Codes from Hadamard Matrices and Profiles of Hadamard Matrices, II

Cantian Lin
Department of Mathematics
University of Nevada, Las Vegas
Las Vegas, NV 89154

Haiping Lin
Department of Mathematics
Southern Illinois University
Carbondale, IL 62901

ABSTRACT. In this paper, we investigate the relationship between the profiles of Hadamard matrices and the weights of the doubly even self-orthogonal/ dual $[n, m, d]$ codes from Hadamard matrices of order $n = 8t$ with $t \geq 1$. We show that such codes have $m \leq \frac{n}{2}$, and give some computational results of doubly even self-orthogonal/dual $[n, m, d]$ codes from Hadamard matrices of order $n = 8t$, with $1 \leq t \leq 9$.

van Lint [12] recently commented: "We do not know if the construction of the extremal code using a Hadamard design (matrix) has been tried in a systematic way." He also mentions that it seems that the existence of a doubly even self-dual $[72, 36, 16]$ code is still open.

Assmus and Key [1] recently considered Hadamard matrices from the viewpoint of coding theory and classified the binary codes from Hadamard matrices of order 24. They also mention that the next case to consider is the binary codes from Hadamard matrices of order 32.

In this paper, we investigate the relationship between the profiles of Hadamard matrices and the weights of the doubly even self-orthogonal/dual $[n, m, d]$ codes from Hadamard matrices of order $n = 8t$ with $t \geq 1$. We show that such codes have $m \leq \frac{n}{2}$, and give an efficient method to determine d. Finally we give some computational results of doubly even self-orthogonal/dual $[n, m, d]$ codes from Hadamard matrices of order $n = 8t$, with $1 \leq t \leq 9$.

For convenience and completeness, we include some necessary notations.

A binary linear $[n, m]$ code C is an m-dimensional subspace of the n-dimensional vector space V_n over $GF(2)$. The elements of the code are called codewords. The addition of codewords is componentwise, and for each component of two codewords addition is defined as follows

$$0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=0. \tag{1}$$

The Hamming weight (or weight) of codeword v is the number of digits 1 occuring in v. A code is called even if all weights of the codewords are even. A code is called doubly even if all weights of the codewords are divisible by 4. A binary linear $[n, m, d]$ code is an $[n, m]$ code in which the minimum weight of all nonzero codewords is d.

A matrix G is called a generator matrix of the binary linear code C if the linear span of its rows is C.

Given an $[n, m]$ code C, the $[n, n-m]$ code

$$C^{\perp} = \{x \epsilon V_n : y^T x = 0 \; for \; each \; y \epsilon C\}$$

is called the orthogonal or dual code of C. The generator matrices of the dual code $C^{\perp}$ are called parity check matrices of C. If $C \subset C^{\perp}$, then C is called self-orthogonal; if $C = C^{\perp}$, then C is called self-dual.

Given a (0,1)-matrix G, we define a (-1,1)-matrix

$$\bar{G} = J - 2G \tag{2}$$

where J has all entries +1. In other words, we change (1,0)-entries in G to (-1,1)-entries in $\bar{G}$, respectively. We call $\bar{G}$ the (-1,1)-matrix corresponding to G.

We define the Hadamard product of two vectors

$$z_1 = (z_{11}, \; z_{12}, \dots, \; z_{1n}),$$

$$z_2 = (z_{21}, \; z_{22}, \dots, \; z_{2n})$$

as follows:

$$z_1 \otimes z_2 = (z_{11}z_{21}, \; z_{12}z_{22}, \dots, \; z_{1n}z_{2n}) \tag{3}$$

i.e. the Hadamard product is componentwise. In particular, for any (-1,1)-vector z, we have $z \otimes z = J$.

It is clear that (1) corresponds to the Hadamard product

$$1 \cdot 1 = 1, \quad 1 \cdot (-1) = -1, \quad (-1) \cdot 1 = -1, \quad (-1) \cdot (-1) = 1 \tag{4}$$

as 0, 1 correspond to 1, -1 respectively. Thus by (1) and (2), the addition of any two binary linear codewords v_1, v_2 is equivalent to the Hadamard product of their corresponding (-1,1)-vectors $\overline{v}_1, \overline{v}_2$. Therefore,

$$b = g_{i_1} + g_{i_2} + \cdots + g_{i_k} \tag{5}$$

is equivalent to

$$\overline{b} = \overline{g}_{i_1} \otimes \overline{g}_{i_2} \otimes \ldots \otimes \overline{g}_{i_k} \tag{6}$$

where g_{i_1}, $g_{i_2}, \ldots g_{i_k}$ are rows of G and $\overline{g}_{i_1}, \overline{g}_{i_2}, \ldots, \overline{g}_{i_k}$ are rows of $\overline{G}$.

For a (-1,1)-matrix $\overline{G}$, we define the generalized inner product $P_{i_1 i_2 \ldots i_k}$, as follows,

$$P_{i_1 i_2 \ldots i_k} = \sum_{j=1}^{n} \overline{g}_{i_1 j} \overline{g}_{i_2 j} \cdots \overline{g}_{i_k j} \tag{7}$$

where $\overline{g}_{i_1 j}, \overline{g}_{i_2 j}, \ldots, \overline{g}_{i_k j}$ are the entries of rows $i_1, i_2, \ldots, i_k$ and column j of $\overline{G}$ and n is the length of $\overline{g}_i$. We define the k-Profile $\pi_k(m)$ as follows,

$$\pi_k(m) = number\ of\ sets\ \{i_1,\ i_2, \ldots,\ i_k\} \tag{8}$$

such that

$$|P_{i_1 i_2 \ldots i_k}| = m. \tag{9}$$

By (1)-(7), the minimum weight of a binary linear $[n, m, d]$ code is equal to the minimum value of $\frac{1}{2}(n - P_{i_1 i_2 \ldots i_k})$ for all k ($1 \leq k \leq n$) and all $i_1, i_2, \ldots, i_k$.

An Hadamard matrix H of order n is an n by n matrix with all entries in the set of {-1, 1} such that

$$HH^T = nI.$$

It is known that if there is an Hadamard matrix of order n, then $n = 1$, or $n = 2$, or n is a multiple of 4. We assume that the first row of H has all -1 entries by appropriate negation, then we denote by H° the rows 2 through n of H.

Let G be a binary generator matrix from Hadamard matrices of order $n = 8t$, with $t \geq 1$, the $[n, m, d]$ code is linear span over $GF(2)$ of rows of G, where m is the maximum number of linearly independent rows of G.

Theorem 1. *$[n, m, d]$ codes are doubly even self-orthogonal/dual with $m \leq \frac{n}{2}$. In addition, if $m = \frac{n}{2}$, then $[n, m, d]$ codes are doubly even self-dual $[n, \frac{n}{2}, d]$ codes.*

Proof: It can be easily verified that for $n = 8t$ with $t \geq 1$, we have

$$GG^T \equiv 0 \, (mod\, 2) \tag{10}$$

$$GJ \quad \equiv 0 \, (mod\, 4). \tag{11}$$

Thus, the code from the linear span over $GF(2)$ of rows of G is self orthogonal by (10), and is doubly even by (11) and a theorem in [9;p14]. Therefore, the $[n, m, d]$ code from the linear span over $GF(2)$ of rows of G is self orthogonal and doubly even.

By applying a theorem in [8;p49], we get

$$m \leq \frac{n}{2}.$$

In addition, if $m = \frac{n}{2}$, then we have doubly even self-dual $[n, \frac{n}{2}, d]$ codes. □

The profiles of Hadamard matrices have been used in the investigating of equivalence of Hadamard matrices ([6], [7]) because equivalent Hadamard matrices have the same profiles. In the following, we illustrate the relationship between the profiles of Hadamard matrices and the weights of codes from Hadamard matrices of order $8t$ with $t \geq 1$, which can be used to determine d.

Lemma 1 (see [13; p427]). *If H is an Hadamard matrix of order n ($n \geq 4$), and k is even, then $P_{i_1 i_2 \ldots i_k}$ and hence $\mid P_{i_1 i_2 \ldots i_k} \mid$ are congruent to n modulo 8 when 4 divides k, and are congruent to 0 modulo 8 when k is congruent to 2 modulo 4.*

Thus, we have

Lemma 2. *If $n = 8t$ with $t \geq 1$, then*

$$P_{i_1 i_2 \ldots i_k}(H) \equiv 0 \, (mod\, 8)$$

and

$$\frac{1}{2}[n - P_{i_1 i_2 \ldots i_k}(H)] \equiv 0 \, (mod\, 4)$$

where k is even and $k \geq 4$.

Theorem 2. *If H is an Hadamard matrix of order $n = 8t$ with $t \geq 1$ and $k \geq 4$, then for H° we have*

$$P_{i_1 i_2 \ldots i_k}(H^\circ) \equiv 0 \, (mod\, 8)$$

and

$$\frac{1}{2}[n - P_{i_1 i_2 \ldots i_k}(H^\circ)] \equiv 0 \ (mod\, 4)$$

Proof: The result follows from the method in Theorem 2 in [5].

Theorem 3. *If H is an Hadamard matirx of order $n = 8t$ with $t \geq 1$, then the $[n, m, d]$ code from H has weights*

$$\frac{1}{2}[n - |P_{i_1 i_2 \ldots i_k}(H)|]$$

$$\frac{1}{2}[n + |P_{i_1 i_2 \ldots i_k}(H)|]$$

and hence $d \geq 4$ where k is even.

Proof: The weights which do not involve row 1 of the generator matrix G are

$$\frac{1}{2}[n - P_{i_1 i_2 \ldots i_k}(H^\circ)],$$

the weights which do involve row 1 of the generator matrix G are

$$n - \frac{1}{2}[n - P_{i_1 i_2 \ldots i_k}(H^\circ)]$$

$$= \frac{1}{2}[n + P_{i_1 i_2 \ldots i_k}(H^\circ)].$$

Thus, the weights are

$$\frac{1}{2}[n - |P_{i_1 i_2 \ldots i_k}(H^\circ)|]$$

and

$$\frac{1}{2}[n + |P_{i_1 i_2 \ldots i_k}(H^\circ)|].$$

Note that

$$P_{i_1 i_2 \ldots i_k}(H) = P_{i_1 i_2 \ldots i_k}(H^\circ)$$

and by Theorem 2, we have $d \geq 4$. □

It is known that there is only one equivalence class of Hadamard matrix of order 8. We found the doubly even self-dual [8,4,4] code. It is known ([2]) that there are exactly 5 equivalence classes of Hadamard matrices of order 16. From these 5 equivalence classes, we found the doubly even self-orthogonal/dual [16,5,8], [16,6,4], [16,7,4] and [16,8,4] codes.

It is known ([3], [4]) that there are exactly 60 equivalence classes Hadamard matrices of order 24. We found the doubly even self-dual [24,12,4] code. The binary codes from Hadamard matrices of order 24 have been classified by Assmus and Key ([1]).

66,104 equivalence classes of Hadamard matrices of order 32 have been constructed and classified in [7]. We computed some of these equivalence classes and found doubly even self-orthogonal/dual [32,12,4], [32,13,4], [32, 16,4] and [32,16,8] codes.

We constructed some equivalence classes of Hadamard matrices of orders 40,48,56,64,72 and found doubly even self-orthogonal/dual [40,20,4], [48,22,4], [48,23,4], [48,24,4], [48,24,12], [56,28,4], [64,27,4], [64,28,4], [64, 29,4], [64,30, 4], [64,31,4], [72,36,4], [72,36,8], [72,36,12] codes which verify our results. We did not find [72,36,16] code from Hadamard matirces of order 72. It seems that some other doubly even self-orthogonal/dual $[n, m, d]$ codes could also be found by constructing more equivalence classes of Hadamard matrices of orders 40,48,56,64,72.

Acknowledgement. The authors thank the referee for useful comments and suggestions on an earlier version of this paper, the authors also thank W.D. Wallis and J.L. Yucas for helpful discussion and suggestions on this paper.

References

[1] E.F. Assmus Jr. and J.D. Key, Hadamard matrices and their designs: a coding-theoretic approach, *Trans. of AMS*, 330(1992), 269–293.

[2] M. Hall Jr., Hadamard matrices of order 16, *J.P.L. Research Summary No.36-10*, 1(1961), 21–26.

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

[4] H. Kimura, New Hadamard matrix of order 24, *Graphs and Combinatorics*, 5(1989), 235–242.

[5] C. Lin, H. Lin, W.D. Wallis and J.L. Yucas, Codes from Hadamard matrices and profiles of Hadamard matrices, *JCMCC*, 12(1992), 57–64.

[6] C. Lin and W.D. Wallis, Profiles of Hadamard matrices of order 24, *Congressus Numerantium*, 66(1988), 93–102.

[7] C. Lin, W.D. Wallis and Zhu Lie, Equivalence classes of Hadamard matrices of order 32, *Congressus Numerantium*, 95(1993), 179–182.

[8] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes", Amsterdam-New York-Oxford, North Holland, 1977

[9] V. Pless, "Introduction to the Theory of Error-Correcting Codes", John Wiley and Sons, New York, 1982.

[10] N.J.A. Sloane, Is there a (72,36) d=16 self-dual code?, *IEEE Trans. Inform. Theory*, IT-19(1975), 251.

[11] V.D. Tonchev, Self-orthogonal designs and extremal doubly even codes, *J. Comb. Theory, A* 52(1989), 197–205.

[12] J.H. van Lint, Codes and combinatorial designs, "Coding Theory, Design Theory and Graph Theory", John Wiley, New York, 1993, 31–39.

[13] W.D. Wallis, On the zeroes of profiles, *J. Austral. Math. Soc., A* 47(1989), 424–429.