ORTHOGONAL SERIES 1 BALANCED INCOMPLETE BLOCK DESIGNS

A FURTHER NOTE

Joiner, J. R. and Federer, W. T.

BU-452-M February, 1973

ABSTRACT

The incidence matrix of the orthogonal Series 1 Balanced Incomplete Block Design has parameters

$$v=n^2 \quad b=n(n+1) \quad r=n+1 \quad k=n \quad \lambda=1 \ .$$

The existence of n-1 orthogonal latin squares of order n is sufficient to construct this design.

This paper utilizes a latin square, L_0, of order $n=p^s$, p a prime, constructed by an automorphism of order $t=p^s-1$ acting on the elements of the Galois Field, $GF(p^s)$, to construct the incidence matrix mentioned above. It is shown that L_0 induces n permutation matrices of order $n \times n$, $P_1=I, P_2, P_3, \cdots, P_r$, which taken together with the matrices T_i of order $n \times n$ composed of 1's in the i^{th} column and 0 elsewhere can be put in the following form:

$$N = \begin{bmatrix} T_1 & P_1 & P_1 & \cdots & P_1 & P_1 \\ T_2 & P_{j_{2,1}} & P_{j_{2,2}} & \cdots & P_{j_{2,n-1}} & P_1 \\ T_3 & P_{j_{3,1}} & P_{j_{3,2}} & \cdots & P_{j_{3,n-1}} & P_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ T_{n-1} & P_{j_{n-1,1}} & P_{j_{n-1,2}} & \cdots & P_{j_{n-1,n-1}} & P_1 \end{bmatrix}$$

with the result that $NN' = nI + J$. The choice of $P_{j_{i,k}}$ depends on the automorphism.

An example with $n=3^2$ is given.

ORTHOGONAL SERIES 1 BALANCED INCOMPLETE BLOCK DESIGNS

A FURTHER NOTE

Joiner, J. R. and Federer, W. T.

BU-452-M February, 1973

INTRODUCTION

Federer and Raghavarao (1972) constructed an OS1 Balanced Incomplete Block design as follows: Let T_i be an $n \times n$ matrix with 1's in the i^{th} column and 0's elsewhere for $i=1,2,\cdots,n$. Let $P_0,P_1,\cdots,P_{n-1}$ be n matrices of order $n \times n$ obtained by cyclic permutation of the identity matrix of order n. When n is a prime number,

$$N = \begin{bmatrix} T_1 & P_0 & P_1 & P_2 & \cdots & P_{n-1} \\ T_2 & P_1 & P_3 & P_5 & \cdots & P_{n-1} \\ T_3 & P_2 & P_5 & P_8 & \cdots & P_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ T_n & P_{n-1} & P_{n-1} & P_{n-1} & \cdots & P_{n-1} \end{bmatrix}$$

and is the incidence matrix of the BIB design with parameters

$$v=n^2,\ b=n(n+1),\ r=(n+1),\ k=n, \text{ and } \lambda=1$$

In an addendum it was shown that the use of transversals of a latin square of order 4 along with proper choice of the subscripts of the P_i's would make a similar construction for $n=2^2$.

Paper Number BU-452-M in the Mimeograph Series of the Biometric Unit, Cornell University.

This paper presents a construction for $n=3^2$, a relationship between n permutation matrices induced by a latin square of order n constructed by the group automorphism technique, and a method of viewing the square as a multiplication table of the permutation matrices. This represents an extension of results by Hedayat and Federer (1969). Lastly, a proof is given to show that a construction is possible for any $n=p^s$ for p a prime number.

The 3^2 Construction

The construction of 3^2 starts with the following square from page 63 of Fisher and Yates (1948).

1	2	3	4	5	6	7	8	9
3	1	2	6	4	5	9	7	8
2	3	1	5	6	4	8	9	7
7	8	9	1	2	3	4	5	6
9	7	8	3	1	2	6	4	5
8	9	7	2	3	1	5	6	4
4	5	6	7	8	9	1	2	3
6	4	5	9	7	8	3	1	2
5	6	4	8	9	7	2	3	1

Nine permutation matrices $P_1=I, P_2,\cdots,P_9$ are formed by inserting a 1 in P_i where i appears in the above square. These matrices form a group under matrix multiplication and their multiplication table is represented by the above square using the first column and row as headings. The arrangement which forms the incidence matrix of a BIB is

$$\begin{matrix} T_1 & P_1 & P_1 & P_1 & P_1 & P_1 & P_1 & P_1 & P_1 & P_1 \\ T_2 & P_2 & P_7 & P_9 & P_8 & P_3 & P_4 & P_5 & P_6 & P_1 \\ T_3 & P_3 & P_4 & P_5 & P_6 & P_2 & P_7 & P_9 & P_8 & P_1 \\ T_4 & P_4 & P_2 & P_6 & P_9 & P_7 & P_3 & P_8 & P_5 & P_1 \\ T_5 & P_5 & P_8 & P_2 & P_4 & P_9 & P_6 & P_3 & P_7 & P_1 \\ T_6 & P_6 & P_5 & P_7 & P_2 & P_8 & P_9 & P_4 & P_3 & P_1 \\ T_7 & P_7 & P_3 & P_8 & P_5 & P_4 & P_2 & P_6 & P_9 & P_1 \\ T_8 & P_8 & P_9 & P_4 & P_3 & P_6 & P_5 & P_7 & P_2 & P_1 \\ T_9 & P_9 & P_6 & P_3 & P_7 & P_5 & P_8 & P_2 & P_4 & P_1 \end{matrix}$$

since N N' is of the desired form, $9I + J$. The second to the ninth columns of the above matrix correspond to the first columns of the 8 orthogonal squares for a latin square of order 9 as given in Fisher and Yates (1948) with the column of T's and P_1 added.

The Matrices as a Group

Let L_0 be a latin square of order $n=p^s$, p a prime number, which was constructed by an automorphism, A, of order $t=p^s-1$. Using the Galois Field $GF(p^s)$, such an automorphism is known to exist, and L_0 can have the following construction for x an element of $GF(p^s)$:

$$L_0 = \begin{bmatrix} 0 & A(x) & A^2(x) & A^3(x) & & A^t(x) \\ A(x) & A(x)*A(x) & A(x)*A^2(x) & A(x)*A^3(x) & \cdots & A(x)*A^t(x) \\ A^2(x) & A^2(x)*A(x) & A^2(x)*A^2(x) & A^2(x)*A^3(x) & \cdots & A^2(x)*A^t(x) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A^t(x) & A^t(x)*A(x) & A^t(x)*A^2(x) & A^t(x)*A^3(x) & \cdots & A^t(x)*A^t(x) \end{bmatrix}$$

0 is the identity element of the addition table and * is the additive operation on

$GF(p^s)$. Obviously L_0 can be regarded as an addition table for $0, A(x), \cdots, A^t(x)$ under $*$. Permute the rows of L_0 to M_0 such that 0 is on the diagonal and form the set $P = \{P_0 = I, P_1, \cdots, P_{n-1}\}$ where P_i is formed by putting a 1 in the locations in P_i where $A^i(x)$ appears in M_0 ; P_0 represents 0 in this manner.

Theorem 1: <u>The set P forms a group under matrix multiplication and M_0 (or L_0) represents the multiplication table of this group with * interpreted as matrix multiplication and 0 as the identity for multiplication.</u>

P is closed because if one multiplies P_m by P_r, the resulting 1 in (say) the (i,j) location represents the product of 1's in the locations in P_r and P_m where in M_0,

$$A^i(x) * A^k(x) = A^r(x)$$

$$A^\ell(x) * A^j(x) = A^m(x)$$

$A^k(x)$ is in the k^{th} column and $A^\ell(x)$ must be in the k^{th} row; hence, since M_0 has 0's on the diagonal, $A^k(x)$ and $A^\ell(x)$ are inverses under $*$. From the preceding

$$A^i(x)*A^k(x)*A^\ell(x)*A^j(x) = A^i(x)*A^j(x) = A^r(x)*A^m(x) = \text{Constant} .$$

This shows closure of P and the use of M_0 as its multiplication table.

The inverse of P_i is its transpose. Suppose that P_i has a 1 in (k,j) . Since only the rows of M_0 were permuted, the entry in M_0 corresponding to (k,j) in P_1 is

$$A^k(x)*A^j(x) = A^i(x) ,$$

and its transpose is

$$A^s(x)*A^m(x) = A^\ell(x) .$$

But $A^j(x)$ and $A^s(x)$ are in the j^{th} column and row respectively and hence are inverses. Likewise, $A^k(x)$ and $A^m(x)$ are in the same row and column; therefore,

$$A^k(x)*A^j(x)*A^s(x)*A^m(x) = 0 = A^i(x)*A^{\ell}(x) \quad .$$

This shows that $A^{\ell}(x)$ is the inverse of $A^i(x)$ under * and that $P_i' = P_{\ell}$. This completes the proof, since associativity obviously holds. The conditions of the theorem are not necessary but are compatible with the purpose of this paper.

Construction of the Incidence Matrix N

The elements of the automorphism A form a group under a composition of mappings. We form a $t \times t$ matrix, M whose i^{th} column is the result of $A^i(A^j(x))$ where $A^j(x)$ is the entry in the successive rows in the first column of M_0, $j=1,2,\cdots,t$.

$$M = \begin{bmatrix} A^{j_1}(A^{k_1}(s)) & A^{j_2}(A^{k_1}(x)) & \cdots & A^{j_t}(A^{k_1}(x)) \\ A^{j_1}(A^{k_2}(x)) & A^{j_2}(A^{k_2}(x)) & \cdots & A^{j_t}(A^{k_2}(x)) \\ \vdots & \vdots & \vdots & \vdots \\ A^{j_1}(A^{k_t}(x)) & A^{j_3}(A^{k_t}(x)) & \cdots & A^{j_t}(A^{k_t}(x)) \end{bmatrix}$$

where $j_i=1,2,\cdots,t$ for $i=1,2,\cdots,t$ and k_i^i ranges over the same values. Note that the 0 entry in the top of the first column of M_0 is not used.

Theorem 2: <u>The vector</u> $t' = \left(A^{j_1}(A^{k_J}(x))*A^{j_1}(A^{k_m}(X)),\ A^{j_2}(A^{k_J}(x))*A^{j_2}(A^{k_m}(x)),\ \ldots,\ A^{j_t}(A^{k_J}(x))*A^{j_t}(A^{k_m}(x))\right)$ <u>contains the distinct elements</u> $A^1(x), A^2(x), \cdots, A^t(x)$ <u>in some order, for any choice of</u> $k,m,\ k\neq m$.

Suppose that

$$A^{j_1}(A^{k_J}(x))*A^{j_1}(A^{k_m}(x)) = A^{j_s}(A^{k_J}(x))*A^{j_s}(A^{k_m}(x))$$

Since A is a homomorphism,

$$A^{j_1}(A^{k_J}(x) * A^{k_m}(x)) = A^{j_s}(A^{k_J}(x) * A^{k_m}(x))$$

or

$$A^{j_i}(x) = A^{j_s}(x)$$

which contradicts the assumption that A is of order t .

Since P_i and $A^i(x)$ have the same multiplication table setting $P = A^{j_i}(A^{k_m}(x))$ for each entry in M forms a matrix M^* with the same properties as M . Specifically the products of any two rows of M^* result in the t distinct products, $P_1, P_2, \cdots, P_t$ and the sum of these is J - I .

Theorem 3:

$$N = \begin{bmatrix} T_1 & P_0 & P_0 & \cdots & P_0 \\ T_2 & & & & P_0 \\ \vdots & \vdots & M^* & \vdots & \vdots \\ T_n & & & & P_0 \end{bmatrix}_{n \times n}$$

is the incidence matrix of a BIB _design, that is,_ $NN' = nI + J$.

Lemma: _If row_ i _of_ M^* _contains_ $P_{j_1}, P_{j_2}, \cdots, P_{j_t}$ _in that order then there is a row in_ M^* _containing_ $P'_{j_1}, P'_{j_2}, \cdots, P'_{j_t}$ _in the same order._

The proof of the lemma depends upon the properties of A . P_{j_1} in M^* corresponds to $A^s(A^t(x)) = A^{j_1}(x)$ in M . There is a row in the same column of M as P_{j_1} where $A^s(A^m(x)) = A^u(x)$ is the inverse under * of $A^{j_1}(x)$. This means that

$$A^s(A^t(x)) * A^s(A^m(x)) = A^s(A^t(x) * A^s(x)) = 0 ,$$

which implies that

$$(1) \qquad A^t(x) * A^m(x) = 0 \quad .$$

Since (1) holds across the entirety of the two rows in question, $A^{j_i}(x)$ in row i is inverse to every element in the row where $A^{j_1}(x)$ has its inverse equal to $A^u(x)$.

To return to the proof of the theorem, note that the diagonal elements of NN' are of the form $\left(T_i T_i' = J\right) + \left(\sum_{k=1}^{t} P_{j_k} P_{j_k}' = nI\right) = J + nI$. On the off-diagonal one has the sum of 3 items:

a. $T_i T_j' = 0$

b. $P_{j_1} P_{k_1}' + P_{j_2} P_{k_2}' + \cdots + P_{j_t} P_{k_t}'$

but the lemma shows that this is just the product of two rows of M^* and hence is equal to $J - I$.

c. $P_0 P_0' = I$

The sum of quantities in a, b, c is J . This completes the proof of theorem 3.

References

1. Federer, W. T. and Raghavarao, D. [1972]. A note on the construction of orthogonal series 1 . Mimeo No. BU-434-M in the Biometrics Unit Series, Cornell University.

2. Fisher, R. A. and Yates, F. [1948]. Statistical Tables for Biological, Agricultural and Medical Research (1st edition 1938), 3rd edition, Hafner Publishing Co., Inc., N. Y.

3. Hedayat, A. and Federer, W. T. [1969]. An application of group theory to the existence and nonexistence of orthogonal latin squares. Biometrika 56: 547-551.