CHAPTER IV

CONSTRUCTION OF SETS OF MUTUALLY ORTHOGONAL LATIN SQUARES FROM ORTHOGONAL ARRAYS

4.1 Characterization of Set of Mutually Orthogonal Latin Squares by Orthogonal Array

4.1.1 Definition. Let $v_1 = (x_1, \ldots, x_{n^2})$, $v_2 = (y_1, \ldots, y_{n^2})$ be any two vectors whose components x_i, y_i are taken from any sets of n objects. The two vectors v_1 and v_2 are said to be orthogonal if the ordered pairs (x_i, y_i), $i = 1, \ldots, n^2$ include all pairs (a,b) from $S \times S$.

4.1.2 Definition. An orthogonal array $OA(n,s)$ of order n and length s is a matrix with s rows and n^2 columns with entries taken from any set of n objects such that every two distinct rows are orthogonal.

Usually we shall denote the objects by $1, 2, \ldots, n$.

4.1.3 Theorem. The existence of k mutually orthogonal Latin squares of order n is equivalent to the existence of $OA(n,k+2)$.

Proof Let $L_1, \ldots, L_k$ be a set of mutually orthogonal Latin squares of order n. Let r_{ij} denote the j^{th} row of L_i, $i = 1, \ldots, k$, $j = 1, \ldots, n$. Construct a matrix A as follows :

$$A = \begin{pmatrix} \bar{1} & \bar{2} & \cdot & \cdot & \cdot & \bar{n} \\ x & x & \cdot & \cdot & \cdot & x \\ r_{11} & r_{12} & \cdot & \cdot & \cdot & r_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ r_{k1} & r_{k2} & \cdot & \cdot & \cdot & r_{kn} \end{pmatrix}$$

where $x = (1,2,\ldots, n)$, $\bar{k} = (k,k,\ldots,k)$, $k = 1,\ldots, n$, are vectors of length n. We shall show that A is an OA(n, k+2). Since A is a matrix with k+2 rows and n^2 columns. The ordered pair (i,j), $i = 1,\ldots, n$ from the first row, $j = 1,\ldots, n$ from the second represents the i^{th} row and j^{th} column of Latin square. The third row and so on are the element in the corresponding cell. Hence any two rows of A are orthogonal by the properties of orthogonal Latin squares. On the other hand if A = OA(n, k+2), we can permute columns of A so that the first and second rows are

$$\begin{matrix} 1 & 1 \ldots 1 & 2 \ldots 2 \ldots n \ldots n \\ 1 & 2 \ldots n & 1 \ldots n \ldots 1 \ldots n \end{matrix}$$

because of orthogonality of any two rows. Then reverse the process of the first part. We can get k mutually orthogonal Latin squares of order n.

Q.E.D.

4.2 Construction of Orthogonal Arrays from Smaller Orthogonal Arrays

4.2.1 Theorem. If $OA(n_1,s)$ and $OA(n_2,s)$ exist, then $OA(n_1n_2,s)$ exists.

Proof Let $A = (a_{ij})$, $B = (b_{ij})$ be $OA(n_1,s)$, $OA(n_2,s)$ respectively. Assume that the objects a_{ij}, b_{ij} are positive integers, $1 \leq a_{ij} \leq n_1$, $1 \leq b_{ij} \leq n_2$.

Form a new matrix $D = (d_{ij})$, $i = 1,\ldots, s$, $j = 1,\ldots, n_1^2 n_2^2$, by replacing a_{ij} in A by the row vector

$$(b_{i1}+ m_{ij}, b_{i2}+ m_{ij}, \ldots, b_{in_2^2}+ m_{ij}) ,$$

where $\qquad m_{ij} = (a_{ij}- 1)n_2 \qquad$ for every i, j.

As the numbers a_{ij} run from 1 to n_1 and the number b_{ij} from 1 to n_2, the numbers $b_{it}+ m_{ij}$ run from 1 to n_1n_2, hence every d_{ij} is one of the numbers $1,2,\ldots, n_1n_2$.

Consider any two rows of D, say the h^{th} row and the i^{th} row. Let u, v be any two numbers in the range $1,\ldots, n_1n_2$. Then we can write

$$u = u_1+ (u_2- 1)n_2 , \qquad v = v_1+ (v_2- 1)n_2$$

with $1 \leq u_1, v_1 \leq n_2$, $\qquad 1 \leq u_2, v_2 \leq n_1$ uniquely.

In A, let us determine j as that column in which

$$a_{hj} = u_2 , \quad a_{ij} = v_2 .$$

In B, let us determine t as that column in which

$$b_{ht} = u_1 , \quad b_{it} = v_1 .$$

Then in D, in column $g = t + n_2^2(j-1)$, we have

$$d_{hg} = b_{ht}+ (a_{hj}- 1)n_2 = u_1+ (u_2- 1)n_2 = u$$

and $\quad d_{ig} = b_{it} + (a_{ij} - 1)n_2 = v_1 + (v_2 - 1)n_2 = v.$

Hence any u, v is paired at least once in any pair of rows.

Since there are $(n_1n_2)^2$ columns and $(n_1n_2)^2$ possible pairs (u,v), hence each u, v are paired exactly once in any two rows. This shows that D is an $OA(n_1n_2,s)$

Q.E.D.

4.2.2 <u>Theorem.</u> If $N(m) \geqslant 2$, then $N(3m+1) \geqslant 2$.

<u>Proof</u> Since $N(m) \geqslant 2$, hence, by Theorem 4.1.3, $OA(m,4)$ exists. Let E be an $OA(m,4)$ with the letters $x_1, \ldots, x_m$ as objects.

Define following vectors of length m of residues modulo 2m+1, for $i = 0,1,\ldots, 2m$

$$a_i = (i, i, \ldots, i) ,$$

$$b_i = (i+1, i+2, \ldots, i+m) ,$$

$$c_i = (i-1, i-2, \ldots, i-m) .$$

Let

$$d_1 = a_i - b_i = (2m, 2m-1, \ldots, m+1),$$

$$d_1' = b_i - a_i = (1, 2, \ldots, m),$$

$$d_2 = a_i - c_i = (1, 2, \ldots, m),$$

$$d_2' = c_i - a_i = (2m, 2m-1, \ldots, m+1),$$

$$d_3 = b_i - c_i = (2, 4, \ldots, 2m),$$

$$d_3' = c_i - b_i = (2m-1, 2m-3, \ldots, 1).$$

Here d_j and d_j' for $j = 1,2,3$ together contain all nonzero residues modulo $2m+1$. Now construct three vectors of length $m(2m+1)$ as follows :

$$A = (a_0, a_1, a_2, \ldots, a_{2m}) ,$$

$$B = (b_0, b_1, b_2, \ldots, b_{2m}) ,$$

$$C = (c_0, c_1, c_2, \ldots, c_{2m}) .$$

We take the m letters $x_1, \ldots, x_m$ and form a vector X of length $m(2m+1)$:

$$X = (\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{2m})$$

where $$\bar{x}_i = (x_1, x_2, \ldots, x_m).$$

Now we form a $4 \times 4m(2m+1)$ matrix D :

$$D = \begin{bmatrix} A & B & C & X \\ B & A & X & C \\ C & X & A & B \\ X & C & B & A \end{bmatrix} .$$

Let $$F = \begin{bmatrix} G & D & E \end{bmatrix},$$

where

$$G = \begin{bmatrix} 0 & 1 & 2 \ldots & 2m \\ 0 & 1 & 2 \ldots & 2m \\ 0 & 1 & 2 \ldots & 2m \\ 0 & 1 & 2 \ldots & 2m \end{bmatrix} .$$

We claim that F is an OA(3m+1,4). We shall verify that for any objects u, v in $\{0,1,\ldots, 2m\} \cup \{x_1,\ldots, x_m\}$, the pair $\binom{u}{v}$ occurs exactly once in every two rows of F.

Since the submatrix E of F is an orthogonal array, hence each of the pairs $\binom{u}{v}$ of the form $\binom{x_i}{x_j}$ occurs in every two rows of E. Thus each of the pairs $\binom{u}{v}$ of the form $\binom{x_i}{x_j}$ occurs in every two rows of F.

Note also that each of the pairs $\binom{u}{v}$ of the form $\binom{i}{i}$ where $i = 0,1,\ldots, 2m$ occurs in every two rows of the submatrix G of F. Hence each of such pairs occurs in every two rows of F.

It remains to be shown that

(1) Each pair $\binom{u}{v}$ with u, v in $\{0,1,\ldots, 2m\}$, $u \neq v$, occurs in every two rows of F.

(2) Each pair $\binom{u}{v}$ with u in $\{0,1,\ldots, 2m\}$ and v in $\{x_1,\ldots, x_m\}$ occurs in every two rows of F.

(3) Each pair $\binom{u}{v}$ with u in $\{x_1,\ldots, x_m\}$ and v in $\{0,1,\ldots, 2m\}$ occurs in every two rows of F.

For convenience, let us call the pairs $\binom{u}{v}$ in (1),(2),(3) the pairs of types I,II,III respectively. We shall show that each of these pairs occurs in every two rows of the submatrix D. Observe that each pair of rows of D contains one of the following submatrices

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}, \quad \begin{pmatrix} A & C \\ C & A \end{pmatrix}, \quad \begin{pmatrix} B & C \\ C & B \end{pmatrix}.$$

To show that each pair $\binom{u}{v}$ of type I occurs in every two rows of D, it suffices to show that each pair $\binom{u}{v}$ of type I occurs in each of these submatrices. Since $u \neq v$, hence there exists e belonging to $\{1,2,\dots, 2m\}$ such that

$$u - v \equiv e \qquad (\text{mod } 2m+1).$$

Thus e must occur in d_1 or d_1'.

If e belongs to d_1, let $h = 2m+1-e$ and choose i from $\{0,1,2,\dots,2m\}$ such that

$$i + h \equiv v \qquad (\text{mod } 2m+1).$$

Since $\quad u - v = e = 2m+1-h,$

$$u = 2m + 1 - h + v,$$

hence $\quad u = 2m + 1 - h + i + h$

$$u = 2m + 1 + i,$$

so that $\quad u \equiv i \qquad (\text{mod } 2m+1).$

Therefore the pair $\binom{u}{v}$ occurs in the h^{th} column of the submatrix $\binom{a_i}{b_i}$. Hence $\binom{u}{v}$ occurs in $\binom{A}{B}$.

If e belongs to d_1', let $h = e$ and choose i from $\{0,1,\dots,2m\}$ such that

$$i \equiv v \qquad (\text{mod } 2m+1).$$

Since $\quad u - v = e = h,$

$$u = h + v,$$

hence $\quad u = h + i,$

so that $\quad u \equiv i + h \qquad (\text{mod } 2m+1).$

Therefore the pair $\binom{u}{v}$ occurs in the h^{th} column of the submatrix $\binom{b_i}{a_i}$. Hence $\binom{u}{v}$ occurs in $\binom{B}{A}$. Thus, each pair $\binom{u}{v}$ of type I occurs in $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$.

Similarly we can show that each pair $\binom{u}{v}$ of type I occurs in submatrix $\begin{pmatrix} A & C \\ C & A \end{pmatrix}$.

It remains to be shown that each pair $\binom{u}{v}$ of type I occurs in submatrix $\begin{pmatrix} B & C \\ C & B \end{pmatrix}$. Observe that e must occur in d_3 or d_3'.

If e belongs to d_3, let $h = \frac{e}{2}$. Clearly h belongs to $\{1,\ldots,m\}$. Choose i from $\{0,1,\ldots,2m\}$ such that

$$i - h \equiv v \qquad (\text{mod } 2m+1).$$

Since
$$u - v = e = 2h,$$
$$u = v + 2h,$$
hence
$$u = i - h + 2h,$$
$$u = i + h,$$
so that
$$u \equiv i + h \qquad (\text{mod } 2m+1).$$

Therefore the pair $\binom{u}{v}$ occurs in the h^{th} column of the submatrix $\binom{b_i}{c_i}$. Hence $\binom{u}{v}$ occurs in $\binom{B}{C}$.

If e belongs to d_3', let $h = \frac{2m+1-e}{2}$. Clearly h belongs to $\{1,\ldots, m\}$. Choose i from $\{0,1,2,\ldots, 2m\}$ such that

$$i + h \equiv v \qquad (\text{mod } 2m+1).$$

Since
$$u - v = e = 2m + 1 - 2h,$$
$$u = v + 2m + 1 - 2h,$$
hence
$$u = i + h + 2m + 1 - 2h,$$
$$u = 2m + 1 + i - h,$$
so that
$$u \equiv i - h \qquad (\text{mod } 2m+1).$$

Therefore the pair $\binom{u}{v}$ occurs in the h^{th} column of the submatrix $\binom{c_i}{b_i}$. Hence $\binom{u}{v}$ occurs in $\binom{C}{B}$. Thus each pair $\binom{u}{v}$ of type I occurs in $\begin{pmatrix} B & C \\ C & B \end{pmatrix}$.

Next, we shall show that each pair $\binom{u}{v}$ of type II occurs in every two rows of D. Observe that each pair of rows of D contains one of the following submatrices

$$\begin{pmatrix} A \\ \\ X \end{pmatrix}, \quad \begin{pmatrix} B \\ \\ X \end{pmatrix}, \quad \begin{pmatrix} C \\ \\ X \end{pmatrix}.$$

To show that each pair $\binom{u}{v}$ of type II occurs in every two rows of D, it suffices to show that each pair $\binom{u}{v}$ of type II occurs in each of these submatrices. Since v belongs to $\{x_1, \ldots, x_m\}$. Hence $v = x_h$, for some $h = 1, \ldots, m$.

Choose i from $\{0, 1, \ldots, 2m\}$ such that

$$u \equiv i \pmod{2m+1}.$$

It can be seen that the pair $\binom{u}{v}$ occurs in the h^{th} column of the submatrix $\binom{a_i}{\bar{x}_i}$. Hence $\binom{u}{v}$ occurs in $\binom{A}{X}$.

Choose i from $\{0, 1, \ldots, 2m\}$ such that

$$u \equiv i + h \pmod{2m+1}.$$

Then the pair $\binom{u}{v}$ occurs in the h^{th} column of the submatrix $\binom{b_i}{\bar{x}_i}$. Hence $\binom{u}{v}$ occurs in $\binom{B}{X}$.

Choose i from $\{0, 1, \ldots, 2m\}$ such that

$$u \equiv i - h \pmod{2m+1}.$$

Then the pair $\binom{u}{v}$ occurs in the h^{th} column of the submatrix $\binom{c_i}{\overline{x}_i}$.
Hence $\binom{u}{v}$ occurs in $\binom{C}{X}$.

Finally, we shall show that each pair $\binom{u}{v}$ of type III occurs in every two rows of D. Observe that each pair of rows of D contains one of the following submatrices

$$\begin{pmatrix} X \\ A \end{pmatrix}, \quad \begin{pmatrix} X \\ B \end{pmatrix}, \quad \begin{pmatrix} X \\ C \end{pmatrix}.$$

By similar arguments it can be shown that each pair $\binom{u}{v}$ of type III occurs in each of these submatrices.

Hence any u, v is paired at least once in any pair of rows. Since there are $2m + 1 + 4m(2m+1) + m^2 = (3m+1)^2$ columns and there are $(3m+1)^2$ possible pairs (u,v), hence each u, v are paired exactly once in any two rows of F. This shows that F is an OA(3m+1,4).

Q.E.D.

4.2.3 Corollary $N(6t+4) \geq 2$.

Proof By Remark 2.4.4, we have $N(2t+1) \geq 2$. Hence by Theorem 4.2.2

$$N(3(2t+1)+1) \geq 2$$

i.e.

$$N(6t+4) \geq 2.$$

Q.E.D.

Example. Two superimposed 10 × 10 orthogonal Latin squares obtained by Theorem 4.2.2 are shown below :

Table I

0,0	6,7	5,8	4,9	9,1	8,3	7,5	1,2	2,4	3,6
7,6	1,1	0,7	6,8	5,9	9,2	8,4	2,3	3,5	4,0
8,5	7,0	2,2	1,7	0,8	6,9	9,3	3,4	4,6	5,1
9,4	8,6	7,1	3,3	2,7	1,8	0,9	4,5	5,0	6,2
1,9	9,5	8,0	7,2	4,4	3,7	2,8	5,6	6,1	0,3
3,8	2,9	9,6	8,1	7,3	5,5	4,7	6,0	0,2	1,4
5,7	4,8	3,9	9,0	8,2	7,4	6,6	0,1	1,3	2,5
2,1	3,2	4,3	5,4	6,5	0,6	1,0	7,7	8,8	9,9
4,2	5,3	6,4	0,5	1,6	2,0	3,1	8,9	9,7	7,8
6,3	0,4	1,5	2,6	3,0	4,1	5,2	9,8	7,9	8,7