LATIN SQUARES AND CRITICAL SETS OF MINIMAL SIZE

JOAN COOPER[1], DIANE DONOVAN[2] AND JENNIFER SEBERRY[3]

[1]Australian National University,
Canberra, ACT, Australia 2601.

[2]The University of Queensland,
Queensland, Australia 4072.

[3]University College,
The University of New South Wales,
Australian Defence Force Academy,
Canberra, ACT, Australia 2600.

ABSTRACT

This paper discusses critical sets for latin squares. We give the cardinality of the minimal critical set for a family of latin squares and for latin squares of small order.

A *latin square* L of order n is an $n \times n$ array with entries chosen from a set of size n such that each entry occurs precisely once in each row and column. 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 entry i occurs in position (j, k) of the latin square L. 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. A latin square is said to be *reduced* or in *standard form* if in the first row and first column the entries $1, 2, \ldots, n$ occur in natural order. Let P be an $n \times n$ array with entries chosen from a set of size n in such a way that each entry 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. Two latin squares L and M are said to be *isotopic* or *equivalent* if there exists an ordered triple $(\alpha,\ \beta,\ \gamma)$, of permutations, such that $\alpha,\ \beta,\ \gamma$ map the rows, columns, and entries, respectively, of L onto M. That is, two latin squares are isotopic, if one can be transformed onto the other by rearranging rows, rearranging columns and renaming entries. If we represent L and M by their quasigroups, then the equivalent definition for quasigroups is given as follows. Let $(L, \circ)$ and $(M, *)$ be two quasigroups. An ordered triple $(\alpha,\ \beta,\ \gamma)$ of one-to-one mappings $\alpha,\ \beta,\ \gamma$ of the set L onto the set M is called an isotopism of $(L, \circ)$ upon $(M, *)$, if $(x\alpha) * (y\beta) = (x \circ y)\gamma$ for all x, y in L. The quasigroups $(L, \circ)$ and $(M, *)$ are then said to be isotopic. Two latin squares (quasigroups) are said to be *isomorphic* if the permutations $\alpha,\ \beta,\ \gamma$ are equal. (For more details see

Australasian Journal of Combinatorics 4(1991), pp 113-120

[3] pages 23 and 124.) It follows from the definition of isotopism that every latin square is isotopic to a reduced latin square.

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 entry i in position (j,k) for each $(i,j,k) \in A$;

(2) no proper subset of A satisfies (1).

A *minimal critical set* of a latin square L is a critical set of minimum cardinality. For example, the latin square given below (on the left) has a minimal critical set $\{(1,1,1),(2,1,2),(4,2,3),(2,3,4),(3,4,2)\}$.

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

Two critical sets A and B are said to be isotopic if there exists an ordered triple of permutations $(\gamma,\ \alpha,\ \beta)$ which maps the entries of A onto B. That is, γ maps the first co-ordinate of an element of A onto the first co-ordinate of an element of B, and α and β map the second and third co-ordinates, respectively. The sets A and B are isomorphic if the permutations α, β, and γ are equal.

Critical sets have a number of applications. They arise naturally in agricultural research and have applications in cryptography as given by Seberry [6]. They have been studied by Colbourn, Colbourn and Stinson [1], Curran and van Rees [2], Nelder [4] and [5], Smetaniuk [7] and Stinson and van Rees [8]. Curran and van Rees gave the cardinality of a minimal critical set for certain latin squares of orders 1, 2, 3, 4 and 5, as well as an upper bound on the size of a minimal critical set for a certain class of latin squares. We extend the results on critical sets for latin squares of small order, and go on to give the cardinality of a critical set for a family of latin squares. In addition, we establish lower bounds for infinite classes of latin squares.

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

(1) $C = P_1 \subset P_2 \subset \cdots \subset P_{m-1} \subset P_m \subset L$;

(2) For any i, $2 \le i \le m$, given $P_i = P_{i-1} \cup \{(r,s,t)\}$, then the set $P_{i-1} \cup \{(r',s,t)\}$ is not a partial latin square for any $r' \in N \backslash \{r\}$.

We have computed, by hand or by computer, strong critical sets of minimum cardinality for all non-isomorphic reduced latin squares of order less than or equal to 5 and for a latin square of order 6. These latin squares have been taken from Dénes and Keedwell [3] page 129 onwards. We summarise our results in Table 1. Note that we have used the numbering system listed by Dénes and Keedwell to distinguish the various latin squares. This numbering system is based on the isomorphism classes of the latin squares and is explained in detail on pages 128 and 129 of [3]. These numbers are listed as the class representation and are given in column two of Table 1. Examples of strong critical sets of minimum cardinality for each latin square are given in the Appendix.

TABLE 1: STRONG CRITICAL SETS FOR LATIN SQUARES

Order	Class	Minimum	Number of non-isomorphic strong
	representation	cardinality	critical sets of minimum cardinality
1		0	0
2	1.1.1	1	1
3	1.1.1	2	1
4	1.1.1	5	1
	2.1.1	4	1
5	1.1.1	6	1
	2.1.1	7	≥ 3
	2.1.2	7	≥ 3
	2.1.3	7	≥ 3
	2.1.4	7	≥ 3
	2.1.5	7	≥ 3
6	1.1.1	9	1
	3.1.1	> 9	
	4.1.1	> 9	

Let L be a latin square in which the rows and columns are indexed by $N = \{0, 1, \ldots, n-1\}$, with $n > 1$. L is said to be a *back circulant latin square*, if the entry in position (i, j) is the integer $i + j$(modulo n). Curran and van Rees [2] showed that the cardinality of a minimal critical set, for a back circulant latin square, is less than or equal to $n^2/4$, if n is even, and less than or equal to $(n^2-1)/4$, if n is odd.

Lemma 1 (Curran and van Rees [2]).

(1) *A back circulant latin square, of even order, is the only latin square which contains the set* $C = \{(i+j, i, j) \mid j = n/2, n/2+1, \ldots, n-1-i$ *and* $i = 0, 1, \ldots, n/2-1\} \cup \{(n-i+j, n-i, j) \mid j = i, i+1, \ldots, n/2-1$ *and* $i = 1, 2, \ldots, n/2-1\}$, *where addition of the first component is taken modulo* n. *The cardinality of this set is* $n^2/4$.

(2) *A back circulant latin square, of odd order, is the only latin square which contains the set* $C = \{(i+j, i, j) \mid j = (n+1)/2, (n+1)/2+1, \ldots, n-1-i$ *and* $i = 0, 1, \ldots, (n-1)/2-1\} \cup \{(n-i+j, n-i, j) \mid j = i, i+1, \ldots, (n-1)/2$ *and* $i = 1, 2, \ldots, (n-1)/2\}$, *where addition of the first component is taken modulo* n. *The cardinality of this set is* $(n^2-1)/4$.

Curran and van Rees showed that the above sets satisfy condition (1) of the definition of minimal critical sets and in the case of n even went on to show that condition (2) was satisfied; that is, any proper subset of this set must be contained in two different latin squares. Essentially their proof points out that for any $(x,i,j) \in C$ we have entry x in positions (i,j) and $(i+n/2, j+n/2)$, and entry $x+n/2$ in positions $(i, j+n/2)$ and $(i+n/2, j)$ of L, where addition is taken modulo n. The set $C \backslash \{(x,i,j)\}$ is contained in L. However, it is also contained in a latin square L' which has entry $x+n/2$ in positions (i,j) and $(i+n/2, j+n/2)$, and entry x in positions $(i, j+n/2)$ and $(i+n/2, j)$, where addition is take modulo n. Hence C is a critical set. In fact what Curran and van Rees have shown is that C is a minimal critical set, as verified in Theorem 3. We go on to show that for n odd the set C satisfies condition (2).

Lemma 2. *Let L be a latin square with a minimal critical set A. Let $S = \{S_i \mid i = 1, \ldots, r\}$ be a set of latin subsquares which partition L and let C_i denote a minimal critical set for S_i, for each $i = 1, \ldots, r$. If $|C_i| = c_i$, for $i = 1, \ldots, r$, then $|A| \geq \sum_{i=1}^{r} c_i$.*

Proof. Since S partitions L, A can be partitioned into subsets A_i, for $i = 1, \ldots, r$, where the elements of A_i correspond to the latin subsquares S_i. For all elements $(u,v,w) \in A_i$, for $i = 1, \ldots, r$, we let (u, v', w') denote the occurrence of the entry u in position (v', w') of the latin subsquare S_i. The set of all such elements (u, v', w') is denoted by A'_i and $|A_i| = |A'_i|$. Assume $|A| < \sum_{i=1}^{r} c_i$. Then $|A_j| = |A'_j| < |C_j|$ for some $j = 1, \ldots, r$. However, C_j is a minimal critical set for S_j. So, by condition (2) of the definition of critical sets, there exist two latin squares R and T, of order $|S_j|$, which have entry u in position (v', w') for each $(u, v', w') \in A'_j$. Hence there exist two latin squares L and L' which contain subsquares R and T respectively, and in addition contain the set A. This is a contradiction. Hence $|A| \geq \sum_{i=1}^{r} c_i$. □

Theorem 3. *Let L be a back circulant latin square.*

(1) *If n is even, then L contains a minimal critical set of size $n^2/4$.*
(2) *If n is odd, then L contains a critical set of size $(n^2-1)/4$.*

Proof. (1) If n is even, then L contains $(n/2).(n/2) = n^2/4$ latin subsquares of order 2. These are given by subarrays which have entry x in positions (i,j), and $(i+n/2, j+n/2)$ and entry $(x+n/2)$(modulo n), in positions $(i, j+n/2)$ and $(i+n/2, j)$ of L, for $1 \leq i, j \leq n/2$. This set of latin subsquares partitions L. The cardinality of the minimal critical set for a latin square of order two is 1 and so by Lemma 2 a minimal critical set for L has cardinality at least $n^2/4$. Lemma 1 establishes the existence of an appropriate set of this size, and so the result follows.

(2) It is easy to verify that L contains subarrays of size $((n-1)/2+1) \times ((n+1)/2+1)$ which have the following properties. Entry x occurs in positions (i,j) and $(i+(n-1)/2, j+(n+1)/2)$, entry y occurs in positions $(i+s, j+(n-1)/2-s)$ for $s = 0, \ldots, (n-1)/2$ and entry z occurs in positions $(i+s, j+(n+1)/2-s)$ for $s = 0, \ldots, (n-1)/2$, where $y = x + (n-1)/2$(modulo n) and

$z = x + (n+1)/2(\text{modulo n})$. That is, L contains subarrays of the form:

$$\begin{array}{cccccccccc}
\mathrm{x} & . & . & . & . & . & . & . & \mathrm{y} & \mathrm{z} \\
. & . & . & . & . & . & . & \mathrm{y} & \mathrm{z} & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & \mathrm{y} & \mathrm{z} & . & . & . & . & . & . & . \\
\mathrm{y} & \mathrm{z} & . & . & . & . & . & . & . & \mathrm{x}.
\end{array}$$

A subarray of this type can be replaced by a subarray of the form: entry x in positions $(i, j+(n+1)/2)$ and $(i+(n-1)/2, j)$, entry y in positions (i,j) and $(i+s, j+(n+1)/2-s)$ for $s = 1, \ldots, (n-1)/2$, and entry z in positions $(i+(n-1)/2, j+(n+1)/2)$ and $(i+s, j+(n-1)/2-s)$ for $s = 1, \ldots, (n-3)/2$. That is, it can be replaced by a subarray of the form:

$$\begin{array}{cccccccccc}
\mathrm{y} & . & . & . & . & . & . & . & \mathrm{z} & \mathrm{x} \\
. & . & . & . & . & . & . & \mathrm{z} & \mathrm{y} & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & \mathrm{z} & \mathrm{y} & . & . & . & . & . & . & . \\
\mathrm{x} & \mathrm{y} & . & . & . & . & . & . & . & \mathrm{z}.
\end{array}$$

The result will be a latin square L' which differs from L in the positions listed above. If we take the set given by Curran and van Rees in Lemma 1, part (2), and take any subset of size $(n^2-1)/4 - 1$, then there are at least two latin squares L and L' which contain this subset. That is, if we remove element x in position (i,j), then we can complete the subset to at least two latin squares each of which has one of the subarrays given above. □

Lemma 2 also allows us to establish lower bounds for the cardinality of minimal critical sets for infinitely many latin squares. For example, the latin square representing the elementary abelian 2-group of order 8

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

can be partitioned into four latin subsquares of order 4. The cardinality of the minimal critical set for latin squares of order 4, isomorphic to these latin subsquares, is 5. By Lemma 2, the cardinality for the minimal critical set of this latin square of order eight is greater than or equal to 20. We state the following more general theorem.

Theorem 4. *The size of the minimal critical set for the latin square representing the abelian 2-group of order 2^n, for $n \geq 2$, is greater than or equal to 5.2^{2n-4}.*

Acknowledgement. The authors wish to thank Kathryn McClaren for her assistance and expertise with the computer programs.

APPENDIX.

The following are examples of strong critical sets of minimum cardinaltiy for the latin squares listed in Table 1.

Latin square of order 2

$$\begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array} \qquad \begin{array}{cc} 1 & * \\ * & * \end{array}$$

Latin square of order 3

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 1 & * & * \\ * & * & * \\ * & * & 2 \end{array}$$

Latin squares of order 4

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

Latin squares of order 5

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{array} \qquad \begin{array}{ccccc} 1 & 2 & * & * & * \\ 2 & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & 3 \\ * & * & * & 3 & 4 \end{array}$$

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \\ 3 & 5 & 1 & 2 & 4 \\ 4 & 3 & 5 & 1 & 2 \\ 5 & 4 & 2 & 3 & 1 \end{array} \qquad \begin{array}{ccccc} 1 & 2 & * & * & * \\ * & * & 4 & 5 & * \\ 3 & * & * & * & * \\ * & * & 5 & 1 & * \\ * & * & * & * & * \end{array} \qquad \begin{array}{ccccc} 1 & 2 & * & * & * \\ * & * & 4 & 5 & * \\ 3 & * & * & * & * \\ * & * & 5 & * & * \\ * & * & * & * & 1 \end{array}$$

$$\begin{array}{ccccc} 1 & 2 & * & * & * \\ * & * & 4 & * & * \\ * & * & * & 2 & * \\ 4 & * & 5 & * & * \\ * & * & * & 3 & * \end{array}$$

```
1 2 3 4 5      1 2 * * *      1 2 * * *
2 1 5 3 4      * * 5 3 *      * * 5 3 *
3 4 2 5 1      * 4 * 5 *      * 4 * * *
4 5 1 2 3      * * * * *      * * * * 3
5 3 4 1 2      * * * * 2      * * * * 2

               1 * 3 * *
               * 1 * * 4
               3 * 2 * *
               * 5 * * *
               * * * * *
```

```
1 2 3 4 5      1 2 * * *      1 2 * * *
2 1 4 5 3      * * 4 5 *      * * 4 5 *
3 4 5 1 2      3 * 5 * *      3 * * * *
4 5 2 3 1      * * * * 1      * * * * 1
5 3 1 2 4      * * * * *      * * * * 4

               1 * * * *
               2 * 4 * *
               * * * * *
               * 5 * 3 *
               * 3 * 2 *
```

```
1 2 3 4 5      1 2 * * *      1 2 * * *
2 1 4 5 3      * * 4 5 *      * * 4 5 *
3 4 5 2 1      3 * * * 1      * * 5 2 *
4 5 1 3 2      * 5 * * *      * * * * *
5 3 2 1 4      * * * * *      * 3 * * *

               1 2 * * *
               * * * 5 3
               * 4 * * *
               * * * 3 *
               * * 2 * *
```

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 5 & 2 & 1 & 4 \\ 4 & 1 & 5 & 3 & 2 \\ 5 & 4 & 1 & 2 & 3 \end{array} \qquad \begin{array}{ccccc} 1 & 2 & * & * & * \\ 2 & * & * & * & * \\ * & * & * & 1 & * \\ * & * & 5 & 3 & * \\ * & * & * & * & 3 \end{array} \qquad \begin{array}{ccccc} 1 & 2 & * & * & * \\ * & * & 4 & 5 & * \\ 3 & * & * & * & * \\ * & * & 5 & * & * \\ * & * & * & 2 & * \end{array}$$

$$\begin{array}{ccccc} 1 & 2 & * & * & * \\ * & * & * & 5 & * \\ * & * & * & * & * \\ 4 & 1 & * & * & * \\ * & * & * & 2 & 3 \end{array}$$

Latin square of order 6

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 4 & 5 & 6 & 1 & 2 & 3 \\ 5 & 6 & 1 & 2 & 3 & 4 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{array} \qquad \begin{array}{cccccc} 1 & 2 & 3 & * & * & * \\ 2 & 3 & * & * & * & * \\ 3 & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & 4 \\ * & * & * & * & 4 & 5 \end{array}$$

REFERENCES.

[1]. 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.

[2]. 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.

[3]. J. Dénes and A.D. Keedwell, Latin squares and their applications, The English Universities Press Ltd, London (1974).

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

[5]. John Nelder, *Private communication from John Nelder to J. Seberry.*

[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 square*, 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.