New and Old Values for Maximal MOLS(n)

David Bedford, Roger M. Whitaker

Department of Mathematics
Keele University
Keele, Staffordshire, ST5 5BG, U.K.

Abstract

Let k Max MOLS(n) denote a maximal set of k mutually orthogonal latin squares of order n, and let the parameter triple (G, n, k) denote the existence of a k Max MOLS(n) constructed from orthogonal orthomorphisms of a group G of order n. We identify all such parameter triples for all G of order ≤ 15, and report the existence of 3 Max MOLS(n) for $n = 15, 16$ and 4 Max MOLS(n) for $n = 12, 16, 24, 28$. Our work shows that for $n \leq 15$, all known parameter pairs (n, k) for which there exists a k Max MOLS(n) can be attained by constructing maximal sets of MOLS from orthomorphisms of groups, except for 1 Max MOLS(n), $n = 5, 7, 9, 13$ and 2 Max MOLS(10).

Keywords: difference matrix; group; latin square; orthogonal; orthomorphism.

1 Introduction

Let $S = \{L_1, L_2, \ldots, L_k\}$ be a set of mutually orthogonal latin squares (MOLS) of order n. If S cannot be extended to a set of $k+1$ MOLS of order n then S is *maximal*, and as in [6], we say that S is a k Max MOLS(n). A set of MOLS S is said to be *based* on a finite group G if every latin square from S can be bordered so as to form the Cayley table of G. A well known method of constructing sets of MOLS based on G is by using *orthogonal orthomorphisms* of G. An *orthomorphism* of G is a permutation ϕ on G with the property that the mapping $\theta : g \mapsto g^{-1}\phi(g)$ is a permutation on G. Two orthomorphisms of G, say ϕ_1, ϕ_2, are said to be *orthogonal* if the mapping $\psi : g \mapsto \phi_1(g)^{-1}\phi_2(g)$ is a permutation on G. The existence of a set of k mutually orthogonal orthomorphisms $\{\phi_1, \phi_2, \ldots, \phi_k\}$ is sufficient for the existence of a set of $k+1$ MOLS based on G, namely $\{L, L_1, \ldots, L_k\}$ where L is the Cayley table of G and L_i is L with columns permuted according to ϕ_i. These results are well known. For a detailed discussion see [2, 5]. We shall call a set of mutually orthogonal orthomorphisms of G *maximal* if it cannot be extended. A set S of k mutually orthogonal orthomorphisms of a group G of order n is equivalent to a $(n, k+1; G)$ *difference matrix*, that is a matrix $D = (d_{ij})$, $i = 1, \ldots, k+1, j = 1, \ldots, n$, where $d_{ij} \in G$ and when G is written additively, $\{d_{ij} - d_{hj} : j = 1, \ldots, n\} = G$ whenever $i \neq h$. For further discussion of difference matrices, see [3, 4].

As noted on p540 of [3] (and also on p7 of [5]), the following theorem was implicitly given in [8] and has been very successful in establishing parameter pairs (n, k) for which there exists k Max MOLS(n).

Theorem 1 *Let L be the Cayley table of a finite group G, let $S = \{\phi_1, \phi_2, \ldots, \phi_k\}$ be a set of mutually orthogonal orthomorphisms of G, and let L_i denote L after permutation of its columns according to ϕ_i. Then S is maximal if and only if $\{L, L_1, \ldots, L_k\}$ is a maximal set of MOLS.*

Proof: See Evans [5], page 7. □

2 Results

Let the parameter triple (G, n, k) denote the existence of a k Max MOLS(n) constructed from orthogonal orthomorphisms of a group G of order n. In [7], Jungnickel and Grams identified all such parameter triples for all G of order ≤ 10. By means of an exhaustive backtracking computer search we extend this to $n \leq 15$. We also extend the results of Table 27.13 of [6] by establishing new values of k for larger n. In Table 1, we document the known values of k for $n \leq 15$. We include a group H in the column headed G if and only if the parameter triple (H, n, k) exists. k^* indicates that k is new and $N(n)$ denotes the best known lower bound on the maximum number of latin squares of order n in a mutually orthogonal set.

n	$N(n)$	k	G
2	1	1	C_2
3	2	2	C_3
4	3	1	C_4
		3	$C_2 \times C_2$
5	4	1	
		4	C_5
6	1	1	C_6, S_3
7	6	1	
		2, 6	C_7
8	7	1	C_8
		2	D_4, Q_4
		3	$C_2 \times C_2 \times C_2, C_2 \times C_4$
		7	$C_2 \times C_2 \times C_2$
9	8	1	

n	$N(n)$	k	G
9	8	2	C_9
		3, 5, 8	$C_3 \times C_3$
10	2	1	C_{10}, D_5
		2	
11	10	2, 3, 4, 10	C_{11}
12	5	1	C_{12}, Q_6
		2	$C_6 \times C_2, D_6, A_4$
		3	$C_6 \times C_2, D_6$
		4^*, 5	$C_6 \times C_2$
13	12	1	
		2, 3, 4, 6, 12	C_{13}
14	3	1	C_{14}, D_7
15	4	2, 3^*, 4	C_{15}

Table 1:

As a part of our work, we have verified that there exist no more than 3 mutually orthogonal orthomorphisms of C_{15}. This confirms unpublished results obtained by Roth and Wilson [11]. Our approach was to use an exhaustive backtracking search for a set $X = \{\theta_1, \ldots, \theta_4\}$, of 4 complete mappings of Z_{15}, whose corresponding orthomorphisms were mutually orthogonal. W.l.o.g, it can be assumed that $\theta_i(0) = 0$, for $i = 1, \ldots, 4$. The search was split into two parts. Let $Y = \{\theta_i(1) : i = 1, \ldots, 4\}$. Part (i) consisted of a search for a set X such that Y contains at least one generator of Z_{15}, whilst part (ii) consisted of a search for a set X such that Y contains no generator of Z_{15}. The total computation time was approximately 650 hours using Pentium 400 MHz machines.

Below we give examples of sets of orthomorphisms which realise the new parameter pairs (12, 4), and (15, 3).

$\{\phi_1, \phi_2, \phi_3\}$ is a maximal set of mutually orthogonal orthomorphisms realising $(C_6 \times C_2, 12, 4)$ where $C_6 \times C_2 = \langle a, b : a^6 = b^2 = e, ab = ba \rangle$ and :

$$\begin{aligned} \phi_1 &= (e)(a, a^2, a^4, a^3b, a^2b, b, a^3, a^4b, ab, a^5, a^5b) \\ \phi_2 &= (e)(a, a^4, ab, a^5b, a^4b, a^3, a^5, b, a^2, a^2b, a^3b) \\ \phi_3 &= (e)(a, a^2b, a^5, ab, a^3b, b, a^5b, a^4, a^4b, a^2, a^3). \end{aligned}$$

$\{\phi_1, \phi_2\}$ is a maximal set of mutually orthogonal orthomorphisms realising $(C_{15}, 15, 3)$ where $C_{15} = \langle a : a^{15} = e \rangle$ and:

$$\begin{aligned} \phi_1 &= (e)(a, a^2, a^4, a^8, a^{14}, a^{11}, a^9, a^5, a^{10}, a^3, a^6, a^{13}, a^{12}, a^7) \\ \phi_2 &= (e)(a, a^3, a^2, a^6, a^{12}, a^{10}, a^7, a^8, a^{11}, a^4, a^{13}, a^5)(a^9, a^{14}). \end{aligned}$$

In addition to the results in Table 1, we have also established (16, 3), (16, 4), (28, 4) and verified (24, 4) which was omitted from Table 27.13 of [6].

$\{\phi_1, \phi_2\}$ is a maximal set of mutually orthogonal orthomorphisms realising $(D_8, 16, 3)$ where $D_8 = \langle a, b : a^8 = e, b^2 = e, ab = ba^{-1} \rangle$ and:

$$\begin{aligned} \phi_1 &= (e)(a, a^2, a^4, a^4b, a^7, a^2b, a^3, a^6, b, a^3b, a^5, a^6b, a^7b, ab, a^5b) \\ \phi_2 &= (e)(a, a^3, a^3b, a^6b, a^7, a^5b, a^4b, ab, a^2b)(a^2, a^6, a^4, b, a^5, a^7b). \end{aligned}$$

In [9], a set of 3 mutually orthogonal orthomorphisms of D_8 were exhibited. No indication was given as to whether this was maximal. From an exhaustive computer search, we report that this set is in fact maximal, thereby establishing $(D_8, 16, 4)$.

Roth and Peters [10] established the existence of 4 pairwise orthogonal latin squares of order 24 from orthogonal orthomorphisms of $C_6 \times C_2 \times C_2$, and as stated by Roth and Peters, these sets are maximal, thereby establishing $(C_6 \times C_2 \times C_2, 24, 4)$.

Abel [1] constructed 4 MOLS of order 28 from a resolvable transversal design. In [2], Bedford used this transversal design to construct a set of 3 mutually orthogonal orthomorphisms of $C_2 \times C_2 \times C_7$. Our computer search has shown that this set of orthomorphisms could not be extended thereby establishing $(C_2 \times C_2 \times C_7, 28, 4)$.

ACKNOWLEDGEMENT
The authors wish to thank the referee for the helpful comments made, and for drawing their attention to the unpublished work by Roth and Wilson.

References

[1] R.J.R. Abel, Four mutually orthogonal latin squares of order 28 and 52, J. Combinatorial Theory (A), 58 (1991), 306-309.

[2] D.Bedford, Orthomorphisms and near-orthomorphisms of groups and orthogonal latin squares: a survey, Bulletin of the Institute of Combinatorics and its Applications, 15 (1995) 13-33.

[3] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, 1985.

[4] C. J. Colbourn, W. De Launey, Difference Matrices, in: C.J. Colbourn, J.H. Dinitz eds., The CRC Handbook of Combinatorial Designs, CRC Press, 1996, 287-297.

[5] A.B. Evans, Orthomorphism Graphs of Groups, Lecture notes in mathematics 1535, (Springer-Verlag, Berlin-Heidelberg, 1992).

[6] A. B. Evans, Maximal sets of MOLS, in: C.J. Colbourn, J.H. Dinitz eds., The CRC Handbook of Combinatorial Designs, CRC Press, 1996, 368-388.

[7] D. Jungnickel, G. Grams, Maximal difference matrices of order ≤ 10, Discrete Math. 58, no. 2, (1986) 199-203.

[8] T.G. Ostrom, Replaceable nets, net collineations and net extensions, Canad. J. Math. 18, (1966) 666-672.

[9] K.A.S. Quinn, A note on difference matrices and orthomorphisms over non-abelian groups, Ars Combinatoria, to appear.

[10] R. Roth and M. Peters, Four pairwise orthogonal latin squares of order 24, J. Combinatorial Theory (A), 44 (1987), 152-155.

[11] R. M. Wilson, private communication, September 1998.