Global Journal of Computer Science and Technology
Volume 11 Issue 10 Version 1.0 May 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
ISSN: 0975-4172 & Print ISSN: 0975-4350

Construction Of Hadamard Matrices From Certain Frobenius Groups

By M.K. Singh, P.K. Manjhi
Ranchi University

Abstract- Hadamard matrices have many application in computer science and communication technology. It is shown that two classical methods of constructing Hadamard matrices viz., those of Paley's and Williamson's can be unified and Paley's and Williamson's Hadamard matrices can be constructed by a uniform method i.e. producing an association scheme or coherent configuration by Frobenius group action and then producing Hadamard matrices by taking suitable (1-1) – linear combinations of adjacency matrices of the coherent configuration.

Keywords: Hadamard matrix, Coherent Configuration. Association Scheme and Frobenius group.

GJCST Classification: F.2.1, G.1.3

Strictly as per the compliance and regulations of:

© 2011 M.K. Singh, P.K. Manjhi. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Construction Of Hadamard Matrices From Certain Frobenius Groups

M.K. Singh[α], P.K. Manjhi[Ω]

Abstract : Hadamard matrices have many application in computer science and communication technology. It is shown that two classical methods of constructing Hadamard matrices viz., those of Paley's and Williamson's can be unified and Paley's and Williamson's Hadamard matrices can be constructed by a uniform method i.e. producing an association scheme or coherent configuration by Frobenius group action and then producing Hadamard matrices by taking suitable (1-1) – linear combinations of adjacency matrices of the coherent configuration.

Keywords – Hadamard matrix, Coherent Configuration. Association Scheme and Frobenius group.

I. Introduction

We begin with following definitions.

a) *Hadamard matrix (H-matrix)*

A Hadamard Matrix H of order m is an m x m matrix of +1's and -1's such that

$$HH^T = mI_m \qquad [1]$$

b) *Coherent configuration (CC)Let X = {1,2,3,....n}, and R = {R₁,R₂...,Rᵣ} be a collection of binary relations on X such that.*

(cc1) $R_i \cap R_j = \phi$ for $1 \le i < j \le r$;

(cc2) $\bigcup_{i=1}^{r} R_i = X^2 = X \times X$

(cc3) For all $i \in \{1,2,3...,r\}$ there exists $i' \in \{1,2,3...,r\}$ such that $R_i^{-1} = R_{i'}$

(cc4) There exists $I \subseteq \{1,2,3...,r\}$ such that $\bigcup_{i \in I} R_i = \Delta$,

Where $\Delta = \{(x,x) \mid (x \in X\}$;

c) *Adjacency matrix of a relation*

Let R be a relation defined on a non-empty finite set X = {1,2,3...,n}.Then adjacency matrix of R = (aij) is defined as

$$a_{ij} = \begin{cases} 1, \text{ iff } (i,j) \in R, \\ 0, \text{ otherwise} \end{cases}$$

d) *Association Scheme (AS)*

Let X = {1,2,3...,n}.The set $R = \{R_1,R_2...,R_r\}$ of r relations R_i (i=0,1,2,...r) is called an AS with r classes if

(As1) $R_0 = \{(x,x) \mid x \in X\}$; (Called a diagonal relation)

(As2) $R_i^{-1} = R_i$, for $i \in \{0,1,2,...,r\}$;

(As3) For all $i,j,k \in \{0,1,2,...,r\}$, for all $(x,y) \in R_k$

$|\{z \in X \mid (x,z) \in R_i \text{ and } (z,y) \in R_j\}| = P_{ij}^k$ [2] and [9]

AS is also defined by the adjacency matrices of the relations

R_i (i = 0, 1,2,...,r)

e) *Coherent configuration from group action*

If G is a group of permutations on a non-empty finite set X, then we say that G act on X. Now define action of G on X x X by $g(x,y) = (g(x),g(y))$ $g \in G$ and $(x,y) \in X \times X$. Then different orbits of G on X x X define a coherent configuration. [9]

f) *Frobenius group*

A group, G is called a Frobenius group. If it has a proper subgroup H such that $(xHx^{-1}) \cap H = \{e\}$ for all $x \in G - H$. The subgroup H is called a Frobenius complement.

Frobenius groups are precisely those which have representations as transitive permutation groups which are not regular – meaning there is at least one non identity element with a fixed point and for which only the identity has more than one fixed point. In that case, the stabilizer of any point may be taken as a Frobenius complement. On the other hand, starting with an abstract Frobenius group with complement H the group of G acts on the collection of left cosets G/H via left multiplication.This gives a faithful permutational represention of G with the desired properties. The Frobenius complement H is unique up to conjugation,

About[α]- Dept. Of Mathematics, Ranchi University, Ranchi – 834008 India
E-mail- mithleshkumarsingh@gmail.com
About[Ω]- Dept. Of Mathematics, Vinoba Bhave University, Hazaribag – 825301
E-mail- 19pankaj81@gmail.com

©2011 Global Journals Inc. (US)

May 2011

Global Journal of Computer Science and Technology Volume XI Issue X Version I

hence the corresponding permutation is unique up to isomorphism.

A theorem of Frobenius says that if G is a finite Frobenius group given as a permutation group, as above, the set consisting of the identity of G and those elements with no fixed point forms a normal subgroup N. The group N is called the Frobenius kernel. We have G = NH with $N \cap H=\{e\}$ where H is Frobenius complement.[1], [3] and [10].

g) *Paley's construction of Hadamard matrix*

If p^{α} =q is prime power and q+1=0(mod 4).Then a Hadamard matrix of order q+1 can be construction as follows.

Suppose the members of the field GF(q) are labeled $a_0,a_1,a_2\ldots$, in some order. A matrix Q of order q is defined as follows. The (i,j) entry of Q equals $\chi(a_i-a_j)$, where χ is the quadratic character on GF(q) defined by, $\chi(0)=0$

$$\chi(b)=\begin{cases} 1, \text{if b is a non zero quadratic element (perfect square in GF (q))} \\ \text{-1 if b is not a quadratic element in GF(q)} \end{cases}$$

$$\text{Set } S=\begin{bmatrix} 0 & 1' \\ -1 & Q \end{bmatrix},\ H=I_{q+1}+S$$

where 1 = q x 1 matrix with each entry 1. H is Hadamard matrix. [11] and [7]

h) *Williamson's Method*

Williamsons takes the array

$$H=\begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

where A,B,C and D are circulant matrices of order n. Williamson constructed these matrices as appropriate (1,-1)-linear combination of (U+Un-1), (U2+Un-2). $\left(U^{\frac{n-1}{2}},U^{\frac{n+1}{2}}\right)$ and Un = In where U = circ (0,1,0…,0)

The coefficients 1, -1 in the linear combination are obtained through computer search. Such that $A^2+B^2+C^2+D^2=4nI_{4n}$ [4], [13] and [7]

Hadamard matrices are used in communication system, digital image processing and orthogonal spreading sequence for direct sequence spread spectrum code division multiple access. They have direct application in constructing error control codes. They have also application in the constructing supersaturated screening design and optimal weighing design.. [9]

II. Construction of Hadamard Matrix From Frobenius Group

Singh, etal [12] forwarded a method of constructing H-matrices from certain AS. Here we forward a method which constructs suitable AS or CC by the action of Frobenius group and then H-matrix is obtained as suitable (1,-1)- linear combinations of adjacency matrices of AS or CC.

a) *Construction of Frobenius group (G) of order $\frac{p(p-1)}{2}$, p is an odd prime of the from 4t-1.*

Let ρ = (123…p) be a cycle in Z_p.
and σ = $(x^2x^4\ldots x^{p-1})$ $(x^3x^5\ldots x^{p-2})$ (p) be a permutation on Z_p.
Where x is primitive root of multiplicative cyclic group of Z_p.
Let K = the cyclic group generated by ρ.
and H = the cyclic group generated by σ.
Let G = KH, We claim that G is Frobenius group. Elements of K, except identity element e, fixes no point and each element of H fixes exactly one point. Next we show that elements in KH-(KUH) fixes exactly one point, take

$\rho^i\sigma^j(0<i<p,\ 0<j<\frac{(p-1)}{2}) \in KH-(KUH)$

Note that if $\rho^i\sigma^j(y) = y$

$\Rightarrow$ yx2j+i=y

$\Rightarrow$ $y=i(1-x^{2j})^{-2}$ we get unique y .[∵ inverse element is unique in a group]

Hence every element in $G-(H\cup K)$ fixes exactly one point. So G = KH is Frobenius group of order $\frac{p(p-1)}{2}$

b) *Orbits of G on X x X. Where X = {1,2…,p}*

Orbit of (p,1) under the action of G

$= \{g(p,1)\ |g\in G\}$

$= \{\rho i\sigma j(p,1)\,|\,1\le i\le p,\ 1\le j\le \frac{p-1}{2}\}$

$= \{(i,x2j+i)\ |1\le i\le p, 1\le j\le \frac{p-1}{2}\}$=R1(say)

This set clearly contains $\frac{p(p-1)}{2}$ distinct elements and difference b-a of each pair (a,b) ∊ R, is a quadratic residue modulo p.

Orbit of (1,p) under the action of G

$= \{x2j+I,i)\,|\,1\le i\le p \text{ and } 1\le j\le \frac{p-1}{2}\}$=R2 (say)

This set contains $\frac{p(p-1)}{2}$ distinct elements and difference of each pair is an non quadratic residue modulo p. Since G is transitive,

Orbit of (1,1) = {(1,1), (2,2),(3,3), …(p,p)}
= R0 (Say)

We can be easily verified that {R0,R1,R2} defines a CC.
Now we extend the action of G on the set X={1,2…,p,p+1} such that G fixes (p+1).

©2011 Global Journals Inc. (US)

Then different orbits of G on X x X are as follows.

$R'_{01} = \{(1,1),(2,2)\ldots,(p,p)\}$;

$R'_{02}=\{(p+1,p+1)\}$;

$R'_1=R_1$;

$R'_2=R_2$;

$R'_3=\{(1,p+1), (2,p+1), (3,p+1)\ldots,(p,p+1)\}$;

$R'_4 = \{(p+1,1), (p+1,2)\ldots, (p+1,p)$

Let, $M_{01},M_{02},M_1,M_2,M_3$ and M_4 be adjacency matrices of the relations $R_{01},R_{02},R_1,R_2,R_3$ and R_4 respectively. Clearly $M_{01}+M_{02} = I_{p+1}$

Let $Q = M_1\text{-}M_2$

and $S = Q + M_3 - M_4$

and $H_{p+1} = I_{p+1}+S$

Then H_{p+1} is a Hadamard matrix equivalent to Hardamard matrix of Paley's form.

Remark : The above construction can be easily extended to GF(p^{α}) to have an H-matrix of order $p^{\alpha}+1$.

Construction of Hadamard matrix from Dihedral group D_{2n} (n is odd) We describe below the construction for H matrix from D_{2n} (n is odd) which is also a Frobenius group. The permutation representation of dihedral group.

D_{2n} is $\{\rho, \rho^2, \rho^3,\ldots \rho^n = e, \rho\sigma, \rho^2\sigma \ldots \rho^n\sigma\}$

where $\rho(x) = x+1 \pmod n$

and $\sigma(x) = n\text{-}x+2 \pmod n$.

Consider the action of D_{2n} on X x X when $X = \{1,2,\ldots,n)$

The orbit of $(1,2) = \{(\rho^i(1), \rho^i(2)) : i=0,1,2,\ldots,n\text{-}1\}$

$\cup\{(\rho^i\sigma(1), \rho^i\sigma(2) : i = 0,1,2\ldots,n\text{-}1\}$

$= \{(1+i,2+i): i = 0,1,2\ldots,n\text{-}1\}$

$\cup\{(1+i,i) : i = 0,1,2,\ldots,n\text{-}1\}$

$= R_1\cup R_2$ (Say).

Let U = Circ (0,1,0,0…,0) (Circulant matrix with 1st row (0,1,0,0…,0))

$$= \begin{bmatrix} 0 & 1 & 0 & 0 \ldots\ldots\ldots 0 \\ 0 & 0 & 1 & 0 \ldots\ldots\ldots 0 \\ 0 & 0 & 0 & 1 \ldots\ldots\ldots 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 \ldots\ldots\ldots 0 \\ 1 & 0 & 0 & 0 \ldots\ldots\ldots 0 \end{bmatrix}_{n\times n}, \text{ Clearly } U^n = I_n$$

Then Adjacency matrix of $R_1 = U$

We have the following matrix representation of the orbits

Orbit of (1,2) $\to U + U^{n-1}$

Similarly orbit of (1,3) $\to U^2 + U^{n-2}$

Orbit of (1,4) $\to U^3+ U^{n-3}$

Orbit of $1,\frac{(n+1)}{2}$ $\to U^{\frac{n-1}{2}}+U^{\frac{n-1}{2}}$

An orbit of (1,1) $\to I_n$

$U^i+U^{n-i},(i=1,2\ldots\frac{(n-1)}{2}))$ and I_n are the adjacency matrices of an AS.

Note that these circulant matrices are used in construction of Williamson's matrices A, B, C and D that Williamson used in his construction of Hadamard matrices.

III. Illustrations

a) *Construction of Hadmard Matrix of Order 7+1=8*
Consider the permutations on X = {1,2,3,4,5,6,7}

Given by

$\rho = (1234567)$

$\sigma = (3^2 3^4 3^6)\ (3^1 3^3 3^4)\ (7) = (241)\ (365)\ (7)$

Then $G = \{\rho^i\sigma^j : 1\le i\le 7, 1\le j\le 3\}$ is Frobenius Group of order 21.

Orbits of G on X x X where X = (1,2,3,4,5,6,7} are obtained as follows.

Orbit of (7,1) =
{(1,2),(1,3),(1,5),(2,3),(2,4),(2,6),(3,4),(3,5),
(3,7),(4,1),(4,5),(4,6),(5,2),(5,6),(5,7),(6,1),
(6,3),(6,7),(7,1),(7,2),(7,4)=R(say).

Orbit of (1,7)-
{((1,4),(1,6),(1,7),(2,1),(2,5),(2,7),(3,1), (3,2),
(3,6),(4,2),(4,3),(4,7),(5,1),(5,3),(5,4),(6,2),
(6,4),(6,5),(7,3),(7,5),(7,6)} = R_2 (say)

Orbit of (1,1)=
{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(7,7)}= R_0 (say)

Note that R_0,R_1,R_2 defines a CC on X = {1,2,3,4,5,6,7}

Now we extend the action of G on the set X=(1,2,3,4,5,6,7,8) such that different orbits of G on X x X are.

$R'_{01} = R_0$;

$R'_{02} = \{8,8)\}$;

$R'_1 = R_1$;

$R'_2 = R_2$;

$R'_3 = \{(1,8), (2,8), (3,8), (4,8), 95,80, (6,8), (7,8)\}$;

$R'_4 = \{(8,1), (8,2), (8,3), (8,4), (8,5), (8,6), (8,7)\}$

M_{01}, M_{02}, M_1, M_2, M_3, and M_4 are adjacency matrices of the relations R_{01}, R_{02}, R_1, R_2, R_3 and R_4 respectively and are given by

Global Journal of Computer Science and Technology Volume XI Issue X Version I May 2011

©2011 Global Journals Inc. (US)

$$M_{01}=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0\end{bmatrix}\qquad M_{02}=\begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1\end{bmatrix}$$

$$M_{1}=\begin{bmatrix}0&1&1&0&1&0&0&0\\0&0&1&1&0&1&0&0\\0&0&0&1&1&0&1&0\\1&0&0&0&1&1&0&0\\0&1&0&0&0&1&1&0\\1&0&1&0&0&0&1&0\\1&1&0&1&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix}\qquad M_{2}=\begin{bmatrix}0&0&0&1&0&1&1&0\\1&0&0&0&1&0&1&0\\1&1&0&0&0&1&0&0\\0&1&1&0&0&0&1&0\\1&0&1&1&0&0&0&0\\0&1&0&1&1&0&0&0\\0&0&1&0&1&1&0&0\\0&0&0&0&0&0&0&0\end{bmatrix}$$

$$M_{3}=\begin{bmatrix}0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&0\end{bmatrix}\qquad M_{4}=\begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\1&1&1&1&1&1&1&0\end{bmatrix}$$

$Q = M_1 \quad M_2 \quad -$

$S = Q+M_3-M_4 = M_1-M_2+M_3-M_4$

We take, $H = I_8 + S = M_{01}+M_{02}+M_1-M_2+M_3-M_4$

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

©2011 Global Journals Inc. (US)

b) *Construction of H-matrix from dihedral group D_6. The permutational representation of dihedral group D_6.*

is $\{\rho, \rho^2, \rho^3 = e, \rho\sigma, \rho^2\sigma, \rho^3\sigma = \sigma\}$

where $\rho(x) = x + 1 \pmod 3$

$\sigma(x) = 3\text{-}x+2 \pmod 3$

i.e. $\sigma = (123)$, $\sigma = (2,3)$

consider the action of D_6 on X x X where X {1,23}

the orbit of (1,1) = {(1,1), (2,2), (3,3)} = R_0 (say)

orbit of (1,2)={(2,3), (3,1),(1,2)}∪{(2,1),(3,2),(1,3)}=$R_1 \cup R_2$ (say)

then adjacency matrix of $R_1 = U$

and adjacency matrix of $R_2 = U^{3-1} = U^2$

matrix representation of orbit of (1,2) is $U+U^2$ =

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

matrix representation of orbit of (1,1)= $U_3 = I_3 =$

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

then A, B, C and D are given by A =

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = U^3 + (U + U^2)$$

$$B = C = D = -(U+U^2) + U^3 = \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}$$

Now we have the following H-matrix of order 12.

$$H_{12} = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

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

IV. Future Prospects

At present no single method of construction can settle Hadamard conjecture which states that there exists an H-matrix of order 4t for all positive integer. By Computer search Djokovic [5] shows that there is no Williamson matrix of order t = 35 and so H-matrix of order 35x4=140 can be constructed by Williamson method. However since 139 is a prime of the form 4t-1, an H-matrix of order 140 can be constructed by the above method. We conjecture that by our general method H-matrix of any order can be constructed from suitable group.

V. Acknowledgement

The second author is indebted to CSIR. New Delhi, India for its financial support.

References Références Referencias

1. J. L. Alperin and Rowen B. Bell, Groups and representation, Springer-Verlog, New York, 1995.
2. R. C. Bose, and Mesner, M. Dale, 'On Linear Associative Algebra corresponding to Association Schemes of Partial Balanced Designs', Ann. Math. Stat. 30(1959), 21-28.
3. Collin, J. and D. Perkinson, Frobenius Polytopes, http://peaplereed.edu/~davidp/homepage/myp aper/ frob.pdf, 2004.
4. Joh D. Dixon and Brian Mortimer, Permutation group, Springer-Verlag, New York, 1996.
5. D. Z. Djokovic, Williamson matrices of order 4n for n=33, 35,39, Discrete Math. 115(1993), 267-271.
6. M. JR. Hall, Combinational Theory. Blaisdell (Ginn), Waltham, Mass (1967).
7. A. Hidayat, and W. D. Wallis, Annals of Statistics, Vol. 6, No. 6 (1978), 1184-1238.
8. K.J.Horadam, Hadamard Matrices and Their Application, Princeton University Press, Princeton 2007.

©2011 Global Journals Inc. (US)

9. D. G. Higman, Coherent Configuration part-1, Ordinary representation Theory, Geometriac Deticata 4 (1976), 1-32.
10. Bertram Huppert, Character theory of finite groups, Walter de Gruyter and Co. Berlin, 1998.
11. R.E.A.C. Paley, On orthogonal matrices J. Math and Physics 12 (1933), 311-320.
12. M. K. Singh, K. Sinha and S. Kageyama, Australasian Journal of combinatorics 26 (2004) PP. 93-97.
13. J. Williamson, Hadamard determinant theorem and the sum of four squares, Duke math J. 11(1944), 65-81.

©2011 Global Journals Inc. (US)