

Construct Hadamard matrices by means of several groups and prime numbers

Hizer Leka¹

^{1*} Department of Mathematics, Faculty of Natural Sciences and Mathematics, University of Tetova, MK

Corresponding Author: hizer.leka@hotmail.com

Abstract

Hadamard matrix, is a square matrix, the elements of which are either 1 or -1 and its rows mutually orthogonal. They have great application in computer science and communication technology. The most important open question in Hadamard matrix theory is that of their existence. There are several methods for constructing them. It will be shown that two classic methods for the Hadamard matrix construct, that of Paley and Williamson, can be unified and Paley and Williamson's method can be constructed with a uniform method by producing a association scheme or coherent configuration from group action to a community X and the production of Hadamard matrices, taking appropriate linear combinations (1,-1) of the matrix representation of coherent configuration. For example, through the orbits of the group, the matrices of group representation orbits are taken and eventually the sum of these matrices gives a Hadamard matrix. Thus, Hadamard matrices are constructed by group's action in the community. It will also be shown that using the Legendre symbol, the prime numbers and congruences according to the module, the first row of the Hadamard matrix is formed, then the other rows of the Hadamard matrix are taken cyclically and thus obtained a Hadamard order matrix n .

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

1. Introduction

We begin with following definitions.

- **Definition of Hadamard matrix:** A Hadamard matrix of order n , H_n , is an $n \times n$ square matrix with elements $+1$ and -1 's such $H_n \cdot H_n^T = nI_n$, where I_n is the identity matrix of order n . [2]

Examples of Hadamard matrix order 1, 2 and 4 :

$$H_1 = [1], H_1' = [-1], H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, H_2' = \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix}, H_2'' = \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, H_4' = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}, H_4'' = \begin{bmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix}.$$

Hadamard's matrices have extensive application in computer science in modern communication and statistics. Also, they can also be used to correct blocked code errors that can correct a large number of errors in the communications field. Their characteristic is the problem of existence.

- **Symmetric H-matrix:** An H -matrix H is said to be symmetric if $H = H^T$. While H -matrix is antisymmetric if $H = -H^T$. [2] and [3]
- **A Cyclic Hadamard matrix** is a Hadamard matrix with an additional property that in the standard form, removing the top row and the left-most column, the rows are cyclic shifts of each other. [2]
- **Coherent configuration:** Let $X = \{1, 2, \dots, n\}$, and $R = \{R_1, R_2, \dots, R_r\}$ be a collection of binary relations on X such that.
 - 1) $R_i \cap R_j = \emptyset$ for $1 \leq i < j \leq r$;
 - 2) $\bigcup_{i=1}^r R_i = X^2 = X \times X$;
 - 3) $\forall i = 1, 2, \dots, r$ there exists $i' = 1, 2, \dots, r$, such that $X = \{1, 2, \dots, n\}$, $R_i^{-1} = R_{i'}$;
 - 4) There exists $I \subseteq \{1, 2, \dots, r\}$ such that $\bigcup_{i \in I} R_i = \Delta$, where $\Delta = \{(x, x) | x \in X\}$. [1]
- **Association Scheme:** Let R_0, R_1, \dots, R_m be binary relations on a set $X = \{1, 2, \dots, n\}$.

Let $A_i = [a_{ij}]$ be the $(0,1)$ matrix defined as

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

The matrix A_i is called adjacency matrix of the relation R_i . [3]

The set $P = \{R_0, R_1, \dots, R_m\}$ is called an m class association scheme if the adjacency matrices A_i of R_i ($i = 0, 1, 2, \dots, m$) satisfying:

- 1) $A_0 = I$ (identity matrix) and $A_i \neq 0, \forall i$;
 - 2) $\sum_{i=0}^m A_i = J$, where J is all-1 matrix;
 - 3) $A_i^T = A_i, \forall i \in \{1, 2, \dots, m\}$;
 - 4) There are numbers p_{ij}^k such that $A_i A_j = \sum_{k=0}^m p_{ij}^k A_k$. [3]
- **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 $X \times X$ by $g(x, y) = (g(x), g(y)), g \in G$ and $(x, y) \in X \times X$. Then different orbits of G on $X \times X$ define a coherent configuration. [7]
 - **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. [1]
 - A. **Williamson's Method:** This construction was first described by Williamson in the early 1940s. Let A, B, C and D be circulant, or back circulant, matrices of order n , satisfying the following equalities:

$$XY^T = YX^T, \quad \forall X, Y \in \{A, B, C, D\}$$

$$AB^T + AC^T + AD^T = 4nI_n. \quad [4]$$

We observe that the first condition is often bypassed by requiring that all component matrices be symmetric. Williamson proves that under these constraints, the above matrices may be composed as follows to give a Hadamard matrix:

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

Williamson constructed these matrices as appropriate $(1, -1)$ -linear combination of $(U + U_{n-1}), (U_2 + U_{n-2}), \left(U^{\frac{n-1}{2}}, U^{\frac{n+1}{2}} \right)$ and $U_n = I_n$ where $U = \text{circl}(0, 1, 0, \dots, 0)$. [4] and [13]

B. Paley's construction of Hadamard matrix : If $p^\alpha = q$ is prime number power $q + 1 = 0 \pmod{4}$.

Suppose the members of the field $GF(q)$ are labeled a_0, a_1, a_2, \dots , in some order. Then a Hadamard matrix of order $q + 1$ can be construction 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 $\chi = 0$.

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

Set $S = \begin{bmatrix} 0 & 1' \\ -1 & Q \end{bmatrix}$, $H = I_{q+1} + S$, where $1' = q \times 1$ matrix with each entry 1. H is Hadamard matrix. [9] [10] and [6]

2. Construct Hadamard matrices by means of several groups

A. Construction of Frobenius group (G) of order $\frac{p(p-1)}{2}$, p is an odd prime of the form $4k - 1$.

Let $\rho = (123\dots p)$ be a cycle in Z_p and $\sigma = (x^2 x^4 \dots x^{p-1})(x^3 x^5 \dots x^{p-2})(p)$ be a permutation on Z_p . Let K the cyclic group generated by ρ and H the cyclic group generated by σ . Then $G = KH$ is Frobenius group of order $\frac{p(p-1)}{2}$. [1]

Orbits of G on $X \times X$, where $X = \{1, 2, \dots, p\}$. Orbit of $(p, 1)$ under the action of $G = \{G(p, 1) | g \in G\} = \left\{ \rho^i \sigma^j(p, 1) | 1 \leq i \leq p, 1 \leq j \leq \frac{p-1}{2} \right\} = R_1$.

This set clearly contains $\frac{p(p-1)}{2}$ distinct elements and $b - a$ is a quadratic residue modulo p , for all $(a, b) \in R$.

Orbit of $(1, p)$ under the action of $G = \left\{ (x^{2j} + I, i) | 1 \leq i \leq p \wedge 1 \leq j \leq \frac{p-1}{2} \right\} = R_2$, which also contains $\frac{p(p-1)}{2}$ elements and $b - a$ difference of each pair is a non quadratic residue modulo p .

Orbit of $(1, 1) = \{(1, 1), (2, 2), (3, 3), \dots, (p, p)\} = R_0$. It is clear that group $\{R_0, R_1, R_2\}$ represents a coherent configuration. [1] and [5]

If we extend the group G action to $X = \{1, 2, \dots, p, p+1\}$ such that G fixes $(p+1)$, then the different orbits of G in $X \times X$ are as follows:

$$R'_{01} = \{(1,1), (2,2), (3,3), \dots, (p, p)\};$$

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

$$R'_1 = R_1;$$

[1] and [5]

$$R'_2 = R_2;$$

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

$$R'_4 = \{(p+1, 1), (p+1, 2), (p+1, 3), \dots, (p+1, p)\}.$$

Let $A_{01}, A_{02}, A_1, A_2, A_3$ and A_4 matrices of relevant representation of relations $R_{01}, R_{02}, R_1, R_2, R_3$ and R_4 . It is clear that: $A_{01} + A_{02} = I_{p+1}$. Let $Q = A_1 - A_2, S = Q + A_3 - A_4$, and $H_{p+1} = I_{p+1} + S$. Then H_{p+1} is a Hadamard matrix equivalent to Hadamard matrix of Paley's form. [12] and [5]

• **Example** [1] and [5]. Construction of Hadamard matrix of order $7+1=8$.

Consider the permutations on $X = \{1, 2, 3, 4, 5, 6, 7\}$ given by: $\rho = (1234567)$ and $\sigma = (3^2 3^4 3^6) (3^1 3^3 3^4) (7) = (241) (364) (7)$. Then, $G = \{\rho^i \sigma^j : 1 \leq i \leq 7, 1 \leq j \leq 3\}$ is Frobenius Group of order 21. Orbits of G on $X \times X$, where $X = \{1, 2, 3, 4, 5, 6, 7\}$ are obtained as follows.:

$$(7,1) = \{(1,2), (1,3), (1,5), (2,3), (2,4), (2,6), (3,4), (3,5), (3,7), (4,1), (4,5), (4,6), (5,2), (5,6), (5,7), (6,1), (6,3),$$

$$(6,7), (7,1), (7,2), (7,4)\} = R_1;$$

$$(1,7) = \{(1,4), (1,6), (1,7), (2,1), (2,5), (2,7), (3,1), (3,2), (3,6), (4,2), (4,3), (4,7), (5,1), (5,3), (5,4), (6,2), (6,4),$$

$$(6,5), (7,3), (7,5), (7,6)\} = R_2;$$

$$(1,1) = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7)\} = R_0$$

Then,

$$R'_{01} = R_0;$$

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

$$R'_1 = R_1;$$

$$R'_2 = R_2;$$

$$R'_3 = \{(1,8), (2,8), (3,8), (4,8), (5,8), (6,8), (7,8)\};$$

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

$$\begin{aligned}
 A_{01} &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} & A_{02} &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} & A_1 &= \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \\
 A_2 &= \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} & A_3 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} & A_4 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}
 \end{aligned}$$

$Q = A_1 - A_2$; $S = Q + A_3 - A_4 = A_1 - A_2 + A_3 - A_4$. Then,

$$H_8 = I_8 + S = A_{01} + A_{02} + A_1 - A_2 + A_3 - A_4 = \begin{bmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \end{bmatrix}.$$

B. Construction of H -matrix from dihedral group D_{2n}

The permutation representation of dihedral group D_{2n} is

$$D_{2n} = \{\rho_1, \rho_2, \dots, \rho_n = e, \rho\sigma, \rho^2\sigma, \rho^3\sigma, \dots, \rho^n\sigma\},$$

where $\rho(x) = x + 1 \pmod{n}$ and $\sigma(x) = n - x + 2 \pmod{n}$.

Consider the action of D_{2n} on $X \times X$, when $X = \{1, 2, \dots, n\}$.

The orbit of

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

$$= \{(1+i, 2+i) : i = 0, 1, 2, \dots, n-1\} \cup \{(1+i, i) : i = 0, 1, 2, \dots, n-1\} = R_1 \cup R_2.$$

Let $U = Cirk(0, 1, 0, 0, \dots, 0)$ (Circulant matrix with 1st row $(0, 1, 0, 0, \dots, 0)$).

Then

$$U^n = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{bmatrix}, \text{ e qartë se } U^n = I_n.$$

Then Adjacency matrix of $R_1 = U$. Then,

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

$(1,3) \rightarrow U^2 + U^{n-2}$;

$(1,4) \rightarrow U^3 + U^{n-3}$.

$\left(1, \frac{(n+1)}{2}\right) \rightarrow U^{\frac{n-1}{2}} + U^{\frac{n-1}{2}}$;

$(1,1) \rightarrow I_n$.

$U^i + U^{i-1}, \left(i = 1, 2, \dots, \frac{(n-1)}{2}\right)$ and I_n are the adjacency matrices of an association scheme. Note that these circulant matrices are used in construction of Williamson's matrices A, B, C dhe D that Williamson used in his construction of Hadamard matrices. [1] [5] and [13]

3. Construction of Hadamard matrices from prime numbers

The following will show the construction of H matrices, by means of one and two prime numbers.

A. Prime construction

Let p be a prime congruent to $3 \bmod 4$, and a_i for $i = 0, 1, 2, \dots, p-1$, be the $(+1, -1)$ -valued sequence of length p we wish to design.

Put $a_0 = -1$. For $1 \leq i \leq p-1$, assign $+1$ or -1 to each a_i according to the following rule:

$$a_i = \begin{cases} +1, & \text{if } i \text{ is a "quadratic residue mod } p" \\ -1, & \text{otherwise} \end{cases}.$$

Then, the sequence a_0, a_1, \dots, a_{p-1} and all of its cyclic shifts together with the additional top row and left-most column of all $+1$'s gives a cyclic Hadamard matrix of order $p+1$. [2] and [5]

- **Example** [2] and [5]. Let $p = 11$. Then:

i	1	2	3	4	5	6	7	8	9	10
$i^2 \pmod{11}$	1	4	9	5	3	3	5	9	4	1

i	0	1	2	3	4	5	6	7	8	9	10
a_i	—	+	—	+	+	+	—	—	—	+	—

According to the conditions listed above Hadamard's matrix of order 12 looks like this:

$$H_{12} = \begin{bmatrix} + & + & + & + & + & + & + & + & + & + & + & + \\ + & - & + & - & + & + & + & - & - & - & + & - \\ + & - & - & + & - & + & + & + & - & - & - & + \\ + & + & - & - & + & - & + & + & + & - & - & - \\ + & - & + & - & - & + & - & + & + & + & - & - \\ + & - & - & + & - & - & + & - & + & + & + & - \\ + & - & - & - & + & - & - & + & - & + & + & + \\ + & + & - & - & - & + & - & - & + & - & + & + \\ + & + & + & - & - & - & + & - & - & + & - & + \\ + & + & + & + & - & - & - & + & - & - & + & - \\ + & - & + & + & + & - & - & - & + & - & - & + \\ + & + & - & + & + & + & - & - & - & + & - & - \end{bmatrix}.$$

B. Twin prime construction

Let both p and $p+1$ be primes, and l be the product $p(p+2)$. Assign $+1$ or -1 to each a_i for $i = 0, 1, 2, \dots, l-1$, by the following rule:

$$a_i = \begin{cases} \left(\frac{i}{p}\right)\left(\frac{i}{p+2}\right), & \text{if } i \text{ is not a multiple of } p \text{ or } p+2 \\ +1, & \text{if } i \neq 0 \text{ is a multiple of } p \\ -1, & \text{if } i \text{ is a multiple of } p+2, \text{ including } 0 \end{cases}$$

where the symbol $\left(\frac{i}{p}\right)$ is defined to be $+1$, if i is a quadratic **mod** p and -1 otherwise.

Then, the sequence a_0, a_1, \dots, a_{l-1} and all of its cyclic shifts together with the additional top row and left-most column of all $+1$'s gives a cyclic Hadamard matrix of order $l+1$. [2] and [5]

- **Example** [2] and [5]. Let $p = 3$. Then, we have:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\left(\frac{i}{3}\right)$		+	—		+	—		+	—		+	—		+	—
$\left(\frac{i}{5}\right)$		+	—	—	+		+	—	—	+		+	—	—	+
$\left(\frac{i}{3}\right)\left(\frac{i}{5}\right)$		+	+		+		—	+			—		—	—	
a'_i	+			—		+	—			—	+		—		
a_i	+	+	+	—	+	+	—	—	+	—	+	—	—	—	—

Then, Hadamard's matrix of order 12 is :

$$H_{16} = \begin{bmatrix} + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\ + & + & + & + & - & + & - & + & - & + & + & - & - & - & - \\ + & - & + & + & + & - & + & - & + & - & + & + & - & - & - \\ + & - & - & + & + & + & - & + & - & + & - & + & + & - & - \\ + & - & - & - & + & + & + & - & + & - & + & - & + & + & - \\ + & + & - & - & - & - & + & + & + & - & + & - & + & - & + \\ + & + & + & - & - & - & - & + & + & + & - & + & - & + & - \\ + & - & + & + & + & - & - & - & + & + & + & - & + & - & + \\ + & + & - & + & + & + & - & - & - & + & + & + & - & + & - \\ + & - & + & - & + & + & + & - & - & - & + & + & + & - & + \\ + & + & - & + & - & + & + & + & - & - & - & + & + & + & - \\ + & - & + & - & + & - & + & + & + & - & - & - & + & + & + \\ + & + & - & + & - & + & - & + & + & + & - & - & - & + & + \\ + & + & + & - & + & - & + & + & + & - & - & - & - & + & + \end{bmatrix}$$

4. Conclusion

By the above, it was shown that two classical methods for the Hadamard matrix concept, that of Paley and Williamson, can be unified and Paley and Williamson's method can be constructed with a uniform method by producing a association scheme and coherent configuration or configuration from group action to a community and the production of Hadamard matrices, taking appropriate linear combinations (1, -1) of matrix representation of coherent configuration. Through the group's orbits, the group's representative orbits matrices are finally taken and the sum of these matrices gives a Hadamard matrix. 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 [11] shows that there is no Williamson matrix of order $t = 35$ and so H-matrix of order $35 \times 4 = 140$ 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. While, from conjecture of M.K Singh, P.K Manjhi [1], that by their general method H-matrix of any order can be constructed from suitable group. It was also shown that by using the Legendre symbol, prime numbers, cyclic matrices, and congruences according to the module, can be constructed Hadamard's matrix of order n.

References

- [1]. M.K Singh, P.K Manjhi "Construction of Hadamard Matrices From Certain Frobenius Group", Ranchi University, May 2011.
- [2]. Hong-Yeop Song "Examples and Constructions of Hadamard matrices" Yonsei University, Seoul 120-749, Korea, June 2002.
- [3]. Singh M.K and Pandey Pinky "Construction of Association Schemes and Coherent Configuration from Williamson's Hadamard Matrices and their Properties" University Department of Mathematics, Ranchi University Ranchi, 834008, Jharkhand, India, Department of Mathematics, Nirmala College, Ranchi, 834002, Jharkhand, India, 2016.
- [4]. Pádraig Ó Catháin "Group actions on Hadamard matrices" National University of Ireland Galway, November 2008.
- [5]. L.Hizer, "Disa metoda për konstruktimin e matricave të Hadamardit", punim magjistrature, Tetovë 2018.
- [6]. I.Alit, Teoria e Bllok Skemave (Dizajneve), dispencë, Tetovë 2013.
- [7]. D. G. Higman "Coherent Configuration part-1, Ordinary representation Theory" Geometriae Dedicata 4 (1976), 1-32.

- [8]. Mikhail Klin “*Coherent Configurations and Association Schemes*”. Part I Definitions, examples, simple facts
Mikhail Klin Department of Mathematics Ben Gurion University of the Negev Beer Sheva, Israel, Mey 2006.
- [9]. R.E.A.C. Paley, On orthogonal matrices J. Math and Physics 12 (1933), 311-320.
- [10]. A. Hidayat and W.D.Wallis, *Annals of statistiks*, Vol.6, No.6 (1978), 1184-1238.
- [11]. D. Z. Djokovic “*Williamson matrices of order $4n$ for $n=33, 35, 39$* , *Discrete Math.*” 115(1993), 267-271.
- [12]. Abdurzak M. Leghwel “*On Some Methods of Constructing Hadamard Matrices*” Department of
Mathematics, Faculty of Science, Alasmarya Islamic University, Zliten – Libya.
- [13]. Jennifer Seberry Wallis, “*Williamson matrices of even order*” New York, (1974), 132-142.