On the Construction of Cyclic Collineations for Obtaining a Balanced Set of Prime-powered Lattice Designs

Sati Mazumdar

BU-208-M November, 1965

ABSTRACT

Raktoe [4] 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, but instead obtained them empirically. The present paper gives an analytic method for constructing the generator matrices of collineations by the application of a particular theorem in projective geometry.

Biometrics Unit, Plant Breeding Department, Cornell University

On the Construction of Cyclic Collineations for Obtaining a Balanced Set of Prime-powered Lattice Designs

Sati Mazumdar

BU-208-M November, 1965

1. Introduction and summary.

Raktoe [4] 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, but instead obtained them empirically. The present paper gives an analytic method for constructing the generator matrices of collineations by the application of a particular theorem in projective geometry.

2. Definitions and previous results.

It is well known that the pseudo effects in a $s^m = (p^n)^m$ lattice design are in 1:1 correspondence with the points of the (m-1)-dimensional projective geometry PG(m-1,s=p^n). (For a definition of an ℓ-flat or ℓ-subspace in PG(m-1,s) see Carmaichael [3].) In order to satisfy the condition that s^m treatments are allocated to the experimental units according to ℓ-restrictions ($\ell \leq m$) we write $s^m = s^{r_1} \cdot s^{r_2} \cdots s^{r_\ell} = \prod_{i=1}^{\ell} s^{r_i}$. A balanced ℓ-restrictional lattice design $s^m = \prod_{i=1}^{\ell} s^{r_i}$ is defined as a lattice design consisting of a

---

Biometrics Unit, Plant Breeding Department, Cornell University

minimal set of arrangements such that each of the $\frac{s^m-1}{s-1}$ pseudo effects is confounded an equal number of times in each of the ℓ-restrictions.

Geometrically the problem of constructing a balanced ℓ-restrictional lattice design $s^m = \prod_{i=1}^{\ell} s^{r_i}$ is equivalent to that of constructing a minimal set of ℓ-tuples of flats $[(r_1-1)\text{-flat}, (r_2-1)\text{-flat}, \cdots, (r_\ell-1)\text{-flat}]$ such that each point of PG(m-1,s) is incident γ_i times with the set of (r_i-1)-flats, $i=1,2,\cdots,\ell$, and such that each ℓ-tuple exhausts PG(m-1,s). In any ℓ-restrictional lattice design with $s^m = \prod_{i=1}^{\ell} s^{r_i}$, the pseudo effects have no physical meaning unless the treatments form a factorial arrangement. We can, therefore, following Raktoe [4], associate with any given ℓ-restrictional lattice design the particular PG(m-1,s) which will make $\frac{s^m-1}{s-1}$ and $\frac{s^{r_i}-1}{s-1}$ $(i=1,2,\cdots,\ell)$ relatively prime to each other. Since s is a prime-power such a choice can always be made. The main results of Raktoe [4] can be stated in the following two theorems.

Theorem 1.

If $s^m = \prod_{i=1}^{\ell} s^{r_i}$ indicates an ℓ-restrictional lattice design, then the number of arrangements required for balancing is given by $\frac{s^m-1}{s-1}$.

Theorem 2.

For any ℓ-restrictional lattice design $s^m = \prod_{i=1}^{\ell} s^{r_i}$ the construction of a balanced set of arrangements is equivalent to the construction of a cyclic collineation of order $\frac{s^m-1}{s-1}$.

The construction of cyclic collineations of different orders was done by him on the computer assuming that these matrices have the rational canonical forms.

Two other theorems which have been used in the present paper are stated below.

Theorem 3. (Singer [3])

There is always at least one collineation of period $\alpha = \frac{s^m-1}{s-1}$ in $PG(m-1,p^n)$ and the matrix of this collineation is given by

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

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

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

Following Dickson [3], let us denote a primitive irreducible polynomial of degree m belonging to $GF(p^n)$ by $IQ(m,p^n)$. Now, we state a theorem also due to him.

Theorem 4. (Dickson [3])

An $IQ(\mu,p^n)$ decomposes in $GF(p^{n\nu})$ into δ factors, each an $IQ(\frac{\mu}{\delta}, p^{n\nu})$, δ being the greatest common devisor of μ and ν.

3. Applications.

The theorem of Singer [5] takes care of two main gaps which are present in the results of Raktoe [4].

In the first place, it proves the existence of a matrix of collineation of a specified order. Secondly, it does not need the assumption of a rational canonical form of the matrix which may or may not exist. By Singer's theorem the problem of constructing a balanced set of arrangements for an ℓ-restrictional lattice design s^m reduces to the problem of finding a primitive irreducible polynomial of degree m belonging to GF(s). In order to obtain these IQ's the following two cases arise.

Case 1. 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 order $\frac{p^m-1}{p-1}$.

Case 2. n > 1 [The lattice design is s^m where s is strictly a power of a prime.]

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 n^{th} degree which is also called an irreducible congruence (mod p). In an IQ(nm,p) the coefficients of the polynomial are elements of $\frac{z}{(p)}$ $\underline{\cap}$ GF(p)

[$\frac{z}{(p)}$ is the group of integers modulo 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 nm^{th} degree with coefficients belonging to $GF(p^n)$. Decomposing this polynomial to n, m^{th} degree irreducible polynomials we get the required $IQ(m,p^n)$. The justification of the above type of decomposition lies in the theorem 4 mentioned in an earlier section.

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, theorem 4 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.

4. Numerical examples.

Example 1.

Let s=2, m=2.

We have a 2^2 lattice design. The required number of arrangements for balancing is given by $\frac{2^2-1}{2-1} = 3$. So we need a collineation of order 3.

x^2+x+1 is an IQ(2,2). Take the polynomial $x^2+x+1 = 0$ or equivalently $x^2 = -x-1 = a_2x + a_1$ where

$$a_2 = -1 = 1 \pmod 2$$

$$a_1 = -1 = 1 \pmod 2$$

The generator matrix A is therefore given by $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ of order 3. The different powers of A are given by $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $A^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $A^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Now the three effects of a 2^2 design can be represented by A, B, AB each carrying one degree of freedom.

As indicated by Raktoe [4], the columns of the matrices are associated with the generators of the flats which are confounded. If a 2^2 design is considered as a 2-restrictional lattice design $2^2 = 2^1 \cdot 2^1$, with two rows and two columns, we can confound one 0-flat with the columns and one 0-flat with the rows in each arrangement and these generators can be directly read off from the columns of the matrices.

	Confounded with rows	Confounded with columns
1st arrangement	AB	A
2nd arrangement	B	AB
3rd arrangement	A	B

Therefore, each pseudo effect has been shown to be confounded once in each row and once in each column.

Example 2.

Let $m=2$, $s=4=2^2$.

This is a case of 4^2 lattice design. The number of arrangements needed for balancing is $\frac{4^2-1}{4-1} = \frac{15}{3} = 5$. Therefore, we need a collineation of order 5. For the construction of this collineation an $IQ(2,2^2)$ is needed. By decomposing (modulo 2) the expression $\frac{(x^{2^4}-x)}{(x^{2^2}-x)}$, three $IQ(4,2)$ are found which are given below

i) $x^4 + x + 1$

ii) $x^4 + x^3 + 1$

iii) $x^4 + x^3 + x^2 + 1$.

Let us take one of them, say $x^4 + x + 1$.

$GF(2^2)$ is defined by means of the irreducible congruence

$$i^2 + i + 1 = 0 \qquad \text{mod } (2) \ .$$

Four elements of $GF(2^2)$ are thus given by

$$0 \equiv 0 \equiv 0$$

$$i^0 \equiv 1 \equiv 1$$

$$i \equiv 2 \equiv i$$

$$i^2 \equiv 3 \equiv i + 1$$

Hence,

$$x^4+x+1 = x^4 + (i^2+i)x + (i^2+i)$$

$$= (x^2+x+i)(x^2+x+i^2)$$

Thus x^4+x+1 decomposes into two factors each an $IQ(2,2^2)$, any one of them can be used for the construction of the required collineation. For example, let us take x^2+x+i. So from the relation $x^2+x+i = 0$ we get $x^2 = -x-i = a_2x + a_1$. Hence,

$$a_2 = -1 = 1 \qquad \text{mod } (2) \quad \equiv \quad 1 \text{ of } GF(2^2)$$

$$a_1 = -i = -i+2i = i \quad \text{mod } (2) \quad \equiv \quad 2 \text{ of } GF(2^2)$$

Therefore, $A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$ order 5.

Taking the different powers of this matrix A, the confounding scheme can be written down easily.

5. Discussions.

(a) 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 [3].)

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 $GF(p^n)$

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

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

(b) Raktoe [4] generated the matrices of cyclic collineations for all δ and m such that $\delta^m < 1000$ where the matrices were assumed to have the rational canonical form. As a matter of fact, he generated the rational canonical forms of these matrices. By defining a series of elementary transformations it is shown below that these collineation matrices always have the rational canonical forms.

A necessary and sufficient condition for a matrix to have the rational canonical form is that the matrix has only one non-trivial similarity invariant factor which is equivalent to the fact that the matrix $A-\lambda I$ has only one non-trivial invariant factor. Now,

$$A-\lambda I = \begin{pmatrix} a_1-\lambda & 1 & 0 & 0 & \cdots & 0 \\ a_2 & -\lambda & 1 & 0 & \cdots & 0 \\ a_3 & 0 & -\lambda & 1 & \cdots & 0 \\ \vdots & & & & & \\ a_{m-1} & 0 & 0 & 0 & \cdots & 1 \\ a_m & 0 & 0 & 0 & \cdots & -\lambda \end{pmatrix}$$

Let the following elementary transformations be applied on $A-\lambda I$.

i) Multiply the 1st row by λ and add it to the 2nd row.

ii) In the resulting matrix, multiply the 2nd row by λ and add it to the 3rd row.

iii) In the resulting matrix, multiply the 3rd row by λ and add it to the 4th row.

iv) Continue as above.

v) The matrix at the last stage of operation will take the following form:

$$\begin{pmatrix} a_1-\lambda & 1 & 0 & 0 & \cdots & 0 \\ a_2+a_1\lambda-\lambda^2 & 0 & 1 & 0 & \cdots & 0 \\ a_3+a_2\lambda+a_1\lambda^2-\lambda^3 & 0 & 0 & 1 & \cdots & 0 \\ a_4+a_3\lambda+a_2\lambda^2+a_1\lambda^3-\lambda^4 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & & & & \\ f_m(\lambda) & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

[Where $f_m(\lambda)$ is a polynomial in λ of degree m.]

If now, from the first column suitable multiples of the other columns are subtracted, a matrix of the following form is obtained:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & & & & \\ f_m(\lambda) & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

vi) Apply elementary transformations so that the first column takes the place of the last column getting the form:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & 0 & \cdots & f_m(\lambda) \end{pmatrix}$$

This shows that $A-\lambda I$ has only one non-trivial invariant factor $f_m(\lambda)$ which is a <u>sufficient</u> condition for the existence of the rational canonical form of the matrix A.

(c) It can be shown that $f_m(\lambda)$ will take the form:

$$a_m + a_{m-1}\lambda + a_{m-2}\lambda^2 + \cdots + a_1\lambda^{m-1} - \lambda^m$$

which shows that the $IQ(m,p^n)$ used in the construction of the collineation matrix is identical with the similarity invariant factor of the matrix.

6. Acknowledgement.

My thanks 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] Carmichael, R. D. (1956) Introduction to the theory of groups of finite order. Dover Publication, Inc., New York.

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

[4] 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.

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