



# Maximal sets of mutually orthogonal Latin squares

David A. Drake<sup>a,\*</sup>, G.H.J. van Rees<sup>b,1</sup>, W.D. Wallis<sup>c</sup>

<sup>a</sup>*Department of Mathematics, University of Florida, Gainesville, FL 36211, USA*

<sup>b</sup>*Department of Computer Science, University of Manitoba, Winnipeg, Canada R3T 2N2*

<sup>c</sup>*Department of Mathematics, Southern Illinois University, Carbondale, IL 62901-4408, USA*

Received 8 October 1996; revised 11 February 1998; accepted 23 February 1998

## Abstract

Maximal sets of  $s$  mutually orthogonal Latin squares of order  $v$  are constructed for infinitely many new pairs  $(s, v)$ . © 1999 Published by Elsevier Science B.V. All rights reserved

## 1. Introduction

A set  $S$  of mutually orthogonal Latin squares (MOLS) is maximal if no Latin square is orthogonal to each member of  $S$ . In Section 2, we introduce the notion of the ‘trial’ of a set of MOLS with subsquares and reprove Parker’s criterion [17] for the maximality of sets of MOLS. In Section 3, we use difference vectors to construct maximal sets of MOLS. In particular, we obtain (Corollary 3.3) the existence of maximal 3-sets of MOLS of order  $v = 8t + 1$  whenever  $6t + 1$  is a prime power and  $t \neq 3, 5$ . In Section 4, we apply constructions of Heinrich [12] to prove (Theorem 4.1) the existence of maximal 2-sets of MOLS of order  $v$  for all  $v > 1$  in each of five congruence classes modulo 18 (with one exception). As a consequence, maximal 2-sets are now known to exist for all values of  $v > 1$  in each of nine classes modulo 18 (with two exceptions). In Section 5, we use the existence of Singer cycles in Desarguesian projective planes to construct (Theorem 5.6) maximal sets of  $s$  MOLS of order  $v$  for infinitely many more new pairs  $(s, v)$ .

## 2. Trails, E.T. Parker’s criterion

Let  $\mathcal{S} = \{L_1, \dots, L_s\}$  be a set of MOLS of order  $v$ . For each  $t$ , represent  $L_t$  as

$$L_t = \begin{pmatrix} A_t & B_t \\ C_t & D_t \end{pmatrix}.$$

\* Corresponding author. E-mail: dad@math.ufl.edu.

<sup>1</sup> The second author’s research was supported by NSERC grant OGP0003558. The second author thanks William Kocay and William Martin for helpful discussions on Theorem 5.6.

Let  $1 \leq r < v$ . Suppose that  $A_t$  is a Latin square of order  $r$  for each  $t$ , and that  $\mathfrak{S}'$  is obtained from  $\mathfrak{S}$  by performing a common row permutation on the  $L_i$ 's and a common column permutation on the  $L_j$ 's. Then  $\mathfrak{S}'$  is said to be an  $s$ -set of  $(v, r)$ -MOLS.

Without loss of generality, we assume that the entries of each  $L_t$  of  $\mathfrak{S}$  belong to a common set of  $v$  elements and that the entries of each  $A_t$  belong to a common subset  $\Sigma$  of cardinality  $r$ . Elements of the set are called *little* if they are in  $\Sigma$ , *big* if they are not. A *cell* is a pair  $(i, j)$  with  $1 \leq i, j \leq v$ . One says that the  $(i, j)$ th entry of a matrix is *in* cell  $(i, j)$  and that the cell  $(i, j)$  is *in* or *from* row  $i$  and column  $j$ . We define the *trail* of  $\mathfrak{S}$  to be the set of all cells  $(i, j)$  with  $r < i, j$  such that the  $(i, j)$ th entry of  $L_t$  is big for each  $L_t$  in  $\mathfrak{S}$ .

**Theorem 2.1** (E.T. Parker, 1963, see [7, Theorem 12.3.3]). *Let  $\mathfrak{S}$  be an  $s$ -set of  $(sr + r + \varepsilon, r)$  MOLS. Then  $\varepsilon \geq 0$ , and the trail consists of  $\varepsilon(sr + \varepsilon)$  cells.*

**Theorem 2.2** (E.T. Parker, 1963, see [7, Theorem 12.3.4]). *Let  $\mathfrak{S}$  be an  $s$ -set of  $(sr + r + \varepsilon, r)$  MOLS. Then  $\mathfrak{S}$  is maximal if*

$$\lfloor r^2 / (sr + r + \varepsilon) \rfloor < (r - \varepsilon) / (s + 1). \quad (1)$$

In [14, 7], only the first of the two conclusions of Theorem 2.1 is stated. Therefore, we repeat the proof, which yields both conclusions. Consider  $i$  with  $r < i \leq sr + r + \varepsilon$ . The  $i$ th row of each  $L_t$  contains  $r$  little entries, none occurring in  $C_t$ . Since the  $L_t$  are mutually orthogonal, these  $r$  entries lie in different cells for different  $L_t$ . The trail contains all cells  $(i, j)$  with  $j > r$  except for the  $sr$  cells that contain a little entry in some  $L_t$ .

For our purposes, Theorem 2.2 is not easily applied. We have found it convenient to prove a lemma which is formulated in the language of ‘trails’. The reader will note that our arguments are similar in spirit to Parker’s proof of Theorem 2.2. Our treatment also permits a proof of Parker’s theorem. A *transversal*  $T$  of  $L_t$  is a set of  $v$  cells from distinct rows and distinct columns such that the entries of  $L_t$  in  $T$  are distinct. A common transversal to  $L_1, \dots, L_s$  is called a *transversal* of  $\mathfrak{S}$ .

**Lemma 2.3.** *Let  $\mathfrak{S}$  be an  $s$ -set of  $(sr + r + \varepsilon, r)$  MOLS. If  $T$  is a transversal to  $\mathfrak{S}$  which contains  $x$  cells of the subsquares, then  $T$  contains  $x(s + 1) - r + \varepsilon$  cells of the trail.*

**Proof.** Since  $T$  meets  $sx$  little entries in the  $A_t$ 's,  $T$  must meet  $sr - sx$  little entries in the  $D_t$ 's. Thus,  $T$  intersects  $D_1$  in  $sr - sx$  non-trail cells. Since  $T$  intersects  $A_1$  in  $x$  cells,  $T$  intersects  $B_1$  in  $r - x$  cells and  $D_1$  in  $(sr + \varepsilon) - (r - x) = sr - r + x + \varepsilon$  cells altogether.

**Proof of Theorem 2.2.** Suppose that  $\mathfrak{S}$  is an  $s$ -set of  $(sr + r + \varepsilon, r)$  MOLS which is not maximal. Then there exists a common orthogonal mate  $L$  which induces  $sr + r + \varepsilon$  disjoint transversals on  $\mathfrak{S}$ . One of these transversals  $T$  contains  $x$  cells of the  $A_t$ 's for

some  $x \leq [r^2/(sr + r + \varepsilon)]$ . By Lemma 2.3,  $T$  contains  $x(s + 1) - r + \varepsilon \geq 0$  trail cells. Thus, inequality (1) fails, and Theorem 2.2 is proved.  $\square$

**Corollary 2.4.** *Let  $\mathfrak{S}$  be an  $s$ -set of  $(sr + r + \varepsilon, r)$  MOLS with  $\varepsilon \geq 0$ . If the residue  $\delta$  of  $\varepsilon - r$  modulo  $s + 1$  satisfies  $0 \neq \delta \geq \varepsilon$ , then  $\mathfrak{S}$  is maximal.*

**Proof.** Assume, by way of contradiction, the existence of a Latin square  $L$  which is orthogonal to each square of  $\mathfrak{S}$ . By Lemma 2.3, each of the  $sr + r + \varepsilon$  transversals to  $\mathfrak{S}$  induced by  $L$  meets the trail of  $\mathfrak{S}$  in at least  $\delta$  cells. Thus, Theorem 2.1 yields the contradiction  $\varepsilon(sr + \varepsilon) \geq (sr + r + \varepsilon) \max\{\varepsilon, 1\}$ .

**Corollary 2.5.** *Let  $\mathfrak{S}$  be an  $s$ -set of  $(sr + r + 1, r)$  MOLS. If  $r \not\equiv 1$  modulo  $s + 1$ , then  $\mathfrak{S}$  is maximal.*

### 3. Difference vectors

To utilize an R.M. Wilson construction, Mullin et al. [16, p. 260] introduced the notation  $V(s, r)$  for a vector  $(b_0, b_1, \dots, b_s)$  over the field  $F = \text{GF}(sr + 1)$  which satisfies the following condition: for each  $k$ , the  $s$  differences  $b_{i+k} - b_i$  with  $i + k \neq 0$  (addition of subscripts modulo  $s + 1$ ) represent all  $s$  cyclotomic classes of index  $s$  in  $F^*$ . The existence of such a difference vector is equivalent (see, e.g., [5, p. 271] or [6, p. 4]) to the existence of a set of  $s$  idempotent MOLS of order  $sr + r + 1$  with one ‘hole’ (see, e.g., [2, p. 143]) or order  $r$ . The following result is an immediate consequence of this equivalence.

**Lemma 3.1** ([16, Lemma 2.9]). *If there are a  $V(s, r)$  and a set of  $s$  MOLS of order  $r$ , then there is an  $s$ -set of  $(sr + r + 1, r)$  MOLS.*

**Theorem 3.2** (van Rees [19] and Ge [10]). *A  $V(3, k)$  exists whenever  $3k + 1$  is a prime power.*

**Corollary 3.3.** *There is a maximal 3-set of MOLS of order  $8t + 1$  for every positive integer  $t \neq 3, 5$  such that  $6t + 1$  is a prime power.*

**Proof.** Suppose that  $6t + 1$  is a prime power and that  $t \neq 1, 3, 5$ . By Theorem 3.2, there is a  $V(3, 2t)$ . The existence of a set of 3 MOLS of order  $2t$  is well known for  $t \neq 1, 3, 5$  (see, e.g., [11]). Thus, Lemma 3.1 yields the existence of a 3-set of  $(8t + 1, 2t)$  MOLS. By Corollary 2.5, this 3-set is maximal. The existence of a maximal 3-set of MOLS of order 9 (the case with  $t = 1$ ) is known (see [9, p. 387]).

**Theorem 3.4** (Colbourn [6, Theorem 3.1]). *Let  $s$  and  $r$  be positive integers with  $s \leq r + 1$ ,  $rs < 5000$ . Then a vector  $V(s, r)$  exists if either of the following sets of*

conditions holds:

- (i)  $s \leq 6$ ,  $rs + 1$  is a prime power,  $(s, r) \neq (3, 5)$ ;
- (ii)  $7 \leq s \leq 10$ ,  $rs + 1$  is a prime,  $(s, r) \neq (9, 8)$ .

**Corollary 3.5.** *Let  $s$  and  $r$  be positive integers with  $s \leq r + 1$  and  $rs < 5000$  such that  $r \not\equiv 1 \pmod{s + 1}$  and such that there exists a set of  $s$  MOLS of order  $r$ . Then there is a maximal  $s$ -set of MOLS of order  $sr + r + 1$  provided that either of the following sets of conditions holds:*

- (i)  $s \leq 6$ ,  $rs + 1$  is a prime power,  $(s, r) \neq (3, 5)$ ;
- (ii)  $7 \leq s \leq 10$ ,  $rs + 1$  is a prime,  $(s, r) \neq (9, 8)$ .

**Proof.** Apply Theorem 3.4, Lemma 3.1 and Corollary 2.5.  $\square$

We remark that for  $s = 2$  and  $3$ , respectively, the conclusions of Corollary 3.5 are subsumed by Theorem 4.1 (below) and Corollary 3.3 (above). For later reference, we apply Corollary 3.5 to some pairs with  $s > 3$ ; namely, to  $(s, r) = (4, 7), (4, 9), (4, 12), (5, 8)$  and  $(6, 7)$ . Using known results on the existence of sets of MOLS (see, e.g., [1]), we obtain the following conclusions:

**Fact 3.6.** *There is a maximal  $s$ -set of MOLS of order  $v$  for each of the pairs  $(s, v) = (4, 36), (4, 46), (4, 61), (5, 49), (6, 50)$ .*

#### 4. Pairs of orthogonal Latin squares without common orthogonal mates

There is a Latin square of order  $v$  without an orthogonal mate for every integer  $v \geq 2$  that satisfies  $v \not\equiv 3 \pmod{4}$ . This result was established for  $v \equiv 2 \pmod{4}$  in 1942 by Mann, for  $v \equiv 0 \pmod{4}$  in 1955 by M. Hall and L.J. Paige and  $v \equiv 1 \pmod{4}$  in 1985 by Beth et al. (see [3, X.8.6], [13, 3.3.4] or [15, p. 4]). In 1977, one of the current authors (see [8, 1.3(c)] or [3, 8.11(b)]) observed that a 1951 theorem of R.H. Bruck yields the existence of a maximal 2-set of MOLS of order  $v$  for all  $v \equiv 3$  or  $6 \pmod{9}$  except for  $v = 6$ . In this section we prove

**Theorem 4.1.** *There is a maximal 2-set of MOLS of order  $v$  for every positive integers  $v \neq 1, 19$  that satisfies one of the congruences  $v \equiv 1$  or  $7 \pmod{9}$ ,  $v \equiv 11 \pmod{18}$ .*

Theorem 4.1 and previously obtained results give the existence of maximal 2-sets of MOLS of order  $v$  for values of  $v$  filling four and one half-congruence classes modulo 9. The application of Theorem 5.6 below with  $n = 2$  yields the existence of a maximal 2-set of MOLS of order  $v$  for infinitely many values of  $v$  from each of two more parallel classes modulo 9, namely, 0 and 4.

A *self-orthogonal Latin square*, briefly an SOLS, is a Latin square that is orthogonal to its transpose. A  $(v, r)$ -SOLS is an SOLS of order  $v$  with a sub-square of order

$r$ . Clearly, the existence of a  $(v, r)$ -SOLS yields the existence of a 2-set of  $(v, r)$ -MOLS.

**Theorem 4.2** (Heinrich [12]). (i) *There is a  $(3r + 1, r)$ -SOLS if  $6 \neq r \geq 4$ .*

(ii) *There is a  $(3r + 2, r)$ -SOLS if  $r$  is an odd integer with  $r \geq 5$ .*

**Lemma 4.3.** (i) *There is a maximal 2-set of MOLS of order  $3r + 1$  for  $r = 5$  and for every  $r \geq 8$  which is not congruent to 1 modulo 3.*

(ii) *There is a maximal 2-set of MOLS of order  $3r + 2$  if  $r \equiv 3 \pmod{6}$  and  $r \geq 9$ .*

**Proof.** Apply Theorem 4.2 and Corollary 2.4.  $\square$

**Proof of Theorem 4.1.** Lemma 4.3(i) gives the asserted result for  $v \equiv 1$  or  $7 \pmod{9}$  except for the values  $v = 7$  and  $v = 10$ . Lemma 4.3(ii) gives the asserted result for  $v \equiv 11 \pmod{18}$  except for the value  $v = 11$ . The existence of maximal 2-sets of MOLS of orders  $v = 7, 10$  and  $11$ , however, are known (see, e.g., [9, 13 or 15]).  $\square$

## 5. Construction of maximal sets of MOLS via Singer cycles

**Lemma 5.1.** *Let  $\mathfrak{S}$  be an  $(n - 1)$ -set of  $((n^{d+1} - 1)/(n - 1), (n^d - 1)/(n - 1))$  MOLS for integers  $n \geq 2, d \geq 1$ . If  $T$  is a transversal which intersects the subsquares in  $x$  cells, then  $T$  intersects the trail in  $xn + 1 - (n^d - 1)/(n - 1)$  cells.*

**Proof.** Apply Lemma 2.3 to  $\mathfrak{S}$  with  $\varepsilon = 1, s = n - 1$  and  $r = (n^d - 1)/(n - 1)$ .  $\square$

**Lemma 5.2.** *Let  $\mathfrak{S}$  be an  $(n - 1)$ -set of  $((n^{d+1} - 1)/(n - 1), (n^d - 1)/(n - 1))$  MOLS for integers  $n \geq 2, d \geq 1$ . Suppose that there is a cyclic Latin square  $L$  which is orthogonal to every member of  $\mathfrak{S}$ , and suppose that an entry 0 of  $L$  occurs in some cell of each row of the subsquares. Then  $\mathfrak{S} \cup \{L\}$  is a maximal set of MOLS.*

**Proof.** Take  $\varepsilon = 1, s = n - 1$  and  $r = (n^d - 1)/(n - 1)$ . By Theorem 2.1, the trail of  $\mathfrak{S}$  consists of  $n^d$  cells. In  $L$ , the entry 0 occupies  $n^d$  cells outside the subsquares, all of which occur in the trail of  $\mathfrak{S}$ . Assume, by way of contradiction, the existence of a Latin square  $M$  which is orthogonal to every member of  $\mathfrak{S} \cup \{L\}$ . Since  $M$  is orthogonal to  $L$ , each of the entries in  $M$  occupies at most one cell in the trail; so some entries in  $M$  occupy exactly one trail cell. By Lemma 5.1, such an entry occupies  $x$  cells of the subsquares where  $x$  satisfies  $xn + 1 - (n^d - 1)/(n - 1) = 1$ . As  $x$  is not an integer, we have produced a contradiction which establishes the maximality of  $\mathfrak{S} \cup \{L\}$ .  $\square$

A *pairwise balanced design* (a PBD) is an incidence structure  $\Pi$  with precisely one line through any two points. A *subspace* of  $\Pi$  is a point set which contains all the points of every line through any two of its points.

**Theorem 5.3** (Bose/Shrikhande). *Let  $G_1, \dots, G_b$  be the lines of a PBD  $\Pi$  defined on points  $P_0, \dots, P_{v-1}$ . For each line  $G_k = \{P_{k_0}, \dots, P_{k_n}\}$ ,  $n$  determined by  $k$ , let  $\{L_1^k, \dots, L_s^k\}$  be a set of MOLS of order  $n + 1$ , each with successive main diagonal entries  $k_0, \dots, k_n$ . For  $1 \leq i \leq s$ , form a  $(v \times v)$ -matrix  $B_i$  as follows: for  $1 \leq k \leq b$ , insert the matrix  $L_i^k$  into the submatrix of  $B_i$  whose rows and columns are numbered  $k_0, \dots, k_n$ . Then each  $B_i$  is well defined, and  $\{B_1, \dots, B_s\}$  is a set of MOLS. If  $\Sigma$  is a subspace of  $\Pi$ , then the rows and columns corresponding to points of  $\Sigma$  are the rows and columns of a subsquare in each  $B_i$ .*

Aside from the final comment on subsquares, the preceding theorem is contained in the proof of a well-known result of Bose and Shrikhande. The reader may either construct his own proof or look it up in any one of a number of standard references such as, for example [7, Proof of Theorem 11.2.2] or [11, p. 196].

**Lemma 5.4.** *If  $q$  is a prime power, there exists a set of  $q - 1$  MOLS of order  $q$ . If  $q$  is a prime, one of the squares in the set may be taken to be cyclic.*

For a proof of Lemma 5.4, see the proof of Theorem 5.2.2 in [7]. A cyclic square is produced by the cited construction for the point at infinity which corresponds to the affine lines of slope 1.

**Lemma 5.5.** (i) *The projective geometry  $\Pi := PG(d, n)$  has a Singer cycle; i.e., a generator of an automorphism group of  $\Pi$  which acts regularly on the  $v := (n^{d+1} - 1)/(n - 1)$  points of  $\Pi$ .*

(ii) *If  $d$  is even, every line orbit of every Singer cycle  $\sigma$  of  $\Pi$  is of size  $v$ .*

(iii) *If  $n + 1$  is a prime, every line orbit of every Singer cycle  $\sigma$  of  $\Pi$  is of size  $v$  or  $v/(n + 1)$ .*

**Proof.** See, for example [3, p. 167, 168] for a proof of (i). To prove (ii) and (iii), suppose that the  $\sigma$ -orbit of a line  $G$  has size  $\ell$ . Then  $\ell|v$ ; and  $G$  is the disjoint union of point orbits of  $\sigma^\ell$ , each of size  $v/\ell$ . Thus  $(v/\ell)|(n + 1)$ . Conclusion (iii) follows immediately. If  $d$  is even, the greatest common divisor  $(n + 1, v) = (n + 1, n^d) = 1$ . Hence, the condition  $(v/\ell)|(n + 1)$  implies that  $\ell = v$ ; so conclusion (ii) holds.  $\square$

**Theorem 5.6.** *Let  $n$  and  $n + 1$  be prime powers,  $d$  be a positive integer. Suppose, either that  $d$  is even or that  $n + 1$  is prime. Then there exists a maximal set of  $n$  MOLS of order  $(n^{d+1} - 1)/(n - 1)$ .*

**Proof.** If  $n + 1$  is a prime, Lemma 5.4 gives a set  $\mathfrak{S} = \{L_1, \dots, L_n\}$  of  $n$  MOLS of order  $n + 1$  such that  $L_1$  is cyclic. In this case, we may and do assume that the entries on the main diagonal of each  $L_i$  with  $i \geq 2$  are, successively from the upper left entry:  $0, 1, \dots, n$ . If  $n + 1$  is a non-prime prime power, we take  $\{L_2, \dots, L_n\}$  to be a set of  $n - 1$  MOLS of order  $n + 1$ , each with successive diagonal entries  $0, 1, \dots, n$  (see [7,

Theorem 5.3.4]). Let  $\sigma$  denote a Singer cycle of  $\Pi := \text{PG}(d, n)$ . We denote the points of  $\Pi$  by the congruence classes of integers modulo  $v := (n^{d+1} - 1)/(n - 1)$  and identify a congruence class  $[j]$  with any of its members  $j$ . Without loss of generality, we name the points so that  $(j)\sigma^i = j + i$  for all  $i$  and  $j$ .  $\square$

Let  $G_1, \dots, G_t$  be a set of lines of  $\Pi$  incident with the point 0, one from each  $\sigma$ -orbit of lines. We form a set of  $v \times v$  matrices  $B_i$ ,  $2 \leq i \leq n$ , as follows. For  $1 \leq k \leq t$ , let  $k_0, k_1, \dots, k_n$  be the points of  $G_k$  where  $0 = k_0 < k_1 < \dots < k_n < v$ . From  $L_2, \dots, L_n$ , form a set  $\mathfrak{E}_k$  of MOLS  $L_2^k, \dots, L_n^k$  by replacing entries of the  $L_i$  according to the map  $y \rightarrow k_y$ . For  $2 \leq i \leq n$ , insert  $L_i^k$  into the  $(n + 1) \times (n + 1)$  submatrix of  $B_i$  whose rows and columns are numbered  $k_0, k_1, \dots, k_n$ . For  $1 \leq x$ ,  $x$  less than the size of the  $\sigma$ -orbit of  $G_k$ , insert into each  $B_i$  in the submatrix positions determined by  $(G_k)\sigma^x$ , the Latin square  $L_i^k + xJ$  where  $J$  denotes an all-ones matrix and addition is taken modulo  $v$ . By the Bose/Shrikhande construction of Theorem 5.3, the resulting matrices  $B_2, \dots, B_n$  are a set of MOLS.

Let  $B_1$  denote the  $v \times v$  cyclic square whose  $d$ th diagonal entries are all  $d$ 's for each  $d$  with  $0 \leq d < v$ . By Theorem 5.3, any hyperplane of  $\Pi$  induces mutually orthogonal subsquares of  $B_2, \dots, B_n$ . These subsquares are of order  $w := (n^d - 1)/(n - 1)$ , and they contain  $w$  cells from the main diagonal. Thus, if  $B_1$  is orthogonal to each  $B_i$  with  $i \geq 2$ , Lemma 5.2 asserts that  $B_1, \dots, B_n$  is a maximal set of MOLS.

We now prove that indeed  $B_1$  is orthogonal to each  $B_i$  with  $i \geq 2$ . Let  $e$  satisfy  $1 \leq e < v$ . Take  $H_e$  to be the line joining the points 0 and  $e$ , and let  $\ell$  denote the size of the  $\sigma$ -orbit of  $H_e$ . Then  $H_e = (G_k)\sigma^i$  for some  $i$  and  $k$  with  $1 \leq k \leq t$ . By Lemma 5.5,  $\ell$  is either  $v$  or  $v/(n + 1)$ . In the former case, the  $v$  cells of the  $e$ -th diagonal correspond to pairs of points  $(x, x + e)$  which are joined by distinct lines of the  $\sigma$ -orbit of  $G_k$ . Thus, each entry of the  $e$ -th diagonal of each  $B_i$  with  $i \geq 2$  is obtained by adding 1 modulo  $v$  to the preceding entry, and so the  $e$ -th diagonal is transversal to each  $B_i$  with  $i \geq 2$ .

Let us treat the latter case; i.e., the case with  $(n + 1)\ell = v$  and, hence, with  $n + 1$  a prime. In this case, the points of  $H_e$  constitute a single point orbit under  $\sigma^\ell$ . Since  $0, e \in H_e$  and  $0 \in G_k$ , so  $H_e$  is the coset  $\langle \ell \rangle + e = \langle \ell \rangle = G_k$  in the group of integers modulo  $v$ . Since  $L_1$  is cyclic, the entries on each diagonal of each  $L_i$  and each  $L_i^k$  with  $i \geq 2$  are distinct. In each  $L_i^k$ , these entries are the elements of  $\langle \ell \rangle$ . The placement of  $L_i^k$  into  $B_i$  will position the entries of a diagonal at intervals of distance  $\ell$  along a diagonal of  $B_i$ . Thus, the  $e$ -th diagonal of each  $B_i$  with  $i \geq 2$  is again a transversal.

Therefore,  $B_1$  is orthogonal to each  $B_i$  with  $i \geq 2$  and Lemma 5.2 yields the maximality of the set of MOLS  $\{B_1, \dots, B_n\}$ .

## 6. Concluding remarks

Theorem 5.6 may be applied with even  $d$  to any Mersenne prime  $n$  and with arbitrary  $d$  whenever  $n + 1$  is a Fermat prime. David Slowinski and Paul Gage [20,21] have

recently found the 32nd and 33rd known Mersenne primes. The extensive lists of Brillhart et al. [4] contain many of the known Mersenne and Fermat primes.

Evans' table [9] gives the state of knowledge regarding the existence of a maximal  $s$ -set of MOLS of order  $v$  for  $v \leq 61$ . For  $2 = s < v$ , the table indicates that existence is in doubt for 34 values of  $v$ . Our results give existence in 13 of these cases with  $s = 2$ : Theorem 5.6 gives existence for  $v = 31$ , and Theorem 4.1 gives existence for  $v = 16, 25, 28, 29, 34, 37, 43, 46, 47, 52, 55$  and 61.

Our results also yield eleven new pairs  $(s, v)$  with  $s > 2$  which can be added to the Evans table. Five of these are listed in Fact 3.6. The four pairs  $(s, v) = (3, 17), (3, 33), (3, 49)$  and  $(3, 57)$  are given by Corollary 3.3. The two pairs  $(s, v) = (3, 13)$  and  $(7, 57)$  are obtained by applying Theorem 5.6 with  $(n, d) = (3, 2)$  and  $(7, 2)$ .

## References

- [1] R.J.R. Abel, A.E. Brouwer, C.J. Colbourn, J.H. Dinitz, Mutually orthogonal Latin squares, in: C.J. Colbourn, J.H. Dinitz (Eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996, pp. 111–142.
- [2] R.J.R. Abel, C.J. Colbourn, J.H. Dinitz, Incomplete MOLS, in: C.J. Colbourn, J.H. Dinitz (Eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996, pp. 142–172.
- [3] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Bibliographisches Institut, Zürich, 1985.
- [4] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, S.S. Wagstaff, *Factorizations of  $b^n \pm 1$* , Contemporary Math. Series, vol. 22, Amer. Math. Soc., Providence, 1983 (1987).
- [5] A.E. Brouwer, G.H.J. van Rees, More mutually orthogonal Latin squares, *Discrete Math.* 39 (1982) 263–281.
- [6] C.J. Colbourn, Some direct constructions for incomplete transversal designs, *J. Statist. Plann. Inf.* 56 (1996) 93–104.
- [7] J. Dénes, A.D. Keedwell, *Latin Squares and Their Applications*, English Universities Press, London, 1974.
- [8] D.A. Drake, Maximal sets of Latin squares and partial transversals, *J. Statist. Plann. Inf.* 1 (1977) 143–149.
- [9] A.B. Evans, Maximal sets of MOLS, in: C.J. Colbourn, J.H. Dinitz (Eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996, pp. 386–388.
- [10] G. Ge, All  $V(3, t)$ 's exist for  $3t + 1$  a prime power, to appear.
- [11] M. Hall Jr., *Combinatorial Theory*, Blaisdell, Waltham, 1967.
- [12] K. Heinrich, Self-orthogonal subsquares, *Ars Combin.* 3 (1977) 251–266.
- [13] D. Jungnickel, Latin squares, their geometries and their groups. A survey, in: Dijen Ray-Chaudhuri (Ed.), *Coding Theory and Design Theory, Part II Design Theory*, vol. 21 of the IMA Volumes in Mathematics and its Applications, Springer, Berlin, 1990, pp. 166–225.
- [14] D. Jungnickel, Maximal sets of mutually orthogonal Latin squares, in: S. Cohen, H. Niederraiter (Eds.), *Proc. 3rd Intern. Conf. at Univ. Glasgow, 1995*, London Math. Soc. Lecture Note Series, 233, Cambridge Univ. Press, Cambridge, 1996, pp. 129–153.
- [15] H.B. Mann, On orthogonal Latin squares, *Bull. Amer. Math. Soc.* 50 (1944) 249–257.
- [16] R.C. Mullin, P.J. Schellenberg, D.R. Stinson, S.A. Vanstone, Some results on the existence of squares, *Ann. Discrete Math.* 6 (1980) 257–274.
- [17] E.T. Parker, Nonextendibility conditions on mutually orthogonal latin squares, *Proc. Amer. Math. Soc.* 13 (1962) 219–221.
- [18] J.H. van Lint, R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.
- [19] G.H.J. van Rees, All  $V(3, t)$ 's exist for  $3t + 1$  a prime, *J. Combin. Des.* 3 (1995) 399–403.
- [20] Unsigned, The latest Mersenne prime, *Amer. Math. Monthly* 99 (1992) 360.
- [21] Unsigned,  $2^{858433} - 1$  is prime, *Amer. Math. Monthly* 101 (1994) 338.