ON THE CONSTRUCTION OF PAIRWISE ORTHOGONAL SETS OF LATIN SQUARES AND THE FALSITY OF A CONJECTURE OF EULER. II

by

R. C. Bose and S. S. Shrikhande

University of North Carolina

This research was supported 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.

Institute of Statistics
Mimeograph Series No. 225
May 1959

ON THE CONSTRUCTION OF PAIRWISE ORTHOGONAL SETS OF LATIN SQUARES AND THE FALSITY OF A CONJECTURE OF EULER. II[1]

by

R. C. Bose and S. S. Shrikhande
University of North Carolina

1. Introduction. This report is a sequel to our earlier report under the same title [1], the notation and terminology of which will be adhered to. Since the earlier report was written Parker [3] has proved that if $4t+3$ is a prime power there exist at least two orthogonal Latin squares of order $6t+4$. The particular case $t=1$ leads to orthogonal squares of order 10 from which follows the existence of two orthogonal Latin squares of all orders which are multiples of 10. We shall here prove that the main theorem of [1] can be improved when certain canditions are satisfied. With the help of this we can in many cases improve lower bounds for $N(v)$ obtained in [1]. We can also demonstrate (using Parker's result) that there exist at least two orthogonal Latin squares of order v for $v > 6$ except for $v = 14$ and 26 which do not follow from our theorems.

---

1 This research was supported 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.

2. Improvement of the main theorem of [1].

Consider a pairwise balanced design (D) of index unity and type $(v; k_1, k_2, \ldots, k_m)$. The set of equiblock components (D_1), (D_2), $\ldots$, (D_ℓ), $\ell < m$, will be said to form a clear set if the $\sum_{i=1}^{\ell} b_i$ blocks comprising (D_1), (D_2), $\ldots$, (D_ℓ) are disjoint, i.e., no two blocks contain a common treatment. Clearly a necessary condition for this is

$$\sum_{i=1}^{\ell} b_i k_i \leq v \ .$$

We shall now prove:

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), $\ell < m$, form a clear set. If there exist $q_i - 1$ p.o.l.s. of order k_i and if

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

then there exist at least q^*-2 p.o.l.s. of order v.

Proof. Let us define

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

and

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

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 $(i \leq \ell)$. By hypothesis there exist $q_i - 1$ p.o.l.s. 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

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

Let Δ_i be the $q^{(1)} \times b_i k_i^2$ matrix obtained from A_i by retaining only the first q* rows, and let

$$\Delta^{(1)} = \left[\Delta_1, \Delta_2, \ldots, \Delta_\ell \right] .$$

Then $\Delta^{(1)}$ has q* rows and $\Sigma\, b_i k_i^2$ 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), ..., or (D_ℓ), then the ordered pair $\binom{t_c}{t_d}$ occurs as a column exactly once in any two rowed submatrix of $\Delta^{(1)}$.

Also let $P_u(D_u)$, $u = \ell+1, \ldots, m$ be defined as in [1] and let Δ_u be the matrix obtained from $P_u(D_u)$ by retaining only the first q* rows, then

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

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

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

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

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

treatments not contained in (D_1), (D_2), ..., 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 coordinatization we get q^*-2 p.o.l.s. of order v. Note that

$$v^2 = \sum_{i=1}^{\ell} b_i k_i^2 + \sum_{u=\ell+1}^{m} b_u k_u (k_u - 1) + v - \sum_{i=1}^{\ell} b_i k_i$$

from (3.1) of [1].

3. Applications to BIB designs.

By omitting a single treatment from the design BIB (v;k) we get a pairwise balanced design of index unity and type (v; 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 $2 \leq x \leq k$ we get a pairwise balanced design of index unity and type (v; k, k-1, k-x) where the equiblock component consisting of the single blocks of size k-x is clear. Hence we have

Theorem 2. Existence of a BIB (v;k) implies

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

and if $2 \leq x \leq k$, then

(ii) $N(v-x) \geq \min(N(k), N(k-1), 1 + N(k-x)) - 1.$

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 $N(267) \geq 10$, $N(265) \geq 8$, $N(264) \geq 7$ where as $n(267) = 2$, $n(265) = 4$ and $n(264) = 2$.

Suppose we omit 3 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; 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

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

Example (2). Consider the BIB (v;k) designs [2] with k = 5 and v = 21, 25, 41, 45, 61, 65, 85, 125. It follows that there exist at least two p.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 $N(78) \geq 6$, $N(70) \geq 6$.

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

Suppose there exists a resolvable BIB design with parameters v, b, r, k, $\lambda = 1$. Let $x \leq r$. To each block of the i-th replication add a new treatment θ_i, i = 1,2,...,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 r-th replication form a clear set. Hence we have

Theorem 4. The existence of a resolvable BIB (v;k) implies

(i) $N(v+x) \geq \min(N(k),\ N(k+1),\ 1 + N(x)) - 1$ if $x \leq r-2$,

(ii) $N(v+r-1) \geq \min(1 + N(k), N(k+1), 1 + N(r-1)) - 1,$

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

Corollary. As noted in [1] a resolvable solution of the design $v = 6t+3$, $b = (2t+1)(3t+1)$, $r = 3t+1$, $k = 3$, $\lambda = 1$ always exists. It follows from the second part of the theorem that $N(9t+3) \geq 2$ if $N(3t) \geq 2$, which is certainly true for all odd values of t.

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

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

Example (6). Taking $t = 3$ in the corollary we get $N(30) \geq 2$.

4. Use of group divisible designs.

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

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

This follows from the fact that in the pairwise balanced design of index unity and type (v; k, m) obtained from the GD design, the blocks of size m form a clear equiblock component.

Corollary. $N(s^2-1) \geq N(s-1)$, if s is a prime or 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

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

and if the design is resolvable then

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

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 size m and m-1 form a clear set. The second part has already been proved in [1] and is given here for completeness.

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

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

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

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

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

(c) $N(v+r+1) \geq \min(N(k+1), N(m+1), 1 + N(r+1)) - 1$,

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

To prove parts (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 i-th replication, i = 1,2,...,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 form a clear set. For the second part we note that the set of equiblock components given by the groups and the new block forms a clear set. To prove part (iii)(a) we add a new treatment θ_i to each block of the i-th replication, i = 1,2,...,r, and 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 i-th replication for the first r-1 replications, and a new treatment θ_o 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 r-th replication, and the newly added block forms a clear set. To prove (iii)(c) we add one new treatment to the blocks of each replication, one new treatment to each of the blocks corresponding to the groups, and one 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 [1] such a design is denoted by SRGD(km; k,m; 0,1). Also from the corollary to Lemma 7 of [1] there exists a resolvable SRGD(km; k,m; 0,1) if $k \leq N(m) + 1$. Combining this with theorem 7 we have

Theorem 8. If $k \leq N(m) + 1$, then

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

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

(iii) $N(km+m) \geq \min(N(k+1), 1 + N(m)) - 1$.

Example (7). Taking k, m and x as shown we derive the lower bound for N(km+x), noting that $N(24) \geq 3$ from Table 1 of [1] and $N(10) \geq 2$ from Parker's result.

(i) $k = 7, m = 11, x = 5;$ $N(82) \geq 4$,

(ii) $k = 8, m = 11, x = 7;$ $N(95) \geq 6$,

(iii) $k = 7, m = 19, x = 5;$ $N(138) \geq 4$,

(iv) $k = 7, m = 8, x = 4;$ $N(60) \geq 3$,

(v) $k = 4, m = 24, x = 10;$ $N(106) \geq 2$,

(vi) $k = 8, m = 13, x = 7;$ $N(111) \geq 6$,

(vii) $k = 4, m = 27, x = 10;$ $N(118) \geq 2$,

(viii) $k = 7, m = 16, x = 10;$ $N(122) \geq 2$,

(ix) $k = 7, m = 17, x = 5;$ $N(124) \geq 4$,

(x) $k = 7, m = 19, x = 5;$ $N(138) \geq 4$.

5. Improved lower bounds for $N(v)$, $v \leq 154$.

We give here those values of $v \leq 154$ for which the lower bound of $N(v)$ can be improved over the bound given in Table I of [1].

Table I

v	n(v)	l.b. for N(v)	Remarks
10	1	2	Parker
18	1	2	Ex. (2), Th. 3
30	1	2	Parker. Also Ex. (6), Th. 4
34	1	2	Parker
38	1	2	Ex. (2), Th. 3
42	1	2	Ex. (2), Th. 3
46	1	2	Parker
54	1	4	Ex. (5), Th. 4
60	2	3	Ex. (7)(iv), Th. 8
62	1	2	Ex. (2), Th. 3
70	1	6	Ex. (3), Th. 3
78	1	6	Ex. (3), Th. 3
82	1	4	Ex. (7)(i), Th. 8
90	1	2	Parker
95	4	6	Ex. (7)(ii), Th. 8
106	1	2	Parker. Also Ex.(7)(v), Th. 8
111	2	6	Ex. (7)(vi), Th. 8
114	1	2	114 = 38.3, Lemma 1 of [1]
118	1	2	Parker. Also Ex.(7)(vii), Th.8
122	1	2	Ex.(2), Th.3. Also Ex.(7)(viii),Th.8
124	3	4	Ex. (7)(ix), Th. 8
138	1	4	Ex. (7)(x), Th. 8
154	1	2	Parker. Also 154=22.7, Lemma 1 of [1]

6. The existence of at least two orthogonal Latin squares of order v for all $v > 26$.

Lemma 1. $N(v) \geq 2$ if $2 < v \leq 270$; $v \neq 6, 14, 26$.

Proof. This result has already been checked in Table I of [1] supplemented by the improvements noted in the last section, up to $v = 154$. Since the result is true for all odd v and all v divisible by 4, we need only check for values of v of the form $4t+2$.

We note that $162 = 9.18$, $170 = 10.17$, $174 = 3.58$, $186 = 3.62$, $190 = 10.19$, $198 = 9.22$, $210 = 10.21$, $222 = 3.74$, $230 = 10.23$, $234 = 13.18$, $238 = 7.34$, $242 = 11.22$, $246 = 3.82$, $250 = 10.25$, $258 = 3.86$, $266 = 7.38$, $270 = 10.27$. Since from Lemma 1 of [1], $N(v_1v_2) \geq \min(N(v_1), N(v_2))$ we have $N(v) \geq 2$ for all values of v the factors of which have been noted above.

We have thus only to check the cases $v = 158, 166, 178, 182, 194, 202, 206, 214, 218, 226, 254$ and 262. If v can be expressed in the form

$$v = km + x$$

where $k \leq N(m) + 1$ and $1 < x < m$, then we can apply part (ii) of Theorem 8. In particular if $k = 4$, $N(m) \geq 3$, $N(x) = 2$ and $1 < x \leq m$, then $N(v) \geq 2$. The proof of the Lemma is completed by noting that $158 = 4.37 + 10$, $166 = 4.37 + 18$, $178 = 4.40 + 18$, $182 = 4.40 + 22$, $194 = 4.44 + 18$, $202 = 4.45 + 22$, $206 = 4.49 + 10$, $214 = 4.49 + 18$, $218 = 4.49 + 22$, $226 = 4.49 + 30$, $254 + 4.61 + 10$, $262 = 4.60 + 22$.

Theorem 9. There exist at least two orthogonal Latin squares for all orders $v > 2$, $v \neq 6, 14, 26$.

The theorem has already been proved for all values of $v \leq 270$. We shall now prove the theorem by induction for all $v > 270$. For this we shall assume that the theorem is true for all $v^* < v$, where $v > 270$ and show that this implies $N(v) \geq 2$. Without loss of generality we can take $v \equiv 2 \pmod 4$, since the required result would be true otherwise. Let

$$v = 4n + 30, \qquad n > 60 \ .$$

Put

$$4n = 2^{\alpha} p_1^{c_1} p_2^{c_2} \ldots p_k^{c_k}$$

where $\alpha \geq 2$, $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, and in general p_i is the i-th odd prime in the ascending order of magnitude. Also p_k is the largest prime occurring in the prime power decomposition of n. Then $c_1, c_2, \ldots, c_k$ are integers positive or zero, and c_k is a non-zero positive integer. We shall consider 6 distinct mutually exclusive and collectively exhaustive cases:

Case I. $c_1 \neq 0$.

Then $v = 3(n_1+10)$, where $n_1 = 2^{\alpha} p_1^{c_1-1} p_2^{c_2} \ldots p_k^{c_k}$. Since $N(3) = 2$ and $N(n_1+10) \geq 2$ by assumption $N(v) \geq 2$.

Case II. $c_1 = 0$, $c_2 \neq 0$.

Then $v = 5(n_2+6)$, where $n_2 = 2^{\alpha} p_2^{c_2-1} \ldots p_k^{c_k}$. Since $N(5) = 4$, and $N(n_2+6) \geq 2$ by assumption $N(v) \geq 2$.

Case III. $c_1 = 0$, $c_2 = 0$, $\alpha = 2$.

Then $v = 4m_1+30$, $m_1 = p_3^{c_3} \ldots p_k^{c_k}$.

Now $\min(p_3^{c_3}, \ldots, p_k^{c_k}) \geq 7$. Hence $N(m_1) \geq n(m_1) \geq 6$. Also since $v > 270$, $m_1 > 60$. It follows from Theorem 8 that $N(v) \geq 2$.

Case IV. $c_1 = 0$, $c_2 = 0$, $\alpha = 3$, $c_3 = 0$.

Then $v = 8m_2+30$ where $m_3 = p_4^{c_4} \dots p_k^{c_k}$.

Now $\min(p_4^{c_4}, \dots, p_k^{c_k}) \geq 11$. Hence $N(m_1) \geq n(m_1) \geq 10$. Also $m_2 > 30$, since $v > 270$. Hence $N(v) \geq 2$ from Theorem 8.

Case V. $c_1 = 0$, $c_2 = 0$, $\alpha = 3$, $c_3 \geq 1$.

Then $v = 7m_3+30$ where $m_3 = 2^3 p_3^{c_3-1} \dots p_k^{c_k}$.

Now $\min(2^3, p_3^{c_3-1}, \dots, p_k^{c_k}) \geq 7$. Hence $N(m_3) \geq 6$, $m_3 > 30$. Hence $N(v) \geq 2$ from Theorem 8.

Case VI. $c_1 = 0$, $c_2 = 0$, $\alpha \geq 4$.

Then $v = 4m_4+30$ where $m_4 = 2^\beta p_3^{c_3} \dots p_k^{c_k}$, $\beta \geq 2$.

Now $\min(2^\beta, p_3^{c_3}, \dots, p_k^{c_k}) \geq 4$. Hence $N(m_4) \geq 3$, $m_4 > 60$. Hence $N(v) \geq 2$ from Theorem 8.

This completes the proof of the theorem.

N.B. We know that for $v = 2$ or 6 two orthogonal Latin squares of order v do not exist. The cases 14 and 26 are still undecided.

Bibliography

[1] Bose, R. C. and Shrikhande, S. S., "On the construction of pairwise orthogonal sets of Latin squares and the falsity of a conjecture of Euler," University of North Carolina, Institute of Statistics Mimeograph Series No. 222, 1959.

[2] Bose, R. C., "On the construction of balanced incomplete block designs," Ann. of Eugen. London, Vol. 9 (1939), pp. 353-399.

[3] Parker, E. T., "Orthogonal Latin squares," appearing in the June issue of Proceedings of National Academy of Science, U.S.A., Vol. 45 (1959).

Addendum

As this report was being readied for mimeographing we received from Parker a communication giving a construction for obtaining two orthogonal Latin squares of orders 14 and 26. Our Theorem 9 should now read:

There exist at least two orthogonal Latin squares for all order $v > 2$, $v \neq 6$.

The question raised inthe concluding remarks of [1] is 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.