SELF-ORTHOGONAL LATIN SQUARES

by

R. K. Brayton
Don Coppersmith
A. J. Hoffman*

RC 4532 (#20181)
September 19, 1973
Mathematics

* The work of this author was supported (in part) by the U. S. Army under contract #DAHC04-72-C-0023.

LIMITED DISTRIBUTION NOTICE

This report has been submitted for publication elsewhere and has been issued as a Research Report for early dissemination of its contents. As a courtesy to the intended publisher, it should not be widely distributed until after the date of outside publication.

Copies may be requested from:
IBM Thomas J. Watson Research Center
Post Office Box 218
Yorktown Heights, New York 10598

I. INTRODUCTION

E. Nemeth [15] has used the term "self-orthogonal" latin square to denote a latin square orthogonal to its transpose. The problem of constructing self-orthogonal latin squares is a natural question to consider, was first posed (we believe) by S. K. Stein in [20], and has been treated in [3], [7]-[11], [13]-[16], [18]-[21].

Without being aware of this literature, we were led to examine this question by John Melian [11], director of the Briarcliff Racquet Club, Briarcliff, N. Y., who asked if it were possible to design what might be termed a spouse-avoiding mixed doubles round robin for n couples (SAMDRR (n)) playing tennis. In such a round robin, there are n couples, and each match consists of a pair of players of opposite sex playing a pair of players of opposite sex, with the surnames of all four players different. (Such matches enhance sociability, avoid family tensions and ameliorate the baby-sitter problem). Every two players of the same sex oppose each other exactly once. Every two players of opposite sex (if they are not husband and wife) play together exactly once as partners and exactly once as opponents. Let $A = (a_{ij})$ be a matrix of order n, in which $a_{ii} = i$ and a_{ij} is the surname of the woman who plays with Mr. i in his match with Mr. j. Then it is easy to see that A is a latin square orthogonal to its transpose, and that, conversely, given such a latin square of order n (where we may assume without loss of generality that $a_{ii} = i$), we may construct by the above association a SAMDRR(n).

As we will see, the techniques of the celebrated disproof by Bose, Parker and Shrikhande of the Euler conjecture on orthogonal latin squares, combined with the methods of Hanani and Wilson in their remarkable work on block design construction, combined with earlier work on self-orthogonal latin squares can be adapted to solve the problem completely.

Theorem. There exists a self-orthogonal latin square of order n if and only if $n \neq 2, 3, 6$.

So far as we are aware, most previous results on this problem have disposed of various infinite classes of n, or some isolated values of n. An exception is [3], in which the first manuscript outlines a method, based on [18], for treating all sufficiently large n; and the second manuscript reports that calculations based on the method prove the existence of a self-orthogonal latin square of order n for all but 217 values of n. The remarkable work of Wilson [22] also readily implies that a self-orthogonal latin square of order n exists for all n sufficiently large.

2. NOTATIONS AND LEMMAS

We shall adhere to the notation of [5], and make frequent reference to it as well.

(2.1) Definition. A special orthogonal array is an OA(n, s) in which n columns consist of $(i, i, \ldots, i)$, $i = 1, \ldots, n$. We shall delete such columns in the special orthogonal array, so only $n^2 - n$ columns remain. A spouse-avoiding special orthogonal array of order n SOA(n) is a special orthogonal array OA(n, 4) in which, whenever (a, b, c, d) is a column of the array, then so is (c, d, a, b). Note that the interpretation (i, a_{ij}, j, a_{ji}) for the columns of a SOA(n) shows that the set of SOA(n) is isomorphic with the set of SAMDRR(n).

(2.2) Definition. $B = \{n \mid \text{there exists a SAMDRR}(n)\}$.

Lemma 2.3. If $n_1, n_2 \in B$, then $n_1 n_2 \in B$. (The usual proof of Mac Neish's theorem ([5], p. 191) applies to SOA's).

Lemma 2.4. If $m \in B$, then $3m+1 \in B$. (The proof in [5], pp. 195, 196 applies to SOA's).

Lemma 2.5. If n is a prime power, $n \neq 2, 3, n \in B$ ([13], [14]).

(2.5) Definition. A pseudo-geometry $\Pi(n)$ of order n is a collection of v points, together with some distinguished subsets, called lines, such that two distinct points are contained in exactly one line.

This concept goes back at least to Parker [17], and has been fundamental in subsequent work.

Lemma 2.7. [22] If the cordinality of each line of $\Pi(v)$ is in B, then $v \in B$.

Proof: Construct a SAMDRR(n) on the points of each line. Then the matches so arranged yield a SAMDRR(v). To find the other players in the match in which Mr. i opposes Mr. j, or Mrs. i opposes Mrs. j, or Mr. i opposes Mrs. j, or Mr. i partners Mrs. j, consult the SAMDRR on the unique line containing i and j.

Lemma 2.8. [22] If $n \in B$, OA(n, 5) exists, $0 \leq m \leq n$, $m \in B$, then $4n+m \in B$.

Proof: We first construct a $\Pi(5,n)$. Our points will be all ordered pairs of integers (r, s), where $1 \leq r \leq n$, $1 < s < 5$. We will have $5+n^2$ lines. Line $\ell_1, \ldots, \ell_5$ are defined by $\ell_s = \{(r, s) \mid r = 1, \ldots, n\}$, $s = 1, \ldots, 5$. The other n^2 lines $k_1, \ldots, k_{n^2}$ are determined by the columns of OA(n, 5) in the following way. If the j^{th} column of OA(n,5) is $(a_{1j}, \ldots, a_{5j})$, then k_j consists of the five points $(a_{1j}, 1), (a_{2j}, 2), \ldots, (a_{5j}, 5)$. Next delete n-m points from ℓ_1, yielding a line ℓ_1', and let $k_1', \ldots, k_{n^2}'$ be what is left of $k_1, \ldots, k_{n^2}$. The geometry $\Pi(4n+m)$ has each line cordinality m, n, 4 or 5. By lemmas 2.5 and 2.7, $4n+m \in B$.

Lemma 2.9. For all $k \geq 1$, $4k \in B$ and OA(4k, 5) exists.

Proof: By [5], p. 192, OA(4k, 5) exists except possibly if k is divisible by 3, but not by 9. We shall show OA(12, 5) and

OA(24, 5) exist, which implies OA(4k, 5) exists for all k. But OA(12, 5) exists [4], and OA(24, 5) exists by deleting a point from EG(25, 2) to define a $\Pi(24)$ and apply [5], p. 196, with the clear set consisting of the lines with 4 points.

By lemmas 2.3 and 2.5, $4k \in B$ for all k if $12 \in B$ and $24 \in B$. To prove $12 \in B$ a special construction is given in the next section. To prove $24 \in B$, we use $\Pi(24)$ described above.

3. SOME SPECIAL CONSTRUCTIONS

We exhibit in this section examples of self-orthogonal latin squares of orders 10, 12, 14, 15, 18. This example for case 10 is due to Hedayat [7], (an earlier example was constructed by Weisner [21]) and 14 and 18 were constructed by exploiting Hedayat's idea.

(3.10)

0	3	9	7	8	1	2	5	6	4
1	6	0	9	2	3	5	4	7	8
2	5	1	6	9	4	0	7	8	3
3	4	7	5	1	9	8	6	2	0
4	0	8	2	7	5	9	3	1	6
5	8	6	3	4	2	7	9	0	1
6	7	3	1	0	8	4	2	9	5
9	1	2	0	5	6	3	8	4	7
8	9	5	4	6	7	1	0	3	2
7	2	4	8	3	0	6	1	5	9

(3.12)

0	8	3	6	2	9	11	1	10	5	7	4
10	1	9	4	7	3	5	6	2	11	0	8
4	11	2	10	5	8	9	0	7	3	6	1
9	5	6	3	11	0	2	10	1	8	4	7
1	10	0	7	4	6	8	3	11	2	9	5
7	2	11	1	8	5	0	9	11	6	3	10
5	7	4	11	1	10	6	2	9	0	8	3
11	0	8	5	6	2	4	7	3	10	1	9
3	6	1	9	0	7	11	5	8	4	11	7
8	4	7	2	10	1	3	11	0	9	5	6
2	9	5	8	3	11	7	4	6	1	10	0
6	3	10	0	9	4	1	8	5	7	2	11

(3.14)

1	9	4	13	10	3	6	11	7	12	2	5	14	8
14	2	10	5	1	11	4	7	12	8	13	3	6	9
7	14	3	11	6	2	12	5	8	13	9	1	4	10
5	8	14	4	12	7	3	13	6	9	1	10	2	11
3	6	9	14	5	13	8	4	1	7	10	2	11	12
12	4	7	10	14	6	1	9	5	2	8	11	3	13
4	13	5	8	11	14	7	2	10	6	3	9	12	1
13	5	1	6	9	12	14	8	3	11	7	4	10	2
11	1	6	2	7	10	13	14	9	4	12	8	5	3
6	12	2	7	3	8	11	1	14	10	5	13	9	4
10	7	13	3	8	4	9	12	2	14	11	6	1	5
2	11	8	1	4	9	5	10	13	3	14	12	7	6
8	3	12	9	2	5	10	6	11	1	4	14	13	7
9	10	11	12	13	1	2	3	4	5	6	7	8	14

(3.15)

13	1	8	5	11	10	3	0	7	4	14	12	6	9	2
3	14	2	9	6	12	11	4	1	8	5	0	13	7	10
11	4	0	3	10	7	13	12	5	2	9	6	1	14	8
9	12	5	1	4	11	8	14	13	6	3	10	7	2	0
1	10	13	6	2	5	12	9	0	14	7	4	11	8	3
4	2	11	14	7	3	6	13	10	1	0	8	5	12	9
10	5	3	12	0	8	4	7	14	11	2	1	9	6	13
14	11	6	4	13	1	9	5	8	0	12	3	2	10	7
8	0	12	7	5	14	2	10	6	9	1	13	4	3	11
12	9	1	13	8	6	0	3	11	7	10	2	14	5	4
5	13	10	2	14	9	7	1	4	12	8	11	3	0	6
7	6	14	11	3	0	10	8	2	5	13	9	12	4	1
2	8	7	0	12	4	1	11	9	3	6	14	10	13	5
6	3	9	8	1	13	5	2	12	10	4	7	0	11	14
0	7	4	10	9	2	14	6	3	13	11	5	8	1	12

(3.18)

1	3	12	7	15	14	2	10	5	8	16	11	17	4	9	13	18	6
18	2	4	13	8	16	15	3	11	6	9	17	12	1	5	10	14	7
15	18	3	5	14	9	17	16	4	12	7	10	1	13	2	6	11	8
12	16	18	4	6	15	10	1	17	5	13	8	11	2	14	3	7	9
8	13	17	18	5	7	16	11	2	1	6	14	9	12	3	15	4	10
5	9	14	1	18	6	8	17	12	3	2	7	15	10	13	4	16	11
17	6	10	15	2	18	7	9	1	13	4	3	8	16	11	14	5	12
6	1	7	11	16	3	18	8	10	2	14	5	4	9	17	12	15	13
16	7	2	8	12	17	4	18	9	11	3	15	6	5	10	1	13	14
14	17	8	3	9	13	1	5	18	10	12	4	16	7	6	11	2	15
3	15	1	9	4	10	14	2	6	18	11	13	5	17	8	7	12	16
13	4	16	2	10	5	11	15	3	7	18	12	14	6	1	9	8	17
9	14	5	17	3	11	6	12	16	4	8	18	13	15	7	2	10	1
11	10	15	6	1	4	12	7	13	17	5	9	18	14	16	8	3	2
4	12	11	16	7	2	5	13	8	14	1	6	10	18	15	17	9	3
10	5	13	12	17	8	3	6	14	9	15	2	7	11	18	16	1	4
2	11	6	14	13	1	9	4	7	15	10	16	3	8	12	18	17	5
7	8	9	10	11	12	13	14	15	16	17	1	2	3	4	5	6	18

4. SOME MORE SPECIAL CONSTRUCTIONS

We use here the method of differences, as explained in [5], p. 201 for the cases 26, 30, 38, 42. Consider, for instance, (4.26) describing matrix P_o whose numbers are taken modulo 19, with indeterminate $x_1, \ldots, x_7$. Let P_1, P_2, P_3 be obtained from P_o by cyclic permutations of the rows, let $A_o = (P_o, P_1, P_2, P_3)$, A_i be obtained by adding i to each number in A_o modulo 19, E be the SOA on $x_1, \ldots, x_7$. Then $[A_o, A_1, \ldots, A_{18}, E]$ is the desired SOA(26).

(4.26)

0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
1	0	0	0	0	0	0	0
3	15	10	7	8	12	9	6
6	1	2	4	6	7	8	10

(4.30)

0	0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
1	10	0	0	0	0	0	0	0
3	7	9	5	7	11	22	19	8
6	2	22	21	19	17	14	10	12

(4.38)

0	0	0	0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
3	1	12	4	0	0	0	0	0	0	0
8	3	6	1	11	27	9	19	6	18	23
15	11	16	18	2	26	7	9	20	13	16

(4.42)

0	0	0	0	0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
3	2	1	14	17	0	0	0	0	0	0	0
8	10	5	3	4	6	13	19	21	27	16	7
17	3	15	26	33	2	28	9	11	22	15	18

5. PROOF OF THEOREM

The proof will rest on lemmas 2.8, 2.9, the constructions given in § 3 and § 4, and some other constructions based on lemma 2.7. We first remark that the impossibility of $n = 2, 6$ follows from the fact that there is no pair of orthogonal latin squares of order 2 or of order 6. The impossibility of 3(also 2) comes from the fact that each match in a SAMDRR(n) consists of four players with different names.

Now, let $n \neq 2, 3, 6$. Write $n = 16k+c$. If $c = 0$, we know already that $n \in B$, since $16k = 4(4k)$, $4k \in B$ by lemma 2.9, $4 \in B$ by lemma 2.5, and lemma 2.3 applies. If $c = 1$, then since $4k \in B$, $1 \in B$, it follows (lemma 2.8) that $n \in B$.

Suppose $c = 2$. If $k = 1$, $n \in B$ by (3.18). If $4k \geq 18$, $n \in B$, by (3.18) and lemma 2.8 (with $m = 18$). So we need only check cases $k = 2, 3, 4$, namely $n = 34, 50, 66$. The case $n = 34$ is covered by lemma 2.4, since $11 \in B$ by lemma 2.5. The case $n = 50$ is covered by adding one point at infinity to EG(2, 7), yielding a pseudo geometry $\Pi(50)$ in which every line has cordinality 7 or 8, with $7, 8 \in B$ by lemma 2.5. To do $n = 66$, consider all 66 points on 5 concurrent lines of PG(2, 13), together with the intersections of the lines of PG(2, 13) with these points. The resulting $\Pi(66)$ has every line cordinality 5 or 14. Since $5 \in B$, and $14 \in B$ by (3.14), it follows from lemma 2.7 that $66 \in B$.

Suppose $c = 3$. Then $19 \in B$ by lemma 2.5, and $n = 16k+3 \in B$ for

all k such that $4k \geq 19$, by reasoning similar to that in case $c = 2$. Therefore, we need only check that $35, 51, 67 \in B$. But $35 = 5 \times 7$, and 67 is prime, so $35, 67 \in B$. To prove $51 \in B$, take the points on 5 parallel lines in EG(2, 11) and delete 4 points from this set which are collinear (but the line they are on is not one of the 5 parallel lines). Call "lines" the intersection of lines of EG(2, 11) with this point set. The resulting $\Pi(51)$ has line cardinalities 11, 5, 4, so $51 \in B$.

Suppose $c = 4$. Then $n = 16k+4 \in B$ provided $4k \geq 4$, so we need only check that $20 \in B$, which is true since $20 = 5 \times 4$.

Suppose $c = 5$. Then $n = 16k+5 \in B$ if $4k \geq 5$, so we need only check that $21 \in B$. This has been shown elsewhere [10], [11], [17]. But it can also be shown by $\Pi(21) = PG(2, 4)$.

Suppose $c = 6$. Now $22 \in B$ by lemmas 2.5 and 2.4. So $n = 16k+6 \in B$ for $k \geq 1$ whenever $4k \geq 22$, so we need only check $n = 38, 54, 70, 86$. But $38 \in B$ by (4.38), $54 \in B$ by deleting one point from a set of 5 parallel lines in EG(2, 11), $70 \in B$ by deleting two points from one of eight parallel lines in EG(2, 9), $86 \in B$ by taking all points on 5 concurrent lines of PG(2, 17).

Suppose $c = 7$. Since $7 \in B$ and $n = 16k+7 \in B$ if $4k \geq 7$, so we need only check $n = 23 \in B$ by lemma 2.5.

Suppose $c = 8$. Since $8 \in B$ we need only verify $n = 24 \in B$, which was already done in proving lemma 2.9.

Suppose $c = 9$, we need only check $n = 9, 25, 41 \in B$, by lemma 2.5.

Suppose $c = 10$, we need only check $n = 10, 26, 42 \in B$, which we learn from (3.10), (4.26) and (4.42).

Suppose $c = 11$, we need only check $n = 11, 27, 43 \in B$, by lemma 2.5.

Suppose $c = 12$, we need only check 12, 28, $44 \in B$. But $12 \in B$ follows from (3.12), and $28, 44 \in B$ follow from lemmas 2.3 and 2.5.

Suppose $c = 13$, we need only check $13, 29, 45, 61 \in B$ which follow from lemmas 2.3 and 2.5.

Suppose $c = 14$, we need only check 14, 30, 46, 62. Now (3.14) yields $14 \in B$, (4.30) yields $30 \in B$. Take all points on 5 concurrent lines of PG(2,9) to yield $46 \in B$ with the help of lemma 2.7 and (3.10). Finally delete 3 points from one line of a set of 5 parallel lines of EG(2,13), to obtain $62 \in B$.

Finally, suppose $c = 1$. We need only check 15, 31, 47, 63. But $15 \in B$ by (3.15), and 31, 47, $63 \in B$ by lemmas 2.3 and 2.5.

We are very grateful for help received from A. J. W. Hilton, D. Knuth, N. S. Mendolsohn, R. C. Mullin and especially C. C. Lindner.

REFERENCES

[1] R. C. Bose, E. T. Parker and S. Shrikhande, "Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture," Can. J. Math., 12 (1960), 189-203.

[2] R. C. Bose, and S. Shrikhande, "On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler." Trans. Amer. Math. Soc., 95 (1960), 191-209.

[3] D. J. Crampin and A. J. W. Hilton, "The spectrum of latin squares orthogonal to their transposes," manuscript; "Remarks on Sade's disproof of the Euler conjecture with an application to latin squares orthogonal to their transpose", manuscript.

[4] A. L. Dulmage, D. M. Johnson, and N. S. Mendelsohn, "Orthomorphisms of groups and orthogonal Latin squares, I," Can. J. Math., 13 (1961), 356-372.

[5] M. Hall, Jr., "Combinatorial Theory", Blaisdell Publishing Co., Waltham, 1967.

[6] H. Hanani, "The existence and construction of balanced incomplete block designs," Ann. Math. Stat., 32(1961), 361-386.

[7] A. Hedayat, "An application of sum composition: a self orthogonal latin square of order ten," J. Combinatorial Theory, Series A 14 (1973), 256-260.

[8] J. D. Horton, "Variations on a theme by Moore," Proceedings of the Louisiana Conference on Graph Theory, Combinatorics and Computing, Louisiana State University, Baton Rouge, March 1-5, 1970.

[9] C. C. Lindner, "The generalized singular direct product for quasigroups," Canad. Math. Bull. 14 (1971), 61-63.

[10] C. C. Lindner, "Construction of quasigroups satisfying the identity $x(xy) = yx$," Canad. Math. Bull. 14 (1971), 57-59.

[11] C. C. Lindner, "Application of the singular direct product to constructing various types of orthogonal latin squares," Memphis State University Combinatorial Conference, 1972.

[12] John Melian, oral communications.

[13] N.S. Mendelsohn, "Combinatorial designs as models of universal algebras," Recent progress in combinatorics, Academic Press, Inc., New York, (1969).

[14] N.S. Mendelsohn, "Latin squares orthogonal to their transposes," J. Comb. Theory, Ser. A., 11 (1971), 187-189.

[15] R.C. Mullin and E. Nemeth, "A construction for self orthogonal latin squares from certain Room squares," Proceedings of the Louisiana Conference on Graph Theory, Combinatorics and computing, Louisiana State University, Baton Route, March 1-5, 1970, 213-225.

[16] E. Nemeth, "Study of Room Squares," Ph.D. Thesis, University of Waterloo.

[17] E. Parker, "Construction of some sets of mutually orthogonal Latin squares," Proc. Amer. Math. Soc., 10 (1959), 946-949.

[18] A. Sade, "Produit direct-singulier de quasigroupes orthogonaux et anti-abéliens," Ann. Soc. Sci. Bruxelles, Ser. 1, 74 (1960), 91-99.

[19] A. Sade, "Une nouvelle construction des quasigroupes orthogonaux à leur conjoint," Notices, American Mathematical Society, 19 (1972), 72T-A105.

[20] S.K. Stein, "On the foundations of quasigroups," Trans. Amer. Math. Soc. 85 (1957), 228-256.

[21] L. Weisner, "Special orthogonal latin squares of order 10", Can. Math. Bull. 6 (1963), 61-63.

[22] R.M. Wilson, "An existence theory for pairwise balanced designs", Part I & II, J. Comb. Theory, Ser. A. 13 (1972), 220-273.