AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **33** (2005), Pages 109–123

Critical sets in orthogonal arrays with 7 and 9 levels

Rita SahaRay

Stat-Math Unit, Indian Statistical Institute
203 B. T. Road, Kolkata-700 108
India
rita@isical.ac.in

Avishek Adhikari

Applied Statistics Unit, Indian Statistical Institute
203 B. T. Road, Kolkata-700 108
India
avishek_r@isical.ac.in

Jennifer Seberry

Center for Computer Security Research, SITACS
University of Wollongong, NSW 2522
Australia
jennifer_seberry@uow.edu.au

Abstract

To date very few results are known on the critical sets for a set of Mutually Orthogonal Latin Squares(MOLS). In this paper, we consider Orthogonal Array $OA(n^2, k+2, n, 2)$ constructed from k mutually orthogonal cyclic latin squares of order n and obtain bounds on the possible sizes of the minimal critical sets. In particular, for $n = 7$ we exhibit a critical set, thereby improving the bound reported in Keedwell (1997). The problem is also addressed for $n = 9$ and a critical set is also presented.

1 Introduction

A number of authors have studied critical sets which consist of the minimum amount of information needed to recreate combinatorial structures uniquely. This research has been motivated by studies of secret sharing schemes by Cooper, Donovan and Seberry [4], Chaudhry et al. [2, 3] key distribution schemes by Merkel [15], data compression and defence against denial of service attacks and some problems in the design of experiments. Results on critical sets for latin squares which have a number of applications in both agriculture and cryptology have appeared in papers by Nelder

[16], Smetaniuk [17], Curran and Van Rees [7], Cooper, Donovan and Seberry [5], Gower [12], Donovan and Cooper [9] and Donovan and Howse [10]. To date, very few results on critical sets for a set of two or more pairwise orthogonal latin squares are known. The only work known to the authors is that of Keedwell [13] which gives a lower bound of the size of the minimal critical set for a set of k pairwise orthogonal latin squares of order n. This lower bound is also shown to be attainable for $n = 3$, 4 and 5 and an upper bound, only, is obtained for $n = 4$ and 7. In the present paper we consider Orthogonal Array $OA(n^2, k+2, n, 2)$ denoted hereafter by simply OA, constructed from k mutually orthogonal latin squares and obtain bounds of the size of the critical sets. As it is well known that the existence of an orthogonal array OA is equivalent to the existence of Mutually Orthogonal Latin Squares (MOLS), there is a close connection between C_{OA}, the size of a critical set for an OA and c_l, the size of a critical set for a latin square of order n. There is not a lot known about the critical sets for latin squares in general. However, a class of critical sets is known for a *back circulant* latin square which is a particular latin square having the initial row in the standard form and subsequent rows are formed by translating the previous row one element to the left. Starting with a back circulant latin square L_1 of order n, for a set S of $k, k > 2$ mutually orthogonal cyclic latin squares Keedwell [13] showed that the size of a minimal critical set for $n = 7$ is at most $h + 15 + 6(k-3)$ where h is the cardinality of the minimum number of cells required to complete L_1 uniquely as a member of S. In the present paper, in section 3, for $n = 7$ we exhibit a critical set of size $h + 13 + 6(k-3)$ for S or equivalently for $OA(49, k+2, 7, 2)$. Thus for $n = 7$ the upper bound given in Keedwell [13] is reduced by 2 and we conjecture that this bound cannot be further improved. In section 4, we consider the case of $n = 9$ and exhibit a critical set for L_2, where L_2 is a cyclic orthogonal mate of the back circulant latin square L_1 and all of its rows starting from the second row are formed by translating the previous row 2 elements to the left. An upper bound for the critical set for the corresponding OA constructed from $S = \{L_1, L_2\}$ is also suggested. The critical set produced in each case is indicated by bold font in this paper.

Before discussing the main results some background information is needed which is given in the next section.

2 Preliminary Definitions and Notations

In this section, we draw the readers' attention to the definitions and known results on critical sets for latin squares of order n which will be used hereafter to derive the main results.

A latin square L of order n is an $n \times n$ array with entries chosen from a set N of size n such that each element of N occurs precisely once in each row and in each column. In what follows N is assumed to be $\{1, 2, \cdots, n\}$. For convenience a latin square L of order n is sometimes represented by a set of ordered triplets $\{(i, j, k) |$ element k occurs in the position (i, j), $i, j, k \in N\}$.

A *partial latin square* P of order n is an $n \times n$ array with entries chosen from N

such that each element of N occurs at most once in each row and in each column of P. Then $|P|$ is said to be the size of the partial latin square and the set of positions $S_P = \{(i,j)|\ (i,j,k) \in P,\ \exists\ k \in N\}$ is said to determine the shape of P. Let P and P' be two partial latin squares of the same order, with the same size and shape. Then P and P' are said to be *mutually balanced* if the entries in each row (and column) of P are the same as those in the corresponding row (and column) of P'. They are said to be *disjoint* if no position in P' contains the same entry as the corresponding position in P.

A *latin interchange* (also referred to as *latin trade*, cf. Keedwell [14]) I is a partial latin square for which there exists another partial latin square I' of the same order, size and shape with the property that I and I' are disjoint and mutually balanced.

A *Uniquely Completable set* (UC set) U of triplets is such that there is only one latin square L of order n which has element k in position (i,j), for each $(i,j,k) \in U$.

A set C is said to be a *critical set* if it is a UC set and omitting any element from C destroys this property. A *minimal critical set* is a critical set of the smallest possible size.

A UC set of cell entries for a set of MOLS is called *strong* if the cell entries in the entire set of squares can be successively filled by a sequence of adjunctions of cell entries to individual squares of the set each of which is forced. A UC set which is *not strong* is called *weak*.

A $k \times m$ matrix A with entries from a set of s (≥ 2) elements is called an orthogonal array of size m, k constraints, s levels, strength t, and index λ if any $t \times m$ submatrix of A contains all possible $t \times 1$ column vectors with the same frequency λ. Such an array is denoted by $OA(m,k,s,t)$. In the present paper we deal with the orthogonal arrays constructed from a set of MOLS only. To this end we observe that if $M = \{M_1, M_2, ..., M_k\}$ is a set of k MOLS of order n on the symbols $\{1,2,\ldots,n\}$ where the entries of M_t are denoted by $m^t_{ij}, i,j = 1,2,\ldots,n$, the following is an $OA(n^2, k+2, n, 2)$.

$$\begin{array}{cccccccccccc}
1 & 1 & .... & 1 & 2 & 2 & .... & 2 & ..... & n & n & .... & n \\
1 & 2 & .... & n & 1 & 2 & .... & n & ..... & 1 & 2 & .... & n \\
m^1_{11} & m^1_{12} & .... & m^1_{1n} & m^1_{21} & m^1_{22} & .... & m^1_{2n} & ..... & m^1_{n1} & m^1_{n2} & .... & m^1_{nn} \\
m^2_{11} & m^2_{12} & .... & m^2_{1n} & m^2_{21} & m^2_{22} & .... & m^2_{2n} & ..... & m^2_{n1} & m^2_{n2} & .... & m^2_{nn} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\
m^k_{11} & m^k_{12} & .... & m^k_{1n} & m^k_{21} & m^k_{22} & .... & m^k_{2n} & ..... & m^k_{n1} & m^k_{n2} & .... & m^k_{nn}
\end{array}$$

See Abel [1] for more details.

While there are $n-1$ mutually orthogonal latin squares of every order n, a prime or prime power, not every latin square of prime or prime power order has $n-1$ mutually orthogonal mates or even necessarily one orthogonal mate. So in the following, we start with a back circulant latin square L_1 of order n, n odd and concentrate on a set of mutually orthogonal mates of L_1. Furthermore, in the present context of shared security system used in financial institutions, in communication network or defence, where a set of mutually orthogonal latin squares is taken to be the secret key or password and therefore kept private, it is not legitimate to

assume the latin squares are in the semi standard form to start with, because this would release complete information about the first row. So in this paper, we deal with MOLS having its initial row as any permutation of the symbols $\{1, 2, \ldots, n\}$ viz. $\{p_1, p_2, \ldots, p_n\}$ and try to identify a minimal critical set for the corresponding orthogonal array. However, for simplicity in notations, without loss of generality, we refer to p_j as j in our subsequent discussion. It is to be noted that all mathematical operations discussed in this paper are taken modulo n, however, we use symbol n instead of 0.

Definition 2.1 *We say a latin square L_t of order n, is a cyclic latin square if its (i, j)th cell contains the entry $1 + (i-1)t + (j-1)$, $t = 1, 2, \ldots, n-1$, $i, j \in N$.*

Definition 2.2 *A critical set of size C_{OA}, for an orthogonal array $OA(n^2, k+2, n, 2)$ is a set $C = \{(i, j, \ell) \mid i \in \{3, 4, ..., k+2\};\ j \in \{1, 2, ..., n^2\};\ \ell \in \{1, 2, ..., n\}\}$ such that:*
(i) OA is the only Orthogonal Array of the format given above which has element ℓ in the position (i, j) for each $(i, j, \ell) \in C$.
(ii) No proper subset of C satisfies (i).
A minimal critical set (mcs) of an OA is a critical set of minimum cardinality.

We now quote the results on critical sets for latin squares of order n which will be used to obtain a minimal critical set for the corresponding OA.

The next Lemma is due to Cooper, Donovan and Seberry [4].

Lemma 2.3 *Let $n = 2m + 1$, for some positive integer m and*

$$\begin{aligned} C &= \{(i, j, i+j-1) \mid i = 1, \ldots, (n-1)/2 \text{ and } j = 1, \ldots, (n-1)/2 - i + 1\} \\ &\cup \{(i, j, i+j-1) \mid i = (n+1)/2 + 1, \ldots, n, \text{ and } j = (n+3)/2 - i, \ldots, n\} \end{aligned}$$

Then C is a critical set for a back circulant latin square of order n.

Definition 2.4 *Two latin squares L and M of order n are said to be isotopic or equivalent if there exists an ordered triplet (α, β, γ) of permutations such that α, β, γ map the rows, columns and the elements respectively of L onto M. That is, if $(i, j, k) \in L$, then $(i\alpha, j\beta, k\gamma) \in M$.*
Along the same lines two critical sets A and B of the same order are said to be isotopic if for all $(x, y, z) \in A$, $(x\alpha, y\beta, z\gamma) \in B$.

The following result on isotopism of critical sets for a latin square is quoted from Donovan, Cooper, Nott and Seberry [8].

Theorem 2.5 *Let L be a latin square of order n with a critical set A. Let (α, β, γ) be an isotopism from the critical set A onto $\bar{A}$. Then $\bar{A}$ is a critical set in a latin square $\bar{L}$ of order n and $\bar{L}$ is isotopic to L.*

Definition 2.6 *In an $n \times n$ array, a transversal is a collection of n cells $\{(i_1, j_1), \ldots, (i_n, j_n)\}$ where $(i_1, \ldots, i_n)$ and $(j_1, \ldots, j_n)$ represent permutations of the numbers $\{1, 2, ...n\}$.*

Now we define two special transversals pertinent to our discussion in this paper.

Definition 2.7 *In an $n \times n$ array, for $i \in N$, the transversal $\{(1,i),(2,i-1),\ldots,(n,i-n+1)\}$ is termed as the ith reverse transversal denoted by T_i.*

Definition 2.8 *In an $n \times n$ array, for $i \in N$, the transversal $\{(1,i),(2,i-2),\ldots,(n,i-2n+2)\}$ is termed as one step back reverse transversal denoted by ${}_bT_i$.*

We denote the *ith* row and the *jth* column of any $n \times n$ array by R_i and C_j respectively.

Remark 1 : It is evident that in the back circulant latin square L_1, the ith symbol occurs in the i th reverse transversal. Also note that any L_t, $t \in \{2,\ldots,n-1\}$ with t and n coprime, has its first row in the standard form and subsequent rows are formed by translating the previous row t elements to the left.

3 Critical sets for Mutually Orthogonal Latin Squares and Orthogonal Arrays with 7 levels

In view of the close connection between mutually orthogonal latin squares and orthogonal arrays discussed in the previous section the following lemma is immediate.

Lemma 3.1 *If the number of elements in the minimal critical set for each $M_t, t = 1,2,...k$ in a set of k MOLS is at most c_ℓ, the set of mutually orthogonal latin squares of order n can be completed from kc_ℓ elements. Hence the minimal critical set for the $OA(n^2,k+2,n,2)$ or equivalently a set of k MOLS of order n satisfies*

$$C_{OA} \leq kc_\ell.$$

The only research work known to the authors improving the above upper bound is due to Keedwell [13]. He carried out a preliminary investigation on the size of a minimal critical set for a set of mutually orthogonal latin squares of small orders. For the sake of completeness, we refer below to two main theorems of Keedwell [13] in this connection.

Theorem 3.2 *Let M be a set of k pairwise orthogonal $n \times n$ latin squares $M_1, M_2, \ldots, M_k$. For each i, $i = 1,2,\ldots,k$, let h_i be the cardinality of the smallest number of cells of the latin square M_i that enable it to be completed uniquely as a member of M when the entries in those cells are specified. Let h, called the smallest UC cardinality, be the smallest of the h_i's. Then the size of the minimal critical set for M is not less than $h + (k-1)(n-1)$.*

Keedwell [13] showed by actual construction that for a complete set of $n-1$ or for a set of k, $k < n-1$, pairwise orthogonal latin squares of order n the lower bound given in the above theorem is attainable for n =3, 4 and 5. However, he claimed that for $n = 7$ this lower bound is no longer attainable and through construction of a UC set he proved the following result.

Theorem 3.3 *For a set of k, $3 < k < 7$, pairwise orthogonal latin squares of order 7, the size of the minimal critical set is at most $h + 15 + 6(k-3)$ where h is defined as in Theorem 3.2. For sets of 2 and 3 cyclic pairwise orthogonal latin squares, the sizes of a minimal critical set are at most $h + 8$ and $h + 15$ respectively.*

Remark 2: Even though the statement of the above theorem is quite general in the proof Keedwell dealt only with the cyclic latin squares L_t, $t = 1, 2, \ldots, 6$ as defined above. Moreover he started with the sequence L_1, L_2 and L_4 and showed that whatever be the fourth member the theorem holds. In a subsequent theorem he showed that uniquely completable sets of 7 and 6 cells respectively exist by means of which L_4 and L_3 can be completed to members of the triad L_1, L_2, L_4 or quadruple L_1, L_2, L_4, L_3 of orthogonal latin squares of order 7.

Remark 3: We note that once L_1 and L_2 are chosen in order, any latin square orthogonal to both of these is necessarily a cyclic one viz. L_t, $t = 3, 4, 5, 6$. However any orthogonal mate of L_1 is not necessarily a cyclic one. So along the lines of Keedwell we confine ourselves to the set of cyclic mutually orthogonal latin squares only, and the first two members are chosen, in order, as L_1 and L_2. Moreover, the third member is chosen to be L_4, to emphasize the redundancy of the elements in the chosen UC set of Keedwell.

In what follows, through construction of critical sets, we establish that for $n = 7$ the upper bound given in Keedwell [13] can be further reduced by 2. To this end, we proceed through the following lemmas.

Lemma 3.4 *For a set $S = \{L_1, L_2\}$ of cyclic mutually orthogonal latin squares of order 7, the size of the minimal critical set is at most $h + 7$ where h is the smallest UC cardinality.*

Proof: The proof is by construction. We assume that guided by Lemma 2.3, L_1 may be completed uniquely from a set of 12 elements given in Fig. 1. We now complete L_2 using its orthogonality to L_1 from the 7 specified entries as shown in Fig. 2 below.

1	2	3				
2	3					
3						
						4
					4	5
				4	5	6

Fig. 1

1		3				
3		5				
				4		
			7		2	

Fig. 2

Towards unique completion of L_2 from the set C where,

$$C = \{(1,1,1), (1,3,3), (2,1,3), (2,3,5), (4,5,4), (6,4,7), (6,6,2)\}, \tag{3.1}$$

we argue as follows :

Step 1: First note that the ith symbol occurs in the ith reverse transversal T_i in L_1 forcing the symbols along T_i of L_2 to be all distinct. Thus, the symbol 3 in C_7 can

occur in one of the cells (5,7) or (6,7) or (7,7). But 3 in (5,7) will force the placement of 3 in C_5 at (3,5) leading no choice for 3 left in C_4. Similarly choice of 3 in (7,7) will determine the placement of 3 in C_5, C_4 and C_2 in order uniquely, leading no place left for 3 in C_6. Thus 3 is uniquely placed in (6,7) forcing unique placement of 3 in C_6, C_5, C_4, C_2 sequentially.

Step 2: Now the only choice for 5 along T_1 is (5,4) or (7,2). Placement of 5 in (7,2) will determine the position of 5 uniquely in C_4, C_1, C_6 sequentially, and hence determine the symbols along T_1 uniquely. Consequently all the possible placements of 1 in C_4 will place 1 sequentially in C_6 and C_5, finally leading to a contradiction in the placement of 1 either in C_2 or C_7. Thus 5 along T_1 has to be in (5,4).

Step 3: Now 7 in T_1 can be in (2,7) or (7,2). If it is in (2,7), occurrences of 2 and 6 are fixed along T_1. Now 2 in C_4 can be placed at two places viz. (2,4) and (3,4). Placement of 2 in C_4 at (2,4) determines 2 in C_1, C_5, C_7 and C_3 sequentially. Then the possibilities remaining for 7 in C_3 are (3,3) or (5,3). But 7 in C_3 at (5,3) leads to a contradiction in the placement of 7 in C_1 after determining, in order, its position in C_5, C_6 and C_2 in order. Similarly 7 in (3,3) forces 7 in C_2 at (1,2) leaving no place for 7 in C_5. Thus 2 in C_4 at (2,4) is not possible. But 2 in C_4 at (3,4) is also not possible since then 2 in C_1 should be at (5,1) leaving no place for 2 in C_3. Hence 7 along T_1 should be at (7,2) uniquely determining T_1.

Step 4: Now 2 can be assigned to (3,4) or (7,4) in C_4, but placement of 2 at (3,4) leads to two possible choices of 2 in C_3 which leads to a contradiction in the placement of 2 either in C_1 or sequentially in C_5 and C_2 respectively. So 2 has to be placed in C_4 at (7,4).

Step 5: Placement of 2 is now uniquely determined in C_1, C_2, C_3, C_5 sequentially.

Step 6: Placement of 1 in C_4 can now be at (2,4) or (3,4). If it is in (2,4), possible allocations of 1 in C_5 are at (5,5) or (6,5). But placement of 1 in (5,5) leads to a contradiction in the placement of 1 in C_3 whereas placement of 1 in (6,5) uniquely determines 1 in C_6 at (4,6), in R_3 at (3,2), in C_3 at (5,3). Then 5 is uniquely placed in C_5 at (1,5), leading to a contradiction in the placement of 5 in C_6. Thus 1 in C_4 must be in (3,4).

Step 7: Now 1 in C_5 can be in (5,5) or (6,5). But (5,5,1) leads to a contradiction in placement of 1 in C_3. Hence (6,5) should contain 1. Then the positions of 1 in C_2, C_7, C_3, C_6 are determined uniquely. Now the positions of 5 is determined uniquely in C_2, C_5, C_1, C_6, C_7 sequentially. Hence L_2 can be filled uniquely as follows.

L_2 :

1	2	**3**	4	5	6	7
3	4	**5**	6	7	1	2
5	6	7	1	2	3	4
7	1	2	3	**4**	5	6
2	3	4	5	6	7	1
4	5	6	**7**	1	**2**	3
6	7	1	2	3	4	5

(3.2)

To show that the set C given in (3.1) is a critical set, we have to verify that no proper subset can be completed to a unique latin square orthogonal to L_1. It suffices

to verify that deleting one element at a time from C there exist more than one latin square orthogonal to L_1. To this end, for each deletion of a single element $(i, j, k) \in C$ we exhibit below one more orthogonal latin square different from L_2 denoted by L_2^{ij}. The notation $r \leftrightarrow s$ denotes that the new latin square is obtained by interchanging the symbols r and s in L_2.

6	2	**3**	4	5	1	7
3	4	**5**	1	7	6	2
5	1	7	6	2	3	4
7	6	2	3	**4**	5	1
2	3	4	5	1	7	6
4	5	1	**7**	6	**2**	3
1	7	6	2	3	4	5

$L_2^{11};\ (1 \leftrightarrow 6)$

1	2	6	4	5	3	7
3	7	**5**	1	2	4	6
4	1	2	6	3	7	5
6	3	7	5	**4**	1	2
7	4	1	2	6	5	3
5	6	3	**7**	1	**2**	4
2	5	4	3	7	6	1

L_2^{13}

1	2	**3**	4	5	6	7
6	7	**5**	1	2	4	3
4	1	2	3	6	7	5
3	6	7	5	**4**	1	2
7	4	1	2	3	5	6
5	3	6	**7**	1	**2**	4
2	5	4	6	7	3	1

L_2^{21}

1	2	**3**	4	6	5	7
3	4	6	5	7	1	2
6	5	7	1	2	3	4
7	1	2	3	**4**	6	5
2	3	4	6	5	7	1
4	6	5	**7**	1	**2**	3
5	7	1	2	3	4	6

$L_2^{23};\ 5 \leftrightarrow 6$

1	2	**3**	4	5	7	6
3	4	**5**	6	2	1	7
7	1	2	3	4	6	5
6	7	1	5	3	4	2
4	6	7	2	1	5	3
5	3	4	**7**	6	**2**	1
2	5	6	1	7	3	4

L_2^{45}

1	2	**3**	4	5	7	6
3	4	**5**	7	6	1	2
5	7	6	1	2	3	4
6	1	2	3	**4**	5	7
2	3	4	5	7	6	1
4	5	7	6	1	**2**	3
7	6	1	2	3	4	5

$L_2^{64};\ 6 \leftrightarrow 7$

1	2	3	4	5	6	7
3	7	5	6	1	4	2
4	6	1	2	3	7	5
2	3	7	5	4	1	6
7	4	2	3	6	5	1
5	1	6	7	2	3	4
6	5	4	1	7	2	3

L_2^{66}

This ends the proof of Lemma 3.4. □

Remark 4: It is interesting to note that for a completion as a latin square L_2 requires at least 8 cell entries to be specified (cf. Cooper, McDonough and Mavron [6] and Fu, Fu and Rodger [11]) where as the condition of orthogonality reduces the size of the critical set to 7. It is also to be noted that that here the critical set C is weakly completable set.

Conjecture: A second latin square mutually orthogonal to a back circulant latin square cannot be completed uniquely, using orthogonality, from a set of 6 or fewer elements .

Lemma 3.5 *For a set $S = \{L_1, L_2, L_4\}$ of cyclic mutually orthogonal latin squares of order 7, the size of the minimal critical set is at most $h + 13$, where h is the smallest UC cardinality.*

Proof: The proof is by construction. Using orthogonality to both L_1 and L_2 we show that a third mutually orthogonal latin square L_4 can be completed from the six specified entries given in Figure 3.

1						
		7				
	3					
			6			2
					5	

Fig. 3

To be precise, we will show here that

$$C = \{(1,1,1),(2,3,7),(3,2,3),(5,4,6),(5,7,2),(6,6,5)\} \tag{3.3}$$

is a critical set for L_4.

Note that in L_2, ${}_bT_i$ contains the ith symbol for $i = 1, 2, \ldots, 7$. Hence orthogonality of L_4 to both L_1 and L_2 demands that in L_4 all the symbols along the transversals ${}_bT_i$, as well as T_i, should be different. We start with placement of 1 along T_4 in L_4.

Step 1: 1 in T_4 can only occur in (7,5) and hence T_4 is determined uniquely. Now along T_3, 1 can be possible only at (2,2) or (5,6) or (4,7). If 1 is placed at (2,2), then the only possibility for 1 in C_6 is at (4,6) and in C_7 at (6,7) which lead to a contradiction to the orthogonality of L_4 and L_2 along ${}_bT_3$ in the cell positions (6,7) and (7,5). Again 1 in (4,7) leaves no place for 1 in C_6. Thus 1 has to occur along T_3 in (5,6).

Step 2: Now 1 is uniquely determined in C_7, C_3, C_4, C_2 sequentially at (3,7), (4,3), (2,4) and (6,2) respectively.

Step 3: Now 6 in C_2 can be at (1,2) or (2,2). But 6 in (1,2) leads to placement of 6 in C_3 at (7,3) leaving no place for 6 in C_6. So 6 in C_2 should be at (2,2).

Step 4: Now 6 is determined uniquely in C_3, C_5, C_6 and C_7 at places (7,3), (3,5), (1,6) and (6,7) uniquely.

Step 5: Now 7 can occur in C_7 at (1,7) or (4,7). But if it is in (4,7) then 7 has no place in C_5. So 7 in C_7 is at (1,7).

Step 6: Now 7 in C_1 can occur in (6,1) or (5,1). But if it is in (5,1) then no place is left for 7 in C_2. So place 7 in (6,1).

Step 7: Now place 7 uniquely in C_2, C_4, C_5, C_6 sequentially.

Step 8: Now the possible places for 2 along T_3 are (1,3) or (3,1). But if it is placed in (1,3) then 2 is uniquely determined in C_1 at (7,1) leaving no place for 2 in C_2. Hence 2 can occur along T_3 only at (3,1), determining 2 uniquely, in order, in C_3, C_4, C_2, C_5, C_6.

Step 9: Now complete C_4, T_6, R_7, R_6, C_6 and C_5 sequentially.

It is now easy to verify that L_4 can be completed as follows.

L_4 :

1	2	3	4	5	6	7
5	6	**7**	1	2	3	4
2	**3**	4	5	6	7	1
6	7	1	2	3	4	5
3	4	5	**6**	7	1	**2**
7	1	2	3	4	**5**	6
4	5	6	7	1	2	3

(3.4)

This ends the proof of Lemma 3.5.

□

Remark 5: Clearly a latin square of order 7 cannot be completed uniquely from a set of 5 or fewer elements. Hence the UC set for L_4 turns out to be critical.

Remark 6: The above theorem demonstrates that there is a critical set of 13 entries as opposed to the UC set of 15 entries as given in Keedwell [13] to complete L_2 and L_4.

Now in view of Lemma 3.4 and Lemma 3.5 we claim the following theorem.

Theorem 3.6 *For a set of k, $3 < k < 7$, pairwise cyclic orthogonal latin squares of order 7 starting with L_1 and L_2 in order the size of the minimal critical set is at most $h + 13 + 6(k-3)$ where h is the smallest UC cardinality.*

Proof: It has been noted earlier that L_1 and L_2 chosen in order, can be extended uniquely to a complete set of 6 MOLS of order 7 having members as L_3, L_4, L_5, L_6 chosen in any sequence. A general representation of L_t is given below where $\{p_{t1}, \ldots, p_{t7}\}$ stands for any permutation of $\{1, 2, \ldots, n\}$ for t=3, 4, 5, 6.

L_3 :

p_{31}	p_{32}	p_{33}	p_{34}	p_{35}	p_{36}	p_{37}
p_{34}	p_{35}	p_{36}	p_{37}	p_{31}	p_{32}	p_{33}
p_{37}	p_{31}	p_{32}	p_{33}	p_{34}	p_{35}	p_{36}
p_{33}	p_{34}	p_{35}	p_{36}	p_{37}	p_{31}	p_{32}
p_{36}	p_{37}	p_{31}	p_{32}	p_{33}	p_{34}	p_{35}
p_{32}	p_{33}	p_{34}	p_{35}	p_{36}	p_{37}	p_{31}
p_{35}	p_{36}	p_{37}	p_{31}	p_{32}	p_{33}	p_{34}

L_4 :

p_{41}	p_{42}	p_{43}	p_{44}	p_{45}	p_{46}	p_{47}
p_{45}	p_{46}	p_{47}	p_{41}	p_{42}	p_{43}	p_{44}
p_{42}	p_{43}	p_{44}	p_{45}	p_{46}	p_{47}	p_{41}
p_{46}	p_{47}	p_{41}	p_{42}	p_{43}	p_{44}	p_{45}
p_{43}	p_{44}	p_{45}	p_{46}	p_{47}	p_{41}	p_{42}
p_{47}	p_{41}	p_{42}	p_{43}	p_{44}	p_{45}	p_{46}
p_{44}	p_{45}	p_{46}	p_{47}	p_{41}	p_{42}	p_{43}

L_5 :

p_{51}	p_{52}	p_{53}	p_{54}	p_{55}	p_{56}	p_{57}
p_{56}	p_{57}	p_{51}	p_{52}	p_{53}	p_{54}	p_{55}
p_{54}	p_{55}	p_{56}	p_{57}	p_{51}	p_{52}	p_{53}
p_{52}	p_{53}	p_{54}	p_{55}	p_{56}	p_{57}	p_{51}
p_{57}	p_{51}	p_{52}	p_{53}	p_{54}	p_{55}	p_{56}
p_{55}	p_{56}	p_{57}	p_{51}	p_{52}	p_{53}	p_{54}
p_{53}	p_{54}	p_{55}	p_{56}	p_{57}	p_{51}	p_{52}

L_6 :

p_{61}	p_{62}	p_{63}	p_{64}	p_{65}	p_{66}	p_{67}
p_{67}	p_{61}	p_{62}	p_{63}	p_{64}	p_{65}	p_{66}
p_{66}	p_{67}	p_{61}	p_{62}	p_{63}	p_{64}	p_{65}
p_{65}	p_{66}	p_{67}	p_{61}	p_{62}	p_{63}	p_{64}
p_{64}	p_{65}	p_{66}	p_{67}	p_{61}	p_{62}	p_{63}
p_{63}	p_{64}	p_{65}	p_{66}	p_{67}	p_{61}	p_{62}
p_{62}	p_{63}	p_{64}	p_{65}	p_{66}	p_{67}	p_{61}

Recall that throughout this paper for convenience we have treated the entry p_{tk} as k only. Moreover to form a set of MOLS, the extension of L_1 and L_2 to

L_3, L_4, L_5 and L_6 is unique in the sense that the symbol p_{ti} occurs along the transversal $\{(1,i), (2,i-t), (3,i-2t), \ldots, (7,i-6t)\}$ only. Now consider $L_t, t = 3,5,6$ which is isotopic to L_4. Now because of the unique extension pointed out above, clearly the corresponding isotopism applied on the critical set of size 6 for L_4 given in Fig. 3 leads to a completion unique to L_t, and no other latin square revealing the identities of p_{tk}'s. Moreover, as no latin square of order 7 can be completed from a set having fewer than 6 elements, the isotopic of the critical set for L_4 turns out to be a critical set for L_t, $t = 3,5,6$. Hence the theorem follows. □

Remark 7: Any cyclic latin square L_t, $t = 1, \ldots 6$ can be permuted to L_1. So, without loss of generality starting with L_1 we try to find a critical set for any other $L_t, t \neq 2$. As $L_t, t \neq 2$ is isotopic to L_2, the corresponding isotopism is applied to the critical set for L_2 and it has been observed that this set can be completed not only to L_t, but also to some other latin squares, as any orthogonal mate of L_1 is not necessarily a cyclic one. But, however, if we restrict ourselves only to cyclic orthogonal mates of L_1, then the corresponding isotopic set turns out to be a critical set for L_t.

Using equivalence of existence of a set of MOLS and OA the next theorem is immediate.

Theorem 3.7 *Consider $OA(49, k+2, 7, 2)$ constructed from the set of k cyclic MOLS of order 7 starting with L_1 and L_2 in order. Then there is a critical set for the $OA(49, k+2, 7, 2)$ satisfying $C_{OA} \leq h + 7 + 6(k-2)$.*

4 Critical sets for Mutually Orthogonal Latin Squares and Orthogonal Arrays with 9 levels

In this section we deal with the set $S = \{L_1, L_2\}$ of two cyclic MOLS of order 9 and identify a critical set for S.

Theorem 4.1 *Let L_1 be the back circulant latin square of order 9 and L_2 be its cyclic orthogonal mate. Then*

$$\begin{aligned} C &= \{(i,j,2i+j-2): \ i = 1,2,\ldots,\frac{9-j}{2}, \quad j = 1,3,5\} \\ &\cup \{(i,j,2i+j-2): \ i = 9,\ldots,9-\frac{j}{2}+1, \quad j = 4,6,\ldots,8\} \end{aligned} \tag{4.1}$$

is a critical set for L_2 as a member of the set of MOLS $S = \{L_1, L_2\}$.

Proof: We first prove the unique completion of L_2 from C. We start with the partial latin square

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

(4.2)

To obtain completion, using the fact that orthogonality of L_2 to L_1 requires all the symbols in L_2 along T_i, besides those in R_i and in C_i, to be different for all $i = 1, 2, \ldots, 9$, we argue as follows:

Step 1: As 7 occurs in T_4, T_5 and T_6 as well as in R_2, R_3 and R_4, there are three possible places for 7 in C_7 viz, (1,7), (5,7) and (6,7). Now 7 in (5,7) determines 7 in C_8 uniquely at (1,8) which leaves no place for 7 in C_6. Similarly 7 in (6,7) determines 7 in C_8 uniquely at (1,8) and in C_6 at (5,6), leaving no place for 7 in C_4. Thus 7 is uniquely determined at (1,7) in C_7.

Step 2: Fill C_8, C_6 and C_4 uniquely in order.

Step 3: Fill R_1 uniquely using the fact that 9 is already on T_2.

Step 4: Using T_6, T_7, T_8 and T_9, C_1 is filled uniquely in R_6, R_7, R_8, R_9 and R_5 sequentially.

Step 5: We use T_7, T_8 and T_9 in order to find C_2 which places 3, 5 and 7 in R_6, R_7 and R_8 respectively.

Step 6: We use T_3, T_4, T_5 in order to find C_2 in R_2, R_3 and R_4 which uniquely places 4, 6 and 8 in the cell positions respectively. The rest of the entries in C_2 can now be determined.

L_2 can now be permuted to L_2' which has the standard form of Cooper, Donovan and Seberry [5] and Smetaniuk [17] where we now have a critical set in the back circulant latin square. This allows us to uniquely complete L_2' and reversing the permutation gives back L_2. It is to be noted that C is a weakly completable set.

Now to prove that the UC set C in (4.2) is a critical set for L_2, we show that for each $(i, j, k) \in C$, there exists a latin trade L_{2t}, $t = 1, 2$ in L_2 satisfying

$$C \bigcap L_{2t} = \{(i, j, k)\}, \quad t = 1, 2.$$

Define

$$C_{20} = \{(i, j, 2i + j - 2) \;\; i = 1, 2, \ldots, \tfrac{9-j}{2}, \;\; j = 1, 3, 5\}$$

and

$$C_{21} = \{(i, j, 2i + j - 2) \;\; i = 9, \ldots, 9 - \tfrac{j}{2} + 1, j = 4, 6, \ldots, 8\}.$$

Clearly, $C = C_{20} \bigcup C_{21}$.

We now observe that taking addition modulo 9, for any $(i,j,k) \in C$, L_2 contains a partial latin square L_{21} of the form

$$\begin{aligned} L_{21} &= \{(i,j,k),(i,j+\alpha,k+\alpha),(i+\alpha,j+\alpha,k),(i+\alpha,j+2\alpha,k+\alpha),\\ &\quad (i+2\alpha,j+2\alpha,k),(i+2\alpha,j,k+\alpha)\}, \end{aligned}$$

which can be replaced by another partial latin square L_{22} of the form

$$\begin{aligned} L_{22} &= \{(i,j,k+\alpha),(i,j+\alpha,k),(i+\alpha,j+\alpha,k+\alpha),(i+\alpha,j+2\alpha,k),\\ &\quad (i+2\alpha,j+2\alpha,k+\alpha),(i+2\alpha,j,k)\}, \end{aligned}$$

yielding a different latin square $\tilde{L_2}$ orthogonal to L_1 where,

$$\alpha = 3 \quad \text{for } (i,j,k) \in C_{20} \setminus \{(4,1,7)\} \cup \{(6,8,9)\}$$

and

$$\alpha = 6 \quad \text{for } (i,j,k) \in C_{21} \setminus \{(6,8,9)\} \cup \{(4,1,7)\}.$$

In order to verify that $\tilde{L_2}$ is also orthogonal to L_1, we recall that in L_1, ith symbol occurs along T_i. Now orthogonality of both L_2 and $\tilde{L_2}$ to L_1 follows from the fact that in L_1, (i,j,k) and $(i+\alpha,j+2\alpha,k+\alpha)$ fall along T_{i+j-1}, similarly $(i,j+\alpha,k+\alpha)$ and $(i+2\alpha,j+2\alpha,k)$ fall along $T_{i+j+\alpha-1}$ and $(i+\alpha,j+\alpha,k)$ and $(i+2\alpha,j,k+\alpha)$ fall along $T_{i+j+2\alpha-1}$ whereas $\tilde{L_2}$ is obtained by interchanging k and $k+\alpha$ along the above mentioned transversals retaining the latin square property.

Thus if we remove any element from C then we can complete the subset to at least two latin squares orthogonal to L_1 each of which has one of the partial latin squares given above. So C with size 18 turns out to be a critical set for L_2, as a member of the set of MOLS $S = \{L_1, L_2\}$. As an illustration, the figures given below present partial latin squares L_{21} and L_{22} for $(1,1,1) \in C$ and L_2 and $\tilde{L_2}$ completed from the subset $C \setminus (1,1,1)$.

1			4					
			1			4		
4						1		

L_{21}

4			1					
			4			1		
1						4		

L_{22}

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

L_2

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

$\tilde{L_2}$

Remark 8: Note that using orthogonality with L_1 the size of the critical set for L_2 can be reduced by 2 from 20, the size of the critical set of smallest size known so far as given in Lemma(2.3) due to Cooper, Donovan and Seberry [5].
The following theorem is now immediate.

Theorem 4.2 *Consider* $OA(81, 4, 9, 2)$ *constructed from the back circulant latin square* L_1 *of order 9, and its cyclic orthogonal mate* L_2. *Then there is a critical set for* $OA(81, 4, 9, 2)$ *constructed from* L_1 *and* L_2 *satisfying* $C_{OA} \leq 38$.

5 Conclusion

The authors are unable to find any latin square of order 9 which is orthogonal to both L_1 and L_2. It turns out that the pattern of the set C given in (4.1) when extended for n, n odd and $n \geq 11$, can be easily shown to be a UC set, thereby providing an upper bound for the size of the minimal critical set for L_2 as $\frac{n^2-1}{4} - 2$, but it is not a critical set for L_2 for any n, $n \geq 11$. Further investigation in connection to obtaining a finer upper bound is on going and will be reported in a subsequent paper.

References

[1] R. Julian R. Abel, Andres E. Brouwer, Charles J. Colburn and Jeffrey H. Dinitz. *Mutually orthogonal latin squares(MOLS)*, in *The CRC Handbook of Combinatorial Designs,* Charles J. Colbourn and Jeffrey H. Dinitz (Eds), CRC Press, Boca Raton, Florida, 1996.

[2] G. R. Chaudhry and J. Seberry. *Secret sharing schemes based on Room squares*, Combinatorics Complexity and Logic, Proceedings of DMTCS'96, Springer-Verlag Singapore, (1996), 158–167.

[3] G. R. Chaudhry, H. Ghodosi and J. Seberry. *Perfect secret sharing schemes from Room squares,* J. Combin. Math. and Combin. Computing 28 (1998), 55–61.

[4] J. Cooper, D. Donovan and J. Seberry. *Secret sharing schemes arising from latin squares*, Bull. ICA 12 (1994), 33–43.

[5] J. Cooper, D. Donovan and J. Seberry. *Latin squares and critical sets of minimal size*, Australas. J. Combin. 4 (1991), 113–120.

[6] J. Cooper, T. P. McDonough and V.C. Mavron, *Critical sets in nets and latin squares*, J. Statist. Plan. Inf. 41 (1994), 241–256.

[7] D. Curran and G. H. J. Van Rees. *Critical sets in latin squares,* in Proc. Eighth Manitoba Conference on Numer. Math and Computing (1978), 165–168.

[8] D. Donovan, J. Cooper, D. J. Nott and J. Seberry, *Latin squares; critical sets and their lower bounds*, Ars Combinatoria 39 (1995), 33–48.

[9] D. Donovan and J Cooper, *Critical sets in back circulant latin squares*, Aequationes Math. 52 (1996), 157–179.

[10] D. Donovan and A. Howse, *Critical sets for latin squares of order 7*, J. Combin. Math. Combin. Computing 28 (1998), 113–123.

[11] Chin-Mei Fu, Hung-Lin Fu and C. A. Rodger, *The minimal size of critical sets in latin squares*, J. Statist. Planning Inference 62 (1997), 333–337.

[12] R. A. H. Gower, *Critical Sets in Latin Squares and their Applications to Minimal Defining Sets of Designs*, PhD Thesis, University of Queensland, Australia, (1995).

[13] A. D. Keedwell, *Critical sets for orthogonal latin squares of small order*, Congr. Numer. 125 (1997), 51–64.

[14] A. D. Keedwell *Critical Sets in Latin Squares and Related Matters: An Update*, Utilitas Mathematica 65 (2004), 97–131.

[15] J. Merkle, *Secrecy, Authentication and Public Key System*, PhD Dissertation, Stanford University, 1979.

[16] J. Nelder, *Critical sets in latin squares*, CSIRO Div. of Math and Stats, Newsletter, 38 (1977).

[17] B. Smetaniuk, *On the minimal critical set of a latin square*, Utilitas Mathematica 16 (1979), 97–100.

(Received 13 Dec 2003)