# Hadamard Matrix and its Application in Coding Theory and Combinatorial Design Theory 

Briji Jacob Chathely<br>Assistant Professor, Department of Mathematics<br>B. K. Birla College of Arts, Science and Commerce<br>Kalyan, Maharashtra, India


#### Abstract

Matrix theory is widely used in a variety of areas including applied mathematics, computer science, economics, engineering, operations research, statistics and others. This paper presents the study of Hadamard Matrices. There are theorems and properties related to this matrix. Also the construction of Hadamard codes and Hadamard 2- Design using Hadamard matrices is discussed in this paper.


Keywords - orthogonal, eigenvalues, tensor product, linear codes, codeword, hamming distance.

## I. Introduction

The origin of mathematical matrices lie with the study of systems of simultaneous linear equations, but they were known as arrays until the 1800s. The term "matrix" (Latin for "womb") was coined by James Joseph Sylvester, an English mathematician in the year 1850.
Matrices find many applications in scientific fields and apply to practical real life problems as well, thus making an indispensable concept for solving many practical problems. In computer based applications, matrices play a vital role in the projection of three dimensional image into a two dimensional screen, creating the realistic seeming motions.
One of the most important usage of matrices in computer science is encryption of message codes. Matrices and their inverse matrices are used by a programmer for coding or encrypting a message. With these encryptions, internet functions are working and even banks could work with transmission of sensitive and private data.
This paper studies a special type of matrix namely Hadamard matrix and also discusses the application of Hadamard matrix in coding theory and combinatorial design theory.
A. Frequently Used Notations and Terminology

- Orthogonal Vectors: [1] Two vectors $x$ and $y$, in an inner product space $V$, are orthogonal if their inner product $\langle x, y\rangle$ is zero.
- Orthogonal Set: [1] A set $\left\{v_{1}, v_{2}, \ldots, v_{n}\right\}$ is said to be orthogonal, if $\left\langle v_{i}, v_{j}\right\rangle$ is zero for $i \neq j$.
- Norm of a vector: [1] Norm of a vector $x$ is given as $\|x\|=\sqrt{\langle x, x\rangle}$.
- Identity Matrix $I_{n}$ : An $n \times n$ matrix $I_{n}$ such that $A I_{n}=A$ where $A$ is an $n \times n$ matrix, is called an Identity matrix.
- Orthogonal Matrix: An $n \times n$ matrix $A$ is orthogonal if $A A^{T}=A^{T} A=I_{n}$
- det (A): Determinant of a matrix $A$.
- $A^{T}$ : Transpose of a matrix $A$.
- Eigenvalues: A real number $\lambda$ is said to be an eigenvalue of an $n \times n$ matrix $A$, if there exists a non-zero vector $x \in \mathbb{R}^{n}$, such that $A x=\lambda x$
- Tensor product of two matrices: [2] Tensor product of two matrices $A$ and $B$ where

$$
A=\left(\begin{array}{cccc}
a_{11} & a_{12} & \ldots & a_{1 n} \\
a_{21} & a_{22} & \ldots & a_{2 n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m 1} & a_{m 2} & \ldots & a_{m n}
\end{array}\right)
$$

and

$$
B=\left(\begin{array}{cccc}
b_{11} & b_{12} & \ldots & b_{1 q} \\
b_{21} & b_{22} & \ldots & b_{2 q} \\
\vdots & \vdots & \ddots & \vdots \\
b_{m 1} & b_{m 2} & \ldots & b_{p q}
\end{array}\right)
$$

is an $m p \times n q$ matrix defined as

$$
A \otimes B=\left(\begin{array}{ccccc}
a_{11} B & a_{12} B & a_{13} B & \ldots & a_{1 n} B \\
a_{21} B & a_{22} B & a_{23} B & \ldots & a_{2 n} B \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_{m 1} B & a_{m 2} B & a_{m 3} B & \ldots & a_{m n} B
\end{array}\right)
$$

## II. Hadamard Matrices

## A. Definition

An $n$-square matrix $H$ with entries +1 and -1 such that the set of its row vectors (or column vectors) forms an orthogonal set is called a Hadamard Matrix.
For example,

$$
H_{2}=\left(\begin{array}{rr}
1 & 1 \\
1 & -1
\end{array}\right), H_{4}=\left(\begin{array}{rrrr}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1
\end{array}\right)
$$

are Hadamard matrices.

## B. Theorems and Properties of Hadamard Matrices

1) If $H$ is an $n$-square Hadamard matrix, then $H H^{T}=n I_{n}$. Conversely if $H H^{T}=n I_{n}$ and entries of $H$ are non-zero integers, then $H$ is a Hadamard matrix [7].

Proof. Since, $H$ is Hadamard, the rows of $H$ are orthogonal.
Consider the $i j^{t h}$-entry of $H H^{T}$,

$$
\begin{aligned}
\left(H H^{T}\right)_{i j} & =\sum_{k=1}^{n} h_{i k} h_{j k} \\
& = \begin{cases}0, & \text { if } i \neq j \\
n, & \text { if } i=j\end{cases}
\end{aligned}
$$

That is,

$$
\begin{aligned}
H H^{T} & =\left(\begin{array}{cccc}
n & 0 & \ldots & 0 \\
0 & n & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & n
\end{array}\right) \\
& =n I_{n}
\end{aligned}
$$

Hence, $H H^{T}=n I_{n}$.
Conversely, if $H H^{T}=n I_{n}$, then

$$
H H^{T}=\left(\begin{array}{cccc}
n & 0 & \ldots & 0 \\
0 & n & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & n
\end{array}\right)
$$

That is, the $i j^{\text {th }}$-entry of $H H^{T}$ is given as

$$
\left(H H^{T}\right)_{i j}= \begin{cases}0, & \text { if } i \neq j \\ n, & \text { if } i=j\end{cases}
$$

which implies that the rows of $H$ are orthogonal.
Now for $i=j$,

$$
\sum_{k=1}^{n} h_{i k}^{2}=n
$$

Since the entries of $H$ are non-zero integers, we get $h_{i k}= \pm 1$ for all $1 \leq i \leq n$ and $1 \leq k \leq n$ That is, $H$ is Hadamard.
2) Let $n>2$. A necessary condition for an $n-$ square matrix $H$ to be a Hadamard matrix is that $n$ is a multiple of 4 .

Proof. Suppose $H$ is a Hadamard matrix of order $n>2$. We rearrange the first 3 rows of $H$ to look like

$$
\begin{array}{lllrlrrlrrrr}
1 & \ldots & 1 & 1 & \ldots & 1 & 1 & \ldots & 1 & 1 & \ldots & 1 \\
1 & \ldots & 1 & 1 & \ldots & 1 & -1 & \ldots & -1 & -1 & \ldots & -1 \\
1 & \ldots & 1 & -1 & \ldots & -1 & 1 & \ldots & 1 & -1 & \ldots & -1
\end{array}
$$

Let $x, y, z, w$ be the number of columns of each type.
Then

$$
\begin{equation*}
x+y+z+w=n \tag{1}
\end{equation*}
$$

Taking inner product of row 1 and row 2 , row 1 and row 3 , and row 2 and row 3 we get,

$$
\begin{align*}
& x+y-z-w=0 \\
& x-y+z-w=0  \tag{2}\\
& x-y-z+w=0
\end{align*}
$$

Solving equations (1) and (2) we get, $x=y=z=w$.
Hence, from equation (1), $n=4 x$, that is $n$ is a multiple of 4 .
3) If $H$ is a Hadamard matrix of order $4 n$, and its first row and column consists of only $+1^{\prime} s$, then any two rows (or columns) other than the first row (or column) contains exactly $n(+1)^{\prime} s$ at same positions.

Proof. Let $R_{1}$ and $R_{2}$ be the two rows of $H$ other than the first row and $p$ be the number of positions where rows $R_{1}$ and $R_{2}$ both have $+1^{\prime} s$ at same place and $q$ be the number of positions where rows $R_{1}$ and $R_{2}$ both have $-1^{\prime} s$ at same place.
Since $H$ is Hadamard, its rows are orthogonal and hence every row of $H$ will have exactly $2 n(+1)^{\prime} s$ and $2 n(-1)^{\prime} s$.
This implies that at $2 n-p$ positions, $R_{1}$ and $R_{2}$ will have $+1^{\prime} s$ and $-1^{\prime} s$ respectively and similarly at $2 n-q$ positions, $R_{1}$ and $R_{2}$ will have $-1^{\prime} s$ and $+1^{\prime} s$ respectively.
Now since $R_{2}$ has $2 n(+1)^{\prime} s$, we get $p+2 n-q=2 n$, that is $p=q$.
Also by the orthogonality of $R_{1}$ and $R_{2}$, by taking their inner product, we get

$$
\begin{aligned}
& p-(2 n-p)-(2 n-q)+q=0 \\
& p-(2 n-p)-(2 n-p)+p=0
\end{aligned}
$$

Hence we get $p=q=n$.
That is $R_{1}$ and $R_{2}$ both have $+1^{\prime} s$ at same place at exactly $n$ positions.
4) If $A$ is an $n-s q u a r e$ Hadamard matrix, then

$$
H=\left(\begin{array}{rr}
A & A \\
A & -A
\end{array}\right)
$$

is also Hadamard.
Proof. Since $A$ is Hadamard, we have $A A^{T}=n I_{n}$.
Consider,

$$
\begin{aligned}
H H^{T} & =\left(\begin{array}{cc}
A & A \\
A & -A
\end{array}\right)\left(\begin{array}{cc}
A^{T} & A^{T} \\
A^{T} & -A^{T}
\end{array}\right) \\
& =\left(\begin{array}{cc}
2 A A^{T} & 0 \\
0 & 2 A A^{T}
\end{array}\right) \\
& =\left(\begin{array}{cc}
2 n I_{n} & 0 \\
0 & 2 n I_{n}
\end{array}\right) \\
& =2 n I_{2 n}
\end{aligned}
$$

That is, we get $H H^{T}=2 n I_{2 n}$. Also, since $A$ is Hadamard, it's entries are +1 and -1 and hence the entries of $H$ are +1 and -1 .
Thus, $H$ is a matrix with non-zero integer entries, such that $H H^{T}=m I_{m}$ where $m=2 n$ is the order of $H$ and hence it is Hadamard.

Consequence: From the above theorem, we can say that, it is possible to generate Hadamard matrices of order $2 n$ recursively, by defining

$$
H_{1}=\left(\begin{array}{rr}
1 & 1 \\
1 & -1
\end{array}\right)
$$

and for $n \geq 2$

$$
H_{n}=\left(\begin{array}{cc}
H_{n-1} & H_{n-1}  \tag{3}\\
H_{n-1} & -H_{n-1}
\end{array}\right)
$$

5) Let $H_{n}$ be defined as in (3). Then $H_{n}$ has eigenvalues $+2^{\frac{n}{2}}$ and $-2^{\frac{n}{2}}$ of multiplicity $2^{n-1}$.

Proof. By induction on $n$
For $n=1, H_{1}$ has eigenvalues $+2^{\frac{1}{2}}$ and $-2^{\frac{1}{2}}$ of multiplicity $1=2^{1-1}$.
Let us assume that the assertion is true for $k<n$, that is the eigenvalue of

$$
H_{n-1}=\left(\begin{array}{rr}
H_{n-2} & H_{n-2} \\
H_{n-2} & -H_{n-2}
\end{array}\right)
$$

is $+2^{\frac{n-1}{2}}$ and $-2^{\frac{n-1}{2}}$ of multiplicity $2^{n-2}$.
Now, for $k=n$

$$
\begin{aligned}
H_{n} & =\left(\begin{array}{ll}
H_{n-1} & H_{n-1} \\
H_{n-1} & -H_{n-1}
\end{array}\right) \\
\operatorname{det}\left(\lambda I-H_{n}\right) & =\left|\begin{array}{cc}
\lambda I-H_{n-1} & -H_{n-1} \\
-H_{n-1} & \lambda I+H_{n-1}
\end{array}\right|
\end{aligned}
$$

Since, $-H_{n-1}$ and $\lambda I+H_{n-1}$ commute, we get

$$
\begin{aligned}
\operatorname{det}\left(\lambda I-H_{n}\right) & =\operatorname{det}\left(\left(\lambda I-H_{n-1}\right)\left(\lambda I+H_{n-1}\right)-\left(-H_{n-1}\right)\left(-H_{n-1}\right)\right) \\
& =\operatorname{det}\left(\lambda^{2} I-2 H_{n-1}^{2}\right)
\end{aligned}
$$

We know that, if $\mu$ is an eigenvalue of $H_{n-1}$, then $\lambda=\sqrt{2} \mu$ is the eigenvalue of $\sqrt{2} H_{n-1}$.
Thus, each eigenvalue of $H_{n-1}$ gives rise to two eigenvalues of $H_{n}$.

By induction hypothesis, $\mu= \pm 2^{\frac{n-1}{2}}$ which implies that $\lambda= \pm \sqrt{2}\left(2^{\frac{n-1}{2}}\right)= \pm 2^{\frac{n}{2}}$ are the eigenvalues of $H_{n}$.
Also since the multiplicity of $\mu$ is $2^{n-2}$, the multiplicity of $\lambda$ is $2^{n-1}$.
6) If $H$ is an $n$-square Hadamard matrix, then $\frac{H}{\sqrt{n}}$ is orthogonal [7].

Proof. Since $H$ is an $n-$ square Hadamard matrix,

$$
H H^{T}=n I_{n}
$$

That is,

$$
\left(\frac{H}{\sqrt{n}}\right)\left(\frac{H}{\sqrt{n}}\right)^{T}=I_{n}
$$

which implies that $\frac{H}{\sqrt{n}}$ is orthogonal.
7) For an $n-$ square Hadamard matrix $H,\|H x\|=\sqrt{n}\|x\|$ [7].

Proof. Consider,

$$
\begin{aligned}
\|H x\|^{2} & =<H x, H x> \\
& =<x, H^{T} H x> \\
& =<x, n I_{n} x> \\
& =n<x, x> \\
& =n\|x\|^{2} .
\end{aligned}
$$

Hence, $\|H x\|=\sqrt{n}\|x\|$.
8) All eigenvalues of an $n$-square Hadamard matrix $H$ have absolute value $\sqrt{n}$ [7].

Proof. Let $\lambda$ be an eigenvalue of $H$, that is there exist a non-zero vector $x$ such that $H x=\lambda x$. From the above property

$$
\begin{aligned}
\|H x\|^{2} & =n\|x\|^{2} \\
<H x, H x> & =n<x, x> \\
<\lambda x, \lambda x> & =n<x, x> \\
|\lambda|^{2}\|x\|^{2} & =n\|x\|^{2}
\end{aligned}
$$

That is, $|\lambda|=\sqrt{n}$.
9) $\operatorname{det}(H)= \pm(n)^{\frac{n}{2}}$ where $H$ is an $n-$ square Hadamard matrix [7].

Proof. Since $H$ is Hadamard $H H^{T}=n I_{n}$, which implies that

$$
\begin{aligned}
\operatorname{det}\left(H H^{T}\right) & =\operatorname{det}\left(n I_{n}\right) \\
\operatorname{det}\left(H H^{T}\right) & =n^{n} \operatorname{det}\left(I_{n}\right) \\
{[\operatorname{det}(H)]^{2} } & =(n)^{n} \\
\operatorname{det}(H) & = \pm(n)^{\frac{n}{2}}
\end{aligned}
$$

10) $H_{1}$ and $H_{2}$ are Hadamard matrices, then the tensor product $H_{1} \otimes H_{2}$ is also Hadamard [6].

Proof. Let $H_{1}$ be an $n-$ square Hadamard matrix and $H_{2}$ be an $m-s q u a r e$ Hadamard matrix.
Then,
$H_{1} H_{1}^{T}=n I_{n}$ and $H_{2} H_{2}^{T}=m I_{m}$.
Consider,

$$
\begin{aligned}
\left(H_{1} \otimes H_{2}\right)\left(H_{1} \otimes H_{2}\right)^{T} & =\left(H_{1} H_{1}^{T}\right) \otimes\left(H_{2} H_{2}^{T}\right) \\
& =\left(n I_{n}\right) \otimes\left(m I_{m}\right) \\
& =(m n) I_{m n}
\end{aligned}
$$

Since $H_{1}$ and $H_{2}$ are Hadamard, entries of $H_{1}$ and $H_{2}$ are +1 and -1 and hence entries of $H_{1} \otimes H_{2}$ are +1 and -1 .
That is, $H_{1} \otimes H_{2}$ is an $m n-$ square matrix with non-zero integer entries, such that $\left(H_{1} \otimes H_{2}\right)\left(H_{1} \otimes H_{2}\right)^{T}=$ $(m n) I_{m n}$.
Hence, $H_{1} \otimes H_{2}$ is Hadamard.

## III. Hadamard Code

Data transmission is the transfer of data over a point-to-point or point-to-multipoint communication channel. Data sequences to be transmitted over a digital communication channel are first modulated, the information symbols are mapped onto signals, which can be transmitted efficiently.
However these signals may be affected by noise during transmission. Error detection and correction are techniques that enable reliable delivery of digital data over unreliable communication channels.
Error detection techniques allow detecting such errors, while error correction enables reconstruction of the original data.
The Hadamard code is an error-correcting code named after French mathematician Jacques Hadamard, that is used for error detection and correction when transmitting messages over very noisy or unreliable channels.
In 1971, the code was used to transmit photos of Mars back to Earth, from the NASA space probe Mariner 9.
A. Definitions [9]

1) Linear Code: A linear code $C$ is a code in $F_{q}^{n}$ such that $a x+b y \in C$ for all $a$ and $b$ in $F_{q}$, whenever $x$ and $y$ are in $C$, where $F_{q}$ is a finite field of order $q$.
Thus a linear code $C$ is a $k$-dimensional subspace of $F_{q}^{n}$ for some integer $k$ with $1 \leq k \leq n$. (A linear code is binary if $q=2$ )
2) Codeword: The vectors in $C$ are called codewords. Thus a linear code $C$ of dimension $k$ is the set of all linear combinations of $k$ linearly independent codewords called basis vectors.
3) Weight of a Codeword: Weight of a codeword $x \in C$ is the number of non zero elements in $x$.
4) Distance of a Linear Code: Distance of a linear code $C \in F_{q}^{n}$ is the minimum weight of the non zero codeword.
5) Hamming Distance: Hamming distance between two codewords of same length is the number of elements in which they differ.

A linear code $C$ of length $n$, dimension $k$ and hamming distance $d$ is called an $[n, k, d]$ code.
6) Hadamard Code: A Hadamard code is a linear code which maps a message of length $k$ to a codeword of length of $2^{k}$, with a hamming distance of $2^{k-1}$. It is an error correcting [ $\left.2^{k}, k, 2^{k-1}\right]$ code.

## IV. Hadamard code using Hadamard Matrix

## A. Sylvester - Hadamard Matrix [8]

James Joseph Sylvester, an English mathematician constructed Hadamard matrices of order $2^{k}$ where $k$ is a positive integer, such that $2 \leq k$, using tensor product as

$$
H_{2^{k}}=H_{2} \otimes H_{2^{k-1}}=\left(\begin{array}{cc}
H_{2^{k-1}} & H_{2^{k-1}}  \tag{4}\\
H_{2^{k-1}} & -H_{2^{k-1}}
\end{array}\right)
$$

called Sylvester-Hadamard matrix.

## B. Construction of Hadamard code using Sylvester Hadamard Matrix

Consider a Sylvester-Hadamard matrix $H_{2^{k}}$ of order $2^{k}$ with $2 \leq k \in \mathbb{N}$ as in (4).
By the mapping $t \rightarrow \frac{1-t}{2}, 1$ is mapped to 0 and -1 is mapped to 1 . Then, the rows of $H_{2^{k}}$ and $-H_{2^{k}}$ gives $2^{k+1}$ codewords of length $2^{k}$.
Since the rows of Hadamard matrix are orthogonal, two distinct rows of $H_{2^{k}}$ will differ in exactly $\frac{2^{k}}{2}$ positions, thus giving the hamming distance between two codewords as $\frac{2^{k}}{2}$. The binary code so formed is called the Hadamard Code.

For example, we consider a Sylvester-Hadamard matrix $H_{4}$.

$$
H_{4}=H_{2} \otimes H_{2}=\left(\begin{array}{rr}
H_{2} & H_{2} \\
H_{2} & -H_{2}
\end{array}\right)=\left(\begin{array}{rrrr}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{array}\right)
$$

By mapping 1 to 0 and -1 to 1 we have

$$
H_{4}=\left(\begin{array}{llll}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0
\end{array}\right)
$$

and

$$
-H_{4}=\left(\begin{array}{llll}
1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1
\end{array}\right)
$$

Then the $[4,2,2]$ Hadamard Code is given by the rows of $H_{4}$ and $-H_{4}$ as $C_{4}=\{0000,0101,0011,0110,1111,1010,1100,1001\}$

## V. Hadamard 2-Designs

Combinatorial design theory is the part of combinatorial mathematics that deals with the existence, construction and properties of systems of finite sets whose arrangements satisfy generalized concepts of balance or symmetry. Modern applications of combinatorial design theory are found in a wide range of areas including finite geometry, tournament scheduling, lotteries, mathematical biology, algorithm design and analysis, networking, group testing and cryptography.
One of the earliest application of combinatorial design is found in India in the book Brhat Samhita by Varahamihira, written around 587 AD , for the purpose of making perfumes using 4 substances selected from 16 different substances using a magic square.

## A. Definitions [5]

1) 2-Designs: Let $S=\{1,2, \ldots, n\}$ be a set of $n$ elements. A collection $\mathscr{D}$ of distinct subsets of $S$ is called $(n, k, \lambda) 2-$ design if
a) $2 \leq k<n$
b) $\lambda>0$
c) each set in $\mathscr{D}$ contains exactly $k$ elements
d) each 2 - element subset of $S$ is contained in exactly $\lambda$ of the sets in $\mathscr{D}$.

The sets of $\mathscr{D}$ are called blocks, and the set $S$ is called the base set.
For example:
Let $n=7$ and $S=\{1,2,3,4,5,6,7\}$.
Then the sets $\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}$ forms a $(7,3,1) 2-$ design.
2) Incidence Matrix of a 2- Design: Let $\mathscr{D}$ be a $(n, k, \lambda) 2-$ design and $m$ be the number of blocks in $\mathscr{D}$. Then the $m \times n$ matrix $A=\left(a_{i j}\right)$ such that

$$
a_{i j}= \begin{cases}1, & \text { if } i^{t h} \text { block contains } j \\ 0, & \text { otherwise }\end{cases}
$$

is called an incidence matrix of the $2-$ design.
For example:
Let $n=7$ and $S=\{1,2,3,4,5,6,7\}$.
Consider the $(7,3,1) 2$ - design as $\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}$.
Then the incidence matrix is given as

$$
A=\left(\begin{array}{lllllll}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1
\end{array}\right)
$$

3) Hadamard 2- Design: A $(4 n-1,2 n-1, n-1) 2-$ design is called a Hadamard $2-$ design of order $n$. For example:
Let $n=7$ and $S=\{1,2,3,4,5,6,7\}$.
Then the sets $\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}$ forms a $(7,3,1)$ Hadamard $2-$ design of order 2 .

## VI. Hadamard 2- Design using Hadamard Matrix

Theorem VI.1. If $n \geq 2$, then there exists a Hadamard matrix of order $4 n$ if and only of there exists a Hadamard $2-$ design of order $n$.

Proof. We first assume that there exists a Hadamard matrix $H$ of order $4 n$.
Arrange the rows and columns of $H$ such that, the first row and column contains only +1 .
Let $A$ be a matrix obtained by removing the first column and first row of $H$. Then the order of $A$ is $(4 n-1) \times(4 n-1)$.
Since $H$ is Hadamard, the rows (or columns) of $H$ are orthogonal, and hence each row (or column) of $H$ except the first row (or column) will have exactly $2 n(+1)^{\prime} s$ and $2 n(-1)^{\prime} s$.
Thus, each row (or column) of $A$ will have exactly $2 n-1(+1)^{\prime} s$ and $2 n(-1)^{\prime} s$.
Construct a matrix $B$ as

$$
B=\frac{1}{2}(A+J)
$$

where J is a $(4 n-1) \times(4 n-1)$ matrix with all entries 1 . That is, $B$ is a $(4 n-1) \times(4 n-1)$ matrix obtained from $A$ by replacing -1 by 0 .

Now, since $H$ is Hadamard, any two columns of $H$ (excluding the first column) will have $1^{\prime} s$ at same place at $\frac{4 n}{4}=n$ positions and hence any two columns of $B$ will have $1^{\prime} s$ at same place at $n-1$ positions.
Hence, considering $B$ as an incidence matrix, this $n-1$ positions denote the number of sets of $\mathscr{D}$ in which the 2 - element subset is contained.
Hence a $(4 n-1,2 n-1, n-1) 2$ - design can be constructed using Hadamard matrix.
That is every Hadamard matrix of order $4 n$ gives a Hadamard $2-$ design of order $n$.
Conversely, assume that there exist a Hadamard $2-$ design of order $n$, that is a $(4 n-1,2 n-1, n-1) 2-$ design. Let $A$ be its $(4 n-1) \times(4 n-1)$ incidence matrix.
We construct a matrix $H$ from $A$ by replacing the $0^{\prime} s$ in $A$ by -1 and adding a row and a column of $1^{\prime} s$.
Thus, we get a $4 n \times 4 n$ matrix $H$ with entries +1 and -1 .
From the definition of $2-$ design, we know that $(4 n-1,2 n-1, n-1) 2$ - design implies that each 2 element set is contained in exactly $n-1$ of the sets of $\mathscr{D}$. Hence, the incidence matrix $A$ has 1 in both $i^{\text {th }}$ and $j^{\text {th }}$ column at exactly $n-1$ positions for every $1 \leq i \leq 4 n-1$ and $1 \leq j \leq 4 n-1$.
Thus $H$ has 1 in both $i^{t h}$ and $j^{t h}$ column at exactly $n-1+1=n$ positions and -1 in both $i^{t h}$ and $j^{t h}$ column at exactly $n$ positions, for every $1 \leq i \leq 4 n$ and $1 \leq j \leq 4 n$.
Now, since the number of $1^{\prime} s$ in each column of $A$ in $2 n-1$, the number of $1^{\prime} s$ in each column of $H$ will be $2 n-1+1=2 n$.
Hence at $n$ positions the $i^{t h}$ and the $j^{t h}$ column of $H$ will have +1 and -1 respectively, and at $n$ positions the $i^{t h}$ and the $j^{\text {th }}$ column of $H$ will have -1 and +1 respectively
By taking the inner product of $i^{t h}$ column and $j^{t h}$ column of $H$ we have $n+(-n)+(-n)+n=0$, for every $1 \leq i \leq 4 n$ and $1 \leq j \leq 4 n$. That is, $H$ is a $4 n \times 4 n$ matrix with entries +1 and -1 such that the columns of $H$ is orthogonal which implies that $H$ is Hadamard.
Hence, there exists a Hadamard matrix of order $4 n$ corresponding to a Hadamard $2-$ design of order $n$.

Now we construct a Hadamard 2 - design using a Hadamard matrix.
Let

$$
H=\left(\begin{array}{rrrrrrrr}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & 1
\end{array}\right)
$$

be a Hadamard matrix of order 8 .
We construct a $7 \times 7$ matrix $B$ as discussed in the above theorem.
That is

$$
B=\left(\begin{array}{lllllll}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1
\end{array}\right)
$$

Taking $B$ to be the incidence matrix of the $2-$ design, we get the $(7,3,1) 2-$ design as $\{1,2,4\},\{2,3,5\},\{3,4,6\}$, $\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}$ called Hadamard $2-$ design of order $\frac{8}{4}=2$

## VII. Conclusions

In this paper we studied Hadamard matrix and its properties. It is observed that inverse and transpose of Hadamard matrices are closely related.
Determinant and eigenvalues of Hadamard matrices are discussed and it is concluded that absolute value of determinant and eigenvalues of an $n-$ square Hadamard matrix is $n^{\frac{n}{2}}$ and $\sqrt{n}$ respectively. Closure property of Hadamard matrices under tensor product is discussed.
The application of Hadamard matrix in the branch of Coding Theory and Combinatorial Design Theory is included. Further the construction of Hadamard Codes using Sylvester- Hadamard matrix is discussed.
Also it is concluded that for any Hadamard matrix of order $4 n$ with $n \geq 2$, there exists a Hadamard $2-$ design of order $n$ and vice versa and hence the construction of Hadamard $2-$ design using Hadamard matrix is included.

## References

[1] S. Kumaresan. Linear Algebra: A Geometric Approach. Prentice-Hall of India Pvt.Ltd, India.
[2] Fuzhen Zhang. Matrix Theory Basic Results and Techniques. USA:Springer International Edition,1999.
[3] F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes. North Holland Publishing Company, New York.
[4] K. J. Horadam. Hadamard Matrices and their Applications. Princeton University Press, Princeton.
[5] Ian Anderson; Iiro Honkala. A Short Course in Combinatorial Designs. Internet Edition, Spring 1997, Revised 2012.
[6] Hadamard Matrices, http://www.sfu.ca/ $\sim$ mdevos/notes/comb_struct/hadamard.pdf
[7] Hadamard Matrices, http://people.cs.uchicago.edu/~laci/reu02
[8] Hadamard Codes, http://www.mcs.csueastbay.edu/~malek/TeX/Hadamard.pdf
[9] Linear Codes, http://www.math.ualberta.ca/~hongchen/m422/Chap3.pdf

