FURTHER RESULTS ON THE CONSTRUCTION OF MUTUALLY ORTHOGONAL LATIN SQUARES AND THE FALSITY OF EULER'S CONJECTURE

R. C. BOSE, S. S. SHRIKHANDE, AND E. T. PARKER

1. Introduction.

If

$$p_1^{n_1} p_2^{n_2} \dots p_u^{n_u}$$

is the prime power decomposition of an integer v, and we define the arithmetic function $n(v)$ by

$$n(v) = \min(p_1^{n_1}, p_2^{n_2}, \dots, p_u^{n_u}) - 1,$$

then it is known, MacNeish **(10)** and Mann **(11)**, that there exists a set of at least $n(v)$ mutually orthogonal Latin squares (m.o.l.s.) of order v. We shall denote by $N(v)$ the maximum possible number of mutually orthogonal Latin squares of order v. Then the Mann-MacNeish theorem can be stated as

$$N(v) \geqslant n(v).$$

MacNeish conjectured that the actual value of $N(v)$ is $n(v)$. This conjecture seemed plausible as it implied the correctness of Euler's conjecture **(8**, p. 383, § 144**)** about the non-existence of two orthogonal Latin squares of order $v = 4t + 2$ (since $n(v) = 1$ in this case), and also the well-known result

$$N(v) = n(v) = p^m - 1 \text{ when } v = p^m \text{ and } p \text{ is a prime.}$$

MacNeish's conjecture was disproved by Parker **(12)** who showed that in certain cases $N(v) > n(v)$ by proving that if there exists a balanced incomplete block (BIB) design with v treatments, $\lambda = 1$, and block size k which is a prime power then $N(v) \geqslant k - 2$, and that this result can be improved to $N(v) \geqslant k - 1$, when the design is symmetric and cyclic.

Parker's result though it did not disprove Euler's conjecture threw serious doubts on its correctness. Bose and Shrikhande **(4)** were able to obtain a counter example by using a general class of designs, viz., the pairwise balanced designs of index unity. They showed **(6)** that Euler's conjecture is false for an infinity of values of $v \geqslant 22$, and obtained improved lower bounds for $N(v)$ for a large class of values of v.

By using the method of differences Parker **(13)** showed that $N(v) \geqslant 2$ for

Received August 30, 1959. This research was supported in part by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF 49(638)-213. Reproduction in whole or in part is permitted for any purpose of the United States Government.

$v = \frac{1}{2}(3q - 1)$, where q is a prime power $\equiv 3 \pmod 4$. This includes the case $v = 10$.

In the present paper (i) the main theorem of **(6)** has been improved enabling us to obtain better bounds on $N(v)$, (ii) the method of differences has been used to show that $N(v) \geqslant 2$ when $v = 14$, 26, or $12t + 10$, and (iii) Euler's conjecture has been shown to be false for all $v = 4t + 2 > 6$.

2. Definitions and notations. We shall try to adhere as much as possible to the notation and definitions used in **(6)**.

A Latin square of order v may be defined as an arrangement of v symbols say, $1, 2, \ldots, v$ in a $v \times v$ square such that each symbol occurs exactly once in every row and once in every column. Two Latin squares are said to be orthogonal if, when they are superposed, each symbol of the first square occurs just once with each symbol of the second square. A set of mutually orthogonal Latin squares is a set of Latin squares any two of which are orthogonal.

An orthogonal array $(k^2, q + 1, k, 2)$ of size k^2, $q + 1$ constraints, k levels and strength 2 is a $k^2 \times (q + 1)$ matrix A whose elements are k symbols, such that every two-rowed submatrix of A contains as a column vector every possible pair of symbols. It is well known **(7; 14)** that the existence of $q - 1$ mutually orthogonal $k \times k$ Latin squares implies the existence of an orthogonal array $(k^2, q + 1, k, 2)$ and conversely.

An arrangement of v objects (called treatments) in b sets (called blocks) will be called a pairwise balanced design of index unity and type $(v; k_1, k_2, \ldots, k_m)$ if each block contains either $k_1, k_2, \ldots,$ or k_m treatments which are all distinct $(k_i \leqslant v, k_i \neq k_j)$, and every pair of distinct treatments occurs in exactly one block of the design. If the number of blocks containing k_i treatments is b_i, then clearly

$$b = \sum_{i=1}^{m} b_i, \qquad v(v - 1) = \sum_{i=1}^{m} b_i k_i (k_i - 1). \tag{2.1}$$

Consider a pairwise balanced design (D) of index unity and type $(v; k_1, k_2, \ldots, k_m)$. The subdesign (D_i) formed by the blocks of size k_i will be called the ith equiblock component of (D), $i = 1, 2, \ldots, m$.

A subset of blocks belonging to any equiblock component (D_i) will be said to be of type I if every treatment occurs in the subset exactly k_i times. The number of blocks in such a subset is clearly v. As noted by Levi using König's theorem on the decomposition of even regular graphs **(9**, pp. 4–6**)**, we can rearrange the treatments within the blocks of the subset in such a way that every treatment comes in each position exactly once. If the v blocks of the subset are written out as columns, each treatment occurs exactly once in every row. When so written out the blocks will be said to be in the standard form. A subset of blocks belonging to (D_i) will be said to be of type II if every treatment occurs in the subset exactly once. The component (D_i) will be defined to be separable if the blocks can be divided into subsets of type I or

type II (both types may occur at the same time). The design (D) is defined to be separable if each equiblock component is separable.

The set of equiblock components $(D_1), (D_2), \ldots, (D_l)$, $l < m$, will be said to be a clear set if the $\sum_{i=1}^{l} b_i$ blocks comprising $(D_1), (D_2), \ldots, (D_l)$ are disjoint, that is, no two blocks contain a common treatment. Clearly a necessary condition for this is

$$\sum_{i=1}^{l} b_i k_i \leqslant v.$$

We shall have occasion to use the following Lemmas proved in **(6)**.

LEMMA 1. *If* $v = v_1 v_2 \ldots v_u$ *then* $N(v) \geqslant \min(N(v_1), N(v_2), \ldots, N(v_u))$.

LEMMA 2. *Suppose there exists a set* $\sum$ *of* $q - 1$ m.o.l.s. *of order* k, *then we can construct a* $q \times k(k-1)$ *matrix* P, *whose elements are the symbols* $1, 2, \ldots, k$ *and such that* (i) *any ordered pair*

$$\binom{i}{j}, \quad i \neq j$$

occurs as a column exactly once in any two-rowed submatrix of P, (ii) P *can be subdivided into* $k - 1$ *submatrices* $P_1, P_2, \ldots, P_{k-1}$ *of order* $q \times k$ *such that in each row of* P_c, $1 \leqslant c \leqslant k - 1$, *each of the symbols* $1, 2, \ldots, k$ *occurs exactly once.*

Let δ be a $k \times 1$ column vector, then following the notation used in **(6)**, we shall denote by $P(\delta)$ the $q \times k(k-1)$ matrix obtained from P on replacing the symbol i by the element occurring in the ith position in δ. A similar meaning will be assigned to $P_i(\delta)$ and $\pi_{cj}(\delta)$ where π_{cj} denotes the jth column of P_c. If D is a $k \times b$ matrix defined by

$$D = [\delta_1, \delta_2, \ldots, \delta_b]$$

where δ_j is a $k \times 1$ column vector, then we define $P(D)$ and $P_i(D)$ by

$$P(D) = [P(\delta_1), P(\delta_2), \ldots, P(\delta_b)]$$
$$P_i(D) = [P_i(\delta_1), P_i(\delta_2), \ldots, P_i(\delta_b)].$$

3. Main theorem. The theorem proved in this section is an improvement of the main theorem of **(6)**.

THEOREM 1. *Let there exist a pairwise balanced design* (D) *of index unity and type* $(v; k_1, k_2, \ldots, k_m)$ *such that the set of equiblock components* $(D_1), (D_2), \ldots, (D_l)$, $l < m$, *is a clear set. If there exist* $q_i - 1$ *mutually orthogonal Latin squares of order* k_i *and if*

$$q^* = \min(q_1 + 1, \ldots, q_l + 1, q_{l+1}, \ldots, q_m),$$

then there exist at least $q^* - 2$ *mutually orthogonal Latin squares of order* v.

Proof. Let us define

$$q^{(1)} = \min(q_1 + 1, q_2 + 1, \ldots, q_l + 1)$$

and

$$q^{(2)} = \min(q_{l+1}, q_{l+2}, \ldots, q_m).$$

Then

$$q^* = \min(q^{(1)}, q^{(2)}).$$

Let

$$\delta_{i1}, \delta_{i2}, \ldots, \delta_{ib_i}$$

be the blocks of the equiblock component (D_i) written out as columns $(i \leqslant l)$. By hypothesis there exist $q_i - 1$ mutually orthogonal Latin squares of order k_i. Hence we can construct an orthogonal array A_{ij} with $q_i + 1$ rows and k_i^2 columns, whose symbols are the treatments occurring in δ_{ij}. Let

$$A_i = [A_{i1}, A_{i2}, \ldots, A_{ib_i}].$$

Let Δ_i be the $q^* \times b_i k_i^2$ matrix obtained from A_i by retaining only the first q^* rows, and let

$$\Delta^{(1)} = [\Delta_1, \Delta_2, \ldots, \Delta_l].$$

Then $\Delta^{(1)}$ has q^* rows and $\sum b_i k_i^2$ columns. Clearly $\Delta^{(1)}$ has the property that if t_c and t_d are any two treatments identical or distinct contained in any block of $(D_1), (D_2), \ldots,$ or (D_l), then the ordered pair t_c, t_d occurs as a column exactly once in any two-rowed submatrix of $\Delta^{(1)}$.

Let Δ_u be the matrix obtained from $P_u(D_u)$ by retaining only the first q^* rows, $u = l + 1, \ldots, m$. Then

$$\Delta^{(2)} = [\Delta_{l+1}, \Delta_{l+2}, \ldots, \Delta_m]$$

has the property that if t_a and t_b are any two distinct treatments contained in any block of $(D_{l+1}), \ldots, (D_m)$ then the ordered pair t_a, t_b occurs exactly once in any two-rowed submatrix of $\Delta^{(2)}$. The number of columns in $\Delta^{(2)}$ is

$$\sum_{u=l+1}^{m} b_u k_u (k_u - 1).$$

Again let $\Delta^{(3)}$ be the $q^* \times v_2$ matrix whose nth column contains in every position the treatment t_n, where t_n is any one of the

$$v_2 = v - \sum_{i=1}^{l} b_i k_i$$

treatments not contained in $(D_1), (D_2), \ldots,$ or (D_l). Then $[\Delta^{(1)}, \Delta^{(2)}, \Delta^{(3)}]$ is an orthogonal array $(v^2, q^*, v, 2)$, and using any two rows for co-ordinatization we get $q^* - 2$ mutually orthogonal Latin squares of order v.

4. Use of BIB designs. A balanced incomplete block (BIB) design with parameters v, b, r, k, λ is an arrangement of v objects or treatments into b sets or blocks such that (i) each block contains $k < v$ different treatments,

(ii) each treatment occurs in r different blocks, and (iii) each pair of treatments occurs together in exactly λ blocks. The parameters satisfy the relations

$$\lambda(v-1) = r(k-1), \quad bk = vr, \quad b \geqslant v.$$

These conditions are necessary but not sufficient for the existence of a BIB design. BIB designs were first introduced into statistical studies by Yates **(15)**, but occur in earlier literature in connection with various combinatorial problems. Subsequent to Yates many authors have dealt with the problem of constructing these designs. Without attempting a complete bibliography we shall only refer to **(1)**. A BIB design is said to be symmetric if $v = b$, and in consequence $k = r$. A BIB design is said to be resolvable **(2)** if the blocks can be divided into sets, such that the blocks of a given set contain each treatment exactly once. A resolvable or a symmetric BIB design is evidently separable.

A BIB design with $\lambda = 1$ is clearly a pairwise balanced design of index unity and type $(v; k)$. We shall denote such a design by BIB $(v; k)$.

By omitting a single treatment from the design BIB $(v; k)$ we get a pairwise balanced design of index unity and type $(v-1; k, k-1)$ where the r blocks of size $k-1$ form a clear set. Again if from a BIB $(v; k)$ we delete x treatments belonging to the same block, $2 \leqslant x \leqslant k$, we get a pairwise balanced design of index unity and type $(v-x; k, k-1, k-x)$ where the equiblock component consisting of the single block of size $k-x$ is clear. Hence we have

THEOREM 2. *Existence of a BIB* $(v; k)$ *implies*

(i) $N(v-1) \geqslant \min(N(k), 1 + N(k-1)) - 1$,

(ii) $N(v-x) \geqslant \min(N(k), N(k-1), 1 + N(k-x)) - 1$, if $2 \leqslant x \leqslant k$.

Example (1). Consider the BIB design with parameters $v = b = s^2 + s + 1$, $r = k = s + 1$, $\lambda = 1$, with $s = 16$. Taking $x = 6, 8, 9$ respectively we get $N(267) \geqslant 10$, $N(265) \geqslant 8$, $N(264) \geqslant 7$, whereas $n(267) = 2$, $n(265) = 4$ and $n(264) = 2$.

Suppose we omit three treatments $\alpha_1, \alpha_2, \alpha_3$ not occurring in the same block of a BIB $(v; k)$, then we get a pairwise balanced design (D) of index unity and type $(v-3; k, k-1, k-2)$. Since in the original BIB $(v; k)$ no two blocks can have more than one treatment in common, the three blocks of (D) of size $k-2$ which have been obtained by deleting (α_1, α_2), (α_2, α_3), (α_1, α_3) have obviously no treatment in common and form a clear equiblock component. Hence we get

THEOREM 3. *The existence of a* BIB $(v; k)$ *implies that*

$$N(v-3) \geqslant \min(N(k), N(k-1), 1 + N(k-2)) - 1.$$

Example (2). Consider the BIB $(v; k)$ designs **(1**, pp. 386–389**)** with $k = 5$ and $v = 21, 25, 41, 45, 61, 65, 85, 125$. It follows that there exist at least two m.o.l.s. of the following orders: 18, 22, 38, 42, 58, 62, 82, and 122.

Example (3). From the designs BIB (81; 9) and BIB (73; 9) we get $N(78) \geqslant 6$, $N(70) \geqslant 6$.

Example (4). From the design BIB (273; 17) we get $N(270) \geqslant 2$ since $N(15) \geqslant n(15) = 2$.

Suppose there exists a resolvable BIB design with parameters v, b, r, k, $\lambda = 1$. Let $1 < x \leqslant r$. To each block of the ith replication add a new treatment θ_i, $i = 1, 2, \ldots, x$, and add a new block $\theta_1, \theta_2, \ldots, \theta_x$. We then get a pairwise balanced design of index unity and type $(v + x; k + 1, k, x)$ if $x < r$, and type $(v + x; k + 1, r)$ if $x = r$. The equiblock component formed by the new block is clear. When $x = r - 1$, the set of equiblock components consisting of the new block, and the blocks of the rth replication is a clear set. Again by adding a treatment θ to all the blocks of a single replication we get $(v + 1; k + 1, k)$. Hence we have

THEOREM 4A. *The existence of a resolvable* BIB $(v; k)$ *implies*

(i) $N(v + x) \geqslant \min(N(k), N(k + 1), 1 + N(x)) - 1$ if $1 < x \leqslant r - 2$,
(ii) $N(v + r - 1) \geqslant \min(1 + N(k), N(k + 1), 1 + N(r - 1)) - 1$,
(iii) $N(v + r) \geqslant \min(N(k + 1), 1 + N(r)) - 1$,
(iv) $N(v + 1) \geqslant \min(N(k), N(k + 1)) - 1$.

Example (5). Taking $x = 5$ in the BIB design with $v = 49$, $b = 56$, $r = 8$, $k = 7$, $\lambda = 1$, we have

$$N(54) \geqslant \min(N(7), N(8), 1 + N(5)) - 1 = 4.$$

Example (6). Using the resolvable BIB design $v = 21$, $b = 70$, $r = 10$, $k = 3$, $\lambda = 1$, **(5**, p. 171, Table III**)** we have from part (ii) of the theorem $N(30) \geqslant 2$.

Again suppose there exists a separable BIB $(v; k)$ in which the blocks can be divided into n sets of type I. The number of replications is $r = kn$. For a symmetric design $n = 1$. Let the blocks be written out as columns, and let (S_j) be the jth subset, the blocks being in the standard form $(j = 1, 2, \ldots, n)$. Let us take r new treatments θ_{ij}, $i = 1, 2, \ldots, k$; $j = 1, 2, \ldots, n$. Let us define the $1 \times v$ row vector $\Theta_{ij} = (\theta_{ij}, \theta_{ij}, \ldots, \theta_{ij})$. Then we can denote by

$$\begin{pmatrix} S_j \\ \Theta_{ij} \end{pmatrix}$$

the result of adding θ_{ij} in the $(k + 1)$th position to each block of the jth subset.

Let $N(k + 1) = q^{(1)} - 1$. Then we can construct a $q^{(1)} \times (k + 1)k$ matrix $P^{(1)}$ with the properties (i) and (ii) of Lemma 2, where $P_1^{(1)}, P_2^{(1)}, \ldots, P_k^{(1)}$ are the submatrices referred to in part (ii). If δ_{ju} is the uth block of (S_j), $u = 1, 2, \ldots, v$, then the corresponding block of

$$\begin{pmatrix} S_j \\ \Theta_{ij} \end{pmatrix}$$

is

$$\begin{pmatrix} \delta_{ju} \\ \theta_{ij} \end{pmatrix}.$$

Consistent with our notation we can denote by

$$P_i^{(1)} \begin{pmatrix} \delta_{ju} \\ \theta_{ij} \end{pmatrix}$$

the result of replacing the symbols $1, 2, \ldots, k, k+1$ in $P_i^{(1)}$ by treatments in the 1st, 2nd, ..., $(k+1)$th position in

$$\begin{pmatrix} \delta_{ju} \\ \theta_{ij} \end{pmatrix}$$

and define

$$P_i^{(1)} \begin{pmatrix} S_j \\ \Theta_{ij} \end{pmatrix} \equiv \left[P_i^{(1)} \begin{pmatrix} \delta_{j1} \\ \theta_{ij} \end{pmatrix}, \ldots, P_i^{(1)} \begin{pmatrix} \delta_{jv} \\ \theta_{ij} \end{pmatrix} \right].$$

A pair of distinct treatments belonging to the original BIB design may be called a pure pair. Again a pair of treatments, one of which belongs to the original BIB design, and the other to the newly added treatments, may be called a mixed pair. Then

$$\Delta_1 = \left[\ldots, P_i^{(1)} \begin{pmatrix} S_j \\ \Theta_{ij} \end{pmatrix}, \ldots \right], i = 1, 2, \ldots, k; j = 1, 2, \ldots, n$$

has the property that any two-rowed submatrix contains as a column each pure and each mixed ordered pair of treatments exactly once.

Again if $q^{(2)} - 1 = N(r)$, we can form an orthogonal array $\Delta_2 = (r^2, q^{(2)}+1, r, 2)$ whose symbols are the r new treatments. Let

$$q = \min(q^{(1)}, q^{(2)} + 1)$$

and let $\Delta^{(1)}$ and $\Delta^{(2)}$ be obtained from Δ_1 and Δ_2 respectively by retaining the first q rows only. Also let $\Delta^{(3)}$ be the $q \times v$ matrix whose uth column contains the uth treatment of the BIB design in each position. Then

$$\Delta = [\Delta^{(1)}, \Delta^{(2)}, \Delta^{(3)}]$$

is an orthogonal array of size $(v+r)^2$, q constraints, $v+r$ levels and strength 2, and is therefore equivalent to a set of $q-2$ mutually orthogonal Latin squares. Hence we have

THEOREM 4B. *If there exists a* BIB $(v; k)$ *with* r *replications, in which the blocks can be subdivided into sets of type I, then*

$$N(v+r) \geqslant \min(N(k+1), 1 + N(r)) - 1.$$

Example (7). The existence of symmetric BIB (7; 3) and BIB (57; 8) implies $N(10) \geqslant 2$ and $N(65) \geqslant 7$.

Example (8). There exists a BIB design **(1**, p. 383**)** with parameters $v = 25$, $b = 50$, $r = 8$, $k = 4$, $\lambda = 1$ for which the blocks can be separated into two subsets of type I. It follows that $N(33) \geqslant 3$.

Theorems 4A and 4B are special cases of the following more general theorem, the proof of which can be given on analogous lines.

THEOREM 4. *If there exists a separable* BIB $(v; k)$ *with* n_1 *subsets of type I and* n_2 *subsets of type II, so that the number of replications is* $r = kn_1 + n_2$, *then*

(i) $N(v + x) \geqslant \min(N(k), N(k + 1), 1 + N(x)) - 1$, if $x = kr_1 + r_2$; $r_1 \leqslant n_1$, $r_2 \leqslant n_2$; $1 < x < r - 1$.

(ii) $N(v + r - 1) \geqslant \min(1 + N(k), N(k + 1), 1 + N(r - 1)) - 1$ if $n_2 > 0$.

(iii) $N(v + r) \geqslant \min(N(k + 1), 1 + N(r)) - 1$.

(iv) $N(v + 1) \geqslant \min(N(k + 1), N(k)) - 1$ if $n_2 > 0$.

5. Use of GD designs. An arrangement of v objects (treatments) in b sets (blocks) each containing k distinct treatments is said to be a group divisible (GD) design if the treatments can be divided into l groups of m treatments each, so that any two treatments belonging to the same group occur together in λ_1 blocks, and any two treatments from different groups occur together in λ_2 blocks. We will denote such a design by the notation GD $(v; k, m; \lambda_1, \lambda_2)$. The combinatorial properties of these designs have been studied in **(3)** where it has been shown that

$$v = lm, \quad bk = vr, \quad \lambda_1(m - 1) + \lambda_2 m(l - 1) = r(k - 1),$$

r being the number of replications, that is, the number of times each treatment occurs in the design. It has also been shown that

$$P = rk - \lambda_2 v \geqslant 0, \qquad Q = r - \lambda_1 \geqslant 0.$$

The GD designs can be divided into three classes.

(i) Regular (R) characterized by $P > 0$, $Q > 0$.

(ii) Semi-regular (SR) characterized by $P = 0$, $Q > 0$.

(iii) Singular (S) characterized by $Q = 0$.

Methods of constructing these designs have been given in **(5)**. So far as the construction of mutually orthogonal Latin squares is concerned a special role is played by GD designs with $\lambda_1 = 0$, $\lambda_2 = 1$, which in our notation can be denoted by GD$(v; k, m; 0, 1)$. If, further, this design is regular we shall denote it by RGD$(v; k, m; 0, 1)$ and if it is semi-regular we shall denote it by SRGD$(v; k, m; 0, 1)$.

If to the b blocks of the GD design with $\lambda_1 = 0$, $\lambda_2 = 1$, we add l new blocks corresponding to the groups, we get a pairwise balanced design of index unity and type $(v; k, m)$. The blocks of size m form a clear equiblock component. Hence we have

THEOREM 5. *If there exists a* GD$(v; k, m; 0, 1)$ *then*

$$N(v) \geqslant \min(N(k), 1 + N(m)) - 1.$$

COROLLARY. $N(s^2 - 1) \geqslant N(s - 1)$, *if* s *is a prime power.*

This follows from the existence of a resolvable GD$(s^2 - 1; s, s - 1; 0, 1)$.

THEOREM 6. *If there exists a* GD$(v; k, m; 0, 1)$ *then*

$$N(v - 1) \geqslant \min(N(k), N(k - 1), 1 + N(m), 1 + N(m - 1)) - 1,$$

and if the design is resolvable then

$$N(v - 1) \geqslant \min(N(k), N(k - 1), N(m), N(m - 1)).$$

The first part follows from the fact that if we omit any particular treatment from the corresponding pairwise balanced design of index unity and type $(v; k, m; 0, 1)$ we get a design of the type $(v - 1; k, k - 1; m, m - 1)$, in which the equiblock components with blocks of sizes m and $m - 1$ form a clear set. The second part has already been proved in **(6)** and is given here for completeness.

THEOREM 7. *Suppose there exists a resolvable* GD$(v; k, m; 0, 1)$ *with* r *replications, then*

(i) $N(v + 1) \geqslant \min(N(k), N(k + 1), 1 + N(m)) - 1$,

(ii) $N(v + x) \geqslant \min(N(k), N(k + 1), 1 + N(m), 1 + N(x)) - 1$ if $1 < x < r$,

(iii) (a) $N(v + r) \geqslant \min(N(k + 1), 1 + N(m), 1 + N(r)) - 1$,

(b) $N(v + r) \geqslant \min(N(k + 1), N(m + 1), 1 + N(k), 1 + N(r)) - 1$,

(iv) $N(v + r + 1) \geqslant \min(N(k + 1), N(m + 1), 1 + N(r + 1)) - 1$,

where in part (iii) *we choose whichever lower bound is better for* $N(v + r)$.

To prove part (i) we add a new treatment θ_1 to each block of one replication. To prove part (ii) we add a new treatment θ_i to each block of the ith replication, $i = 1, 2, \ldots, x$, and take a new block $(\theta_1, \theta_2, \ldots, \theta_x)$. For the first part we note that the equiblock component given by the groups forms a clear set. For the second part we note that the set of equiblock components given by the groups and the new block is a clear set. To prove part (iii) (a) we add a new treatment θ_i to each block of the ith replication, $i = 1, 2, \ldots, r$, and a new block $(\theta_1, \theta_2, \ldots, \theta_r)$. To prove part (iii) (b) we add a new treatment θ_i to each block of the ith replication for the first $r - 1$ replications, and a new treatment θ_0 to each of the groups, and add a new block $(\theta_0, \theta_1, \ldots, \theta_{r-1})$. We note in this case that the set of equiblock components given by the rth replication, and the newly added block is a clear set. To prove (iv) we add one new treatment to the blocks of each replication, one new treatment to each of the blocks corresponding to the groups, and take a block containing the new treatments.

The group designs most useful to us are the semi-regular group divisible designs with $\lambda_1 = 0$, $\lambda_2 = 1$. For such a design the number of replications r is equal to the group size m, and $v = km$ In the notation used in **(6)** such a design is denoted by SRGD $(km; k, m; 0, 1)$. It is known **(5)** that for an

SRGD design each block contains the same number of treatments from each group. We shall now prove

LEMMA 3. *There exists a resolvable* SRGD $(km; k, m; 0, 1)$ *if* $k \leqslant N(m) + 1$. *For this design the block size is* k, $r = m$, *and* $b = m^2$.

Applying Lemma 2 we find that there exists a matrix P with $N(m) + 1$ rows and $m(m-1)$ columns such that in every two-rowed submatrix of P every ordered pair of distinct symbols occurs exactly once, and it can be subdivided into $m - 1$ parts such that in each row of every part every symbol occurs once. Let P_k be the matrix obtained from P by retaining only k rows. Let E_k be a $k \times m$ matrix such that the ith column contains the ith symbol in each position. Let $\Delta_k = [E_k, P_k]$. Now let us consider km treatments $t_1, t_2, \ldots, t_{km}$. Let the symbols $1, 2, \ldots, m$ in the jth row of Δ_k be replaced by

$$t_{\alpha+1}, t_{\alpha+2}, \ldots, t_{\alpha+m} \quad \text{where} \quad \alpha = (j-1)m.$$

This gives an SRGD with the required properties. The blocks are given by the columns. The replications consist of E_k and subdivisions of P_k.

Combining Lemma 3 and Theorem 7 we have

THEOREM 8. *If* $k \leqslant N(m) + 1$, *then*

(i) $N(km + 1) \geqslant \min(N(k), N(k+1), 1 + N(m)) - 1$,

(ii) $N(km + x) \geqslant \min(N(k), N(k+1), 1 + N(m), 1 + N(x)) - 1$ if $1 < x < m$.

Example (9). Taking k, m, and x as shown we derive the lower bound for $N(km + x)$, noting that $N(24) \geqslant 3$ from Table 1 of **(6)** and $N(10) \geqslant 2$ from Example (7), Theorem 4B.

(i)	$k = 7,\ m = 11,\ x = 5;$	$N(82) \geqslant 4,$
(ii)	$k = 8,\ m = 11,\ x = 7;$	$N(95) \geqslant 6,$
(iii)	$k = 7,\ m = 19,\ x = 5;$	$N(138) \geqslant 4,$
(iv)	$k = 7,\ m = 8,\ x = 4;$	$N(60) \geqslant 3,$
(v)	$k = 4,\ m = 24,\ x = 10;$	$N(106) \geqslant 2,$
(vi)	$k = 8,\ m = 13,\ x = 7;$	$N(111) \geqslant 6,$
(vii)	$k = 4,\ m = 27,\ x = 10;$	$N(118) \geqslant 2,$
(viii)	$k = 7,\ m = 16,\ x = 10;$	$N(122) \geqslant 2,$
(ix)	$k = 7,\ m = 17,\ x = 5;$	$N(124) \geqslant 4.$

6. Use of the method of differences. Let $0, 1, 2, \ldots, n-1$ be the elements of the ring R of residue classes (mod n). We shall consider matrices whose elements belong either to R or to the set X of m indefinites $x_1, x_2, \ldots, x_m$. We shall say that the difference associated with the ordered pair $\binom{i}{j}$, where i and j belong to R is c where $i - j \equiv c \pmod{n}$, $0 \leqslant c < n$. Conversely to each element c of R there correspond n ordered pairs which have c as their associated difference. If $\binom{i}{j}$ is one of these pairs then the other pairs are $\binom{i+\theta}{j+\theta}$ where $\theta = 0, 1, 2, \ldots, n-1$, and $i + \theta$ and $j + \theta$ are reduced (mod n).

The ordered pair $\binom{i}{j}$ both members of which belong to R will be called an R-pair. A pair $\binom{i}{x_j}$ where i belongs to R and x_j to X is called an RX-pair and the difference associated with it is defined to be x_j. If θ is any element of R we shall formally define $x_j + \theta = x_j$. With this definition, corresponding to any indefinite x_j, there are n RX pairs, the difference associated with each of which is x_j. If $\binom{i}{x_j}$ is one of these pairs then the other pairs are $\binom{i+\theta}{x_j}$ where $\theta = 0, 1, \ldots, n-1$. These pairs are of course all the pairs $\binom{i}{x_j}$, $i = 0, 1, \ldots, n-1$ in some order or other. We may similarly define XR pairs. The difference associated with the XR pair $\binom{x_i}{j}$ is x_i.

We shall now prove the following theorem:

THEOREM 9. *If m is odd there exist at least two orthogonal Latin squares of order $3m + 1$. Taking $m = 4t + 3$ this implies the existence of a pair of orthogonal Latin squares for all orders $12t + 10$.*

Consider the $4 \times 4m$ matrix A_0 given below (to exhibit the structure of A_0 it is divided into 4 parts), whose elements belong to R the ring of residue classes mod$(2m + 1)$ or X the set of indefinites $x_1, x_2, \ldots, x_m$.

$$A_0 = \begin{bmatrix} 0 & 0 & \ldots 0 & 1 & 2 & \ldots m & 2m & 2m-1 & \ldots m+1 \\ 1 & 2 & \ldots m & 0 & 0 & \ldots 0 & x_1 & x_2 & \ldots x_m \\ 2m & 2m-1 & \ldots m+1 & x_1 & x_2 & \ldots x_m & 0 & 0 & \ldots 0 \\ x_1 & x_2 & \ldots x_m & 2m & 2m-1 & \ldots m+1 & 1 & 2 & \ldots m \end{bmatrix}$$

$$\begin{matrix} x_1 & x_2 & \ldots x_m \\ 2m & 2m-1 & \ldots m+1 \\ 1 & 2 & \ldots m \\ 0 & 0 & \ldots 0 \end{matrix} \Bigg].$$

We note that of the $4m$ pairs occurring as columns in any two-rowed submatrix of A_0, $2m$ are R-pairs, the differences associated with which are all the non-null elements of R, m are RX-pairs the differences associated with which are all the elements of X and the same is true of XR pairs. Let A_θ be the matrix derived from A_0 by adding θ, $0 \leqslant \theta \leqslant 2m$, to every element of A_0 and reducing mod$(2m + 1)$; $x_i + \theta$ being considered as x_i. Let

$$A = [A_0, A_1, \ldots, A_{2m}].$$

Then it is evident that in any two-rowed submatrix of A, any R-pair formed by two distinct elements of R, or any RX or XR-pair occurs exactly once. Let A^* be an orthogonal array $[m^2, 4, m, 2]$ corresponding to two orthogonal Latin squares formed by the symbols $x_1, x_2, \ldots, x_m$, and let E be a $4 \times (2m + 1)$ matrix whose ith column contains i in each place $(0 \leqslant i \leqslant 2m)$. Then

$$\Delta = [E, A, A^*]$$

is an orthogonal array $[(3m + 1)^2, 4, 3m + 1, 2]$, which proves the result.

Example (10). Taking $t = 0, 1, 2, 3, 4, 8, 9$, and 12 respectively it follows that $N(v) \geqslant 2$ for $v = 10, 22, 34, 46, 58, 106, 118$, and 154.

Two superposed 10×10 orthogonal squares obtained by this method are exhibited below. The symbols x_1, x_2, x_3 have been replaced by 7, 8, 9.

A Pair of 10×10 Orthogonal Squares

00	67	58	49	91	83	75	12	24	36
76	11	07	68	59	92	84	23	35	40
85	70	22	17	08	69	93	34	46	51
94	86	71	33	27	18	09	45	50	62
19	95	80	72	44	37	28	56	61	03
38	29	96	81	73	55	47	60	02	14
57	48	39	90	82	74	66	01	13	25
21	32	43	54	65	06	10	77	88	99
42	53	64	05	16	20	31	89	97	78
63	04	15	26	30	41	52	98	79	87

We shall now give two special examples of the use of the method of differences.

Example (11). Consider the matrix

$$P_0 = \begin{bmatrix} 0 & x_1 & x_2 & x_3 \\ 1 & 0 & 0 & 0 \\ 4 & 4 & 6 & 9 \\ 6 & 1 & 2 & 8 \end{bmatrix}$$

whose elements belong to the ring R of residue classes (mod 11) and the set X of indefinites x_1, x_2, x_3. Let P_1, P_2, P_3 be obtained from P_0 by cyclic permutation of the rows, and let

$$A_0 = [P_0, P_1, P_2, P_3].$$

Then it is easy to verify that each two-rowed submatrix of A_0 contains as columns 10 R-pairs, the differences associated with which are all the non-null elements of R; 3 RX-pairs the differences associated with which are the 3 elements of X, and 3 XR pairs for which the same is true. Let A_θ be the matrix obtained from A_0 by adding θ to elements of A_0, where θ belongs to R. Then

$$A = [A_0, A_1, \ldots, A_{10}]$$

is a matrix such that any two-rowed submatrix contains as a column every R-pair consisting of distinct elements of R, and every RX and XR-pair, exactly once. If A^* is the orthogonal array of strength 2 and 4 constraints with the symbols x_1, x_2, x_3 and E is the 4×11 matrix for which the ith column contains i in every place ($i = 0, 1, \ldots, 10$) then

$$\Delta = [E, A, A^*]$$

is an orthogonal array $[14^2, 4, 14, 2]$ from which a pair of orthogonal Latin squares of order 14 can be constructed.

Example (12). Similarly by starting with the matrix

$$P_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & x_1 & x_2 & x_3 \\ 3 & 6 & 2 & 1 & 0 & 0 & 0 \\ 8 & 20 & 12 & 16 & 20 & 17 & 8 \\ 12 & 16 & 7 & 2 & 19 & 6 & 21 \end{bmatrix}$$

whose elements belong to the ring R of residue classes (mod 23) and the set X of indefinites x_1, x_2, x_3, we can construct two mutually orthogonal Latin squares of order 26.

7. Improved lower bounds for $N(v)$, $v \leqslant 154$. We give here those values of $v \leqslant 154$ for which the lower bound of $N(v)$ can be improved over the bound given in Table I of **(6)**.

TABLE I

v	$n(v)$	l.b. for $N(v)$	Remarks
10	1	2	Ex. (7), Th. 4B or Ex. (10), Th. 9
14	1	2	Ex. (11)
18	1	2	Ex. (2), Th. 3
26	1	2	Ex. (12)
30	1	2	Ex. (6), Th. 4A
33	2	3	Ex. (8), Th. 4B
34	1	2	Ex. (10), Th. 9
38	1	2	Ex. (2), Th. 3
42	1	2	Ex. (2), Th. 3
46	1	2	Ex. (10), Th. 9
54	1	4	Ex. (5), Th. 4A
60	2	3	Ex. (9) (iv), Th. 8
62	1	2	Ex. (2), Th. 3
65	4	7	Ex. (7), Th. 4B
70	1	6	Ex. (3), Th. 3
78	1	6	Ex. (3), Th. 3
82	1	4	Ex. (9) (i), Th. 8
90	1	2	$90 = 10 \times 9$ and Lemma 1
95	4	6	Ex. (9) (ii), Th. 8
106	1	2	Ex. (10), Th. 9, or Ex. (9) (v), Th. 8
111	2	6	Ex. (9) (vi), Th. 8
114	1	2	$114 = 38 \times 3$ and Lemma 1
118	1	2	Ex. (10), Th. 9, or Ex. (9) (vii), Th. 8
122	1	2	Ex. (2), Th. 3, or Ex. (9) (viii), Th. 8
124	3	4	Ex. (9) (ix), Th. 8
138	1	4	Ex. (9) (iii), Th. 8
154	1	2	Ex. (10), Th. 9, or $154 = 22 \times 7$ and Lemma 1

8. The existence of at least two orthogonal Latin squares of order $v > 6$. If v is divisible by 4 or if v is odd then $N(v) \geqslant n(v) \geqslant 2$. Hence we need only consider numbers for which $v \equiv 2 \pmod 4$. We shall first prove

LEMMA 4. *$N(v) \geqslant 2$ if $6 < v \leqslant 726$.*

This result has already been checked in Table I of **(6)**, supplemented by the improvements noted in Table I of the last section, up to $v = 154$.

Any integer v lying in the closed interval $I_i = (a_i, b_i)$ shown in column (2) of Table II can be expressed in the form

$$v = 4m_i + x_i, \qquad 10 \leqslant x_i \leqslant c_i$$

where m_i and c_i are given in columns (3) and (4), since $a_i = 4m_i + 10$, $b_i = 4m_i + c_i$.

TABLE II

i	Interval $I_i = (a_i, b_i)$	m_i	c_i
1	(158, 182)	37	34
2	(186, 218)	44	42
3	(222, 262)	53	50
4	(266, 310)	64	54
5	(314, 374)	76	70
6	(378, 454)	92	86
7	(458, 550)	112	102
8	(554, 662)	136	118
9	(666, 726)	164	70

It is readily verified that $N(m_i) \geqslant n(m_i) \geqslant 3$. Again $N(x_i) \geqslant 2$ since $10 \leqslant x_i \leqslant c_i < 154$. If we take $k = 4$ in part (ii) of Theorem 8, the conditions $k \leqslant N(m_i) + 1$ and $1 < x_i < m_i$ are obviously satisfied. Hence if v lies in any of the closed intervals I_i $(i = 1, 2, \ldots, 9)$, $N(v) \geqslant 2$. The Lemma follows by noting that any $v \equiv 2 \pmod 4$ and satisfying $154 < v \leqslant 726$ lies in one of the closed intervals I_i.

THEOREM 10. *There exist at least two orthogonal Latin squares of any order $v > 6$.*

It is sufficient to prove the theorem for numbers $v \equiv 2 \pmod 4$, $v \geqslant 730$. If v satisfies these conditions we can write

$$v - 10 = 144g + 4u, \qquad g \geqslant 5, \qquad 0 \leqslant u \leqslant 35$$

therefore

$$v = 4(36g) + 4u + 10.$$

Since the least factor in the prime power decomposition of $36g$ is necessarily greater than or equal to 4, $N(36g) \geqslant n(36g) \geqslant 3$. If in Theorem 8 part (ii)

we take $k = 4$, $m = 36g$, $x = 4u + 10$, then $k \leqslant 1 + N(m)$. Also $10 \leqslant x \leqslant 150$, $m \geqslant 180$. Hence $1 < x < m$, and $N(x) \geqslant 2$. It follows that $N(v) \geqslant 2$.

The question raised in the concluding remarks of **(6)** is thus completely answered. If a positive integer $v > 2$ is called Eulerian if two orthogonal Latin squares of order v do not exist, then 6 is the only Eulerian number.

References

1. R. C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugen. London, *9* (1939), 353-399.
2. ——— *A note on the resolvability of balanced incomplete block designs*, Sankhyā, *6* (1942), 105–110.
3. R. C. Bose and W. S. Connor, *Combinatorial properties of group divisible incomplete block designs*, Ann. Math. Stat., *23* (1952), 367–383.
4. R. C. Bose and S. S. Shrikhande, *On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order $4t + 2$*, Proc. Nat. Acad. Sci. U.S.A., *45* (1959), 734–737.
5. R. C. Bose, S. S. Shrikhande, and K. Bhattacharya, *On the construction of group divisible incomplete block designs*, Ann. Math. Stat., *24* (1953), 167–195.
6. ——— *On the construction of pairwise orthogonal Latin squares and the falsity of a conjecture of Euler*, U. N. C., Institute of Statistics, Mimeo. series no. 222. To be published in Trans. Amer. Math. Soc.
7. K. A. Bush, *Orthogonal arrays of index unity*, Ann. Math. Stat., *23* (1952), 426–434.
8. L. Euler, *Recherches sur une nouvelle espece des quarres magiques*, Verh. zeeuwsch Genoot. Weten. Vliss., *9* (1782), 85–239.
9. F. W. Levi, *Finite geometrical systems* (University of Calcutta, 1942).
10. H. F. MacNeish, *Euler squares*, Ann. Math., *23* (1922), 221–227.
11. H. B. Mann, *The construction of orthogonal Latin squares*, Ann. Math. Stat., *13* (1942), 418–423.
12. E. T. Parker, *Construction of some sets of pairwise orthogonal Latin squares*, Amer. Math. Soc. Notices *5* (1958), 815 (abstract). (To be published in Proc. Amer. Math. Soc. under the title: *Construction of some sets of mutually orthogonal Latin squares.*)
13. ——— *Orthogonal Latin squares*, Proc. Nat. Acad. Sci. U.S.A., *45* (1959), 859–862.
14. C. R. Rao, *Factorial experiments derivable from combinatorial arrangements of arrays*, J. Roy. Stat. Soc. Suppl., *9* (1947), 128–139.
15. F. Yates, *Incomplete randomised blocks*, Ann. Eugen. London, *7* (1936), 121–140.

University of North Carolina,
Case Institute of Technology
and
Remington Rand Univac, St. Paul, Minnesota