Abstract No: 174 ***ICT, Mathematics and Statistics***

A METHOD OF CONSTRUCTING HADAMARD MATRICES OF ORDER $2^{n+1}(q+1)$ FOR $q \equiv 1(\text{mod } 4)$

A.P. Batuwita[1,2*], N.T.S.G. Gamachchige[2], P.G.R.S. Ranasinghe[3] and A.A.I. Perera[3]

[1]Postgraduate Institute of Science, University of Peradeniya, Peradeniya, Sri Lanka
[2]Department of Science and Technology, Faculty of Applied Sciences, Uva Wellassa University, Badulla, Sri Lanka
[3]Department of Mathematics, Faculty of Science, University of Peradeniya, Peradeniya, Sri Lanka
[*]anushabatuwita@gmail.com

A Hadamard matrix H of order n with entries ± 1 satisfying $HH^T = nI_n$, where H^T is the transpose of H and $I_n$is the identity matrix of order n. If $H = H^T$, then H is called a symmetric Hadamard matrix. The French mathematician Jacques Hadamard proved that such matrices could exist only if n is $1, 2$, or a multiple of 4. There are many properties and features that define a Hadamard matrix. Two Hadamard matrices are said to be equivalent if one can be obtained from the other by a combination of elementary row operations and column operations. Hadamard matrices can be constructed in many ways such as Sylvester Construction, Paley Construction, Kronecker product construction, Williamson construction etc. In this study, we propose an alternative method to construct inequivalent symmetric Hadamard matrices. A symmetric Hadamard matrix $(H_{2^{n+1}(q+1)})$ 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 $A_{2^{n+1}} = \begin{bmatrix} A_{2^n} & -A_{2^n} \\ -A_{2^n} & -A_{2^n} \end{bmatrix}$, where$A_2 = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$, and all ± 1 entries by the matrix $\pm B_{2^{n+1}} = \pm \begin{bmatrix} B_{2^n} & B_{2^n} \\ B_{2^n} & -B_{2^n} \end{bmatrix}$, where $B_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and j is a column vector of length q with all entries 1. Here, $q \equiv 1(\text{mod } 4)$ for a positive integer n. Moreover, R is a Symmetric matrix of order q and it is constructed by using $\overline{\chi(a)}$, where

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

The quadratic character $\chi(a)$ indicates whether the given finite field element a is a perfect square. If element a in $GF(q)$ is said to be quadratic residue if it is a perfect square in $GF(q)$ otherwise a is a quadratic non-residue. Furthermore, these Hadamard matrices and the Hadamard matrices constructed by using the Sylvester construction are inequivalent. As future work, we plan on implementing a computer programme to construct large inequivalent symmetric Hadamard matrices of order $2^{n+1}(q+1)$.

Keywords: In-equivalent, Quadratic non-residue, Symmetric Hadamard matrices