Construction Of Hadamard Matrices From Certain Frobenius Groups

M.K.Singh[1] and P.K.Manjhi[2]

[1] Deprtment of Mathematics Ranchi University Ranchi

Received: 20 March 2011 Accepted: 19 April 2011 Published: 29 April 2011

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) â??” linear combinations of adjacency matrices of the coherent configuration.

Index terms— adamard matrix, Coherent Configuration. Association Scheme and Frobenius group.

1 Introduction

We begin with following definitions. a) Hadamard matrix (H-matrix) HH T = ml m [1] b) Coherent configuration (CC)Let X = {1,2,3,?.n}, and R = {R 1 ,R 2 ?,R r } be a collection of binary relations on X such that.

(cc1) R i ? R j = ? for 1? i<j ?r;

(cc2) ? r i=1 R i = X 2 = X x X (cc3) For all i ? {1,2,3?,r} there exists i' ? {1,2,3?,r} such that' 1 i i =R R ?

(cc4) There exists I?{1,2,3?,r} such thati I i R ? ? = ? ,

Where ? = {(x,x)|(x? 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 About ? -Dept. Of Mathematics, Ranchi University, Ranchi -834008 India E-mail-mithleshkumarsingh@gmail.com About ? -Dept. Of Mathematics, Vinoba Bhave University, Hazaribag -825301 E-mail-19pankaj81@gmail.coma i j = ? ? ? ? ? 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)? x? X};

(As2)i i ?1 ,for i ?{0,1,2,?,r}; (As3) ? ?R k ? {z? X? ?R i ? R j }? = k ij

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? G and (x,y) ? X x 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) ?H = {e} for all x?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, For all i,j,k {0,1,2,?,r}, for all (x,y) (x,z) and (z,y) [2] and [9] 1, iff (i,j) R, ? 0, otherwise hence the corresponding permutation is unique up to isomorphism.

2 Global

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 ? H={e} where H is Frobenius complement. [1], [3] and [10]. g) Paley's construction of Hadamard matrix If p ? =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 ?, in some order. A matrix Q of order q is defined as follows. The (i,j) entry of Q equals ? (a i -a j), where ? is the quadratic character on GF(q) defined by, ? (0)=0? ? ? = GF(q) in element quadratic a not is b if 1 - (q)) GF in square (perfect element quadratic zero non a is b if 1,) (b ? Set S = ? ? ? ? ? ? ? ? ? ? ? ? Q 1 1 0

' , H = I q+1 +S where 1 = q x 1 matrix with each entry 1. H is Hadamard matrix.

[11] and Williamson constructed these matrices as appropriate (1,-1)-linear combination of (U+Un-1), (U2+Un-2).? ? ? ? ? ? ? ? + ? 2 1 2 1 , n n U U

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.

3 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 , p is an odd prime of the from 4t-1.

Let ? = (123?p) be a cycle in Z p . and ? = (x 2 x 4 ?x p-1) (x 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). ? i ? i (0<i<p, 0<j<) ?KH-(KUH) Note that if ? i ? j (y) = y ? yx2j+i=y ? y=i(1-x 2j

4 , 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)? U + U n-1 Similarly orbit of (1,3) ? U 2 + U n-2 Orbit of (1,4) ? U 3 + U n-3 Orbit of ? + An orbit of (1,1) ? I n U i +U n-i ,(i=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.

5 III.

6 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 ? =(1234567) ? = (3 2 3 4 3 6) (3 1 3 3 3 4) (7) = (241) (365) (7) Then G = {? i ? j :1?i?7,1?j?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, **??**), (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, **??**),(1,7),(2,1),(2,5),(2,7),(3,1), (3,2), (3, **??**),(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 = {(1,2 1 n 1,) (+ 2 1 n) (? U U n-1 2 n-1 2 ? 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 ? 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 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 0 0 0 0 0 1 0 0 0 0 1 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 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 ? 1 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 0 0 0 0 ? 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0 0 1 0 1 1 0 1 0 1 0 0 1 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 ? 0 0 0 0 0 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 1 0 1 0 1 1 0 1 0 1 0 0 0 0 1 0 0 1 0 1 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 M 0 1 = M 0 2 = M 1 = M 2 = M 3 = M 4 = Q = M 1 - M 2 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 = ?

? 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 b) Construction of H-matrix from dihedral group D 6 .

The permutational representation of dihedral group D 6 .

is {?, ? 2 , ? 3 = e, ??, ? 2 ?, ? 3 ? = ?} where ?(x) = x + 1 (mod 3) ?(x) = 3-x+2 (mod 3) i.e. ? = (123), ? = (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 ?R 2 (say) then adjacency matrix of R 1 = U and adjacency matrix of R2 = U 3-1 =U 2 matrix representation of orbit of (1,2) is U+U 2 = ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? 0 1 1 1 0 1 1 1 0 matrix representation of orbit of (1,1)= U 3 =I 3 = ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? 1 0 0 0 1 0 0 0 1

then A, B, C and D are given by A =) (1 1 1 1 1 1 1 1 1 2 3 U U U + + ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? B = C = D = -(U+U 2) + U 3 = ? 1 1 1 1 1 1 1 1 1

Now we have the following H-matrix of order 12. 1

IV.

7 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. [1] [2]

Figure 1:

.1 ACKNOWLEDGEMENT

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

.2 May

[Paley ()] , R E A C Paley . *On orthogonal matrices J. Math and Physics* 1933. 12 p. .

[Collin et al. ()] , J Collin , D Perkinson , Frobenius Polytopes . `http://peaplereed.edu/~davidp/homepage/mypaper/frob.pdf` 2004.

[Singh et al. ()] , M K Singh , K Sinha , S Kageyama . *Australasian Journal of combinatorics* 2004. 26 p. .

[Huppert ()] *Character theory of finite groups*, Bertram Huppert . 1998. Berlin: Walter de Gruyter and Co.

[Higman ()] 'Coherent Configuration part-1, Ordinary representation Theory'. D G Higman . *Geometriac Deticata* 1976. 4 p. .

[Alperin and Bell ()] *Groups and representation*, J L Alperin , Rowen B Bell . 1995. New York: Springer-Verlog.

[Williamson ()] 'Hadamard determinant theorem and the sum of four squares'. J Williamson . *Duke math J* 1944. 11 p. .

[Bose et al. ()] 'On Linear Associative Algebra corresponding to Association Schemes of Partial Balanced Designs'. R C Bose , M Mesner , Dale . *Ann. Math. Stat* 1959. 30 p. .

[Joh et al. ()] *Permutation group*, D Joh , Brian Dixon , Mortimer . 1996. New York: Springer-Verlag.

[Djokovic ()] *Williamson matrices of order 4n for n=33, 35,39, Discrete Math*, D Z Djokovic . 1993. 115 p. .