JOURNAL OF COMBINATORIAL THEORY, Series A 44, 274–287 (1987)

Hadamard Matrices and Doubly Even Self-Dual Error-Correcting Codes

MICHIO OZEKI

Department of Mathematics, Faculty of Liberal Arts,
Nagasaki University, 1–14, Bunkyo-machi, Nagasaki, Japan

Communicated by the Managing Editors

Received May 9, 1986

Let n be an integer with $n \equiv 4 \pmod 8$. For any Hadamard matrices H_n of order n, we give a method to define a doubly even self-dual $[2n, n]$ code $\mathscr{C}(NH_n)$. Then we will prove that two Hadamard equivalent matrices define equivalent codes. © 1987 Academic Press, Inc.

1. INTRODUCTION

A Hadamard matrix H_n of order n is defined to be a square matrix of order n, whose entries consist of ± 1, satisfying

$$H_n \, {}^tH_n = nI_n,$$

where ${}^tH_n$ is the transpose of H_n and I_n is the unit matrix of order n. It is known that Hadamard matrices H_n exist only when $n = 2$ or n is a multiple of 4. Hereafter, we assume that $n \equiv 4 \pmod 8$. Two Hadamard matrices $H_n^{(1)}$ and $H_n^{(2)}$ of the same order n are said to be Hadamard equivalent (abbreviated H-equivalent) if $H_n^{(2)}$ is obtained from $H_n^{(1)}$ by a sequence of operations of (i) exchanging two rows (or columns) of $H_n^{(1)}$ or (ii) multiplying some rows (or columns) of $H_n^{(1)}$ by -1. It is easily seen that any Hadamard matrix H_n is H-equivalent to the matrix of the shape

$$NH_n = \begin{pmatrix} -1 & 1 & 1 & \cdots & 1 \\ 1 & & & & \\ 1 & & & & \\ \vdots & & & * & \\ 1 & & & & \end{pmatrix} \tag{1}$$

Although most authors call Hadamard matrices, whose entries of the first row and column are all 1, normalized Hadamard matrices (or normal

0097-3165/87 $3.00

forms of Hadamard matrices), we would like to call Hadamard matrices of the shape (1) normalized Hadamard matrices (or normal forms of Hadamard matrices), because the matrices of the shape (1) are more suitable for our present work.

Let $\mathbf{F}_2 = GF(2)$ be the field consisting of elements 0 and 1. Let V_n be the vector space $\mathbf{F}_2^n$ of dimension n over $\mathbf{F}_2$. A binary linear code $[n, k]$ is a vector subspace of V_n of dimension k. In what follows, we treat only binary linear codes, and we drop the adjective "binary." For two elements $\mathbf{x} = (x_1 . x_2, ..., x_n)$ and $\mathbf{y} = (y_1, y_2, ..., y_n)$ in V_n, the inner product $(\mathbf{x}, y)$ is defined by

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

The Hamming distance $d(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is defined to be the number of indices i such that $x_i \neq y_i$. The Hamming weight $\mathrm{wt}(\mathbf{x})$ of the vector $\mathbf{x}$ is defined to be $d(\mathbf{x}, \mathbf{0})$, where $\mathbf{0}$ is the zero vector in V_n. The dual code $[n, k]^{\perp}$ of a linear code $[n, k]$ is the space defined by

$$[n, k]^{\perp} = \{\mathbf{y} \in V_n \mid (\mathbf{x}, \mathbf{y}) = 0 \qquad \text{for all} \quad \mathbf{x} \in [n, k]\}.$$

A linear code $[n, k]$ is said to be self-orthogonal (resp. self-dual) if it holds that

$$[n, k] \subset [n, k]^{\perp} \qquad (\text{resp. } [n, k] = [n, k]^{\perp}).$$

A linear code $[n, k]$ is said to be even (resp. doubly even) if the weight $\mathrm{wt}(\mathbf{x})$ of any element $\mathbf{x}$ in $[n, k]$ is divisible by 2 (resp. 4). Two codes $[n, k]_{(1)}$ and $[n, k]_{(2)}$ of the same dimension k are said to be equivalent if we can find a basis $\{\mathbf{x}_i\}$ of $[n, k]_{(1)}$ and a basis $\{\mathbf{y}_i\}$ of $[n, k]_{(2)}$ such that the vectors $\mathbf{y}_i$ are obtained from $\mathbf{x}_i$ by exchanging some coordinates of $\mathbf{x}_i$ simultaneously for $i = 1, 2, ..., k$.

In this paper, we give a method to obtain a doubly even self-dual linear code $\mathscr{C}(NH_n)$ of length $2n$ over $\mathbf{F}_2$ from a normalized Hadamard matrix NH_n of order n (Theorem 1). In the existing literature (e.g., [4] or [5]), some non-linear codes are called Hadamard codes, but they are different from $\mathscr{C}(NH_n)$. Theorem 1 can produce many doubly even self-dual $[2n, n]$ codes, which have not been obtained by other methods.

Before defining code $\mathscr{C}(NH_n)$, we study the properties of the normalized Hadamard matrix NH_n in Section 2. In Section 3, we describe the definition of $\mathscr{C}(NH_n)$ and the properties of $\mathscr{C}(NH_n)$. In Section 4, we give a test to determine the minimal weight of $\mathscr{C}(NH_n)$. In Section 5, we show some consequences of our present method. In Section 6, we pose some questions arising from our investigation. Unfortunately, our method is successful only for the case $n \equiv 4 \pmod 8$.

2. A Study of the Normalized Hadamard Matrix

Let

$$NH_n = \begin{pmatrix} -1 & 1 & 1 & \cdots & 1 \\ 1 & & & & \\ 1 & & & & \\ \vdots & & & * & \\ 1 & & & & \end{pmatrix} = (s_{ij})$$

be a normalized Hadamard matrix of order n. We let ξ_i denote the ith row vector of NH_n. Let $\nu_1(i)$ (resp. $\nu_2(i)$) be the number of 1's (resp. -1's) in the last $n-1$ entries of ξ_i. By definition, we have

$$\nu_1(1) = n-1 \qquad \text{and} \qquad \nu_2(1) = 0. \tag{2}$$

It is easy to show that

$$\nu_1(i) = n/2 \tag{3a}$$

and

$$\nu_2(i) = n/2 - 1 \qquad \text{for} \quad 2 \leqslant i \leqslant n. \tag{3b}$$

Furthermore, let $\mu_1(i, h)$, $\mu_2(i, h)$, $\mu_3(i, h)$ and $\mu_4(i, h)$ $(1 \leqslant i < h \leqslant n)$, respectively, be the cardinalities of the sets defined by

$$\{j \mid s_{ij} = s_{hj} = 1 \qquad 2 \leqslant j \leqslant n\},$$

$$\{j \mid s_{ij} = 1, s_{hj} = -1 \qquad 2 \leqslant j \leqslant n\},$$

$$\{j \mid s_{ij} = -1, s_{hj} = 1 \qquad 2 \leqslant j \leqslant n\}$$

and

$$\{j \mid s_{ij} = s_{hj} = -1 \qquad 2 \leqslant j \leqslant n\},$$

respectively. We see that, for $2 \leqslant i < h \leqslant n$,

$$\mu_1(i, h) + \mu_2(i, h) = \nu_1(i) = n/2, \tag{4a}$$

$$\mu_3(i, h) + \mu_4(i, h) = \nu_2(i) = n/2 - 1, \tag{4b}$$

$$\mu_1(i, h) + \mu_3(i, h) = \nu_1(h) = n/2, \tag{4c}$$

and

$$\mu_2(i, h) + \mu_4(i, h) = \nu_2(h) = n/2 - 1. \tag{4d}$$

By the orthogonality of ξ_i with ξ_h $(2 \leqslant i < i < h \leqslant n)$, we have

$$\sum_{j=1}^{n} s_{ij} s_{hj} = 1 + \mu_1(i, h) + \mu_4(i, h) - \mu_2(i, h) - \mu_3(i, h) = 0. \tag{5}$$

From (4a)-(4d) and (5), we have

$$\mu_1(i, h) = \mu_2(i, h) = \mu_3(i, h) = n/4 \tag{6}$$

and

$$\mu_4(i, h) = n/4 - 1 \qquad \text{for} \qquad 2 \leqslant i < h \leqslant n.$$

3. The Definition and the Properties of the Code $\mathscr{C}(NH_n)$

Let $NH_n = (s_{ij})$ be a normalized Hadamard matrix of order n. Let J_n be the all 1 square matrix of order n. We put

$$K_n = 1/2(NH_n + J_n).$$

By definition, K_n is a (0, 1) matrix. Let

$$C_n = (I_n K_n)$$

be an $n \times 2n$ matrix, and $\mathbf{x}_1, \ldots, \mathbf{x}_n$ be the row vectors of C_n. Regarding $\mathbf{x}_i$ $(1 \leqslant i \leqslant n)$ as vectors in the vector space $V_{2n} = \mathbf{F}_2^{2n}$, we may define the vector subspace $\mathscr{C}(NH_n)$ of V_{2n} generated by $\mathbf{x}_i$'s over $\mathbf{F}_2$. By the definition, it is clear that the vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ are linearly independent over $\mathbf{F}_2$, so that dim $\mathscr{C}(NH_n) = n$. By this fact, we call C_n the generator matrix of the linear code $\mathscr{C}(NH_n)$. If we write

$$\mathbf{x}_i = (\mathbf{e}_i, \mathbf{y}_i) \qquad (1 \leqslant i \leqslant n), \tag{7}$$

using the first half row $\mathbf{e}_i$ of $\mathbf{x}_i$ and the last half row $\mathbf{y}_i$ of $\mathbf{x}_i$, then the ith entry of the vector $\mathbf{e}_i$ is 1 and the remaining entries of $\mathbf{e}_i$ are all 0. Note that $\mathbf{y}_i(1 \leqslant i \leqslant n)$ are the row vectors of the matrix K_n. By (7), we see that

$$\mathrm{wt}(\mathbf{x}_i) = 1 + \mathrm{wt}(\mathbf{y}_i), \qquad 1 \leqslant i \leqslant n. \tag{8}$$

Let y_{ij} be the entries of the vector $\mathbf{y}_i$; then we see that

$$y_{ij} = 1 \Leftrightarrow s_{ij} = 1 \tag{9a}$$

and

$$y_{ij} = 0 \Leftrightarrow s_{ij} = -1 \qquad \text{for} \quad 1 \leqslant i, j \leqslant n. \tag{9b}$$

By virtue of (2), (3a), (8), (9a), and (9b), we get

$$\mathrm{wt}(\mathbf{x}_1)=n \tag{10a}$$

and

$$\mathrm{wt}(\mathbf{x}_i)=n/2+2, \qquad 2\leqslant i\leqslant n. \tag{10b}$$

The inner product $(\mathbf{x}_i, \mathbf{x}_h)$ is clearly given by

$$(\mathbf{x}_i, \mathbf{x}_h)=\sum_{j=1}^{n} y_{ij}y_{hj}, \qquad 1\leqslant i<h\leqslant n.$$

By (9a) and (9b), the above sum equals the parity of $v_1(h)$ (resp. $\mu_1(i, h)+1$) for $1=i<h$ (resp. $1<i<h\leqslant n$), and we have

$$(\mathbf{x}_i, \mathbf{x}_h)=0 \qquad \text{for} \quad 1\leqslant i<h\leqslant n, \tag{11}$$

because of the equations (3a), (6) and our assumption that $n\equiv 4 \pmod 8$. Here, we quote a theorem in [6], which is useful for our present work.

PROPOSITION 3.1 (Theorem 4 in [6]). *If the rows of a generator matrix C_n for a binary $[n, k]$ code C have weights divisible by* 4 *and are orthogonal to each other, then C is self-orthogonal and all weights in C are divisible by* 4.

We prove:

THEOREM 1. *Let the notations be as abbove. When $n\equiv 4$ $(mod\, 8)$, then $\mathscr{C}(NH_n)$ is a doubly even self-dual linear $[2n, n]$ code.*

Proof. By (10a) and (10b), the generators of the code $\mathscr{C}(NH_n)$ have weights divisible by 4. By (11), the generators are mutually orthogonal, and $\mathscr{C}(NH_n)$ is a self-orthogonal $[2n, n]$ code because of the Proposition 3.1. Thus, by Proposition 3.1, $\mathscr{C}(NH_n)$ is a doubly even self-dual linear $[2n, n]$ code. Q.E.D.

Although a Hadamard matrix H_n of order n has many H-equivalent normal forms, we can prove:

THEOREM 2. *We assume that $n\equiv 4$ (mod 8). Suppose $NH_n^{(1)}$ and $NH_n^{(2)}$ are two normalized and H-equivalent Hadamard matrices of order n; then the codes $\mathscr{C}(NH_n^{(1)})$ and $\mathscr{C}(NH_n^{(2)})$ are equivalent codes.*

Proof. To prove this theorem, it is sufficient to show that the code $\mathscr{C}(NH_n^{(2)})$ is equivalent to the code $\mathscr{C}(NH_n^{(1)})$ in the cases (α) when $NH_n^{(2)}$ is obtained from $NH_n^{(1)}$ by exchanging two different rows of $NH_n^{(1)}$, (β) when $NH_n^{(2)}$ is obtained from $NH_n^{(1)}$ by exchanging two different columns of $NH_n^{(1)}$, and more generally (γ) when $NH_n^{(2)}$ is obtained from $NH_n^{(1)}$ as

$$NH_n^{(2)} = PNH_n^{(1)}Q,$$

where P and Q are monomial permutation matrices of $+1$'s and -1's. Since such matrix P (resp. Q) can be written as a product of a pure permutation matrix (i.e., a monomial permutation matrix of $+1$'s) and a diagonal matrix with diagonal entries ± 1's, the proof for the case (γ) is done similarly to that of (α) or (β), and we omit the detail.

Throughout the proof, we use y_{ij} (resp. z_{ij}) for the right half of the $n \times n$ matrix $K_n^{(1)}$ (resp. $K_n^{(2)}$) of the generator matrix $C_n^{(1)}$ (resp. $C_n^{(2)}$) for the code $\mathscr{C}(NH_n^{(1)})$ (resp. $\mathscr{C}(NH_n^{(2)})$).

Case (α). When $NH_n^{(2)}$ is obtained from $NH_n^{(1)}$ by exchanging the ith and the hth rows of $NH_n^{(1)}$ with $1 < i < h \leqslant n$, then the theorem is obvious.

When we exchange the first and the hth ($h > 1$) rows of $NH_n^{(1)}$, then the resulting matrix M_1 is not in normal form. Apart from the trivial way (i.e., the exchange of the first and the hth rows of M_1 again), there are two ways to return to normal form. One way is (i) to multiply the first column by -1, (ii) to multiply all the rows other than the first and the hth rows by -1, (iii) to multiply each kth ($k > 1$) column by -1 whenever the top entry of the column is -1. The resulting matrix is denoted by M_2, which is in normal form. Another way is (iv) to multiply the hth row by -1, (v) to multiply the first row by -1, and (vi) to multiply each kth ($k > 1$) column by -1 whenever the top entry of the column is -1. However, the resulting matrix is identical to the matrix M_2. Let s_{ij} (resp. t_{ij}) be the entries of $HN_n^{(1)}$ (resp. $NH_n^{(2)} = M_2$).

Suppose that

$$s_{hj} = -1 \qquad \text{for} \quad j = j_1, j_2, ..., j_r \quad \text{with} \quad 1 < j_1 < \cdots < j_r$$

and

$$s_{hj} = 1 \qquad \text{for} \quad j \neq j_1, j_2, ..., j_r;$$

then, from the processes (i) $\sim$ (iii), we see that

$$\begin{gathered}
t_{11} = s_{11} = -1, \qquad t_{1j} = s_{1j} = 1 \qquad (2 \leqslant j \leqslant n), \\
t_{i1} = s_{i1} = 1 \qquad (2 \leqslant i \leqslant n), \qquad t_{hj} = s_{hj} \qquad (2 \leqslant j \leqslant n), \\
t_{ij} = s_{ij} \qquad \text{for} \quad j = j_1, j_2, ..., j_r \qquad \text{and} \qquad i \neq 1, h, \\
t_{ij} = -s_{ij} \qquad \text{for} \quad j \neq 1, j_1, j_2, ..., j_r \quad \text{and} \quad i \neq 1, h.
\end{gathered}$$

By the above relations, we can infer the relations between y_{ij} and z_{ij}, namely,

$$\begin{aligned} &y_{11}=z_{11}=0, \quad y_{1j}=z_{1j}=1 \quad (2\leqslant j\leqslant n),\\ &y_{i1}=z_{i1}=1 \quad (2\leqslant i\leqslant n), \quad y_{hj}=z_{hj} \quad (2\leqslant j\leqslant n),\\ &y_{ij}=z_{ij} \quad \text{for} \quad j=j_1, j_2,..., j_r \quad \text{and} \quad i\neq 1, h,\\ &y_{ij}+z_{ij}=1 \quad \text{for} \quad j\neq 1, j_1, j_2,..., j_r \quad \text{and} \quad i\neq 1, h. \end{aligned}$$

Let $\mathbf{u}_i=(\mathbf{e}_i, \mathbf{z}_i)$ $(1\leqslant i\leqslant n)$ be the row vectors of the generator matrix $C_n^{(2)}$ of $\mathscr{C}(NH_n^{(2)})$, where $\mathbf{z}_i=(z_{i1}, z_{i2},..., z_{in})$. Then, it is clear that the vectors $\mathbf{v}_1=\mathbf{u}_1$, $\mathbf{v}_2=\mathbf{u}_2+\mathbf{u}_h,...,$ $\mathbf{v}_{h-1}=\mathbf{u}_{h-1}+\mathbf{u}_h$, $\mathbf{v}_h=\mathbf{u}_h$, $\mathbf{v}_{h+1}=\mathbf{u}_{h+1}+\mathbf{u}_h,...,$ $\mathbf{v}_n=\mathbf{u}_n+\mathbf{u}_h$ form a basis of $\mathscr{C}(NH_n^{(2)})$. If we exchange the hth column with the $(n+1)$st column in the $n\times 2n$ matrix

$$\begin{pmatrix} \mathbf{v}_1\\ \mathbf{v}_2\\ \vdots\\ \mathbf{v}_n \end{pmatrix},$$

then we get the generator matrix $C_n^{(1)}$ of the code $\mathscr{C}NH_n^{(1)})$. This implies that the code $\mathscr{C}(NH_n^{(2)})$ is equivalent to the code $\mathscr{C}(NH_n^{(1)})$.

Case (β). When $NH_n^{(2)}$ is obtained from $NH_n^{(1)}$ by exchanging the jth and the k-th columns of $NH_n^{(1)}$ with $1<j<k\leqslant n$, then the theorem is obvious.

When we exchange the first and the kth $(k>1)$ columns of $NH_n^{(1)}$, then the resulting matrix M_3 is not in normal form. There are two ways to return to another normal form. One way is (vii) to multiply the first row by -1, (viii) to multiply all the columns other than the first and the kth columns by -1, (ix) to multiply each hth $(h>1)$ row by -1 whenever the first entry of the row is -1, obtaining another normal form M_4. Another way also leads to the same matrix M_4 as in the row case.

Let s_{ij} (resp. t_{ij}) be the entries of $NH_n^{(1)}$ (resp. $NH_n^{(2)}=M_4$). Suppose that

$$s_{ik}=1 \quad \text{for} \quad i=1, i_1, i_2,..., i_r \quad \text{with} \quad 1<i_1<\cdots<i_r$$

and

$$s_{ik}=-1 \quad \text{for} \quad i\neq 1, i_1, i_2,..., i_r,$$

then, from the processes (vii) ~ (ix), we see that

$$\begin{aligned} &t_{11}=s_{11}=-1, \qquad t_{1j}=s_{1j}=1 \qquad (2\leqslant j\leqslant n),\\ &t_{i1}=s_{i1}=1 \qquad (2\leqslant i\leqslant n), \qquad t_{ik}=s_{ik} \qquad (2\leqslant i\leqslant n),\\ &t_{ij}=-s_{ij} \qquad \text{for} \quad i=i_1, i_2,\ldots, i_r \quad \text{and} \quad j\neq 1, k \end{aligned}$$

and

$$t_{ij}=s_{ij} \qquad \text{for} \quad i\neq i_1, i_2,\ldots, i_r \quad \text{and} \quad j\neq 1, k.$$

By the above relations, we infer the relations between y_{ij} and z_{ij}, namely,

$$\begin{aligned} &y_{11}=z_{11}=0, \qquad y_{1j}=z_{1j}=1 \qquad (2\leqslant j\leqslant n),\\ &y_{i1}=z_{i1}=1 \qquad (2\leqslant i\leqslant n), \qquad y_{ik}=z_{ik} \qquad (2\leqslant i\leqslant n),\\ &z_{ij}+y_{ij}=1 \quad \text{for} \quad i=i_1, i_2,\ldots, i_r \quad \text{and} \quad j\neq 1, k \end{aligned}$$

and

$$z_{ij}=y_{ij} \qquad \text{for} \quad i\neq i_1, i_2,\ldots, i_r \quad \text{and} \quad j\neq 1, k.$$

Let $\mathbf{x}_i$ (resp. $\mathbf{u}_i=(\mathbf{e}_i, \mathbf{z}_i)$) $(1\leqslant i\leqslant n)$ be the row vectors of the generator matrix $C_n^{(1)}$ (resp. $C_n^{(2)}$) of the code $\mathscr{C}(NH_n^{(1)})$ (resp. $\mathscr{C}(NH_n^{(2)})$). It can be observed that

$$\mathbf{u}_i=\mathbf{x}_i \qquad \text{for} \quad i\neq i_1, i_2,\ldots, i_r.$$

Putting

$$\mathbf{v}_i=\mathbf{u}_i \qquad \text{for} \quad i\neq i_1, i_2,\ldots, i_r$$

and

$$\mathbf{v}_i=\mathbf{u}_i+\mathbf{u}_1 \qquad \text{for} \quad i=i_1\cdot i_2,\ldots, i_r,$$

we see that the matrix

$$D=\begin{pmatrix} \mathbf{v}_1\\ \mathbf{v}_2\\ \vdots\\ \mathbf{v}_n \end{pmatrix}$$

forms a generator matrix of $\mathscr{C}(NH_n^{(2)})$. If we exchange the first and the $(n+k)$th columns of D, we obtain the generator matrix $C_n^{(1)}$ of $\mathscr{C}(NH_n^{(1)})$.

This implies that two codes $\mathscr{C}(NH_n^{(1)})$ and $\mathscr{C}(NH_n^{(2)})$ are equivalent. We have thus proved the Theorem 2.

4. A Test to Determine the Minimal Weight of the Code $\mathscr{C}(NH_n)$

As before, we let $\mathbf{x}_i$ $(1 \leqslant i \leqslant n)$ denote the row vectors of the generator matrix C_n of the code $\mathscr{C}(NH_n)$. When we want to prove that a given natural number d is the minimal non-zero weight of the code $\mathscr{C}(NH_n)$ for a given normalized Hadamard matrix NH_n of order n, we must show that the inequalities

$$\mathrm{wt}(\mathbf{f}_r) \geqslant d \qquad \text{with} \quad 1 \leqslant r \leqslant d-1 \tag{12}$$

hold, where $\mathbf{f}_r$'s run over all r linear combinations chosen from the vectors $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n$. By Theorem 1, we may assume that d is a multiple of 4. Let $\mathbf{y}_i$ be the last half of the vector $\mathbf{x}_i = (\mathbf{e}_i, \mathbf{y}_i)$ as in Section 3, then by (8) we see that the condition (12) is equivalent to the condition

$$r + \mathrm{wt}(\mathbf{g}_r) \geqslant d \qquad \text{with} \quad 1 \leqslant r \leqslant d-1, \tag{13}$$

where $\mathbf{g}_r$ runs over all r linear combinations chosen from the vectors $\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_n$. We prove

THEOREM 3. *Let the notations be as above. Assume that*

$$n \geqslant 2d - 4 \tag{14}$$

and

$$\mathrm{wt}(\mathbf{g}_r) \geqslant d - r - 3 \qquad \textit{with} \quad 3 \leqslant r \leqslant d-1, \tag{15}$$

where $\mathbf{g}_r$ runs over all r linear combinations chosen from the vectors $\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_n$. Then the code $\mathscr{C}(NH_n)$ is a code with minimal weight d.

Proof. First we remark that if $r \geqslant d$ and $\mathbf{f}_r$ is any one of r linear combination chosen from $\mathbf{x}_1, ..., \mathbf{x}_n$ then it automatically holds that

$$\mathrm{wt}(\mathbf{f}_r) \geqslant d$$

because of the shape $\mathbf{x}_i = (\mathbf{e}_i, \mathbf{y}_i)$ $(1 \leqslant i \leqslant n)$.

It is easy to show that the inequalities

$$\mathrm{wt}(\mathbf{g}_1) \geqslant d - 2 \tag{16}$$

$$\mathrm{wt}(\mathbf{g}_2) \geqslant d - 2 \tag{17}$$

are derivable from the assumption (14).

We see that inequalities

$$\mathrm{wt}(\mathbf{y}_1+\mathbf{y}_i)=\nu_2(i)+1=n/2\geqslant d-2$$

hold for $2\leqslant i\leqslant n$, and the inequalities

$$\begin{aligned}\mathrm{wt}(\mathbf{y}_i+\mathbf{y}_h)&=\mu_2(i,h)+\mu_3(i,h)\\&=n/2\geqslant d-2\end{aligned}$$

hold for $2\leqslant i<h\leqslant n$, which imply (17). If the inequalities (15) hold for $3\leqslant r\leqslant d-1$, then we have

$$\mathrm{wt}(\mathbf{f}_r)=r+\mathrm{wt}(\mathbf{g}_r)\geqslant d-3,$$

for each r linear combination $\mathbf{f}_r$ chosen from the vectors $\mathbf{x}_1, \mathbf{x}_2,..., \mathbf{x}_n$. By Theorem 1, any codeword is divisible by 4, and $\mathrm{wt}(\mathbf{f}_r)$ must be a multiple of 4. Hence we have

$$\mathrm{wt}(\mathbf{f}_r)\geqslant d \qquad \text{for } 3\leqslant r\leqslant d-1.$$

By the above argument, any element $\mathbf{x}$ in $\mathscr{C}(NH_n)$ satisfies $\mathrm{wt}(\mathbf{x})\geqslant d$, and this completes the proof of Theorem 3.

5. Some Consequences of the Present Method

When we take Hadamard matrix H_4 of order 4, our code $\mathscr{C}(NH_4)$ is equivalent to the Hamming code of length 8. When we take any Hadamard matrix H_{12} of order 12, our code $\mathscr{C}(NH_{12})$ is equivalent to the Golay code of length 24. These facts are easily shown by using Theorems 1 and 2 and the known result that there is only one H-equivalence class in the Hadamard matrices H_n of order n for $n=4$ and 12. (Conf. [8].)

When we apply our method to the case $n=20$, we obtain two new doubly even extremal [40, 20] codes and a doubly even extremal [40, 20] code, which is equivalent to the known code explained in [5, p. 507–509]. By Hall [3], there are three H-equivalent classes of Hadamard matrices of order 20. We can take the Paley matrix $H_{20,1}$, the Williamson matrix $H_{20,2}$ and the matrix $H_{20,3}$ constructed from the symmetric conference matrix of order 10 [8, p. 339], respectively, as the representatives of the three H-equivalent classes. By Theorem 2, our method gives at most three non-equivalent doubly even (extremal) self-dual [40, 20] codes. In the Appendix, we give the right half 20×20 matrices of the generator matrices of the two codes $\mathscr{C}(NH_{20,2})$ and $\mathscr{C}(NH_{20,3})$. Since $\mathscr{C}(NH_{20,1})$ is equivalent to the code explained in [5], we do not give its generator matrix. By virtue of the arguments in Section 4, to prove that the minimal weight of a given [40, 20] code is 8, it is sufficient to verify the inequalities

$$\mathrm{wt}(\mathrm{g}_r) \geqslant 5-r$$

hold for $r=3$ and 4, where g_r runs over all r combinations formed from the row vectors of the right half 20×20 matrix of the generator matrix of the code. These inequalities are easily verified by an electronic computer of lower ability for each one of the codes $\mathscr{C}(NH_{20,2})$ and $\mathscr{C}(NH_{20,3})$. To show that three codes $\mathscr{C}(NH_{20,1})$, $\mathscr{C}(NH_{20,2})$ and $\mathscr{C}(NH_{20,3})$ are inequivalent to one another, we introduce invariants for the equivalence classes of the doubly even extremal [40, 20] codes. Let $\mathcal{O}_i$ $(i=1,2,3)$ be the set of all octads in the code $\mathscr{C}(NH_{20,i})$. By a theorem in [1], we know that each $\mathcal{O}_i$ retains the structure of a $1-(40, 8, 57)$ design. This means that for any one of the 40 coordinates of the code $\mathscr{C}(NH_{20,i})$ there exist exactly 57 octads in $\mathcal{O}_i$ with the nth coordinate 1. Let n_1 and n_2 be the numbers such that $1 \leqslant n_1 < n_2 \leqslant 40$. We say that an octad in $\mathcal{O}_i$ passes through the pair (n_1, n_2) if the n_1th and n_2th coordinates of the octad have the value 1. Let $\mathrm{ind}(n_1, n_2)$ be the number of the octads which pass through the pair (n_1, n_2). We call the number $\mathrm{ind}(n_1, n_2)$ the index of the pair of coordinates (n_1, n_2). If we vary the pair (n_1, n_2), then the value of $\mathrm{ind}(n_1, n_2)$ may vary accordingly. The values $\mathrm{ind}(n_1, n_2)$ and their multiplicities are clearly invariants in the equivalence class of the codes. In each above $\mathcal{O}_i$, we have calculated the values $\mathrm{ind}(n_1, n_2)$ with multiplicities. We only describe the results.

In $\mathcal{O}_1$,

for 20 pairs of (n_1, n_2), $\mathrm{ind}(n_1, n_2)=0$,

for 380 pairs of (n_1, n_2), $\mathrm{ind}(n_1, n_2)=9$,

and

for 380 pairs of (n_1, n_2), $\mathrm{ind}(n_1, n_2)=12$.

In $\mathcal{O}_2$,

for 700 pairs of (n_1, n_2), $\mathrm{ind}(n_1, n_2)=9$

and

for 80 pairs of (n_1, n_2), $\mathrm{ind}(n_1, n_2)=21$.

In $\mathcal{O}_3$,

for 740 pairs of (n_1, n_2), $\mathrm{ind}(n_1, n_2)=9$

and

for 40 pairs of $(n_1 \cdot n_2)$, $\mathrm{ind}(n_1, n_2)=33$.

TABLE I

The Right Half of the Generator Matrix for the Code $\mathscr{C}(NH_{20,2})$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1		1		1				1	1				1	1	1		1	1
3	1	1	1	1	1	1			1		1			1			1	1		
4	1			1			1		1	1		1		1	1	1	1	1		
5	1	1		1	1			1	1	1			1	1	1				1	
6	1			1	1	1	1	1			1	1			1			1	1	
7	1	1	1		1		1			1	1	1	1		1		1			
8	1	1	1	1			1	1				1		1			1		1	1
9	1	1				1	1	1	1				1		1		1	1		1
10	1		1			1		1	1	1	1	1		1	1					1
11	1			1	1			1	1		1	1	1			1	1			1
12	1	1	1		1				1			1			1	1		1	1	1
13	1	1	1	1		1		1		1		1	1			1		1		
14	1	1				1	1		1		1	1	1	1		1			1	
15	1		1					1			1		1	1	1	1	1	1	1	
16	1		1		1	1	1	1	1	1						1	1		1	
17	1				1	1				1		1	1	1			1	1	1	1
18	1	1			1		1	1		1	1			1		1		1		1
19	1		1	1			1		1	1	1		1					1	1	1
20	1		1	1	1	1	1						1	1	1	1				1

TABLE II

The Right Half of the Generator Matrix for the Code $\mathscr{C}(NH_{20,3})$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1			1		1		1		1	1			1		1	
3	1	1	1	1	1					1	1	1		1	1					1
4	1	1	1	1		1		1			1	1	1			1		1		
5	1		1		1	1	1			1	1		1			1	1			1
6	1			1	1	1	1	1			1			1	1		1	1		
7	1	1			1	1	1		1		1	1			1	1			1	
8	1			1		1		1	1	1	1			1		1			1	1
9	1	1					1	1	1	1	1	1					1	1		1
10	1		1		1			1	1	1	1		1		1			1	1	
11	1										1	1	1	1	1	1	1	1	1	1
12	1	1			1	1		1		1		1	1	1			1		1	
13	1		1			1	1	1	1			1	1	1	1					1
14	1			1	1		1		1	1		1	1	1		1		1		
15	1	1		1	1			1	1				1		1	1	1			1
16	1	1	1			1			1	1				1	1	1	1	1		
17	1		1	1			1	1		1		1			1	1	1		1	
18	1	1	1		1		1	1						1		1		1	1	1
19	1		1	1	1	1			1			1					1	1	1	1
20	1	1		1		1	1			1			1		1			1	1	1

By the above calculation, we can say that three codes $\mathscr{C}(NH_{20,1})$, $\mathscr{C}(N_{20,2})$ and $\mathscr{C}(NH_{20,3})$ are inequivalent to one another, and we summarize the results as

THEOREM 4. *There are at least three inequivalent doubly even self-dual extremal* [40, 20] *codes.*

6. A CONCLUDING REMARK AND TWO REMAINING QUESTIONS

Remark. When we apply our method to the case $n=36$, we may get a doubly even self-dual [72, 36, 16] code, which has not been found by anyone [7]. We have tested some Hadamard matrices H_{36} of order 36 hoping to find such a code. We have not found a [72, 36, 16] code by our present method. Many [72, 36] codes obtained by our method seem to have the minimal weight 12, and some minimal weight 8! By [2], there are at least 110 H-equivalence classes at order 36. We are not so patient as to test such enormous H-equivalence classes of Hadamard matrices.

Theoretically, there remain two fundamental questions.

(I) Are two codes $\mathscr{C}(NH_n^{(1)})$ and $\mathscr{C}(NH_n^{(2)})$ not equivalent to each other if the Hadamard matrices of order n $NH_n^{(1)}$ and $NH_n^{(2)}$ are not H-equivalent?

This is the converse assertion to Theorem 2.

(II) Is there a method to define doubly even self-dual codes from Hadamard matrices of order n in the case $n \equiv 0 \pmod 8$?

APPENDIX

We give the right half 20×20 matrices K_2 and K_3 of the generator matrices of the two codes $\mathscr{C}(NH_{20,2})$ and $\mathscr{C}(NH_{20,3})$ (Tables I, II). The blanks mean the zeros. Each generator matrix C_2 (resp. C_3) of $\mathscr{C}(NH_{20,2})$ (resp. $\mathscr{C}(NH_{20,3})$) is given by

$$C_2 = (I_{20} K_2) \qquad (\text{resp. } C_3 = (I_{20} K_3)).$$

REFERENCES

1. E. F. ASSMUS, JR. AND H. F. MATTSON, JR., New 5-designs, *J. Combin. Theory* **6** (1969), 122–151.

2. J. COOPER, J. MILAS, AND W. D. WALLIS, Hadamard equivalence, *in* "Combinatorial

Mathematics, Proc. Canberra, 1977" (D. A. Halton and J. Seberry, Eds.) Lecture Notes in Mathematics Vol. 686 pp. 126–135, Springer-Verlag, Berlin/New York/Heidelberg, 1978.

3. M. Hall, Jr., "Hadamard Matrices of Order 20," Jet Propulsion Laboratory Technical Report No. 32-761, 1965.
4. J. van Lint, "Introduction to Coding Theeory," Graduate Texts in Mathematics Vol. 86 Springer-Verlag. Berlin/New York/Heidelberg, 1981.
5. F. J. MacWilliams and N. J. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam/New York/Oxford, 1977.
6. V. Pless, "An Introduction to the Theory of Error Correcting Codes," Wiley–Interscience, New York, 1982.
7. N. J. A. Sloane, Is there a (72, 36) $d=16$ Self-dual Code? *IEEE Trans. Inform. Theory* **IT-19** (1973), 251.
8. W. D. Wallis, A. P. Street, and J. S. Wallis, "Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices." Lecture Notes in Mathematics Vol. 292, Springer-Verlag, Berlin/New York/Heidelberg, 1972.