Critical Sets In Back Circulant Latin Squares *

Diane Donovan and Joan Cooper

September 26, 2002

Abstract

To date very few families of critical sets for latin squares are known. In this paper a new family of critical sets for back circulant latin squares is identified. The proof that each element of the critical set is an essential part of the reconstruction process relies on the proof of the existence of a large number of latin interchanges.

1 Introduction

A critical set is a partial latin square which is contained in precisely one latin square, of the same order, with the additional property that if one removes any entry from the partial latin square, then what is left is contained in at least two latin squares of the same order. Critical sets were first discussed by Nelder [**7**] in 1977. Critical sets are of use when studying isotopy classes of latin squares and have applications in cryptology, see for example [**2**] and [**4**].

In the late 1970's Nelder [**8**] conjectured that if one takes the latin square which represents the addition table of the integers modulo n, then the upper left triangle of entries bounded by, but not including, the main right-to-left diagonal, is a critical set in this latin square. Nelder commented that it is easy to show that this set is contained in precisely one latin square, but not so easy to show that the omission of any entry leads to ambiguity, [**8**]. In Section 3 of this paper, new techniques will be developed which verify that every element of the partial latin square is necessary and, in Section 4, a proof will be given that verifies the truth of this conjecture. However, before this can be done the above ideas must be defined formally.

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. If $N = \{0, 1, \ldots, n-1\}$, then a *back circulant latin square* has the integer $i + j \pmod n$ in cell (i, j). A back circulant latin square, of order n, corresponds to the cyclic group C_n. For convenience, a latin square will sometimes be represented as a set of ordered

*Subject Classification: 05B15

triples $(i,j;k)$, and this is taken to mean that element k occurs in cell (i,j) of the latin square. Using this notation, a back circulant latin square can be represented by the set $\{(i,j;i+j) \mid 0 \leq i,j \leq n-1\}$, where addition is taken modulo n. Since this paper deals specifically with back circulant latin squares it will be assumed, unless otherwise stated, that all addition is taken modulo n. If L contains an $s \times s$ subarray S and if S is a latin square of order s, then S is said to be a *latin subsquare* of L. A *partial latin square* P 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 at most once in each row and column. A partial latin square $C = \{(i,j;k) \mid i,j,k \in N\}$, of order n, is said to have a *unique completion* to the latin square L, if L is the only latin square of order n which has element k in position (i,j), for each $(i,j;k) \in C$; A *critical set*, in a latin square L of order n, is a set $C = \{(i,j;k) \mid i,j,k \in N\}$ such that,

1. C has a unique completion to L, and
2. no proper subset of C satisfies 1.

Let L be a back circulant latin square of order 7 and take the set $C = \{(0,0;0), (0,1;1), (0,2;2), (0,3;3), (1,0;1), (1,1;2), (1,2;3), (2,0;2), (2,1;3), (3,0;3), (5,6;4), (6,5;4), (6,6;5)\}$. Then C is a critical set in L. The latin square L and the critical set C are displayed below. The entry $*$ indicates that the appropriate cell is empty.

0	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

L

0	1	2	3	*	*	*
1	2	3	*	*	*	*
2	3	*	*	*	*	*
3	*	*	*	*	*	*
*	*	*	*	*	*	*
*	*	*	*	*	*	4
*	*	*	*	*	4	5

C

In 1978, Curran and van Rees [**3**] showed that the set

$$\begin{aligned} C = \quad & \{(i,j;i+j) \mid \quad i = 0,\ldots,n/2-1 \text{ and } j = 0,\ldots,n/2-1-i\} \quad \cup \\ & \{(i,j;i+j) \mid \quad i = n/2+1,\ldots,n-1 \text{ and } j = n/2-i,\ldots,n-1\}, \end{aligned}$$

of cardinality $n^2/4$, is a critical set in a back circulant latin square of even order n. They showed that C has a unique completion, and further, if any element $(i,j;k)$ of C is removed, then $C \setminus \{(i,j;k)\}$ has at least two completions. The proof of this result relies on the fact that for each element $(i,j;k)$ of C, there exists a subsquare

$$S = \{(i,j;k), (i+n/2, j; k+n/2), (i, j+n/2; k+n/2), (i+n/2, j+n/2; k)\},$$

such that $S \cap C = \{(i,j;k)\}$. (See also Smetaniuk, [**9**].)

Curran and van Rees also showed that the set

$$C = \{(i,j;i+j) \mid i = 0,\ldots,(n-3)/2 \text{ and } j = 0,\ldots,(n-3)/2-i\} \cup \{(i,j;i+j) \mid i = (n-1)/2+1,\ldots,n-1 \text{ and } j = (n-1)/2-i,\ldots,n-1\},$$

of cardinality $(n^2-1)/4$, has a unique completion to a back circulant latin square of odd order n. However, they failed to show that if one removes an element from C, then the remaining partial latin square has at least two completions. This fact was verified by Cooper, Donovan and Seberry in [**1**]. The sets given by Curran and van Rees [**3**] are the only known examples of general families of critical sets. Stinson and van Rees [**10**] have shown that given a critical set in a latin square L which satisfies certain properties, one may use a product construction to identify a critical set in $C_2 \times L$. This is the only known construction for critical sets. The main aim of this paper is to establish the existence of a new family of critical sets in back circulant latin squares, and so settle Nelder's conjecture. It will be shown that the partial latin square

$$A = \{(i,j;i+j) \mid i = 0,\ldots,n-2 \text{ and } j = 0,\ldots,n-2-i\}$$

is a critical set in a back circulant latin square of order n. This will be achieved by generalising ideas from [**1**].

Cooper, Donovan and Seberry [**1**] showed that if one removes an element from the set

$$C = \{(i,j;i+j) \mid i = 0,\ldots,(n-3)/2 \text{ and } j = 0,\ldots,(n-3)/2-i\} \cup \{(i,j;i+j) \mid i = (n-1)/2+1,\ldots,n-1 \text{ and } j = (n-1)/2-i,\ldots,n-1\},$$

then the remaining partial latin square has at least two completions. They achieved this by showing that, for each $(i,j;k) \in C$, there exists a partial latin square I in L which satisfies the following properties,

- $C \cap I = \{(i,j;k)\}$ and
- there exists a latin square L' distinct from L which agrees with L everywhere except in I.

The partial latin square I is termed a latin interchange and is defined as follows. Let $I = \{(i,j;k) \mid i,j,k \in N\}$ be a partial latin square of order n. Then $|I|$ is said to be the *size* of the partial latin square and the set of cells $\{(i,j) \mid (i,j;k) \in I,\ \exists k \in N\}$ is said to determine the *shape* of I. Let $I' = \{(i,j;k') \mid i,j;k' \in N\}$ be a partial latin square with the same shape as I. The partial latin squares I and I' are said to be *mutually balanced* if the entries in the cells of each row (and column) of I are the same as those in the corresponding row (and column) of I'. They are said to be *disjoint* if no cell in I' contains the same entry as the corresponding cell of I. Let I and I' be two partial latin squares of the same size and shape. If I and I' are disjoint

and mutually balanced, then I is said to be a *latin interchange* and I' is said to be a *disjoint mate* of I. Keedwell [**6**] uses the term *critical partial latin squares* for latin interchanges.

Note that if I can be completed to a latin square L of order n, then I' can be completed to a latin square which agrees with L everywhere except in the partial latin square I'. So one may easily verify the following lemma.

Lemma 1 *Let L be a latin square of order n, and $C = \{(i,j;k) \mid i,j,k \in N\}$ a critical set in L. Then*

- *if I is a latin interchange in L, then $C \cap I \geq 1$, and*
- *for each $(i,j;k) \in C$ there exists a latin interchange I in L such that $I \cap C = \{(i,j;k)\}$.*

With this in mind the following steps will be used to prove Nelder's conjecture. Let

$$A = \{(i,j;i+j) \mid i = 0,\ldots,n-2 \text{ and } j = 0,\ldots,n-2-i\},$$

where all arithmetic is done modulo n.

1. It will be shown that A has a unique completion to a back circulant latin square L, of order n.

2. It will be shown that for each element $(0,j;j)$, $0 \leq j \leq n-2$, in the first row of A there exists a latin interchange I in L such that

$$A \cap I = \{(0,j;j)\}.$$

To show this for all possible j it will be necessary to develop three separate recursive constructions. In each case a number of small examples will be given and then these will be used to prove the existence of latin interchanges with the required property.

3. Finally, the cyclic nature of the back circulant latin square will be used to show that for all $(i,j;i+j) \in A$, there exists a latin interchange I such that

$$A \cap I = \{(i,j;i+j)\}.$$

On completion of the above steps, it will follow that A is indeed a critical set.

The next two general lemmas will be needed in Step 3.

In a *symmetric* latin square the entry in cell (i,j) is the same as the entry in cell (j,i), for all i,j.

Lemma 2 *If $I = \{(i,j;k) \mid i,j,k \in N\}$ is a latin interchange in a symmetric latin square L, then the set $I^T = \{(j,i;k) \mid (i,j;k) \in I\}$ is also a latin interchange in L.*

Proof. If I' is a disjoint of mate of I, then it is easy to see that the set $\{(j,i;k') \mid (i,j;k') \in I'\}$ and I^T have the same size and shape, are disjoint and mutually balanced. Therefore this set forms the disjoint mate of I^T and I^T is a latin interchange.

□

Lemma 3 *Let L be a back circulant latin square of order n and let $I = \{(i,j;k) \mid i,j,k \in N\}$ be a latin interchange in L. Then for any integers α and β, $J = \{(i+\alpha, j+\beta; k+\alpha+\beta) \mid (i,j;k) \in I\}$ is a latin interchange in L.*

Proof. Let $I' = \{(i,j;k') \mid i,j,k' \in N\}$ be a disjoint mate of I. First it is established that $J' = \{(i+\alpha, j+\beta; k'+\alpha+\beta) \mid i,j,k' \in N\}$ is a disjoint mate of J. Since I and I' have the same size and shape, J and J' will have the same size and shape. It also follows that J and J' must be disjoint. Next it is shown that J and J' are mutually balanced. Assume they are not. Then without loss of generality we may assume that there exists an entry in row $i_0+\alpha$ of J which does not occur in row $i_0+\alpha$ of J'. But this implies that I and I' differ in row i_0, which is a contradiction. One may repeat this argument for the columns of J. Consequently, J and J' are mutually balanced and so J is a latin interchange.

□

2 Unique Completion

Lemma 4 *Let L be a back circulant latin square of order n and let*

$$A = \{(i,j;i+j) \mid i = 0,\ldots,n-2 \text{ and } j = 0,\ldots,n-2-i\},$$

where arithmetic is done modulo n. Then L is the only latin square of order n containing A.

Proof. It must be shown that A has a unique completion to L.

The element $n-1$ does not occur in the partial latin square A. Therefore, $n-1$ must be placed in n empty cells. The only possible way of doing this is to place $n-1$ in the cells $(i, n-1-i)$ for $i = 0,\ldots,n-1$. Similarly it can be shown that the element k must occur in the cell $(k+i, n-i)$ for $k = 0,\ldots,n-2$ and $i = 1,\ldots,n-1-k$. Thus A has a unique completion to L.

□

3 Families of Latin Interchanges

In what follows the notation $I_{e,n}$ is used to represent a partial latin square, of order n, which includes, among its entries, $(0, e; e)$ and $(0, n-1; n-1)$. It will be shown that for all $n \geq 2$ and for all e, $0 \leq e \leq n-2$, it is possible to construct a partial latin square $I_{e,n}$ which has the following properties.

- The partial latin square $I_{e,n}$ will be contained in a back circulant latin square of order n.
- The only entries in the first row of $I_{e,n}$ will be $(0, e; e)$ and $(0, n-1; n-1)$.
- All other entries of $I_{e,n}$ will occur in columns e to $n-1$ and either on the right–to–left diagonal or below it.
- The partial latin square $I_{e,n}$ is a latin interchange.

From the third property above it can be seen that such a latin interchange will intersect A in the entry e in the first row and in no other entry. Since all the entries of $I_{e,n}$ will occur in columns e to $n-1$ the distance between these columns will be of importance in the construction of the latin interchanges. So, for each $n \geq 2$, let $x = n-1-e$ where $0 \leq e \leq n-2$ and so

$$e = n-1-x,$$

where $1 \leq x \leq n-1$. Thus, for each $n \geq 2$ and for each x, $1 \leq x \leq n-1$, a partial latin square $I_{n-1-x,n}$ will be constructed such that $I_{n-1-x,n}$ is a latin interchange and

$$I_{n-1-x,n} \cap A = \{(0, n-1-x; n-1-x)\}, \tag{1}$$

where

$$A = \{(i, j; i+j) \mid i = 0, \ldots, n-2 \text{ and } j = 0, \ldots, n-2-i\}.$$

For completeness the case where $n = 2$ and $x = 1$ will be considered. There is one possible partial latin square $I_{0,2}$ which is a latin interchange and satisfies (1). This latin interchange together with its disjoint mate $I'_{0,2}$ are given below.

$I_{0,2}$	0	1
0	0	1
1	1	0

$I'_{0,2}$	0	1
0	1	0
1	0	1

Let $n = 3$ and $x = 1, 2$. The following two partial latin squares $I_{1,3}$ and $I_{2,3}$ satisfy (1) and are both latin interchanges.

$I_{1,3}$	0	1	2
0		1	2
1		2	0
2		0	1

$I_{0,3}$	0	1	2
0	0		2
1		2	0
2	2	0	

The disjoint mates of these two latin interchanges are the partial latin squares $I'_{1,3}$ and $I'_{2,3}$ (respectively) given below.

$I'_{1,3}$	0	1	2
0		2	1
1		0	2
2		1	0

$I'_{0,3}$	0	1	2
0	2		0
1		0	2
2	0	2	

It will now be proven that for any $n \geq 2$ there exist partial latin squares $I_{n-2,n}$ and $I_{0,n}$ which are latin interchanges and satisfy (1) and, further in the case where x is a divisor of n or $n-x$ is a divisor of x, it will be shown that there exists a partial latin square $I_{n-1-x,n}$ which is a latin interchange with the required property.

Lemma 5 *Let L be a back circulant latin square of order $n \geq 2$.*

1. *There exists a partial latin square $I_{n-2,n}$ in L which is a latin interchange and is such that $I_{n-2,n} \cap A = \{(0, n-2; n-2)\}$.*

2. *There exists a partial latin square $I_{0,n}$ in L which is a latin interchange and is such that $I_{0,n} \cap A = \{(0, 0; 0)\}$.*

3. *For any x, where $2 \leq x \leq n/2$ and $n \equiv 0 (\mathrm{mod}\ x)$, there exists a partial latin square $I_{n-1-x,n}$ in L which is a latin interchange and is such that $I_{n-1-x,n} \cap A = \{(0, n-1-x; n-1-x)\}$.*

4. *For any x, where $n/2 < x < n-1$ and $x \equiv 0 (\mathrm{mod}\ n-x)$, there exists a latin interchange $I_{n-1-x,n}$ in L such that $I_{n-1-x,n} \cap A = \{(0, n-1-x; n-1-x)\}$.*

Proof.
Case 1: For any n the last two columns form the required latin interchange.
Case 2: For any n the set $\{(i, n-i; 0), (i, n-(i+1); n-1) \mid i = 0, \ldots, n-1\}$ is a latin interchange satisfying (1).
Case 3: Fix n and take x such that $2 \leq x \leq n/2$ where $n \equiv 0 (\mathrm{mod}\ x)$. Let

$$I_{n-1-x,n} = \{(ix, n-1-x; (n-1)+(i-1)x), (ix, n-1; n-1+ix) \mid i = 0, 1, \ldots, (n/x)-1\}.$$

This set is displayed in the following table.

$I_{n-1-x,n}$	$n-1-x$	$n-1$
0	$n-1-x$	$n-1$
x	$n-1$	$x-1$
$2x$	$x-1$	$2x-1$
.		.
.		.
.		.
$n-x$	$n-1-2x$	$n-1-x$

Let

$$I'_{n-1-x,n} = \{(ix, n-1-x; n-1+ix), (ix, n-1; (n-1)+(i-1)x) \mid i = 0, 1, \ldots, n/x-1\}.$$

It is easy to check that $I'_{n-1-x,n}$ is the disjoint mate of $I_{n-1-x,n}$ and so $I_{n-1-x,n}$ is a latin interchange which satisfies (1).

Case 4: Fix n and take the case where $n/2 < x < n-1$ and $x \equiv 0 (\text{mod } n-x)$. Let

$$\begin{aligned} I_{n-1-x,n} = \{ & (i(n-x), (n-1)+(i-1)x; n-1-x), \\ & (i(n-x), (n-1)+ix; n-1) \mid i = 0, \ldots, x/(n-x)\}, \end{aligned}$$

where all arithmetic is done modulo n, and

$$\begin{aligned} I'_{n-1-x,n} = \{ & (i(n-x), (n-1)+(i-1)x; n-1), \\ & (i(n-x), (n-1)+ix; n-1-x) \mid i = 0, \ldots, x/(n-x)\}. \end{aligned}$$

The partial latin square $I_{n-1-x,n}$ can be represented by the following table.

$I_{n-1-x,n}$	$n-1-x$	$n-1-2x$	$\ldots$	$n-1+x$	$n-1$
0	$n-1-x$				$n-1$
$n-x$				$n-1$	$n-x-1$
$n-2x$				$n-1-x$	
$\vdots$				$\vdots$	
$n+2x$		$n-1$	$\ldots$		
x	$n-1$	$n-1-x$			

Once again it is easy to check that $I'_{n-1-x,n}$ is the disjoint mate of $I_{n-1-x,n}$ and so $I_{n-1-x,n}$ is a latin interchange which satisfies (1).

□

At this point it has been shown that in a back circulant latin square of order 4, there exist partial latin squares $I_{2,4}$, $I_{1,4}$ and $I_{0,4}$, which are latin interchanges and all of which satisfy (1).

Consider a back circulant latin square of order 5. Latin interchanges $I_{0,5}$ and $I_{3,5}$ exist by Lemma 5. The following tables give the partial latin squares $I_{2,5}$ and $I_{1,5}$, and it is easy to check that they are in fact latin interchanges with the required property.

$I_{2,5}$	0	1	2	3	4
0			2		4
1					
2			4	0	1
3			0	1	2
4					

$I_{1,5}$	0	1	2	3	4
0		1			4
1				4	0
2				0	1
3		4		1	
4					

Given a back circulant latin square of order n, where $2 \leq n \leq 5$, it has been shown that for all x, where $1 \leq x \leq n-1$ there exist a partial latin square $I_{n-1-x,n}$, which is a latin interchange and satisfies (1).

Lemma 5 deals with a number of special cases and uses a simple construction which does not work in general. However variations of Cases 3 and 4, in Lemma 5, can be used to cover all possible values. So to develop general techniques, n is fixed and separate constructions are developed for the cases where $2 \leq x \leq n/2$ and $n/2 < x \leq n-2$. The constructions will be recursive in nature and somewhat complicated. Therefore, a general description of the constructions will be given, followed by a formal statement of the construction with a proof that the partial latin square is a latin interchange and then an example will be given.

When x is in the range 2 to $n/2$, one constructs a partial latin square $I_{n-1-x,n}$ which has entries in the columns bordered by columns $n-1-x$ and $n-1$ and in the rows bordered by rows 0 and $n-x$. Since $n-x-0 = n-x > n-1-(n-1-x) = x$ this subarray is "longer" than it is "wider" and so a technique similar to that used in Case 3 of Lemma 5 will be developed. Basically this region of L will be divided into as many overlapping 2×2 subarrays each spanning $x+1$ rows and $x+1$ columns as possible. Thus the following entries will be placed in $I_{n-1-x,n-1}$:

$$\begin{aligned} &(0, n-1-x; n-1-x), && (0, n-1; n-1), \\ &(x, n-1-x; n-1), && (x, n-1; x-1), \\ &(2x, n-1-x; x-1), && (2x, n-1; 2x-1), \end{aligned}$$

$$\vdots$$

$$((p-1)x, n-1-x; (p-2)x-1), \qquad ((p-1)x, n-1; (p-1)x-1)$$

where $p = \lfloor \frac{n-x}{x} \rfloor$. However since $n-x = px+u$, where $1 \leq u < x$ this set will not form a latin interchange. In fact it only accounts for rows 0 to $(p-1)x$. To obtain a latin interchange entries from rows px to $n-x$, (note that this is $u+1$ rows intersecting $x+1$ columns), must be included in such a way that it is possible to prove that $I_{n-1-x,n}$ has a disjoint mate. To choose the pattern for the non-empty cells in these rows it is assumed that there exists a partial latin square $I_{x-1,x+u}$ of order $x+u$, which is a latin interchange in a back circulant latin square of order $x+u$ and satisfies (1). Note that since $x \leq n/2$ and $1 \leq u < x$, $x+u < n$. This smaller latin interchange is chosen in such a way that the non–empty cells occur in columns $x-1$

to $x+u-1$ and rows 0 to x. So the non–empty cells in this smaller latin interchange occur in a subarray with $x+1$ rows and $u+1$ columns. Further, it will be chosen in such a way that the only entries in the first row are $x-1$ and $x+u-1$ and the only other occurence of $x-1$ is in the cell $(x, x+u-1)$ so this implies that the cell $(x, x-1)$ is also non–empty. The transpose of this smaller latin interchange is taken and used to identify the entries from rows px to $n-x$ which are to be included in $I_{n-1-x,n}$.

This method is described formally in Construction 1 and an example produced after this description.

When x is in the range $n/2 < x \leq n-2$ it is not possible to use the above construction to obtain a latin interchange which intersects A only in the prescribed element. However, the columns $n-1-x$ to $n-1$, $x+1$ columns in total, can be divided into groups of $n-x$ columns and the last $v+1$ columns, where $x = p(n-x)+v$, are treated separately. The elements in $I_{n-1-x,n}$ follow the pattern of Case 4 Lemma 5 up until the last $v+1$ columns and here a smaller latin interchange is used to provide the pattern for the elements chosen from these columns. The smaller latin interchange will have been constructed using Construction 1 or by taking the transpose of a latin interchange constructed using Construction 1. Each of these two situations will be treated as separate subcases. A formal description of both methods will be given in Constructions 2 and 3.

Construction 1

Fix n and take x such that $2 \leq x \leq n/2$ and $n \equiv u (\mathrm{mod}\ x)$, where $u \neq 0$. Let L be a back circulant latin square of order n. It will be shown that there exists a partial latin square $I_{n-1-x,n}$ in L which is a latin interchange and is such that $I_{n-1-x,n} \cap A = \{(0, n-1-x; n-1-x)\}$.

Note that, since $2 \leq x \leq n/2$ and $1 \leq u < x$, $u+x < n$.

Assume there exists a partial latin square $I_{x-1,x+u}$ in a back circulant latin square of order $x+u$, which is an latin interchange and has the following properties.

- If the cell (i,j) of $I_{x-1,x+u}$ is non-empty, then $0 \leq i \leq x$ and $x-1 \leq j \leq x+u-1$, and

- $I_{x-1,x+u} \cap \{(i,j;i+j) \mid i = 0,\ldots,x+u-2 \text{ and } j = 0,\ldots,x+u-2-i\}$
$= \{(0, x-1; x-1)\}$.

By Lemma 2, $T_{x-1,x+u} = \{(j,i;k) \mid (i,j;k) \in I_{x-1,x+u}\}$ is also a latin interchange and

$$T_{x-1,x+u} \cap \{(i,j;i+j) \mid i = 0,\ldots,x+u-2 \text{ and } j = 0,\ldots,x+u-2-i\} = \{(x-1, 0; x-1)\}. \quad (2)$$

Denote the disjoint mate of $T_{x-1,x+u}$ by $T'_{x-1,x+u}$. The latin interchange $T_{x-1,x+u}$ is used to determine the shape of a partial latin square R in L.

Let $p = \lfloor \frac{n-x}{x} \rfloor$. For each non-empty cell (j,i) of $T_{x-1,x+u}$ place an entry in the cell $((px+u)-(x+u-1-j), n-x-1+i) = ((p-1)x+j+1, n-x-1+i)$ of R. The entry in this cell should be the sum $((p-1)x+j+1+n-x-1+i) (\mathrm{mod}\ n)$ and so

$$R = \{((p-1)x+j+1, n-x-1+i; (p-2)x+i+j) \mid (j,i;k) \in T_{x-1,x+u}\}.$$

Now it may be deduced that R has the following structure.

- Column 0 of $T_{x-1,x+u}$ contains the two entries $x-1$ and $x+u-1$. Therefore column $n-x-1$ of R will contain the entries $(p-1)x-1$ and $(p-1)x-1+u$.
- The entries in columns 1 to u of $T_{x-1,x+u}$ must be drawn from the set $\{0,1,\ldots, u-1, x+u-1\}$. The entry $x+u-1$ in $T_{x-1,x+u}$ will be mapped to the entry $(p-1)x-1+u$ in column $n-x-1+u$ of R and the remaining entries $k \in \{0,1,\ldots,u-1\}$ will be mapped to the entries $(p-1)x+u+k$ in columns $n-x$ to $n-x-1+u$ of R.
- Any entry $k \in \{0,1,\ldots,x-1\}$ in columns $u+1$ to x of $T_{x-1,x+u}$ will be mapped to the entry $(p-1)x+u+k$ in columns $n-x+u$ to $n-1$ of R.

Now define $I_{n-1-x,n}$ to be the set

$$\begin{array}{rr} \{(0, n-1-x; n-1-x), & (0, n-1; n-1), \\ (x, n-1-x; n-1), & (x, n-1; x-1), \\ (2x, n-1-x; x-1), & (2x, n-1; 2x-1), \end{array}$$

$$\vdots$$

$$((p-1)x, n-1-x; (p-2)x-1), \qquad ((p-1)x, n-1; (p-1)x-1)\}$$

$$\cup \qquad R.$$

To prove that $I_{n-1-x,n}$ is a latin interchange the disjoint mate $I'_{n-1-x,n}$ of $I_{n-1-x,n}$ is identified. This is achieved by defining a set R' as follows. Take cell $((p-1)x+j+1, n-x-1+i)$ of R, for some i,j. This cell corresponds to cell (j,i) in $T_{x-1,x+u}$ and cell (j,i) of $T'_{x-1,x+u}$. Assume element k' occurs in cell (j,i) of $T'_{x-1,x+u}$. The partial latin squares $T_{x-1,x+u}$ and $T'_{x-1,x+u}$ are mutually balanced, therefore there exists an i' such that k' occurs in cell (j,i') of $T_{x-1,x+u}$. Since R is contained in a back circulant latin square entry $(p-2)x+i'+j$ must occur in cell $((p-1)x+j+1, n-x-1+i')$ of $I_{n-1-x,n}$. The entry $(p-2)x+i'+j$ is now placed in cell $((p-1)x+j+1, n-x-1+i)$ of R'. Repeat this process for each cell of R and define $I'_{n-1-x,n}$ to be the set

$$\{(0, n-1-x; n-1), \qquad (0, n-1; n-1-x),$$
$$(x, n-1-x; x-1), \qquad (x, n-1; n-1),$$
$$(2x, n-1-x; 2x-1), \qquad (2x, n-1; x-1),$$
$$\vdots$$
$$((p-1)x, n-1-x; (p-1)x-1), \qquad ((p-1)x, n-1; (p-2)x-1)\}$$
$$\cup \qquad R'.$$

Then $I_{n-1-x,n}$ and $I'_{n-1-x,n}$ will certainly have the same size and shape. Since $T_{x-1,x+u}$ and $T'_{x-1,x+u}$ are disjoint and mutually balanced, it follows that $I_{n-1-x,n}$ and $I'_{n-1-x,n}$ have the same entries in corresponding rows and are disjoint in these rows. Finally, one needs to check that $I_{n-1-x,n}$ and $I'_{n-1-x,n}$ have the same entries in their corresponding columns. Consider column $n-1-x$ of $I'_{n-1-x,n}$. It is easy to see that it contains the entries $n-1,\ x-1,\ 2x-1, \ldots, (p-1)x-1$. Therefore one need only show that it also contains the entries $n-1-x$ and $(p-1)x-1+u$. The entry $n-1-x$ occurred in cell $(n-x, n-1)$ of $I_{n-1-x,n}$ and its corresponding entry in $T_{x-1,x+u}$ was the entry $x-1$ in cell $(x+u-1, x)$. Now since $T_{x-1,x+u}$ and $T'_{x-1,x+u}$ are mutually balanced and the only entries in column 0 of $T_{x-1,x+u}$ are $x+u-1$ and $x-1$, it follows that $x-1$ must occur in cell $(x+u-1, 0)$ of $T'_{x-1,x+u}$. Thus entry $n-1-x$ must occur in cell $(n-x, n-1-x)$ of $I'_{n-1-x,n}$. A similar argument verifies that $(p-1)x-1+u$ must occur in cell $(px, n-1-x)$ of $I'_{n-1-x,n}$. Therefore, $I_{n-1-x,n}$ and $I'_{n-1-x,n}$ have the same entries in column $n-1-x$. Next consider columns c, for $n-x \leq c \leq n-2$. Recall that the entry $(p-1)x+u+k$ has been placed in a cell of R if the corresponding cell in $T_{x-1,x+u}$ contained the entry k, for $k \in \{0, 1, \ldots, x-1\}$. Therefore if k is in cell (r, c) of $T'_{x-1,x+u}$, then $(p-1)x+u+k$ will be in the corresponding cell of $I'_{n-1-x,n}$. Similarly, it can be shown that $(p-1)x-1+u$ occurs in a cell of $I'_{n-1-x,n}$ if the corresponding cell in $T'_{x-1,x+u}$ contained the entry $x+u-1$. Therefore, since $T_{x-1,x+u}$ and $T'_{x-1,x+u}$ are mutually balanced $I_{n-1-x,n}$ and $I'_{n-1-x,n}$ will have the same entries in any particular column c where $n-x \leq c \leq n-2$. Finally, a combination of the above two arguments shows that $I_{n-1-x,n}$ and $I'_{n-1-x,n}$ both contain the same entries in column $n-1$. Thus $I_{n-1-x,n}$ and $I'_{n-1-x,n}$ are mutually balanced and $I_{n-1-x,n}$ is a latin interchange.

Example 1 A partial latin square $I_{10,14}$ which is a latin interchange and satisfies (1) will be constructed. Since $n = 14$ and $n-1-x = 10$, this implies $x = 3$ and $n-x = 11 = 3.3+2$, so $u = 2$. Therefore, a partial latin square $I_{2,5}$, which was constructed earlier, will be needed. Note that it has all the required properties. The transpose of $I_{2,5}$ is

$$T_{2,5} = \{(2,0;2), (2,2;4), (2,3;0), (3,2;0), (3,3;1), (4,0;4), (4,2;1), (4,3;2)\}.$$

Using $p = \lfloor \frac{n-x}{x} \rfloor$, gives $p = \lfloor \frac{14-3}{3} \rfloor = 3$ and so R is taken to be the partial latin square

$$\begin{aligned} R \ = \{ \ & (9,10;5),(9,12;7),(9,13;8),(10,12;8), \\ & (10,13;9),(11,10;7),(11,12;9),(11,13;10)\}. \end{aligned}$$

The set $I_{10,14}$ is taken to be the set

$$\begin{aligned} I_{10,14} = \{ & (0,10;10),(0,13;13),(3,10;13),(3,13;2),(6,10;2),(6,13;5),(9,10;5), \\ & (9,12;7),(9,13;8),(10,12;8),(10,13;9),(11,10;7),(11,12;9),(11,13;10)\}. \end{aligned}$$

This set is displayed in the following table.

$I_{10,14}$	10	11	12	13
0	10			13
3	13			2
6	2			5
9	5		7	8
10			8	9
11	7		9	10

The disjoint mate of the latin interchange $I_{10,14}$ is the set

$$\begin{aligned} I'_{10,14} \ = \ & \{(0,10;13),(0,13;10),(3,10;2),(3,13;13),(6,10;5),(6,13;2),(9,10;7), \\ & (9,12;8),(9,13;5),(10,12;9),(10,13;8),(11,10;10),(11,12;7),(11,13;9)\}. \end{aligned}$$

The cases dealt with by Construction 1 are summarised in the following lemma.

Lemma 6 *Let L be a back circulant latin square of order $n \geq 3$. Assume that for all $m \leq n-1$ and for all x, where $1 \leq x \leq m/2$, there exists latin interchanges $I_{m-1-x,m}$ in a back circulant latin square of order m such that,*

- *if the cell (i,j) of $I_{m-1-x,m}$ is non–empty, then $0 \leq i \leq m-x$ and $m-1-x \leq j \leq m-1$, and*

$$\bullet I_{m-1-x,m} \cap \{(i,j;i+j) \mid i = 0,\ldots,m-2 \text{ and } j = 0,\ldots,m-2-i\} = \{(0,m-1-x;m-1-x)\}.$$

Then for all y, where $2 \leq y \leq n/2$ and $n \not\equiv 0 (\mathrm{mod}\ y)$, there exists latin interchanges $I_{n-1-y,n}$ such that

$$I_{n-1-y,n} \cap \{(i,j;i+j) \mid i = 0,\ldots,n-2 \text{ and } j = 0,\ldots,n-2-i\} = \{(0,n-1-y;n-1-y)\}.$$

Proof.

Let $2 \leq y < n/2$ and $n \equiv u(\text{mod } y)$, where $0 < u < y$. Then $y + u \leq n - 1$. So by the assumption there exists a latin interchange $I_{y-1,y+u}$ in a back circulant latin square of order $y + u$. Now Construction 1 may be used to prove the existence of the latin interchange $I_{n-1-y,n}$.

□

Construction 2

Fix n and take x such that $n/2 < x < n - 1$ and $x \equiv v(\text{mod } n - x)$, where $0 < v \leq (n-x)/2$. Let L be a back circulant latin square of order n. It will be shown that there exists a partial latin square $I_{n-1-x,n}$ in L which is a latin interchange and is such that $I_{n-1-x,n} \cap A = \{(0, n-1-x; n-1-x)\}$.

Let $p = \lfloor \frac{x}{n-x} \rfloor$. Assume there exists a partial latin square $I_{n-x-1-v,n-x}$ in a back circulant latin square of order $n-x$, which is a latin interchange and has the following properties.

- If the cell (i, j) of $I_{n-x-1-v,n-x}$ is non-empty, then $0 \leq i \leq n - x - v$ and $n - x - 1 - v \leq j \leq n - x - 1$, and

- $I_{n-x-1-v,n-x} \cap \{(i, j; i + j) \mid i = 0, \ldots n - x - 2 \text{ and } j = 0, \ldots, n - x - 2 - i\}$
$$= \{(0, n - x - 1 - v; n - x - 1 - v)\}. \quad (3)$$

Set R equal to the set

$$R = \{(i + v, x + j; x + i + j + v) \mid (i, j; k) \in I_{n-x-1-v,n-x},\ \exists k\},$$

where arithmetic is done modulo n. Using (3) it may be deduced that R has the following structure.

- Row 0 of $I_{n-x-1-v,n-x}$ contains the two entries $n - x - 1 - v$ and $n - x - 1$. These entries are mapped to the entries $n - 1$ and $v - 1$, respectively, in row v of R.

- The entries in rows 1 to v of $I_{n-x-1-v,n-x}$ must be drawn from the set $\{0, 1, \ldots, v - 1, n - x - 1\}$. The entry $n - x - 1$ will be mapped to the entry $v - 1$ in R and the remaining entries $k \in \{0, 1, \ldots, v - 1\}$ will be mapped to the entries $k + v$ in R.

- Any entry k in rows $v + 1$ to $n - x - v$ of $I_{n-x-1-v,n-x}$ will be mapped to the entry $k + v$ of R.

Now let $I_{n-1-x,n}$ be the set

$$\begin{array}{rcl} \{(0, n-1-x; n-1-x), & & (0, n-1; n-1)\} \\ \cup & R & \cup \\ \{(v-x, n-1-v+x; n-1), & & (v-x, n-1-v; n-1-x), \\ (v-2x, n-1-v+2x; n-1), & & (v-2x, n-1-v+x; n-1-x), \\ & \vdots & \\ (v-px, n-1-v+px; n-1), & & (v-px, n-1-v+(p-1)x; n-1-x)\}. \end{array}$$

(Note that the calculations above are taken modulo n.)

A partial latin square R' is constructed as in Construction 1. Take cell $(i+v, x+j)$ of R, for some i, j. This cell corresponds to cell (i, j) in $I_{n-1-x-v,n-x}$ and cell (i, j) of $I'_{n-1-x-v,n-x}$, the disjoint mate of $I_{n-1-x-v,n-x}$. Assume element k' occurs in cell (i, j) of $I'_{n-1-x-v,n-x}$. There must exist a column j' such that k' occurs in cell (i, j') of $I_{n-x-1-v,n-x}$. Since R is contained in a back circulant latin square entry $i+v+j'+x$ must occur in cell $(i+v, j'+x)$ of $I_{n-1-x,n}$. The entry $i+v+j'+x$ is now placed in cell $(i+v, j+x)$ of R'. This process is repeated for each cell of R and $I'_{n-1-x,n}$ is defined to be the set

$$\begin{array}{rcl} \{(0, n-1-x; n-1), & & (0, n-1; n-1-x)\} \\ \cup & R' & \cup \\ \{(v-x, n-1-v+x; n-1-x), & & (v-x, n-1-v; n-1), \\ (v-2x, n-1-v+2x; n-1-x), & & (v-2x, n-1-v+x; n-1), \\ & \vdots & \\ (v-px, n-1-v+px; n-1-x), & & (v-px, n-1-v+(p-1)x; n-1)\}. \end{array}$$

It follows that $I_{n-1-x,n}$ and $I'_{n-1-x,n}$ have the same size and shape and are disjoint. In addition, one may use a similar argument to that used in Construction 1 to show that they have the same entries in corresponding rows and columns. Hence $I_{n-1-x,n}$ is a latin interchange which satisfies (1).

The example below illustrates this construction.

Example 2 A partial latin square $I_{4,17}$ in a back circulant latin square of order 17, which is a latin interchange and satisfies (1) will be constructed. Since $n = 17$ and $n-1-x = 4$, it follows that $x = 12$. From the equation $x \equiv v (\mathrm{mod}\ n-x)$ it may be deduced that $v = 2$ and since $p = \lfloor \frac{x}{n-x} \rfloor$, $p = 2$. It has been shown that there exists

a latin interchange $I_{2,5}$ which satisfies (1). So let

$$R = \{(2,14;16),(2,16;1),(4,14;1),(4,15;2),(4,16;3),(5,14;2),(5,15;3),(5,16;4)\}$$

and

$$\begin{aligned} I_{4,17} = \{ & (0,4;4),(0,16;16),(2,14;16),(2,16;1),(4,14;1),(4,15;2),(4,16;3), \\ & (5,14;2),(5,15;3),(5,16;4),(7,9;16),(7,14;4),(12,4;16),(12,9;4)\}. \end{aligned}$$

This set is displayed in the following table.

$I_{4,17}$	4	9	14	15	16
0	4				16
2			16		1
4			1	2	3
5			2	3	4
7		16	4		
12	16	4			

Then

$$R' = \{(2,14;1),(2,16;16),(4,14;2),(4,15;3),(4,16;1),(5,14;4),(5,15;2),(5,16;3)\}$$

and

$$\begin{aligned} I'_{4,17} = \{ & (0,4;16),(0,16;4),(2,14;1),(2,16;16),(4,14;2),(4,15;3),(4,16;1), \\ & (5,14;4),(5,15;2),(5,16;3),(7,9;4),(7,14;16),(12,4;4),(12,9;16)\}. \end{aligned}$$

The cases covered by this construction are summarised in the following lemma.

Lemma 7 *Let L be a back circulant latin square of order $n \geq 3$. Assume that for all $m \leq n-1$ and for all x, where $1 \leq x \leq m/2$, there exists latin interchanges $I_{m-1-x,m}$ in a back circulant latin square of order m such that,*

- *if the cell (i,j) of $I_{m-1-x,m}$ is non–empty, then $0 \leq i \leq m-x$ and $m-1-x \leq j \leq m-1$, and*

- $I_{m-1-x,m} \cap \{(i,j;i+j) \mid i = 0,\ldots,m-2 \text{ and } j = 0,\ldots,m-2-i\} = \{(0,m-1-x;m-1-x)\}.$

Then for all y satisfying the conditions, $n/2 < y < n-1$ and $y = w(n-y)+v$, where w and v are positive integers and $0 < v \leq (n-y)/2$, there exists a partial latin square $I_{n-1-y,n}$ which is a latin interchange and is such that

$$I_{n-1-y,n} \cap \{(i,j;i+j) \mid i = 0,\ldots,n-2 \text{ and } j = 0,\ldots,n-2-i\} = \{(0,n-1-y;n-1-y)\}.$$

Proof.

Let $n/2 < y < n-1$ and $y \equiv v(\text{mod } n-y)$, where $0 < v \leq (n-y)/2$. Then $n-y \leq n-1$. So by the assumption there exists a latin interchange $I_{n-y-1-v,n-y}$ in a back circulant latin square of order $n-y$. Now Construction 2 may be used to prove the existence of the latin interchange $I_{n-1-y,n}$.

□

Construction 3

Fix n and take x such that $n/2 < x < n-1$ and $x \equiv v(\text{mod } n-x)$, where $v > (n-x)/2$. Let L be a back circulant latin square of order n. It will be shown that there exists a partial latin square $I_{n-1-x,n}$ which is a latin interchange and is such that $I_{n-1-x,n} \cap A = \{(0, n-1-x; n-1-x)\}$.

Let $p = \lfloor \frac{x}{n-x} \rfloor$. Assume there exists a partial latin square $I_{v-1,n-x}$ in a back circulant latin square of order $n-x$, which is an latin interchange and has the following properties.

- If the cell (i,j) of $I_{v-1,n-x}$ is non-empty, then $0 \leq i \leq v$ and $v-1 \leq j \leq n-x-1$, and

- $I_{v-1,n-x} \cap \{(i,j;i+j) \mid i = 0, \ldots n-x-2 \text{ and } j = 0, \ldots, n-x-2-i\}$
$= \{(0, v-1; v-1)\}$.

Then its transpose $T_{v-1,n-x}$ is a latin interchange which satisfies the condition

$$T_{v-1,n-x} \cap \{(i,j;i+j) \mid i = 0, \ldots n-x-2 \text{ and } j = 0, \ldots, n-x-2-i\} = \{(v-1, 0; v-1)\}. \quad (4)$$

Define R as follows.

$$R = \{(j+1, i-1-v; i+j-v) \mid (j,i;k) \in T_{v-1,n-x}\}.$$

Take $I_{n-1-x,n}$ to be the set

$$\begin{array}{rcl} \{(0, n-1-x; n-1-x), & & (0, n-1; n-1)\} \\ \cup & R & \cup \\ \{(v-x, n-1-v; n-1-x), & & (v-x, n-1+x-v; n-1), \\ (v-2x, n-1-v+x; n-1-x), & & (v-2x, n-1-v+2x; n-1), \\ \vdots & & \\ (v-px, n-1-v+(p-1)x; n-1-x), & & (v-px, n-1-v+px; n-1)\}. \end{array}$$

The partial latin square R' is constructed as in Construction 1 and take $I'_{n-1-x,n}$ to be the set

$$\begin{array}{rcl} \{(0, n-1-x; n-1), & & (0, n-1; n-1-x)\} \\ \cup & R' & \cup \\ \{(v-x, n-1-v; n-1), & & (v-x, n-1+x-v; n-1-x), \\ (v-2x, n-1-v+x; n-1), & & (v-2x, n-1-v+2x; n-1-x), \\ \vdots & & \\ (v-px, n-1-v+(p-1)x; n-1), & & (v-px, n-1-v+px; n-1-x)\}. \end{array}$$

As in Construction 1 it can be verified that $I_{n-1-x,n}$ is a latin interchange which satisfies (1).

The cases covered by this construction are summarised in the following lemma.

Lemma 8 *Let L be a back circulant latin square of order $n \geq 3$. Assume that for all $m \leq n-1$ and for all x, where $1 \leq x \leq m/2$, there exists latin interchanges $I_{m-1-x,m}$ in a back circulant latin square of order m such that,*

- *if the cell (i,j) of $I_{m-1-x,m}$ is non-empty, then $0 \leq i \leq m-x$ and $m-1-x \leq j \leq m-1$, and*

$$\bullet I_{m-1-x,m} \cap \{(i,j;i+j) \mid i = 0, \ldots, m-2 \text{ and } j = 0, \ldots, m-2-i\} = \{(0, m-1-x; m-1-x)\}.$$

Then for all y satisfying the conditions, $n/2 < y < n-1$ and $y = w(n-y)+v$, where w and v are positive integers and $(n-y)/2 < v < n-y$, there exists a partial latin square $I_{n-1-y,n}$ which is a latin interchange and is such that

$$I_{n-1-y,n} \cap \{(i,j;i+j) \mid i = 0, \ldots, n-2 \text{ and } j = 0, \ldots, n-2-i\} = \{(0, n-1-y; n-1-y)\}.$$

Proof.

Let $n/2 < y < n-1$ and $y \equiv v (\text{mod } n-y)$, where $(n-y)/2 < v < n-y$. Then $n-y \leq n-1$. So by the assumption there exists a latin interchange $I_{v-1,n-y}$ in a back circulant latin square of order $n-y$. Now Construction 3 may be used to prove the existence of the latin interchange $I_{n-1-y,n}$.

□

The results of Lemmas 5, 6, 7 and 8 are brought together in Lemma 9.

Lemma 9 *Let L be a back circulant latin square of order $n \geq 3$. Assume that for all $m \leq n-1$ and for all x, where $1 \leq x \leq m/2$, there exists latin interchanges $I_{m-1-x,m}$ in a back circulant latin square of order m such that*

- *if the cell (i,j) of $I_{m-1-x,m}$ is non–empty, then $0 \leq i \leq m-x$ and $m-1-x \leq j \leq m-1$, and*

- $I_{m-1-x,m} \cap \{(i,j;i+j) \mid i = 0,\ldots,m-2 \text{ and } j = 0,\ldots,m-2-i\} = \{(0,m-1-x;m-1-x)\}$.

Then for all y, where $1 \leq y \leq n-1$, there exists latin interchanges $I_{n-1-y,n}$ such that

$$I_{n-1-y,n} \cap \{(i,j;i+j) \mid i = 0,\ldots,n-2 \text{ and } j = 0,\ldots,n-2-i\} = \{(0,n-1-y;n-1-y)\}.$$

Proof. If $y = 1$ or $n-1$, then the result follows directly from Lemma 5. The result also follows from Lemma 5 if n is divisible by y, or y is divisible by $n-y$.

So assume that none of the above hold. If $2 \leq y \leq n/2$, then the result follows from Lemma 6 and if $n/2 < y < n-1$ then the result follows from Lemmas 7 and 8.

□

These results lead to the proof of the following theorem.

Theorem 1 *Let L be a back circulant latin square of order n and*

$$A = \{(i,j;i+j) \mid i = 0,\ldots,n-2 \text{ and } j = 0,\ldots,n-2-i\}.$$

Then for each x, where $1 \leq x \leq n-1$, there exists a partial latin square $I_{n-1-x,n}$ in L which is a latin interchange and is such that

$$A \cap I_{n-1-x,n} = \{(0,n-1-x;n-1-x)\}.$$

Proof. The initial cases given in this section together with the above lemma can be used to prove this result.

□

4 A New Family of Critical Sets

The constructions and proofs given in the previous two sections lead to the main theorem of this paper.

Theorem 2 *Let L be a back circulant latin square of order n and let*

$$A = \{(i, j; i + j) \mid i = 0, \ldots, n-2 \text{ and } j = 0, \ldots, n-2-i\}.$$

Then A is a critical set in L.

Proof. In order to prove that A is a critical set it must be shown that A has a unique completion to L and that any proper subset of A has at least two completions.

Lemma 4 verifies that A has a unique completion to a back circulant latin square of order n.

Assume that the element $(0, c; c)$ is removed from A. In Section 3, it was shown that there exists a partial latin square $I_{c,n}$, which is a latin interchange and is such that $A \cap I_{c,n} = \{(0, c; c)\}$. Therefore the set $A \setminus \{(0, c; c)\}$ has at least two completions, L and $(L \setminus I_{c,n}) \cup I'_{c,n}$ where $I'_{c,n}$ is a disjoint mate of $I_{c,n}$. If $c \geq \lfloor (n-1)/2 \rfloor$, then the entries of $I_{c,n}$ occur in rows 0 to $c+1$. Therefore, by Lemma 3 for each s, where $1 \leq s \leq n-c-2$,

$$\{(i + s, j; i + j + s) \mid (i, j; k) \in I_{c,n}\}$$

is a latin interchange which intersects A in the unique entry $(s, c; s + c)$. If $c < \lfloor (n-1)/2 \rfloor$, then the entries of $I_{c,n}$ occur in rows 0 to $n-c-1$. Therefore, by Lemma 3 for each s, where $1 \leq s \leq c$,

$$\{(i + s, j; i + j + s) \mid (i, j; k) \in I_{c,n}\}$$

is a latin interchange which intersects A in the unique entry $(s, c; s + c)$.

It has been shown that the entries of any one of the entries $(i, j; i + j)$, where $i = 0, \ldots, \lfloor n/2 - 1 \rfloor$ and $j = i, \ldots, n-2-i$, is removed from A the remaining partial latin square has at least two completions. Now by Lemma 2 the transpose of each of these latin interchanges is a latin interchange and so if one removes any one of the entries $(j, i; i + j)$, where $i = 0, \ldots, \lfloor n/2 - 1 \rfloor$ and $j = i, \ldots, n-2-i$, from A the remaining partial latin square has at least two completions.

It has been shown that if any entry from A is removed the resulting partial latin square has at least two completion. Thus A is a critical set.

□

Theorem 3 *Let L be a back circulant latin square of order n and, for some r, where $\frac{n-3}{2} \leq r \leq n-2$, let*

$$\begin{aligned} B \;=\; & \{(i, j; i + j) \mid i = 0, \ldots, r \text{ and } j = 0, \ldots, r - i\} \quad \cup \\ & \{(i, j; i + j) \mid i = r + 2, \ldots, n-1 \text{ and } j = r + 1 - i, \ldots, n-1\}. \end{aligned}$$

Then B is a critical set in L.

Proof. Using a similar argument to that used in the proof of Theorem 2 it can be shown that B has a unique completion to a back circulant latin square of order n.

Next consider the entries in the set $\{(i,j;i+j) \mid i=0,\ldots,r \text{ and } j=0,\ldots,r-i\}$ It was shown in the proof of Theorem 2 that for each $(i,j;i+j)$ in this set there exists a latin interchange I such that $I \cap A = \{(i,j;i+j)\}$. The entries in I belong to the set $\{0,\ldots,i+j,n-1\}$, where $i+j$ is taken modulo n. Therefore it follows that $I \cap B = \{(i,j;i+j)\}$.

If n is even, then for each element $(r,c;r+c)$ of L the set $I = \{(r,c;r+c),(r+n/2,c;r+c+n/2),(r,c+n/2;r+c+n/2),(r+n/2,c+n/2;r+c)\}$ is a latin interchange. Further if $(r,c;r+c)$ is an element of the set $\{(i,j;i+j) \mid i=r+2,\ldots,n-1 \text{ and } j=r+1-i,\ldots,n-1\}$, then $I \cap B = \{(r,c;r+c)\}$. (See [**3**].)

If n is odd, then for each element $(r,c;r+c)$ of L the set $I = \{(r,c;r+c),(r-s,c-(n-1)/2+s;r+c-(n-1)/2),(r-s,c-(n+1)/2+s;r+c-(n+1)/2),(r-(n-1)/2,c-(n+1)/2;r+c) \mid s=0,\ldots,(n-1)/2\}$ is a latin interchange. Further if $(r,c;r+c)$ is an element of the set $\{(i,j;i+j) \mid i=r+2,\ldots,n-1 \text{ and } j=r+1-i,\ldots,n-1\}$, then $I \cap B = \{(r,c;r+c)\}$. (See [**1**].)

Consequently if any element is removed from B the remaining partial latin square has at least two completions. Thus B is a critical set.

□

5 Conclusion

In this paper the existence of a new family of critical sets in back circulant latin squares has been established. The importance of identifying large families of latin interchanges has been highlighted and general methods for constructing latin interchanges in back circulant latin squares have been given.

Acknowledgement The authors would like to thank the referees for their suggestions. The first author would like to acknowledge the support of a New Staff Research Grant at the University of Queensland and a Postdoctoral Fellowship at Queensland University Technology. The second author would like to acknowledge the support of an ARC Grant S6600306.

References

[1] Joan Cooper, Diane Donovan and Jennifer Seberry, *Latin squares and critical sets of minimal size*, Australas. J. Combin., **4**, 1991, pp. 113–120.

[2] Joan Cooper, Diane Donovan and Jennifer Seberry, *Secret sharing schemes arising from latin squares*, Bull. Inst. Combin. Applications, (to appear).

[3] D. Curran and G.H.J. van Rees, *Critical sets in latin squares*, Congressus Numerantium, **22**, 1978, pp. 165–168.

[4] Ed Dawson, Diane Donovan and Alan Offer, *Quasigroups, isotopisms and authentications schemes*, (submitted).

[5] Diane Donovan, Joan Cooper, D.J. Nott and Jennifer Seberry, *Latin squares: critical sets and their lower bounds*, Ars Combinatoria, to appear

[6] D. Keedwell, *Critical sets and Critical partial latin squares*, Proc. Third China–USA Internation. Conf. on Graph Theory, Combinatorics, Algorithms and Applications, Beijing, June 1993, (to appear).

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

[8] John Nelder, *Private communications from John Nelder to J. Seberry*, Jan. 1979.

[9] Bohdan Smetaniuk, *On the minimal critical set of a latin square*, **16**, Utilitas Math., 1979, pp. 97–100.

[10] D.R. Stinson and G.H.J. van Rees, *Some large critical sets*, Congressus Numerantium, **34**, 1982, pp. 441–456.

Centre for Combinatorics,
Mathematics Department,
The University of Queensland,
Brisbane, 4072, Australia,

and

Department of Information and
Communication Technology,
University of Wollongong,
Wollongong, 2500, Australia.