On the Maximum Number of Different Ordered Pairs of Symbols in Sets of Latin Squares

Jeffrey H. Dinitz
Department of Mathematics and Statistics
University of Vermont
Burlington, Vermont 05405, U.S.A.

Douglas R. Stinson
School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada

September 26, 2003

Abstract

In this paper we study the problem of constructing sets of s latin squares of order m such that the average number of different ordered pairs obtained by superimposing two of the s squares in the set is as large as possible. We solve this problem (for all s) when m is a prime power, and we present upper and lower bounds for all m.

1 Introduction

Suppose that L_1 and L_2 are latin squares of order m. Define $P(L_1, L_2)$ to be the number of different ordered pairs that are obtained when L_1 and L_2 are superimposed. If the rows and columns of L_1 and L_2 are indexed by the m-set X, then let

$$P(L_1, L_2) = |\{(L_1(x,y), L_2(x,y)) : x, y \in X\}|.$$

The set of possible values of $P(L_1, L_2)$, given that L_1 and L_2 are latin squares of order m, is studied in [1] and solved almost completely in [4].

Now suppose that $L_1, \dots, L_s$ are latin squares of order m, where $s > 2$, define

$$P(L_1, \dots, L_s) = \sum_{1 \le i < j \le s} P(L_i, L_j).$$

It is clear that

$$m \le P(L_1, L_2) \le m^2,$$

and hence

$$\binom{s}{2} m \le P(L_1, \dots, L_s) \le \binom{s}{2} m^2.$$

In this paper, we are interested in determining the maximum value of $P(L_1, \dots, L_s)$ over all possible sets of s latin squares of order m. We will denote this maximum by $\mathsf{P}(s, m)$.

Keedwell and Mullen [5] have provided some algebraic constructions using neofields that yield lower bounds on $\mathsf{P}(s,m)$. They concentrate on the cases where $s \leq m-1$ in general and on the case $s = m-1$ in particular. We will give some combinatorial constructions which lead to some improved lower bounds on $\mathsf{P}(s,m)$. In addition, we prove an upper bound on $\mathsf{P}(s,m)$. When m is a prime power, the upper and lower bounds that we prove coincide for all s, so we have determined the optimal solution in these cases. We formulate a conjecture about the structure of the optimal solutions and we derive some partial results relating to this conjecture. Finally, we conclude with some numerical results for small orders.

2 Constructions

A set of s latin squares of order m, say $L_1, \ldots, L_s$, are called *R-orthogonal* if $P(L_i, L_j) = R$ for all i, j with $1 \leq i < j \leq s$. Hence a set of two or more m^2-orthogonal latin squares of order m are in fact a set of mutually orthogonal latin squares (or *MOLS*) of order m. The following result is obvious.

Theorem 2.1 *Let $L_1, \ldots, L_s$ be latin squares of order m. Then $P(L_1, \ldots, L_s) \leq \binom{s}{2} m^2$, and equality occurs if and only if $L_1, \ldots, L_s$ are mutually orthogonal.*

Corollary 2.2 $\mathsf{P}(s,m) \leq \binom{s}{2} m^2$, *with equality if and only if there exist s MOLS of order m.*

The next theorem gives a bound on $\mathsf{P}(s,m)$ when a set of t R-orthogonal latin squares of order m is known to exist.

Theorem 2.3 *Suppose there exist t R-orthogonal latin squares of order m, and suppose that $s = qt + r$, where $q \geq 0$ and $0 \leq r \leq t-1$. Then*

$$\mathsf{P}(s,m) \geq R\binom{s}{2} - (R-m)\left(r\binom{q+1}{2} + (t-r)\binom{q}{2}\right).$$

Proof. Let $L_0, \ldots, L_{t-1}$ be t R-orthogonal latin squares of order m. For $t \leq i \leq s-1$, define $L_i = L_{i \bmod t}$. Thus the collection $L_0, \ldots, L_{s-1}$ consists of $q+1$ copies of each of $L_0, \ldots, L_{r-1}$, and q copies of each of $L_r, \ldots, L_{t-1}$. It is obvious that

$$P(L_i, L_j) = \begin{cases} R & \text{if } i \not\equiv j \pmod{t} \\ m & \text{if } i \equiv j \pmod{t}. \end{cases}$$

A simple calculation yields the result that

$$P(L_0, \ldots, L_{s-1}) = R\binom{s}{2} - (R-m)\left(r\binom{q+1}{2} + (t-r)\binom{q}{2}\right).$$

□

Corollary 2.4 *Suppose there exist t MOLS of order m, and suppose that $s = qt + r$, where $q \geq 0$ and $0 \leq r \leq t-1$. Then*

$$\mathsf{P}(s,m) \geq m^2\binom{s}{2} - (m^2-m)\left(r\binom{q+1}{2} + (t-r)\binom{q}{2}\right).$$

Proof. Apply Theorem 2.1 with $s = 2$ and Theorem 2.3 with $R = m^2$. □

Informally, an (m,u)-*incomplete latin square* (or (m,u)-*ILS*) is a latin square of order m missing a sub-latin square of order u. More formally, suppose that X is an m-set, $Y \subseteq X$ and $|Y| = u$. Let L be an $m \times m$ square of order m on symbol set X whose rows and columns are indexed by X. L is an (m,u)-ILS if the following properties are satisfied:

1. If $(x, x') \in Y \times Y$, then $L(x, x')$ is empty, otherwise $L(x, x') \in X$.

2. Row or column x contains all the symbols in X if $x \in X \backslash Y$.

3. Row or column x contains all the symbols in $X \backslash Y$ if $x \in Y$.

The empty $u \times u$ subarray of L, indexed by $Y \times Y$, is called the *hole*.

We say that we have a set of *compatible* (m,u)-ILS if

1. all the squares are defined on a common m-set X, and

2. the holes in all the squares are defined on a common u-subset $Y \subseteq X$.

A set of s compatible (m,u)-ILS are said to be *R-orthogonal* (m,u)-*ILS* if the superposition of any two ILS in the set yields exactly R different ordered pairs of symbols, where we exclude any ordered pairs in which both symbols are contained in the hole. More formally, if $L_1, \ldots, L_2$ are compatible (m,u)-ILS, then

$$|\{(L_i(x,y), L_j(x,y)) : (x,y) \in X^2 \backslash Y^2\} \cap (X^2 \backslash Y^2)| = R$$

for all i, j such that $1 \le i < j \le s$.

It is clear that two or more R-orthogonal (m,u)-ILS can exist only if $R \le m^2 - u^2$. In the boundary case, where $R = m^2 - u^2$, the squares are known as (m,u)-*incomplete MOLS*, or *IMOLS*(m,u). The next theorem uses MOLS or order n sharing a common transversal to construct sets of n^2-orthogonal incomplete latin squares.

Theorem 2.5 *Suppose there exist $t+1$ MOLS of order n, and suppose that $1 \le \theta \le n$. Then there exist t n^2-orthogonal $(n+\theta, \theta)$-ILS.*

Proof. It is well-known that $t+1$ MOLS of order n are equivalent to t MOLS of order n containing n common disjoint transversals, say $T_1, \ldots, T_n$. Choose θ of these transversals, say $T_1, \ldots, T_\theta$, and project them onto θ new rows and columns. For $1 \le i \le \theta$, create a new symbol ∞_i, and place ∞_i in every cell of T_i in each of the t latin squares. Each of the resulting squares is an $(n+\theta, \theta)$-ILS in which the hole is defined on the infinite symbols. The superposition of each pair of these squares yields all n^2 pairs of finite symbols. □

We now generalize Theorem 2.3 to the case of R-orthogonal incomplete latin squares.

Theorem 2.6 *Suppose there exist t R-orthogonal (m,u)-ILS, and suppose that $s = qt + r$, where $q \ge 0$ and $0 \le r \le t-1$. Then*

$$\mathsf{P}(s,m) \ge R\binom{s}{2} - (R - m + u)\left(r\binom{q+1}{2} + (t-r)\binom{q}{2}\right) + \mathsf{P}(s,u).$$

Proof. We use the same technique as in the proof of Theorem 2.3. Let $L_0, \dots, L_{t-1}$ be t R-orthogonal (m,u)-ILS. For $t \le i \le s-1$, define $L_i = L_{i \bmod t}$. Let $M_0, \dots, M_{s-1}$ be latin squares of order u such that $P(M_1, \dots, M_t) = \mathsf{P}(t,u)$. Define these t latin squares on the symbols in the holes of the L_i's. Now fill in the hole in each L_i with M_i. Call the resulting squares $L'_0, \dots, L'_{s-1}$. A straightforward calculation shows that

$$P(L'_0, \dots, L'_{s-1}) = R\binom{s}{2} - (R - m + u)\left(r\binom{q+1}{2} + (t-r)\binom{q}{2}\right) + \mathsf{P}(s,u).$$

□

Corollary 2.7 *Suppose there are t IMOLS$(m,2)$, and suppose that $s = qt + r$, where $q \ge 0$ and $0 \le r \le t-1$. Then*

$$\mathsf{P}(s,m) \ge (m^2 - 2)\binom{s}{2} - (m^2 - m - 2)\left(r\binom{q+1}{2} + (t-r)\binom{q}{2}\right).$$

Proof. Apply Theorem 2.6 with $u = 2$ and $R = m^2 - 4$, noting that $\mathsf{P}(s,2) = 2\binom{s}{2}$ for all $s \ge 2$. □

Corollary 2.8 *Suppose there are $t+1$ MOLS of order $m-1$, and suppose that $s = qt + r$, where $q \ge 0$ and $0 \le r \le t-1$. Then*

$$\mathsf{P}(s,m) \ge ((m-1)^2 + 1)\binom{s}{2} - (m-1)(m-2)\left(r\binom{q+1}{2} + (t-r)\binom{q}{2}\right).$$

Proof. Apply Theorem 2.5 with $\theta = 1$ and then apply Theorem 2.6 with $u = 1$ and $R = (m-1)^2$, noting that $\mathsf{P}(s,1) = \binom{s}{2}$ for all $s \ge 2$. □

The quantity $\mathsf{P}(s,m)/\binom{s}{2}$ is the average number of different ordered pairs of symbols obtained from the relevant set of s latin squares of order m. If we divide by m^2, then the result is the proportion of different ordered pairs of symbols obtained from the relevant set of s latin squares of order m. This quantity, which we denote by $\rho(s,m)$, is computed as

$$\rho(s,m) = \frac{\mathsf{P}(s,m)}{\binom{s}{2} m^2}.$$

2.1 An example: $m = 10$

We look at the case $m = 10$ to compare the various constructions we have described. It is well-known that there exist two MOLS of order 10 and eight MOLS of order 9 (see, for example, [3]). Also, Brouwer constructed four IMOLS$(10,2)$ in [2].

Keedwell and Mullen [5] have constructed a certain set of nine latin squares of order 10 using D-neofields. These latin squares can be denoted $L_0, \dots, L_8$ such that the following holds:

$$P(L_i, L_j) = \begin{cases} 100 & \text{if } i - j \equiv \pm 1 \pmod 9 \\ 82 & \text{if } i - j \equiv \pm 2, \pm 4 \pmod 9 \\ 64 & \text{if } i - j \equiv \pm 3 \pmod 9). \end{cases}$$

Table 1: Latin Squares of Order 10

	2	3	4	5	6	7	8	9	10
Corollary 2.4	1.00	.70	.70	.64	.64	.61	.61	.60	.60
Corollary 2.7	.98	.98	.98	.89	.86	.85	.85	.83	.82
Corollary 2.8	.82	.82	.82	.82	.82	.82	.79	.78	.77
Keedwell and Mullen [5]	1.00	.94	.88	.86	.84	.83	.82	.82	

In Table 1, we list lower bounds on $\rho(s,10)$ that are obtained from Corollary 2.4 with $m=10$ and $t=2$; Corollary 2.7 with $m=10$ and $t=4$; and Corollary 2.8 with $m=10$ and $t=7$. We also tabulate the values obtained by using the sets of squares $\{L_0,\dots,L_i\}$ $(2\le i\le 9)$ from [5] that are mentioned above.

It can be seen that Corollary 2.7 yields the best results for $3\le s\le 10$. It is not hard to see that this is true for large values of s, too. Suppose we denote the four lower bounds on $\rho(s,10)$ by $\rho_1(s)$, $\rho_2(s)$, $\rho_3(s)$ and $\rho_4(s)$, respectively. For simplicity, assume that $s=qt$, where q is an integer. Then, for $1\le i\le 4$, it is straightforward to see that

$$\rho_i(qt_i)=\frac{A_i}{m^2}-\frac{B_i(q-1)}{m^2(qt_i-1)},$$

where

$$\begin{array}{lll} A_1=100, & B_1=90, & t_1=2,\\ A_2=98, & B_2=88, & t_2=4,\\ A_3=82, & B_3=72, & t_3=7,\\ A_4=82, & B_4=72, & t_4=9, \end{array}$$

and $m=10$. Taking the limit as q approaches ∞, we have

$$\lim_{q\to\infty}\rho_i(qt_i)=\frac{A_i}{m^2}-\frac{B_i}{m^2t_i},$$

$1\le i\le 4$. Then it is straightforward to compute the following limits: $\lim_{q\to\infty}\rho_1(qt_1)=.55$, $\lim_{q\to\infty}\rho_2(qt_2)=.76$, $\lim_{q\to\infty}\rho_3(qt_3)=.717$, and $\lim_{q\to\infty}\rho_4(qt_4)=.74$.

The best result among the four is the one obtained from Corollary 2.7, which says that one can construct arbitrarily large sets of latin squares of order 10 in which the number of different ordered pairs (obtained from superimposing any two of them) is, on average, almost 76.

3 Bounds

In this section, we derive an upper bound on $\mathsf{P}(s,m)$. The following simple counting argument yields an upper bound on $\mathsf{P}(s,m)$ that is stronger than Theorem 2.1 whenever $s\ge m$.

Theorem 3.1 *Suppose that $s=a(m-1)+b$, $a\ge 0$, and $0\le b\le m-2$. Then*

$$\mathsf{P}(s,m)\le m^2\binom{s}{2}-(m^2-m)\left(b\binom{a+1}{2}+(m-1-b)\binom{a}{2}\right).$$

Proof. Let $L_1, \ldots, L_s$ be s latin squares of order m on symbol set $1, \ldots, m$. We can assume without loss of generality that these s latin squares are *standardized*; i.e., the first row of each of these s squares is $1\ 2\ \cdots\ m$. For $i \neq j$, define

$$P^*(L_i, L_j) = |\{(L_i(x,y), L_j(x,y)) : x, y \in X\} \backslash \{(1,1), \ldots, (m,m)\}|.$$

Then it is easy to see that

$$P(L_1, \ldots, L_s) = m\binom{s}{2} + \sum_{1 \le i < j \le s} P^*(L_i, L_j). \tag{1}$$

Now consider any cell not in the first row, say cell (x, y). It is clear that $L_i(x,y) \neq y$, $1 \le i \le s$. For $1 \le z \le m$, $z \neq y$, we define $f_{x,y,z}$ as the number of squares that contain z in the (x,y) cell. More formally,

$$f_{x,y,z} = |\{i : L_i(x,y) = z\}|.$$

Denote

$$T_{x,y} = \sum_{z \neq y} \binom{f_{x,y,z}}{2}.$$

It is not hard to see that $T_{x,y}$ is minimized by taking the "$f_{x,y,z}$"s to be as equal as possible. Therefore

$$T_{x,y} \ge b\binom{a+1}{2} + (m-1-b)\binom{a}{2}, \tag{2}$$

where $s = a(m-1) + b$, $a \ge 0$, and $0 \le b \le m-2$.

Finally, it is easy to see that

$$\sum_{1 \le i < j \le s} P^*(L_i, L_j) \le \sum_{x=2}^{m} \sum_{y=1}^{m} \left(\binom{s}{2} - T_{x,y} \right). \tag{3}$$

Using (1), (2) and (3) and simplifying, the desired result is obtained. □

For future use, we denote the upper bound on $\mathsf{P}(s,m)$ obtained from Theorem 3.1 by $\Pi(s,m)$. Hence, if $s = a(m-1)+b$, $a \ge 0$, and $0 \le b \le m-2$, then

$$\Pi(s,m) = m^2\binom{s}{2} - (m^2 - m)\left(b\binom{a+1}{2} + (m-1-b)\binom{a}{2} \right).$$

We now record a useful corollary.

Corollary 3.2 *Suppose that $L_1, \ldots, L_s$ are latin squares of order m such that $P(L_1, \ldots, L_s)$ $= \Pi(s,m)$. Then there do not exist $i \neq j$ and $z \neq z'$ such that the superposition of L_i and L_j contains more than one occurrence of the ordered pair (z, z').*

Proof. In order for the upper bound of Theorem 3.1 to be attained, it must be the case that inequality (3) is an equality. The right side does not count any repeated ordered pairs of the form (z,z) in the superpositions of any of the pairs of squares L_i, L_j. Therefore, in order for (3) to be an equality, there can be no repeated pairs of the form (z,z') with $z \neq z'$. □

The bound of Theorem 3.1 is best possible whenever we have a complete set of MOLS of order m.

Theorem 3.3 *Suppose there exist $m-1$ MOLS of order m (i.e., a projective plane of order m). Write $s = q(m-1) + r$, where $q \geq 0$ and $0 \leq r \leq m-2$. Then*

$$\mathsf{P}(s, m) = \Pi(s, m).$$

Proof. Let $t = m-1$ in Corollary 2.4 and Theorem 3.1. ∎

4 Two Conjectures

As demonstrated in Theorem 3.3 the equality in Theorem 3.1 is attained by starting with a complete set of $m-1$ MOLS of order m and then repeating squares in this set as evenly as possible. It is natural to ask if this is the only way that the bound can be reached. Therefore we state the following two open problems, which present two versions of a conjecture related to this question.

Conjecture 4.1 *Suppose that $s \geq m-1$ and $L_1, \ldots, L_s$ are latin squares of order m such that $P(L_1, \ldots, L_s) = \Pi(s, m)$. Then $\{L_1, \ldots, L_s\}$ contains a subset of $m-1$ MOLS of order m.*

Conjecture 4.2 *Suppose that $s \geq m-1$ and $L_1, \ldots, L_s$ are latin squares of order m such that $P(L_1, \ldots, L_s) = \Pi(s, m)$. Then $\{L_1, \ldots, L_s\}$ contains a subset of $m-1$ MOLS of order m, and the list $L_1, \ldots, L_s$ consists only of copies of these $m-1$ orthogonal latin squares, where each copy occurs either $\lfloor \frac{s}{m-1} \rfloor$ or $\lceil \frac{s}{m-1} \rceil$ times in the list.*

Clearly, Conjecture 4.2 implies Conjecture 4.1. Perhaps surprisingly, we can also show that Conjecture 4.1 implies Conjecture 4.2. In order to prove this result, we state and prove some lemmas.

Lemma 4.1 *Suppose that $L_1, \ldots, L_{m-1}$ are a set of $m-1$ standardized MOLS of order m. Let $(x, y), (x', y') \in \{2, \ldots, m\} \times \{1, \ldots, m\}$, $x \neq x'$, $y \neq y'$. Then there exists a unique i, $1 \leq i \leq m-1$, such that $L_i(x, y) = L_i(x', y')$.*

Proof. A set of $m-1$ MOLS of order m is equivalent to an affine plane with the m^2 cells corresponding to the points and the m cells which contain a common symbol in a given latin square corresponding to a line of the plane. Since each pair of points is on a unique line, we have that each pair of cells shares a common symbol in exactly one square. ∎

Lemma 4.2 *Suppose that $s \geq m-1$ and $L_1, \ldots, L_s$ are latin squares of order m such that $P(L_1, \ldots, L_s) = \Pi(s, m)$. Suppose also that $L_1, \ldots, L_{m-1}$ are mutually orthogonal. Then $L_j \in \{L_1, \ldots, L_{m-1}\}$ for all j, $1 \leq j \leq s$.*

Proof. Assume without loss of generality that all s latin squares are standardized. Choose any $L \in \{L_m, \ldots, L_s\}$. For any symbol s, define $\mathcal{T}_s = \{(x, y) : L(x, y) = s\}$; note that $(1, s) \in \mathcal{T}_s$. Let (x, y) and (x', y') be any two distinct cells in $\mathcal{T}_s \backslash \{(1, s)\}$. Applying Lemma

4.1, there is a unique i, $1 \le i \le m-1$, such that $L_i(x,y) = L_i(x',y')$. Denote $t = L_i(x,y)$; then

$$(s,t) = (L(x,y), L_i(x,y)) = (L(x',y'), L_i(x',y')).$$

Since $P(L_1,\ldots,L_s) = \Pi(s,m)$, Corollary 3.2 asserts that it must be the case that $s = t$. Repeating this argument, it is easy to see that $L_i(x,y) = L(x,y) = s$ for all $(x,y) \in \mathcal{T}_s$.

Now pick another symbol $s' \neq s$. By the same argument, there is an i' such that $L_{i'}(x,y) = L(x,y) = s'$ for all $(x,y) \in \mathcal{T}_{s'}$. Suppose that $i \neq i'$. Then the ordered pair (s,s') cannot occur in the superposition of L_i and $L_{i'}$, because $\mathcal{T}_s$ and $\mathcal{T}_{s'}$ are disjoint. This contracts the assumption that L_i and $L_{i'}$ are orthogonal, and hence it must be the case that $i = i'$.

From the above argument, it follows that $L = L_i$, as desired. ∎

Theorem 4.3 *Suppose that $s \ge m-1$ and $L_1,\ldots,L_s$ are latin squares of order m such that $P(L_1,\ldots,L_s) = \Pi(s,m)$. Suppose further that $\{L_1,\ldots,L_s\}$ contains a subset of $m-1$ MOLS of order m. Then the list $L_1,\ldots,L_s$ consists only of copies of these $m-1$ orthogonal latin squares, where each copy occurs either $\lfloor \frac{s}{m-1} \rfloor$ or $\lceil \frac{s}{m-1} \rceil$ times in the list. If $1 \le s < m-1$, then $P(L_1,\ldots,L_s) = \Pi(s,m)$ if and only if $L_1,\ldots,L_s$ are a set of mutually orthogonal latin squares of side m.*

Proof. When $1 \le s < m-1$ this is obvious. Now suppose that $s \ge m-1$ and that $L_1,\ldots,L_{m-1}$ are mutually orthogonal. From Lemma 4.2, it follows that the list $L_1,\ldots,L_s$ consists only of copies of $L_1,\ldots,L_{m-1}$. Suppose that L_i occurs c_i times, $1 \le i \le m-1$. Assume that $c_i \ge c_j + 2$, for some i and j. Construct a modified list, say $L'_1,\ldots,L'_s$, by replacing one occurrence of L_i by L_j. Then it is easy to see that

$$P(L'_1,\ldots,L'_s) > P(L_1,\ldots,L_s),$$

which contradicts the fact that $P(L_1,\ldots,L_s)$ is as large as possible. The desired result follows. ∎

Since we have shown that Conjecture 4.2 and Conjecture 4.1 are equivalent, we will now refer to both Conjecture 4.2 and Conjecture 4.1 simply as *the conjecture*, and use whichever form is more convenient.

5 Latin squares of small orders

To gain some evidence in favor of the conjecture, it is instructive to look at latin squares of small orders.

5.1 Squares of order 3

In the case of latin squares of order 3, there are only two standardized latin squares and they are orthogonal. Hence it follows that the only way that s latin squares of order 3 can attain the bound of Theorem 3.1 is if they contain a pair of orthogonal latin squares of order 3. Thus the conjecture is true for $m = 3$.

5.2 Squares of order 4

We prove the conjecture is true for latin squares of order 4.

Theorem 5.1 *Suppose that $L_1, \dots, L_s$ are latin squares of order 4 such that $P(L_1, \dots, L_s) = \Pi(s,4)$. Then the list $L_1, \dots, L_s$ consists only of copies of latin squares from a set of three MOLS or order 4, where each latin square occurs either $\lfloor \frac{s}{3} \rfloor$ or $\lceil \frac{s}{3} \rceil$ times in the list.*

Proof. Assume $L_1, \dots, L_s$ are latin squares of order 4 with $P(L_1, \dots, L_s) = \Pi(s,4)$. We proceed by induction on s, noting first that the conjecture is trivially true for $s = 2$ and 3. We have also verified the validity of the conjecture for $4 \le s \le 8$. Hence we can assume that $s \ge 9$.

If this set contains a set of three MOLS of order 4, then the set satisfies the conjecture. We can therefore assume that the set contains *at most* two MOLS or order 4. First, we assume that the set contains a pair of MOLS of order 4. Call these orthogonal squares L_1 and L_2. We have shown by computer that, if L is any latin square of order 4 not orthogonal to L_1, then one of the following conditions holds:

a) $P(L_1, L) + P(L_2, L) = 24$, in which case $P(L_1, L) = P(L_2, L) = 12$, or

b) $P(L_1, L) + P(L_2, L) \le 18$.

Assume we are in case a) and L_3 has the property that $P(L_1, L_3) + P(L_2, L_3) = 24$ (hence, by what was said above, $P(L_1, L_3) = P(L_2, L_3) = 12$). From a computer search, we have the following result: if L is any latin square of order 4 not orthogonal to L_1, then

$$P(L_1, L) + P(L_2, L) + P(L_3, L) \le 33.$$

Hence, we have that

$$P(L_1, \dots, L_s) \le 33(s-3) + (16 + 12 + 12) + \Pi(s-3, 4) = 33s - 59 + \Pi(s-3, 4). \quad (4)$$

Now, from Theorem 3.3 we know that the upper bound $\Pi(s,4)$ can be attained in the manner prescribed by Conjecture 4.2. Let $M_1, M_2, \dots M_{s-3}$ be a set of latin squares of order 4 such that $P(M_1, \dots, M_{s-3}) = \Pi(s-3, 4)$ and which satisfy the conclusion of Conjecture 4.2. That is, they consist of copies of some set of three MOLS of order 4, say N_1, N_2, N_3. We can assume that there are a_i copies of N_i, $1 \le i \le 3$, where

$$\left\lceil \frac{s-3}{3} \right\rceil = a_1 \ge a_2 \ge a_3 = \left\lfloor \frac{s-3}{3} \right\rfloor$$

and

$$s - 3 = a_1 + a_2 + a_3.$$

Now add three more squares M_{s-2}, M_{s-1}, and M_s to this set, where $M_{s-2} = N_1$, $M_{s-1} = N_2$ and $M_s = N_3$. We have

$$\begin{aligned} &P(M_1, \dots, M_s) \\ &= 16(a_2 + a_3) + 16(a_1 + a_3) + 16(a_2 + a_3) + 4(a_1 + a_2 + a_3) + 48 + \Pi(s-3, 4) \\ &= 36(a_1 + a_2 + a_3) + 48 + \Pi(s-3, 4) \\ &= 36(s-3) + 48 + \Pi(s-3, 4) \\ &= 36s - 60 + \Pi(s-3, 4). \end{aligned}$$

Comparing this to the bound in (4), we have that $P(L_1, \ldots, L_s) < P(M_1, \ldots, M_s) = \Pi(s, 4)$, contradicting the fact that the set $L_1, \ldots, L_s$ attains the bound of Theorem 3.1. Thus there is no set attaining the bound that contains two MOLS of order 4 (but not three MOLS of order 4) in case a).

Now we look at case b), above assuming that case a) does not occur. Here, we have that L_1 is orthogonal to L_2, and for any $3 \leq i \leq s$, it holds that $P(L_1, L_i) + P(L_2, L_i) \leq 18$. Hence, we see that

$$P(L_1, \ldots, L_s) \leq 18(s-2) + 16 + \Pi(s-2, 4) = 18s - 20 + \Pi(s-2, 4). \tag{5}$$

Similar to what was done above, we now let $M_1, M_2, \ldots M_{s-2}$ be a set of latin squares of order 4 such that $P(M_1, \ldots, M_{s-2}) = \Pi(s-2, 4)$ and which satisfy the conclusion of Conjecture 4.2. That is, they consist of copies of some set of three MOLS of order 4, say N_1, N_2, N_3. We again assume that there are a_i copies of N_i, $1 \leq i \leq 3$, where

$$\left\lceil \frac{s-2}{3} \right\rceil = a_1 \geq a_2 \geq a_3 = \left\lfloor \frac{s-2}{3} \right\rfloor$$

and

$$s - 2 = a_1 + a_2 + a_3.$$

Now add two more squares M_{s-1} and M_s to this set, where $M_{s-1} = N_2$, $M_s = N_3$. We have

$$\begin{aligned} P(M_1, \ldots, M_s) &= 16(a_1 + a_3) + 16(a_1 + a_2) + 4(a_2 + a_3) + 16 + \Pi(s-2, 4) \\ &= 32a_1 + 20(a_2 + a_3) + 16 + \Pi(s-2, 4) \\ &\geq 20(a_1 + a_2 + a_3) + 16 + \Pi(s-2, 4) \\ &= 20(s-2) + 16 + \Pi(s-2, 4) \\ &= 20s - 4 + \Pi(s-2, 4). \end{aligned}$$

Comparing this to the bound in (5), we have that $P(L_1, \ldots, L_s) < P(M_1, \ldots, M_s) = \Pi(s, 4)$, contradicting the fact that the set $L_1, \ldots, L_s$ attains the bound of Theorem 3.1. From this case and from case a), there is no set attaining the bound that contains two MOLS of order 4 (but not three MOLS of order 4).

Finally, we assume that no two of the latin squares $L_1, \ldots, L_s$ are orthogonal. By computer, we have shown the following fact: Given any set of four latin squares L_1, L_2, L_3 and L_4 of order 4 with the property that no two of them are orthogonal, it holds that

$$P(L_1, L_2, L_3, L_4) \leq 69.$$

From this, it follows that

$$P(L_1, \ldots, L_s) \leq \frac{69}{6} \times \binom{s}{2} = 11.5 \times \binom{s}{2}.$$

It is not hard to check that

$$\Pi(s, 4) \geq 12 \times \binom{s}{2}$$

for all $s > 2$. Hence the set $L_1, \ldots, L_s$ can not attain the upper bound in this last case, which completes the proof. $\square$

5.3 Squares of order 5

We now prove that the conjecture is also true for $m = 5$.

Theorem 5.2 *Suppose that $L_1, \ldots, L_s$ are latin squares of order 5 such that $P(L_1, \ldots, L_s) = \Pi(s, 5)$. Then the list $L_1, \ldots, L_s$ consists only of copies of latin squares from a set of four MOLS or order 5, where each latin square occurs either $\lfloor \frac{s}{4} \rfloor$ or $\lceil \frac{s}{4} \rceil$ times in the list.*

Proof. There are precisely 1344 standardized latin squares of order 5 and it can be checked that $P(L, M) = 25$ or $P(L, M) \leq 21$ for any two latin quares L and M of order 5. Assume $L_1, \ldots, L_s$ are latin squares of order 5 with $P(L_1, \ldots, L_s) = \Pi(s, 5)$. We proceed by induction on s, noting first that the conjecture is trivially true for $s = 2, 3$ and 4. So we can assume $s \geq 5$.

If this set contains four MOLS of order 5, then the set satisfies the conjecture (Conjecture 4.1). Next, we assume that the maximum number of mutually orthogonal squares in this set is three (say L_1, L_2 and L_3 are orthogonal). We have found by exhaustive computer search that if L is any latin square of order 5 not orthogonal to L_1, then $P(L_1, L) + P(L_2, L) + P(L_3, L) \leq 57$. Since there is not a set of four MOLS in the set $L_1, \ldots, L_s$ then none of the squares $L_4, \ldots, L_s$ can be orthogonal to L_1 (or it would be orthogonal to L_2 and L_3 also and would result in a set of four MOLS).

Hence we have that

$$P(L_1, \ldots, L_s) \leq 57(s-3) + 75 + \Pi(s-3, 5) = 57s - 96 + \Pi(s-3, 5). \tag{6}$$

Now, from Theorem 3.3 we know that the upper bound $\Pi(s, 5)$ can be attained in the manner prescribed by Conjecture 4.2. Let $M_1, M_2, \ldots M_{s-3}$ be a set of latin squares of order 5 such that $P(M_1, \ldots, M_{s-3}) = \Pi(s-3, 5)$ and which satisfy the conclusion of Conjecture 4.2. That is, they consist of copies of some set of four MOLS of order 5, say N_1, N_2, N_3, N_4. We can assume that there are a_i copies of N_i, $1 \leq i \leq 4$, where

$$\left\lceil \frac{s-3}{4} \right\rceil = a_1 \geq a_2 \geq a_3 \geq a_4 = \left\lfloor \frac{s-3}{4} \right\rfloor$$

and

$$s - 3 = a_1 + a_2 + a_3 + a_4.$$

Now add three more squares M_{s-2}, M_{s-1}, and M_s to this set, where $M_{s-2} = N_2$, $M_{s-1} = N_3$ and $M_s = N_4$. These three squares are orthogonal to each other and are copies of three of the squares in the set $M_1, M_2, \ldots, M_{s-3}$ that occur the least number of times.

Now we have

$$\begin{aligned} & P(M_1, \ldots, M_s) \\ \geq \;& 25(a_1 + a_3 + a_4) + 25(a_1 + a_2 + a_4) + 25(a_1 + a_2 + a_3) + 5(a_2 + a_3 + a_4) \\ & \quad +75 + \Pi(s-3, 5) \\ = \;& 75a_1 + 55(a_2 + a_3 + a_4) + 75 + \Pi(s-3, 5) \\ \geq \;& 75 \left\lceil \frac{s-3}{4} \right\rceil + 165 \left\lfloor \frac{s-3}{4} \right\rfloor + 75 + \Pi(s-3, 5). \end{aligned}$$

Looking at the four different residue classes of s modulo 4, we obtain in each case that

$$P(M_1,\ldots,M_s) \geq 60s - 105 + \Pi(s-3,5).$$

Comparing the above to the bound in (6), we have that $P(L_1,\ldots,L_s) < P(M_1,\ldots,M_s) = \Pi(s,5)$, contradicting the fact that the set $L_1,\ldots,L_s$ attains the bound of Theorem 3.1. Thus there is no set attaining the bound that contains three MOLS of order 5 (but not four MOLS of order 5).

Next, assume that the maximum number of mutually orthogonal squares in this set is two (say L_1, L_2 are orthogonal). By computer search we have that if L is any latin square of order 5 not orthogonal to L_1, then $P(L_1,L) + P(L_2,L) \leq 38$. Then we have that

$$P(L_1,\ldots,L_s) \leq 38(s-2) + 25 + \Pi(s-2,5) = 38s - 51 + \Pi(s-2,5). \qquad (7)$$

We again know that the upper bound can be attained in the manner prescribed by Conjecture 4.2. Let $M_1, M_2, \ldots M_{s-2}$ be a set of latin squares satisfying $P(M_1,\ldots,M_{s-2}) = \Pi(s-2,5)$ and satisfying the conclusion of Conjecture 4.2 (i.e., copies of the squares in some set of four MOLS of order 5). Add two more squares, M_{s-1} and M_s, to this set in such a way that they are orthogonal to each other and are copies of two of the squares in the set $M_1, M_2, \ldots M_{s-2}$ that occur the least. Proceeding in a manner similar to the last case, it is possible to show that

$$\begin{aligned} P(M_1,\ldots,M_s) &\geq 50\left\lceil\frac{s-2}{4}\right\rceil + 50\left\lfloor\frac{s-2}{4}\right\rfloor + 2\times 30\left\lfloor\frac{s-2}{4}\right\rfloor + 25 + \Pi(s-2,5) \\ &\geq 40s - 55 + \Pi(s-2,5). \end{aligned}$$

Comparing the above bound to that in (7) we have that $P(L_1,\ldots,L_s) < P(M_1,\ldots,M_s) = \Pi(s,5)$, contradicting the fact that the set $L_1,\ldots,L_s$ attains the bound of Theorem 3.1. Thus there is no set attaining the bound that contains at two MOLS of order 5 (but not three MOLS of order 5).

Finally, we assume that no two of the latin squares $L_1,\ldots,L_s$ are orthogonal. By computer, we have shown the following fact: Given any set of five latin squares $L_1,\ldots,L_5$ of order 5 with the property that no two of them are orthogonal, then $P(L_1,\ldots,L_5) \leq 194$. From this we see that

$$P(L_1,\ldots,L_s) \leq 19.4 \times \binom{s}{2}.$$

Now it is not hard to check that $\Pi(s,5) \geq 20 \times \binom{s}{2}$ for all $s > 1$ Hence the set $L_1,\ldots,L_s$ can not attain the upper bound in this last case. This completes the proof. ∎

5.4 Squares of order 6

From the results of Keedwell and Mullen [5], it follows that $\mathsf{P}(s,6) \geq 26\binom{s}{2}$ for $s = 3, 4$ and 5, and hence that $\mathsf{P}(3,6) \geq 78$, $\mathsf{P}(4,6) \geq 156$, and $\mathsf{P}(5,6) \geq 260$. Also, it is well known that a two MOLS of order 6 do not exist, but that there exist two IMOLS(6, 2) (see, for example, [3]). Therefore, $\mathsf{P}(2,6) = 34$. The two latin squares L_1 and L_2 attaining this bound are given below.

$$L_1 = \begin{array}{|cccccc|}\hline 5&6&3&4&1&2\\ 2&1&6&5&3&4\\ 6&5&1&2&4&3\\ 4&3&5&6&2&1\\ 1&4&2&3&5&6\\ 3&2&4&1&6&5\\ \hline\end{array} \qquad L_2 = \begin{array}{|cccccc|}\hline 1&2&5&6&3&4\\ 6&5&1&2&4&3\\ 4&3&6&5&1&2\\ 5&6&4&3&2&1\\ 2&4&3&1&5&6\\ 3&1&2&4&6&5\\ \hline\end{array}$$

We have done some brief computations with latin squares of order 6. Starting with L_1 and L_2, we have found latin squares L_3, L_4 and L_5 such that the set of latin squares $L_1, L_2, \ldots, L_i$ improves the lower bound for $\mathsf{P}(i, 6)$ for $i = 3, 4$ and 5. Let

$$L_3 = \begin{array}{|cccccc|}\hline 1&2&3&4&5&6\\ 2&1&6&5&4&3\\ 3&4&5&6&2&1\\ 5&3&2&1&6&4\\ 4&6&1&2&3&5\\ 6&5&4&3&1&2\\ \hline\end{array} \qquad L_4 = \begin{array}{|cccccc|}\hline 1&2&3&4&5&6\\ 5&4&6&2&1&3\\ 4&6&2&1&3&5\\ 6&1&5&3&4&2\\ 3&5&4&6&2&1\\ 2&3&1&5&6&4\\ \hline\end{array} \qquad L_5 = \begin{array}{|cccccc|}\hline 1&2&3&4&5&6\\ 3&5&4&6&1&2\\ 5&3&1&2&6&4\\ 4&6&2&1&3&5\\ 2&1&6&5&4&3\\ 6&4&5&3&2&1\\ \hline\end{array}.$$

It is not difficult to check that $P(L_1, L_2, L_3) = 91$, $P(L_1, L_2, L_3, L_4) = 178$ and that $P(L_1, L_2, L_3, L_4, L_5) = 295$. Hence we have that $\mathsf{P}(3, 6) \geq 91$, $\mathsf{P}(4, 6) \geq 178$, and $\mathsf{P}(5, 6) \geq 295$, improving upon the results of [5]. We believe that all of these bounds can probably be further improved.

6 Comments

Proving or disproving the conjecture is a very interesting open problem. It would also be of interest to find good upper and lower bounds on $\mathsf{P}(s, m)$ which can be applied if $m - 1$ MOLS of order m do not exist.

Acknowledgments

Research of the second author is supported by NSERC grant RGPIN 203114-02.

References

[1] G.B. Belyavskaya. r-orthogonal Latin squares. In "Latin Squares: New Developments in the Theory and Applications", North-Holland, 1991, pp. 169–202.

[2] A.E. Brouwer. Four MOLS of order 10 with a hole of order 2. *J. Statist. Plann. Inference* **10** (1984), 203–205.

[3] C.J. Colbourn and J.H. Dinitz. *The CRC Handbook of Combinatorial Designs*, CRC Press, 1996.

[4] C.J. Colbourn and L. Zhu. The spectrum of R-orthogonal Latin squares. In "Combinatorics Advances", Kluwer Academic Publishers, 1995, pp. 49–75.

[5] A.D. Keedwell and G.L. Mullen. Sets of partially orthogonal Latin squares and projective planes. Preprint.