Codes from Hadamard Matrices and Profiles of Hadamard Matrices

Cantian Lin
Department of Mathematical Sciences
University of Nevada
Las Vegas, NV, 89154

Haiping Lin, W.D. Wallis, and J.L. Yucas
Department of Mathematics Southern Illinois University
Carbondale, IL, 62901

Abstract. In this paper, we illustrate the relationship between profiles of Hadamard matrices and weight distributions of codes, give a new and efficient method to determine the minimum weight d of doubly even self-dual $[2n, n, d]$ codes constructed by using Hadamard matrices of order $n = 8t + 4$ with $t \geq 1$, and present a new proof that the $[2n, n, d]$ codes have $d \geq 8$ for all types of Hadamard matrices of order $n = 8t + 4$ with $t \geq 1$. Finally we discuss doubly even self-dual $[72, 36, d]$ codes with $d = 8$ or $d = 12$ constructed by using all currently known Hadamard matrices of order $n = 36$.

I. Introduction

In his recent expository survey [16], van Lint comments: "We do not know if the construction of the extremal code using a Hadamard design 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. In this paper we shall illustrate the relationship between the profiles of a Hadamard matrix and the weight distribution of a doubly even self-dual $[2n, n, d]$ code constructed from a Hadamard matrix of order $n = 8t+4$ with $t \geq 1$ and then give a new and efficient method to determine the minimum weight d of the code, based on the profiles of the Hadamard matrix. The computation time of our method is a quarter of the computation time of the best previous method in the literature (see [12]). We present a different proof that doubly even self-dual $[2n, n, d]$ codes constructed by using Hadamard matrices of order $n = 8t + 4$ with $t \geq 1$ have $d \geq 8$ for all types of Hadamard matrices of order $n = 8t + 4$ with $t \geq 1$. The proof is different than that of [14] and [15]. Finally, we use our method to discuss doubly even self-dual $[72, 36, d]$ codes with $d = 8$ or $d = 12$ constructed by using all currently known Hadamard matrices of order $n = 36$.

For completeness and convenience, we now give 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 in 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 code C if the linear span of its rows is C.

Given an $[n, m]$ code C, the $[n, n-m]$ code $C^{\perp} = \{x \in V_n : y^T x = 0$ for each $y \in C\}$ 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

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

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

We define the Hadamard product of two vectors z_1, z_2 as follows

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

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

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

Thus by (1) and (2), the sum 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

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

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

For a $(-1, 1)$-matrix $\overline{G}$, we define the generalized inner product $P_{i_1 i_2 \ldots i_k}$, and the k-Profile $\pi_k(m)$ 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 $\overline{g}_i$.

$$\pi_k(m) = \text{number of sets} \{i_1, i_2, \ldots, i_k\} \text{ such that } |P_{i_1 i_2 \ldots i_k}| = m. \tag{8}$$

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

II. Codes from Hadamard Matrices

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

$$HH^T = nI. \tag{9}$$

It is known that if there is a Hadamard matrix of order n. then $n = 1$, or $n = 2$, or n is a multiple of 4.

A Hadamard matrix H is called normalized if all the entries of its first row and first column are +1. For convenience, we denote by $H°$ rows 2 through n of the normalized Hadamard matrix H.

We now describe two ways of constructing codes from Hadamard matrices.

Type 1: If H is a normalized Hadamard matrix of order $n = 8t+4$, let $\overline{B}$ be the matrix.by deleting the first row and first column of H and $b = \frac{1}{2}(J+\overline{B})$. Then the codewords are all linear combinations over GF(2) of rows of (I, B). This code is self-dual (see [1] and [15]).

Type 2: Write

$$A = \begin{bmatrix} 0 & J \\ J^T & B \end{bmatrix}$$

where $J = (1, 1, \ldots, 1)$ and B is defined as in Type 1. Then the codewords are the linear span over GF(2) of rows of (I, A). This is also self-dual (see [1] and [15]).

Profiles of Hadamard matrices have been used in the investigation of eqivalence of Hadamard matrices (see [4],[10],[17],[18] and [19]) because equivalent Hadamard matrices have the same profiles. In the following, we illustrate a relationship between the profiles of a Hadamard matrix and the weight distribution of a code constructed from the Hadamard matrix of order $8t+4$ with $t \geq 1$, and then use this relationship to give a new and efficient method to determine the minimum wight d of the code.

Theorem 1 ([18, p427]). *If H is an Hadamard matrix of order $n (n \geq 4)$, and k is even, then $P_{i_1 i_2 \ldots i_k}(H)$ and hence $|P_{i_1 i_2 \ldots i_k}(H)|$ 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.*

Theorem 2. *If H is a normalized Hadamard matrix of order $n (n \geq 4)$ and $k \geq 4$, then for $H°$*

$$P_{i_1 i_2 \ldots i_k}(H°) \equiv n \pmod 8 \quad \textit{if } k \equiv 0 \textit{ or } 3 \pmod 4$$
$$P_{i_1 i_2 \ldots i_k}(H°) \equiv 0 \pmod 8 \quad \textit{if } k \equiv 1 \textit{ or } 2 \pmod 4.$$

Proof: If $k \equiv 0 \pmod 4$ or $k \equiv 2 \pmod 4$, then the results follow directly from Theorem 1. If $k \equiv 3 \pmod 4$ or $k \equiv 1 \pmod 4$, then

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

since all the entries of row 1 of a normalized Hadamard matrix are +1's. Now apply Theorem 1, the result follows.

Theorem 3. *If H is a normalized Hadamard matrix of order $n (n \geq 4)$ and $k \geq 4$, then*

$$P_{i_1 i_2 \ldots i_k}(H^\circ) = P_{j_1 j_2 \ldots j_{n-1-k}}(H^\circ)$$

where $\{i_1, i_2, \ldots, i_k\} \cup \{j_1, j_2, \ldots, j_{n-1-k}\}$ is a partition of $\{2, 3, \ldots, n\}$.

Proof: Since H is a normalized Hadamard matrix, except for column 1 every column has exactly $\frac{n}{2}$ of -1's, we have

$$P_{i_1 i_2 \ldots i_k j_1 j_2 \ldots j_{n-1-k}}(H^\circ) = P_{23 \ldots n}(H^\circ) = n.$$

So the Hadamard product of rows $i_1, i_2, \ldots, i_k$ is equal to the Hadamard product of rows $j_1, j_2, \ldots, j_{n-1-k}$, thus

$$P_{i_1 i_2 \ldots i_k}(H^\circ) = P_{j_1 j_2 \ldots j_{n-1-k}}(H^\circ).$$

Theorem 4. *If H is a normalized Hadamard matrix of order $n (n \geq 4)$ and $k \geq 4$, then $P_{i_1 i_2 \ldots i_k}(H^\circ)$ when k is even is equivalent to $P_{i_1 i_2 \ldots i_k}(H^\circ)$ when k is odd.*

Proof: The result follows from Theorem 3.

Theorem 5. *If H is a normalized Hadamard matrix of order $n (n \geq 4)$ and $k \geq 4$, then $P_{i_1 i_2 \ldots i_k}(H)$ for $2 \leq k \leq \frac{n}{2}$ is equivalent to $P_{i_1 i_2 \ldots i_k}(H^\circ)$ for $1 \leq k \leq n-1$.*

Proof: The result follows from Theorem 2 and 4.

Theorem 6. *If H is a normalized Hadamard of order n, then the weights of the code of Type 2 are*

$$k + \frac{1}{2}\left(n - |P_{i_1 i_2 \ldots i_k}(H)|\right) + \frac{\left[1 + (-1)^{k+1}\right]}{2},$$
$$k + \frac{1}{2}\left(n + |P_{i_1 i_2 \ldots i_k}(H)|\right) + \frac{\left[1 + (-1)^{k+1}\right]}{2},$$

where k is even and $2 \leq k \leq \frac{n}{2}$.

Proof: By Theorems 2 and 4, the weights of the code of Type 2 which do not involve row 1 of the generator matrix are

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

the weights which involve row 1 are

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

i.e.

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

Then the result follows from Theorem 5.

Theorem 7. *If H is a normalized Hadamard matrix of order n, then the minimum weight d of the code of Type 2 is*

$$d=\min\{k+\frac{1}{2}\left(n-|P_{i_1 i_2 \ldots i_k}(H)|\right)+\frac{[1+(-1)^{k+1}]}{2},$$
$$k+\frac{1}{2}\left(n+|P_{i_1 i_2 \ldots i_k}(H)|\right)+\frac{[1+(-1)^{k+1}]}{2},$$

where k is even and $2 \leq k \leq \frac{n}{2}$.

Note that the computation time of our method is a quarter the time of the best previously known method (see [12]).

Theorem 8 ([4], [10]). *If H is a normalized Hadamard matrix of order* $n = 8t+4$, *then* $|P_{i_1 i_2 i_3 i_4}(H)| \neq n$.

Theorem 9. *If H is a normalized Hadamard matrix of order* $n = 8t+4$ *with* $t \geq 1$, *the the corresponding codes of Type 1,2 have a minimum weights* $d \geq 7, 8$ *respectively.*

Proof: Here we only consider Type 2; the other case is similar. By Theorem 8, $|P_{i_1 i_2 i_3 i_4}(H)| \leq (8-1)t+4$, so by Theorems 2 and 6, $d_{i_1 i_2 i_3} \geq 8$ and $d_{i_1 i_2 i_3 i_4} \geq 8$. By Theorem 1 again, $|P_{i_1 i_2 i_3 i_4 i_5 i_6}(H)| \leq 8t$, thus by Theorems 2 and 6, $d_{i_1 i_2 i_3 i_4 i_5} \geq 8$ and $d_{i_1 i_2 i_3 i_4} \geq 8$, Finally, by Theorems 2 and 6, it is obvious that $d_{i_1 i_2 i_3 i_4 i_5 i_6 i_7 i_8} \geq 8$. The required result follows immediately.

Theorem 10. *If H is a normalized Hadamard matrix of order* $n = 8t+4$ *with* $t \geq 1$, *then the code of Type 2 is a doubly even self-dual* $[2n, n, d]$ *code with minimum weight* $d \geq 8$.

Proof: The self-duality of the code follows from Theorem 2.1 in [1]. By Theorems 2 and 6, we have that if $k \equiv 0$ or $3 \pmod 4$, then the weights are congruent to 0 $\pmod 4$, if $k \equiv 1$ or $2 \pmod 4$, then the weights are congruent to $0 \pmod 4$. It follows from Theorem 9 that $d \geq 8$.

III. Codes from Hadamard Matrices of Lower Orders

The profiles of Hadamard matrices of order 12 can be found in [19] and the corresponding code is the well-known Golay code $[24, 12, 8]$. The profiles of Hadamard matrices of order 20 can be found in [19] and the corresponding codes are doubly even self-dual codes $[40, 20, 8]$. Many Hadamard matrices of order 28 have been constructed in [6],[7], [8] and [9]. Equivalence classes of extremal doubly-even codes from Hadamard matrices of order 20 and 28 have been considered in [2] and [3]. We computed the 4-profiles of the 487 equivalence classes of Hadamard matrices of order 28 listed in [6], [7],[8] and [9], and found that each Hadamard matrix of order 28 has same 4-profiles as its transpose. We applied Theorems 6 and 7 to these 4-profiles and found that all the codes from Hadamard matrices of order 28 are doubly even self-dual codes $[56, 28, 8]$. The 4-profiles of Hadamard matrices of order 28 are available from the authors.

The question of the existence of a doubly even self-dual $[72, 36, 16]$ code has been mentioned in, for example, [13],[15] and [16]. It still appears to be open (see [16]).

It is appealling to try to find a doubly even self-dual $[72, 36, 16]$ code by using a Hadamard matrix of order 36. Since the method in [12] requires lengthy computations, only some of the cuurently known equivalence classes of Hadamard matrices of order 36 were tested in that paper, and only doubly even self-dual $[72, 36, 8]$ and $[72, 36, 12]$ codes were found.

We applied Theorems 6 and 7 to the 4-profiles of the 110 equivalence classes of Hadamard matrices of order 36 listed in [4]. Without further computation we saw immediately that the majority of $[72, 36]$ codes of Type 2 constructed from these equivalence classes are of minimum weight $d = 8$, and some of the remainder are of minimum weight $d = 8$ or 12. By further computing 6-profiles, we found that the codes of the remaining cases are of minimum weight $d = 8$ or 12.

By applying our method to first four rows of the normalized Hadamard matrices of order 36 constructed from [11], it is immediate that the code of Type 2 is of minimum weight $d = 8$. We computed the 4-profile of Hadamard matrix of order 36 in [5]; it is

$$\pi(4) = 52920, \ \pi(12) = 5040, \ \pi(20) = 0, \ \pi(28) = 945, \ \pi(36) = 0.$$

Hence the code Type 2 is of minimum weight $d = 8$.

Thus we have not found a $[72, 36, 16]$ code from all currently known Hadamard matrices of order 36. We tabulate the results of computations below. The first eleven constructions are listed in [4], and follow the notation there. The twelveth and thirteenth constructions come from [11] and [5] respectively.

(1) CONSTRUCTION 1 Codes 1 through 79: $d = 8$, Code 80: $d = 8$ or 12.
(2) CONSTRUCTION 2 Codes I through IX: Codes XI,XII,XV,XVI and XVII: $d = 8$, Codes X,XIII and XIV: $d = 8$ or 12.
(3) CONSTRUCTION 3 Code: $d = 8$.
(4) CONSTRUCTION 4 Codes 1,2, and 4: $d = 8$, Code 3: $d = 8$ or 12.
(5) CONSTRUCTION 5 Code: $d = 8$ or 12.
(6) CONSTRUCTION 6 Code: $d = 8$.
(7) CONSTRUCTION 7 Code: $d = 8$ or 12.
(8) CONSTRUCTION 8 Code: $d = 8$ or 12.
(9) CONSTRUCTION 9 Code: $d = 8$ or 12.
(10) CONSTRUCTION 10 Codes 1 through 9: $d = 8$, Code 10: $d = 8$ or 12, Codes 11,12 and 13: $d = 8$.
(11) CONSTRUCTION 11 Codes 1 through 4: $d = 8$.
(12) CONSTRUCTION 12 Code: $d = 8$.
(13) CONSTRUCTION 13 Code: $d = 8$.

Acknowledgements

The authors thank the referee for helpful comments on an earlier version of this paper. This research was carried out while the first author was at the Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931.

References

1. V.K. Bhargava and J.M. Stein, (v, k, λ) *Configurations and Self-Dual Codes*, Inform. and Control **28** (1975), 352–355.
2. F.C. Bussemaker and V.D. Tonchev, *New extremal doubly-even codes of length 56 derived from Hadamard matrices of order 28*, Discrete Math. **76** (1989), 45–49.
3. F.C. Bussemaker and V.D. Tonchev, *Extremal doubly-even codes of lenght 40 derived from Hadamard matrices of order 20*, Discrete Math. **82** (1990), 317–321.
4. J. Cooper, J. Milas and W.D. Wallis, *Hadamard equivalence*, Combinatorial Mathematics, Proc. Canberra, 1977, Lecture Notes in Mathematics **686**, 126–135.
5. N. Ito and J.S. Leon, *Note: An Hadamard Matrix of order 36*, J. Comb. Theory A34 (1983), 244–247.
6. H. Kimura, *On equivalence of Hadamard matrices*, Hokkaido Math. J. **17** (1988), 139–146.
7. H. Kimura, *Classification of Hadamard matrices of order 28 with Hall sets and new matrices*. preprint.

8. H. Kimura and H. Ohmori, *Construction of Hadamard matrices of order 28*, Graphs and Comb. 2 (1986), 247–257.
9. H. Kimura and H. Ohmori, *Hadamard matrices of order 28*, Mem. Fac. Educ. Ehime Univ. Nat. Sci. 7 (1987), 7–57.
10. C. Lin and W.D. Wallis, *Profiles of Hadamard Matrices of order 24*, Congressus Numerantium 66 (1988), 93–102.
11. J.Q. Longyear, *Note: A New Construction for Hadamard Matrices of Orders* $8t+4$, J. Comb. Theory A38 (1985), 99–104.
12. M. Ozeki, *Hadamard Matrices and Doubly Even Self-Dual Erroe-correcting Codes*, J. Comb. Theory A44 (1987), 274–287.
13. N.J.A. Sloane, *Is there a* $(72,36)$ $d = 16$ *Self-dual Code?*, IEEE Trans, Inform. Theory IT-19 (1973), 251.
14. V.D. Tonchev, *Block designs of Hadamard type and self-dual codes*, Problemy Peredachi Informatsii 19 No. 4 (1983), 25–30.
15. V.D. Tonchev, *Self-orthonogal Designs and Extremal Doubly Even Codes*, J. Comb. Theory A52 (1989), 197–205.
16. J.H. van Lint, *Codes and Combinatorial Designs.* to appear in Proceeding of Marshall Hall Memorial Conference.
17. W.D. Wallis, *Hadamard equivalence*, Congressus Numerantium 28 (1980), 15–25.
18. W.D. Wallis, *On the Zeroes of Profiles*, J. Austral. Math. Soc. A47 (1989), 424–429.
19. W.D. Wallis, "Combinatorial Designs", Marcel Dekker, New York, 1989.