© MAY 2020 | IRE Journals | Volume 3 Issue 11 | ISSN: 2456-8880

On Construction of Hadamard Matrices

W. V. NISHADI1, A. A. I. PERERA[2]
[1, 2] *Department of Mathematics, Faculty of Science, University of Peradeniya, Sri Lanka*

Abstract- This paper describes a specific construction of Hadamard matrices of order $4n$ with the help of two block matrices A and B order n under some conditions. It is tested that this construction works for $n = 3$. Some related results are also given.

Indexed Terms- Block matrices, Hadamard Matrices, Kronecker Product.

I. INTRODUCTION

Definition 1.1 A square matrix H of order n with entries from the set $\{+1, -1\}$ is called $Hadamard$ matrix if

$$HH^T = nI_n$$

where H^T is the transpose of H and I_n is the identity matrix of order n.

This implies that the rows of the matrix H are pairwise orthogonal [1], [2].

It is known that Hadamard matrices exist only when $n = 1,2$ or n is a multiple of 4. Surprisingly, no other restrictions on the order of a Hadamard matrix are known. However, the converse still remains as a conjecture at present.

Conjecture 1.2 There exist Hadamard matrices of order n if and only if $n = 1,2$ or $n \equiv 0(mod4)$.

A lot of research has been done on this conjecture, as this conjecture has remained unsolved for over 100 years. Presently, the smallest order for which it is unknown whether a real Hadamard matrix exists is 4·167 = 668. As of 2008, there are 13 multiples of 4 less than or equal to 2000 for which no Hadamard matrix of that order is known. They are: 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, and 1964 [2-4].

Definition 1.3 Two Hadamard matrices of the same order are said to be equivalent if one can be obtained from the other by a permutation of the rows or the columns or by multiplication of certain rows or columns by -1.

Definition 1.4 A Hadamard matrix is in normal form, or normalized, if the first row and first column of the matrix consists of only 1's.

Example. The followings are normalized Hadamard matrices of order 2 and 4:

$$\begin{bmatrix} + & + \\ + & - \end{bmatrix}, \begin{bmatrix} + & + & + & + \\ + & + & - & - \\ + & - & - & + \\ + & - & + & - \end{bmatrix}$$

(Here $+$ stands for $+\ 1$ and $-$ stands for -1).

II. PRELIMINARIES

Having defined Hadamard matrices and introduced some of their most fundamental concepts, we now turn our attention to the construction of Hadamard matrices. Various researches have shown the conjecture of Hadamard for special cases, though a complete proof or counter example remains as of the present unknown. In this section we will present four important constructions discovered while the study of Hadamard matrices was in its infancy.

A. Sylvester Construction

Sylvester, who was the first mathematician to consider Hadamard matrices in 1867 and he observed that on a chessboard, the patterns of colours in any pair of rows agreed either everywhere or nowhere. His investigation of the problem of constructing arrays in which any two rows had exactly half of their entries in common, led to the discovery of a construction method for what would become known as Sylvester Hadamard matrices of order 2^{n} [5], [6].

Theorem 1. Let H be a Hadamard matrix of order n. Then the block matrix

$$\mathrm{A} = \begin{bmatrix} \mathrm{H} & \mathrm{H} \\ \mathrm{H} & -\mathrm{H} \end{bmatrix}$$

is a Hadamard matrix of order 2n.

B. Construction by Kronecker product of two Hadamard matrices

Despite Hadamard matrices being his namesake, Jacques Hadamard did not study Hadamard matrices until about twenty five years after Sylvester. In fact, Hadamard generalized Sylvester's construction for Hadamard matrices, as we will show shortly. For this, we need the Kronecker product is also called Tensor product definition [7], [8].

Definition 2.1 The Kronecker product any two matrices $A = (a_{ij})$ and B denoted by $A \otimes B$ is defined by the block matrix:

$$\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

Theorem 2. If H_1 is a Hadamard matrix of order n and H_2 is a Hadamard matrix of order m then $H_1 \otimes H_2$ is a Hadamard matrix of order nm.

C. Paley Construction

Paley's construction makes use of quadratic residues over a field $\mathbb{F}_p$ (p prime), which we introduce below.

Definition 2.2 If $x \equiv a^2 \pmod p$ then x is a solution in $\mathbb{F}_p$, where $x, a \in \mathbb{F}_p$.

Lemma 2.3 If $q = p^\alpha$, where p is an odd prime, then exactly half of the nonzero elements of $\mathbb{F}_q$ are quadratic residues.

Definition 2.4 Let p be prime. The Legendre symbol $\chi(x)$ is defined to be

$$\chi(x) = \begin{cases} 0, & \text{if } x = 0 \\ 1, & \text{if x is a non} - \text{zero quadratic residue modulo p} \\ -1, & \text{if x is not a quadratic residue modulo p} \end{cases}$$

Theorem 3. If $q = p^\alpha$, where p is a prime and $q + 1 \equiv 0 \pmod 4$, then there is a Hadamard matrix of order $q + 1$.

Then writing $S = \begin{bmatrix} 0 & \mathbf{1} \\ \mathbf{-1} & Q \end{bmatrix}$, then $H = I_{q+1} + S$ is the Hadamard matrix of order $q + 1$.

Theorem 4. If $q = p^\alpha$, where p is a prime and $q + 1 \equiv 2 \pmod 4$, then there is a Hadamard matrix of order $2(q + 1)$.

Then $H = I_{q+1} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} + S \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is the Hadamard matrix of order $2(q + 1)$ [2].

D. Williamson Construction

Williamson introduced an 4×4 block matrix for his construction:

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

Theorem 5. If there exist $n \times n$ matrices A, B, C and D consisting $\{1, -1\}$ which satisfy

$$AA^T + BB^T + CC^T + DD^T = 4nI_n$$

for every pair U, V of distinct matrices chosen from A, B, C, D;

$$UV^T = VU^T$$

then A, B, C and D can be used to construct Hadamard matrix H of order 4n [2],[9].

III. THE CONSTRUCTION

We determine the appropriate parameters of all the sub matrices, having order n that will yield a Hadamard matrix of order $4n$. We consider the following structure of a Hadamard matrix of order $4n$ and denote it by H_{4n}.

$$H_{4n} = \begin{bmatrix} A & B & B & B \\ -B & A & B & -B \\ -B & -B & A & B \\ -B & B & -B & A \end{bmatrix} \quad (1)$$

To construct matrix (1), we need to find the block matrices A and B of order n. If $H_{4n}H_{4n}^T$ is considered as a block matrix with sub matrices A and B, then the diagonal blocks each equal $AA^T + 3BB^T$. This must be $4nI_n$ H_{4n} to be a Hadamard matrix. The (1,3)block is $-AB^T + BA^T$. This is going to be zero if $AB^T = BA^T$. Similar results hold for other off diagonal blocks. Then we have:

Theorem

If A and B are $(1,-1)$ symmetric matrices of order n, Then in (1) is a Hadamard matrix of order $4n$ if

$$A^2 + 3B^2 = 4nI_n \qquad (2)$$

and

$$AB = BA \qquad (3)$$

Proof:

$$H_{4n}H_{4n}^T$$

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

$$= \begin{bmatrix} A & B & B & B \\ -B & A & B & -B \\ -B & -B & A & B \\ -B & B & -B & A \end{bmatrix} \begin{bmatrix} A^T & -B^T & -B^T & -B^T \\ B^T & A^T & -B^T & B^T \\ B^T & B^T & A^T & -B^T \\ B^T & -B^T & B^T & A^T \end{bmatrix};$$

since A, B are symmetric matrices =

$$\begin{bmatrix} A^2+3B^2 & -AB+BA & -AB+BA & -AB+BA \\ -AB+BA & A^2+3B^2 & -AB+BA & -AB+BA \\ -AB+BA & -AB+BA & A^2+3B^2 & -AB+BA \\ -AB+BA & -AB+BA & -AB+BA & A^2+3B^2 \end{bmatrix}$$

$$= \begin{bmatrix} 4nI_n & 0 & 0 & 0 \\ 0 & 4nI_n & 0 & 0 \\ 0 & 0 & 4nI_n & 0 \\ 0 & 0 & 0 & 4nI_n \end{bmatrix}; \text{ since } A, B \text{ commute}$$

and $A^2 + 3B^2 = 4nI_n$.

$$= 4nI_{4n}$$

IV. ILLUSTRATION

In this part we construct a Hadamard matrix of order 12 with the help of method explained above.

Let $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix}$.

Then

$BA = BA = \begin{bmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix}$, $A^2 = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}$ and $B^2 = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$.

Also, we have

$$A^2 + 3B^2 = 12 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 4 \times 3\, I_3.$$

Thus, A and B fulfill the requirements for H to be a Hadamard matrix.

$H_{12} =$

$$\begin{bmatrix}
+ & + & + & - & + & + & - & + & + & - & + & + \\
+ & + & + & + & - & + & + & - & + & + & - & + \\
+ & + & + & + & + & - & + & + & - & + & + & - \\
+ & - & - & + & + & + & - & + & + & + & - & - \\
- & + & - & + & + & + & + & - & + & - & + & - \\
- & - & + & + & + & + & + & + & - & - & - & + \\
+ & - & - & + & - & - & + & + & + & - & + & + \\
- & + & - & - & + & - & + & + & + & + & - & + \\
- & - & + & - & - & + & + & + & + & + & + & - \\
+ & - & - & - & + & + & + & - & - & + & + & + \\
- & + & - & + & - & + & - & + & - & + & + & + \\
- & - & + & + & + & - & - & - & + & + & + & +
\end{bmatrix}$$

is a Hadamard matrix of order 12.

The normalized Hadamard matrix of order 12 is:

$H_{12} =$

$$\begin{bmatrix}
+ & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & - & - & + & - & - & + & - & - & + \\
+ & + & + & - & + & - & - & + & - & - & + & - \\
+ & - & - & - & + & + & + & + & + & - & - & - \\
+ & - & + & + & - & - & + & + & - & - & - & + \\
+ & + & - & + & - & - & + & - & + & - & + & - \\
+ & - & - & - & - & - & - & + & + & + & + & + \\
+ & - & + & - & - & + & + & - & - & + & + & - \\
+ & + & - & - & + & - & + & - & - & + & - & + \\
+ & - & - & + & + & + & - & - & - & - & + & + \\
+ & - & + & + & + & - & - & - & + & + & - & - \\
+ & + & - & + & - & + & - & + & - & + & - & -
\end{bmatrix}$$

Consider the special case of Williamson method when $B = C = D$. Then there exists Hadamard matrix of order $4n$ from the block matrix:

$$\begin{bmatrix} A & B & B & B \\ -B & A & -B & B \\ -B & B & A & -B \\ -B & -B & B & A \end{bmatrix} \qquad (4)$$

with the required conditions. Note that the block matrices (a) and (d) are different.

When $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix}$, the normalized Hadamard matrix obtained from the special case of Williamson's method is given below.

H

$$= \begin{bmatrix}
+ & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & - & - & + & - & - & + & - & - & + \\
+ & + & + & - & + & - & - & + & - & - & + & - \\
+ & - & - & - & + & + & - & - & - & + & + & + \\
+ & - & + & + & - & - & - & - & + & + & + & - \\
+ & + & - & + & - & - & - & + & - & + & - & + \\
+ & - & - & + & + & + & - & + & + & - & - & - \\
+ & - & + & + & + & - & + & - & - & - & - & + \\
+ & + & - & + & - & + & + & - & - & - & + & - \\
+ & - & - & - & - & - & + & + & + & - & + & + \\
+ & - & + & - & - & + & + & + & - & + & - & - \\
+ & + & - & - & + & - & + & - & + & + & - & -
\end{bmatrix}$$

V. CONCLUSIONS AND FUTURE WORKS

This paper progresses on the idea of construction of Hadamard matrices in [2], [9] focusing on Williamson construction. We introduce here block matrix of order $4n$ with the help of two other matrices of order n. We have also provided an example for the method by constructing Hadamard matrix of order 12. In particular, normalized Hadamard matrix of order 12 obtained from our method and the normalized Hadamard matrix of order 12 obtained from the special case of Williamson method have a connection. That is one is the transpose of the other. Notice that block matrix (1) is not the transpose of (4).

The major question is about the existence of orders of matrices A and B. This will be the concern of our future work.

REFERENCES

[1] K. J. Horadam, Hadamard matrices and their applications, ‖ *Princeton University press*, 2007.

[2] A. Hedayat, W. D. Waliis, Hadamard matrices and their applications, ‖ *The Annals of Statistics*, vol. 6, no. 6, pp. 1184-1238, 1978.

[3] E. Tressler, A Survey of the Hadamard Conjecture,‖ M.S. thesis, Fac. of Virginia Polytechnic Institute and State Univ., 2004.

[4] M. Miyamoto, A construction of Hadamard matrices, ‖ *Journal of combinatorial theory*, pp. 86-108, 1991.

[5] P. C. Leopardi, Constructions for Hadamard matrices using Clifford algebras, and their relation to amicability/anti-amicability graphs, ‖ *Australian Journal of Combinatorics*, vol. 58(2), pp. 214–248, 2014

[6] M. A. Morad, A. A. Mahmood, K. H. Hameed,Construction of Sylvester-Hadamard Matrices by Using Binary Code , ‖ *J. of al-anbar university for pure* science, vol. 3, no.1, 2009

[7] J. Seberry, A construction for Generalized Hadamard matrices, ‖ *Journal of statistical planning and Inference 4*, pp. 365-368, 1980.

[8] M. K. Singh, P. K. Manjhi, Construction of Hadamard matrices from certain frobenius Groups, ‖ *Global Journal of Computer Science and Technology*, vol. 4550 (11), 2011.

[9] L. D. Baumert, T. R. M. Hall, Hadamard matrices of the Williamson type, ‖ *Math. Comput.19*, pp. 442-447, 1965