A SURVEY ON GENERALIZED HADAMARD MATRICES AND THEIR CONSTRUCTIONS

D.G.T.K. Samarasiri and A.A.I. Perera

Department of Mathematics, Faculty of Science, University of Peradeniya

Introduction

Let $A=(a_{ij})$ be an $n\times n$ real matrix whose entries satisfy $|a_{ij}|\le 1$ for all i, j. Then $|\det(A)|\le n^{n/2}$. Equality holds if and only if $a_{ij}=\pm 1$ for all i, j and $AA^T=nI$.

An $n\times n$ matrix $[h_{ij}]$ is called a Hadamard matrix of order n if $h_{ij}=\pm 1$ for each i, j and

$$HH^T=nI.$$

It is conjectured that a Hadamard matrix of order n exists if and only if $n=1,\ 2$ or $n\equiv 0 \pmod 4$ (Anderson, 1974).

A new Hadamard matrix can always obtain from a known Hadamard matrix. If H is $n\times n$ Hadamard matrix, we can define a $2n\times 2n$ matrix K by

$$K=\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

If $A=(a_{ij})_{n\times n}$ and B are matrices, their tensor product (Kronecker product) is defined by

$$A\otimes B=\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & & a_{2n}B \\ \vdots & & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{bmatrix}$$

Methodology

A $v\times v$ matrix M with entries in a finite multiplicative group C of order w where v/w is a generalized Hadamard matrix $GH(w, v/w)$ over C if, whenever $i\neq k$ and $i, k\in\{1,\ldots\ldots, v\}$, the list of quotients $m_{ij}m_{kj}^{-1}$, $1\le j\le v$, contains each element of C exactly v/w times. A $GH(w, v/w)$ is a normalized if the first row and first column consist entirely of the identity element of C (Butson, 1962), (Haden, 1997).

For instance, setting $C=\{\pm 1\}$ makes it clear that a Hadamard matrix of order v is a $GH(2,\ v/2)$. A $GH(4,\ v/4)$ with $C=\{\pm 1, \pm i\}$ is a complex Hadamard matrix of order v.

However, non-abelian examples of C are known: De Launey construct $GH(w, v/w)$ with entries from non-abelian groups of prime-power order. No example is known of a $GH(w, v/w)$ for which w is not a prime power. No example is known of a $GH(w, v/w)$ will still give a $GH(w, v/w)$ for which w is not a prime power. Left multiplying a row or right multiplying a column, of a $GH(w, v/w)$ will still give a $GH(w, v/w)$ (De Launey, 1984).

Construction of generalized Hadamard matrices by using generalized Hadamard difference sets

Theorem A $GHDS(H;G)$ is equivalent to a $GH(h;G)$ which is developed modulo H.

Theorem Let p be a prime. The set $S_p = \{(ip+ij) \mid i,j = 0,1,\ldots\ldots,p-1\}$ is a $GHDS(Z_{p^2};Z_p)$. In general, the circulant $p^2 \times p^2$ matrix where first row has its $(ip+j)^{th}$ entry; $i;j = 0,1,\ldots\ldots,p-1$ equal to $ij \pmod p$ is a $GH(p^2;Z_p)$.

Construction using Kronecker Product

Proposition If H and H' are GH-matrices of orders r and r', respectively defined over an abelian group G, then the Kronecker product $H \times H'$ is a GH –matrix of order rr' over G.

Results

Construction of some generalized Hadamard matrices are given in Table 1 (Appendix).

Non-Existence of some generalized Hadamard matrices

For groups G and H with $|G| = g$ and $|H| = \lambda$, potential generalized Hadamard matrices $GH(g,\lambda)$ and $GH(\lambda,g)$ satisfy reciprocity relation provided both exist or both do not exist.

Eg. $GH(3,5)$ and $GH(5,3)$ are reciprocally non-existent, as in each case the pertinent reduced equation is of the form $5a^2 = 3b^2 + c^2$.
This equation has no nontrivial integer solutions (a,b,c), since ± 3 is a quadratic non-residue of 5.

Theorem: Let λ be a prime number. If $(-1)^{\frac{5+1}{2}}\lambda$ and $(-1)^{\frac{\lambda-1}{2}}\lambda$ are both quadratic non-residues of 5, or if $(-1)^{\frac{5+1}{2}}5$ and $(-1)^{\frac{\lambda-1}{2}}5$ are both quadratic non-residues of λ, then $GH(5,\lambda)$ and $GH(\lambda,5)$ constitute a reciprocally non-existent pair (De Launey ,1984).

Corollary: If $7+5k$ is a prime number, then $GH(5,7+5k)$ and $GH(7+5k,5)$ constitute a reciprocally non-existent sequence of potential generalized Hadamard matrices.
*Eg.*GH(5,17) and GH(17,5) do not exist.

Theorem Let $p = 4k+3$ and $q = 4k+5$ be prime numbers, where 2 is a quadratic non-residues of p. Then (p,q) is a reciprocal pair.

Reciprocity Theorem Let $p = 4k+3$ and $a = 4l+5$ be odd primes which satisfy Eulers's condition $a^{(p-1)/2} \equiv -1 \pmod p$ Then $GH(a,p)$ and $GH(p,a)$ constitute a reciprocal non-existent pair of generalized Hadamard matrices over groups G and H of order p and a respectively.

E.g. 3,17 are reciprocal pair and if $p=3$ and $a=17$ then it satisfies Euler's condition. Therefore $GH(3,17)$ and $GH(17,3)$ do not exist.

Conclusion

Hadamard matrices of order up to 100 have been constructed and exhibited in the Table 1 (Appendix). Further, existence and non-existence of some generalized Hadamard matrices are also discussed in this research work. These can be used to construct corresponding Relative difference sets and Group divisible designs.

References

Anderson I.A. (1974). First Course in Combinatorial Mathematics, Clarendon Press, Oxford.

Butson A.T. (1962). Generalized Hadamard Matrices, Proc. Amer. Math Soc., 13: 894 – 898.

De Launey W. (1984). On the Non-existence of Generalized Hadamard Matrices, J. of Statistical Planning and Inference, 10: 385-396.

Haden J. L. (1997). Generalized Hadamard Matrices, Designs codes and Criptography, 12: 69-73.

Appendix

Table 1. Construction of some generalized Hadamard matrices

n	0	10	20	30	40	50	60	70	80	90	100
0		5^2	2,5	3^2	2	25^2,5	2		2,5	$3,5^2$	
1		11	3,7	31	41	3,17	61	71	81		101
2	2	3,4	11^2	32		2,13	31^2	2,9,3	41^2	2,23	
3	3	13	23		43	53	3	73	83		103
4	4	7^2	2,3	17^2	2,11	27^2,3	64	37^2	2	47^2	2
5	5	3,5	25	5,7		5,11	5,13		5,17		3,5
6	3^2	16	13^2	4,9,3	23^2	8,2		2,19	43^2	3,4,2	
7	7	17	27	37	47		67		3,29	97	107
8	8	3,92	2,7	19^2	3,4,2	29^2	2,17		2	47^2,7	3,4
9	9	19	29		49	59		79	89		109