SANKHYĀ

THE INDIAN JOURNAL OF STATISTICS

Edited by : P. C. MAHALANOBIS

VOL. 5. PART 4. 1941.

ON COMPLETE SETS OF LATIN SQUARES

BY R. C. BOSE and K. R. NAIR

Statistical Laboratory, Calcutta

INTRODUCTION

1. A set of m numbers 0, 1, 2, ... $m-1$, when arranged in an $m \times m$ square in such a way that every letter or number occurs just once in every row and once in every column, may be said to form a Latin Square. The Latin Square is said to be in the standard form if the numbers of the top row and the left hand column are in the natural order 0, 1, 2,..., $m-1$. Two Latin Squares are said to be orthogonal, when if they are superimposed, any number of the first square occurs just once with each number of the second square. $m-1$ mutually orthogonal $m \times m$ Latin Squares are said to form a 'complete set of orthogonal Latin Squares'. It was well known that a complete set of orthogonal Latin Squares exists when m is a prime integer. Such sets were also known to exist for the values $m=4$, 8, 9.[1a, 2] One of the authors (R. C. Bose) first showed, by using the properties of Galois Fields, that such a set can always be constructed when m is the power of a prime[1b]. Stevens also independently obtained the same result, practically at the same time[2]. Bose also showed that every plane Finite Projective Geometry with $m+1$ points on every line has associated to it a system of 'complete sets' of orthogonal $m \times m$ Latin Squares. Conversely to a given 'complete set of orthogonal Latin Squares' there is associated a unique Plane Finite Projective Geometry, with $m+1$ points on every line. To every Galois field $GF(p^n)$, with $m=p^n$ elements, there corresponds a unique Finite Projective Geometry $PG(2,p^n)$, which is the only Finite Projective Geometry with $m+1$ points on every line, in which Desargues Theorem holds. The complete sets of orthogonal Latin Squares associated to this geometry may be called 'Desarguesian sets' as distinguished from 'Non-Desarguesian sets' corresponding to Non-Desarguesian finite geometries (for which Desargues theorem does not hold).

2. A complete set of orthogonal Latin Squares is said to be a 'standardised set', if the first square be in the standard from, and the numbers in the top rows of the other squares are in their natural order. It is an interesting problem to determine the number of Desarguesian standardised $m \times m$ sets. This number has been shown to be

$$(p^s-2)! \mid n \tag{0·20}$$

where $m=p^s$.

It has also been shown that all Desarguesian $m \times m$ sets ($m=p^s$), can be constructed by means of the formula

$$l_j=l_s+l_i l_t \tag{0·21}$$

by identifying the symbols $l_0, l_1, \ldots . l_{m-1}$ with the p^s elements of the Galois field $GF(p^s)$, in any order, except that l_s must always be the null element and l_1 the unit element of the field, and then putting the number j in the cell (s, t) of the i-th square. It has already been noticed by Stevens that Fisher's 9×9 set is derivable from the above formula, so that this set must be Desarguesian. The 8×8 set given in Fisher's *Design of Experiments*[4] and the 8×8 set given in Fisher and Yates' *Statistical Tables*[5] have both been shown to be Desarguesian by us, but it is interesting to note that the 9×9 set given in the *Tables* turns out to be non-Desarguesian. It has been shown to be derivable by means of the formula (0·21) from a certain Dicksonian[2] Algebra $A(3^2)$.

3. Any given complete set of orthogonal Latin Squares, can be brought in the standard form, by applying to all the squares of the set, row and column interchanges bringing, one square to the standard form, and then by bringing the numbers of the top row in every other square in their natural order, by a permutation of the numbers in each square. When thus standardised all the hitherto known complete sets of orthogonal Latin Squares' (as noticed by Stevens[6]) are such that all squares of a given set are derivable from any one square by suitable row permutations only. We have shown that this property is certainly true for every Desarguesian set, but there exist Non-Desarguesian sets, in which this property does not hold.

4. A standardised set of orthogonal Latin squares, may be said to be in the 'canonical form,' if the rows of the i-th square (excepting the top row which is 0, 1, 2,... $m-1$) are obtainable by a cyclic permutation of the rows (other than the top row) of the first square. The number of Desarguesian canonical $m \times m$ sets has been shown to be

$$\phi(p^s-1) / n$$

where $m=p^s$, and ϕ is the well known Euler function giving the number of integers, less than a given integer and prime to it.

A canonical set can be completely written down, when we know the row number one (*i.e.*, the row just below the top row) of the first square in the set. This row may be called the key row of the set. Key rows for all possible Desarguesian canonical $m \times m$ sets for the values 3, 4, 5, 7, 8, 9, 11, 16, 25, 27 of m have been tabulated.

§ 1. STANDARDISED SETS OF ORTHOGONAL LATIN SQUARES ASSOCIATED TO THE GEOMETRY PG $(2, p^s)$.

1. It has been shown in the earlier paper of Bose,[1] that from a given Plane Finite Projective Geometry with $m+1$ points on it we can obtain a complete set of orthogonal Latin Squares in the following manner :—

Mark out any line of the geometry as the 'line at infinity' and the $m+1$ points X, Y, U_1, U_2, ... U_{m-1}, on it as the points at infinity. The remaining m^2+m lines, and m^2 points are called 'finite points'. Then m finite lines through each of X, Y, U_1, U_2, ... U_{m-1} respectively are said to form the pencils (X), (Y), (U_1), (U_2), ... (U_{m-1}) respectively. Attach in any arbitrary manner the numbers 0, 1, 2, ... $m-1$ to the lines of the pencil (X), and do the same to the lines of (Y), (U_1), (U_2), ..., (U_{m-1}). We take now an $m \times m$ square, and number its columns beginning from the left hand: 0, 1, 2, ... $m-1$; similarly the rows beginning from the top row are numbered 0, 1, 2, ... $m-1$. The cell formed by the intersection of the column number s with the row number t is called the cell (s, t).* Any finite point of the geometry is given as the intersection of one line of the pencil (X), say the line number s, with a line of the pencil (Y) say the line number t. Then this finite point is made to correspond to the cell (s, t) of the $m \times m$ square. There is thus a (1,1) correspondence between the m^2 cells, and the m^2 finite points. If now in each cell (s, t) of the $m \times m$ square we put the number j carried by that line of the pencil (U_j) which passes through the corresponding finite point, we get a Latin square $[L_j]$. The Latin squares $[L_1]$, $[L_2]$, ... $[L_{m-1}]$ obtained in this manner, form a complete set of mutually orthogonal Latin squares. This set may be said to be associated to the geometry from which it has been derived. Conversely the set being given the associated geometry can be reconstructed from it.

2. Given an integer $m \geqq 2$ of the form p^s, where p is a prime, it is well known that by the help of the Galois Field $GF(p^s)$ we can construct a Plane Finite Projective Geometry[2] $PG(2, p^s)$ in which Desargues Theorem holds. In the earlier paper[1] this geometry was constructed by taking non-homogeneous coordinates, thus getting at first the 'finite points' and 'finite lines' only and then completing the geometry by addition of the conceptual 'elements at infinity'. For the purpose of the present paper it would be more convenient to generate the geometry by using homogeneous coordinates.

Consider the Galois field $GF(p^s)$. If (ξ, η, ζ) be any ordered triplet of the elements of the field $(\xi, \eta, \zeta$, not being simultaneously zero), then (ξ, η, ζ) represents a point of our Geometry, it being understood that (ξ, η, ζ) and (ξ', η', ζ') represent the same point when and only when there exists an element $\rho \neq 0$ of the field such that $\xi' = \rho\,\xi$, $\eta' = \rho\,\eta$, $\zeta' = \rho\zeta$ whence $\xi = \rho^{-1}\,\xi'$, $\eta = \rho^{-1}\,\eta'$, $\zeta = \rho^{-1}\,\zeta'$. The point is said to have the coordinates (ξ, η, ζ). The coordinates of a point are arbitrary to the extent of a non-zero multiplicative factor, so that the same point can be represented by $m-1$ triplets. There are m^3-1 possible triplets, excluding the triplet (0, 0, 0). Hence the number of points in the geometry is $(m^3-1)/(m-1) = m^2+m+1$.

All points whose coordinates satisfy a linear equation of the form

$$a\,\xi + b\,\eta + c\,\zeta = 0 \qquad .. \quad (1{\cdot}20)$$

where a, b, c are not simultaneously zero, are said to lie on a line of the projective geometry. (1·20) is said to be the equation of this line. Clearly this line is identical with the line

$$a'\,\xi + b'\eta + c'\,\zeta = 0 \qquad .. \quad (1{\cdot}21)$$

---

* This differs from the notation of the earlier paper[1], the cell (t, s) of the old notation being now called the cell (s, t).

if and only if there exists an element $\sigma \neq 0$ of G F(p^s). Such that $a' = \sigma a$, $b' = \sigma b$, $c' = \sigma c$, so that $a = \sigma^{-1} a'$, $b = \sigma^{-1} b'$, $c = \sigma^{-1} c'$. The number of lines in our geometry is $m^2 + m + 1$.

Since the operations of addition, subtraction, multiplication, and division (by a non-zero element) are possible in GF(p^s) it follows as in ordinary analytical geometry, that any two points lie on one and only one line ; and any two lines intersect in one and only one point.

In the equation (1·20), at least one of the elements a, b, c is non-zero. Let $c \neq 0$. Then corresponding to any value of ξ, η we have a unique value of ζ. Hence excluding (0, 0, 0), $m^2 - 1$ triplets satisfy the equation. These represent the same point in sets of $m-1$. Hence the number of points on any line is $m+1$. Similarly $m+1$ lines pass through every point.

The 'points' and 'lines' here defined therefore satisfy all the axioms for a Plane Finite Projective Geometry. The geometry here obtained is usually denoted by PG(2, p^s). It is the only Desarguesian Geometry with $p^s + 1$ points on every line. Complete sets of orthogonal Latin Squares, associated to this geometry, may be called Desarguesian sets.

3. To actually obtain from PG(2, p^s), a complete set of orthogonal Latin Squares, we have to carry out the procedure indicted in para 1. Let us choose the line $\zeta = 0$, as the line at infinity. The points (0, 1, 0) and (1, 0, 0) clearly lie on this line. They may be taken as the points X and Y. The remaining $m-1$ points on this line can be taken as

$$U_1 = (q_1, -1, 0),\ U_2 = (q_2, -1, 0),\ \ldots\ U_{m-1} = (q_{m-1}, -1, 0) \qquad \ldots\ (1{\cdot}30)$$

where $q_1, q_2, \ldots q_{m-1}$ are all the non- zero elements of GF(p^s) in some order.

The pencils (X), (Y), (U_1), (U_2), ... (U_{m-1}) being defined as in paragraph (1), we attach to the m lines of each pencil the numbers 0, 1, 2, ... $m-1$, in an arbitrary manner. Let the equation of the line number s of the pencil (X) be

$$\xi + c_s\, \zeta = 0 \qquad \ldots\ (1{\cdot}31)$$

and the equation of the line number t of (Y) be

$$\eta + d_t\, \zeta = 0 \qquad \ldots\ (1{\cdot}32)$$

Then $c_0, c_1, \ldots c_{m-1}$ are the m elements of GF(p^s) in some order and the same holds for $d_0, d_1, \ldots d_{m-1}$.

Taking any $m \times m$ square we let the cell (s, t) correspond to the point of intersection of (1·31) and (1·32), *i.e.*, to the point $(c_s, d_t, -1)$.

The m finite lines through the point U_i, with coordinates given by (1·32), form the pencil (U_i). For each value of i, we attach to the lines of U_i the numbers 0, 1, 2, ... $m-1$ in any manner. Let the equation of line number j of (U_i) be

$$\xi + q_i\, \eta + l_j\, \zeta = 0 \qquad (1{\cdot}33)$$

where $l_0, l_1, \ldots l_{m-1}$ are the m elements of GF(p^s) in some order.

ON COMPLETE SETS OF LATIN SQUARES

The $m \times m$ square is converted into a Latin Square $[L_i]$ by putting in the cell (s, t), the number j carried by that line of (U_i) which passes through the corresponding point $(c_s, d_t, -1)$. Hence j is determined by

$$P_j = c_s + q_i d_t \qquad .. \quad (1{\cdot}34)$$

The Latin squares $[L_1]$, $[L_2]$, ... $[L_{m-1}]$ are then mutually orthogonal. We thus get the following theorem :—

Theorem I. *Let $m = p^n$, and let the elements in each row of the following scheme, be all the elements of GF (p^n) in some order (not necessarily the same for every row)* :—*

$$\left.\begin{array}{ccccc} c_0 & c_1 & .... & .... & c_{m-1} \\ d_0 & d_1 & .... & .... & d_{m-1} \\ P_0 & P_1 & .... & .... & P_{m-1} \\ P_0^2 & P_1^2 & .... & .... & P_{m-1}^2 \\ .... & .... & .... & .... & .... \\ P_0^{m-1} & P_1^{m-1} & .... & .... & P_{m-1}^{m-1} \end{array}\right\} \qquad .. \quad (1{\cdot}35)$$

Also let

$$q_1, q_2 \ldots . q_{m-1} \qquad .. \quad (1{\cdot}36)$$

denote the non-zero elements of GF (p^n) taken in some order.

Keeping i fixed if we put in every cell (s, t) of an $m \times m$ square the number j $(0 \leqq j \leq m-1)$ determined by

$$P_j = c_s + q_i d_t \qquad .. \quad (1{\cdot}34)$$

we obtain a Latin square $[L_i]$.

The Latin square $[L_1], [L_2], \ldots . [L_{m-1}]$ obtained by taking $i = 1, 2, \ldots . m-1$ form a complete set of mutually orthogonal Latin squares.

It should be observed that the sets obtainable from Theorem I constitute all the complete sets of orthogonal Latin Squares' associated to PG$(2, p^n)$; for no new sets are obtained by taking a new choice of the 'line at infinity' and the points X and Y upon it. Suppose that an arbitrary line

$$a\xi + b\eta + c\zeta = 0 \qquad .. \quad (1{\cdot}37)$$

is chosen as the 'line at infinity' and the points (l, m, n), (l', m', n') are chosen as the points X and Y. Then

$$al + bm + cn = 0, \; al' + bm' + cn' = 0 \qquad .. \quad (1{\cdot}38)$$

---

* In theorem I the in P_j is an upper suffix, so that P_j denotes any element of the field, and not the j-th power of l_1.

Now as the points X and Y are distinct, at least one of the quantities $mn'-m'n$, $nl'-n'l$, $lm'-l'm$ is non-vanishing. Suppose $mn'-m'n=d\neq 0$. Then from (1·37), $a\neq 0$. The linear transformation

$$\left.\begin{aligned}\xi' &= -n\,d^{-1}\,\eta + m\,d^{-1}\,\zeta\\ \eta' &= n'd^{-1}\,\eta + m'\,d^{-1}\,\zeta\\ \zeta' &= a\,\xi + b\,\eta + c\,\zeta\end{aligned}\right\} \qquad \ldots\ (1{\cdot}39)$$

with non-vanishing determinant, carries points of PG(2, p^s) into points, and lines into lines, incidence relations remaining invariant. Also (1·37) is carried to $\zeta'=0$, and X and Y to (0, 1, 0), (1, 0, 0). This proves our observation.

4. The elements of any row of (1·35) can be identified with the element of GF(p^s) in $m!$ ways. Also $q_1, q_2, \ldots q_{m-1}$ can be identified with the non-zero elements of GF(p^s) in $(m-1)!$ ways. Hence there are $(m!)^{m-1}\,(m-1)!$ ways of identifying the elements in (1·35), (1·36). The complete set of orthogonal Latin Squares corresponding to any one of these identifications is not necessarily in the standard form. Let us now determine those modes of identification for which the corresponding complete set of Latin Squares is in the standard form.

The top rows are now in natural order. Hence in the cell $(s, 0)$ of $[L_1]$ we have the number s. Thus

$$P_s=c_s+q_1\,d_s \qquad \ldots\ (1{\cdot}40)$$

Also the elements in the initial column of $[L_1]$ are in natural order. Hence the cell $(0, t)$ of $[L_1]$ contains the number t. So

$$P_t=c_0+q_1\,d_t \qquad \ldots\ (1{\cdot}41)$$

Since the number 0 occurs in the cell (0, 0) of the column 0 of (L_1), so the cell (0, 1) must contain a number $k_1\neq 0$. Now if $[L_1]$ is superimposed on $[L_1]$, the number k_1 of $[L_1]$ occurs together with the number k_1 of $[L_1]$ in the cell $(k_1, 0)$. Hence the number $k_1\neq 0$ of $[L_1]$ in the cell (0, 1) is different from k_1. Thus the cells (0, 1) of $[L_1]$, $[L_2]$, $\ldots$. $[L_{m-1}]$ contain the numbers 1, 2, $\ldots$. $m-1$ in some order or other. By writing the Latin squares of the set in a suitable order, we can arrange for the number i to appear in the cell (0, 1) of $[L_i]$. In this case

$$P_1=c_0+q_1\,d_1 \qquad (1{\cdot}42)$$

Putting $i=1$ and $s=t$ in (1·40) we have

$$P_1=c_1+q_1\,d_0 \qquad (1{\cdot}43)$$

From (1·41) and (1·43) we get

$$q_1(d_t-d_0)=c_1-c_0 \qquad (1{\cdot}431)$$

Putting $s=i$ in (1·40) we have

$$P_i=c_i+q_1\,d_0 \qquad (1{\cdot}432)$$

From (1·42) and (1·432) we get

$$q_i(d_1-d_\infty)=c_1-c_\infty \qquad .. \quad (1·433)$$

Changing t to i in (1·431) and comparing with the above, we have

$$q_i(d_1-d_\infty)=q_1(d_1-d_\infty)=(c_1-c_\infty). \quad (i=1, 2, \ldots m-1) \qquad .. \quad (1·434)$$

Let us now define l_i, $(i=1, 2, \ldots m-1)$ by

$$q_i=l_i q_1 \qquad .. \quad (1·44)$$

Clearly $l_1=1$, while $l_2, l_3, \ldots l_{m-1}$ are the other non-zero elements of GF(p^n) in some order.

From (1·434) and (1·44) we get after putting $d_1-d_\infty=\alpha\neq 0$

$$d_i=d_\infty+l_i\alpha \qquad .. \quad (1·45)$$

$$c_i=c_\infty+q_1 l_i\alpha \qquad .. \quad (1·46)$$

The relations (1·45) and (1·46) which hold for $i=1, 2, \ldots m-1$ also remain true for $i=0$, if we define $l_0=0$.

Finally from (1·40) we get

$$b_s=c_\infty+q_1 l_s\alpha+l_i q_1 d_\infty \qquad .. \quad (1·47)$$

for $(i=1, 2, \ldots m-1\,;\ s=0, 1, 2, \ldots m-1)$.

Conversely if the relations (1·44) to (1·47) hold, then the relations (1·40), (1·41), (1·42) also hold (as is seen by direct substitution). But these latter relations are sufficient to ensure that the set $[L_1], [L_2], \ldots, [L_{m-1}]$ is all the standard form with the number i in the cell $(0,1)$ of $[L_i]$. Hence we have the following Theorem.

Theorem II(A). *The necessary and sufficient conditions, that the complete set of orthogonal Latin Squares, derived in Theorem I, should be in standard form with number i in the cell $(0,1)$ of $[L_i]$ are that q_i, d_i, c_i, b_s should satisfy (1·44) to (1·46) where $l_0=0$, $l_1=1$, and $l_2, l_3, \ldots l_{m-1}$ are the remaining elements of* GF(p^n) *in some order.*

Substituting from (1·44) to (1·47) in the fundamental formula (1·34) we get

$$c_\infty+q_i l_j\alpha+l_i q_1 d_\infty=c_\infty+q_1 l_s\alpha+l_i q_1(d_\infty+l_t\alpha) \text{ or since } \alpha\neq 0,\ q_1\neq 0$$

$$l_j=l_s+l_i l_t \qquad .. \quad (1·48)$$

This relation involves only the numbers l_i. Hence we can state—

Theorem II(B). *Let $l_0=0$, $l_1=1$ and $l_2, l_3, \ldots, l_{m-1}$ the other elements of* GF(p^n) *in some order or other, $(m=p^n)$. Keeping i fixed if we put in every cell (s, t) of an $m\times m$ square the number j determined by*

$$j=l_s+l_i l_t \qquad .. \quad (1·48)$$

we obtain a Latin square $[L_i]$. The Latin Squares $[L_1], [L_2], \ldots [L_{m-1}]$ form a complete set of mutually orthogonal Latin squares, in the standard form (written in an order in which the number i appears in the cell $(0, 1)$ of $[L_i]$. The sets derivable in this way are the only standard sets associated to the geometry PG $(2, p^n)$.

5. Let $a_0, a_1, a_2, \ldots a_{m-1}$ and $a'_0, a'_1, a'_2, \ldots a'_{m-1}$ be the elements of GF(p^n) in two orders (not necessarily the same). The correspondence $a_j \rightarrow a'_j$, ($j=0, 1, 2, \ldots m-1$) is said to be an automorphism of GF(p^n) provided $a_i+a_j=a_k$ implies $a'_i+a'_j=a'_k$ and $a_i\ a_j=a_k$ implies $a'_i\ a'_j=a'_k$ for $i, j, k=0, 1, 2, \ldots m-1$. It is known[4] that there are just n automorphisms of GF(p^n), viz,

$$a_j \rightarrow a_j^{p^k},\ (k=0,1,\ 2,\ \ldots,\ n-1) \qquad \ldots \quad (1{\cdot}50)$$

It is obvious from (1·50) that in an automorphism of GF(p^n), $0\rightarrow 0$ and $1\rightarrow 1$. Let $a_1\rightarrow a'_1$ be an automorphism of GF(p^n) where $a_0=0$ and $a_1=1$. Then $a'_0=0$, $a'_1=1$. In Theorem II(B), the identifications $l_i=a_i$ ($i=0,\ 1,\ \ldots\ m-1$) and $l_i=a'_i$ ($i=0,\ 1,\ \ldots\ m-1$) lead to the same set of orthogonal Latin Squares.

Conversely if in Theorem II(B), the identifications $l_i=a_i (i=0,\ 1,\ \ldots.\ m-1)$ and $l_i=a'_i (i=0,\ 1,\ \ldots\ m-1)$ where $a_0=a'_0=0$, $a_1=a'_1=1$, lead to the same set of orthogonal Latin Squares, then $a_i=a_s+a_t\ a_u$ would imply $a_i=a'_s+a'_t\ a'_u$ for $s,\ t,\ j=0,\ 1,\ 2,\ \ldots\ m-1$, $i=1,\ 2,\ \ldots,\ m-1$. Taking $i=1$ in particular we find that $a_j=a_s+a_t$ implies $a'_j=a'_s+a'_t$ for $s, t, j=0,\ 1,\ 2,\ \ldots, m-1$. Taking $s=0$, we similarly find that $a_j=a_t\ a_u$ implies $a'_j=a'_t\ a'_u$ for $t, j=0, 1, 2, \ldots, m-1$; $i=1, 2, \ldots, m-1$. But for $i=0$, $a_j=a_1\ a_t$ obviously implies $a'_j=a'_1\ a'_t$. Hence the correspondence $a_j\rightarrow a'_j$ is an automorphism of GF(p^n).

Hence the $(m-2)!$ ways of identifying the elements $l_0, l_1, l_2, \ldots, l_{m-1}$ with the elements of GF(p^n) in Theorem II(B), (l_0 being identified with 0, and l_1 with 1), lead in sets of n, to the same complete set of orthogonal Latin Squares in the standard form Thus we get the following theorem :—

Theorem II(C). *The number of complete sets of mutually orthogonal Latin Squares in the standard form, associated to the geometry PG(2, p^n) is exactly* $(p^n-2)!/n$.

A complete set of orthogonal Latin Squares associated to the geometry PG(2,p^n) may be called a Desarguesian set. If N_m be the number of standardised Desarguesian $m\times m$ sets, then values of N_m for small values of m are shown below :

m	2	3	4	5	7	8	9
N_m	1	1	1	6	120	240	2520

Now it is known that there exists just one 'standardised complete set of orthogonal Latin Squares' for the cases $m=2, 3, 4$; there are 6 such sets for the case $m=5$, (Fisher[14]) and 120 sets for the case $m=7$ (Norton[11]). It appears therefore that for $m\leqq 7$, all the possible complete sets of orthogonal Latin Squares are Desarguesian. There exists therefore no Non-Desarguesian geometry with 8 or less points on a line.

§ 2. Identifications for the 8×8 and 9×9 sets of Fisher and Yates Non-desarguesian 9×9 sets

1. A complete set of orthogonal Latin Squares may be standardised by first bringing the first square to a standard form by row and column interchanges, applying (simultaneously the same interchanges to all squares of the set) and then by an interchange of letters within the remaining squares to bring the top rows in natural order. The first process amounts to changing the numbering of the lines of the pencils (X) and (Y), and the second to changing the numbering of the lines in the pencils $(U_2), (U_3), \ldots, (U_{m-1})$ in §1 para 1. Hence the geometry associated to a given set remains unaltered by the process of standardisation.

Consequently a Desarguesian set remains Desarguesian, and a Non-Desarguesian set remains Non-Desarguesian by standardisation.

Consider a standardised Desarguesian $m \times m$ set ($m = p^s$),

$$[L_1], [L_2], \ldots, [L_{m-1}]$$

the Latin Squares $[L_i]$ being supposed to be written in an order such that in the cell (0, 1) of $[L_i]$ there appears the number i. The number in the cell (s, t) of $[L_i]$ is then derivable by the formula (1.48) of Theorem IIB, where $l_0 = 0, l_1 = 1, l_2, l_3, \ldots, l_{m-1}$ are elements of $GF(p^s)$.

The row number t of $[L_i]$, will then be identical with some row (number t') of $[L_{i'}]$. For there is a unique element $l_{t'}$ ($t' \neq 0$), $GF(p^s)$ determined by

$$l_i l_t = l_{t'} l_{t'}$$

when $l_i \neq 0$, $l_{t'} \neq 0$ and l_i are known. The number in the cell (s, t) of $[L_i]$ is identical with the number in the cell (s, t') of $[L_{i'}]$ for $s = 0, 1, 2, \ldots m-1$. As l_i runs over all elements of $GF(p^s)$, $l_{t'}$ does the same. Hence

Theorem III. *A standardised Desarguesian set possesses the property D_0, that the rows of any square $[L_{i'}]$ of the set, are the same as that of any other square $[L_i]$ of the set, except that they occur in a different order.*

A standardised set not possessing the property D_0 is necessarily Non-Desarguesian. An example of such a set constructed from the Non-Desarguesian Geometry of Veblen and Wedderburn[19] (Carmichael [2] p. 411), by the process of §1, para 1, is given below. However the possession of the property D_0 by a standardised set is not sufficient to ensure that the set is Desarguesian. In fact the 9×9 set given in Fisher and Yates' *Tables* (*cf.* para 4) possesses the property but is nevertheless Non-Desarguesian.

STANDARDISED SET (NOT POSSESSING THE PROPERTY D_0) ASSOCIATED TO THE NON-DESARGUAN GEOMETRY OF VEBLEN & WEDDERBURN

$[L_1]$

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

$[L_4]$

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

STANDARDISED SET (NOT POSSESSING THE PROPERTY D_0) ASSOCIATED TO THE NON-DESARGUAN GEOMETRY OF VEBLEN & WEDDERBURN.

[L_3]

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

[L_4]

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

[L_5]

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

[L_6]

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

[L_1]

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

[L_4]

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

2. Consider a standardised set of orthogonal $m \times m$ Latin Squares ($m = p^s$)

$$[L_1], [L_2], \ldots, [L_{m-1}] \tag{2·20}$$

possessing the property D_0, and supposed to be written in an order such that the cell (0, 1) of $[L_i]$ contains the number i.

Corresponding to the set we can set up an Algebra in the following manner :—Let the numbers 0, 1, 2, ... $m-1$ with which the squares are filled correspond to the elements $l_0, l_1, l_2 \ldots l_{m-1}$ of our Algebra. Corresponding to the square $[L_i]$ (*i.e.*, by replacing every number j by the corresponding element l_j) we get what may be termed the 'addition table' of our Algebra. Again form an $m \times m$ square M, and put in the cell (i, t) of M the number appearing in the cell $(0, t)$ of $[L_i]$, ($i = 1, 2, \ldots m-1$). Also in every cell $(0, t)$ of M put the number 0. (The square M is thus formed by juxtaposing the left hand columns of $[L_1]$, $[L_2]$, ... $[L_{m-1}]$, prefixing a column composed of zeros only to the left). Corresponding to the square M (*i.e.*, by replacing every number j by the element l_j) we get what may be termed the 'multiplication table' for our Algebra.

For example the addition and multiplication tables for the algebra corresponding to the 9×9 set given in Fisher and Yates' tables are shown below in Table 1.

Given two elements l_u, l_v of our Algebra, their sum $l_u + l_v$ is defined as the element l_w appearing in the cell (u, v) of the 'addition table'. The product $l_u l_v$ of the two elements is defined as the element l_w appearing in the cell (u, v) of the multiplication table. In virtue of the property D_0, the number j in the cell (s, t) of $[L_i]$ satisfies

$$l_j = l_s + l_i l_t$$

which tallies with the formula (1·48) of Theorem 11B. Hence in the special case when the set (2·20) is Desarguesian, $l_0, l_1, l_2, \ldots l_{m-1}$ are the elements of the Galois field $GF(p^s)$ in some order, l_0 being the null element and l_1 the unit element.

Table 1. Algebra Corresponding to the 9×9 Set of Fisher and Yates' Tables

Addition Table

l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8
l_1	l_2	l_0	l_4	l_5	l_3	l_7	l_8	l_6
l_2	l_0	l_1	l_5	l_3	l_4	l_8	l_6	l_7
l_3	l_4	l_5	l_6	l_7	l_8	l_0	l_1	l_2
l_4	l_5	l_3	l_7	l_8	l_6	l_1	l_2	l_0
l_5	l_3	l_4	l_8	l_6	l_7	l_2	l_0	l_1
l_6	l_7	l_8	l_0	l_1	l_2	l_3	l_4	l_5
l_7	l_8	l_6	l_1	l_2	l_0	l_4	l_5	l_3
l_8	l_6	l_7	l_2	l_0	l_1	l_5	l_3	l_4

Multiplication Table

l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0
l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8
l_0	l_2	l_1	l_6	l_8	l_7	l_3	l_5	l_4
l_0	l_3	l_6	l_2	l_7	l_4	l_1	l_8	l_5
l_0	l_4	l_8	l_7	l_2	l_6	l_5	l_1	l_3
l_0	l_5	l_7	l_4	l_3	l_2	l_8	l_6	l_1
l_0	l_6	l_3	l_1	l_5	l_8	l_4	l_2	l_7
l_0	l_7	l_5	l_8	l_1	l_3	l_2	l_4	l_6
l_0	l_8	l_4	l_5	l_6	l_1	l_7	l_3	l_2

In the general case it is easy to verify that the following properties hold for our Algebra.

(i) The sum l_u+l_v, and the product $l_u\, l_v$ of two elements l_u and l_v uniquely exist (by definition).

(ii) Subtraction is possible and unique, *i.e.*, the equations

$$x+l_u=l_v,\ l_u+y=l_v$$

have unique solutions.

(iii) There exists a unique null element, *viz.*, l_0, *i.e.* l_0 is the only element with the properties that

$$l_u+l_0=l_u,\quad l_0+l_v=l_v,\quad l_0\, l_v=l_0,\quad l_u\, l_0=l_0$$

for any arbitrary element l_u of the algebra.

(iv) Division (except by the null element) is possible and unique, *i.e.*, the equations

$$x\, l_u=l_v,\quad l_u\, y=l_v\ (l_u\neq l_0)$$

have unique solutions.

(v) There exists a unique unit element, *viz.*, l_1 *i.e.*, l_1 is the only element with the property

$$l_u\, l_1=l_u,\quad l_1\, l_u=l_u$$

for an arbitrary element of the Algebra.

(vi) There holds the orthogonality property, namely that the simultaneous equations

$$x+l_i\, y=l_j$$
$$x+l_i\cdot g=l_j'$$

have a unique solution, when $l_j\neq l_j'$ (since the number j of $[L_j]$ occurs with the number of $[L_j']$ in just one cell).

(*vii*) The simultaneous equations

$$l_s + y\, l_t = x$$

$$l_{s'} + y\, l_{t'} = x$$

have a unique solution, when $l_t \neq l_{t'}$ (this follows by considering the corresponding geometry, and remembering that the points corresponding to the cells (s, t) and (s', t') are joined by one and only one line, which belongs to one of the pencils (X), (Y), (U_1), (U_2), ... (U_{m-1}). When $l_s \neq l_{s'}$ i.e. $s \neq s'$, the points must be joined by a line of (U_j) carrying say the number j. Then the solution is $x = l_j$, $y = l_j$. When $l_s = l_{s'}$, the points are joind by the same line of the pencil (X). No line belonging to any one of the pencils (U_j) can therefore pass through both points. Hence besides the obvious solution $x = l_s$, $y = 0$, there is no other solution.

The properties (*i*)—(*vii*) are of course not all independent, some of them being formally deducible from others.

Nothing however can be affirmed about the commutativity or associativity of the addition or the multiplication, or about the holding of the distributive law (from the right or the left). One or more of these laws may hold in special cases. All of them certainly hold when the set is Desarguesian. For the Algebra corresponding to the 9×9 set given in Fisher and Yates' *Statistical Tables* and shown in Table 1, it is easy to verify that both the addition and multiplication are associative, the addition is commutative and that the distributive law from the left holds, *i.e.*, $a(b+c) = ab + ac$. But the multiplication is not commutative, as is shown by the fact that the multiplication table is not symmetrical about the leading diagonal, for example $l_2 l_4 = l_3$, $l_4 l_2 = l_7$. Also the distributive law from the right does not hold, for example $(l_2 + l_3)\, l_5 = l_3\, l_5 = l_1$, $l_2 l_5 + l_3 l_5 = l_4 + l_7 = l_2$. This incidentally proves that the 9×9 set of Fisher and Yates' *Statistical Tables* must be Non-Desarguesian.

3. Let us now investigate the nature of the 8×8 set given in Fisher and Yates' *Statistical Tables*. The algebra corresponding to this 8×8 set is given below:

TABLE 2. ALGEBRA CORRESPONDING TO THE 8×8 SET GIVEN IN FISHER AND YATES' STATISTICAL TABLES

Addition Table

l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7
l_1	l_0	l_3	l_2	l_5	l_4	l_7	l_6
l_2	l_3	l_0	l_1	l_6	l_7	l_4	l_5
l_3	l_2	l_1	l_0	l_7	l_6	l_5	l_4
l_4	l_5	l_6	l_7	l_0	l_1	l_2	l_3
l_5	l_4	l_7	l_6	l_1	l_0	l_3	l_2
l_6	l_7	l_4	l_5	l_2	l_3	l_0	l_1
l_7	l_6	l_5	l_4	l_3	l_2	l_1	l_0

Multiplication Table

l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0
l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7
l_0	l_2	l_3	l_7	l_1	l_6	l_4	l_5
l_0	l_3	l_7	l_4	l_5	l_6	l_2	l_1
l_0	l_4	l_1	l_5	l_6	l_2	l_7	l_3
l_0	l_5	l_6	l_6	l_2	l_7	l_1	l_4
l_0	l_6	l_4	l_2	l_7	l_1	l_3	l_5
l_0	l_7	l_5	l_1	l_3	l_4	l_5	l_6

It can be verified that for this algebra, all the laws for a field hold. Hence the algebra must be the algebra GF(2^3) and the set in question must be Desarguesian.

Taking x^3+x^2+1 as the minimum function, the elements of GF(2^3) can be represented as (*cf.* Bose, 1938, §4, para 2)

$$0,\ x^0=1,\ x=x,\ x^2=x^2,\ x^3=x^2+1,\ x^4=x^2+x+1,\ x^5=x+1,\ x^6=x^2+x \qquad .. \quad (2{\cdot}30)$$

where x is a primitive element of GF(2^3), so that $x^7=1$.

It would be interesting to discover the identification for l_2, l_3, l_4, l_5, l_6, l_7 (of course $l_0=0$, $l_1=1$).

Now from the addition and multiplication tables we get

$$\left.\begin{array}{lll} l_2+l_3=1, & l_4+l_5=1, & l_6+l_7=1 \\ l_2\,l_4=1, & l_3\,l_5=1, & l_7\,l_6=1 \end{array}\right\} \qquad .. \quad (2{\cdot}31)$$

whereas in our representation of GF(2^3)

$$\left.\begin{array}{lll} x+x^3=1, & x^2+x^5=1, & x^4+x^6=1 \\ x\,x^6=1 & x^2\,x^5=1, & x^3\,x^4=1 \end{array}\right\} \qquad .. \quad (2{\cdot}32)$$

In the following representation, the elements whose sum is unity are joined by a thick line, while the elements whose product is unity are joined by a dotted line.

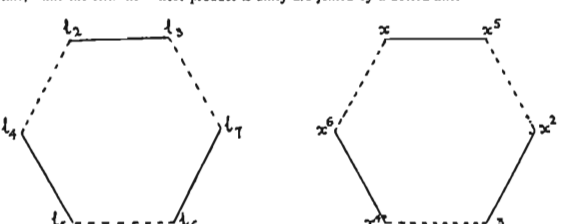

Fig 1

It is then apparent that the identification for l_2 determines the identification for l_3, l_4, l_5, l_6, l_7. Thus only the identifications shown in the following table are possible.

The identifications (3), (5), (6) are automorphic (*cf.* §1, para. 5), and as can be verified by direct substitution, satisfy the conditions of Table 2. The identifications (1), (2), (4) are automorphic, but do not satisfy all the conditions of Table 2. We can thus state :

The 8×8 *set given in Fisher and Yates' 'Statistical Tables' is Desarguesian and can be generated by the formula* (1·48) *of Theorem II*(*B*), *taking any one of the identifications* (3), (5), (6) *of Table III A. the elements of GF* (2^3) *being represented as in* (2·30).

We have been considering 'standardised sets' in which the top rows are in the natural order. The 8×8 set given in Fisher's *Design of Experiments* can be brought in this form by interchanging the columns with the rows. We can then prove as before, that the set is Desarguesian and can be generated by using the formula (1·48) of Theorem IIB, if we make any of the three identifications of Table 3B, the elements of GF(2^3) being represented as in (2·30).

TABLE 3(A). IDENTIFICATION

	l_1	l_2	l_3	l_4	l_5	l_6
(1)	x	x^2	x^3	x^4	x^5	x^6
(2)	x^2	x^3	x^4	x^5	x	x^6
(3)	x^3	x^4	x^5	x^6	x	x^2
(4)	x^4	x^5	x	x^2	x^3	x^6
(5)	x^5	x	x^2	x^3	x^4	x^6
(6)	x^6	x^4	x	x^3	x^5	x^2

TABLE 3(B). IDENTIFICATION

	l_1	l_2	l_3	l_4	l_5	l_6
(1)	x	x^2	x^3	x^5	x^4	x^6
(2)	x^2	x^3	x^4	x^6	x	x^5
(3)	x^4	x^6	x	x^5	x^3	x^2

4. Let us now consider the 9×9 set given by Fisher, in his *Design of Experiments* The corresponding algebra (when the set is written in the standardised form) is given below:

TABLE 4. ALGEBRA CORRESPONDING TO THE 9×9 SET OF FISHER'S DESIGN OF EXPERIMETS

Addition Table

	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8
l_0	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8
l_1	l_1	l_2	l_0	l_4	l_5	l_3	l_7	l_8	l_6
l_2	l_2	l_0	l_1	l_5	l_3	l_4	l_8	l_6	l_7
l_3	l_3	l_4	l_5	l_6	l_7	l_8	l_0	l_1	l_2
l_4	l_4	l_5	l_3	l_7	l_8	l_6	l_1	l_2	l_0
l_5	l_5	l_3	l_4	l_8	l_6	l_7	l_2	l_0	l_1
l_6	l_6	l_7	l_8	l_0	l_1	l_2	l_3	l_4	l_5
l_7	l_7	l_8	l_6	l_1	l_2	l_0	l_4	l_5	l_3
l_8	l_8	l_6	l_7	l_2	l_0	l_1	l_5	l_3	l_4

Multiplication Table

	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8
l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0
l_1	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8
l_2	l_0	l_2	l_1	l_6	l_8	l_4	l_3	l_5	l_7
l_3	l_0	l_3	l_6	l_4	l_7	l_1	l_5	l_8	l_2
l_4	l_0	l_4	l_8	l_7	l_1	l_6	l_2	l_3	l_5
l_5	l_0	l_5	l_4	l_1	l_6	l_2	l_8	l_7	l_3
l_6	l_0	l_6	l_3	l_5	l_2	l_8	l_7	l_4	l_1
l_7	l_0	l_7	l_5	l_8	l_3	l_7	l_4	l_1	l_6
l_8	l_0	l_8	l_7	l_2	l_5	l_3	l_1	l_6	l_4

It is easily verifiable that for the above algebra all the laws for a 'field' hold. Hence Fisher's 9×9 set is Desarguesian.

Taking x^2+x+2 as the minimum function the elements of GF(3^2) can be represented as (*cf.* Bose, 1938, § 4, para 3),

$$0, x^0=1, x=x, x^2=2x+1, x^3=2x+2, x^4=2, x^5=2x, x^6=x+2, x^7=x+1 \quad .. \quad (2{\cdot}33)$$

From Table 4 we find $l_1+l_2=0$. Since $l_1=1$, $l_2=2=x^4$ it remains to discover the identification for l_3, l_4, l_5, l_6, l_7, l_8. Now from Table 4,

$$l_3+l_6=0, \quad l_4+l_8=0, \quad l_5+l_7=0$$
$$l_3+l_7=1, \quad l_4+l_6=1, \quad l_5+l_8=1$$

whereas in our representation of GF(3^2)

$$x+x^3=0, \quad x^7+x^5=0, \quad x^6+x^2=0$$
$$x^3+x^7=1, \quad x^5+x^6=1, \quad x^2+x=1$$

In the following representation, elements whose sum is 0 are joined by a thick line, elements whose sum is 1 are joined by dotted line.

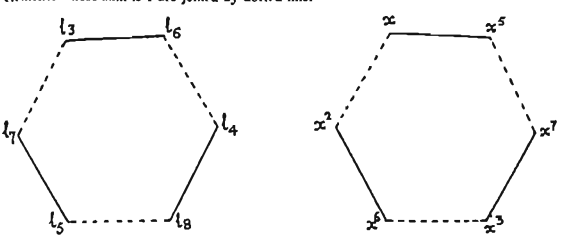

Fig 2

Hence only the six identifications shown in the following table are possible. They are automorphic, in pairs, viz., (1) and (4); (5) and (6); and (2) and (3).

Each of the above six identifications satisfies the Addition Table, as can be readily verified. Now from the multiplication table $l_3 . l_7=1$. This is satisfied only by the identifications (1) and (4). We may verify that they satisfy all the conditions of Table 4. Hence we can state :

The 9×9 *set given by Fisher in his 'Design of Experiments' is Desarguesian, and can be generated by the formula* (1·48) *of Theorem II(B), taking any one of the identifications* (1) *and* (4) *of Table 5, the elements of GF* (3^2) *being represented as in* (2·33).

5. Let us now consider more fully the nature of the 9×9 set given in Fisher and Yates' *Statistical Tables*. We note that the addition table for this set is the same as for Fisher's 9×9 set given in the *Design of Experiments* (when written in the standardised form). The two sets have the same common first square (L_1). Remembering that the identifications

TABLE 5. IDENTIFICATION

	l_0	l_1	l_2	l_3	l_4	l_5	l_6
(1)	x^4	x	x^5	x^7	x^3	x^6	x^2
(2)	x^4	x^3	x	x^5	x^6	x^2	x^7
(3)	x^4	x^7	x^5	x^6	x^2	x	x^3
(4)	x^4	x^3	x^7	x^5	x	x^2	x^6
(5)	x^4	x^6	x^2	x	x^5	x^7	x^3
(6)	x^4	x^2	x^6	x^3	x^7	x^5	x

in Table 5, were derived only on the basis of the addition table, we can make the following interesting observations: there are exactly three Desarguesian complete sets of 9×9 orthogonal Latin squares, which contain $[L_1]$, the common first square of the 9×9 sets given in the *Design of Experiments* and in the *Statistical Tables*. Of course one of these sets is Fisher's set itself. As the existence of the 9×9 set given in the *Statistical Tables*, and the set derived from Veblen and Wedderburn's geometry (*cf.* § 2, para. 1) shows, there are other Non-Desarguesian sets containing $[L_1]$.

From the Galois Algebra $GF(3^2)$ we can construct a new Dicksonian Algebra[2] in the following manner:—Let $\alpha_0=0$, α_1, α_2, ... α_8 be the elements of $GF(3^2)$. The 8 non-zero elements can be divided into two classes. An element belongs to the first class if it can be expressed as the square of another element, while it belongs to the second class if it cannot be so expressed. Each class contains four elements. Now we take a new set of nine elements $\beta_0=0, \beta_1, \beta_2 \ldots \beta_8$ as the elements of the new algebra (β_1 corresponding to α_1) and define addition and multiplication of these elements as follows:—

(*i*) $\beta_i+\beta_j=\beta_k$ when $\alpha_i+\alpha_j=\alpha_k$

(*ii*) $\beta_i\ \beta_j=0$ when $\beta_j=0$

(*iii*) If α_j belongs to the first class $\beta_i\ \beta_j=\beta_k$, when $\alpha_i\ \alpha_j=\alpha_k$

(*iv*) If α_j belongs to the second class $\beta_i\ \beta_j=\beta_k$ when $\alpha_i\ \alpha^3{}_j=\alpha_k$

It can now be verified that if we take $l_i (i=0, 1, \ldots 8)$ to be the elements of a Dicksonian Algebra constructed as above, and make l_i correspond to the element of $GF(3^2)$ appearing under l_i in any (fixed) row of the Table 5 (l_0 and l_1 corresponding to the null and unit elements of $GF(3^2)$), then we get just the algebra (of Table I) corresponding to the 9×9 set given in Fisher and Yates' *Statistical Tables*.

For example let the elements of $GF(3^2)$ be taken as in (2·33); and for the elements of the new algebra take $l_0, l_1, l_2, l_3, l_4, l_5, l_6, l_7, l_8$ corresponding to the elements 0, 1, x^4, x, x^7, x^5, x^3, x^6, x^2. Then $l_1+l_2=l_3$, since $x^7+x^5=(x+1)+(2x+1)=2=x^4$; $l_1\,l_1=l_2$, since $x^7\,x^7=x$; $l_1\,l_6=l_8$ since $x^7\,(x^3)^3=x^6$. These results can be seen to tally with Table 1.

The result obtained in the last paragraph can be stated in a slightly different form :—

The complete set of 9×9 orthogonal Latin squares given in Fisher and Yates' 'Statistical Tables' can be generated by putting in the cell (s, t) of the i^{th} square (L_i) the number j determined by

$$l_j = l_s + l_1 l_t \quad \textit{when } l_t \textit{ belongs to the first class (squares)}$$

$$l_j = l_s + l_1 l_t^3 \quad \textit{when } l_t \textit{ belongs to second class (non-squares)}$$

$l_0=0$, $l_1=1$, $l_2 \ldots l_8$ being elements of $GF(3^2)$, any one of the identifications (1)—(6) of Table 5 being taken for $l_2, l_3, \ldots, l_8$.

We finally notice one more interesting point. The set considered above possesses the property D_0 (*cf.* Theorem III), but we can construct from it a set which does not have this property, by first obtaining the projective geometry associated to the set, suitably changing the line at infinity, and then deriving another set by the process of § 1, para 1.

§ 3. Canonical sets of orthogonal Latin Squares associated to the geometry PG $(2, p^n)$.

1. A standardised set of orthogonal Latin squares, $[L_1], [L_2], \ldots [L_{m-1}]$ is said to be in the canonical form if the row number t or $[L_{i,1}]$ is identical with the row number $t+1$ of $[L_i]$, for $t=1, 2, \ldots m-2$, while the row number $m-1$ of $[L_{i,1}]$ is identical with the row number 1 of $[L_i]$. Thus the rows of $[L_{i,1}]$ (other than the row number zero which is automatically 0, 1, 2, $\ldots m-1$) are obtainable by a cyclic permutation of the rows of $[L_i]$ (other than the row number zero). Hence when the set $[L_1], [L_2], \ldots [L_{m-1}]$ is in the canonical form, we can at once write down $[L_2], \ldots [L_{m-1}]$ knowing $[L_1]$.

Let us consider for what identifications of the l_i's in Theorem II(B), we get a canonical set. The number j in the cell (s, t) of $[L_{i,1}]$ is given by

$$l_j = l_s + l_{i,1}\, l_t \qquad .. \quad (3{\cdot}10)$$

the number occurring in the cell $(s, t+1)$ of $[L_i]$ is given by

$$l_{j'} = l_s + l_i\, l_{t,1} \qquad .. \quad (3{\cdot}11)$$

since $j=j'$, we have

$$l_{i,1}\, l_t = l_i\, l_{t,1}, \quad (i, t=2 \ldots m-2) \qquad .. \quad (3{\cdot}12)$$

Keeping i fixed and varying t we get

$$\frac{l_2}{l_1} = \frac{l_3}{l_2} = \ldots = \frac{l_{m-1}}{l_{m-2}} = y \text{ (say)}$$

Remembering that $l_1=1$, we have

$$l_1 = y^0,\ l_2 = y,\ l_3 = y^2, \ldots .\ l_{m-1} = y^{m-2} \qquad .. \quad (3{\cdot}13)$$

Since $l_1, l_2, \ldots l_{m-1}$ are all the non-zero elements of $GF(p^n)$, y must be a primitive element of $GF(p^n)$.

Conversely, if $l_1, l_2, l_3, \ldots l_{m-1}$ satisfy (3·13) where y is a primitive element of GF(p^n) then (3·12) is satisfied. Since the numbers j and j' in the cells (s, t) of $[L_{t-1}]$ and $(s, t+1)$ of $[L_t]$ are determined by (3·10) and (3·11), $j=j'$. Hence the row number t of $[L_t]$, $(t, t=1, 2, \ldots m-2)$. Again the numbers k and k' in the cells $(s, m-1)$ of $[L_{t-1}]$ and $(s, 1)$ of $[L_1]$ are determined by

$$l_s = l_s + l_{t-1}\, l_{m-1}$$

$$l_s' = l_s + l_1\, l_1$$

$$l_{t-1}\, l_{m-1} = y^t\, y^{m-2} = y^{t-1} = l_1\, l_1$$

since $y^{m-1}=y^0=1$, x being a primitive element of GF(p^n). Therefore $k=k'$ which shows that the row number $m-1$ of $[L_{t-1}]$ is identical with the row number 1 of $[L_t]$.

Hence we get the following theorem :—

Theorem IV(A). *The necessary and sufficient condition that the standardised set of orthogonal Latin squares of the theorem II(B) is in the canonical form is that*

$$l_1 = y^0,\ l_2 = y,\ l_3 = y^2,\ \ldots .\ l_{m-1} = y^{m-2} \qquad \ldots \quad (3\cdot13)$$

where y is a primitive element of GF(p^n).

The number of primitive elements of GF(p^n) is $\phi(m-1)$ where ϕ is well known Euler function giving the number of integers less than a given integer and prime to it. Among the $(m-2)!$ identifications for the l_i's in Theorem II (B) exactly $\phi\,(m-1)$ lead to canonical sets. But to a given set correspond just n of these identifications (*cf.* § 1 para.5). Hence the following theorem :—

Theorem IV(B). *The number of canonical sets of orthogonal Latin squares associated to the geometry* PG(2, p^n) *is exactly* $\phi\,(p^n-1)/n$.

2. The identification arrived at in the Theorem IV(A), is the same which has been adopted as the simplest identification in Bose's[1] paper already referred to. The sets obtained in the § 4 of that paper are all in the canonical form (except that owing to the change of notation rows are interchanged with columns). A canonical set can be completely written down by knowing the first square $[L_1]$ of the set. This square can however be quickly written down as soon as the row number 1 of $[L_1]$ is known, by following the rule of § 4, para. 4 of Bose's paper (the change of notation does not affect $[L_1]$ owing to its symmetry), viz :—The row number 0 is composed of the numbers 0, 1, 2, ... $m-1$ in their natural order. Fill in the row number 1. Starting from any number of the row number 1, proceed by single step in the direction of the leading diagonal. If the initial number with which you start in the row number 1 is 0, fill in each successive cell by 0. If however the initial number is other than 0, then fill in each successive cell by putting a number one greater than the number in the preceding cell, remembering however that when the number $m-1$ is reached in a cell, the succeeding cell must be filled by the number 1_s. Complete the square by remembering that there is symmetry about the leading diagonal.

If follows from Theorem IV(B), that the number of 'canonical sets' for the values $m=3, 4, 5, 7, 8, 9, 11, 16, 25, 27$, is $1, 1, 2, 2, 2, 2, 4, 2, 4, 4$, respectively. Let us consider the particular case $m=9$. We shall take the representation (2·33) for the elements of $GF(3^2)$.

The primitive roots are x, x^3, x^5, x^7. The identification in Theorem IV(A), is completely determined by knowing l_2. The identifications $l_2=x$ and $l_2=x^3$ are automorphic and lead to one canonical set. The remaining identifications $l_2=x^5$ and $l_2=x^7$ are automorphic and lead to the second canonical set. Let us determine the row number 1 for the second set, taking the identification determined by $l_2=x^5$. In this case

$$l_0=0 \qquad l_1=1, \qquad l_2=x^5=2x$$

$$l_3=x^2=2x+1, \quad l_4=x^7=x+1, \quad l_5=x^4=2$$

$$l_6=x, \qquad l_7=x^6=x+2, \quad l_8=x^3=2x+2$$

The number in the cell $(0, 1)$ of the Key Latin square $[L_1]$ is of course 1. The number in the cell $(s, 1)$ when $s \geqq 1$ is the number $j=j(s, 1)$ given by

$$l_j=1+l_s$$

Now

$$1+l_1=2 \quad =l_3, \quad 1+l_2=0 \quad =l_0$$

$$1+l_3=2x+1=l_7, \quad 1+l_4=x+1=l_4$$

$$1+l_5=2x+2=l_8, \quad 1+l_7=x \quad =l_6$$

$$1+l_8=x+2=l_7, \quad 1+l_8=2x \quad =l_2$$

Hence the row number 1 of $[L_1]$ is

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

The complete Latin square $[L_1]$ developed according to the rule given before is

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

3. We tabulate below, the row number 1 for all possible canonical sets corresponng to the values $m=3, 4, 5, 7, 8, 9, 11, 16, 25, 27$.

TABLE 6. ROW NUMBER 1, OF THE KEY LATIN SQUARE.

$m=3$.		1, 2, 0.
$m=4$.		1, 0, 3, 2.
$m=5$.	Set I	1, 2, 4, 0, 3.
	Set II	1, 4, 3, 0, 2.
$m=7$.	Set I	1, 3, 5, 2, 0, 6, 4.
	Set II	1, 5, 4, 2, 0, 6, 3.
$m=8$.	Set I	1, 0, 6, 4, 3, 7, 2, 5.
	Set II	1, 0, 4, 7, 2, 6, 5, 3.
$m=9$	Set I	1, 5, 8, 4, 6, 0, 3, 2, 7.
	Set II	1, 5, 3, 8, 7, 0, 4, 6, 2.
$m=11$.	Set I	1, 2, 9, 5, 7, 10, 0, 6, 4, 3, 8.
	Set II	1, 8, 3, 6, 10, 9, 0, 5, 7, 4, 2.
	Set III	1, 4, 10, 8, 5, 7, 0, 3, 2, 6, 9.
	Set IV	1, 10, 4, 9, 8, 6, 0, 2, 5, 7, 3.
$m=16$.	Set I	1, 0, 13, 10, 5, 4, 11, 9, 14, 7, 3, 6, 15, 2, 8, 12.
	Set II	1, 0, 5, 9, 15, 2, 11, 14, 10, 3, 8, 6, 13, 12, 7, 4.
$m=23$.	Set I	1, 19, 4, 10, 18, 6, 16, 13, 24, 5, 23, 22, 20, 0, 9, 12, 14, 21, 17, 7, 11, 2, 15, 8, 3.
	Set II	1, 7, 18, 6, 3, 12, 14, 19, 22, 5, 20, 2, 10, 0, 23, 16, 11, 21, 15, 13, 9, 8, 24, 4, 17.
	Set III	1, 19, 9, 22, 2, 18, 17, 13, 11, 5, 15, 10, 3, 0, 16, 24, 6, 21, 4, 7, 12, 14, 23, 20, 8.
	Set IV	1, 7, 23, 18, 11, 24, 15, 19, 9, 5, 12, 14, 17, 0, 6, 4, 3, 21, 2, 13, 10, 20, 8, 16, 22.
$m=27$.	Set I	1, 14, 10, 22, 2, 19, 18, 12, 5, 16, 4, 7, 11, 3, 6, 17, 26, 23, 21, 8, 24, 0, 13, 15, 25, 20, 9.
	Set II	1, 14, 20, 23, 6, 2, 13, 18, 12, 23, 10, 10, 22, 4, 0, 18, 11, 26, 7, 17, 5, 9, 8, 24, 3, 21, 19.
	Set III	1, 14, 9, 7, 26, 4, 20, 19, 23, 11, 21, 2, 17, 10, 0, 24, 6, 18, 12, 3, 16, 13, 15, 26, 22, 5, 8.
	Set IV	1, 14, 19, 8, 3, 13, 18, 22, 4, 20, 7, 5, 2 11, 0, 25, 17, 21, 24, 12, 23, 16, 10, 9, 26, 6, 18.

REFERENCES

1. BOSE, R. C. : On the application of the properties of Galois Fields to the problem of construction of Hyper-Graeco-Latin Squares. *Sankhyā*, Vol. 3, 1938, pp. 328-338.
2. CARMICHAEL, R. D. : *Introduction to the Theory of Groups of Finite Order*, Boston, U. S. A. and London : Gin and Co., 1937.
3. DICKSON, L. E. : On finite Algebras. *Gothinger Nachrichten*, 1905, pp. 358-394.
4. FISHER, R. A. : *The Design of Experiments*, Edinburgh : Oliver and Boyd, 2nd Edition, 1937.
5. FISHER, R. A. and YATES, F. : *Statistical Tables*. Edinburgh : Oliver and Boyd, 1938.
6. LEVI, F. W. : *Algebra*. Vol. I. Calcutta University Publication. (In the press).
7. NORTON, H. W. : The 7 × 7 squares. *Annals of Eugenics*, Vol. 9, 1939, pp. 269-307.
8. STEVENS, W. L. : The completely orthogonalised Latin Square. *Annals of Eugenics*, Vol. 9, 1939, pp. 82-93.
9. VEBLEN, O. and MACLAGAN-WEDDERBURN, F. H. : Non-Desarguesian and non-Pascalian geometries. *Trans. American. Math. Soc.* Vol. 8, 1907, pp. 379-388.

[*Paper received : 12 November, 1941.*]