Abstract No: 173 ***ICT, Mathematics and Statistics***

AN ALTERNATIVE METHOD OF CONSTRUCTING SYMMETRIC HADAMARD MATRICES OF ORDER $2(q+1)$, WHERE $q \equiv 1(mod\ 4)$

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 square design with parameters (v, k, λ) with $v = 4m-1, k = 2m-1$ and $\lambda = m-1$ for integers $m \geq 2$, is called a *Hadamard design* and the corresponding incidence structure determines a square matrix of order $4m$ with ± 1 entries when 0 is replaced by -1 and first row and column with entries 1 is added. This matrix is called a Hadamard matrix. Hadamard introduced his matrices when studying how large the determinant of a square matrix can be. A matrix H of order n 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. It is conjectured that a Hadamard matrix of order n exists if and only if $n = 1, 2$ or $n \equiv 0(\text{mod } 4)$. Still there are unknown Hadamard matrices of order of multiple of 4. In the present study, we propose an alternative method of constructing symmetric Hadamard matrices. This method is easy to understand and apply. A symmetric Hadamard matrix H of size $2(q+1)$ can be constructed using quadratic non-residues over a finite field and the general form of the proposed method is provided. Let $H = \begin{bmatrix} A+I & A-I \\ A-I & -A-I \end{bmatrix}$, where $A = \begin{bmatrix} R & j \\ j^T & 0 \end{bmatrix}$ with j being a column vector of length q with all entries 1 and R is a Symmetric matrix of order q constructed by using $\overline{\chi(a)}$. The quadratic character $\overline{\chi(a)}$ indicates whether the given finite field element a is a perfect square. If $\overline{\chi(a)} = 0$, $\overline{\chi(a)} = -1$ if $a = b^2$ for some non-zero finite field element b, and $\overline{\chi(a)} = 1$ if a is not the square in $GF(q)$. The element a in $GF(q)$ is said to be a quadratic residue if it is a perfect square in $GF(q)$, otherwise a is a quadratic non-residue. As a future work, we are planning on implementing a computer programme to construct large Hadamard matrices of order $2(q+1)$.

Keywords: Quadratic non-residues, Quadratic residues, Symmetric Hadamard matrices