ON THE CONSTRUCTION OF CYCLIC COLLINEATIONS FOR OBTAINING A BALANCED SET OF L-RESTRICTIONAL PRIME-POWERED LATTICE DESIGNS.

BY SATI MAZUMDAR

Cornell University

1. Introduction and Summary. Raktoe [3] has recently developed a procedure for obtaining a balanced confounding scheme for any l-restrictional lattice design of s^m treatments where s is a prime or a power of a prime and m is a positive integer. He has shown that the generators of the confounding scheme in each arrangement can be taken from the columns of different powers of the rational canonical form of a matrix of cyclic collineation of a particular order. However, he did not indicate how to construct the generator matrices analytically except for the case $s = p = 2$. In all other cases, he obtained these matrices empirically. The present paper gives an analytic method for constructing the generator matrices of collineations for all values of s, by the application of a particular theorem in projective geometry and another one from group theory.

2. Results. The two theorems which are used to obtain the results of this paper are by Singer [4] and Dickson [2]. The theorems are stated below.

THEOREM 1 (Singer [4]). *There is always at least one collineation of period* $\alpha = (s^m - 1/s - 1)$ *in* $PG(m - 1, p^n)$ *and the matrix of this collineation is given by:*

$$\begin{bmatrix} a_{m,1} & 1 & 0 & \cdots & 0 \\ a_{m,2} & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ a_{m,m} & 0 & 0 & \cdots & 0 \end{bmatrix} m \times m$$

where $a_{m,i}$'s are the coefficients of an irreducible primitive polynomial of mth degree belonging to $GF(p^n)$ which can be written as follows:

$$x^m - a_{m,1}x^{m-1} - a_{m,2}x^{m-2} - \cdots - a_{m,m} = 0.$$

THEOREM 2 (Dickson [2]). *An* $IQ(\mu, p^n)$ *decomposes in* $GF(p^{n\nu})$ *into* δ *factors, each an* $IQ(\mu/\delta, p^{n\nu})$, *where* δ *is the greatest common divisor of* μ *and* ν, *and where* $IQ(\mu, p^n)$ *is a primitive irreducible polynomial of degree* μ *belonging to* $GF(p^n)$.

The notations and definitions of this paper follow those of Raktoe [3]. In addition to other results, he showed that the problem of finding a balanced set of l-restrictional lattice designs of s^m treatments reduces to the problem of finding a matrix of cyclic collineation of a particular order. But in order to find these required matrices he made two assumptions. The first assumption is that these

Received 31 May 1966; revised 23 February 1967.

matrices of cyclic collineations exist, and the second one is that if they exist, they possess rational canonical forms. These two assumptions represent two gaps in his results. In the present paper it will be shown how the application of Singer's theorem takes care of these two facts.

In the first place Singer's [4] theorem proves the *existence* of a matrix of collineation of a specified order. Secondly, there is no need for the assumption of a rational canonical form of the matrix of cyclic collineation. By this theorem the problem of constructing a balanced set of arrangements for an l-restrictional lattice design of s^m treatments reduces to the problem of finding a primitive irreducible polynomial of degree m belonging to $GF(s)$. It is to be mentioned here that Raktoe [3] noticed this property in the case $s = p = 2$ which he indicated in the discussion.

The problem of finding these irreducible polynomials of degree m belonging to $GF(s)$ denoted by $IQ(m, s)$, is discussed below.

Two cases arise here:

CASE 1. [The lattice design is s^m where s is strictly a *prime*, i.e. $n = 1$.]

In the lattice design s^m if $s = p$ (where p is a prime) we need to find $IQ(m, p)$ which is easily identified to be the minimum function for the construction of $GF(p^m)$. The procedure for obtaining such an IQ has been discussed by Bose [1] and is not reviewed here. Therefore, the same polynomial which is used for the construction of $GF(p^m)$ can be used for the construction of a cyclic collineation of order $(p^m - 1/p - 1)$.

CASE 2. [The lattice design is s^m where s is strictly a power of a prime, i.e. $n > 1$.]

An $IQ(nm, p)$ can be obtained by the usual method of cyclotomic polynomials (see Bose [1]). The method of getting an $IQ(m, p^n)$ from an $IQ(nm, p)$ is discussed below. The elements of $GF(p^n)$ can be defined by an irreducible polynomial of nth degree which is also called an irreducible congruence (mod p). In an $IQ(nm, p)$ the coefficients of the polynomial are elements of $z/(p)$, where $z/(p)$ is the group of integers modulo p and is isomorphic to $GF(p)$. Therefore, with the help of the given congruence which defines $GF(p^n)$, these elements can be rewritten as elements of $GF(p^n)$. An $IQ(nm, p)$ will thus give a polynomial of nmth degree with coefficients belonging to $GF(p^n)$. Decomposing this polynomial to n, mth degree irreducible polynomials we get the required $IQ(m, p^n)$. The justification of the above type of decomposition lies in Theorem 2 (Dickson [2]).

By putting $\nu = n$, $n = 1$, $\mu = nm$, the greatest common divisor of μ and ν becomes the greatest common divisor of nm and n which is simply n. So $\delta = n$. With this appropriate substitution, Dickson's theorem takes the following form: "*An $IQ(nm, p)$ decomposes in $GF(p^n)$ into n factors, each an $IQ(m, p^n)$.*" This justifies the decomposition mentioned earlier.

It may be mentioned here that by defining a series of elementary transformations it can be shown that these matrices of cyclic collineations always possess a rational canonical form, the property which was assumed by Raktoe [4]. In his construction of the matrices of cyclic collineations he limited himself to the cases where the matrices possess their rational canonical form. But in fact, the results obtained by him are quite general as the above mentioned transformations prove the existence of the rational canonical form of these matrices.

3. Discussion. It is interesting to note that known theorems connecting different irreducible quantics can be used to construct generator matrices of collineations for one group of designs from those of another. Two such theorems are quoted below without proof (Dickson [2]).

(A) *An* $IQ(m, p^{\delta})$ *is irreducible in* $GF(p^{nd})$ *if* n *be prime to* m. Thus the matrix of collineation for the lattice design $(p^{nd})^m$ is the same as that of $(p^d)^m$ if n is prime to m.

(B) *If* $F(\xi)$ *be an* $IQ(m, p^n)$ *in which the coefficient* α of ξ^{m-1} *is such that in the* $GF(p^n)$

$$\alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} \neq 0,$$

then $F(\xi^p - \xi)$ *is an* $IQ(mp, p^n)$.

4. Acknowledgment. The author is grateful to Professor Alfredo Jones for his helpful comments.

REFERENCES

[1] Bose, R. C. (1939). On the application of Galois fields to the problem of construction of hyper-graeco latin squares. *Sankhyā* **3** 323–338.

[2] Dickson, L. E. (1958). *Linear groups with an exposition to Galois field theory.* Dover Publication, Inc. New York.

[3] Raktoe, B. L. (1964). Application of cyclic collineation to the construction of balanced l-restrictional prime-powered lattice designs. Ph.D. Dissertation, Biometrics Unit, Cornell University.

[4] Singer, James. (1938). A theorem in finite projective geometry and some application to number theory. *Trans. Amer. Math. Society.* **43** 377–385.