

Bull. Pure Appl. Sci. Sect. E Math. Stat. **39E**(1), 77–83 (2020) e-ISSN:2320-3226, Print ISSN:0970-6577 DOI 10.5958/2320-3226.2020.00006.5 ©Dr. A.K. Sharma, BPAS PUBLICATIONS, 387-RPS-DDA Flat, Mansarover Park, Shahdara, Delhi-110032, India. 2020

Bulletin of Pure and Applied Sciences Section - E - Mathematics & Statistics

Website: https://www.bpasjournals.com/

# On the existence of a special type of symmetric matrix and the construction of Hadamard matrices \*

M.M.  $Nair^{1,\dagger}$ 

 Department of Applied Mathematics, Adama Science and Technology University, Adama, P.O. Box. 1888, Ethiopia.

1. E-mail: madhukkdnair@yahoo.co.in

**Abstract** In this paper we consider a symmetric matrix  $A^2$  which is the square of an unknown matrix A with only the two numbers +1 and -1 as its entries and we establish the existence of a special type of square matrix  $A^2$ . From this special square matrix  $A^2$  all the possible matrices A can be obtained and used for the construction of Hadamard matrices. These Hadamard matrices are much useful in coding theory, communication theory, signal processing and cryptography.

Key words Hadamard matrix, Block matrix, Hadamard conjecture.

2020 Mathematics Subject Classification 05B20, 15B34.

# 1 Introduction

There are various types of matrices in the literature having distinct properties useful for numerous applications. The famous matrix with orthogonal property was introduced by Sylvester [10] and further studied by Hadamard [1] which is now known as the Hadamard matrix. Hadamard matrix has a wide range of applications in coding theory, combinatorial designs, communication theory and cryptography. It plays a major role in theory and construction of experimental designs. The Hadamard matrix H is a square matrix which satisfies the property  $HH^T = nI_n$  and has all its entries as +1 or -1. The inner product of any of the two rows or columns of a Hadamard matrix is zero. This property is called the orthogonality. The well-known Hadamard conjecture is that "there exists a Hadamard matrix for every order 4n where, n is a positive integer". That is, "a Hadamard matrix of order  $n \times n$  exists iff n = 2, or,  $n \equiv 0 \pmod{4}$ ". There are several methods to construct Hadamard matrices. Kimura and Ohmori [2] constructed Hadamard matrices of order 28. Koukouvinos and Seberry [3] used orthogonal designs, Singh et al. [8] and Singh and Manjhi [9] constructed using Balanced Incomplete Block Design (BIBD) and Frobenius groups, Sajadieh et al. [6] used Vandermonde matrices for the construction. Miyamoto [5] constructed a series of Hadamard matrices by proving the existence of Hadamard matrices of order 4q for prime power q if there is a Hadamard matrix of order q-1, using C-matrix. With elements from the elementary abelian group  $Z_p \times Z_p \times \ldots \times Z_p$ , Seberry [7] constructed generalized Hadamard matrices of order  $p^r(p^r-1)$ , where  $p^r$  and  $p^r-1$  are both prime powers.

<sup>\*</sup> Communicated, edited and typeset in Latex by Lalit Mohan Upadhyaya (Editor-in-Chief). Received November 24, 2018 / Revised July 17, 2019 / Accepted August 09, 2019. Online First Published on June 30, 2020 at https://www.bpasjournals.com/.

<sup>&</sup>lt;sup>†</sup>Corresponding author M.M. Nair, E-mail: madhukkdnair@yahoo.co.in

78 M.M. Nair

### 2 Preliminaries

Manjhi and Kumar [4] used a square matrix A of order n consisting only of the elements +1 or -1 satisfying the property  $3A^2 = -nJ_n + 4nI_n$ , where  $J_n$  is a square matrix of order n consisting of 1 as all its elements to construct a Hadamard matrix. In particular they showed that the matrix H defined as below is a Hadamard matrix of order 4n:

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

#### 3 Main results

In this paper we prove that there exists a symmetric matrix A with its entries as only the elements of the set  $\{-1,+1\}$  of order n=3t, for every positive integer t which implies the existence of a special type of matrix  $A^2$  that satisfies the condition  $3A^2=-nJ_n+4nI_n$ , where  $J_n$  is a square matrix of order n whose all entries are 1. As mentioned above that Manjhi and Kumar [4] used the same type of matrix A and satisfying the very same relation for the construction of Hadamard matrices but they did not answer the crucial question 'how to find the matrix A?' In this paper we provide an answer to this question by retrieving all the possible symmetric matrices A from the special matrix  $A^2$  and use the same for the construction of Hadamard matrices. This method has much importance due to its multiplicity and the Hadamard matrices so obtained can be used effectively in cryptography, coding theory, communication theory and signal processing.

**Proposition 3.1.** Let A be a symmetric matrix of order n = 3t, t = 1 with the entries  $\pm 1$ , then  $A^2$  is a symmetric matrix with entries  $\pm 3t$  and  $\pm t$  only, 3t being the principal diagonal entries.

**Proof.** Consider the symmetric matrix A of order n=3t, t=1 with  $\pm 1$  as its elements. The first row and hence the first column of A can be obtained in  $2^3=8$  ways as its elements are the binary digits  $\{-1,+1\}$ . Now the second row of A excluding the first element in second row and consequently the second column of the matrix A exclusive of the first element in second column shall be formed in  $2^2=4$  ways. After deciding the second row (second column), the third row (third column) exclusive of the first two entries in their respective rows (columns) shall be obtained in  $2^1=2$  ways. Thus, we can form  $2^3\times 2^2\times 2=64$ symmetric matrices of order n=3t with  $\pm 1$ . For each of these 64 matrices we

may form the matrices  $A^2$ . Let A be the symmetric matrix  $\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}$  of order 3 with  $\pm 1$  entries,

then

$$A^{2} = \begin{pmatrix} a^{2} + b^{2} + c^{2} & ab + bd + ce & ac + be + cf \\ ab + bd + ce & b^{2} + d^{2} + e^{2} & bc + de + ef \\ ac + be + cf & bc + de + ef & c^{2} + e^{2} + f^{2} \end{pmatrix}$$

The principal diagonal elements are always 3 as each element is the sum of 3 squares of  $\pm 1$ . The other elements, each one is the sum of three terms in which each term is the product of two  $\pm 1$ 's. Hence each sum can be any one of the following  $2^3 = 8$  types:

$$(1,1,1),(1,1,-1),(1,-1,1),(1,-1,-1),(-1,1,1),(-1,1,-1),(-1,-1,1),(-1,-1,-1).$$

Obviously, the respective sums are 3, 1, 1, -1, 1, -1, -1, -3 which means that the elements in the matrix  $A^2$  are  $\pm t, \pm 3t$ .

Illustration 3.2. Let 
$$A = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$$
 be of order  $n = 3t, t = 1$ , then 
$$A^2 = \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix} = \begin{pmatrix} 3t & -t & -t \\ -t & 3t & -t \\ -t & -t & 3t \end{pmatrix}$$



Corollary 3.3. If A is a square matrix of order n = 3t, t = 1 with the entries  $\pm 1$ , then  $A^2$  is a matrix of order n with entries  $\pm t$  and  $\pm 3t$ .

**Proof.** The proof is like the one used in the Proposition 3.1. In the principal diagonal entries, each element is the sum of three terms in which any one term is a square and for the other two terms, each one is the product of two elements. The following are the possibilities:(1,1,1), (1,1,-1), (1,-1,1), (1,-1,-1). Clearly, we get the sum 3,1,1,-1 respectively. The same argument shall be used to establish that the other entries in the matrix  $A^2$  are  $\pm 1$  and  $\pm 3$ , means all entries are of the form  $\pm t$  and  $\pm 3t$ .

Illustration 3.4. Let 
$$A = \begin{pmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} \Rightarrow A^2 = \begin{pmatrix} -1 & 3 & -1 \\ -1 & -1 & 3 \\ 3 & -1 & -1 \end{pmatrix} = \begin{pmatrix} -t & 3t & -t \\ -t & -t & 3t \\ 3t & -t & -t \end{pmatrix}.$$

**Proposition 3.5.** Let A be a symmetric matrix of order n=3t, t=2 with  $\pm 1$  entries. Then  $A^2$  is a symmetric matrix of order n with the entries  $0, \pm t, \pm 2t, \pm 3t$ , the principal diagonal elements being 3t.

**Proof.** In  $A^2$ , the principal diagonal entries are the sum of 6squares of either +1 or -1, which clearly yields the sum 3t=6. The other elements, each one being the sum of 6 terms in which each term is a product of  $\pm 1$  and  $\pm 1$ . There are  $2^6=64$  possibilities of getting each sum and on verification it is found that the sums are  $0, \pm t, \pm 2t, \pm 3t$ .

**Note 3.6.** When n=3t is the order of A, where t=3, the elements of  $A^2$  are of the form  $\pm (t-2), \pm t, \pm (t+2), \pm (2t+1), \pm 3t$ . The principal diagonal entries are all 3t.

**Theorem 3.7.** If A is a symmetric matrix of order n = 3t, t = 1, 2, 3, ... with  $\pm 1$  elements then A satisfies the matrix equation  $3A^2 = -nJ_n + 4nI_{n,i}f$  and only if the matrix  $A^2$  is of the form

$$\begin{pmatrix}
3t & -t & -t & \cdots & -t & -t \\
-t & 3t & -t & \cdots & -t & -t \\
-t & -t & 3t & \cdots & -t & -t
\end{pmatrix}$$

$$\vdots$$

where  $J_n$  is an all 1 matrix of order n and  $I_n$  is a unit matrix of order n.

**Proof.** This can be proved by induction on t. Let Abe of order n = 3t, t = 1 and  $3A^2 = -nJ_n + 4nI_n$  then

$$-nJ_n + 4nI_n = 3\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} + 4 \times 3\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 9 & -3 & -3 \\ -3 & 9 & -3 \\ -3 & -3 & 9 \end{pmatrix} = 3\begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}$$

$$= 3\begin{pmatrix} 3t & -t & -t \\ -t & 3t & -t \\ -t & -t & 3t \end{pmatrix} = 3A^2 \Rightarrow A^2 = \begin{pmatrix} 3t & -t & -t \\ -t & 3t & -t \\ -t & -t & 3t \end{pmatrix}$$

Conversely, let



80 M.M. Nair

Now assume the theorem be true for n = 3m, where, t = m, i.e.,  $3A^2 = -3mJ_{3m} + 4 \times 3mI_{3m}$ . When t = m + 1, n = 3(m + 1), then,

Similarly, by reversing the above steps, the converse can also be seen to be true, which establishes the validity of the theorem for n=3 (m+1),  $m=0,1,2,\ldots$ , i.e. for  $n=3,6,9,12,\ldots$ 

Illustration 3.8. Let A be a symmetric matrix of order n = 3t, t = 2 with  $\pm 1$  elements. Then

$$A^{2} = \begin{pmatrix} 3t & -t & -t & -t & -t & -t \\ -t & 3t & -t & -t & -t & -t \\ -t & -t & 3t & -t & -t & -t \\ -t & -t & -t & 3t & -t & -t & -t \\ -t & -t & -t & -t & 3t & -t & -t \\ -t & -t & -t & -t & -t & 3t & -t \\ -t & -t & -t & -t & -t & 3t \end{pmatrix} = \begin{pmatrix} 6 & -2 & -2 & -2 & -2 & -2 \\ -2 & 6 & -2 & -2 & -2 & -2 \\ -2 & -2 & 6 & -2 & -2 & -2 \\ -2 & -2 & -2 & 6 & -2 & -2 \\ -2 & -2 & -2 & -2 & 6 & -2 \\ -2 & -2 & -2 & -2 & -2 & 6 \end{pmatrix}.$$

Then

$$3A^{2} = \begin{pmatrix} 18 & -6 & -6 & -6 & -6 & -6 \\ -6 & 18 & -6 & -6 & -6 & -6 \\ -6 & -6 & 18 & -6 & -6 & -6 \\ -6 & -6 & -6 & 18 & -6 & -6 \\ -6 & -6 & -6 & -6 & 18 & -6 \\ -6 & -6 & -6 & -6 & -6 & 18 \end{pmatrix},$$

and

The converse is trivial.

**Theorem 3.9.** If  $A^2 = \begin{pmatrix} 3t & -t & -t \\ -t & 3t & -t \\ -t & -t & 3t \end{pmatrix}$  then there exists a symmetric matrix A of order n = 3t, t = 1 with  $\pm 1$  elements.



**Proof.** Given that the matrix A is of order n = 3t, t = 1, therefore,

$$A^2 = \left( \begin{array}{rrr} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{array} \right).$$

The principal diagonal elements are always 3. So that let us examine only the cases for getting the product -1. The first row of the matrix A shall be any one of the following eight possibilities namely,

$$(1,1,1),(1,1,-1),(1,-1,1),(1,-1,-1),(-1,1,1),(-1,1,-1),(-1,-1,1),(-1,-1,-1)$$

The sum of the product of a row vector  $(a_1, a_2, a_3)$  with a column vector  $(b_1, b_2, b_3)^T$  is -1, if any one element or any two elements of the row vector are -1. So the possibilities (1, 1, 1) and (-1, -1, -1) are ruled out.

**Case 1.** Any one element of the row vector is -1.

Let  $a_3 = -1$ . So that the element  $b_3$  in the column vector must be +1 and any one of the other two elements, viz.,  $b_1$  or  $b_2$  must be -1. Hence corresponding to the row vector  $(a_1, a_2, -a_3)$  the column vector is  $(b_1, -b_2, b_3)^T$  or  $(-b_1, b_2, b_3)^T$ . The first row and the first column of the matrix A is  $(a_1, a_2, -a_3)$ , A being symmetric. The second, third columns are  $(b_1, -b_2, b_3)^T$  and  $(-b_1, b_2, b_3)^T$  respectively. So, we get the desired matrix A as

$$A = \left( \begin{array}{rrr} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{array} \right).$$

Similarly for the first row (1, -1, 1) the second and third columns are  $(-1, 1, 1)^T$  or  $(1, 1, -1)^T$ . So that,

$$A = \left( \begin{array}{rrr} 1 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & 1 & -1 \end{array} \right).$$

Corresponding to the first row (-1, 1, 1) or the first column  $(-1, 1, 1)^T$  the matrix  $A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$ .

In this matrix A we can permute the second and third columns to obtain

$$A = \left( \begin{array}{rrr} -1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{array} \right).$$

Case 2. Any two elements of the row vector are -1.

Let  $a_2 = a_3 = -1$ . So that the element  $b_1$  in the column vector must be -1 and any one of the other two elements namely  $b_2$  or  $b_3$  must be -1. Corresponding to the first row (1, -1, -1) the second and third columns are  $(-1, 1, -1)^T$  and  $(-1, -1, 1)^T$  respectively. Therefore, the matrix A is obtained as

$$A = \left( \begin{array}{rrr} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{array} \right).$$

We may permute the second and third columns of the above matrix to construct another matrix A without violating the symmetry property, so,

$$A = \left( \begin{array}{rrr} 1 & -1 & -1 \\ -1 & -1 & 1 \\ -1 & 1 & -1 \end{array} \right).$$

Similarly, when the first row is (-1, 1, -1) the second and third columns are  $(1, -1, -1)^T$  and  $(-1, -1, 1)^T$  which results in

$$A = \left(\begin{array}{rrr} -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & 1 \end{array}\right).$$



82 M.M. Nair

Corresponding to the first row (-1,-1,1) the columns are  $(-1,1,-1)^T$  and  $(1,-1,-1)^T$ . Hence

**Note.3.10:** Out of the total 64 symmetric matrices of order n = 3t, t = 1 with the numbers  $\pm 1$  as its only elements, there exists only eight of the matrices as obtained above whose square results into a symmetric matrix of the given form.

#### 4 Construction of Hadamard matrices

As per the criterion developed by Manjhi and Kumar [4], the eight matrices constructed in the Theorem 3.9 can be used to construct eight Hadamard matrices of order 4n = 12 each.

**Illustration 4.1.** Let  $A = \begin{pmatrix} -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$  be a block matrix in H. This square matrix of order

3 satisfies the property  $3A^2 = -nJ_n + 4nI_n$  for n = 3, so, we can construct a Hadamard matrix of order 4n = 12 as follows:

# 5 Conclusion and future scope of the work

When the existence of the matrix A, corresponding to  $A^2$  for n=6,9 is also established, then it will be a step forward towards the partial proof of the Hadamard conjecture. For the case n=6 we may form  $2^{21}$  symmetric matrices of order n=6. There are  $2^6=64$  ways to get the first row (column). Corresponding to each of these ways  $2^{15}$  matrices can be formed. Inspecting each of these  $2^{15}$  matrices manually for the special matrix  $A^2$  is a challenge. But this is possible with the help of a suitably developed computer program, which may appear as a sequel to this paper. We can also establish the existence of the matrix A of order n=3t, t=2,3 with only the elements  $\pm 1$  as its entries corresponding to the matrix  $A^2$  as defined for n=3t. But the determination of the matrix A in this case would be a challenging problem. If we can get such a matrix A then the construction of Hadamard matrices of orders 24 and 36 is possible.

**Acknowledgments** The author expresses his thanks the Editor-in-Chief for many modifications in this paper leading to its better presentation.

# References

- Hadamard, J. (1893). Resolution dúne question relative aux determinants, Bull. Des Sciences Mathematiques, 17, 240–246.
- [2] Kimura, H. and Ohmori, H. (1986). Construction of Hadamard martices of order 28, Graphs and Combinatorics, 2, 247–257.



- [3] Koukouvinos, C. and Seberry J. (1992). Constructing Hadamard matrices from orthogonal designs, Australian J. Combinatorics, 6, 267–278.
- [4] Manjhi, P.K. and Kumar, A. (2018). On the construction of Hadamard matrices, *International Journal of Pure and Applied Mathematics*, 120 (1), 51–58.
- [5] Miyamoto, M. (1991). A construction of Hadamard matrices, Journal of Combinatorial theory Series- A, 57, 86–108.
- [6] Sajadieh, M., Dakhilalian, M., Mala H. and Omoomi, B. (2012). On construction of involutory MDS matrices from Vandermonde matrices, Des. Codes and Crypto, 64, 287–308.
- [7] Seberry, J. (1980). A construction of generalized Hadamard matrices, *Journal of Statistical Plan*ning and Inference, 4, 365–368.
- [8] Singh, M.K., Sinha, K., and Kageyama, S. (2002). A construction of Hadamard matrices from BIBD  $(2k^2 2k + 1, k, 1)$ , Australian J. Combinatorics, 26, 93–97.
- [9] Singh, M.K. and Manjhi, P.K. (2011). Construction of Hadamard matrices from certain Frobenius Groups, Global Journal of Computer Science and Technology, 11(I), 45–50.
- [10] Sylvester, J.J. (1867). Thoughts on orthogonal matrices, simultaneous sign successions and tessellated parements in two or more colors, with application to Newton's rule, ornamental tile work and the theory of numbers, *Phil. Mag.*, 34, 461–475.

