Latin Squares: Critical Sets and their Lower Bounds

Diane Donovan[1]
Information Security Research Centre, Faculty of Information Technology
Queensland University of Technology
Queensland, Australia 4001

Joan Cooper[2]
Department of Information and Communication Technology
University of Wollongong
Wollongong, Australia 2522

D.J. Nott[3]
Centre for Combinatorics, Mathematics Department
The University of Queensland
Queensland, Australia 4072

Jennifer Seberry[4]
Centre for Computer Security Research, Computer Science Department
University of Wollongong
Wollongong, Australia 2522

Abstract. In this paper we establish a number of new lower bounds on the size of a critical set in a latin square. In order to do this we first give two results which give critical sets for isotopic latin squares and conjugate latin squares. We then use these results to increase the known lower bound for specific classes of critical sets. Finally, we take a detailed look at a number of latin squares of small order. In some cases, we achieve an exact lower bound for the size of the minimal critical set.

1. Introduction.

This paper deals with critical sets in latin squares. A critical set is a partial latin square which is uniquely completable to a latin square and omitting an entry of the partial latin square destroys this property. A formal definition is given later in the introduction. One may refer to Street [9] for a brief survey on the topic.

The problem of recognising critical sets is inherently difficult. Colbourn, Colbourn, and Stinson [2], have shown that deciding whether or not a partial latin square has a unique completion is NP-complete. However, certain classes of critical sets have been identified, and these appear in papers by Cooper, Donovan, and

[1] Supported by ARC Grant no. 92 421420660000 and a Postdoctoral Fellowship at QUT.
[2] Supported by ARC Grant no. S6600306.
[3] Supported by ARC Grant no. A49130102. I wish to thank Prof. A.P. Street for her support.
[4] Supported by Telecom Grant no. 7027 and ARC Grant no. A49130102.

Seberry [1], Curran and van Rees [3], Smetaniuk [7], and Stinson and van Rees [8]. Critical sets have a number of applications in both agriculture and cryptography, see [6]. Of particular interest are critical sets of minimal size. There is only one general class of minimal critical sets known and this was given by Curran and van Rees in [3]. Curran and van Rees obtained a lower bound on the size of the critical set and then showed that a given critical set achieved this bound. In Section 2 we prove a number of new results and then, in Section 3, use these to improve the known lower bounds for specific classes of critical sets. With the aid of the computer, critical sets in latin squares of small orders have been determined. These results appear in papers by Cooper, Donovan, and Seberry [1], Curran and van Rees [3] and Stinson and van Rees [8]. In Section 4, the results from Section 2 and Section 3 are used to verify that under certain conditions some of these sets are in fact minimal critical set.

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 column. For example, let us index the rows and columns of the array by the set $\{0, 1, \ldots, n-1\}$. If we place the integer $i + j \pmod{n}$ in position (i, j) of the array, then the result is a latin square. This particular latin square is termed a back circulant latin square. For convenience, we will sometimes talk of the latin square L as a set of ordered triples $(i, j; k)$ and read this to mean that element k occurs in position (i, j) of the latin square L. A back circulant latin square can be denoted by the set $\{(i, j; i + j) \mid 0 \leq i, j \leq n-1\}$. If L contains an $s \times s$ subarray S and if S is a latin square of order s, then we say that S is a *latin subsquare* of L. Given any latin square one may permute the entries of certain cells with the result being a latin square distinct from the original. So in a sense, one is identifying a path through the latin square, then interchanging the elements in the cells of this path to obtain another latin square. The partial latin square determined by the cells is termed a latin path. A formal definition follows. Let $\mathcal{L}$ be the set of all latin squares of order n where the elements are chosen from a set N of size n. Let L be a latin square in $\mathcal{L}$, and P a partial latin square in L. That is, $P = \{(i, j; k) \mid 1 \leq i, j \leq n \text{ and } k \in N\} \subset L$. We call P a *latin path* in L if

(1) there exists a latin square $L' \in \mathcal{L}$ such that $L \cap L' = \{(i, j; k) \mid (i, j; k) \in L \backslash P\}$, and
(2) for all $Q \subset P$, there exists no $L_i \in \mathcal{L} \backslash L$ such that $L \cap L_i = \{(i, j; k) \mid (i, j; k) \in L \backslash Q\}$.

The order of the set P is said to be the length of the latin path P. The set $P = \{(1,2;2), (1,3;3), (1,4;4), (2,1;2), (2,2;1), (2,4;3), (3,1;3), (3,2;4), (3,3;1), (4,1;4), (4,3;2), (4,4;1)\}$ is a latin path of length 12 in the latin square given on the left in Table 1 below. Latin paths based on two elements, say k and k', of N were termed cycles by Elliot and Gibbons in [4].

Table 1

1	2	3	4		1	2	$\star$	$\star$
2	1	4	3		$\star$	$\star$	4	$\star$
3	4	1	2		$\star$	$\star$	$\star$	2
4	3	2	1		$\star$	3	$\star$	$\star$

Let P be an $n \times n$ array with entries chosen from a set N, of size n, in such a way that each element of N occurs at most once in each row and at most once in each column. Then P may contain a number of empty cells and is said to be a *partial latin square* of order n. We are interested in partial latin squares which satisfy the following properties. A *critical set* in a latin square L of order n, is a set $A = \{(i, j; k) \mid i, j, k \in \{1, \ldots, n\}\}$ such that,

(1) L is the only latin square of order n which has element k in position (i, j) for each $(i, j; k) \in A$;
(2) no proper subset of A satisfies (1).

For example, the latin square representing the elementary abelian 2-group of order 2^2 is given in Table 1 above (on the left). A critical set $\{(1, 1; 1), (1, 2; 2), (2, 3; 4), (3, 4; 2), (4, 2; 3)\}$, for this latin square is given on the right. A *minimal critical set* in a latin square L is a critical set of minimum cardinality. In fact, it will be proven in Lemma 4.9 that the critical set given above is a minimal critical set.

The definition of a critical set can be strengthened as follows. Let L be a latin square, of order n, based on the set N. Let L contain a critical set A. The set A is said to be a *strong critical set* if there exists a set $\{P_1, \ldots, P_m\}$ of $m = n^2 - |A|$ partial latin squares, of order n, which satisfy the following properties:

(1) $A = P_1 \subset P_2 \subset \ldots \subset P_{m-1} \subset P_m \subset L$;
(2) for any i, $2 \leq i \leq m$, given $P_i = P_{i-1} \cup \{(s, t; r)\}$, then the set $P_{i-1} \cup \{(s, t; r')\}$ is not a partial latin square for any $r' \in N \backslash \{r\}$.

Let L be a latin square based on the set N. We define $A - e_x$ to be a critical set in L such that $(i, j; x) \notin A$ for all i, j. That is, the triples of $A - e_x$ are based on the $n - 1$ elements of $N \backslash \{x\}$. Similarly, we can define $A - r_x$ to be a critical set with triples chosen from $n - 1$ rows, distinct from row x, of L; that is, $A - r_x$ contains no triples chosen from row x of L. Likewise, we define $A - c_x$ to be a critical set in which the triples are chosen from $n - 1$ columns, distinct from column x, of L; that is, $A - c_x$ contains no triples chosen from column x of L.

Colbourn, Colbourn, and Stinson [2] characterise critical sets in graph theoretic terms. We will use this characterisation to prove some of the general results in Section 2. Given a partial latin square, P of order n, the *"row-column-element" defect graph* of P is a $3n$ vertex graph with vertex set $\{r(1), \ldots, r(n), c(1), \ldots, c(n), e(1), \ldots, e(n)\}$. The edge $\{r(i), c(j)\}$ is included if the (i, j) entry of the partial latin square is empty. The edge $\{r(i), e(k)\}$ is included if row i does not

contain element k. The edge $\{c(j), e(k)\}$ is included if column j does not contain element k. This defect graph has an edge partition into triangles if and only if the partial latin square has a completion. It follows that the partial latin square has a unique completion if and only if the defect graph has a unique edge-partition into triangles. We will also need the following definition of isomorphic graphs. An isomorphism from a graph G onto a graph H is a one-to-one map ϕ from the vertex set of G onto the vertex set of H with the property that a and b are adjacent vertices in G if and only if $a\phi$ and $b\phi$ are adjacent vertices in H.

Finally, we wish to draw the reader's attention to three results which will be used throughout this paper. The first is Lemma 2.4 of [8] by Stinson and van Rees, the second a variation of this, and the third is Lemma 1.2 of [1] by Cooper, Donovan, and Seberry.

Lemma 1.1. *Let L be a latin square, A a critical set in L, and S a latin subsquare of order 2 in L. Then $A \cap S \geq 1$.*

Lemma 1.2. *Let L be a latin square, A a critical set in L, and P a latin path in L. Then $A \cap P \geq 1$.*

Lemma 1.3. *Let L be a latin square with a critical set A. Let $S = \{S_i \mid i = 1, \ldots, r\}$ be a set of latin subsquares which partition L and let A_i denote a minimal critical set in S_i, $i = 1, \ldots, r$. If $|A_i| = a_i$, for $i = 1, \ldots, r$, then $|A| \geq \sum_{i=1}^{r} a_i$.*

2. Isotopisms, conjugates and complements.

It is useful to discuss latin squares in terms of quasigroups, and use the corresponding algebraic theory to prove results relating to latin squares. One of the algebraic definitions we will require is that of an isotopism. Let $(\mathcal{L}, o)$ and $(\mathcal{M}, \star)$ be two quasigroups. An ordered triple (α, β, γ) of one-to-one mappings α, β, γ of the set $\mathcal{L}$ onto the set $\mathcal{M}$ is called an isotopism of $(\mathcal{L}, o)$ upon $(\mathcal{M}, \star)$, if $(x\alpha) \star (y, \beta) = (x \circ y)\gamma$ for all x, y in $\mathcal{L}$. The quasigroups $(\mathcal{L}, o)$ and $(\mathcal{M}, \star)$ are then said to be isotopic. The corresponding definition for latin squares is: two latin squares L and M are said to be *isotopic* or *equivalent* if there exists an ordered triple (α, β, γ), of permutations, such that α, β, γ map the rows, columns, and elements, respectively, of L onto M. That is, if $(i, j; k) \in L$, then $(i\alpha, j\beta; k\gamma) \in M$. (Two latin squares are isotopic, if one can be transformed onto the other by rearranging rows, rearranging columns, and renaming elements.) Two latin squares (quasigroups) are said to be *isomorphic* if the permutations α, β, γ are equal. (For more details see [5, pages 23 and 124].) Two critical sets A and B are said to be isotopic if there exists an ordered triple of permutations (α, β, γ) which maps the entries of A onto B such that, for all $(x, y; z) \in A$, $(x\alpha, y\beta; z\gamma) \in B$. The sets A and B are isomorphic if the permutations α, β, and γ are equal.

It is relatively easy to see that, once we obtain a critical set in a latin square L, then we can use it to find a critical set in any latin square isotopic to L.

Theorem 2.1. *Let L be a latin square with a critical set A. Let (α, β, γ) be an isotopism from the critical set A onto $\overline{A}$. Then $\overline{A}$ is a critical set in a latin square $\overline{L}$ and $\overline{L}$ is isotopic to L.*

Proof: Consider the defect graphs of A and $\overline{A}$. If (α, β, γ) is an isotopism which maps A onto $\overline{A}$, then the defect graphs of A and $\overline{A}$ are isomorphic. Since A has a unique edge-partition into triangles so does $\overline{A}$. Therefore there is precisely one latin square which contains the partial latin square $\overline{A}$. It follows that this latin square must be the isotopic image of L. It also follows that any subset of $\overline{A}$ must be contained in two latin squares. Hence $\overline{A}$ is a critical set in $\overline{L} = L(\alpha, \beta, \gamma)$. ∎

If A is a minimal critical set in L, then $A(\alpha, \beta, \gamma)$ is a minimal critical set in $L(\alpha, \beta, \gamma)$.

We can obtain a similar result for the conjugates of a latin square. Formally, we let $(\mathcal{L}, \theta)$ be a quasigroup [and L its corresponding latin square]. Then we define five conjugate quasigroups as follows. Let $a\theta b = c$, for $a, b, c \in \mathcal{L}$, $[(a, b; c) \in L]$. We set

(1) $b\theta^* a = c$ in the quasigroup $(\mathcal{L}, \theta^*)$, $[(b, a; c) \in L^*]$;
(2) $c({}^{-1}\theta)b = a$ in the quasigroup $(\mathcal{L}, {}^{-1}\theta)$, $[(c, b; a) \in {}^{-1}L]$;
(3) $a(\theta^{-1})c = b$ in the quasigroup $(\mathcal{L}, \theta^{-1})$, $[(a, c; b) \in L^{-1}]$;
(4) $b\{{}^{-1}(\theta^{-1})\}c = a$ in the quasigroup $(\mathcal{L}, {}^{-1}(\theta^{-1}))$, $[(b, c; a) \in {}^{-1}(L^{-1})]$; and
(5) $c\{({}^{-1}\theta)^{-1}\}a = b$ in the quasigroup $(\mathcal{L}, ({}^{-1}\theta)^{-1})$, $[(c, a; b) \in ({}^{-1}L)^{-1}]$.

Similarly we can define the conjugates of a critical set.

Theorem 2.2. *Let L be a latin square with critical set A. Let A' be a conjugate of A. Then A' is a critical set in the corresponding conjugate L' of L.*

Proof: The proof follows as in Theorem 2.1. ∎

Let $L = \{(i, j; k) \mid i, j, k \in \{1, \ldots, n\}\}$ be a latin square and $A = \{(i, j; k) \mid i, j, k \in \{1, \ldots, n\}\}$ be a critical set in L. It is interesting to ask whether $L \backslash A$ is a critical set. The answer is not necessarily! Take the following critical set in the latin square representing the elementary abelian 2-group of order 2^2.

1	2	3	⋆
2	1	⋆	⋆
3	⋆	1	⋆
⋆	⋆	⋆	⋆

The complement of this critical set is contained in at least two latin squares. Even in the case where the complement is contained in precisely one latin square the set need not be a critical set. To see this we need only consider a critical set A which contains no entries from row q. The complement of this set is not critical.

3. Lower bounds.

In [3, Lemma 2.3] Curran and van Rees showed that, if you take the ordered triples $(x, y; z)$ of a critical set, then the ith component of these triples must cover at least $n-1$ of the values $1, \ldots, n$, thereby showing that the size of the minimal critical set is greater than or equal to $n-1$. We improve on this bound for certain classes of latin squares.

Lemma 3.1. *Let L be a latin square of order $n \geq 4$, with entries chosen from the set N, and let A be a critical set in L. Then $|A| \geq n$.*

Proof: Assume $|A| = n-1$. We know that for the $n-1$ triples $(i, j; k)$ of A the ith components of these triples must cover $n-1$ of the values $1, \ldots, n$. Hence A must be isotopic to a set $A_0 = \{(i, i; x_i) \mid (x_i \in N) \wedge (i = 0, \ldots, n-2)\}$. If n is odd, then A_0 is contained in at least two latin squares, the one denoted by the set $\{(i+j, i-j; i) \mid i, j = 0, \ldots, n-1\}$, (working modulo n) and its conjugate ${}^{-1}L$. If n is even, then A_0 is contained in at least two latin squares; a latin square representing an idempotent quasigroup of order n and its conjugate L^*. (For the existence of an idempotent quasigroup of even order refer to [5, page 195].) Since A_0 is isotopic to A, Theorem 2.1 can be used to prove that $|A| \geq n$. ∎

Lemma 3.2. *Let L be a latin square of order n and let A be a critical set in L,*

(1) *if L contains a subsquare of order $m = 2$ or 3, then $|A| \geq 4m - 4$, and*
(2) *if L contains a subsquare of order $m \geq 4$, then $|A| \geq 4m - 3$.*

Proof: Let L_1 be a latin subsquare of order m in L, and L_2, L_3, L_4, subarrays of size $m \times (n-m)$, $(n-m) \times m$ and $(n-m) \times (n-m)$, respectively. Then L can be partitioned as follows.

L_1	L_2
L_3	L_4

Assume A contains at most $m-2$ triples from the subarray L_2. Then there must be two rows r_1 and r_2 of L_2 such that A does not contain any triples from either of these rows. It now follows that A must be contained in at least two latin squares L and L'. The latin square L' will agree with L everywhere except in the partial rows r_1 and r_2, and here these partial rows will be interchanged. This is a contradiction as A is a critical set. Hence A must contain at least $m-1$ triples from both of the subarrays L_2 and L_3. If $m = 2$ or 3, then A must contain $m-1$ triples from L_1. If $m \geq 4$, then by Lemma 3.1, A must also contain at least m triples from

L_1. Now let L_1 be based on the elements $1, \ldots, m$ of N. Each of these elements occurs once in every row and once in every column of L_4. Therefore, A must also contain at least $m-1$ triples from L_4. Thus, if $m = 2$ or 3, then $|A| \geq 4m-4$, and if $m \geq 4$, then $|A| \geq 4m-3$. ∎

Let L_k be an arbitrary latin square of order k. Then if k is some integer such that $k \leq n/2$, there exists at least one latin square L_n, of order n, such that L_k is a latin subsquare of L_n ([5, page 44]). And so we have the following corollary.

Corollary 3.3. *There exists a latin square L, of order $n \geq 8$, which contains a minimal critical set A of size greater than or equal to*

(1) $2n-3$ *if n is even, and*
(2) $2n-5$ *if n is odd.*

If we restrict ourselves to strong critical sets, then we can obtain the following lower bound.

Lemma 3.4. *Let L be a latin square of order n and A a strong critical set in L. Then*

$$|A| \geq (4n-6)/3.$$

Proof: From the definition of a strong critical set, there exists a triple $(s,t;r) \in L$ such that $(s,t;r) \notin A$ and A contains $n-1$ triples of the form either $(s,j;x_j)$ or $(i,t;x_i)$, for any i,j, and where the x_i's and x_j's are all distinct. Therefore A contains at most $|A|-(n-1)$ triples which do not belong to row s or column t of L. In addition, one of row s or column t must contain less than or equal to $\lfloor |A|/2 \rfloor$ triples which also belong to A. Assume, without loss of generality, that it is row s and so the triples of the form $(s,j;x_j)$ or $(i,t;x_i)$, for any i,j and any $x_i, x_j \in N$, are drawn from at most $\lfloor |A|/2 \rfloor + 1$ columns of L. The set A contains at most $|A|-(n-1)$ triples distinct from those in row s and column t and so A contains triples from at most $\lfloor |A|/2 \rfloor + 1 + |A| - (n-1)$ columns of L. However A must contain triples from at least $n-1$ columns of L. Thus

$$\lfloor |A|/2 \rfloor + 1 + |A| - (n-1) \geq n-1, \text{ and so}$$
$$|A|/2 + 1 + |A| - (n-1) \geq n-1.$$

The result now follows. ∎

If we restrict ourselves to latin squares of order 5, then we have the following lower bound on the size of a critical set.

Lemma 3.5. *Let L be a latin square of order 5 and A a critical set in L. Then* $|A| \geq 6$.

Proof: Assume $|A| = 5$. Up to isotopism, we have four cases to consider. Case 1: The triples of A are based on all the five rows, five columns, and five elements

of L. Case 2: The triples of A are based on five rows, and five columns of L, but only four elements of N. Case 3: The triples of A are based on five rows of L but only four columns, and four elements. Case 4: The triples of A are based on four rows, four columns, and four elements of L.

(1) Here it is easy to see that A is contained in two latin squares, one isotopic to the latin square denoted by the set $\{(i+j, i-j; i) \mid i, j = 0, 1, \ldots, n-1\}$ (working modulo n) and the other isotopic to its conjugate ${}^{-1}L$.

(2) Once again it is easy to see that A will be contained in a latin square isotopic to

0	3	1	2	4
1	2	3	4	0
3	1	4	0	2
2	4	0	1	3
4	0	2	3	1

and its conjugate L^*.

(3) Up to isotopism we have two subcases to consider. They are critical sets isotopic to the set $\{(0,0;0),(1,1;2),(2,2;4),(3,3;1),(4,1;0)\}$ and the set $\{(0,0;0),(1,4;0),(2,2;4),(3,3;1),(4,3;2)\}$. Both of these sets are contained in the back circulant latin square of order 5, as well as the latin square given above.

(4) Up to isotopism we have three subcases to consider. They are critical sets isotopic to the sets $\{(0,2;2),(1,1;2),(1,3;4),(2,3;0),(3,0;3)\}$, $\{(0,0;0),(0,1;1),(2,2;4),(3,3;1),(4,1;0)\}$, $\{(0,0;0),(1,1;2),(1,4;0),(2,2;4),(4,4;3)\}$. These three sets are contained in the back circulant latin square of order 5 and the following three latin squares, respectively.

0	3	2	1	4
1	2	0	4	3
4	1	3	0	2
3	0	4	2	1
2	4	1	3	0

0	1	3	2	4
3	2	1	4	0
1	3	4	0	2
2	4	0	1	3
4	0	2	3	1

0	3	1	2	4
1	2	3	4	0
3	1	4	0	2
2	4	0	3	1
4	0	2	1	3

In each case we have shown that A is contained in at least two latin squares and, thus, obtained a contradiction. So $|A| \geq 6$. ∎

4. Lower bounds for groups.

If A is a critical set in a latin square L representing a group, then Cauchy's Theorem (given below) gives a sharper lower bound.

Cauchy's Theorem. *Let G be a finite group. If a prime p divides the order of the group G, then G has a subgroup of order p.*

Theorem 4.1. *Let L be a latin square representing a finite group of order n, and A a critical set in L. Let p be the smallest prime number which divides n. Let $M = \{M_i \mid i = 0, \ldots, k$ for some positive integer $k\}$, be the set of all latin squares of order p, and B_i be a minimal critical set in M_i, for $i = 0, \ldots, k$. Further, let B_0 be a critical set such that $|B_0| \leq |B_i|$, for all i. Then $|A| \geq (n/p)^2 |B_0|$.*

Proof: It follows from Cauchy's Theorem that the group G, corresponding to the latin square L, has a subgroup of order p. This subgroup, together with it's cosets, may be used to partition L into subsquares of order p. This together with Lemma 1.3 can then be used to complete the proof of the result. ∎

Corollary 4.2. *Let L be a latin square representing a group of even order n. Then the size of a minimal critical set in L is greater than or equal to $n^2/4$.*

Corollary 4.3. *Let L be a latin square representing a group of order n where $n = 3m$, for some m. Then the size of the minimal critical set for L is greater than or equal to $(2n^2)/9$.*

Corollary 4.4. *Let L be a latin square representing a group of order n where $n = 5m$, for some m. Then the size of the minimal critical set for L is greater than or equal to $6n^2/25$.*

Proof: The proof of this result follows directly from Lemma 4.1 and Lemma 3.5. ∎

Once again we turn our attention to the back circulant latin square of odd order. We shall show the existence of a family of latin paths in these latin squares and then go on to give a lower bound on the size of a critical set $A - e_x$. Recall that the triples of a critical set $A - e_x$ are based on the $n - 1$ elements of $N\backslash\{x\}$.

Lemma 4.5. *Let L be a back circulant latin square of odd order $n \geq 5$ and take a transversal $T = \{(s + r, t + r; s + t + 2r) \mid r = 0, \ldots, n - 1\}$, in L, for any fixed s, t. Let $(i, j; \alpha)$ and $(k, \ell; \beta)$ be any two elements of T. Then L contains a latin path S of length $n+3$ such that the elements $(i, j; \alpha)$ and $(k, \ell; \beta)$ belong to S.*

Proof: Fix s and t and let $(i, j; \alpha) \in T$ and $(k, \ell; \beta) \in T$. Since L is a back circulant latin square, there exists a γ such that $(i, \ell; \gamma)$ and $(k, j; \gamma)$ are in L, and that $i + \ell = k + j$. Hence

$$(i_1, j; \beta) \in L, \text{where } i_1 = \beta - j = k + \ell - j = (k + \ell) - (i + j) + i = i + 2(k - i).$$

If we add $2(k - i)$ to i a further $\frac{n-1}{2}$ times, then

$$2(k - i)\left(\frac{n-1}{2} + 1\right) + i = k(n + 1) - ni = k.$$

Similarly,

$$2(\ell - j)\left(\frac{n-1}{2} + 1\right) + j = \ell.$$

So it follows that L contains the set

$$S = \{(i,j;\alpha),(k,j;\gamma),(i_1,j;\beta),(i_1,j_1;\alpha),(i_2,j_1;\beta),(i_2,j_2;\alpha),$$
$$\ldots,(i_{\frac{n-1}{2}},j_{\frac{n-1}{2}-1};\beta),(i_{\frac{n-1}{2}},j_{\frac{n-1}{2}};\alpha),(k,\ell;\beta),(i,\ell;\gamma)\}.$$

Further, if we let that $(L\backslash S) \cup S'$, where

$$S' = \{(i,j;\gamma),(k,j;\beta),(i_1,j;\alpha),(i_1,j_1;\beta),(i_2,j_1;\alpha),(i_2,j_2;\beta),$$
$$\ldots,(i_{\frac{n-1}{2}},j_{\frac{n-1}{2}-1};\alpha),(i_{\frac{n-1}{2}},j_{\frac{n-1}{2}};\beta),(k,\ell;\gamma),(i,\ell;\alpha)\},$$

then $(L\backslash S) \cup S'$, is a latin square distinct from L. The result now follows. ∎

This lemma enables us to construct a set of $\frac{n-1}{2}$ latin paths with certain desirable properties and shall be used to achieve a lower bound on the size of certain critical sets for back circulant latin squares of odd order.

Corollary 4.6. *Let L be a back circulant latin square of odd order $n \geq 5$. Then L contains latin paths S_m, for $m = 1,\ldots,\frac{n-1}{2}$, based on the elements α,β,γ of N, such that*

(1) *for some $i,j \in \{0,\ldots,n-1\}$ $(i,j;\alpha) \notin S_m$, for any m and*
(2) *if $(s,t;\gamma) \in S_p$, for some p, then $(s,t;\gamma) \notin S_q$ for any $q \neq p$.*

Lemma 4.7. *Let L be a back circulant latin square of odd order $n \geq 7$ and $A - e_x$ a critical set in L. Then $|A - e_x| \geq 2(n-1)$.*

Proof: Assume $|A - e_x| = 2(n-1) - 1$ and that for a given $x \in N$ the triple $(i,j;x) \notin (A - e_x)$, for all i,j. There exists a $y \in N$ such that $|\{(i,j;y) \in A - e_x \mid 0 \leq i,j \leq n-1\}| = 1$. By Corollary 4.6 L contains $(n-1)/2$ latin paths based on the elements x, y and z, for some z in N. In addition these latin paths can be chosen so that they do not contain the triple $(k,\ell;y)$ and are distinct in the triples $(i,j;z)$. Therefore, by Lemma 1.2, $A - e_x$ must contain at least $(n-1)/2$ triples based on some element $z \in N$. If we consider the remaining $n-3$ elements of $N\backslash\{x,y,z\}$, then there are $2(n-1) - 1 - 1 - (n-1)/2 = (3n-7)/2$ triples of $A - e_x$ based on these elements. A repetition of the above argument yields a further $1 + (n-1)/2$ triples in $A - e_x$ based on the elements v and w, say, of $N\backslash\{x,y,z\}$. Now there are at most $n-4$ triples in $A - e_x$ based on $n-5$ elements of N. But this is impossible as we have just stated that if an element distinct from x occurs once in $A - e_x$, then there exists an element on which $(n-1)/2$ triples of $A - e_x$ are based. Thus, we have a contradiction and $|A - e_x| \geq 2(n-1)$. ∎

We have now shown that the partial latin square given by Curran and van Rees, in [3], is a minimal critical set for $n = 5$ and a minimal critical set, of the form $A - e_x$, for $n = 7$.

Next, let us consider a latin square L representing an elementary abelian 2-group. But before we begin, we wish to remind the reader of the following property. It will be used extensively throughout this subsection. If we take any two triples in the same row or column or on the same element of L, then there exists a latin subsquare of order 2 containing these two triples. It follows from Lemma 1.1 that any critical set for L must contain at least one triple from each such subsquare.

For the remainder of this paper all rows and columns of L shall be indexed by the numbers $1, \ldots, n$ and let $N = \{1, \ldots, n\}$.

Theorem 4.8. *Let L be a latin square representing the elementary abelian 2-group C_2^v, of order $n = 2^v$. Let $A - r_x$ be a critical set in L. Then*

$$|A - r_x| \geq n(n-1)/2 = 2^{v-1}(2^v - 1).$$

Proof: Without loss of generality, we can assume that $A - r_x$ is a critical set which contains no triples chosen from row 1 of L. For $\ell = 2, \ldots, n$, the rows 1 and ℓ can be partitioned into $n/2$ disjoint latin subsquares of order 2. Since $A - r_x$ is a critical set in L, $A - r_x$ must contain a triple from each of these subsquares. By assumption none of the triples belong to row 1. Hence $A - r_x$ must contain $n/2$ triples from row ℓ. If we let ℓ range over the values $2, \ldots, n$, then $|A - r_x| \geq n(n-1)/2$. ∎

If we let $v = 2$, then $|A - r_x| = 2 \times 3 = 6$. We list below one such critical set in the latin square representing the elementary abelian 2-group of order 2^2.

⋆	⋆	⋆	⋆
⋆	1	4	⋆
3	4	⋆	⋆
⋆	⋆	2	1

If we take the latin square representing the elementary abelian 2-group of order 2^3, as given below, then $|A - r_x| = 2^2 \times (2^3 - 1) = 28$. An example of a critical set of size 28 is given also.

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

⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆
2	⋆	⋆	3	6	⋆	⋆	7
3	4	⋆	⋆	⋆	⋆	5	6
4	⋆	2	⋆	8	⋆	6	⋆
⋆	6	⋆	8	1	⋆	3	⋆
⋆	5	8	7	⋆	1	⋆	⋆
⋆	⋆	5	⋆	⋆	4	1	2
8	⋆	⋆	5	⋆	3	2	⋆

Lemma 4.9. *Let L be the latin square representing the elementary abelian 2-group of order 2^2. Let A be a minimal critical set in L. Then $|A| = 5$.*

Proof: Assume A has order less than 5. Theorem 2.1 and Theorem 4.8 imply that A must contain triples chosen from every row and column of L, and A must

contain at least one triple based on every element of N. Hence A must contain precisely four triples. Without loss of generality, assume that $(1,1;1)$ and $(2,3;4)$ are in A. It now follows that $(3,4;2)$ and $(4,2;3)$ are in A. But there are two latin squares containing A, namely,

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array} \qquad \begin{array}{cccc} 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4. \end{array}$$

This is a contradiction. Thus $A \geq 5$. A critical set of size 5 has been given in Table 1. ∎

The latin square representing the elementary abelian 2-group of order 8 can be partitioned into four latin subsquares, of order 4, isomorphic to the elementary abelian 2-group of order 2^2. Lemma 1.3 implies that any critical set for the latin square representing this group must be of size at least 20. However, this lower bound can be improved on. It is possible to show that the size of the minimal critical set is greater than or equal to 24. To see this we assume the order of the critical set is less than 24 and proceed as follows.

Given Theorem 4.8, we may assume that the critical set contains at least one triple chosen from each row, each column, and based on each element of L. Let L be a latin square representing the elementary abelian 2-group of order 2^3. Let A be a critical set in L.

We will begin by assuming that A contains precisely one triple chosen from row p of L, further that $p = 1$ and $(1,1;1) \in A$. Using a similar argument to that used in the proof of Theorem 4.8, it follows that A must contain at least three triples chosen from each of the remaining rows of L. Consider the rows 1, 2, 3, and 4. They can be partitioned as follows:

$$\begin{array}{cccc|cccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5. \end{array}$$

It follows that A must contain at least two triples chosen from each of the rows 2, 3, and 4 and based on the set of elements $\{5,6,7,8\}$. Recall, A must contain at least five triples from every latin subsquare of order 4. Thus A must also contain four triples selected from rows 2, 3, and 4 and based on the set of elements $\{1,2,3,4\}$. Hence A must contain at least four triples selected from one of the rows 2, 3, or 4. Without loss of generality, assume it is row 2. Now, if we consider rows 1, 3, 5, 7, rows 1, 3, 6, 8, rows 1, 4, 5, 8 and rows 1, 4, 6, 7, we see that A must contain four triples selected from each of the rows 3, 4, or each of the rows 5, 6, or each of the rows 7, 8. Thus, $|A| \geq 1 + 4 + 2.4 + 4.3 = 25$.

Next, we consider the case where A contains at least two triples from each row of L. Assume A contains precisely two triples chosen from row p of L. Without loss of generality, we can assume $p = 1$ and $(1,1;1)$ and $(1,2;2)$ belong to A. It follows that A must contain at least three triples chosen from row 2. Also A must contain at least six triples from each of the pairs of rows 3,4 and rows 5,6 and rows 7,8. Let us assume, without loss of generality, that row 3 contributes two triples to A. This implies that rows 2 and 4 must each contribute four triples to A. Hence, $|A| \geq 2.2 + 2.4 + 2.6 = 24$.

However, if each of the rows distinct from row 1 contribute three triples to A, then $|A| \geq 2 + 7.3 = 23$. Let us investigate this case further. Assume $|A| = 23$ and that there is precisely one row of L which contributes less than three triples to A, precisely one column of L which contributes less than three triples to A and precisely one element of N for which A contains less than three triples based on this element. Let us assume, without loss of generality, that A contains precisely two triples from row 1 and these are $(1,1;1)$ and $(1,2;2)$. Without loss of generality, we may also assume that A contains the triples $(2,4;3)$, $(2,5;6)$ and $(2,7;8)$. And now we have two cases to consider: Case 1: $(3,2;4) \in A$. Case 2: $(3,3;1) \in A$.

Case 1: Since $(3,2;4) \in A$, then $(4,3;2) \in A$. If we look at row 5 together with rows 1 and 2, then it follows that $(5,j_s;k_s) \in A$, for $s = 1,2,3,4$ where $k_1 \in \{3,7\}$, $k_2 \in \{4,8\}$, $k_3 \in \{2,5\}$ and $k_4 \in \{4,7\}$. Note that the k_s's need not be distinct. Assume $(5,8;4) \notin A$. In this case it follows that $k_2 = 8$ and $k_4 = 7$, and $(5,2;6) \notin A$ and $(5,7;3) \notin A$. Next we infer that $\{(4,7;6),(4,8;5)\} \subset A$. Assume that $(5,6;2) \in A$ and it follows that $\{(3,7;5),(3,6;8)\} \subset A$. The set A now contains three triples on the elements 2 and 8 and two triples on the element 6. But now, if we investigate the subsquares on the elements 2 and 6, and 6 and 8 we obtain a contradiction. Therefore $(5,1;5) \in A$. Next, assume $(3,6;8) \in A$ and note that A contains three triples on the element 8. This infers that one of $(6,1;6)$ or $(8,3;6)$ is in A as well as one of $(6,2;5)$ or $(7,3;5)$. One may now deduce that $(7,8;2) \in A$ and $(8,7;2) \in A$, a contradiction. Thus A must contain the triples $(3,8;6)$ and $(3,5;7)$. However, we have now selected three triples from column 1 and three triples based on the element 6. This leads to $\{(6,3;8),(6,4;7)\} \subset A$, but this is impossible. Hence $(5,8;4) \in A$ and $(5,4;8) \notin A$. We know that $(5,5;1)$ cannot be a triple of A and so $\{(4,5;8),(4,6;7),(5,7;3)\} \subset A$. Now if we take row 6 together with row 1 and row 2 we see that $(6,j_s,k_s) \in A$ for $j = 1,\ldots,7$ where $k_1 \in \{3,8\}$, $k_2 \in \{4,7\}$, $k_3 \in \{1,5\}$, $k_4 \in \{3,6\}$, $k_5 \in \{4,5\}$, $k_6 \in \{2,7\}$, and $k_7 \in \{3,5\}$. This in turn implies that $\{(6,2;5),(6,4;7),(6,8;3),(5,6;2),(7,3;5),(7,1;7)\} \subset A$. However, this is impossible as A does not intersect the subsquare on the elements 6 and 8 in rows 5 and 6. Thus, Case 1 leads to a contradiction.

Case 2: A similar argument to that given in Case 1 also leads to a contradiction.

The above argument provides a proof of the following lemma.

Lemma 4.10. *Let L be a latin square representing the elementary abelian 2-group of order 2^3. Let A be a critical set in L. Then $|A| \geq 24$.*

This result can be used to obtain a sharper lower bound for latin squares representing the elementary abelian 2-group of order 2^v.

Theorem 4.11. *Let L be a latin square representing the elementary abelian 2-group of order 2^v where $v \geq 4$. Let A be a critical set in L. Then $|A| \geq 24.2^{2v-6}$.*

Proof: The proof of this result follows directly from Lemma 1.3 and Lemma 4.10. ∎

Finally we consider the latin square representing the elementary abelian group C_3^v of order 3^v. This latin square can be partitioned into 3^{2v-2} latin subsquares of order 3. It follows from Lemma 1.3 that any critical set for this latin square must have size greater than or equal to 2.3^{2v-2}. But once again, we can improve this lower bound. We begin by considering the elementary abelian group of order 3^2. The latin square representing this group is given below.

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

We observe that if we take any two rows in this latin square there exists a third row such that these three rows can be partitioned into latin subsquares of order 3.

Lemma 4.12. *Let L be a latin square representing the elementary abelian group C_3^2, of order 3^2, and $A - r_x$ a critical set in L. Then $|A - r_x| \geq 24$.*

Proof: Assume that, without loss of generality, $A - r_x$ contains no triples selected from row 1 of L. The sets of rows $\{1,2,3\}$, $\{1,4,7\}$, $\{1,5,9\}$, and $\{1,6,8\}$ each contain three subsquares of order 3. Thus $A - r_x$ must contain at least two triples selected from each of these subsquares. And so $A - r_x$ must contain six triples selected from each of the pairs of rows 2,3, 4,7, 5,9, and 6,8. Therefore, $|A - r_x| \geq 6 \times 4 = 24$. ∎

This argument can be generalised.

Lemma 4.13. *Let L be a latin square representing the elementary abelian group C_3^v, of order 3^v, and $A - r_x$ a critical set in L. Then $|A - r_x| \geq 3^{v-1}(3^v - 1)$.*

Let us return to C_3^2.

Lemma 4.14. *Let L be a latin square representing the elementary abelian group C_3^2 and let A be a critical set in L. Then $|A| \geq 21$.*

Proof: Assume that $|A| = 20$. It follows from Lemma 4.12 that A must contain triples selected from each row, each column, and based on each element of L. We begin by assuming that A contains at most one triple from row p of L. Assume, without loss of generality, that $p = 1$ and $(1, 1; 1) \in A$. Then once again A must contain five triples selected from each of the pairs of rows $2,3$, $4,7$, $5,9$, and $6,8$. It is immediate that $|A| \geq 4 \times 5 + 1 = 21$.

Since $|A| = 20$, it follows that A contains at most two triples from each of seven rows of L. Therefore, without loss of generality, assume that A contains precisely two triples from each of the rows 1, 2, and 3. We may assume that $\{(1, 1; 1), (1, 4; 4)\} \subset A$ and, without loss of generality, deduce that $\{(2, 5; 6), (3, 3; 2)\} \subset A$.

Now consider rows 1,4,7. They are as follows:

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 & 3 \\ 7 & 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6. \end{array}$$

These rows contain three latin subsquares of order 3 on the sets of elements $\{1,4,7\}$, $\{2,5,8\}$, and $\{3,6,9\}$. The subsquare on the set $\{1,4,7\}$ intersects A in the triples $(1, 1; 1)$ and $(1, 4; 4)$, but these two triples do not form a critical set for this subsquare. Further, A contains no triples selected from row 1 and which intersect the subsquares on the sets $\{2,5,8\}$ and $\{3,6,9\}$. Hence A must contain three triples from one of the rows 4 and 7.

If $(2, 8; 9)$ belongs to A, then so does $(3, 9; 8)$. But now one of rows $2, 5, 8$, and one of rows $3, 6, 9$ must contribute three triples to A. But this implies that $|A| > 20$, a contradiction. We have two remaining cases to consider: A contains the triple $(2, 9; 7)$, and A contains the triple $(2, 7; 8)$.

In the first of these one may compare rows 1, 2, 3, and 7, and deduce that row 7 must contribute at least three triples to A. It now follows that two of rows 4, 5, or 6 must contribute at most two triples to A. But when we look at each of these rows in conjunction with rows 1, 2, and 3, we obtain a contradiction.

In the second case, a comparison of rows 1, 2, 3, and 4, shows that row 4 must contribute at least three triples to A. However, this also leads to a contradiction.

We may now deduce that $|A| \geq 21$. ∎

Theorem 4.15. *Let L be a latin square representing the elementary abelian group C_3^r of order 3^r where $r \geq 3$. Let A be a critical set in L. Then $|A| \geq 21.3^{2r-4}$.*

Proof: The proof follows directly from Lemma 1.3 and Lemma 4.14. ∎

Acknowledgement. The authors wish to thank the referee for his suggestlons.

References

1. Joan Cooper, Diane Donovan, and Jennifer Seberry, *Latin squares and critical sets of minimal size*, Australas. J. Combin. **4** (1991), 113–120.
2. C.J. Colbourn, M.J. Colbourn, and D.R. Stinson, *The computational complexity of recognizing critical sets.* in Proc. 1st Southeast Asian Graph Theory Colloquium, Lecture Notes in Math. **1073** (Springer-Verlag, 1984), 248–253.
3. D. Curran and G.H.J. van Rees, *Critical sets in latin squares.* Proc. 8th Manitoba Conference on Numerical Mathematics and Computing, (Congressus Numerantium XXII), Utilitas Math. Pub., Winnipeg (1978), 165–168.
4. J.R. Elliott and P.B. Gibbons, The construction of subsquare free latin squares by simulated annealing, Australas. J. Combin. **5** (1992), 209–228.
5. J. Dénes and A.D. Keedwell, "Latin Squares and their Applications", The English Universities Press Ltd, London, 1974.
6. J. Seberry, *Secret sharing and group identification.* Research and Development Studies, Stage 3 Report from the Centre for Computing and Communication Security Research to Telecom Australia (June 1990)
7. Bohdan Smetaniuk, *On the minimal critical set of a latin sqare*, Utilitas Math. **16** (1979), 97–100.
8. D.R. Stinson and G.H.J. van Rees, *Some large critical sets*, Congressus Numerantium **34** (1982), 441–456.
9. Anne Penfold Street, *Defining sets for t-designs and critical sets for Latin squares*, New Zealand Journal of Mathematics **21** (1992), 133–144..