Hadamard Matrices

[Handwritten Study Material]

[Part of Advance Discrete Mathematics & Orthogonal Arrays]

P. Kalika
PhD (NET(JRF), GATE, SET)
Email: maths.whisperer@gmail.com

No. of Pages: 18

Download NET/GATE/SET Study Materials & Solutions at https://pkalika.in/
Telegram: https://t.me/pkalika_mathematics **FB Page:** https://www.facebook.com/groups/pkalika/

P Kalika
A Site for Learning Mathematics

(Your Feedbacks/Comments at maths.whisperer@gmail.com)

Hadamard Matrices

- A hadamard matrices is an $n \times n$ - matrix H with entries ± 1, which satisfies $HH^T = nI$.

OR i.e A square matrix with elts ± 1 & size n, whose distinct row-vectors are orthogonal is an Hadamard matrix of order n.

The smallest examples are —

$[1]$ OR $[+]$, $\begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}$ OR $\begin{bmatrix} + & + \\ + & - \end{bmatrix}$; $\left[\begin{array}{cc|cc} - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \\ \hline 1 & 1 & - & 1 \\ 1 & 1 & 1 & - \end{array}\right]$ (- is written for -1)

* If H is an Hadamard matrix then —

$\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$ is also an Hadamard matrix.

Lemma (1) There is an Hadamard matrix of order 2^t for all positive integer t. (Sylvester)

NB. We call matrices of order 2^t constructed by Sylvster's Construction (sylvester-Hadamard matrices)

- Using sylvester's method, first few Hadamard matrices are —

$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}_{2\times 2}$ $\downarrow$ 0, 1

$\left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right]_{4\times 4} = H_1$,

$\left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right]_{8\times 8}$

P Kalika Notes

For these matrices, we count, row by row, the no. of times the sign changes ($+1 \to -1$ or -1 to $+1$)

	row-1st	2nd
For the matrix of order 2 =	0,	1
For the matrix of order 4 =	0, 3,	1, 2
For the matrix of order 8 =	0, 7,	3, 4, 1, 6, 2, 5

Indeed, Here we observe that, the set of no. of sign changes in a Sylvester-Hadamard matrix of order n is— $\{0, 1, 2, \ldots n-1\}$.

Lemma(2) Let H be an Hadamard matrix of order n.

Then— (i). $HH^T = nI_n$

(ii). $|\det H| = n^{n/2}$

(iii). $HH^T = H^TH$.

(iv) H may be changed into other H' by permuting rows & cols OR multiplying row & cols by -1.

(These matrics are called H-equivalent matrices).

(v). Order of H-matrix is 1, 2 or $4n$, $n \in \mathbb{N}$.

Result: (3) If H is a Hadamard matrix of order n, then $n = 1, 2$ or $n \equiv 0 \pmod 4$ ie $4n$.

OR If is a Hadamard matrix of order n, when $4 \mid n$.

Tensor Product (Kronecker Product)

Let $A = \{a_{ij}\}_{m \times n}$ & B, then $A \otimes B =$

$$\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & & & \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

Pkaika Notes

Note: If A, B have the same dimensions & C, D have the same dimensions, then —

(a) $(A \otimes C)(B \otimes D) = (AB) \otimes (CD)$ ✓

(b) $(A \otimes C)^T = A^T \otimes C^T$ ✓

Observation (4): If H_1, H_2 are Hadamard matrices, then $H_1 \otimes H_2$ is a Hadamard matrix.

↳ [Kronecker / "tensor Product]

* **Def^n:** If $M = (m_{ij})_{m \times p}$ & $N = (n_{ij})_{n \times q}$ then the Kronecker Product $M \times N$ is $(mn \times pq)$ is given by —

$$M \times N = \begin{bmatrix} m_{11}N & m_{21}N & \cdots & m_{1p}N \\ m_{12}N & m_{22}N & \cdots & m_{2p}N \\ \vdots & & & \\ m_{m1}N & m_{m2}N & \cdots & m_{mp}N \end{bmatrix}_{mn \times pq}$$

Example

$$M = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad N = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \text{ then}$$

$$M \times N = \begin{bmatrix} N & N \\ N & -N \end{bmatrix}$$

$$M \times N = \left[\begin{array}{cccc:cccc} -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ \hdashline -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \end{array}\right]$$

P Kalika Notes

Conference Matrix :

A matrix $A_{n\times n}$ with all diagonal entries 0 & other entries ± 1 & $AA^T = (n-1)I$ is called a Conference matrix.

Lemma (5) Let C be a Conference matrix then—

(i). If C = Antisymmetric (Skew-symmetric), then $I+C$ is a Hadamard matrix.

(ii). If C = symmetric, then $\begin{bmatrix} I+C & -I+C \\ -I+C & -I-C \end{bmatrix}$ is a Hadamard matrix.

Result (4) H_m & H_n are Hadamard matrices of order m & n then Kronecker product is also Hadamard matrix.

Soln (i.e The direct product of two Hadamard matrix is also a Hadamard matrix)

Let $H_{m\times m}$ & $G_{n\times n}$ be two Hadamard matrix.

∴ we know that, if H_n is Hadamard matrix then it satisfies $HH^T = nI_n$

Now

$$\therefore (H_m \otimes G_n)(H_m \otimes G_n)^T$$

$$= (H_m \otimes G_n)(H_m^T \otimes G_n^T)$$

$$= H_m H_m^T \otimes G_n G_n^T$$

$$= mI_m \otimes nI_n = mn\, I_m \times I_n$$

$$= mn\, I_{mn}$$

P Kalika Notes

$\Rightarrow (H_m \otimes G_n)(H_m \otimes G_n)^T = mn\, I_{mn}$

$\Rightarrow H_m \otimes G_n$ is Hadamard matrix. Proved

Que

If $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is Hadamard matrix then $H' = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}$ is again a Hadamard matrix.

P Kalika Notes

SHIPRA 28/11/18

(5) Normalised Hadamard matrix:—

A Hadamard matrix H is known as normalised Hadamard matrix if its first row & first column contain only 1.

(6) Properties of Kronecker Product

(a) $A \otimes B \cong B \otimes A$ with proper permutation of rows & columns.

Pf: Here we do it by taking 2×2 matrix

Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$

then

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{bmatrix} = \begin{bmatrix} a_{11}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{bmatrix}$$

$$= \left[\begin{array}{cc|cc} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ \hline a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{array}\right]$$

$C_2 \leftrightarrow C_3$, then $R_2 \leftrightarrow R_3$

$$\left[\begin{array}{cc|cc} a_{11}b_{11} & a_{12}b_{11} & a_{11}b_{12} & a_{12}b_{12} \\ a_{21}b_{11} & a_{22}b_{11} & a_{21}b_{12} & a_{22}b_{22} \\ \hline a_{11}b_{21} & a_{12}b_{21} & a_{11}b_{22} & a_{12}b_{22} \\ a_{21}b_{21} & a_{22}b_{21} & a_{21}b_{22} & a_{22}b_{22} \end{array}\right] = 2 \begin{bmatrix} b_{11}\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} & b_{12}\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \\ b_{21}\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} & b_{22}\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} b_{11}A & b_{12}A \\ b_{21}A & b_{22}A \end{bmatrix} = B \otimes A$$

$\Rightarrow A \otimes B = B \otimes A$ Proved

(6) Properties of Kronecker Product

(a) $A \otimes B \cong B \otimes A$ (Proved earlier)

(b) $A \otimes (B \otimes C) = (A \otimes B) \otimes C$

(c) $a(A \otimes B) = aA \otimes B = A \otimes aB$

(d) $(A_1 + A_2) \otimes B = A_1 \otimes B + A_2 \otimes B$

(e) $A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2$

(f) $(A \otimes B)(C \otimes D) = AC \otimes BD$ if $O(A) = O(C)$, $O(B) = O(D)$

(g) $(A \otimes B)^T = A^T \otimes B^T$

Theorem 4 (Already done) If H a Hadamard matrix of order m & n then their Kronecker product (direct product) is also a Hadamard matrix of order mn.

(7) Quadratic Residue

(eg. $Z_7 = \{0, 1, 2, 3, 4, 5, 6, 7\}$
1, 2, 4 → quadratic Residue
3, 5, 6 → Quadratic non-Residue.)

Let $Z_p = \{0, 1, \ldots p-1\}$

take $p = 7$

$1^2 = 1$
$2^2 = 4 \bmod p$
$3^2 = 9 \bmod p$

then $1, 4 \pmod p$, $9 \pmod p$ — are quadratic Residue.

P Kalika Notes

(182)

a Rest elt (except than 1, 4(mod p), 9(mod p)...) an quadratic non-Residue.

Example: (a) Let $Z_9 = \{0, 1, 2, \ldots 8\}$

$1^2 = 1$	$5^2 = 7$
$2^2 = 4$	$6^2 = 1$
$3^2 = 0$	$7^2 = 4$
$4^2 = 7$	$8^2 = 1$

So In Z_9, 1, 4, 7 are Quad. Res.
2, 3, 5, 6 are Quad non. Res.

(b) If p = prime then Z_p = field
then # Quad. Residue = # Quad non. Residue

Extended Quadratic ~~Residue~~ Character :—

(8) Let $\chi(a)$ be a map from F to set $\{-1, 0, 1\}$ defined as

$$\chi(a) = \begin{cases} 1 & : \text{if } a = \text{quadratic residue} \\ 0 & : a = 0 \\ -1 & : a = \text{quadratic non-residue.} \end{cases}$$

(9) Paley Construction – I [For construction of Hadamard matrix of order 4n]

($q = N-1$)

Let $q = p^r$, where p is prime, of the form $4k+3$

Then ∃ a Hadamard matrix of order $4n = N$, ($q = N-1$)

Let $[Q]_q$ where q is a prime, be a conference matrix of order q. Then

$$H = \begin{bmatrix} 1 & e \\ e^T & Q_q - I \end{bmatrix}_{(q+1)\times(q+1)} \text{ is a Hadamard matrix.}$$

$= N \times N$

where $e = [1, 1, 1 \ldots 1]_{1\times q}$

↓

string of 1

P Kalika Notes

Que(10) : Construct a Hadamard matrix of order 8 (181)

$N = 8, \Rightarrow q = N-1 = 7$

Consider in $Z_7 : \{0,1,2,3,4,5,6\}$

Here 1, 2, 4 → Quadratic Residue
3, 5, 6 → Quadratic non Residue

Then Conference matrix $[Q]_7$ is —

$$Q_7 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{bmatrix} x(0-0) & x(1-0) & x(2-0) & x(3-0) & x(4-0) & x(5-0) & x(6-0) \\ x(0-1) & x(1-1) & x(2-1) & x(3-1) & x(4-1) & x(5-1) & x(6-1) \\ x(0-2) & x(1-2) & x(2-2) & x(3-2) & x(4-2) & x(5-2) & x(6-2) \\ \vdots & & & & & & \vdots \\ \vdots & & & & & & \vdots \\ \vdots & & & & & & \vdots \\ x(0-6) & x(1-6) & \cdots & \cdots & \cdots & \cdots & x(6-6) \end{bmatrix} \end{array} \quad 7 \times 7$$

$$= \begin{bmatrix} x(0) & x(1) & x(2) & x(3) & x(4) & x(5) & x(6) \\ x(-1) & x(0) & x(1) & x(2) & x(3) & x(4) & x(5) \\ x(-2) & x(-1) & x(0) & x(1) & x(2) & x(3) & x(4) \\ x(-3) & x(-2) & x(-1) & x(0) & x(1) & x(2) & x(3) \\ x(-4) & x(-3) & x(-2) & x(-1) & x(0) & x(1) & x(2) \\ x(-5) & x(-4) & x(-3) & x(-2) & x(-1) & x(0) & x(1) \\ x(-6) & x(-5) & x(-4) & x(-3) & x(-2) & x(-1) & x(0) \end{bmatrix}$$

In Z_7, $-1 = 6$, $-2 = 5$, $-3 = 4$, $-4 = +3$, $-5 = 2$, $-6 = 1$

$$Q_7 = \begin{bmatrix} x(0) & x(1) & x(2) & x(3) & x(4) & x(5) & x(6) \\ x(6) & x(0) & x(1) & x(2) & x(3) & x(4) & x(5) \\ x(5) & x(6) & x(0) & x(1) & x(2) & x(3) & x(4) \\ x(4) & x(5) & x(6) & x(0) & x(1) & x(2) & x(3) \\ x(3) & x(4) & x(5) & x(6) & x(0) & x(1) & x(2) \\ x(2) & x(3) & x(4) & x(5) & x(6) & x(0) & x(1) \\ x(1) & x(2) & x(3) & x(4) & x(5) & x(6) & x(0) \end{bmatrix}$$

& $x(0) = 0$

P Kalika Notes

(120)

Now Replace $\chi(0)=0$, $\chi(3,5,6)=-1$, & $\chi(1,2,4)=1$

$$Q_2 = \begin{bmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{bmatrix}_{7\times 7}$$

$\Rightarrow Q-I$ = diagonal entry in Q becomes -1

$\therefore$ Hadamard matrix H is, $H = \begin{bmatrix} 1 & e \\ e^T & Q-I \end{bmatrix}_{8\times 8}$

$$H_8 = \left[\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & +1 & -1 & +1 & -1 & -1 & -1 \end{array}\right]_{8\times 8}$$

$e = [1, 1, \ldots]_{1\times q}$

← Required Hadamard matrix of order 8.

Now, using similar method, Construct H_4 ($N=4$)

(a)

$q = N-1 = 3$

Consider $Z_3 = \{0, 1, 2\}$

1 → Quadratic residue
2 → Quadratic non-residue

So, Q_3 is constructed as

$$Q_3 = \begin{matrix} \\ 0 \\ 1 \\ 2 \end{matrix}\begin{matrix} \begin{matrix} 0 & 1 & 2 \end{matrix} \\ \begin{bmatrix} \chi(0) & \chi(1) & \chi(2) \\ \chi(-1) & \chi(0) & \chi(1) \\ \chi(-2) & \chi(-1) & \chi(0) \end{bmatrix} \end{matrix}$$

$\therefore$ in Z_3; $-1 = 2$ & $-2 = 1$

$$\therefore Q_3 = \begin{bmatrix} \chi(0) & \chi(1) & \chi(2) \\ \chi(2) & \chi(0) & \chi(1) \\ \chi(1) & \chi(2) & \chi(0) \end{bmatrix}_{3\times 3} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix}$$

Now, we have to construct $H_4 = \begin{bmatrix} 1 & e \\ e^T & Q_3 \end{bmatrix}$

P Kalika Notes

(179)

[10] Paley Construction - II

Let $q = p^r$, where p is a prime & q is of the form $4k+1$.

Then we construct $Q_{q\times q}$ (a conference matrix)

as $S_n = \begin{bmatrix} 0 & e \\ e^T & Q \end{bmatrix}_{(q+1)\times(q+1)} \Rightarrow \frac{N}{2} \times \frac{N}{2}$

Then Hadamard matrix H is constructed as

$$H = \begin{bmatrix} S_n + I_n & S_n - I_n \\ S_n - I_n & -S_n - I_n \end{bmatrix}_{2n\times 2n \text{ or } 2(q+1)\times 2(q+1)}$$

$N = 2(q+1)$
$\Rightarrow q = \frac{N}{2} - 1$

How to choose q

Suppose given N, then take $q = \frac{N}{2} - 1 \equiv 4k+1$

Que 11 Construct a Hadamard matrix of order 12 (i.e $n=12$) (exam)

$(\because q = \frac{12}{2} - 1 = 5 \equiv 4\times 1 + 1$ type)

Consider $Z_5 = \{0, 1, 2, 3, 4\}$

$1^2 = 1$
$2^2 = 4$
$3^2 = 4$
$4^2 = 1$

1, 4 → Quad. Resi
2, 3 → Quad non-Resi

$$\therefore Q_5 = \begin{bmatrix} x(0) & x(1) & x(2) & x(3) & x(4) \\ x(4) & x(0) & x(1) & x(2) & x(3) \\ x(3) & x(4) & x(0) & x(1) & x(2) \\ x(2) & x(3) & x(4) & x(0) & x(1) \\ x(1) & x(2) & x(3) & x(4) & x(0) \end{bmatrix}_{5\times 5} = \begin{bmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \end{bmatrix}$$

Then $S_6 = \begin{bmatrix} 0 & e \\ e^T & Q_5 \end{bmatrix}$, $e = [1, 1, 1, -1, 1]_{1\times 5}$

P Kalika Notes

(178)

$$\therefore S_6 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{bmatrix}_{6\times 6}$$

$$\therefore H_{12} = \begin{bmatrix} S_6+I_6 & S_6-I_6 \\ S_6-I_6 & -S_6-I_6 \end{bmatrix} = \left[\begin{array}{cccccc:cccccc} 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ \hdashline -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 \end{array}\right]$$

Que (12) Check for $n=20$ order that which construction is applicable.

Sol^n $\because n-1 = 19 = 4k+3 = 4\times 4+3$ (Prime → I)

So, we may apply Paley construction – I, for H.

Next $\because q = \frac{n}{2}-1 = \frac{20}{2}-1 = 9$ ($= 4k+1 = 4\times 2+1$ ←*)

Here 9 is not prime but $9 = 3^2 =$ prime^2.

So, Paley construction – II is applicable.

P Kalika Notes

(172)

Theorem (13): Prove that

$$\sum \chi(b)\cdot\chi(b+c) = -1 \quad \text{if } c\neq 0 \ \& \ b,c\in F$$

Pf: Since we have $\chi(0)=0$ ✓

so $\chi(0)\cdot\chi(0+c)=0 \quad \forall c$ (if $b=0$)

So, For $b\neq 0$, there is a unique $z\neq 1$ s.t $b+c=bz$

As b runs over the non-zero elt. of F (field), z runs over all element of F except 1.

Hence

$$\sum_b \chi(b)\chi(b+c) = \sum_{b\neq 0}\chi(b)\cdot\chi(b+c) + \underbrace{\sum_{b=0}\chi(b)\cdot\chi(b+c)}_{=0}$$

$$\Rightarrow = \sum_{b\neq 0}\chi(b)\chi(b+c)$$

$$= \sum_{b\neq 0}\chi(b)\cdot\chi(bz)$$

Since $\chi(a)$ is a multiplicative function, so,

$$\sum_b \chi(b)\cdot\chi(b+c) = \sum_{b\neq 0}\chi(b)\cdot\chi(b)\chi(z)$$

$$= \sum_{b\neq 0}(\chi(b))^2\cdot\chi(z)$$

Here either $\chi(b)=1$ or $\chi(b)=-1$.

$$= \sum_{b\neq 0,\, z\neq 1}\chi(z)$$

$$= \sum_z \chi(z) - \chi(1)$$

$$= -1$$

Since in field, no. of quadratic Residue = no. of non-quadratic Residue

(176)

quadratic Residue

$= 0 - 1$

$= -1 \qquad \left(\because \chi\left(\frac{1}{1}\right) = 1\right)$

$\Rightarrow \sum \chi(b)\chi(b+c) = -1$ Proved

Example

(14) Check which construction is applicable for which N

N		$(4k+3)$ P.C-I $(q=N-1)$	$(4k+1)$ P.C-II $(q_2=\frac{N}{2}-1)$	S.H
4	$N=4=2^2$, $q_1=3, q_2=1$	3 ✓	1 ✓	✓ $=2^4$
16	$N=16$, $q_1=15$, $q_2=7$	✗	✗	✓
12	$q_1=11$, $q_2=5$	✓	✓	✗
20	$q_1=19$, $q_2=9$	✓	✓	✗
24	$q_1=23$, $q_2=11$	✓	✗	✗
28	$q_1=27$, $q_2=13$ ($4\times6+3$, $4\times3+1$)	✓	✓	✗
32	$q_1=31$ ($4\times7+3$), $q_2=15$ ($4\times3+3$)	✓	✗	✗
36	$q_1=35$ ($4\times8+3$), $q_2=17$ ($4\times4+1$)	✗	✓	✗
40	$q_1=39$, $q_2=19$ ($4\times4+3$) (Williamsony)	✗	✗	✗
44	$q_1=43$ ($4\times10+3$), $q_2=21$	✓	✗	✗
48	$q_1=47$ ($4\times13+3$), $q_2=23$ ($4\times5+3$)	✓	✗	✗
52	$q_1=51$, $q_2=25=4\times6+1$ $=52$	✗	✓	✗
56	$q_1=55$, $q_2=27=4\times6+3$ $=32$	✗	✗	✗
92	$q_1=91$, $q_2=45$	✗	✗	✗
116	2 ✗	$\frac{116}{2}-1=58-1=57=4\times14+1=4k+1$ $\downarrow$ =not prime		

P Kalika Notes

Circulant Matrix

(175)

An $n \times n$ matrix of the form —

$$C = \begin{bmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & \cdots & c_3 & c_2 \\ c_2 & c_1 & c_0 & \cdots & & c_3 \\ \vdots & & & & & \\ c_{n-2} & \cdots & & & & c_{n-1} \\ c_{n-1} & \cdots & & & c_1 & c_0 \end{bmatrix}_{n \times n}$$

As, $C_{4\times4} = \begin{bmatrix} c_0 & c_3 & c_2 & c_1 \\ c_1 & c_0 & c_3 & c_2 \\ c_2 & c_1 & c_0 & c_3 \\ c_3 & c_2 & c_1 & c_0 \end{bmatrix}$ OR $\begin{bmatrix} c_0 & c_1 & c_2 & c_3 \\ c_3 & c_0 & c_1 & c_2 \\ c_2 & c_3 & c_0 & c_1 \\ c_1 & c_2 & c_3 & c_0 \end{bmatrix}$

A circulant matrix is fully specified by one vector, which appears as the first column of C or first row of C.

Def^n: The 'circulant matrix $C = \text{circ}\{c\}$ associated to the vector $c \in \mathbb{C}^n$ is the $n \times n$ matrix whose rows (or col.) are given by iterations of the shift operator acting on c.

- This matrix is identified with its first row/col. or
- They have orthonormal Eigen vectors.
- Multiplying by a circulant matrix is equivalent to circular convolution.
- Eigen-vector of circulant matrices are always the same, while Eigen-values are different

P Kalika Notes

(174)

Que(i) Prove that the product of two circulant matrix is commutative.

Pf. Let $A_{n\times n}$ & $B_{n\times n}$ be two circulant matrix of same order.

claim: $AB = BA$ (i.e product is commutative)

let $A = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & & & & \\ a_2 & a_3 & \cdots & & a_1 \end{bmatrix}$, $B = \begin{bmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ b_n & b_1 & b_2 & \cdots & b_{n-1} \\ b_{n-1} & b_n & b_1 & \cdots & b_{n-2} \\ \vdots & & & & \\ b_2 & b_3 & b_4 & \cdots & b_1 \end{bmatrix}$

for simplicity take $n=3$

then $AB = \begin{bmatrix} a_1b_1 + a_2b_3 + a_3b_2 & a_1b_2 + a_2b_1 + a_3b_3 & a_1b_3 + a_2b_2 + a_3b_1 \\ a_3b_1 + a_1b_3 + a_2b_2 & a_3b_2 + a_1b_1 + a_2b_3 & a_3b_3 + a_1b_2 + a_2b_1 \\ a_2b_1 + a_3b_3 + a_1b_2 & a_2b_2 + a_3b_1 + a_1b_3 & a_2b_3 + a_3b_2 + a_1b_1 \end{bmatrix}$

$= \begin{bmatrix} c_1 & c_2 & c_3 \\ c_3 & c_1 & c_2 \\ c_2 & c_3 & c_1 \end{bmatrix}$

On observing, we found that AB looks like

& $BA = \begin{bmatrix} c_1 & c_2 & c_3 \\ c_3 & c_1 & c_2 \\ c_2 & c_3 & c_1 \end{bmatrix}$

[Result is true for $n=1,2,3\ldots$ so by mathematical Induction it is true for $n=n$.]

Thus, circulant matrix is commutative for $n=3$

Also [if A & B are circulant then AB & BA are also circulant matrix]

P Kalika Notes

Some Useful Links:

1. **Free Study Materials(By P Kalika) (**https://pkalika.in/2019/10/14/study-material/**)**

2. **Free Maths Study Materials(Donated) (**https://pkalika.in/2020/04/06/free-maths-study-materials/**)**

3. **MSc Entrance Exam Que. Paper: (**https://pkalika.in/2020/04/03/msc-entrance-exam-paper/**)**
   [JAM(MA), JAM(MS), BHU, CUCET, ...etc]

4. **PhD Entrance Exam Que. Paper: (**https://pkalika.in/que-papers-collection/**)**
   [CSIR-NET, GATE(MA), BHU, CUCET,IIT, NBHM, ...etc]

5. **CSIR-NET Maths Que. Paper: (**https://pkalika.in/2020/03/30/csir-net-previous-yr-papers/**)**
   [Upto 2019 Dec]

6. **Practice Que. Paper: (**https://pkalika.in/2019/02/10/practice-set-for-net-gate-set-jam/**)**
   [Topic-wise/Subject-wise]

P Kalika Notes

(Provide your Feedbacks/Comments at maths.whisperer@gmail.com)