FACTA UNIVERSITATIS (NIŠ)
SER. MATH. INFORM. Vol. 34, No 4 (2019), 797–803
https://doi.org/10.22190/FUMI1904797F

THE WEIGHT HIERARCHY OF HADAMARD CODES

Farzaneh Farhang Baftani and Hamid Reza Maimani*

Abstract. The support of an (n, M, d) binary code C over the set $\mathbf{A} = \{0, 1\}$ is the set of all coordinate positions i, such that at least two codewords of C have distinct entry in coordinate i. If C is a code of size M, then r-th generalized Hamming weight, $d_r(C)$, $1 \leq r \leq 1 + log_2(M-1)$, of C is defined as the minimum of the cardinalities of the supports of all subset of C of cardinality $2^{r-1} + 1$. The sequence $(d_1(C), d_2(C), \ldots, d_k(C))$ is called the Hamming weight hierarchy (HWH) of C. In this paper we obtain HWH for $(2^k - 1, 2^k, 2^{k-1})$ binary Hadamard code corresponding to Sylvester Hadamard matrix H_{2^k} and we show that

$$d_r = 2^{k-r}(2^r - 1).$$

Also we compute the HWH of $(4n - 1, 4n, 2n)$ Hadamard codes for $2 \leq n \leq 8$.
Keywords. Binary code; Hamming weight; Hadamard codes.

1. introduction

Let $\mathbf{A} = \{0, 1\}$. For positive integer n, every non-empty subset, C, of $\mathbf{A}^n$ is called a *binary code* of length n. The *Hamming distance* of two vectors X, Y is defined the number of the coordinates that they differ and is denoted by $d(X, Y)$. The Hamming distance of C is denoted by $d = d(C)$ and defined as

$$\min_{X \neq Y \in C} d(X, Y).$$

A binary code C of length n, size M and distance d is called (n, M, d) binary code. The *support* of an (n, M, d) binary code C over the set $\mathbf{A} = \{0, 1\}$ is the set of all coordinate positions i, such that at least two codewords have distinct entry in coordinate i and is denoted by $supp(C)$. The *rth generalized Hamming weight* (GHW), $d_r(C)$, $1 \leq r \leq 1 + log_2(M-1)$, of C is defined as follows

Received June 25, 2019; accepted August 03, 2019
2010 *Mathematics Subject Classification.* Primary 94B25; Secondary 05B20
*Corresponding Author

$$d_r = d_r(C) = \min\{\|D\| : D \subset C, |D| = 2^{r-1} + 1\},$$

where $\|D\| = |supp(D)|$. The sequence $(d_1(C), d_2(C), \ldots, d_k(C))$ is called the *Hamming weight hierarchy* (HWH) of C.

For the first time, the generalized Hamming weights (GHW) were introduced by V. K. Wei in [17] for linear codes. In [17] , the basic properties of GHW are studied and the weight hierarchy for Hamming code, Reed-Solomon codes, binary Reed-Muller code, etc are determined. This concept is a generalization of minimum Hamming weight of a code. It is not difficult to see that $d_1(C) = d(C)$. The concept of GHW were extended for various version of codes, such as non-linear code and codes over rings, for example see [2, 3]. Study of this notion was motivated by applications in cryptography. It is a well-known fact that the sequence of generalized Hamming weights is strictly increasing, that is,

$$d_1(C) < d_2(C) < \cdots < d_k(C) = n.$$

Among non-linear codes, Hadamard codes are the most useful codes in engineering, coding theory and mathematics. First we mention the definition of Hadamard matrices and specific version of Hadamard codes which are not linear. Then we obtain GHW for these codes.

A square matrix H of order n with elements in $\{1, -1\}$ is called a *Hadamard matrix* when $HH^t = I_n$, in which I_n denotes the identity matrix. We will denote by H_n the Hadamard matrix of order n. For clarifying we bring some examples:

$$H_1 = \begin{pmatrix} 1 \end{pmatrix}, H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{1.1}$$

It is known (Paley, 1933) that if Hadamard matrices of order n exist, then $n = 1, 2$ or $n = 4s$, where s is a positive integer. Note that changing the sign of elements in a row or column can not affect the orthogonality. Hence a Hadamard matrix can always be reduced to the standard form in which the initial row and column contain only $+1$.

The *Kronecker product* or *tensor product* of matrices A and B is defined as follows

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \ddots & \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{pmatrix} \tag{1.2}$$

Lemma 1.1. *(Sylvester) Let H_1 and H_2 be Hadamard matrices of orders h_1 and h_2, then the Kronecker product of H_1 and H_2 is an Hadamard matrix of order h_1h_2.*

Lemma 1.2. *(Sylvester (1867)) There is an Hadamard matrix of order* 2^t *for all non-negative* t*.*

The matrices of order 2^t constructed using Sylvester's construction are usually referred to as *Sylvester-Hadamard matrices*. The Sylvester-Hadamard matrices are associated with discrete orthogonal functions called Walsh functions [15].

A (v, k, λ) *design*, is a pair $(\mathcal{P}, \mathcal{B})$ where $\mathcal{P}$ is a set of v elements, called *points* and $\mathcal{B}$ is a collection of distinct subsets of $\mathcal{P}$ of size k, called *blocks*, such that every pair is contained in precisely λ blocks. The number of blocks in $\mathcal{B}$ is denoted by b and *Fisher's inequality* state that $b \geq v$. If $b = v$, the (v, k, λ) design is called *symmetric*. Symmetric designs have interesting properties. One of them is that every two distinct blocks intersect in exactly λ points. Another properties is that every point appears in exactly k blocks. For a (v, k, λ) design $D = (\mathcal{P}, \mathcal{B})$, consider $\overline{\mathcal{B}} = \{\mathcal{P} \setminus B : B \in \mathcal{B}\}$. It is not difficult to see that $\overline{D} = (\mathcal{P}, \overline{\mathcal{B}}$ is a $(v, v-n, v-2k+\lambda)$ design. Let $\mathcal{P} = \{x_1, x_2, \ldots, x_v\}$ and $\mathcal{B} = \{B, B_2, \cdots, B_v\}$. The *Incidence matrix* of a (v, k, λ) design, $(\mathcal{P}, \mathcal{B})$, is the $v \times b$ matrix M whose entries m_{ij} are defined as $m_{ij} = 1$ if $x_i \in B_j$ and $m_{ij} = 0$ if $x_i \notin B_j$. In the next section we compute the weight hierarchy of some families of code arising from Hadamard matrix by properties of symmetric designs.

2. Main Result

We firstly recall Levenshtein's method [13] for constructing optimal error correcting codes from suitable Hadamard matrices. Starting from a normalized (i.e. the first row and column formed all of $1'$s) Hadamard matrix H of order $4n$, some codes (which are termed Hadamard codes) may be constructed (see [14], for instance). More concretely, consider the matrix A_{4n} related to H_{4n}, which consists in replacing the $+1'$s by $0'$s and the $-1'$s by $1'$s. Since the rows of H_{4n} are orthogonal, any two rows of A_{4n} agree in $2n$ places and differ in $2n$ places and so have Hamming distance $2n$ apart. In these circumstances, one may construct an $(4n-1, 4n, 2n)$ code, C_{4n}, consisting of the rows of A_{4n} with the first column deleted. This code called *Hadamard code*. Also if we deleted the first row and column of A_{4n}, then the remaining matrix is the incidence matrix of a $(4n-1, 2n, n-1)$ symmetric design, which called *Hadamard design*. For further information about Hadamard matrices and Hadamard design reader can see [1].

Theorem 2.1. *Suppose that* H_n *is a Hadamard matrix and* C_n *is the Hadamard code corresponding to* H_n*. Then* $d_2(C_n) = \frac{3n}{4}$*.*

Proof. Since $d_2(C_n) = min\{\|D\|; D \subseteq C_n, |D| = 3\}$, therefore there are the rows r_1, r_2, r_3 in A_n such that $\|r_1, r_2, r_3\| = d_2(C_n)$. Let $D = \{\{r_1, r_2, r_3\}\}$. Hence the elements of D may have the following cases:

$$\begin{array}{cccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{-1} & \mathbf{-1} \\ \underbrace{\mathbf{1}}_{a-tuple} & \underbrace{\mathbf{-1}}_{b-tuple} & \underbrace{\mathbf{1}}_{c-tuple} & \underbrace{\mathbf{-1}}_{d-tuple} \end{array}$$

Note that **1** denotes the $m-$ tuple vector of 1, in which $m \leq n$.

Using the orthogonality of the distinct rows and $H_n H_n^t = I_n$, we have the following equations:

$$a+b+c+d = n-1, a+b-c-d = -1, a-b+c-d = -1, a-b-c+d = -1.$$

The solution of this system of equations is $b = c = d = \frac{n}{4}$. So, we have

$$\|D)\| = b+c+d = \frac{3n}{4}.$$

□

Theorem 2.2. *Suppose that H_{2^k} is the Sylvester Hadamard matrix. If C_{2^k} is the Hadamard code of order 2^k corresponding to H_{2^k}, then*

$$d_r(C_{2^k}) = 2^{k-r}(2^r - 1).$$

Proof. Let C_{2^k} be the code associated with the Sylvester Hadamard matrix H_{2^k}. The proof is by induction on k. It is true for $k = 1$. Suppose that the relation is true for k. In the other words, suppose that the weight hierarchy of C_{2^k} is $d_r = 2^{k-r}(2^r - 1)$. We know that

$$d_r = min\{\|D\|; D \subset C_{2^k}, |D| = 2^{r-1} + 1\}.$$

Therefore there are $2^{r-1} + 1$ rows in C_{2^k}, say them $h_1, h_2, ..., h_{2^{r-1}+1}$, such that

$$supp(h_1, h_2, ..., h_{2^{r-1}+1}) = 2^{k-r}(2^r - 1).$$

We know that

$$H_{2^{k+1}} = \begin{pmatrix} H_{2^k} & H_{2^k} \\ H_{2^k} & -H_{2^k} \end{pmatrix}.$$

Now by using the construction of $H_{2^{k+1}}$, the support of $h_1, h_2, ..., h_{2^{r-1}+1}$ in $C_{2^{k+1}}$ is equal to $2.2^{k-r}(2^r - 1)$. □

Two Hadamard matrices are called *equivalent* if one is obtained from the other by a sequence of permutations and negations of rows and columns. The equivalent classes of Hadamard matrices of small orders have been determined by several authors. It is well known that order up to 12, there is a unique Hadamard matrix. For orders

16, 20, 24, 28 and 32 there are 5, 3, 60, 487 and 3710027 inequivalent Hadamard matrices, respectively [4, 5, 6, 7, 8, 9, 10, 11, 12, 16].
It is obvious that, if H and H' are two equivalent Hadamard matrices of order $4n$ and C and C' are two $(4n-1, 4n, 2n)$ nonlinear codes correspondence to H and H', with $r-th$ generalized Hamming weight d_r and d'_r, respectively, then $d_r = d'_r$. In the following theorem, we prove that if C_n is a code from H_n, then $d_r(C_n)$ is independent of choice of H_n for $8 \leq n \leq 32$.

Theorem 2.3. *Let C_{4n} be a $(4n-1, 4n, 2n)$ Hadamard code. If $k = 1+[log_2(4n-1)]$, then $d_k = 4n-1$ and $d_{k-1} = 4n-2$.*

Proof. Let D_{4n} be the $(4n-1, 2n-1, n-1)$ Hadamard design, corresponding to C_{4n}. If $d_k \leq 4n-2$, then there exist a coordinate, i, such that all code words are equal to 1 or all code words are equal to 0 in position i. Hence there exists an element of $x \in \mathcal{P}$ such that x belong to every blocks of D_{4n} (or $\overline{D_{4n}}$), which is impossible. Hence $d_k = 4n-1$. If $d_{k-1} \leq 4n-3$, then there are a subset D Of C_{4n} of size $2^{k-2}+1$ and two coordinates j_1 and j_2, such that all code word of D are agree in these coordinates. If $j_1 = j_2 = 1$, then every code word of D indicated a block of D_{4n}, and hence there exists a pair, which appear in $|D|$ blocks, which is impossible. If $j_1 = j_2 = 0$, then there exists a pair, which appear in at least $|D|-1$ blocks of $\overline{D_{4n}}$, which is impossible. If $j_1 = 1$ and $j_2 = 0$, then there exists a pair $\{x, y\}$ such that there are at least $|D|$ blocks $B_1, B_2, \cdots, B_{|D|}$ of D_{4n}, which $x \in B_i$ and $y \notin B_i$ for $1 \leq i \leq |D|$. But the number of blocks , B, such that $x \in B$ and $y \notin B$ is equal to n and we get a contradiction. Hence $d_{k-1} = 4n-2$. □

Theorem 2.4. *Suppose that $n = 4k$ and $2 \leq k \leq 8$. If C_{4n} and C'_{4n} are two $(4n-1, 4n, 2n)$ binary Hadamard codes, corresponding to two Hadamard matrices H_{4n} and H'_{4n}, respectively, then $d_r(C_{4n}) = d_r(C'_{4n})$.*

Proof. For $n \in \{2, 3\}$, the result is obvious, since H_8 and H_{12} are unique. Suppose that C_{16} is the $(15, 16, 8)$ binary Hadamard, constructed by a Hadamard matrix of order 16. By Theorem 2.2, $d_2(C_{16}) = 12$. Since generalized Hamming weights is strictly increasing, then $d_3(C_{16}) = 13, d_4(C_{16}) = 14, d_5(C_{16}) = 15$. Now consider the code C_{20} constructed from H_{20}. The code C_{20} is a $(19, 20, 10)$ binary code. Theorem 2.2 implies that $d_2(C_{20}) = 15$ and by Theorem 2.3 we have $d_4(C_{20}) = 18$ and $d_5(C_{20}) = 19$. If $d_3(C_{20}) = 16$, then there are 5 code words, which agree in 3 coordinates. But all 3 inequivalent Hadamard matrices have not this property. The same argument works for other cases. □

In the following table we give the generalized Hamming weights of Hadamard matrices of order up to 32.

Acknowledgments

The authors would like to thank the referee for his/her helpful remarks which have contributed to improve the presentation of the article.

Hadamard Matrix	Code	Design	d_1	d_2	d_3	d_4	d_5
H_8	$(7, 8, 4)$	$(7, 3, 1)$	4	6	7	-	-
H_{12}	$(11, 12, 6)$	$(11, 5, 2)$	6	9	10	11	-
H_{16}	$(15, 16, 8)$	$(15, 7, 3)$	8	12	13	14	15
H_{20}	$(19, 20, 10)$	$(19, 9, 4)$	10	15	17	18	19
H_{24}	$(23, 24, 12)$	$(23, 11, 5)$	12	18	21	22	23
H_{28}	$(27, 28, 14)$	$(27, 13, 6)$	14	21	25	26	27
H_{32}	$(31, 32, 16)$	$(31, 15, 7)$	16	24	28	30	31

REFERENCES

1. R. Craigen and H. Kharaghani, *Hadamard matrices and Hadamard designs*, in: Handbook of Combinatorial Designs (C.J. Colbourn and J.H. Dinitz, eds.) Seconed edition, pp. 273–280, Chapman Hall/CRC Press, Boca raton, FL, (2007).
2. S. T. Dougherty and S. Han, *Higher Weights and Generalized MDS Codes*, Korean Math. Soc. 6(2010), 1167-1182.
3. S.T. Dougherty, S. Han and H. Liu, *Higher weights for codes over Rings*, Appl. Algebra Engrg. Comm. Comput. 22(2011), 113-135.
4. M. Hall Jr., *Hadamard matrices of order 16*, J.P.L. Research Summery 36-10, 1(1961), 21-26.
5. M. Hall Jr., *Hadamard matrices of order 20*, J.P.L. Tecnical Report, (1965), 32-761.
6. K.J. Horadam, *Hadamard matrices and their applications*, Princeton University Press, Princeton, NJ, (2007).
7. N. ITO, J. S, Leon and J.Q. Langyear, *Classification of 3-(24,12,5) designs and 24-dimensional hadamard matrices*, J. Combin. Theory Ser A. 27(1979), 289-306.
8. H. Kharaghani, B. Tayfeh-Rezaie, *Hadamard matrices of order 32*, J. Combin. Des., 21(2013), 212-221.
9. H. Kimura, *Classification of Hadamard matrices of order 28 with Hall sets*, Discrete Math., 128(1994), 257-268.
10. H. Kimura, *Classification of Hadamard matrices of order 28* , Discrete Math., 133(1994), 171-180.
11. H. Kimura, *New Hadamard matrices of order 24*, Graphs, Combin., 5(1989), 236-242.
12. H. Kimura and H. Ohmori, *Construction of Hadamard matrices of order 28* , Graphs, Combin., 2(1986), 247-257.
13. V.I. Levenshtein, *Application of the Hadamard matrices to a problem in coding*, Problems of Cybernetics, 5(1964), 166-184.
14. F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North Holland, New York, (1977).
15. J. Seberry and M. Yamada, *Hadamard matrices, sequences and block designs* in: Contemporary Design Theory: A collection of surveys (J. H. Dinitz and D.R. Stinson, eds.) 431-560, John Wiely and Sons, Inc. New York, (1992).
16. E. Spence, *Classification of Hadamard matrices of order 24 and 28* , Discrete Math., 140(1995), 185-243.

17. V.K.Wei, *Generalized Hamming Weights for linear codes*, IEEE Trans. Inform. Theory 37(1991) ,no.5,1412-1418.

Farzaneh Farhang Baftani
Department of Mathematics
Science and Research Branch, Islamic Azad University
Tehran, Iran
far_farhang2007@yahoo.com

Hamid Reza Maimani
Mathematics Section, Department of Basic Sciences
Shahid Rajaee Teacher Training University
P.O. Box 16785-163
Tehran, Iran
maimani@ipm.ir