APPLICATION OF CYCLIC COLLINEATIONS TO THE CONSTRUCTION OF BALANCED *L*-RESTRICTIONAL PRIME POWERED LATTICE DESIGNS[1]

By B. L. Raktoe

Cornell University

1. Summary. The main problem encountered with any s^m lattice design, where $s(= p^n)$ is a prime positive integer, is the construction of a balanced lattice so that after ordering the experimenter may select a best set of arrangements. When s and m are large the usual method of construction becomes quite laborious. The object of this paper is to develop a method of obtaining a balanced set of arrangements by means of cyclic collineations on the finite projective geometry $PG(k, s)$, where $k = m - 1$.

Considerations are to be limited to collineations whose characteristic matrices $A(\rho) = A - \rho I$ have a single non-trivial invariant factor. The Smith canonical form of $A(\rho)$ is then diagonal $(1, 1, \cdots, 1, f_m(\rho))$ and thus we can limit consideration to the associated rational canonical form. Such matrices can be generated and the orders found by electronic computers for any s^m lattice.

It is shown that with proper choice of $GF(s)$ any balanced l-restrictional s^m lattice is given by $\alpha = \sum_{i=0}^{m-1} s^i$ arrangements. Associating with the α arrangements the α powers of a cyclic collineation in rational canonical form of order α it is shown that the generators of the confounding scheme in each arrangement can immediately be taken from the columns of the respective powers of the matrix of the cyclic collineation.

Balanced arrangements for lattices with $s^m < 1000$ are typified by presenting the associated cyclic collineations of order α.

2. Introduction. Yates (1937) stated that a four restrictional lattice design for s^4 treatments could be obtained by setting up a lattice square design with s^2 split plot treatments arranged in a lattice square design. Kempthorne (1952) suggested that a two restrictional lattice design could be constructed for s^m treatments in s^r rows and s^c columns where $s = p^n$ is a power of a prime positive integer and r, c, and m are positive integers such that $r + c = m$; he constructed a specific example of three arrangements for 2^5 treatments in 2^2 rows and 2^3 columns. Such a design as the latter one was denoted a lattice rectangle design by NaNagara (1957).

In the study of designs of the above type the first problem encountered was the construction of a minimal set of arrangements such that treatment association in the various blockings was balanced. Or, likening the s^m treatments in a

Received 14 September 1964; revised 27 February 1967.

[1] This paper is based on the author's Ph.D. thesis, presented to the Graduate School of Cornell University for partial fulfillment of his Ph.D. degree in Biometry.

lattice rectangle design to a factorial arrangement, this means that each effect will be confounded an equal number of times in the rows and an equal number of times in the columns. Such a confounding scheme is called a *balanced lattice rectangle.*

It is obvious that the construction of balanced lattice designs is an enumerative problem, which is encountered in any l-restrictional lattice design with s^m treatments and is for example denoted in Carmichael (1956) as the construction of tactical configurations. In the construction of an l-restrictional lattice design or for that matter in an s^m factorial system, there are basically two approaches, one being the finite geometrical method and the other the finite Abelian group theoretic approach. For example, Bose and Kishen (1940) utilized finite geometrical methods, while Fisher (1942) used finite Abelian group theory in treating the confounding problem in an s^m factorial with s^k blocks of s^{m-k} plots each. Kishen (1948) showed that these two methods were exactly equivalent by using the fact given in Carmichael (1956), that every finite m-dimensional Euclidean geometry $EG(m, s = p^n)$ is capable of a concrete representation by means of an Abelian group G or order s^m and type $(1, 1, \cdots, 1)$. A lucid summary of these two methods and their relationship in their application to the above confounding problem is given by Kishen (1958).

The aim of this paper is to construct balanced l-restrictional lattices, $l \leqq m$, using the finite geometrical approach, more specifically cyclic collineations on the finite projective geometry $PG(k, s)$. It will be shown that any specified balanced l-restrictional lattice design of s^m treatments can be obtained from the powers of a specified cyclic collineation. This approach leads to an easy solution of the balancing problem and lends itself to electronic computer treatment. Also, a list of cyclic collineations is presented to characterize all possible l-restrictional lattices for $s^m < 1000$.

3. Number of arrangements for balancing an l-restrictional prime powered lattice design. In this section we establish a formula for the required number of arrangements for a balanced l-restrictional s^m lattice, $l \leqq m$, so that, for example, several blanks in Federer (1955), Table XI-2, can be filled easily. Before doing that let us state the notions and definitions formally.

Denote by $PG(m - 1, s = p^n)$ the $(m - 1)$-dimensional analytic projective geometry consisting of m-tuples $(x_0 \, x_1 \cdots x_{m-1})$ based on the Galois field $GF(s)$. We know (see Kempthorne (1952)), that the pseudo-effects in a $s^m = (p^n)^m$ lattice design are 1:1 correspondence with the points of $PG(m - 1, s)$.

For example, consider the $(2^2)^3 = (2^2)^{2+1}$ lattice and associate with it the 2-dimensional $PG(2, 2^2)$. We know (see Dickson (1958) or Carmichael (1956)) that $GF(2^2)$ is found by taking residues of polynomials with coefficients in the ring of integers, modulo 2 and modulo the mod 2 irreducible polynomial $x^2 + x + 1$ (usually written as $F(x) = f(x)$ (modd 2, $x^2 + x + 1$). These residues are of the form $ax + b$, where a and b are in $GF(2)$. Hence we obtain the following $GF(2^2)$, where x is a primitive mark: $\{0 = 0, x^0 = 1, x = x, x^2 = x + 1\}$.

The addition and multiplication tables for $GF(2^2)$ are:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1		0	$x+1$	x
x			0	1
$x+1$				0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1		1	x	$x+1$
x			$x+1$	1
$x+1$				x

Identifying the levels 0, 1, 2, 3 of the 3 factors in the $(2^2)^3 = 4^3$ lattice with the marks 0, 1, x, $x + 1$ respectively of $GF(2^2)$, we have immediately, that the pseudo-effects A, B, C, AB, AB^2, AB^3, AC, AC^2, AC^3, BC, BC^2, BC^3, ABC, ABC^2, ABC^3, AB^2C, AB^2C^2, AB^2C^3, AB^3C, AB^3C^2, AB^3C^3 correspond respectively to the points (100), (010), (001), (110), (120), (130), (101), (102), (103), (011), (012), (013), (111), (112), (113), (121), (122), (123), (131), (132), (133) of $PG(2, 2^2)$. Here we have used the convention that in any pseudo-effect the first factor should be at the first power, which corresponds to the fact that in any $PG(m - 1, s)$ we can select a point to represent the class $\rho(x_0 x_1 \cdots x_{m-1})$, where ρ is a non-zero mark of $GF(s)$. Thus in our example (120) represents the class $\rho(120)$, where $\rho = 1, 2$ or 3 of $GF(2^2)$.

Definite the l-restrictional lattice design as $s^m = s^{r_1} \cdot s^{r_2} \cdot \cdots \cdot s^{r_l} = \prod_{i=1}^{l} s^{r_i}$ where $\sum_{i=1}^{l} r_i = m$, denoting that the s^m treatments are allocated to the experimental units according to l restrictions, $l \leqq m$. For example, when $l = 1$, we have the 1-restrictional lattice design $s^m = s^{r_1} \cdot s^{m-r_1}$, i.e., s^r blocks of s^{m-r} plots each; for $l = 2$, $s^m = s^{r_1} \cdot s^{r_2}$ indicates the 2-restrictional lattice design with s^{r_1} rows and s^{r_2} columns; etc.

Since in any l-restrictional lattice design $s^m = \prod_{i=1}^{l} s^{r_i}$ the pseudo-effects have no physical meaning (unless the treatments form a factorial arrangement) we make the convention that with any given l-restrictional lattice design we will always use that $PG(m - 1, s)$ such that $(s^m - 1)/(s - 1)$ and $(s^{r_i} - 1)/(s - 1)$, $i = 1, 2, \cdots, l$ are relatively prime. Thus for the $2^4 = 2^2 \cdot 2^2$ lattice square we would use the $PG(1, 2^2)$ and not the $PG(3, 2)$. This latter geometry would be used for example for the lattice rectangle $2^4 = 2^3 \cdot 2$. This convention and notation will be used throughout the following discussions and results.

Define a balanced l-restrictional lattice design $s^m = \prod_{i=1}^{l} s^{r_i}$ as a lattice design, consisting of a minimal set of arrangements such that each of the $(s^m - 1)/(s - 1)$ pseudo-effects is confounded an equal number of times in each of the l-restrictions. For example, Kempthorne and Federer (1948a) give a method of finding such minimal sets for some simple cases, such as the $3^3 = 3^2 \cdot 3$ and $3^4 = 3^3 \cdot 3$. Kempthorne (1952) gives a suggestion for the 2-restrictional lattice using group theoretical techniques. This method becomes quite laborious for large s and m. It is our object to construct these sets using geometric rather than group-theoretic methods.

Geometrically the problem of constructing a balanced l-restrictional lattice design $s^m = \prod_{i=1}^{l} s^{r_i}$ is equivalent to constructing a minimal set of l-tuples of flats $((r_1 - 1)\text{-flat}\ (r_2 - 1)\text{-flat} \cdots (r_l - 1)\text{-flat})$ such that each point of

$PG(m-1, s)$ is incident γ_i times with the set of $(r_i - 1)$-flats, $i = 1, 2, \cdots, l$, and such that each l-tuple exhausts $PG(m-1, s)$ in the sense that each l-tuple of flats generate the $PG(m-1, s)$. Now let α denote the number of l-tuples in this minimal set, then our problem is equivalent to constructing the tactical configuration

$$\begin{pmatrix} (s^{r_1}-1)/(s-1) & \gamma_1 & (s^{r_2}-1)/(s-1) & \gamma_2 & \cdots & (s^{r_l}-1)/(s-1) & \gamma_l \\ (s^m-1)/(s-1) & \alpha & (s^m-1)/(s-1) & \alpha & \cdots & (s^m-1)/(s-1) & \alpha \end{pmatrix}$$

where α and the γ_i's are to be determined. This notation for a tactical configuration is an extension of the notation used by Winger (1962), whereas Carmichael (1956) would have used the symbol

$$\triangle \begin{matrix} (s^{r_1}-1)/(s-1)\,\gamma_1\,(s^{r_2}-1)/(s-1)\,\gamma_2 \cdots (s^{r_l}-1)/(s-1)\,\gamma_l \\ (s^m-1)/(s-1)\,\alpha\,(s^m-1)/(s-1)\,\alpha \cdots (s^m-1)/(s-1)\,\alpha. \end{matrix}$$

We now are ready to prove the following theorem.

THEOREM 1. *If $s^m = \prod_{i=1}^{l} s^{r_i}$ indicates an l-restrictional lattice then the configuration associated with the balanced case is*

$$\begin{pmatrix} \gamma_1 & \gamma_1 & \gamma_2 & \gamma_2 & \cdots & \gamma_l & \gamma_l \\ \alpha & \alpha & \alpha & \alpha & \cdots & \alpha & \alpha \end{pmatrix},$$

where $\alpha = (s^m-1)/(s-1)$ and $\gamma_i = (s^{r_i}-1)/(s-1)$.

PROOF. We must show that $\alpha = (s^m-1)/(s-1)$ and $\gamma_i = (s^{r_i}-1)/(s-1)$. To show this, let us associate with the l-restrictional lattice design $s^m = \prod_{i=1}^{l} s^{r_i}$ the $PG(m-1, s)$, where according to our convention $(s^m-1)/(s-1)$ and $(s^{r_i}-1)/(s-1)$, $i = 1, 2, \cdots, l$, are relatively prime. We know from Carmichael (1956), pages 347 and 348, that every $PG(m-1, s)$ affords the configuration

$$\begin{pmatrix} (s^{m-1}-1)/(s-1) & (s^{m-1}-1)/(s-1) \\ (s^m-1)/(s-1) & (s^m-1)/(s-1) \end{pmatrix}$$

i.e. this configuration corresponds to the one-restrictional lattice design $s^m = s^{m-1}\cdot s$. Now, because the dual of an $(m-2)$-flat is a point or 0-flat it is clear that we can construct from the $(s^m-1)/(s-1)$, $(m-2)$-flats the resulting $(s^m-1)/(s-1)$ two-tuples ($(m-2)$-flat 0-flat), where the $(s^m-1)/(s-1)$ 0-flats run through the $PG(m-1, s)$. Hence we have the configuration

$$\begin{pmatrix} (s^{m-1}-1)/(s-1) & (s^{m-1}-1)/(s-1) & 1 & 1 \\ (s^m-1)/(s-1) & (s^m-1)/(s-1) & (s^m-1)/(s-1) & (s^m-1)/(s-1) \end{pmatrix},$$

which represents the two-restrictional lattice (or lattice rectangle) $s^m = s^{r_1}\cdot s^{r_2}$, where $r_1 = m-1$ and $r_2 = 1$. In exhibiting this configuration it is enough to exhibit the generators of the flats in each of the two-tuples, i.e. $(m - 1)$ generating points for each of the $(m - 2)$-flats and 1 point for the 0-flat.in each two-tuple. Now ordering these $(s^m - 1)/(s - 1)$ sets of m generators, such that each column runs through the points of the $PG(m - 1, s)$[2] and partitioning each set of m generators into the first r_1, next r_2, etc., and finally the last r_l generators, where $\sum_{i=1}^{l} r_i = m$, it is clear that we have formed $(s^m - 1)/(s - 1)$ l-tuples of flats $((r_1 - 1)$-flat $(r_2 - 1)$-flat $\cdots$ $(r_l - 1)$-flat$)$ with the property that each point is incident now with $(s^{r_i} - 1)/(s - 1)$ of the $(r_i - 1)$-flats, $i = 1, 2, \cdots, l$, i.e. $\alpha = (s^m - 1)/(s - 1)$ and $\gamma_i = (s^{r_i} - 1)/(s - 1)\cdot$Q.E.D.

As an example consider the one-restrictional lattice design $2^3 = 2^2 \cdot 2$, i.e. 8 treatments in 4 blocks of 2 plots each, then associating the $PG(2, 2)$ with this lattice design we have the configuration $\begin{pmatrix} 3 & 3 \\ 7 & 7 \end{pmatrix}$ corresponding to the lines of this geometry. Forming the 7 two-tuples (line point) as indicated in Theorem 1 above, we have immediately the balanced lattice rectangel $2^3 = 4$ rows $\times$ 2 columns with configuration $\begin{pmatrix} 3 & 3 & 1 & 1 \\ 7 & 7 & 7 & 7 \end{pmatrix}$ and explicitly given by:

	Line (1-flat)	Point (0-flat)
1	C, A, AC	BC
2	BC, C, B	ABC
3	ABC, BC, A	AB
4	AB, ABC, C	AC
5	AC, AB, BC	B
6	B, AC, ABC	A
7	A, B, AB	C

Now, note that the generators are written out in such a fashion that each column runs through the 7 points of the $PG(2, 2)$. Forming the seven 3-tuples (0-flat 0-flat 0-flat) we have immediately the three-restrictional lattice design $2^3 = 2^1 \cdot 2^1 \cdot 2^1$ with configuration matrix $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 7 & 7 & 7 & 7 & 7 & 7 \end{pmatrix}$ and confounding pattern:

	0-flat	0-flat	0-flat
1	C	A	BC
2	BC	C	ABC
3	ABC	BC	AB
4	AB	ABC	AC
5	AC	AB	B
6	B	AC	A
7	A	B	C

[2] The existence of an array of m columns and $(s^m - 1)/(s - 1)$ rows such that every point of $PG(m - 1, s)$ occurs once and only once in each column and every row is a set of m generators can be demonstrated by taking the m columns of the matrix of cyclic collineation A of period $(s^m - 1)/(s - 1)$, as the generators of the first row. From the initial row, the succeeding rows can be cyclically developed by premultiplying the generators (regarded as columnvectors) by A. The existence of A follows from James Singer's theorem (*Trans. Amer. Math. Soc.* **43** 377–385).

4. Cyclic collineations and balanced l-restrictional lattice designs. Consider the collineation in the projective group $P(m-1, s)$ in $PG(m-1, s)$. We know (see Carmichael (1956), page 355), that this group comprises all transformations of the form

$$\rho y_i = \sum_{j=1}^{m} \alpha_{ij} x_j$$

where α_{ij} are marks of $GF(s)$ such that the determinant $|\alpha_{ij}| \neq 0$ and ρ stands for the fact that two transformations represent the same collineation if their respective matrices are related by a canonical transformation diagonal $(\rho\, \rho \cdots \rho)$, ρ being a non-zero mark of $GF(s)$. We know that each element of $P(m-1, s)$ transforms the $PG(m-1, s)$ into itself in the sense that flats are transformed into flats and also that the order of $P(m-1, s)$ is $(1/(s-1)) \prod_{i=0}^{m-1} (s^m - s^i)$.

Now consider the l-restrictional lattice design $s^m = \prod_{i=1}^{l} s^{r_i}$. Then from Theorem 1 we know that $(s^m-1)/(s-1)$ l-tuples $((r_1-1)$-flat (r_2-1)-flat $\cdots$ (r_l-1)-flat$)$ represent the balanced case. If we consider only the m generators involved in each such l-tuple, then it is clear that these m generators, written as columns form the $m \times m$ matrix of a collineation. Conversely, it is also clear that every collineation represents m generators. Since every collineation transforms an $(m-1)$-flat into an $(m-1)$-flat and since $(s^m-1)/(s-1)$ such $(m-1)$-flats are required for the balanced case it is obvious that we need $(s^m-1)/(s-1)$ collineations to form a balanced l-restrictional lattice design. Since these $(s^m-1)/(s-1)$ collineations are closed under multiplication and have an inverse, they form a subgroup of $P(m-1, s)$. In fact, since $(s^m-1)/(s-1)$ is a divisor of $(1/(s-1)) \prod_{i=0}^{m-1} (s^m - s^i)$ we know from group theory that such a subgroup exists. There are two possibilities, either the subgroup of order $(s^m-1)/(s-1)$ is cyclic or it is non-cyclic. (This statement and the two preceding ones need not worry us, since from the footnote of Theorem 1 we know that there always exists a matrix of cyclic collineation of period $(s^m-1)/(s-1)$.) It is evident from the fact that each of the m columns of generators represents all points of the $PG(m-1, s)$ and from the fact that every row of m generators exhaust the $PG(m-1, s)$, that if we want to read off such a structure the collineatory subgroup must be cyclic. Hence in order to construct a balanced l-restrictional lattice design all we need is a cyclic collineation of order $(s^m-1)/(s-1)$. This result is stated in the following theorem.

THEOREM 2. *For any l-restrictional lattice design* $s^m = \prod_{i=1}^{l} s^{r_i}$ *the constrvction of a balanced set of arrangements is equivalent to the construction of a cyclic collineation of order* $\alpha = (s^m-1)/(s-1)$.

Geometrically this theorem says that if A is the matrix of a cyclic collineation of order α, then the powers of A (i.e., $A, A^2, A^3, \cdots, A^\alpha = I$) take any point of the $PG(m-1, s)$ through all the points of the $PG(m-1, s)$. Therefore all the jth, $j = 1, 2, \cdots, m$, columns of the α powers of A comprise the α points of the $PG(m-1, s)$. Now in each A^u, $u = 1, 2, \cdots, \alpha$, the first r_1 columns generate an (r_1-1)-flat, the next r_2 columns generate an (r_2-1)-flat and finally the last r_l columns generate an $(r_l - 1)$-flat, where $\sum_{i=1}^{l} r_i = m$. Hence we obtain l-tuples of flats $((r_1 - 1)$-flat $(r_2 - 1)$-flat $\cdots$ $(r_l - 1)$-flat$)$, resulting in α arrangements of an l-restrictional lattice design $s^m = \prod_{i=1}^{l} s^{r_i}$ with configuration matrix

$$\begin{pmatrix} \gamma_1 & \gamma_1 & \gamma_2 & \gamma_2 & \cdots & \gamma_l & \gamma_l \\ \alpha & \alpha & \alpha & \alpha & \cdots & \alpha & \alpha \end{pmatrix},$$

where $\alpha = (s^m - 1)/(s - 1)$, $\gamma_i = (s^{r_i} - 1)/(s - 1)$, $i = 1, 2, \cdots, l$.

The construction of cyclic collineations of order α may be done with an electronic computer. Before proceeding to show how the computer performs this task let us limit ourselves to a relatively small class of collineations by using the following approach.

Consider the collineations $\rho y = Ax$ in the projective group $P(k, s)$ in the $PG(k, s)$. Since $P(k, s)$ is a finite group of order $(1/(s - 1)) \prod_{i=0}^{k} (s^m - s^i)$ we know that every element of $P(k, s)$ generates a cyclic group, whose order divides the order of $P(k, s)$. We shall be concerned with finding an element of $P(k, s)$ of order α, so that by Theorem 2 we can immediately construct balanced l-restrictional lattice designs.

By considering the fixed points for vertices of the fundamental simplex we know (see for example Winger (1962)) that the general collineation in $P(k, s)$ can be written in canonical form:

$$\rho y_i = c_i x_i, \qquad i = 1, 2, \cdots, m,$$

where the c_i's are invariants of ith degree on the coefficients of A satisfying the characteristic equation $(\rho - k_1)(\rho - k_2) \cdots (\rho - k_m) = 0$. Taking the unit point also as a fixed point we get the identical collineation

$$\rho y_i = x_i, \qquad i = 1, 2, \cdots, m,$$

since $c_1 : c_2 : \cdots : c_m = 1$. An immediate consequence of this last case is that if a collineation leaves invariant each of $m + 1$ points, no m of which lie in a $(m - 1)$-flat, then it leaves invariant every point of $PG(k, s)$. If a general collineation in $P(k, s)$ is to be cyclic of order α, then we must have, that the invariants be nth roots of unity, that is, $c_1^{\alpha} = c_2^{\alpha} = \cdots = c^{\alpha} = 1$. The invariant $c_i = (-1)^m$ times the sum of all m-square principal minors of $A = (a_{ij})$, $i, j = 1, 2, \cdots, m$, for example $c_1 = \text{trace } A$, $c_m = |A|$. From this it follows that conditions connecting the invariants can be deduced such that A is cyclic of order α, which imply conditions on the elements of A.

Thus for example in order that the binary collineation in $P(1, s)$ be cyclic of order 2, conditions can be established as follows: If

$$\rho y_1 = a x_1 + b x_2,$$

$$\rho y_2 = c x_1 + d x_2,$$

i.e. $\rho y = Ax$, $a, b, c, d \, \varepsilon \, GF(s)$, then the general canonical form can be written as

$$\rho y = \begin{pmatrix} a + d & 0 \\ 0 & ad - bc \end{pmatrix} x.$$

If the order is to be 2 then from above we must have $(a + d)^2 = (ad - bc)^2 = 1$. Hence:

$$a + d + ad - bc = 0,$$

$$a + d - ad + bc = 0,$$

that is, $a + d = 0$ or simply $c_1 = 0$ in $GF(s)$. Thus if $GF(s) = GF(2)$, a binary cyclic collineation in $P(1, 2)$ is determined by taking any 2×2 matrix such that trace $A = c_1 = 0 \pmod 2$, for example $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Similarly the conditions for a binary cyclic collineation in $P(1, s)$ to be of order 3 or 4 are given by $c_1^2 - c_2 = 0$ and $c_1^2 - 2c_2 = 0$ in $GF(s)$ respectively. For example if $GF(s) = GF(3)$, we see that $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is of order 4 in $P(1, 3)$.

The above procedure for finding conditions on the invarants or equivalently on the elements of A becomes very complex for large m and large order, so that we must look for other avenues of approach.

Consider therefore the subgroup of collineations of the form HAH^{-1}, that is the transforms of A by H, where H, is an element of $P(k, s)$. Then since $|HAH^{-1} - \rho I| = |A - \rho I|$ we see that HAH^{-1} and A have the same characteristic equation and hence the same roots (also called multipliers). Consequently the multipliers are invariants of the collineation. Hence when x is a fixed (or latent) point of A (that is $Ax = cx$, where c is a root of the characteristic equation) we can then say that A carries x into cx, and if H is a collineation that changes x into y then the effect on x when A is transformed by H is that HAH^{-1} carries y into cy. Hence H transforms fixed points of A into fixed points of HAH^{-1}.

From the above we may conclude that when A is cyclic of order α, then HAH^{-1} is also cyclic of order α, since their characteristic equation is the same as are also the invariants in the coefficients of A on which we had found conditions earlier. The above conclusion can be proved directly by noting the following properties of HAH^{-1} (see Turnbull and Aitken (1961)):

(1) $(HAH^{-1})^\alpha = HAH^{-1}HAH^{-1} \cdots HAH^{-1} = HA^\alpha H^{-1}$;

(2) $(HAH^{-1})^{-1} = HA^{-1}H^{-1}$.

The importance of this subgroup of transforms is now evident, since with a suitable choice of H, we can bring A into an operationally nice form. Before proceeding further with our search for cyclic collineations of order α, we quote the following theorems without proofs, since these can be found in most standard texts, such as Turnbull and Aitken (1961), Ayres (1962) and van der Waerden (1950).

THEOREM (a) (Smith Normal Form). *If A is the matrix of a collineation in*

$P(k, s)$ then its characteristic matrix $A(\rho) = \rho I - A$ can be reduced by elementary transformations over $GF(\rho)$ (here $GF(\rho)$ denotes the polynomial domain over $GF(s)$) to the Smith normal form:

$$N(\rho) = \begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & 0 & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & f_j(\rho) & & & \\ & & & & & f_{j+1}(\rho) & & \\ & 0 & & & & & \ddots & \\ & & & & & & & f_m(\rho) \end{bmatrix},$$

where each nontrivial invariant factor $f_i(\rho)$ is monic of degree t_i, $i = j, j + 1, \cdots, m$, and $f_u(\rho)/f_{u+1}(\rho)$, $u = j, j + 1, \cdots, m - 1$.

THEOREM (b). *If A is the matrix of a collineation in $P(k, s)$ then the characteristic and minimum polynomial of A is identical if and only if A has just one nontrivial similarity invariant ($=$ invariant factor).*

DEFINITION (Companion matrix). If A of Theorem (b) has non-trivial similarity invariant $f_m(\rho) = \rho^m + a_{m+1}\rho^{m-1} + \cdots + a_1\rho + a_0$ then by definition the companion matrix of $f_m(\rho)$ is:

$$C(f_m) = -a \quad \text{if} \quad f_m(\rho) = \rho + a$$

and for $m > 1$

$$C(f_m) = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{m-3} & -a_{m-2} & -a_{m-1} \end{bmatrix}$$

Note that the companion matrix $C(f_m)$ of a polynomial $f_m(\rho)$ has $f_m(\rho)$ as both its characteristic and minimum polynomial.

THEOREM (c) (Rational canonical form). *If A is the matrix of a collineation in $P(k, s)$ and if its characteristic matrix $A(\rho) = A - \rho I$ has just one non-trivial invariant factor $f_m(\rho)$ then the companion matrix $C(f_m)$ of $f_m(\rho)$ is similar to A,* i.e. *there exists an H in $P(k, s)$ such that $HAH^{-1} = C(f_m)$, where this last matrix is called the rational canonical form of A.*

Now let us restrict consideration to collineations with matrix A in $P(k, s)$ having only one non-trivial similarity invariant, that is with Smith canonical form (see Theorem (a)):

$$N(\rho) = \begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & 1 & \\ & & & & & f_m(\rho) \end{bmatrix}$$

Then by Theorems (b) and (c) we have immediately that all matrices similar to A have a rational canonical form $HAH^{-1} = C(f_m)$. Earlier considerations show that if A is cyclic of degree α, then so is $HAH^{-1} = C(f_m)$. Since $a_0 = |A| = |HAH^{-1}|$ and A is in $P(k, s)$ we know that $a_0 \neq 0$ in $GF(s)$. Using an electronic computer we can generate the rational canonical forms of Theorem (c) for those A in $P(k, s)$, having *one* non-trivial invariant factor and then find their orders by computation of their powers. Then in view of Theorem 2, the problem is solved by selecting a $C(f_m)$ having the desired order α.

5. Generating matrices for balanced l-restrictional lattice designs for $s^m < 1000$. In the enumeration of those $C(f_m)$ which are cyclic of desired order α it is evident that we need only consider $(s - 1)s^{m-1}$ matrices, since each a_i, $i = 1, 2, \cdots, m - 1$, can be chosen in s ways and a_0 in $(s - 1)$ ways in the non-trivial similarity invariant $f_m(\rho) = \rho_m + a_{m-1}\rho^{m-1} + \cdots + a_1\rho + a_0$. This enumerative work is easily done by an electronic computer, i.e. the computer generates the matrix, finds the power at which it becomes cyclic, stops immediately when a matrix of order α is reached and prints only this last one.

A set of generating matrices for balanced prime-powered l-restrictional lattices for $s^m < 1000$ treatments is given by the following list (a major part of these generators was recently published by W. T. Federer and B. L. Raktoe in a paper entitled "General Theory of Prime-Power Lattice Designs," *J. Amer. Statist. Assoc.* **60** (1965) 891–904):

s^m	*Generator*	*Order*	s^m	*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

s^m	*Generator*	*Order*	s^m	*Generator*	*Order*
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	$\begin{bmatrix} 0&1 \\ 1&1 \end{bmatrix}$	4	3^3	$\begin{bmatrix} 0&1&0 \\ 0&0&1 \\ 1&1&0 \end{bmatrix}$	13
3^4	$\begin{bmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&1&0&0 \end{bmatrix}$	40	3^5	$\begin{bmatrix} 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \\ 1&1&0&0&0 \end{bmatrix}$	121
3^6	$\begin{bmatrix} 0&1&0&0&0&0 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \\ 1&1&0&0&0&0 \end{bmatrix}$	364	4^2	$\begin{bmatrix} 0&1 \\ 2&2 \end{bmatrix}$	5
4^3	$\begin{bmatrix} 0&1&0 \\ 0&0&1 \\ 2&2&2 \end{bmatrix}$	21	4^4	$\begin{bmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 2&2&2&0 \end{bmatrix}$	85
5^2	$\begin{bmatrix} 0&1 \\ 2&2 \end{bmatrix}$	6	5^3	$\begin{bmatrix} 0&1&0 \\ 0&0&1 \\ 2&2&0 \end{bmatrix}$	31
5^4	$\begin{bmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 3&3&0&3 \end{bmatrix}$	156	7^2	$\begin{bmatrix} 0&1 \\ 1&1 \end{bmatrix}$	8
7^3	$\begin{bmatrix} 0&1&0 \\ 0&0&1 \\ 2&2&0 \end{bmatrix}$	57	8^2	$\begin{bmatrix} 0&1 \\ 4&4 \end{bmatrix}$	9
8^3	$\begin{bmatrix} 0&1&0 \\ 0&0&1 \\ 2&2&0 \end{bmatrix}$	73	9^2	$\begin{bmatrix} 0&1 \\ 6&6 \end{bmatrix}$	10
9^3	$\begin{bmatrix} 0&1&0 \\ 0&0&1 \\ 3&3&0 \end{bmatrix}$	91	11^2	$\begin{bmatrix} 0&1 \\ 3&3 \end{bmatrix}$	12
13^2	$\begin{bmatrix} 0&1 \\ 5&5 \end{bmatrix}$	14	16^2	$\begin{bmatrix} 0&1 \\ 2&2 \end{bmatrix}$	17

s^m	*Generator*	*Order*	s^m	*Geeerator*	*Order*
17^2	$\begin{bmatrix} 0 & 1 \\ 5 & 5 \end{bmatrix}$	18	19^2	$\begin{bmatrix} 0 & 1 \\ 4 & 4 \end{bmatrix}$	20
23^2	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	24	25^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	26
27^2	$\begin{bmatrix} 0 & 1 \\ 3 & 3 \end{bmatrix}$	28	29^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	30
31^2	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	32			

For all those cases above where $s = p^n$, with $n > 1$, we have used the following Galois fields. (The addition and multiplication tables are given by Raktoe (1964).)

$GF(2^2)$: $P(x) = x^2 + x + 1$ with primitive mark x; $0 = 0 = 0$, $1 = x^0 = 1$, $2 = x = x$, and $3 = x^2 = x + 1$.

$GF(2^3)$: $P(x) = x^3 + x^2 + 1$ with primitive mark x; $0 = 0 = 0$, $1 = x^0 = 1$, $2 = x = x$, $3 = x^2 = x^2$, $4 = x^3 = x^2 + 1$, $5 = x^4 = x^2 + x + 1$, $6 = x^5 = x + 1$, and $7 = x^6 = x^2 + x$.

$GF(2^4)$: $P(x) = x^4 + x + 1$ with primitive mark x; $0 = 0 = 0$, $1 = x^0 = 1$, $2 = x = x$, $3 = x^2 = x^2$, $4 = x^3 = x^3$, $5 = x^4 = x + 1$, $6 = x^5 = x^2 + x$, $7 = x^6 = x^3 + x^2$, $8 = x^7 = x^3 + x + 1$, $9 = x^8 = x^2 + 1$, $10 = x^9 = x^3 + x$, $11 = x^{10} = x^2 + x + 1$, $12 = x^{11} = x^3 + x^2 + x$, $13 = x^{12} = x^3 + x^2 + x + 1$, $14 = x^{13} = x^3 + x^2 + 1$, and $15 = x^{14} = x^3 + 1$.

$GF(3^2)$: $P(x) = x^2 + x + 2$ with primitive mark x; $0 = 0 = 0$, $1 = x^0 = 1$, $2 = x = x$, $3 = x^2 = 2x + 1$, $4 = x^3 = 2x + 2$, $5 = x^4 = 2$, $6 = x^5 = 2x$, $7 = x^6 = x + 2$, and $8 = x^7 = x + 1$.

$GF(3^3)$: $P(x) = x^3 + 2x + 1$ with primitive mark x; $0 = 0 = 0$, $1 = 1 = 1$, $2 = x = x$, $3 = x^2 = x^2$, $4 = x^3 = x + 2$, $5 = x^4 = x^2 + 2x$, $6 = x^5 = 2x^2 + x + 2$, $7 = x^6 = x^2 + x + 1$, $8 = x^7 = x^2 + 2x + 2$, $9 = x^8 = 2x^2 + 2$, $10 = x^9 = x + 1$, $11 = x^{10} = x^2 + x$, $12 = x^{11} = x^2 + x + 2$, $13 = x^{12} = x^2 + 2$, $14 = x^{13} = 2$, $15 = x^{14} = 2x$, $16 = x^{15} = 2x^2$, $17 = x^{16} = 2x + 1$, $18 = x^{17} = 2x^2 + x$, $19 = x^{18} = x^2 + 2x + 1$, $20 = x^{19} = 2x^2 + 2x + 2$, $21 = x^{20} = 2x^2 + x + 1$, $22 = x^{21} = x^2 + 1$, $23 = x^{22} = 2x + 2$, $24 = x^{23} = 2x^2 + 2x$, $25 = x^{24} = 2x^2 + 2x + 1$, and $26 = x^{25} = 2x^2 + 1$.

$GF(5^2)$: $P(x) = x^2 + x + 2$ with primitive mark x; $0 = 0 = 0$, $1 = 1 = 1$, $2 = x = x$, $3 = x^2 = 4x + 3$, $4 = x^3 = 4x + 2$, $5 = x^4 = 3x + 2$, $6 = x^5 = 4x + 4$, $7 = x^6 = 2$, $8 = x^7 = 2x$, $9 = x^8 = 3x + 1$, $10 = x^9 = 3x + 4$, $11 = x^{10} = x + 4$, $12 = x^{11} = 3x + 3$, $13 = x^{12} = 4$, $14 = x^{13} = 4x$, $15 = x^{14} = x + 2$, $16 = x^{15} = x + 3$, $17 = x^{16} = 2x + 3$, $18 = x^{17} = x + 1$, $19 = x^{18} = 3$, $20 = x^{19} = 3x$, $21 = x^{20} = 2x + 4$, $22 = x^{21} = 2x + 1$, $23 = x^{22} = 4x + 1$, and $24 = x^{23} = 2x + 2$.

The group-theoretic confoundings associated with the powers of the matrices is read off for example as follows:

$2^3 = 2^2 \cdot 2^1$. This is a lattice rectangle with 4 rows and 2 columns and the confounding scheme for the balanced case is:

		Confounded in: Rows	Columns
1	$\begin{bmatrix}0&1&0\\0&0&1\\1&0&1\end{bmatrix} = A$	$C, A,/AC$	BC
2	$\begin{bmatrix}0&0&1\\1&0&1\\1&1&1\end{bmatrix} = A^2$	$BC, C,/B$	ABC
3	$\begin{bmatrix}1&0&1\\1&1&1\\1&1&0\end{bmatrix} = A^3$	$ABC, BC,/A$	AB
4	$\begin{bmatrix}1&1&1\\1&1&0\\0&1&1\end{bmatrix} = A^4$	$AB, ABC,/C$	AC
5	$\begin{bmatrix}1&1&0\\0&1&1\\1&0&0\end{bmatrix} = A^5$	$AC, AB,/BC$	B
6	$\begin{bmatrix}0&1&1\\1&0&0\\0&1&0\end{bmatrix} = A^6$	$B, AC,/ABC$	A
7	$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} = A^7$	$A, B,/AB$	C

In the row confounding above the generators are written first and then the generated pseudo-effect after the slash, /. It is readily seen, as shown in Theorem 2, that the $\alpha = 7$ arrangements are given by the powers of A, which is cyclic of order 7. Also, each pseudo-effect is confounded in 3 arrangements in rows and in 1 arrangement in columns.

For the 1-restrictional lattice in the above case one merely takes either the 1st, 2nd or 3rd column of each of the 7 powers to get a balanced set of arrangements. Note that the column confounding in the 2-restrictional lattice above gives such a confounding scheme for the 1-restrictional lattice.

6. Discussion. The results obtained in the last section are very simple from a construction viewpoint. However, there remain some unsolved problems. One of them is to determine the relation between the collineations in rational canonical form or the invariant factors associated with these and the irreducible polynomials $P(x)$ with primitive mark x in the construction of the Galois fields $GF(s)$. For example, in the 2^m (here $n = 1$) series the invariant factors associated with the matrices in rational canonical form are exactly identical with irreducible polynomials $P(x)$ in the construction of $GF(2^m)$. The multiplicative group in $GF(2^m)$ is generated by x and the cyclic group of matrices is generated by A. Setting up the correspondence $x \rightarrow A$, we have the fact that the cyclic group generated by A is isomorphic to the multiplicative group generated by x of $GF(2^m)$. This remarkable fact does not lead to generalization of cases with $p \neq 2$. But still there may exist analytical methods which will lead to the same result as in Section 4 and hence be more "exact" than the enumerative approach.

Another problem is that of ordering the α arrangements or equivalently the α powers of A, such that the experimenter can choose any best set of r arrangements. It is conjectured here that this task can be handled by use of an electronic computer.

Finally generalization of the analysis to the l-restrictional lattice design is possible within the framework given by Kempthorne and Federer (1948a), (1948b).

7. Acknowledgment. The author wishes to acknowledge the help of Professors W. T. Federer, D. S. Robson, and J. Kiefer in the formulation of the problem and for their constructive comments during the research. Thanks go also to the referees for extremely helpful suggestions for improvement; the two footnotes in the paper are entirely due to them, for which I am deeply indebted.

REFERENCES

Ayers, F. (1962). *Theory and Problems of Matrices*. Schaum, New York.

Blumenthal, L. (1961). *A Modern View of Geometry*. San Francisco and London.

Bose, R. C. and Kishen, K. (1940). On the problem of confounding in the general symmetrical factorial design. *Sankhyā* **5** 21–36.

Carmichael, R. D. (1956). *Introduction to the Theory of Groups of Finite Order*. (First published 1937) Dover, New York.

Dickson, L. (1958). *Introduction to the Theory of Linear Groups*. (First published 1905) Dover, New York.

Federer, W. T. (1955). *Experimental Design—Theory and Applications*. Macmillan, New York.

Federer, W. T. (1949). The general theory of prime-power lattice designs. III. The analysis for p^3 varieties in blocks of p plots with more than 3 replicates. *Biometrics* **5** 144–161.

Federer, W. T. (1950). The general theory of prime-power lattice designs. IV. The analysis for p^4 treatments in blocks of p plots with 4 or more replicates. Cornell Univ. Agr. Exp. Sta. Memoir 299.

Federer, W. T. and Robson, D. S. (1952). General theory of prime-power lattice designs. VI. Incomplete block design and analysis for p^5 varieties in blocks of p^2 plots. Cornell Univ. Agr. Sta. Memoir 309.

Fisher, R. A. (1942). The theory of confounding in factorial experiments in relation to the theory of groups. *Ann. Eugen.* **11** 341–353.

Kempthorne, O. (1952). *The Design and Analysis of Experiments*. Wiley, New York.

Kempthorne, O. and Federer, W. T. (1948a). The general theory of prime-power lattice designs. I. Introduction and designs for p^n varieties in blocks of p plots. *Biometrics* **4** 54–79.

Kempthorne, O. and Federer, W. T. (1948b). The general theory of prime-power lattice designs. II. Designs for p^n varieties in blocks of p^5 plots and in squares. *Biometrics* **4** 109–121.

Kishen, K. (1948). On factorial replication of the general symmetrical factorial design. *J. Indian Soc. Agric. Statist.* **1** 91–106.

Kishen, K. (1958). Presidential address. Recent developments in experimental design. 45th Indian Science Congress, Madras, 1958, 1–32.

Na Nagara, P. (1958). Lattice rectangles for $v = k(k + 1)$ treatments. Ph.D. Thesis, Cornell Univ.

Turnbull, H. W. and Aitken, A. C. (1961). *An Introduction to the Theory of Canonical Matrices*. Dover, New York.

van der Waerden, B. L. (1950). *Modern Algebra*, **2**. Ungar, New York.

Winger, R. M. (1962). *An Introduction to Projective Geometry*. Dover, New York.

Yates, F. (1937). The design and analysis of factorial experiments. *Imp. Bur. Soil. Sci., Tech. Comm.* **35** 1–95.

Yates, F. (1940). Lattice squares. *J. Agric. Sci.* **30** 672–687.