

RESEARCH ARTICLE

AN ALTERNATIVE METHOD FOR CONSTRUCTING HADAMARD MATRICES

A. P. Batuwita[1], N. T. S. G. Gamachchige[1], P. G. R. S. Ranasinghe[2], A. A. I. Perera[2]*

[1]*Department of Science and Technology, University of Uva Wellassa, Sri Lanka.*
[2]*Department of Mathematics, Faculty of Science, University of Peradeniya, Sri Lanka.*

ABSTRACT

Symmetric Hadamard matrices are investigated in this research and an alternative method of construction is introduced. Using the proposed method, we can construct Hadamard matrices of order $2^{n+1}(q+1)$ where $q \equiv 1 (\bmod 4)$ and $n \geq 1$.

This construction can be used to construct an infinite number of Hadamard matrices. For the present study, we use quadratic non-residues over a finite field.

Keywords: *Hadamard matrices, quadratic non-residue, symmetric hadamard matrices*

DOI. *http://doi.org/10.4038/jsc.v12i2.33*

1. INTRODUCTION

A Hadamard matrix H of order n whose rows and columns are mutually orthogonal with entries ± 1 and satisfying $HH^T = nI_n$, where H^T is the transpose of H and I_n is the identity matrix of order n [1]. French mathematician Jacques Hadamard proved that such matrices could exist only if n is 1,2 or a multiple of 4 [2]. Still there are unknown Hadamard matrices of order of multiple of 4. If $H = H^T$, then H is called symmetric Hadamard matrix. These matrices can be transformed to produce incomplete block design, *t*-design, error correcting and detecting codes, and other mathematical and statistical objects [3].

Hadamard matrices can be constructed in many ways. The first construction was published by Sylvester in 1867. A new Hadamard matrix can always be obtained from a known Hadamard matrix using the method known as the Sylvester construction [4]. If H_n is an $n \times n$ Hadamard matrix, then a $2n \times 2n$ matrix H_{2n} can be defined as

$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}.$$

*Corresponding author: *anushabatuwita@gmail.com*

In 1893, Jacques Hadamard introduced Hadamard matrices of order 12 and 20. He introduced his matrices when studying how large the determinant of a square matrix can be [5]. Another popular construction of Hadamard matrices were due to the English Mathematician Raymond Paley. He gave construction methods for various infinite classes of Hadamard matrices. The Paley construction is a method for constructing Hadamard matrices using finite fields $\mathrm{GF(q)}$ [6]. This method uses quadratic residues in $\mathrm{GF(q)}$ where q is a power of an odd prime number, $\mathrm{GF(q)}$ is a Galois field of order q. An element a in $\mathrm{GF(q)}$ is a quadratic residue if and only if there exists b in $\mathrm{GF(q)}$ such that $\mathrm{a} = \mathrm{b^n}$. Otherwise, a is quadratic non-residue. Paley define quadratic character $\chi(\mathrm{a})$ indicates whether the given finite field element a is a perfect square or not.

$$\chi(a) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue in } GF(q), \\ -1 & \text{if } a \text{ is a quadratic non} - \text{residue in } GF(q), \\ 0 & \text{if } a = 0 \end{cases}$$

Paley construction-I gives Hadamard matrices of order $q+1$, where $q \equiv 3(mod\ 4)$ and Paley construction-II gives symmetric Hadamard matrices. It has been shown that, if $q \equiv 1(mod\ 4)$, then by replacing all 0 entries of $H = \begin{bmatrix} 0 & j^T \\ j & Q \end{bmatrix}$ by the matrix $\begin{bmatrix} 1 & - \\ - & - \end{bmatrix}$ and all ±1 entries by the matrix $\pm\begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}$, one can construct a symmetric Hadamard matrix of size $2(q+1)$ (Here, we denote -1 by – sign). Where Q is a symmetric matrix of order q (Q constructed using $\chi(a)$) and j is a column vector of length q with all entries 1. Also, symmetric matrix Q has the properties

$$QQ^T = Q^2 = J - qI \text{ and}$$

$$QJ = JQ = 0,$$

where, J is the $q \times q$ matrix with all entries 1.

Another popular construction was discovered by John Williamson in 1944 which are generalizations of some of Paley's work. He constructed Hadamard matrices of order $4u$ using four symmetric circulant matrices A, B, C, D of order u with entries ± 1 and satisfying both,

$$XY^T = Y^TX, \text{ for } X \neq Y \in \{A, B, C, D\} \text{ and } AA^T + BB^T + CC^T + DD^T = 4uI_u \quad [7].$$

In 1970, Symmetric Hadamard matrices of order 36 were constructed by [8] Bussemaker and Seidel and Symmetric conference matrices of order 46 were constructed by R. Mathon in 1978 [9].

A conference matrix is a square matrix C with 0 on the diagonal and ± 1 on the off diagonal such that C^TC is a multiple of the identity matrix I. Thus, if the matrix has order n, $C^TC = (n-1)I$. There are some relations between conference matrices and

Hadamard matrices of order n. But not all conference matrices represent Hadamard matrices since conference matrices of size $n = 2(\ mod\ 4)$ exist.

In 2014, by modifying Mathon's construction, Balonin and Seberry have constructed symmetric conference matrices of order 46 [10]. It is inequivalent to those Mathon. If two Hadamard matrices (H_1 and $H_2$with same order) are said to be equivalent, if H_1can be obtained from H_2 by permuting rows and columns and by multiplying rows and columns by -1. Up to equivalence a unique Hadamard matrix of order 1, 2, 4, 8 and 12 exists [11]. Matteo, Dokovic and Kotsireas constructed symmetric Hadamard matrices of order $92,116,172$ [12]. All of them are constructed by using the GP array of Balonin and Seberry. Moreover, Kharaghani and Tayfeh discovered Hadamard matrix of order 428 using T-sequences [13]. Now unknown smallest order Hadamard matrix is $668\ 276$ for skew-Hadamard matrices, and 188 for symmetric Hadamard matrices [14].

In this paper we propose an alternative method of constructing symmetric Hadamard matrices using quadratic non-residues over finite fields.

2. MATERIAL AND METHODS

First, we define a function, $\overline{\chi(a)}$ as follows. It indicates whether the given finite field element a is a perfect square or not.

$$\overline{\chi(a)} = \begin{cases} -1 & if\ a \text{ is a non zero quadratic residue in } GF(q), \\ 1 & if\ a \text{ is a quadratic non} - \text{residue in } GF(q), \\ 0 & \text{if } a = 0 \end{cases}$$

Let R be the matrix whose rows and columns are indexed by elements of $GF(q)$ and construct using $\overline{\chi(a)}$.

The matrix $R = -Q$ is Symmetric matrix of order q with zero diagonal and ± 1 elsewhere. Also, symmetric matrix R has the properties

$$RR^T = R^2 = J - qI \text{ and}$$

$$RJ = JR = 0$$

Where, J is the $q \times q$ matrix with all entries 1.

Method: Let $q \equiv 1(mod\ 4)$.

For $n \geq 1$

A symmetric Hadamard matrix of order $2^{n+1}(q+1)$ can be constructed by replacing all 0 entries of

$$H_{2^{n+1}(q+1)} = \begin{bmatrix} 0 & j^T \\ j & R \end{bmatrix}$$

by the matrix

$$A_{2^{n+1}} = \begin{bmatrix} A_{2^n} & A_{2^n} \\ A_{2^n} & -A_{2^n} \end{bmatrix},$$

and all ±1 entries by the matrix

$$\pm A'_{2^{n+1}} = \pm \begin{bmatrix} A'_{2^n} & A'_{2^n} \\ A'_{2^n} & -A'_{2^n} \end{bmatrix},$$

where

$$A_2 = \begin{bmatrix} 1 & - \\ - & - \end{bmatrix}, A_2' = \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix},$$

and j is a column vector of length q with all entries 1.

Example I (Using proposed method)

Consider $q = 5$ (quadratic non-residues are 2 and 3) and $n = 1$.

A symmetric Hadamard matrix H_{24} of order $2^2(5+1) = 24$ can be constructed by replacing all 0 entries of

$$H_{24} = \begin{bmatrix} 0 & j^T \\ j & R \end{bmatrix},$$

by the matrix

$$A_{2^2} = \begin{bmatrix} A_2 & -A_2 \\ -A_2 & -A_2 \end{bmatrix},$$

and all ±1 entries by the matrix

$$\pm A'_{2^2} = \pm \begin{bmatrix} A_2' & A_2' \\ A_2' & -A_2' \end{bmatrix}.$$

R=

0	-	1	1	-
-	0	-	1	1
1	-	0	-	1
1	1	-	0	-
-	1	1	-	0

Then, clearly

$$H_{24}H_{24}^T = 24\,I \text{ and } H_{24} = H_{24}^T.$$

Therefore, H_{24} is a symmetric Hadamard matrix of order 12, where H_{24} is given by

$$H_{24}=\begin{bmatrix}
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 & - & - & - & 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 & - & 1 & - & - & 1 & 1 & - & - & 1 & - & 1 & 1 & - & - & - & 1 & 1
\end{bmatrix}$$

Example II (Using proposed method)

Consider $q = 5$ (quadratic non-residues are 2 and 3) and $n = 2$.

A symmetric Hadamard matrix H_{48} of order $2^3(5+1) = 48$ can be constructed by replacing all 0 entries of $H_{48} = \begin{bmatrix} 0 & j^T \\ j & R \end{bmatrix}$ by the matrix $A_{2^3} = \begin{bmatrix} A_{2^2} & -A_{2^2} \\ -A_{2^2} & -A_{2^2} \end{bmatrix}$, and all ±1 entries by the matrix $\pm A'_{2^3} = \pm\begin{bmatrix} A'_{2^2} & A'_{2^2} \\ A'_{2^2} & -A'_{2^2} \end{bmatrix}$.

We can get, $H_{48}H_{48}{}^T = 48\,I$ and $H_{48} = H_{48}{}^T$

Therefore, H_{48} is a symmetric Hadamard matrix of order 48.

Example III

Now consider $q = 13$ (quadratic non-residues are 2,5,6,7,8 and 11) and $n = 1$.

$$R=\begin{bmatrix}
0 & 1 & - & 1 & 1 & - & - & - & - & 1 & 1 & - & 1\\
1 & 0 & 1 & - & 1 & 1 & - & - & - & - & 1 & 1 & -\\
- & 1 & 0 & 1 & - & 1 & 1 & - & - & - & - & 1 & 1\\
1 & - & 1 & 0 & 1 & - & 1 & 1 & - & - & - & - & 1\\
1 & 1 & - & 1 & 0 & 1 & - & 1 & 1 & - & - & - & -\\
- & 1 & 1 & - & 1 & 0 & 1 & - & 1 & 1 & - & - & -\\
- & - & 1 & 1 & - & 1 & 0 & 1 & - & 1 & 1 & - & -\\
- & - & - & 1 & 1 & - & 1 & 0 & 1 & - & 1 & 1 & -\\
- & - & - & - & 1 & 1 & - & 1 & 0 & 1 & - & 1 & 1\\
1 & - & - & - & - & 1 & 1 & - & 1 & 0 & 1 & - & 1\\
1 & 1 & - & - & - & - & 1 & 1 & - & 1 & 0 & 1 & -\\
- & 1 & 1 & - & - & - & - & 1 & 1 & - & 1 & 0 & 1\\
1 & - & 1 & 1 & - & - & - & - & 1 & 1 & - & 1 & 0
\end{bmatrix}$$

A symmetric Hadamard matrix H_{56} of order $2^2(13+1)=56$ can be constructed by replacing all 0 entries of

$$H_{56}=\begin{bmatrix}0 & j^T\\ j & R\end{bmatrix}$$

by the matrix

$$A_{2^2}=\begin{bmatrix}A_2 & -A_2\\ -A_2 & -A_2\end{bmatrix},$$

and all ±1 entries by the matrix $\pm A'_{2^2}=\pm\begin{bmatrix}A_2{}' & A_2{}'\\ A_2{}' & -A_2{}'\end{bmatrix}$.

We can get, $H_{56}H_{56}{}^T=56\,I$ and $H_{56}=H_{56}{}^T$

Therefore, H_{56} is a symmetric Hadamard matrix of order 56.

3. RESULTS AND DISCUSSION

Using the proposed method, we can construct symmetric Hadamard matrix of order $2^{n+1}(q+1)$ where $q\equiv 1(\mathrm{mod}\ 4)$ and $n\geq 1$.

CONCLUSIONS

The proposed alternative method which is our main result, can be used to construct an infinite number of Hadamard matrices. In this work, we used quadratic non-residues over a finite field. Using proposed method, we can construct symmetric Hadamard matrix of order $2^{n+1}(q+1)$ where $q\equiv 1(\mathrm{mod}\ 4)$ and $n\geq 1$. As a future work, planning to implement a computer programme to prove our method and construct large symmetric Hadamard matrices of order $2^{n+1}(q+1)$.

REFERENCE

[1] H. J., " Résolution d’une Question Relative aux Déterminants," *Bulletin des Sciences Mathématiques,* vol. 17, pp. 240-246, 1893.

[2] K. Horadam, Hadamard Matrices and Their Applications, Princeton University Press, 2006.

[3] A. Hedayat and W. Wallis, "Hadamard matrices and their applications," *The annals of statistics,* vol. 6, pp. 1184-1238, 1978.

[4] J. Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tesselated pavenments in two or more colors, with application to Newton's rule, ornamental tile-work, and the theory of numbers," *Phil. Mag.,* vol. 4, pp. 461-475, 1867.

[5] J. Hadamard, "Resolution d’une question relative aux d ´ eterminants," *Bull. Sciences Math,* pp. 240-246, 1893.

[6] R. Paley, "On Orthogonal Matrices," *Journal of Mathematics and Physics,* pp. 311-320, 1933.

[7] J. Williamson, "Hadamard’s determinant theorem and the sum of four squares," *Duke Math J.,* pp. 65-81, 1944.

[8] F. Bussemaker and J. Seidel, "Symmetric Hadamard matrices of order 36," Technological University, Eindhoven, 1970.

[9] R. Mathon, "Symmetric conference matrices of order pq2 + 1," *Canad. J. Math,* vol. 30, pp. 321-331, 1978.

[10] N. Balonin and J. Seberry, "A review and new symmetric conference matrices," *Informatsionno-upravliaiushchie sistemy,* vol. 4(71), pp. 2-7, 2014.

[11] H. Kharaghani and B. Tayfeh-Rezaie, "Hadamard matrices of order 32," *Journal of Combinatorial Designs,* vol. 21(5), pp. 212-221, 2012.

[12] O. Matteo, D. Đoković and S. Kotsireas, "Symmetric Hadamard matrices of order 116," *De Gruyter,* vol. 3, pp. 227-234, 2015.

[13] H. Kharaghani and B. Tayfeh- Rezaie, "A Hadamard matrix of order 428," *Journal of Combinatorial Designs,* pp. 435-440, 2005.

[14] N. Balonin, D. Đoković. and D. Karbovskiy, "Construction of symmetric Hadamard matrices of order 4v for v = 47, 73, 113," *De Gruyter,* vol. 6, pp. 11-22, 2017.