The Annals of Mathematical Statistics
1970, Vol. 41, No. 5, 1530–1540

ON THE EQUIVALENCE OF MANN'S GROUP AUTOMORPHISM METHOD OF CONSTRUCTING AN $O(n, n-1)$ SET AND RAKTOE'S COLLINEATION METHOD OF CONSTRUCTING A BALANCED SET OF L-RESTRICTIONAL PRIME-POWERED LATTICE DESIGNS

BY A. HEDAYAT AND W. T. FEDERER

Cornell University

0. Summary. This paper demonstrates the direct relationship which exists between $O(p^m, p^m-1)$ sets and a balanced set of ℓ-restrictional lattice designs for p^m treatments. For instance, we will show that

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

which, as has been shown by Raktoe [5] completely specifies a balanced set of 2-restrictional lattice designs for $7^2 = 49$ treatments, will also completely characterize a set of 48 mutually orthogonal latin squares of order 49, i.e. an $O(49, 48)$ set. In other words, if our interest is to exhibit an $O(49, 48)$ set, the above 2×2 matrix will do the job. Strangely enough, as will be shown, A also completely characterizes an $O(4, 3)$ set.

Note that, since a balanced set of 1-restrictional lattice designs is simply a BIB design, this paper shows in particular a different proof for the known equivalence of the $O(p^m, p^m-1)$ sets with a class of resolvable BIB designs. Consequently, the content of this paper will be useful for those who are concerned with tabulating the designs or writing an efficient program for generating designs on a computer.

1. Definitions.

DEFINITION 1.1. Let L_i be a latin square of order n on an n-set Σ_i, $i = 1, 2, \cdots, t$. Then the set $S = \{L_1, L_2, \cdots, L_t\}$ is said to be a mutually orthogonal set of t latin squares if the projection of the superimposed form of the t latin squares on any two n-sets Σ_i and Σ_j, $i \neq j$, forms a permutation of the Cartesian product set of Σ_i and Σ_j, viz., $\Sigma_i \times \Sigma_j$. Such a set is denoted as an $O(n, t)$ set. For example the following set is an $O(3, 2)$ set.

$$S = \left\{ L_1 = \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1, \\ 3 & 1 & 2 \end{matrix} \qquad L_2 = \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix} \right\}.$$

DEFINITION 1.2. A collection of r ℓ-way tables each of dimension $v_1, v_2, \cdots, v_\ell$ filled out with $v_1 v_2 \cdots v_\ell = V$ distinct objects is said to be an ℓ-restrictional balanced lattice design if the collection is a BIB with respect to each dimension and r is

Received July 31, 1969.

minimal. For example the following collection of seven 2-way tables each of dimensions 4 and 2 filled out with $1, 2, \cdots, 8$ is a 2-restrictional balanced lattice design.

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

Note that the above arrangement is a BIB with respect to both rows ($v = 8$, $b = 28$, $k = 2$, $r = 7$, $\lambda = 1$) and columns ($v = 8$, $b = 14$, $k = 4$, $r = 7$, $\lambda = 3$). Note also that a 1-restrictional balanced lattice design is simply a classical BIB design.

2. The results. Mann [3] proved the following theorem:

THEOREM 2.1. *Let $G = \{a_1 = e \text{ the identity}, a_2, \cdots, a_n\}$ be a group of order n and let α be an automorphism of order t on G. Then*

(1) *$S = \{L_1, L_2, \cdots, L_t\}$ is an $O(n, t)$ set, where*

$$L_i = \begin{array}{cccc} e & a_2 & \cdots & a_n \\ \alpha^i(a_2) & \alpha^i(a_2)a_2 & \cdots & \alpha^i(a_2)a_n \\ \alpha^i(a_3) & \alpha^i(a_3)a_2 & \cdots & \alpha^i(a_3)a_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^i(a_n) & \alpha^i(a_n)a_2 & \cdots & \alpha^i(a_n)a_n \end{array} \quad i = 1, 2 \cdots, t.$$

(2) *If in particular $t = n-1$, then one can simplify the construction of an $O(n, n-1)$ set from the following latin square by a cyclic permutation of its last $n-1$ rows.*

$$L_0 = \begin{array}{ccccc} e & \alpha(a_2) & \alpha^2(a_2) & \cdots & \alpha^t(a_2) \\ \alpha(a_2) & \alpha(a_2)\alpha(a_2) & \alpha(a_2)\alpha^2(a_2) & \cdots & \alpha(a_2)\alpha^t(a_2) \\ \alpha^2(a_2) & \alpha^2(a_2)\alpha(a_2) & \alpha^2(a_2)\alpha^2(a_2) & \cdots & \alpha^2(a_2)\alpha^t(a_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^t(a_2) & \alpha^t(a_2)\alpha(a_2) & \alpha^t(a_2)\alpha^2(a_2) & \cdots & \alpha^t(a_2)\alpha^t(a_2) \end{array}$$

Note that a_2 can be any member of G except e.

We see, therefore, that by means of Theorem 2.1 we can construct an $O(n, t)$ set if we can find a group G and an automorphism α of order t. In particular if $t = n-1$ the whole task of construction reduces to the construction of L_0 since the other $n-2$ latin squares can easily be derived from L_0 as described above.

Mann [3] stated that if G is an elementary abelian p-group then *it can be shown that every such G admits an automorphism α of order $n-1$* and hence we can construct an $O(n, n-1)$ set based on such G and α. Mann [3] did not give a specific procedure for the construction of these automorphisms. He only exhibited such an automorphism for $n = 8, 9, 16, 25$, and 27. Here we will present a general method of constructing such an automorphism for any $n = p^m$. In particular we will exhibit such automorphisms for the following n.

$$n = 2^m, \quad m = 2, 3, \cdots, 9$$

$$n = 3^m, \quad m = 2, 3, \cdots, 6$$

$$n = 5^m, \quad m = 2, 3, 4$$

$$n = 7^m, \quad m = 2, 3$$

$$n = 11^2, 13^2, 17^2, 19^2, 23^2, 29^2, \text{ and } 31^2.$$

This will then perhaps be the largest table that has ever been produced so far for $O(n, n-1)$ sets.

Note that there is no loss of generality if we limit ourselves to the following elementary abelian p-group of order $n = p^m$.

$$G^* = \{(b_1 b_2 \cdots b_m), b_j = 0, 1, 2, \cdots, p-1, j = 1, 2, \cdots, m\}.$$

The binary operation on G^* is addition mod p componentwise, viz. $(b_1 b_2 \cdots b_m) + (b_1' b_2' \cdots b_m') = (c_1 c_2 \cdots c_m)$ where $c_i = b_i + b_i' \pmod p$. Note that the elements of G^* are simply the treatment combinations of m factors each at p levels. This is why we have chosen this particular elementary abelian p-group; it has a well-known structure to those who are concerned with design construction. Note also that G^* is the direct product of m Galois fields, each of order p.

The generator set for every elementary abelian p-group of order p^m consists of m elements, and for uniformity, we may choose the following ordered generator set for G^*.

$$g = \{(100\cdots 0), (0100\cdots 0), \cdots, (00\cdots 010), (00\cdots 01)\}.$$

Note that the structure of every automorphism α on G^* is completely defined if we know the image of each element of g under α. G^* is a vector space of dimension m over $GF[p]$.

Before proceeding further we need the following known theorem:

THEOREM 2.2. *Let G be an elementary abelian p-group of order $n = p^m$. Then Auto G is isomorphic to the (multiplicative) group of all non-singular $m \times m$ matrices with entries in the field of integers* mod p.

Therefore, the construction of an automorphism of order $n-1$ for G^* is equivalent to the construction of an $m \times m$ matrix A such that $A^{n-1} = I$ but $A^t \neq I$ if t is not a multiple of $n-1$, over the field of integers mod p.

We know from linear algebra that if ϕ is a linear map on a vector space V and if $x \in V$ such that $x \neq 0$ but $\phi(x) = x$, then 1 is an eigenvalue of ϕ. Moreover, if $\{\lambda_1, \lambda_2, \cdots, \lambda_t\}$ is the set of eigenvalues of ϕ, then $\{\lambda_1^s, \lambda_2^s, \cdots, \lambda_t^s\}$ is the set of eigenvalues of ϕ^s. Therefore, for our problem we must find a linear map on G^* with a set of eigenvalues λ_i having the property that for each i, $\lambda_i^s \neq 1 \pmod{p}$ for all $s = 1, 2, \cdots, n-2$ and $\lambda_i^{n-1} = 1$. To do so let F be a $GF[p^m]$ and let β be a generator of the multiplicative cyclic group of $GF[p^m]$, i.e. $\beta^i \neq 1$, $i = 1, 2, \cdots, n-2$ while $\beta^{n-1} = 1$. Let $f(x)$ be a monic irreducible polynomial over $GF[p]$ for β. Note that $f(x)$ has degree m. β is sometimes called a primitive root or mark of F. Now if we let A be the companion matrix for β, then A has the desired property.

EXAMPLE. Let us find an automorphism of order 3 for $G^* = \{(00), (01), (10), (11)\}$. It is sufficient by previous arguments to find a 2×2 matrix A of order 3 over the field of integer mod 2. Let $GF(2^2) = \{0, 1, \beta, \beta+1\}$ with following multiplication $(\cdot)$ and addition $(+)$ tables:

$\cdot$	0	1	β	$\beta+1$
0	0	0	0	0
1		1	β	$\beta+1$
β			$\beta+1$	1
$\beta+1$				β

$+$	0	1	β	$\beta+1$
0	0	1	β	$\beta+1$
1		0	$\beta+1$	β
β			0	1
$\beta+1$				0

Note that β is a primitive root for $GF[2^2]$ and $f(x) = x^2+x+1$ is a monic irreducible polynomial for β, since $f(\beta) = \beta^2+\beta+1 = \beta+1+\beta+1 \equiv 0 \pmod{2}$. The companion matrix associated with $f(x)$ is

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

As a check:

$$A^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{over} \quad GF(2),$$

$$A^3 = A^2A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{over} \quad GF(2).$$

Let us now determine the image of the ordered generator set $g = \{(10), (01)\}$ under A.

$$Ag = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} (10) \\ (01) \end{bmatrix} = \begin{bmatrix} (01) \\ (10)+(01) \end{bmatrix} = \begin{bmatrix} (01) \\ (11) \end{bmatrix}.$$

Therefore, $A(10) = (01)$, $A(01) = (11)$, and since $(11) = (10)+(01)$, $(00) = 2(10)+2(01)$ then we have $A(11) = (01)+(11) = (10)$, $A(00) = 2(01)+2(11) = (02)+(22) = (00)$.

Now we have a group G^* of order 4 and an automorphism of order 3 on G^*. Therefore, we can now construct an $O(4, 3)$ set. Since $e = (00)$ for our G^* then letting $a_2 = (10)$ in Theorem 2.1 we obtain

$$L_0 = \begin{matrix} (00) & A(10) & A^2(10) & A^3(10) \\ A(10) & A(10)A(10) & A(10)A^2(10) & A(10)A^3(10) \\ A^2(10) & A^2(10)A(10) & A^2(10)A^2(10) & A^2(10)A^3(10) \\ A^3(10) & A^3(10)A(10) & A^3(10)A^2(10) & A^3(10)A^3(10) \end{matrix}$$

$$= \begin{matrix} (00) & (01) & (11) & (10) \\ (01) & (00) & (10) & (11) \\ (11) & (10) & (00) & (01) \\ (10) & (11) & (01) & (00) \end{matrix}.$$

The other two latin squares are obtained by a cyclic permutation of the last three rows of L_0. Thus

$$L_1 = \begin{matrix} (00) & (01) & (11) & (10) \\ (10) & (11) & (01) & (00) \\ (01) & (00) & (10) & (11) \\ (11) & (10) & (00) & (01) \end{matrix} \quad \text{and} \quad L_2 = \begin{matrix} (00) & (01) & (11) & (10) \\ (11) & (10) & (00) & (01) \\ (10) & (11) & (01) & (00) \\ (01) & (00) & (10) & (11) \end{matrix}.$$

To simplify the notation we set $(00) = 1, (01) = 2, (11) = 3, (10) = 4$ to obtain

$$L_0 = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix}, \quad L_1 = \begin{matrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{matrix}, \quad L_2 = \begin{matrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{matrix}.$$

Raktoe [5], in addition to other results, showed that:

THEOREM 2.3. *For any* $\mathfrak{l}$*-restrictional lattice design* $s^m = \prod_{i=1}^{\mathfrak{l}} s^{r_i}$ *the construction of a balanced set of arrangements is equivalent to the construction of a cyclic collineation of order* $\alpha = (s^m - 1)/(s-1)$.

By considering Mazumdar's results [4] and the method of construction of an automorphism of order $n-1$ which was presented above, we have in effect shown the equivalence of Mann's [3] group automorphism method of constructing an

$O(n, n-1)$ set and Raktoe's [5] collineation method of constructing a balanced set of ℓ-restrictional prime-powered lattice designs. We can now summarize the above results in the following theorem.

THEOREM 2.4. *The existence of a collineation of order* $(p^m-1)/(p-1)$ *is equivalent to the existence of an* $O(p^m, p^m-1)$ *set.*

We exhibit in Table 1 a generating matrix of order $n-1 = p^m - 1$ with entries from $GF[p]$ for those n promised before. These generating matrices are the same as those exhibited by Raktoe [5] for the construction of a balanced set of ℓ-restrictional lattice designs.

TABLE 1

Generating Matrix

n	Generator	Order	n	Generator	Order
2^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	3	2^3	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$	7
2^4	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	15	2^5	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$	31
2^6	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$	63	2^7	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	127
2^8	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$	255	2^9	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$	511
3^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	8	3^3	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$	26

TABLE 1—*continued*

n	Generator	Order	n	Generator	Order
3^4	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	80	3^5	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$	242
3^6	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$	728	5^3	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 2 & 0 \end{bmatrix}$	124
5^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	24	7^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	48
5^4	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 3 & 3 & 0 & 3 \end{bmatrix}$	624	11^2	$\begin{bmatrix} 0 & 1 \\ 3 & 3 \end{bmatrix}$	120
7^3	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 2 & 0 \end{bmatrix}$	342	13^2	$\begin{bmatrix} 0 & 1 \\ 5 & 5 \end{bmatrix}$	168
17^2	$\begin{bmatrix} 0 & 1 \\ 5 & 5 \end{bmatrix}$	288	19^2	$\begin{bmatrix} 0 & 1 \\ 4 & 4 \end{bmatrix}$	360
23^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	528	27^2	$\begin{bmatrix} 0 & 1 \\ 3 & 3 \end{bmatrix}$	728
29^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	840	31^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	960

REMARK. Note that our usage of the word "order" differs from that of Raktoe [5]. For instance, $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ associated with 3^2, which is of order 8 to us, is of order $(3^2-1)/(3-1) = 4$ to Raktoe. In fact, if a generating matrix is of order $(p^m-1)/(p-1)$ to Raktoe it is of order (p^m-1) to us. This is so because if α is a collineation on a finite projective geometry which is based on a $GF[p^m]$, then the image of every point and line is invariant under multiplication of α by non-zero elements of $GF[p^m]$.

Before closing this section we exhibit L_0 and hence a complete set for $n = 2^3$ and $n = 3^2$ using the related generating matrices given in the above list. We accept this task mainly for two reasons. First, to further clarify the idea of this section, and secondly, to compare the derived $O(8, 7)$ and $O(9, 8)$ sets with those exhibited by Fisher and Yates [1].

$$n = 2^3 = 8$$

$$G^* = \{(000), (001), (010), (011), (100), (101), (110), (111)\},$$

$$g = \{(100), (010), (001)\} \quad \text{and} \quad A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

$$Ag = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} (100) \\ (010) \\ (001) \end{bmatrix} = \begin{bmatrix} (010) \\ (001) \\ (101) \end{bmatrix}.$$

Let a_2 in Theorem 2.1 be (100). Then since

$$\begin{aligned}
&A(100) = (010), \; A^2(100) = (001), \; A^3(100) = (101), \\
&A^4(100) = A(101) = A[(100)+(001)] = A(100)+A(001) \\
&\qquad = (010)+(101) = (111), \\
&A^5(100) = A(111) = A[(100)+(010)+(001)] = A(100)+A(010)+A(001) \\
&\qquad = (010)+(001)+(101) = (110), \\
&A^6(100) = A(110) = A[(100)+(010)] = A(100)+A(010) \\
&\qquad = (010)+(001) = (011), \\
&A^7(100) = A(011) = A[(010)+(001)] = A(010)+A(001) \\
&\qquad = (001)+(101) = (100)
\end{aligned}$$

as expected since A is of order 7. Therefore, we obtain L_0 as follows:

$$L_0 = \begin{matrix}
(000) & (010) & (001) & (101) & (111) & (110) & (011) & (100) \\
(010) & (000) & (011) & (111) & (101) & (100) & (001) & (110) \\
(001) & (011) & (000) & (100) & (110) & (111) & (010) & (101) \\
(101) & (111) & (100) & (000) & (010) & (011) & (110) & (001) \\
(111) & (101) & (110) & (010) & (000) & (001) & (100) & (011) \\
(110) & (100) & (111) & (011) & (001) & (000) & (101) & (010) \\
(011) & (001) & (010) & (110) & (100) & (101) & (000) & (111) \\
(100) & (110) & (101) & (001) & (011) & (010) & (111) & (000)
\end{matrix}.$$

Setting (000) = 1, (010) = 2, (001) = 3, (101) = 4, (111) = 5, (110) = 6, (011) = 7,

(100) = 8, then L_0 in a compact form will be:

$$L_0 = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 7 & 5 & 4 & 8 & 3 & 6 \\ 3 & 7 & 1 & 8 & 6 & 5 & 2 & 4 \\ 4 & 5 & 8 & 1 & 2 & 7 & 6 & 3 \\ 5 & 4 & 6 & 2 & 1 & 3 & 8 & 7 \\ 6 & 8 & 5 & 7 & 3 & 1 & 4 & 2 \\ 7 & 3 & 2 & 6 & 8 & 4 & 1 & 5 \\ 8 & 6 & 4 & 3 & 7 & 2 & 5 & 1 \end{matrix}.$$

Now we can derive $L_1, L_2, \cdots, L_6$ from L_0 by a cyclic permutation of the last 7 rows of L_0.

$$L_1 = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 6 & 4 & 3 & 7 & 2 & 5 & 1 \\ 2 & 1 & 7 & 5 & 4 & 8 & 3 & 6 \\ 3 & 7 & 1 & 8 & 6 & 5 & 2 & 4 \\ 4 & 5 & 8 & 1 & 2 & 7 & 6 & 3 \\ 5 & 4 & 6 & 2 & 1 & 3 & 8 & 7 \\ 6 & 8 & 5 & 7 & 3 & 1 & 4 & 2 \\ 7 & 3 & 2 & 6 & 8 & 4 & 1 & 5 \end{matrix}, \qquad L_2 = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 2 & 6 & 8 & 4 & 1 & 5 \\ 8 & 6 & 4 & 3 & 7 & 2 & 5 & 1 \\ 2 & 1 & 7 & 5 & 4 & 8 & 3 & 6 \\ 3 & 7 & 1 & 8 & 6 & 5 & 2 & 4 \\ 4 & 5 & 8 & 1 & 2 & 7 & 6 & 3 \\ 5 & 4 & 6 & 2 & 1 & 3 & 8 & 7 \\ 6 & 8 & 5 & 7 & 3 & 1 & 4 & 2 \end{matrix},$$

and so on. Note the way L_1 is derived from L_0: Except for the first rows of L_0 and L_1, which are identical, the ith row of L_0 becomes the $(i+1)$th rows of L_1, and the last row of L_0 becomes the second row of L_1. In general L_j is derived from L_{j-1} in the same fashion as L_1 is derived from L_0.

$$n = 3^2 = 9$$

$$G^* = \{(00), (01), (02), (10), (11), (12), (20), (21), (22)\}$$

$$g = \{(10), (01)\} \quad \text{and} \quad A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$Ag = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} (10) \\ (01) \end{bmatrix} = \begin{bmatrix} (01) \\ (11) \end{bmatrix}.$$

Let a_2 in Theorem 2.1 be (10). Then following similar steps to those given in the case of $m = 2^3$ we obtain L_0 as follows:

$$L_0 = \begin{array}{ccccccccc} 00 & 01 & 11 & 12 & 20 & 02 & 22 & 21 & 10 \\ 01 & 02 & 12 & 10 & 21 & 00 & 20 & 22 & 11 \\ 11 & 12 & 22 & 20 & 01 & 10 & 00 & 02 & 21 \\ 12 & 10 & 20 & 21 & 02 & 11 & 01 & 00 & 22 \\ 20 & 21 & 01 & 02 & 10 & 22 & 12 & 11 & 00 \\ 02 & 00 & 10 & 11 & 22 & 01 & 21 & 20 & 12 \\ 22 & 20 & 00 & 01 & 12 & 21 & 11 & 10 & 02 \\ 21 & 22 & 02 & 00 & 11 & 20 & 10 & 12 & 01 \\ 10 & 11 & 21 & 22 & 00 & 12 & 02 & 01 & 20 \end{array}.$$

By setting $(00) = 1$, $(01) = 2$, $(11) = 3$, $(12) = 4$, $(20) = 5$, $(02) = 6$, $(22) = 7$, $(22) = 8$, and $(10) = 9$ we obtain L_0 in a compact form as follows:

$$L_0 = \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 4 & 9 & 8 & 1 & 5 & 7 & 3 \\ 3 & 4 & 7 & 5 & 2 & 9 & 1 & 6 & 8 \\ 4 & 9 & 5 & 8 & 6 & 3 & 2 & 1 & 7 \\ 5 & 8 & 2 & 6 & 9 & 7 & 4 & 3 & 1 \\ 6 & 1 & 9 & 3 & 7 & 2 & 8 & 5 & 4 \\ 7 & 5 & 1 & 2 & 4 & 8 & 2 & 9 & 6 \\ 8 & 7 & 6 & 1 & 3 & 5 & 9 & 4 & 2 \\ 9 & 3 & 8 & 7 & 1 & 4 & 6 & 2 & 5 \end{array}.$$

Now we can derive $L_1, L_2, \cdots, L_7$ by a cyclic permutation of the last 8 rows of L_0 (see the description given for 8).

$$L_1 = \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 8 & 7 & 1 & 4 & 6 & 2 & 5 \\ 2 & 6 & 4 & 9 & 8 & 1 & 5 & 7 & 3 \\ 3 & 4 & 7 & 5 & 2 & 9 & 1 & 6 & 8 \\ 4 & 9 & 5 & 8 & 6 & 3 & 2 & 1 & 7 \\ 5 & 8 & 2 & 6 & 9 & 7 & 4 & 3 & 1 \\ 6 & 1 & 9 & 3 & 7 & 2 & 8 & 5 & 4 \\ 7 & 5 & 1 & 2 & 4 & 8 & 3 & 9 & 6 \\ 8 & 7 & 6 & 1 & 3 & 5 & 9 & 4 & 2 \end{array}, \qquad L_2 = \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 6 & 1 & 3 & 5 & 9 & 4 & 2 \\ 9 & 3 & 8 & 7 & 1 & 4 & 6 & 2 & 5 \\ 2 & 6 & 4 & 9 & 8 & 1 & 5 & 7 & 3 \\ 3 & 4 & 7 & 5 & 2 & 9 & 1 & 6 & 8 \\ 4 & 9 & 5 & 8 & 6 & 3 & 2 & 1 & 7 \\ 5 & 8 & 2 & 6 & 9 & 7 & 4 & 3 & 1 \\ 6 & 1 & 9 & 3 & 7 & 2 & 8 & 5 & 4 \\ 7 & 5 & 1 & 2 & 4 & 8 & 3 & 9 & 6 \end{array},$$

and so on.

The $O(8, 7)$ and $O(9, 8)$ sets exhibited by Fisher and Yates [1] also have the property that each latin square in the given set can be obtained from any other member of the set by a reshuffling of the rows. However, Fisher and Yates have given no procedural rules to accomplish this. Hence their sets do not possess the simple property that it suffices to have but one latin square of the set.

REFERENCES

[1] FISHER, R. A. and YATES, F. (1953). *Statistical Tables for Biological, Agricultural and Medical Research*, (4th ed.). Oliver and Boyd, Edinburgh.

[2] HEDAYAT, A. (1969). On the theory of the existence, non-existence, and the construction of mutually orthogonal F-squares and latin squares. Ph. D. thesis, Cornell Univ.

[3] MANN, H. B. (1943). On the construction of sets of orthogonal latin squares. *Ann. Math. Statist.* **14** 401–414.

[4] MAZUMDAR, S. (1967). On the construction of cyclic collineations for obtaining a balanced set of L-restrictional prime powered lattice designs. *Ann. Math. Statist.* **38** 1293–1295.

[5] RAKTOE, B. L. (1967). Application of cyclic collineations to the construction of balanced L-restrictional prime powered lattice designs. *Ann. Math. Statist.* **38** 1127–1141.