ORTHOGONAL ARRAYS OF INDEX UNITY[1]

By K. A. Bush

University of North Carolina and University of Illinois

Summary. In this paper we shall proceed to generalize the notion of a set of orthogonal Latin squares, and we term this extension an orthogonal array of index unity. In Section 2 we secure bounds for the number of constraints which are the counterpart of the familiar theorem which states that the number of mutually orthogonal Latin squares of side s is bounded above by $s - 1$. Curiously, our bound depends upon whether s is odd or even. In Section 3 we give a method of constructing these arrays by considering a class of polynomials with coefficients in the finite Galois field $GF(s)$, where s is a prime or a power of a prime. In the concluding section we give a brief discussion of designs based on these arrays.

1. Introduction.

Let a set of s integers $0, 1, \cdots, s - 1$ be arranged in an $s \times s$ square in such a way that every integer occurs s times. If each integer occurs once and only once in every row and column, the square is said to be a Latin square of side s. Two squares are said to be orthogonal to one another if, when one square is superimposed upon the other square, every number of the first occurs once and only once with every number of the second square. To the set of at most $s - 1$ Latin squares which are mutually orthogonal, we may adjoin two other squares which are not Latin squares but which are orthogonal to each other and to every other Latin square in the orthogonal set. The first of these squares is constructed by taking each element of the first row as 0, each element of the second row as 1, and so on. The second square is the transpose of the first square. Conversely it may be noted that any square orthogonal to these two squares must be a Latin square. Thus a total of $s + 1$ orthogonal squares is possible at best, and it is known that this bound is attainable when s is a prime or a power of a prime [1]. When this bound is attained, we say that we have a complete set of orthogonal squares. As an example [illegible] a complete set, we might choose $s = 3$ and write

$$\begin{array}{ccc} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

If we write in order the elements of each square in a line, we can display these squares in the following form:

$$\begin{array}{ccccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{array} \qquad \begin{array}{r} \text{[first square]} \\ \text{[second square]} \end{array}$$

[1] This note is a revision of one part of the author's doctoral dissertation submitted to the University of North Carolina at Chapel Hill.

$$\begin{array}{ccccccccccl} 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 & & \text{[third square]} \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 & & \text{[fourth square]} \end{array}$$

In this form we see that any two rows have the property that each one of the nine possible ordered pairs occurs exactly once when one row is superimposed on another row. We now generalize this basic idea.

Let us consider a matrix $A = [a_{ij}]$, where each a_{ij} represents one of the integers $0, 1, \cdots, s-1$, $s > 1$. The matrix is rectangular with N columns, which we shall call the blocks of the array, and k rows. Consider all t-rowed submatrices of N columns which can be formed from this array, $t \leqq k$. Each column of any t-rowed submatrix can be regarded as an ordered t-plet so that each t-rowed submatrix contains N such t-plets. The matrix A will be called an orthogonal array $[N, k, s, t]$ of *size* N, k *constraints*, s *levels*, *strength* t and *index* λ if each of the C_t^k t-rowed N-columned submatrices that may be formed from the array contains every one of the s^t possible ordered t-plets each repeated λ times. It is clear that this definition implies that each row contains the s integers $0, 1, \cdots, s-1$, each repeated λs^{t-1} times. We shall consider the case where $\lambda = 1$ and refer to such arrays as "orthogonal arrays of index unity." We shall consider arrays where $t > 2$ since the case $t = 2$ has been completely discussed and solved for s a prime or a power of prime. References [1], [2], [7], [8], and [11] discuss this problem.

2. Upper bounds for the number of constraints. We shall use the notation $f(N, s, t)$ to denote the maximum number of constraints which are possible. Thus $f(N, s, 2) = s + 1$ when s is a prime or a power of a prime. We prove first the

THEOREM. *If* $s \leqq t$, *then* $f(s^t, s, t) \leqq t + 1$.

PROOF. We shall make repeated use of the following fact: selecting any $t - 1$ rows, any specified $(t-1)$-plet must occur exactly s times, for these s identical $(t-1)$-plets may be enlarged to t-plets by the adjunction of another row in exactly s ways since a given t-plet occurs once and only once. If possible let there exist $t + 2$ orthogonal rows. In order to facilitate notation we shall assume that one of the blocks consists entirely of zeros. This is justified because within each row we can always make a permutation of the elements $0, 1, 2, \cdots, s-1$ without destroying the orthogonality of the array. The general case proceeds along slightly different lines from the special cases $s = 2$ and $s = 3$ which we shall consider first.

Proof for the case $s = 2$. We divide the array into two parts. The first part, A, consists of three rows, and the second part, B, consists of $t - 1$ rows. There will be exactly two blocks which will have zero in every row of B. One of these blocks is our initial block consisting exclusively of zeros. In the second block the three rows of A must contain the symbol 1, for otherwise there would be two identical t-plets. Now there will be two blocks which will have the symbol 1 in the first row of B and zero in all other rows. Let these be the third and fourth blocks. The first four blocks of the array we have just described will have the form:

$$\begin{array}{c|cccc}
 & 0 & 1 & . & . \\
A & 0 & 1 & . & . \\
 & 0 & 1 & . & . \\
\hline
 & 0 & 0 & 1 & 1 \\
B & 0 & 0 & 0 & 0 \\
 & . & . & . & . \\
 & 0 & 0 & 0 & 0
\end{array}$$

The third block already has $t - 2$ elements in common with each of the first two blocks. Therefore it can have at the most one more element in common with any of these blocks. Since the three rows of A for the third block have to be filled in by using the symbols 0 and 1 only, we cannot avoid the situation in which it has at least two elements in part A in common with one of the first two blocks. The theorem is thus proved for the case $s = 2$.

We now proceed to the case $s = 3$ using the same general type of argument although there are more complications. We divide the array into two parts as before, three rows in A and $t - 1$ rows in B. In this case the first fifteen blocks of the array can be written as follows:

$$\begin{array}{c|ccc ccc ccc ccc ccc}
 & 0 & & & 0 & & & 0 & & & 0 & & & 0 & & \\
A & 0 & & & & 0 & & & 0 & & & 0 & & & 0 & \\
 & 0 & & & & & 0 & & & 0 & & & 0 & & & 0 \\
\hline
 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
B & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\
 & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

The blank spaces in A are to be filled in with 1 or 2. Obviously with each group of three blocks with identical $(t - 1)$-plets in B, we must include 0 from each row of A, and two 0's may not occur in the same block since then a t-plet identical with a t-plet from the first block would arise. We will encounter a somewhat similar type of arrangement in the general case shortly to be discussed. Each row of B in the portion of the array exhibited contains only zeros with the exception of the first two rows.

Let us consider the four blocks in the array which have 0 in the top line of A not counting the initial block. We now attempt to complete the second and third rows of A for these four blocks. We note that these four blocks already have a common element in A so that if two of the four blocks were completed using the same pair we would have two identical triplets in A. However any two blocks have at least $t - 3$ 0's in common in B so that two identical t-plets would eventuate. Therefore the four pairs must be distinct. From the elements 1 and 2 we can make only four distinct ordered pairs so that each possible pair must be utilized in these four blocks.

In completing the second and third blocks we must therefore repeat these pairs. Hence we can find two blocks with two elements in common in A. But this is impossible since (say) the second block has $t - 2$ 0's in common with every other block in the B portion.

Proof for the case $s > 3$. We shall use the same notations and procedures employed in the proof of the previous cases. We shall have an initial block consisting of $t + 2$ zeros. We divide the array into an A group with three rows and a B group with $t - 1$ rows. We then write down the $s - 1$ blocks which contain only 0's in the rows of B. We shall call this group of blocks F. We follow this with a group of s blocks which have the element 1 in the top row of B and the element 0 in the remaining rows of B. This is followed by a group of s blocks containing the element 2 in the top row of B, 0's elsewhere. Finally we arrive at a group of blocks which have the element $s - 1$ in the top row with 0's elsewhere. We have now secured $s - 1$ groups with s blocks in a group in addition to the group F. We now generate $s - 1$ further groups each containing s blocks by choosing the second row of B as our non-zero row. Proceeding in this way we finally obtain $(t - 1)(s - 1)$ groups each containing s blocks since there are $t - 1$ rows in B.

Consider one of these groups other than F which have identical $(t - 1)$-plets in B. Over such a group the rows of A must contain some permutation of the elements $0, 1, \cdots, s - 1$ in order that no t-plet be repeated. Hence the element 0 must occur once in each row of A over such a group; further, it must not occur twice in the same block, for then a t-plet consisting exclusively of 0's would arise. There are thus $(s - 3)(t - 1)(s - 1)$ blocks in these groups (exclusive of F) which contain no element 0 in the three rows of A.

Over every row of A each of the elements $1, 2, \cdots, s - 1$ occurs once in each group. If this condition is not met, then we either lose a t-plet or we secure more than one t-plet since in B each group exhausts a given $(t - 1)$-plet. Let us denote by e that element which occurs most frequently in the first row of A in those blocks which do not contain the element 0 and are not in F. Then e occurs in these blocks at least $(s - 3)(t - 1)$ times, for this is the number of blocks averaged over the number of elements, and there are $s - 1$ nonzero elements.

The element e will also occur in some block of F in the first row of A. Suppose that in this block the elements a and b occur in the second and third row. Now no element in the second row of A can be the element a if the same block contains the element e in its first row, for then we would have two elements in common in A, and any block in F has $t - 2$ elements in common with any other block in B; this would yield two identical t-plets. A similar remark applies to the element b in the third row of A. Since we are considering only those blocks not in F which contain no zero in any row of A, we may therefore form but $(s - 2)^2$ pairs when the element e occurs in such a block.

However, the pairs in these blocks must all be distinct. If they were not, then we would have three elements in common in A, and always there are $t - 3$ zeros in common in B so that again two t-plets would be identical. Furthermore, none of these pairs in the second and third rows may coincide with a pair in the second and third row of F by a like argument, that is, two elements alike in A, $t - 2$ elements alike in B. There are $s - 2$ pairs which remain in F since we must obviously exclude the pair (a, b) for which we have made a stronger statement. Now there are at least $(s - 3)(t - 1)$ distinct pairs not in F so that we must have

$$(s - 2)^2 \geqq (s - 2) + (s - 3)(t - 1),$$

for the total number of allowable pairs must not be less than the total number of distinct pairs required. Upon simplification we obtain

$$(3 - s)(t - s + 1) \geqq 0,$$

which is a contradiction. This proves our theorem for $s > 3$.

We now prove a special result for the case $t = 3$. In the proof we require the following definition.

DEFINITION. *Two blocks will be called disjoint if corresponding elements are different, that is, $a_{ij} \neq a_{ik}$ for each value of i.*

THEOREM. *When s is odd, $f(s^3, s, 3) \leqq s + 1$.*

PROOF. Suppose that $s + 2$ orthogonal rows can be constructed. Now each element is repeated s^2 times in each row and each pair of elements occurs s times in any two rows. Consider the elements in the first block, and let us select a particular element in this block. With the other elements in the block we can form $s + 1$ pairs where the particular element selected is used as one component of the pairs. Taking into account the fact that each of these pairs occurs once in the initial block and that we have also here used one replication of our selected element, we have to form pairs in other blocks containing the element selected $(s + 1)(s - 1)$ times. But this exhausts the replications of the element chosen. Consequently any two blocks have either two elements in common or are disjoint. From the $s + 2$ elements in the initial block we can form $(s + 2)(s + 1)/2$ pairs which are repeated $s - 1$ times. But

$$(s + 2)(s + 1)(s - 1)/2 < s^3 - 1, \quad s > 1,$$

so that disjoint blocks exist. Let us consider two disjoint blocks, and all other blocks $(s - 1)$ in number which contain the same pair in the first two rows as the second of these disjoint blocks. We can then represent the situation as

$$\begin{array}{ccccccccc}
a_1 & b_1 & b_1 & b_1 & \cdot & b_1 & \cdot & \cdot & \cdot \\
a_2 & b_2 & b_2 & b_2 & \cdot & b_2 & \cdot & \cdot & \cdot \\
a_3 & b_3 & & & & & & & \cdot \\
a_4 & b_4 & & & & & & & \cdot \\
\cdot & \cdot & \cdot & & & & & & \cdot \\
a_{s+2} & b_{s+2} & \cdot & & & & & & \cdot
\end{array}$$

where $a_i \neq b_i$, $i = 1, 2, \cdots, s + 2$. Since every triplet occurs exactly once, then the last s elements in the last s rows of the first block must occur exactly once in these $s - 1$ blocks. But since two blocks have either none or two elements in common, we get a contradiction since s is odd.

We are now in a position to state the general theorem.

THEOREM. *The maximum number of constraints is bounded above by* $s + t - 1$ *if* $t \leqq s$ *and* s *is even. In case* s *is odd, we may refine the inequality to* $s + t - 2$ *when* $3 \leqq t \leqq s$.

PROOF. This theorem is an immediate consequence of the preceding theorem, for the existence of an array with $k + 1$ constraints and strength t implies the existence of an array with k constraints of strength $t - 1$ since we may select a particular row in the first array and consider the s^{t-1} blocks which have 0 as the element in that row. Evidently the k rows which remain form an orthogonal array of strength $t - 1$, for each $(t - 1)$-plet occurs exactly one time; otherwise with 0 as a common element some t-plet would occur more than once in the first array. Hence increasing t by one can increase the number of constraints at most by one.

The inequality given above represents a substantial improvement over a similar inequality due to Rao [8]. Rao's result states that the number of constraints k is bounded above by

$$s^t - 1 \geqq C_1^k(s - 1) + \cdots + C_u^k(s - 1)^u \qquad \text{if } t = 2u,$$

$$s^t - 1 \geqq C_1^k(s - 1) + \cdots + C_u^k(s - 1)^u + C_u^{k-1}(s - 1)^{u+1} \qquad \text{if } t = 2u + 1.$$

When $t = 3$, the Rao bound is $s + 2$, so that we have reduced the bound by unity if s is odd. When $t = 4$ and $s = 2$, the Rao bound is 5, agreeing with our result. When $s = 3$ and $t = 4$, the bound is 6 against our 5; when $s = 4$ and $t = 4$, the bound is 7 against our 5; when $s = 5$ and $t = 4$, we have 9 against 7. The differential tends to increase both with increasing s and increasing t. Thus when $t = 6$ and $s = 11$, the Rao bound is 22 against our 15.

3. Construction of orthogonal arrays of index unity. We now prove the following theorem which, in conjunction with a corollary, provides a complete answer to the problem of construction of orthogonal arrays of index unity and strength three when s is a prime or a power of a prime.

THEOREM. *If* $s = p^n$, *where* p *is a prime and* $s > t$, *then we can construct the array* $(s^t, s + 1, s, t)$.

PROOF. Let $GF(s)$ denote the finite Galois field with $s = p^n$ elements which may be denoted by e_i, $i = 0, 1, \cdots, s - 1$. Consider the polynomials

$$y_j(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1x + a_0,$$

where the coefficients range over the field $GF(s)$. It is clear that there are s^t such polynomials, since each of the t coefficients can assume s different values in the field, and the subscript j ranges over the values $0, 1, \cdots, s^t - 1$. We now form an s by s^t array numbering the rows from 0 to $s - 1$ and the columns from 0 to $s^t - 1$. In the ith row and jth column we agree to insert the integer u with the property

$$y_j(e_i) = e_u.$$

We assert that the resulting array is orthogonal of strength t and index unity.

Suppose on the contrary that we can select t rows such that two t-plets are identical, and let the associated polynomials be

$$(1)\qquad \begin{aligned} a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1x + a_0 &= y_j(x), \\ a'_{t-1}x^{t-1} + a'_{t-2}x^{t-2} + \cdots + a'_1x + a'_0 &= y_{j'}(x). \end{aligned}$$

Let the rows be those rows which correspond to the Galois field elements $e_{i_1}, e_{i_2}, \cdots, e_{i_t}$. Upon inserting the element e_{i_r} in equations (1) above and subtracting these two equations, we have

$$A_{t-1}e_{i_r}^{t-1} + A_{t-2}e_{i_r}^{t-2} + \cdots + A_1e_{i_r} + A_0 = 0,$$

where $A_u = a'_u - a_u$. As we allow r to range from 1 to t, we secure t homogeneous equations linear in the t quantities $A_{t-1}, A_{t-2}, \cdots, A_1, A_0$. Not all the A's can be zero, since then the two polynomials would be identical. Consequently for a solution to exist the determinant of the matrix V, where

$$V = \begin{bmatrix} e_{i_1}^{t-1} & e_{i_1}^{t-2} & \cdots & e_{i_1} & 1 \\ e_{i_2}^{t-1} & e_{i_2}^{t-2} & \cdots & e_{i_2} & 1 \\ \cdot & \cdot & & & \cdot \\ \cdot & \cdot & & & \cdot \\ \cdot & \cdot & & & \cdot \\ e_{i_t}^{t-1} & e_{i_t}^{t-2} & \cdots & e_{i_t} & 1 \end{bmatrix},$$

must vanish. However, it is well known that this matrix of Vandermonde type has the property

$$\det [V] = \prod_{u<v} (e_{i_u} - e_{i_v}),$$

and so is nonsingular unless $e_{i_u} = e_{i_v}$, which is clearly impossible since the rows were all distinct.

We have thus shown that all t-plets are distinct, and this completes the demonstration that we can construct s rows. However, we can adjoin one more row in an orthogonal manner by assigning the value u to those columns which are associated with the polynomial whose leading coefficient is e_u. In this case $A_{t-1} = 0$, and we have $t - 1$ equations in $t - 1$ unknowns. Here for a solution to exist we must demand that the Vandermonde determinant of order $t - 2$ vanish, and this is impossible. (We use *order* to indicate the highest degree of terms in the matrix.)

For the special case $t = 3$, it is possible to add yet another orthogonal row when $s = 2^n$ by assigning the value u to those columns which have e_u as the coefficient of the term of degree $t - 2$. It is clear that any t-plet which is constructed by using two components from these two rows and $t - 2$ components from the original s rows occurs just once. Here both A_{t-1} and A_{t-2} vanish, and we have a nonvanishing determinant of Vandermonde type of order $t - 3$.

On the other hand, if our t-plet includes only the final row, the resultant matrix is no longer of Vandermonde type and may be singular. This cannot happen over fields of characteristic 2 when $t = 3$, for we obtain the matrix:

$$\begin{bmatrix} e_{i_1}^2 & 1 \\ e_{i_2}^2 & 1 \end{bmatrix}.$$

The determinant of the matrix is $(e_{i_1} - e_{i_2})(e_{i_1} + e_{i_2})$, and since every element is its own additive inverse in fields of characteristic 2, it is clear that the matrix is nonsingular. We may therefore state the

COROLLARY. *For the array* $(s^3, k, s = p^n, 3)$, *where* p *is a prime, we have*

$$f(s^3, s, 3) = s + 1, s = p^n, \qquad p \text{ an odd prime,}$$
$$f(s^3, s, 3) = s + 2, s = 2^n,$$

by virtue of this construction and the inequalities of Section 2.

THEOREM. *If* $s \leqq t, f(s^t, s, t) = t + 1$, *where* $s = p^n$, p *a prime.*

PROOF. In Section 2, we showed that for this case $f(s^t, s, t) \leqq t + 1$. We now show that this bound is attainable by using the same constructive procedure employed in securing the additional rows in the last case we discussed. For example, the third row will have the integer u in every column which has e_u as the coefficient of the term of degree $t - 3$. In this way we clearly succeed in constructing an array of strength t and index unity which is orthogonal. To this array we can add another row by the process we first used where we now substitute into the various polynomials one of the nonzero elements of the field. For convenience we may as well associate the additional row with the unity of our field. It is clear that the matrix is nonsingular; indeed, it consists of a single nonzero term.

We may summarize these results when $t > 3$ as follows:

(i) If $s = 2^n > t$, then $s + 1 \leqq f(s^t, s, t) \leqq s + t - 1$.

(ii) If $s = p^n > t$, where p is an odd prime, then $s + 1 \leqq f(s^t, s, t) \leqq s + t - 2$.

4. Uses of orthogonal arrays. A problem which often arises in the design of an experiment is that of ascertaining the effect of quantitative or qualitative alterations in the various components upon some measurable characteristic of the complete assembly. The traditional case is that of k fertilizers each of which can be applied at s different levels. To carry out a complete factorial experiment would require s^k plots or *assemblies* to use a more general term applicable to any type of experiment, agronomic or otherwise.

Rao [8] has shown that if the design is an array of strength t, then the estimates of main effects and interactions are unaffected by interactions of order greater than one and less than $t - 1$, but the estimate of error is enhanced by their presence. If t is even, we can measure interactions up to order $t/2$ supposing the higher order interactions absent. When t is odd, we can measure interactions up to order $(t - 1)/2$. Thus an array of appropriate strength must be chosen to handle those interactions which are deemed important, but it will not in general be necessary to construct an array of size s^k.

REFERENCES

[1] R. C. Bose, "On the application of the properties of Galois fields to the construction of hyper Graeco-Latin squares," *Sankhyā*, Vol. 3 (1938), pp. 328–338.

[2] R. C. Bose and K. R. Nair, "On complete sets of Latin squares," *Sankhyā*, Vol. 5 (1941), pp. 361–382.

[3] R. H. Bruck and H. J. Ryser, "The nonexistence of certain finite projective planes," *Canadian Jour. Math.*, Vol. 1 (1949), pp. 88–94.

[4] R. A. Fisher, "A system of confounding for factors with more than two alternatives giving completely orthogonal cubes and higher powers," *Annals of Eugenics*, Vol. 12 (1942), pp. 283–290.

[5] R. A. Fisher and F. Yates, "The 6 × 6 Latin squares," *Proc. Cambridge Philos. Soc.*, Vol. 30 (1934), pp. 482–507.

[6] H. F. MacNeish, "Euler's squares," *Annals of Mathematics*, Vol. 23 (1922), pp. 221–227.

[7] H. B. Mann, "The construction of orthogonal Latin squares," *Annals of Math. Stat.*, Vol. 13 (1942), pp. 418–423.

[8] C. R. Rao, "Factorial arrangements derivable from combinatorial arrangements of arrays," *Jour. Roy. Stat. Soc.*, Vol. 9 (1947), pp. 128–139.

[9] C. R. Rao, "On a class of arrangements," *Proc. Edinburgh Math. Soc.*, Vol. 8 (1949), pp. 119–125.

[10] W. L. Stevens, "The completely orthogonalized Latin square," *Annals of Eugenics*, Vol. 9 (1939), pp. 82–93.

[11] G. Tarry, "Le problème des 36 officiers," *Comptes Rendus de l'Association Française pour l'Avancement de Science Naturel*, Vol. 1 (1900), pp. 122–123; Vol. 2 (1901), pp. 170-203.