On Construction of Hadamard Rhotrix using a Special Type of $M_n$- Matrix

M. M. Nair

Abstract: The Hadamard matrix $H$ is a square matrix with all the entries $+1$’s or $-1$’s which satisfies the property $HH^T = nI_n$. Rhotrix is a new concept for mathematical enrichment with much scope for research and has a wide range of applications in coding theory and cryptography. $M_n$-matrix is also a matrix with $\pm$1 entry, like the Hadamard matrix, but the orthogonality property is not satisfied. It is shown in this paper that Hadamard matrices and thereby Hadamard rhotrices can be constructed by using a special type of $M_n$-matrix, named N-matrix, which is a unique approach.

Key words: coupled matrix, Hadamard matrix, Hadamard Rhotrix, $M_n$-matrix, N-matrix.

I. INTRODUCTION

Various types of matrices are available in the literature having distinct properties with numerous applications. A matrix with orthogonal property was introduced by Sylvester [16] and further studied by Hadamard [2] popularly known as the Hadamard matrix. Hadamard matrix has a wide range of applications in many fields like coding theory, combinatorial designs, communication theory, cryptography, image analysis, signal processing, fault-tolerant systems and stock market data analysis etc. Hadamard matrices are used for the construction of experimental designs as well. Rhotrix is a relatively new concept for mathematical enrichment introduced in 2003 [1] with objects that are placed in between 2x2 and 3x3 matrices. The properties of rhotrices are studied in [10,11] and a Hadamard matrix over finite field is defined in [17].

Mohan [8] defined an $M_n$- matrix and used it for constructing matrices with $\pm$1 elements. Using the $M_n$-matrix pattern Vasic and Milenkovic [18] gave a method of construction of Low-Density Parity Check (LDPC) codes. $\mu$- resolvable and affine $\mu$-resolvable Balanced Incomplete Block Designs (BIBD) and Partially Balanced Incomplete Block Designs (PBIBD) were constructed by Kageyama and Mohan [3] using the $M_n$-matrices.

A. Hadamard Matrix.

A Hadamard matrix is defined as a square matrix with entries $\pm$1 satisfying $HH^T = nI_n$. This Hadamard matrix has a unique property called orthogonality property which means the inner product of any two rows or columns are always zero.

Example: $H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix}$

B. Rhotrix and Hadamard rhotrix.

Rhotrix is a mathematical object which is placed in between 2x2 dimensional and 3x3 dimensional matrices. A rhotrix of dimension 3 is given by

$R_3 = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix}$

where $a_1, a_2, a_3, a_4, a_5 \in R$

Hadamard rhotrix over finite field is defined in [17]. A rhotrix $R_n$ is Hadamard rhotrix over GF (2) if and only if there exist two coupled square matrices whose rows are orthogonal to each other. Also, it is established that a rhotrix $R_n$ of order $n > 3$ is Hadamard rhotrix if and only if the sub rhotrices of $R_n$ given by $R_{n,(2p+2)}$, $p = 1, 2, 3, \ldots \ldots$ are Hadamard over GF (2) [13].

C. $M_n$-matrices.

The $M_n$-matrices are constructed from the formula $M_n = (d_i \otimes d_j \otimes d_3 \otimes d_4) \mod n$ by suitably defining $d_i, d_j, d_3$ and $\otimes$. Three types of $M_n$-matrices are introduced.

Type I matrix. When ‘$n$’ is a prime an $M_n$ – matrix ($a_{ij}$) is defined as a matrix obtained from $a_{ij} = 1 + [(i-1)\mod n]$ where $i = 1, 2, 3, \ldots \ldots n$. In the resulting matrix $a_{ij}$ is an integer and $i = 1, 2, 3, \ldots \ldots n$. In this matrix each row (column) consists of an equal number of $+1$’s and $-1$’s.

Type II matrix is obtained by the equation $a_{ij} = (i+j) \mod n$. Each row (column) consists of an equal number of $+1$’s and $-1$’s.

Type III matrix is the matrix generated from $a_{ij} = (i+j) \mod n$ where $n$ is any integer and $i, j = 1, 2, 3, \ldots \ldots n$. In this matrix each row (column) has ‘$n$’ elements. In this resulting matrix substitute 1 for even numbers and -1 for odd numbers. Also change all +1’s to -1’s.

To construct a Hadamard matrix there are various

Revised Manuscript Received on July 09, 2019

M. M. Nair, Department of Applied Mathematics, Adama Science and Technology University, PO BOX 1888, Adama, Ethiopia.
methods available like Sylvester’s method, Paley’s method, Williamson’s method etc. Kimura and Ohmori [4] constructed Hadamard matrices of order 28. Koukouvinos and Seberry [5] used orthogonal designs, Singh et al. [14,15] constructed using BIBD and Frobenius groups, Sajadieh et al. [9] used Vandermonde matrices for the construction. Manjhi et al. [6] used a ± 1 matrix A of order n satisfying the property $3A^2 = -nI + 4nI_e$.

II. MAIN RESULT

M_{m,n} matrix of Type IV and Type V are introduced here for mathematical enrichment and for brevity let us name them as $N_1$- Matrix and $N_2$- matrix respectively. In $M_{m,n}$-Matrix, the inner products of the rows are non-zero. So that the orthogonality property is not satisfied. It is shown in this paper that Hadamard matrices are constructed using the N-matrices defined here. Using these Hadamard matrices as the coupled matrices, Hadamard rhotrices are constructed.

D. $N_1$- Matrix.

An $N_1$-matrix is defined as the matrix obtained by the equation $(a_{ij}) = (i + j) \mod \frac{n+1}{2}$, where ‘n’ is odd number.

Each row (column) of the matrix so obtained has ‘n’ elements and every row (column) has elements 1,2……., $\frac{n+1}{2}$. The off-diagonal elements are always $\frac{n+1}{2}$ and the matrix obtained is a symmetric matrix.

If $\frac{n+1}{2}$ is odd, then in the resulting matrix, substitute +1 for odd numbers, -1 for even numbers and change +1 to -1. Then change all the -1’s to zeroes so that the resultant matrix is Hadamard over GF (2).

Note: II.1 If $\frac{n+1}{2}$ is even number, then this method fails. In this case we define $N_2$- matrix.

E. $N_2$ – Matrix.

An $N_2$-matrix is defined as the matrix obtained from $a_{ij} = (i+j) \mod \frac{n-1}{2}$, where ‘n’ is odd number. If $\frac{n-1}{2}$ is even and ‘n’ is non-prime, then in the resulting matrix, substitute +1 for odd numbers, -1 for even numbers and change +1 to -1. If $\frac{n-1}{2}$ is odd or n is prime, then in the resulting matrix, substitute +1 for odd numbers, -1 for even numbers and retain 1 as 1 itself. Finally change all the -1’s to Zeros. In both the cases the resultant matrix so obtained will be a Hadamard matrix over GF (2).

Note: II. 2 To construct a Hadamard matrix $H_n$ of order m = 2p where p = 2,3,4,……we use the $N_2$-matrix for n = m+1 then from the resultant matrix delete (n-m) rows and columns. In the same way, if $H_{m}$ is of order m = 2p+1, use the $N_2$- matrix for odd p and $N_2$- matrix for even values of p. If $N_2$- matrix is used, then let n=m+2 and from the resultant matrix delete (n-m) rows and columns. For example, to construct $H_6$, we take n=7 and use $N_2$- matrix. From the resultant matrix delete 1 row and 1 column (n-m = 7-6=1). To construct $H_5$, take n=9 and after constructing the $N_2$- matrix, delete n-m=2 rows and 2 columns.

III. CONSTRUCTION OF HADAMARD MATRIX

F. Hadamard matrix of order $m = 5$

The $N_1$-matrix is given by $(a_{ij}) = (i + j) \mod \frac{n+1}{2}$. Let n = 5.

So, we construct a matrix $(a_{ij}) = (i+j) \mod 3$. The following matrix is obtained.

$$\begin{pmatrix} 2 & 3 & 1 & 2 & 3 \\ 3 & 1 & 2 & 3 & 1 \\ 1 & 2 & 3 & 1 & 2 \\ 2 & 3 & 1 & 2 & 3 \\ 3 & 1 & 2 & 3 & 1 \end{pmatrix}$$

Now substitute -1 for even numbers, +1 for odd numbers and change +1 to -1, to get

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

Finally, replace -1’s by zeros to result

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The inner products of the rows are all zeros. Therefore, the matrix $M_1$ is a Hadamard matrix of order 5.

G. Hadamard matrix of order $m = 4$

Let n = 5. So that m = n-1. The $N_2$- matrix $a_{ij} = (i + j) \mod \frac{n-1}{2}$ is used for this construction. For $\frac{n-1}{2} = 2$, the matrix obtained is
From this matrix delete the first row and the last column. So that
\[ \begin{bmatrix}
1 & 2 & 1 & 2 \\
2 & 1 & 2 & 1
\end{bmatrix} \]
for odd numbers and retain 1 as 1 itself to get,
\[ \begin{bmatrix}
1 & -1 & 1 & -1 \\
-1 & 1 & -1 & 1
\end{bmatrix} \]
Finally, replace all -1’s by 0’s so that \( M_2 = \begin{bmatrix}
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1
\end{bmatrix} \)
The inner products of the rows are orthogonal. Hence \( M_2 \) is a Hadamard matrix of order 4.

H. Hadamard matrix of order \( m = 6 \)

Let \( n = 7 \). Consider the \( N_2 \)- matrix to construct a Hadamard matrix of order 6.
\[ M_3 = \begin{bmatrix}
2 & 3 & 1 & 2 & 3 & 1 & 2 \\
3 & 1 & 2 & 3 & 1 & 2 & 3 \\
1 & 2 & 3 & 1 & 2 & 3 & 1 \\
2 & 3 & 1 & 2 & 3 & 1 & 2
\end{bmatrix} \]
From \( M_3 \), delete the first row and first column then substitute -1 for even numbers, +1 for odd numbers and change 1 to -1 as \( \frac{n-1}{2} = \frac{6}{2} = 3 \) is odd. In the resultant matrix replace -1’s by 0’s.
\[ \begin{bmatrix}
0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0
\end{bmatrix} \]
the inner products of the rows are all 0’s. Therefore, \( M_3 \) is a Hadamard matrix of order 6 over GF (2).

I. Hadamard matrix of order \( m = 7 \).

Here \( n = 7 \) and \( \frac{n+1}{2} = \frac{7+1}{2} = 4 \), even. Hence, we use \( N_2 \)- matrix \( a_{ij} = (i+j) \mod \frac{n-1}{2} \) for \( n=9 \).
\[ \begin{bmatrix}
2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 \\
3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 \\
4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4
\end{bmatrix} \]
From \( M_4 \), delete the first and last rows and first two columns (the first two rows and the first and last columns) and then substitute -1 for even numbers, 1 for odd numbers and change +1 to -1. Finally replace all -1’s by 0’s.
\[ \begin{bmatrix}
0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0
\end{bmatrix} \]
This is a Hadamard matrix of order 7 over GF (2) as all the inner products of rows are 0’s.

Note: III. 1. If we interchange the rows of the Hadamard matrix over GF (2), the inner products of the rows remain the same and hence the resulting matrix will also be Hadamard. But the matrix may not be symmetric. This exercise is required in some cases to ensure that the sub rhotrices are also Hadamard. This interchange is required mainly in case of matrix of odd order ‘m’ in which the \( \left( \frac{m+1}{2} \right) \)th entry.
On Construction of Hadamard Rhotrix using a Special Type of $M_n$-Matrix

in the $\left(\frac{m+1}{2}\right)$th row is 1 and all other entries are zeros.

**Note:** III. 2. The required number of rows and columns are to be deleted in such a way that in the resultant matrix there shall not be any row (column) with odd number of 1’s.

### IV. CONSTRUCTION OF HADAMARD RHOTRICES

#### J. Hadamard Rhotrix $R_9$ of order 9.

The Hadamard matrices $M_1$ and $M_2$ of orders 5 and 4 respectively are used to construct the Hadamard rhotrix of order 9. Let us consider

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

If we interchange the 3rd row of the matrix $M_1$ with any other row say, 2nd, we get,

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Take $M_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$

$$R_{9} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

The sub rhotrix of $R_9$ is given by $R_{9-(2p+2)} = R_{9-4} = R_5$ for $p = 1$.

The coupled matrices of $R_5$ are

$$H_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad H_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

In both $H_1$ and $H_2$, the rows are orthogonal to each other. Therefore, $R_5$ is a Hadamard Rhotrix.

Another sub rhotrix $R_3$ is obtained from $R_9$ as

$$R_3 = \begin{pmatrix} 0 \\ 1 & 0 & 1 \\ 0 \end{pmatrix}$$

The coupled matrices of $R_3$ are $H_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $H_4 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

$R_3$ is also a rhotrix because the rows are orthogonal to each other in both the coupled matrices. Hence $R_3$ is a Hadamard rhotrix.

In the same way the rhotrix $R_{13}$ can be constructed using $M_3$ and $M_4$, Hadamard matrices of order 6 and 7 respectively. In $M_4$, interchange the 3rd and 4th rows to get

$$M_4 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Hence the Hadamard rhotrix of order 13, that is $R_{13}$ is obtained as
This is a Hadamard rhotrix because all its sub rhotrices namely $R_p$, $R_p$, and $R_2$ are Hadamard rhotrices.

V. CONCLUSION

The Hadamard rhotrices are constructed by many authors using different methods. But the method of construction used in this paper is much easier and can be used extensively in cryptography and in coding theory for error detection and correction.

REFERENCES

1. Ajibade, A.O., (2003). The concept of rhotrices in mathematical enrichment, Int. J. Math. Educ. Sci. Tech., 34(2), 175-179.
2. Hadamard, J., (1893). Resolution d’une question relative aux determinants. Bull. Des Sciences Mathematiques, 17, 240-246.
3. Kageyama, S., and Mohan, R. N., (1993). On $\mu$-resolvable BIB designs, Discrete Mathematics, Vol. 45, pp. 113-122.
4. Kimura, H., and Ohmori, H., (1986). Construction of Hadamard matrices of order 28, Graphs and Combinatorics, 2, 247-257.
5. Koukouvinos, C., and Seberry, J., (1992). Constructing Hadamard from orthogonal designs, Australian J. of Combinatorics, 6, 267-278.
6. Manjhi, P. K., Kumar, A., (2018). On the construction of Hadamard matrices, International Journal of Pure and Applied Mathematics, Volume 120, No.1, 51-58
7. Miyamoto, M., (1991). A construction of Hadamard matrices, Journal of Combinatorial theory Series-A, 57, 86-108.
8. Mohan, R. N., (2001). Some classes of Mn-matrices and Mn-graphs and their applications, JCSS, Vol.26, 1-4, pp. 51-78.
9. Sajadieh, M., Dakhilalian M., Mala H., and Omoomi B., (2012), construction of involutory MDS matrices from Vandermonde matrices,Des. Codes and Crypto,64, 287-308.
10. Sani B., (2004). An alternative method for multiplication of rhotrices. Int. J. Math. Educ. Sci. Tech.,35, 777-781.
11. Sani B., (2008). Conversion of a rhotrix to a coupled matrix, Int. J. Math. Educ. Sci. Tech., 39, 244-249.
12. J. Seberry., (1980). A construction of Generalized Hadamard matrices, Journal of Statistical Planning and Inference 5, 365-368.
13. Sharma, P. L., Kumar, S., and Rehan, M., (2013). On Hadamard Rhotrix over Finite field, Bulletin of Pure and Applied Sciences Vol. 32 E (Math & Stat.), (2), 181-190.
14. Singh M. K., Sinha K., and Kageyama S., (2002). A construction of Hadamard matrices from BIBD (2k- 2k+1, k, 1) Australian J. of Combinatorics, 26, 93-97.
15. Singh, M. K., Manjhi, P. K., (2011). Construction of Hadamard matrices from certain Frobenius Groups, Global Journal of Computer science and Technology, Volume 11, version I, 45-50.
16. Sylvester J. J., (1867). Thoughts on orthogonal matrices, Simultaneous sign successions and tessellated paraments in two or more colors, with application to Newton’s rule, Ornamental Tile-Work and the Theory of Numbers, Phil. Mag., 34, 461-475.
17. Tudunkaya S. M and Makanjula S. O., (2010). Rhotrices and the construction of finite fields, Bulletin of Pure and Applied Sciences, 29E (2), 225-229.
18. Vasić, Bane Vasic, Bane and Melenkovis, Olgica, (2004). For iterative decoding. IEEE Trans. on Information Theory, Vol. 50 (6), pp. 1156-1176.

AUTHORS PROFILE

M. M. Nair has obtained his B. Sc. Degree from Kerala University, M. Sc Maths from Jodhpur University and Doctorate from Jawaharlal Nehru Technological University, Hyderabad. His research interest is in Combinatorics, BIB Designs, Cryptography and Coding. He is a Gold medalist in his PG and possesses 3 decades of experience in teaching in various institutions of repute and for more than 15 years served as Principal and Director of Engineering colleges. At present he is a Professor in Addama Science and Technology University, Ethiopia. A dozen of research papers are on his credit in addition to the published conference papers.