, 22, 22, 23, 23, 25, 26)
(3, 3, 3, 3, 6, 7, 8, 9, 12, 12, 12, 12, 15, 16, 19, 20, 20, 21, 21, 21, 21, 22, 22, 23, 23, 23, 24, 25)
(3, 3, 3, 3, 6, 7, 8, 9, 12, 12, 12, 12, 15, 18, 19, 19, 20, 20, 21, 21, 21, 21, 22, 22, 23, 23, 25, 26)
(3, 3, 3, 6, 6, 6, 9, 9, 9, 12, 12, 12, 16, 16, 16, 20, 20, 20, 21, 21, 21, 21, 23, 23, 23, 25, 25, 25)
(3, 3, 3, 6, 6, 6, 9, 9, 9, 12, 12, 12, 16, 16, 17, 19, 20, 20, 21, 21, 21, 21, 22, 23, 23, 25, 25, 26)
(3, 3, 3, 6, 6, 7, 8, 9, 9, 12, 12, 12, 15, 16, 16, 20, 20, 21, 21, 21, 21, 22, 23, 23, 23, 24, 25, 25)
(3, 3, 3, 6, 6, 7, 8, 9, 9, 12, 12, 12, 15, 16, 17, 19, 20, 21, 21, 21, 21, 22, 22, 23, 23, 24, 25, 26)
(3, 3, 3, 6, 6, 7, 8, 9, 9, 12, 12, 12, 15, 16, 18, 19, 20, 20, 21, 21, 21, 21, 22, 23, 23, 25, 25, 26)
(3, 3, 6, 6, 7, 7, 8, 8, 9, 9, 12, 12, 15, 15, 16, 17, 21, 21, 21, 21, 22, 22, 23, 23, 24, 24, 25, 26)
(3, 3, 6, 6, 7, 7, 8, 8, 9, 9, 12, 12, 15, 15, 16, 18, 20, 21, 21, 21, 21, 22, 23, 23, 24, 25, 25, 26)
(3, 3, 6, 6, 7, 7, 8, 8, 9, 9, 12, 12, 15, 16, 17, 18, 19, 20, 21, 21, 21, 21, 22, 23, 24, 25, 26, 27)

$$H = \left(\begin{array}{c|c|c|c|c|c}
11 & 111111 & 111111 & 111111 & 111111 & 111111 \\
11 & 110000 & 111111 & 111111 & 000000 & 000000 \\
11 & 001100 & 111111 & 000000 & 111111 & 000000 \\
11 & 000011 & 000000 & 111111 & 111111 & 000000 \\
\hline
11 & & & & & \\
\vdots & A_1 & & & & \\
11 & & & & & \\
\hline
10 & & & & & \\
10 & & & & & \\
\vdots & & & & & \\
10 & & & & & \\
10 & & & & &
\end{array}\right)$$

Figure 1: A Hadamard matrix of type 2

3.5 Type 3

Suppose that H is of type 3. If H^T is of type $0, 1$ or 2, then by Lemmas 6, 9 and 11, $C(H)$ is not extremal. Hence, for the remainder of this subsection, we assume that both H and H^T are of type 3, unless specified otherwise.

We first show that every Hadamard matrix of type 3 has a set of rows of type 4. To make it computationally feasible, it is better to use the four rows of type 4.

Lemma 12. *If both H and H^T are of type 3, then H contains a set of four rows of type 4.*

Proof. We may assume that H contains the following five rows:

$$M_3 = \left(\begin{array}{c|c|c|c|c|c|c|c}
11111 & 111 & 111 & 111 & 111 & 11111 & 11111 & 11111 \\
11111 & 111 & 111 & 000 & 000 & 11111 & 00000 & 00000 \\
11111 & 111 & 000 & 111 & 000 & 00000 & 11111 & 00000 \\
11111 & 000 & 111 & 111 & 000 & 00000 & 00000 & 11111 \\
v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7
\end{array}\right),$$

where v_i $(i = 0, 5, 6, 7)$ are vectors of length 5 and v_i $(i = 1, 2, 3, 4)$ are vectors of length 3. Let n_i denote the number of 1's in v_i. We remark that the above form is slightly different from that in (1). Because there are eight columns such that all entries in the first three rows are 1 from the property of the corresponding Hadamard 2-designs, we take these columns as the first eight ones. Moreover, we may assume that v_0 has the form of one of the following three cases:

Case	3-1	3-2	3-3
v_0	(11111)	(11110)	(11100)

- Case 3-1: First we show that $n_1 = n_2 = n_3 = 0$ and $n_4 = 3$. Suppose contrary, that is, for some i $(i = 1, 2, 3)$ $n_i > 0$ or $n_4 \leq 2$. Then there is a set of four rows among the first five rows which is of type ≤ 2. Hence, $n_1 = n_2 = n_3 = 0$ and $n_4 = 3$. From the orthogonality of the 5-th row to each of the other rows, we have the following:

$$\begin{aligned} n_5 + n_6 + n_7 &= 8, \\ n_5 - n_6 - n_7 &= -2, \\ -n_5 + n_6 - n_7 &= -2, \\ -n_5 - n_6 + n_7 &= -2. \end{aligned}$$

  This system of equations has no solution.

- Case 3-2: From the orthogonality of the 5-th row to each of the other rows, we have the following:

$$\begin{aligned} n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 &= 12, \\ n_1 + n_2 - n_3 - n_4 + n_5 - n_6 - n_7 &= -4, \\ n_1 - n_2 + n_3 - n_4 - n_5 + n_6 - n_7 &= -4, \\ -n_1 + n_2 + n_3 - n_4 - n_5 - n_6 + n_7 &= -4. \end{aligned}$$

  This gives the following:

$$\begin{aligned} n_4 &= n_1 + n_2 + n_3, n_5 = 4 - n_1 - n_2, \\ n_6 &= 4 - n_1 - n_3, n_7 = -4 - n_2 - n_3. \end{aligned}$$

  If $n_i \geq 2$ $(i = 1, 2, 3)$, then, by interchanging the 5-th row and the $(5 - i)$-th row, the set of the first four rows is of type ≤ 2. Then we may assume that $n_1 \leq 1$, $n_2 \leq 1$ and $n_3 \leq 1$. Similarly, we have $n_4 \geq 2$. Hence, we have the following four possible (n_1, n_2, n_3, n_4):

	n_1	n_2	n_3	n_4
(a)	1	1	0	2
(b)	1	0	1	2
(c)	0	1	1	2
(d)	1	1	1	3

For (a), the set of the i-th rows ($i = 1, 3, 4, 5$) is of type 4. Similarly, for (b) and (c), there is a set of four rows of type 4. For (d), by interchanging the first row and the second row, the matrix satisfies the condition (a).

- Case 3-3: If for some i $n_i = 1$ ($i = 1, 2, 3$) or $n_4 = 2$, then, by interchanging the 5-th row and the j-th row ($j = 1, 2, 3, 4$), the set of the first four rows is of type 4. Similarly, if $n_i = 3$ ($i = 1, 2, 3$) or $n_4 = 0$, then we have a set of four rows of type ≤ 2. Hence, we have the following:

$$n_1, n_2, n_3, 3 - n_4 \in \{0, 2\}. \tag{2}$$

From the orthogonality of the 5-th row to each of the other rows, we have the following:

$$\begin{aligned} n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 &= 13, \\ n_1 + n_2 - n_3 - n_4 + n_5 - n_6 - n_7 &= -3, \\ n_1 - n_2 + n_3 - n_4 - n_5 + n_6 - n_7 &= -3, \\ -n_1 + n_2 + n_3 - n_4 - n_5 - n_6 + n_7 &= -3. \end{aligned}$$

So, we have $n_1 + n_2 + n_3 = n_4 + 2$. This contradicts (2).

This completes the proof. $\square$

By the above lemma, we may assume that H contains the following five rows:

$$M_4 = \left(\begin{array}{c|c|c|c|c|c|c|c} 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ 1111 & 1111 & 1111 & 0000 & 0000 & 1111 & 0000 & 0000 \\ 1111 & 1111 & 0000 & 1111 & 0000 & 0000 & 1111 & 0000 \\ 1111 & 0000 & 1111 & 1111 & 0000 & 0000 & 0000 & 1111 \\ v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \end{array} \right),$$

where v_i ($i = 0, \dots, 7$) are vectors of length 4. Similar to the proof of Lemma 12, we consider the above form instead of that in (1). Let n_i denote the number of 1's in v_i. From the property of the corresponding Hadamard 2-designs, we may assume that v_0 has the form of one of the following two cases:

Case	4-1	4-2
v_0	(1111)	(1110)

- Case 4-2: For $n_1 = 3$, we may assume that $v_1 = (1110)$. The first, second, third rows and 5-th row can be converted to the following form:

$$\left(\begin{array}{c|c|c|c|c|c|c|c} 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ 1111 & 1111 & 1111 & 0000 & 0000 & 1111 & 0000 & 0000 \\ 1111 & 1111 & 0000 & 1111 & 0000 & 0000 & 1111 & 0000 \\ 1111 & 1100 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \end{array}\right),$$

by interchanging the 4-th and 6-th columns. The set of the four rows is of type 2. For $n_1 = 0$ or 4, this case is contained in Case 4-1 by permuting and negating rows and columns. For $n_1 = 2$, the set of the i-th rows ($i = 1, 2, 3, 5, 6$) of H^T is in Case 4-1, which is discussed below.

Now consider $n_1 = 1$. By an argument similar to the above, we may assume that $n_2 = n_3 = 1$. Indeed, if $n_2 \neq 1$ or $n_3 \neq 1$, then each of H, H^T is in Case 4-1 or of type ≤ 2. From the orthogonality of the 5-th row to each of the other rows, we have the following:

$$\begin{aligned} n_4 + n_5 + n_6 + n_7 &= 10, \\ -n_4 + n_5 - n_6 - n_7 &= -4, \\ -n_4 - n_5 + n_6 - n_7 &= -4, \\ -n_4 - n_5 - n_6 + n_7 &= -4. \end{aligned}$$

This system of equations has the following unique solution:

$$n_4 = 1, n_5 = 3, n_6 = 3, n_7 = 3.$$

By considering permutations, we may assume that $v_i = (1000)$ ($i = 1, 2, 3, 4$) and $v_i = (1110)$ ($i = 5, 6, 7$). Hence, the first five rows are as follows:

$$\left(\begin{array}{c|c|c|c|c|c|c|c} 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 & 1111 \\ 1111 & 1111 & 1111 & 0000 & 0000 & 1111 & 0000 & 0000 \\ 1111 & 1111 & 0000 & 1111 & 0000 & 0000 & 1111 & 0000 \\ 1111 & 0000 & 1111 & 1111 & 0000 & 0000 & 0000 & 1111 \\ 1110 & 1000 & 1000 & 1000 & 1000 & 1110 & 1110 & 1110 \end{array}\right).$$

By considering the i-th rows ($i = 2, 3, 4, 5$), H is of type ≤ 2.

- Case 4-1: If for some i $n_i \geq 2$ $(i = 1, 2, 3)$, then, by interchanging the 5-th row and the $(5-i)$-th row, the set of the first four rows is of type ≤ 2. Then we may assume that $n_1 \leq 1$, $n_2 \leq 1$ and $n_3 \leq 1$. Similarly, we have $n_4 \geq 3$. From the orthogonality of the 5-th row to each of the other rows, we have the following:

$$\begin{aligned}
n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 &= 12, \\
n_1 + n_2 - n_3 - n_4 + n_5 - n_6 - n_7 &= -4, \\
n_1 - n_2 + n_3 - n_4 - n_5 + n_6 - n_7 &= -4, \\
-n_1 + n_2 + n_3 - n_4 - n_5 - n_6 + n_7 &= -4.
\end{aligned}$$

Hence, we have $n_1 + n_2 + n_3 = n_4$, which gives:

$$n_1 = n_2 = n_3 = 1 \text{ and } n_4 = 3.$$

Since H^T is of type 3, we may assume that H has the form given in Figure 2 which is not a normalized Hadamard matrix. This form is obtained by negating the i-th rows $(i = 15, 16, 17)$ and the j-columns $(j = 17, 18, 19, 20)$ of a normalized Hadamard matrix. The above form reduces our computation for finding the possible Hadamard matrices by considering the conditions given below.

Let H' be the submatrix of the $(0,1)$-Hadamard matrix $(H+J)/2$ consisting of the i-th rows $(i = 6, \ldots, 32)$ and j-th columns $(j = 5, \ldots, 32)$. Here we define an order on the set of $(0,1)$-vectors of length 28. For a $(0,1)$-vector $v = (e_1, e_2, \ldots, e_{28})$ of length 28, we define

$$\begin{aligned}
\alpha(v) &= \sum_{i=1}^{4} 8^{4-i} n_{\sigma(i)}, \\
\beta(v) &= 2^{16}\alpha(v) + \sum_{j=1}^{16} 2^{16-j} e_j \text{ and} \\
\gamma(v) &= 2^{12}\beta(v) + \sum_{j=17}^{28} 2^{28-j} e_j,
\end{aligned}$$

where σ is a permutation of $\{1, 2, 3, 4\}$ satisfying $n_{\sigma(1)} \geq n_{\sigma(2)} \geq n_{\sigma(3)} \geq n_{\sigma(4)}$ for $n_i = 4e_{4i-3} + e_{4i-2} + e_{4i-1} + e_{4i}$ $(i = 1, 2, 3, 4)$. In fact, $\gamma(v)$ gives a total order in the set of vectors of length 28.

$$H = \left(\begin{array}{c|c|c|c|c|c|c|c}
1111 & 1111 & 1111 & 1111 & 0000 & 1111 & 1111 & 1111\\
1111 & 1111 & 1111 & 0000 & 1111 & 1111 & 0000 & 0000\\
1111 & 1111 & 0000 & 1111 & 1111 & 0000 & 1111 & 0000\\
1111 & 0000 & 1111 & 1111 & 1111 & 0000 & 0000 & 1111\\ \hline
1111 & 1000 & 1000 & 1000 & 1000 & 1100 & 1100 & 1100\\ \hline
1110 & & & & & & & \\
1110 & A_{1,1} & A_{1,2} & A_{1,3} & A_{1,4} & & & \\
1110 & & & & & & & \\ \hline
1101 & & & & & & & \\
1101 & A_{2,1} & A_{2,2} & A_{2,3} & A_{2,4} & & & \\
1101 & & & & & & & \\ \hline
1011 & & & & & & & \\
1011 & A_{3,1} & A_{3,2} & A_{3,3} & A_{3,4} & & & \\
1011 & & & & & & & \\ \hline
0111 & & & & & & & \\
0111 & A_{4,1} & A_{4,2} & A_{4,3} & A_{4,4} & & & \\
0111 & & & & & & & \\ \hline
1100 & & & & & & & \\
\vdots & & & & & & & \\
1100 & & & & & & & \\ \hline
1010 & & & & & & & \\
\vdots & & & & & & & \\
1010 & & & & & & & \\ \hline
1001 & & & & & & & \\
\vdots & & & & & & & \\
1001 & & & & & & &
\end{array}\right)$$

Figure 2: A Hadamard matrix in Case 4-1

Each of $A_{i,j}$ in H can be moved to the place of $A_{1,1}$ preserving the i-th rows ($i = 1, 2, 3, 4, 5$) and the j-th columns ($j = 1, 2, 3, 4$) by permuting rows and columns and negating some of i-th rows ($i = 18, 19, \ldots, 32$) and some of j-th columns ($j = 17, 18, \ldots 32$). Hence, by permuting and negating rows and columns, H can be converted to a matrix preserving the i-rows ($i = 1, 2, 3, 4, 5$) and the j-th columns ($j = 1, 2, 3, 4$) of H and satisfying the following conditions:

1. $\beta(r_1) = \max\{\beta(r) \mid \alpha(r) = \alpha(r_1), r \in \{0, 1\}^{28}\}$,
2. $\gamma(r_i) \geq \gamma(r_{i+1}) \geq \gamma(r_{i+2})$ for $i = 1, 4, 7, 10$,
3. $\gamma(r_1) \geq \gamma(r_4) \geq \gamma(r_7) \geq \gamma(r_{10})$ and
4. $\gamma(r_i) \geq \gamma(r_{i+1}) \geq \gamma(r_{i+2}) \geq \gamma(r_{i+3}) \geq \gamma(r_{i+4})$ for $i = 13, 18, 23$,

where r_i is the i-th row of its 27×28 submatrix H'.

Starting from the first five rows, we tried to construct Hadamard matrices H, row by row under the above four conditions in such a way that both H and H^T are of type 3. We found exactly twelve Hadamard matrices. Finally, we verified that each of the matrices and their transposed matrices is equivalent to the Paley-Hadamard matrix.

The above argument shows that if both H and H^T are of type 3, then H is equivalent to the Paley-Hadamard matrix, which completes the proof of Proposition 3. In addition, by considering the case which does not assume that H^T is of type 3, we have the following:

Lemma 13. *If H is of type 3, then either H is equivalent to the Paley-Hadamard matrix or $C(H)$ is not extremal.*

By Lemmas 9, 11 and 13, any Hadamard matrix H of order 32 satisfies one of the following:

(1) H is equivalent to the Paley-Hadamard matrix,

(2) $C(H)$ is not extremal.

This completes the proof of Theorem 1.

Acknowledgments. The authors would like to thank Hadi Kharaghani for sending a preprint of [4]. The authors would also like to thank the anonymous referees for their useful comments on the manuscript.

References

[1] J.H. Conway, V. Pless and N.J.A. Sloane, Self-dual codes over GF(3) and GF(4) of length not exceeding 16, *IEEE Trans. Inform. Theory* **25** (1979), 312–322.

[2] E. Dawson, Self-dual ternary codes and Hadamard matrices, *Ars Combin.* **19** (1985), 303–308.

[3] M. Harada, New extremal ternary self-dual codes, *Australas. J. Combin.* **17** (1998), 133–145.

[4] H. Kharaghani and B. Tayfeh-Rezaie, On the classification of Hadamard matrices of order 32, *J. Combin. Designs*, (to appear).

[5] H. Kimura, Classification of Hadamard matrices of order 28, *Discrete Math.* **133** (1994), 171–180.

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

[7] 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.