THE CONSTRUCTION OF ORTHOGONAL LATIN SQUARES[1]

By Henry B. Mann[2]

Columbia University

A Latin square is an arrangement of m variables $x_1, x_2, \cdots, x_m$ into m rows and m columns such that no row and no column contains any of the variables twice. Two Latin squares are called orthogonal if when one is superimposed upon the other every ordered pair of variables occurs once in the resulting square.

The rows of a Latin square are permutations of the row $x_1, x_2, \cdots, x_m$. Let P_i be the permutation which transforms $x_1, x_2, \cdots, x_m$ into the ith row of the Latin square. Then $P_iP_j^{-1}$ leaves no variable unchanged for $i \neq j$. For otherwise one column would contain a variable twice. On the other hand each set of m permutations $P_1, P_2, \cdots, P_m$ such that $P_iP_j^{-1}$ leaves no variable unchanged generates a Latin square. We may therefore identify every Latin square with a set of m permutations $(P_1, P_2, \cdots, P_m)$ such that $P_iP_j^{-1}$ leaves no variable unchanged.

Now let $(P_1, P_2, \cdots, P_m)$, $(Q_1, Q_2, \cdots, Q_m)$ be a pair of orthogonal Latin squares. We shall show that $(P_1^{-1}Q_1, P_2^{-1}Q_2, \cdots, P_m^{-1}Q_m)$ is a Latin square. $P_i^{-1}Q_i$ is the transformation which transforms the ith row of $(P_1, P_2, \cdots, P_m)$ into the ith row of $(Q_1, Q_2, \cdots, Q_m)$. Since every pair of variables occurs exactly once if the second square is imposed upon the first, the square $(P_1^{-1}Q_1, P_2^{-1}Q_2, \cdots, P_m^{-1}Q_m)$ contains for every i and k a permutation which transforms x_i into x_k. But then it can not contain two permutations which transform x_i into x_k. This argument can be reversed and it follows that $(P_1, P_2, \cdots, P_m)$ and $(Q_1, Q_2, \cdots, Q_m)$ are orthogonal if and only if $(P_1^{-1}Q_1, P_2^{-1}Q_2, \cdots, P_m^{-1}Q_m)$ is a Latin square.

Denote now by an m sided square S any set of m permutations $(S_1, S_2, \cdots, S_m)$ and by the product SS' of two squares S and S' the square $(S_1S_1', S_2S_1', \cdots, S_mS_m')$. Then we can state: Two Latin squares L_1 and L_2 are orthogonal if and only if there exists a Latin square L_{12} such that

$$L_1L_{12} = L_2. \tag{1}$$

Now let $L_1, L_2, \cdots, L_r$ be a set of r mutually orthogonal Latin squares. Then we must have $L_iL_{ik} = L_k$ where L_{ik} is a Latin square if $i \neq k$. Hence we have the theorem

Theorem 1: *The Latin squares $L_1, L_2, \cdots, L_r$ are orthogonal if and only if there exist $r(r-1)$ Latin squares $L_{ik}(i \neq k)$ such that $L_iL_{ik} = L_k$.*

Corollary: *If L^i, L^k and L^{i-k} are Latin squares then L^i is orthogonal to L^k.*

For instance if L and L^2 are Latin squares then L is orthogonal to L^2.

[1] Presented to the Mathematical Society October 31st, 1942. After I submitted this paper for publication Dr. Edward Fleisher sent me his thesis on Eulerian squares which he submitted in 1934 and in which he proved Theorem 3 in a different manner.

[2] Research under a grant in aid of the Carnegie Corporation of New York.

If $A = (A_1, A_2, \cdots, A_m)$ and P is any permutation then we put $PA = (PA_1, PA_2, \cdots, PA_m)$ and $AP = (A_1P, A_2P, \cdots, A_mP)$. If A is a Latin square then also AP and PA are Latin squares. If A is orthogonal to B then AP is orthogonal to BQ for any permutations P and Q. For if $AC = B$ then $AP(P^{-1}CQ) = BQ$, since the associative law holds for the operations indicated. This means that A and B remain orthogonal if we permute the variables in both squares in any arbitrary way.

Hence if A is orthogonal to B also AA_1^{-1} is orthogonal to BB_1^{-1}. We can therefore, while preserving orthogonality, always transform the pair A and B so that $A_1 = B_1 = 1$ where 1 denotes the identity. We shall then say that the pair A, B is written in the reduced form.

DEFINITION 1: *If A is orthogonal to B, and if in the reduced form the permutations of A are the same as those of B in a different order, and if these permutations form a group G, then the pair A and B is said to be based on the group G.*

A pair of orthogonal Latin squares is called a Graeco-Latin square. The Graeco-Latin squares constructed by Bose [1] Stevens [2] and Fisher and Yates [3] are all based on groups. There exist Graeco-Latin squares, however, which are not based on a group.

If the orthogonal pair A, B is based on a group G and if $AC = B$ then also C contains only permutations of G, and since C is a Latin square it must contain all the permutations of G. Calling C_i the image of A_i we obtain a biunique mapping S of G into itself. Let $A_i^S = C_i$ then $B_i = A_iA_i^S$ and S has therefore the property that every element of G is of the form XX^S where X is in G.

DEFINITION 2: *A biunique mapping S of a group G into itself will be called a complete mapping if every element of G can be represented in the form XX^S where X is an element of G and X^S the image of X under the mapping S.*

If an abstract group G of order m admits a complete mapping S then we can immediately construct an m sided Graeco-Latin square based on G. To do this we represent G as a regular permutation group. Let $P_1, P_2, \cdots, P_m$ be the permutations of this representation. Then $A = (P_1, P_2, \cdots, P_m)$, $C = (P_1^S, P_2^S, \cdots, P_m^S)$ and $B = (P_1P_1^S, P_2P_2^S, \cdots, P_mP_m^S)$ are Latin squares and hence A is orthogonal to B and AP_1^{-1} and $B(P_1P_1^S)^{-1}$ form a reduced pair.

If $L_1, L_2, \cdots, L_r$ are orthogonal Latin squares and $L_iL_{ik} = L_k$ then we form the product

$$L_1L_{12}L_{23} \cdots L_{r-1r}. \tag{2}$$

From $L_iL_{ik} = L_k$, $L_kL_{kj} = L_j$ we find $L_iL_{ik}L_{kj} = L_j$ and hence $L_{ik}L_{kj} = L_{ij}$. L_{ik} is therefore orthogonal to L_{ij}. The product (2) has the property that for any $s \leqslant r$ the product of s successive factors is a Latin square. On the other hand if a product of r Latin squares $L_1, L_{12}, \cdots, L_{r-1r}$ has this property then the Latin squares $L_1, L_2, \cdots, L_r$ where $L_i = L_1L_{12}L_{23} \cdots L_{i-1i}$ are orthogonal.

DEFINITION 3: *A set of r orthogonal Latin squares will be called based on a group G if every pair in the set is based on G.*

If $L_1, L_2, \cdots, L_r$ are based on a group G then G must admit r mappings $S_1 = 1, S_2, \cdots, S_r$ into itself such that every element of G can be written in

the form $X^{S_i+S_{i+1}+\ldots+S_{i+h}}$ for every i and h with $1 \leqslant i \leqslant r$ and $0 \leqslant h \leqslant r-i$, where $A^{S+S'} = A^S A^{S'}$, and A^S is the image of A under the mapping S.

DEFINITION 4: *The mappings $S_1 = 1, S_2, \cdots, S_r$ of a group G into itself will be called r-fold complete if every element of G is of the form $X^{S_i+S_{i+1}+\ldots+S_{i+h}}$ for every i and h with $1 \leqslant i \leqslant r$ and $0 \leqslant h \leqslant r-i$.*

Now let G be an abstract group of order m admitting an r-fold complete set of mappings $S_1 = 1, S_2, \cdots, S_r$. Put

$$L_i = (1^{S_1+S_2+\ldots+S_i}, P_2^{S_1+S_2+\ldots+S_i}, \cdots, P_m^{S_1+S_2+\ldots+S_i})$$

where $1, P_2, \cdots, P_m$ is a regular representation of G. Then $L_1, L_2, \cdots, L_r$ is a set of r orthogonal Latin squares based on G. Put $A_i = 1^{S_1+S_2+\ldots+S_i}$ then $L_1A_1^{-1}, \cdots, L_rA_r^{-1}$ are written in the reduced form. Hence we have

THEOREM 2: *A set of r orthogonal Latin squares based on a group G exists if and only if G admits an r-fold complete set of mappings.*

If G is of order $m = 4n + 2 = 2m'$ then G has a self-conjugate subgroup H of order m'. Suppose G admits a complete mapping S. We have

$$G = H + HA.$$

$XX^S \subset H$ if either X and X^S or neither of them are in H. Further $XX^S \subset HA$ if either X or X^S but not both of them are in H.

Let a be the number of elements $X \subset H$ such that $X^S \subset H$,

b the number of elements $X \subset H$ such that $X^S \subset HA$,

c the number of elements $X \subset HA$ such that $X^S \subset H$,

then $a + b = m'$, $a + c = m'$. Of the products XX^S exactly $b + c$ are in HA. Hence $b + c = m'$, $a = b$ and therefore $m' = 2a$, which is impossible since m' is odd. We have therefore:

THEOREM 3: *No $4n + 2$ – sided Graeco-Latin square based on a group can exist.*

If a group G admits r automorphisms $T_1 = 1, T_2, \cdots, T_r$ such that $X^{T_i} \neq X^{T_j}$ for $i \neq j$ and $X \neq 1$ then the mappings $S_1 = 1$, $S_i = X^{-T_{i-1}}X^{T_i}$ for $i = 2, 3, \cdots, r$ are r-fold complete; for if

$$X^{S_i+S_{i+1}+\ldots+S_{i+h}} = Y^{S_i+S_{i+1}+\ldots+S_{i+h}}$$

we have for $i = 1$

$$X^{T_{i+h}} = Y^{T_{i+h}}$$

and for $i > 1$

$$X^{-T_{i-1}}X^{T_{i+h}} = Y^{-T_{i-1}}Y^{T_{i+h}}$$

and therefore

$$(YX^{-1})^{T_{i-1}} = (YX^{-1})^{T_{i+h}}$$

and hence $Y = X$ in both cases since by hypothesis $X^{T_i} \neq X^{T_j}$ for $i \neq j$ and $X \neq 1$, $X^{S_i+\ldots+S_{i+h}}$ therefore takes m different values and reproduces every element of G.

If we represent G as a regular permutation group then the squares $L_1 = (1, P_2, \cdots, P_m)$, $L_2 = (1, P_2^{T_2}, \cdots, P_m^{T_2})$, $\cdots$, $L_r = (1, P_2^{T_r}, \cdots, P_m^{T_r})$ are orthogonal Latin squares by Theorems 1 and 2. There exist however complete

mappings which are not derivable from automorphisms. For instance every group of odd order admits the complete mapping $A^S = A$ but $A^T = A^2$ is not an automorphism if the group is not abelian.

Most of the sets of orthogonal Latin squares that have been constructed so far are based on abelian groups of type $(p, p, \cdots, p)$ and the mappings of the squares of the sets into each other are automorphisms of this group. R. C. Bose [1] and W. L. Stevens [2] for instance use the cyclic group of automorphisms of the additive group of a G. F. (p^n) induced through multiplication by the elements of the Galois field that are different from 0. In this way they assure that different automorphisms will map the same element into different elements. They give a convenient method for finding a base element of the group of automorphisms. In this way they reduce considerably the labor involved in the construction of $p^n - 1$ orthogonal Latin squares of side p^n. The 9 x 9 squares in the statistical tables by Fisher and Yates [3] are also based on the abelian group of type (3,3) but another set of automorphisms is used.

If $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ (p_i prime $p_i \neq p_k$ for $i \neq k$) and if $r = \min p_i^{e_i} - 1$ then a set of r orthogonal Latin squares can always be constructed from the abelian group of type $(p_1 \cdots p_1, p_2 \cdots p_2, \cdots, p_n, \cdots, p_n)$ and its automorphisms. This can be done by finding r automorphisms $T_1^{(i)}, T_2^{(i)}, \cdots, T_r^{(i)}$ for each of the subgroups of order $p_i^{e_i}$ such that $T_k^{(i)} T_j^{(i)-1}$ leaves no element unchanged except 1. If we apply the automorphisms $T_j^{(1)}, T_j^{(2)}, \cdots, T_j^{(n)}$ simultaneously, for $j = 1, 2, \cdots, r$, we obtain r automorphisms of the desired type.

Once the automorphisms are known the construction of the set of orthogonal Latin squares can easily be carried out. To do this we have to write down the multiplication table of the group and obtain the orthogonal squares by interchanging the rows in accord with the automorphisms.

DEFINITION 5: *A set of orthogonal Latin squares derived from a group and its automorphisms will be called constructed by the automorphism method.*

We now prove:

THEOREM 4: *Let c_q be the number of classes of elements of order q of a group G. Let $s = \min c_q$; then not more than s orthogonal Latin squares can be constructed from G by the automorphism method.*

PROOF: Let T be an automorphism which leaves no element unchanged except 1. If A is of order q then A^T is also of order q. If $A^T = P^{-1}AP$ then there exists an element Q such that $P = Q^{-1}Q^T$ because, as we have shown, every element can be represented in the form $X^{-1}X^T$. But then

$$(QAQ^{-1})^T = QPP^{-1}APP^{-1}Q = QAQ^{-1}.$$

Hence $A = 1$. T can therefore not transform any element except 1 into an element of the same class. Hence not more than $s = \min c_q$ automorphisms, $T_1, \cdots, T_s$ can exist such that $T_i^{-1}T_j$ leave no element except 1 fixed and this proves our theorem.

COROLLARY: *If $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ (p_i prime $p_j \neq p_k$ for $j \neq k$) then not more than $r = \min p_i^{e_i} - 1$ orthogonal m-sided Latin squares can be constructed from any group with the automorphism method.*

PROOF: The Sylow group of order $p_i^{e_i}$ contains a representative of every class of elements of order p_i hence $\min c_q \leqslant \min p_i^{e_i} - 1$.

Below are given two examples of Graeco-Latin squares obtained from complete mappings which are not obtained from automorphisms. Neither could have been obtained by combining Graeco-Latin squares constructed by the method of Bose [1] and Stevens [2].

The first example is based on the abelian group of type (2,2,3). If the basis elements are defined by $P^2 = R^2 = Q^3 = 1$ the complete mapping used is given by

$$L_1 = (1, P, R, PR, Q, PQ, RQ, PRQ, Q^2, PQ^2, RQ^2, PRQ^2)$$

$$L_{12} = (1, RQ, PRQ^2, PQ^2, Q, RQ^2, PR, P, Q^2, R, PRQ, PQ)$$

$$L_2 = (1, PRQ, PQ^2, RQ^2, Q^2, PR, PQ, RQ, Q, PRQ^2, P, R).$$

The second square is based on the regular representation of the A_4 the alternating group in 4 variables. The generating relations are $P^2 = R^2 = Q^3 = 1$, $QP = RQ$, $QR = PRQ$. The complete mapping is given by

$$L_1 = (1, P, R, PR, Q, PQ, RQ, PRQ, Q^2, PQ^2, RQ^2, PRQ^2)$$

$$L_{12} = (1, R, PR, P, Q, PQ, RQ, PRQ, Q^2, PQ^2, RQ^2, PRQ^2)$$

$$L_2 = (1, PR, P, R, Q^2, PRQ^2, PQ^2, RQ^2, Q, RQ, PRQ, PQ).$$

EXAMPLE 1

1,1	2,2	3,3	4,4	5,5	6,6	7,7	8,8	9,9	10,10	11,11	12,12
2,8	1,7	4,6	3,5	6,12	5,11	8,10	7,9	10,4	9,3	12,2	11,1
3,10	4,9	1,12	2,11	7,2	8,1	5,4	6,3	11,6	12,5	9,8	10,7
4,11	3,12	2,9	1,10	8,3	7,4	6,1	5,2	12,7	11,8	10,5	9,6
5,9	6,10	7,11	8,12	9,1	10,2	11,3	12,4	1,5	2,6	3,7	4,8
6,4	5,3	8,2	7,1	10,8	9,7	12,6	11,5	2,12	1,11	4,10	3,9
7,6	8,5	5,8	6,7	11,10	12,9	3,12	10,11	3,2	4,1	1,4	2,3
8,7	7,8	6,5	5,6	12,11	11,12	10,9	9,10	4,3	3,4	2,1	1,2
9,5	10,6	11,7	12,8	1,9	2,10	3,11	4,12	5,1	6,2	7,3	8,4
10,12	9,11	12,10	11,9	2,4	1,3	4,2	3,1	6,8	5,7	8,6	7,5
11,2	12,1	9,4	10,3	3,6	4,5	1,8	2,7	7,10	8,9	5,12	6,11
12,3	11,4	10,1	9,2	4,7	3,8	2,5	1,6	8,11	7,12	6,9	5,10

EXAMPLE 2

1,1	2,2	3,3	4,4	5,5	6,6	7,7	8,8	9,9	10,10	11,11	12,12
2,4	1,3	4,2	3,1	6,8	5,7	8,6	7,5	10,12	9,11	12,10	11,9
3,2	4,1	1,4	2,3	7,6	8,5	5,8	6,7	11,10	12,9	9,12	10,11
4,3	3,4	2,1	1,2	8,7	7,8	6,5	5,6	12,11	11,12	10,9	9,10
5,9	7,12	8,10	6,11	9,1	11,4	12,2	10,3	1,5	3,8	4,6	2,7
6,12	8,9	7,11	5,10	10,4	12,1	11,3	9,2	2,8	4,5	3,7	1,6
7,10	5,11	6,9	8,12	11,2	9,3	10,1	12,4	3,6	1,7	2,5	4,8
8,11	6,10	5,12	7,9	12,3	10,2	9,4	11,1	4,7	2,6	1,8	3,5
9,5	12,7	10,8	11,6	1,9	4,11	2,12	3,10	5,1	8,3	6,4	7,2
10,7	11,5	9,6	12,8	2,11	3,9	1,10	4,12	6,3	7,1	5,2	8,4
11,8	10,6	12,5	9,7	3,12	2,10	4,9	1,11	7,4	6,2	8,1	5,3
12,6	9,8	11,7	10,5	4,10	1,12	3,11	2,9	8,2	5,4	7,3	6,1

REFERENCES

[1] R. C. Bose, "On the application of the properties of Galois fields to the problem of construction of Hyper-Graeco-Latin-squares," *Sankhya*, 1938.

[2] W. L. Stevens, "The completely orthogonalized Latin-square," *Annals of Eugenics*, 1939.

[3] R. A. Fisher and F. Yates, *Statistical Tables for Agricultural, Biological, and Medical Research*, Edinburgh: Oliver and Boyd.