

ON THE CONSTRUCTION OF HADAMARD MATRICES

P.K. Manjhi^{1 §}, Arjun Kumar²

^{1,2}University Department of Mathematics
Vinoba Bhawe University
Hazaribag, INDIA

Abstract: In this paper we forward a method of construction of hadamard matrix with the help of two block matrices J and A under some restrictions on matrix A.

AMS Subject Classification: 05B, 05D

Key Words: Hadamard matrix

1. Introduction

Let us begin with the definition of Hadamard matrix.

Definition 1. Hadamard Matrix: A hadamard matrix H of order m with entries +1 and -1 is called hadamard matrix if

$$HH^T = mI_m$$

Examples. $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$.

Received: May 15, 2017

Revised: August 13, 2018

Published: August 13, 2018

© 2018 Academic Publications, Ltd.

url: www.acadpubl.eu

[§]Correspondence author

1.1. Applications of Hadamard matrices

Applications of hadamard matrices are especially those in communication system, digital image processing and orthogonal spreading sequences for direct sequences spread spectrum code division multiple access. Hadamard matrices have direct applications in error control codes. hadamard matrices have also a very wide variety of applications in modern communications and Statistics (see [5], [4], [3], [12],[3],[8]).

1.2. Properties of hadamard Matrices

If H_m be a hadamard Matrix of order m then

1. $|\det(H_m)| = m^{\frac{m}{2}}$
2. $HH_m^T = H_m^T H_m$
3. hadamard matrices can be change into other hadamard matrices by permuting rows and columns and by multiplying rows and columns by -1 .
4. The order of hadamard matrix is 1, 2 or $4m$, where m is a positive integer.
5. If H_{4m} is a normalized hadamard matrix of order $4m$ then every row (column), except the 1st has $2m$ ones minus and $2m$ plus ones in each row (column).
6. The rows and columns of any hadamard matrix are pair wise orthogonal. This means that the dot product of any two distinct rows or columns will be zero.
7. The rows and columns of any hadamard matrix are pair wise balanced, that is when comparing the elements in any distinct pair of rows or columns component wise there will be an equal number of pairs of identical entries and pair of non identical entries

(see [3], [5],[6])

2. Preliminaries

The main challenge in the construction of hadamard matrices is to settle hadamard conjecture. The statement of hadamard conjecture is given below:

There exist a hadamard matrix for every order $4m$, where m is some positive integer.

There are many methods of construction of hadamard matrices some of them are given below:

2.1. Construction by tensor product of two hadamard matrices

The Tensor product of two matrices A and B is defied as a matrix $C =$

$$\begin{pmatrix} a_{11}B & a_{12}B & \dots & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & \dots & a_{2m}B \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1}B & a_{m2}B & \dots & \dots & a_{mm}B \end{pmatrix}$$

this product is denoted by $A \otimes B$

Theorem: The tensor product of two hadamard matrices is a hadamard matrix. (see [6],[10],[3])

2.2. Sylvester’s construction of Hadamard Matrices

This method is based on the following two theorems:

Theorem 2. *There is a hadamard matrix of order 2^m for all positive integers m .*

Theorem 3. *If H_m and H_n are hadamard matrices of order m and n respectively then their kronecker product $H = H_m \otimes H_n$ is an hadamard matrix of order mn .*

With the help of above two theorems one can construct a hadamard matrix of order 2^m

Examples 2.2.1: $H_2 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, it is a hadamard matrix of order 2 and

$$H_4 = H_2 \otimes H_2 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. H_4 \text{ is a}$$

hadamard matrix constructed using Sylvester’s method.

(see [3])

2.3. Paley's method

If $p^\alpha = q$ is a prime power and $q + 1 \equiv 0 \pmod{4}$, then a hadamard matrix of order $q + 1$ can be constructed as follows:

suppose the member of the field $\text{GF}(q)$ are labelled $a_0, a_1, a_2, a_3, \dots$ in some order. A matrix Q of order q is defined as follows:

the (i, j) entry of Q equal to $\chi(a_i - a_j)$, where χ is quadratic character on $\text{GF}(q)$ define by $\chi(0) = 0$

and $\chi(b) = \begin{cases} 1, & \text{if } b \text{ is non-zero quadratic element in } \text{GF}(q) \\ -1, & \text{if } b \text{ is not a quadratic element in } \text{GF}(q). \end{cases}$

set $S = \begin{pmatrix} 0 & 1 \\ -1 & Q \end{pmatrix}$, then $H = I_{q+1} + S$, where 1 equal to $q \times 1$ matrix with each entry 1 is a hadamard matrix.

(see [10],[8])

2.4. Williamson's method

Williamson takes array

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

where A, B, C and D are circulant matrices each of order n .

Williamson constructed these matrices as appropriate $(1,-1)$ -linear combination of $(U + U^{n-1}), (U^2 + U^{n-2}), \dots, (U^{\frac{n-1}{2}} + U^{\frac{n+1}{2}})$, where U is circulant matrix of order n with first row $(0 \ 1 \ 0 \ 0 \dots 0)$. Clearly $U^n = I_n = \text{unit matrix of order } n$. The condition on A, B, C and D is $A^2 + B^2 + C^2 + D^2 = 4nI_{4n}$, then H is a hadamard matrix of order $4n$. This method needs computer search for the construction of higher order of hadamard matrices. (see [10],[8])

3. Main Results

In this paper we forward a method of construction of hadamard matrix with the help of one unknown matrix A . further, some conditions on matrix A is

discussed. We have constructed a hadamard matrix of order 12 with the help of this method.

The method and properties of matrix A are explained through the following theorems:

Theorem 4. *If A is an $n \times n$ ± 1 matrix with the property $3A^2 = -nJ + 4nI_n$, then the following matrix*

$$H = \begin{pmatrix} J & A & A & A \\ -A & J & A & -A \\ -A & -A & J & A \\ -A & A & -A & J \end{pmatrix}$$

where J is all 1 matrix of order n , is a hadamard matrix of order $4n$.

Proof.

$$\begin{aligned} HH^T &= \begin{pmatrix} J & A & A & A \\ -A & J & A & -A \\ -A & -A & J & A \\ -A & A & -A & J \end{pmatrix} \begin{pmatrix} J & -A & -A & -A \\ A & J & -A & A \\ A & A & J & -A \\ A & -A & A & J \end{pmatrix} \\ &= \begin{pmatrix} J^2 + 3A^2 & 0 & 0 & 0 \\ 0 & J^2 + 3A^2 & 0 & 0 \\ 0 & 0 & J^2 + 3A^2 & 0 \\ 0 & 0 & 0 & J^2 + 3A^2 \end{pmatrix} \\ &= \begin{pmatrix} 4nI_n & 0 & 0 & 0 \\ 0 & 4nI_n & 0 & 0 \\ 0 & 0 & 4nI_n & 0 \\ 0 & 0 & 0 & 4nI_n \end{pmatrix} = 4nI_{4n} \end{aligned}$$

[since $3A^2 = -nJ + 4nI_n$] $\implies H$ is a hadamard matrix of order $4n$. □

Theorem 5. *IF $H = \begin{pmatrix} J & A & A & A \\ -A & J & A & -A \\ -A & -A & J & A \\ -A & A & -A & J \end{pmatrix}$ is a hadamard matrix of*

order $4n$, then the order of block matrix A is $3t$ for some integer t .

Proof. Since $3A^2 = -nJ + 4nI_n$, therefore $A^2 = \frac{-n}{3}J + \frac{4n}{3}I_n$. Also since A is a square matrix with entries ± 1 , therefore each entry in A^2 must be an integer. $\implies \frac{-n}{3} = \text{an integer} \implies 3$ divides n . □

Corollary 6. IF $H = \begin{pmatrix} J & A & A & A \\ -A & J & A & -A \\ -A & -A & J & A \\ -A & A & -A & J \end{pmatrix}$ is a hadamard matrix of order $4n$, then the dot product of any two different rows in $\frac{-n}{3}$.

Proof. Since A is a Symmetric matrix, therefore dot product of i th and j th rows ($i \neq j$) = dot product of i th and j th columns = (i, j) th entry of $A^2 = \frac{-n}{3}$. [Since $A^2 = \frac{-n}{3}J + \frac{4n}{3}I_n$.] \square

Theorem 7. IF $H = \begin{pmatrix} J & A & A & A \\ -A & J & A & -A \\ -A & -A & J & A \\ -A & A & -A & J \end{pmatrix}$ is a hadamard matrix of order $4n$, then in any two different rows or columns of A^2 there are $\frac{n}{3}$ places where sign is same.

Proof. Since $A^2 = \frac{-n}{3}J + \frac{4n}{3}I_n$, therefore each non diagonal entry in A^2 is $\frac{-n}{3}$ and each diagonal entry in A^2 is $\frac{4n}{3} - \frac{n}{3} = n$. Now let $R_i = (a_{i1}, a_{i2}, a_{i3}, \dots, a_{in})$ and $R_j = (a_{j1}, a_{j2}, a_{j3}, \dots, a_{jn})$ be two different rows of A^2 (That is $i \neq j$), then $R_i R_j = \sum_{r=1}^n a_{ir} a_{jr} = \frac{-n}{3}$. Since in $\sum_{r=1}^n a_{ir} a_{jr}$ there are n terms each of which is either $+1$ or -1 , therefore in $\sum_{r=1}^n a_{ir} a_{jr}$ there are $\frac{4n}{3}$ terms of $+1$ and $\frac{n}{3}$ terms of -1 . Since -1 in the dot product indicate that corresponding terms have different sign, therefore in R_i and R_j there are $\frac{n}{3}$ places where sign is different. \square

4. Illustration

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

Consider $A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$, then $H = \begin{pmatrix} J & A & A & A \\ -A & J & A & -A \\ -A & -A & J & A \\ -A & A & -A & J \end{pmatrix} =$

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

H is a hadamard matrix of order 12.

Here A is a symmetric matrix of order 3 and $A^2 = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}^2 =$

$$\begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix} \implies J^2 + 3A^2 = \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix} + \begin{pmatrix} 9 & -3 & -3 \\ -3 & 9 & -3 \\ -3 & -3 & 9 \end{pmatrix} =$$

$\begin{pmatrix} 12 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 12 \end{pmatrix} = 4 \times 3I_3 \implies 3A^2 = -3J + 4 \times 3I_3$. Thus A fulfill the condition for H to be a hadamard matrix.

5. Future Prospects

The main question is about the existence of matrix A of above type. Whether there exist a matrix A for every order 3t or not?

If there exist Matrix A of order 3t for every positive integer t, then it will be a partial proof of hadamard conjecture.

References

- [1] L.D.Baumert, Tr.M. Hall, Hadamard matrices of the Williamson type, Math.Comput.19,442-447(1965).
- [2] L.D.Baumert and JR.Marshall, A new construction for Hadamard matrices, Ball.Amer.Math,Soc.V.71,169-170(1965).
- [3] Haralambos Evangelars, Christos Koukouvinos and Jennifer seberry, Application of Hadamard matrices, Journal of telecommunications and information technology,2,1-10(2003).

- [4] A. Hedayat, W.D.Wailis, Hadamaed matrices and their applications,Ann.Stat.6,1184-1238(1978).
- [5] K.J.Horadam,Hadamard matrices and their applications,Princeton university press(2007).
- [6] Ben Lantz and Michael Zowada:An over view of complex Hadamard cubes,Rose-Hulman undergraduate mathematics journal, volumes 13,No.2 Fall, 32-42, 2012.
- [7] M.Miyamoto, A construction of Hadamard matrices,Journal of combinatorial theory,series-A,57,86-108(1991).
- [8] M.K.Singh,P.K.Manjhi, Construction of Hadamard matrices from certain frobenius Groups,Global Journal of computer science and Techonology,volume 11,version I,45-50,10th may 2011(USA).
- [9] J. Seberry, A construction for Generalized Hadamard matrices,Journal of statistical planning and Inference 4 ,365-368(1980).
- [10] Eric Tressler:A Survey of the Hadamard Conjecture,M.Sc. thesis, Faculty of Virginia Polytechnic Institute and State University, 22 April,2004.
- [11] J.S.Wallis, Construction of Williamson type matrices,Linear and multilinear Algebra 3 ,197-207(1975).
- [12] Yang Yixian, Theory and application of Higher Dimensional Hadamard matrices, Science Press(2006).