

# LATIN TRADE ALGORITHMS AND THE SMALLEST CRITICAL SET IN A LATIN SQUARE

NICHOLAS J. CAVENAGH  
CENTRE FOR DISCRETE MATHEMATICS AND COMPUTING  
DEPARTMENT OF MATHEMATICS  
THE UNIVERSITY OF QUEENSLAND  
QUEENSLAND 4072  
AUSTRALIA

Abstract: A critical set is a partial Latin square that has a unique completion to a Latin square, and is minimal in this property. Suppose that  $P$  is a critical set in a Latin square  $L$  of order  $n$ , and there is one row of  $P$  which is empty. Then there are at most two rows of  $P$  with precisely one entry, and  $|P| \geq 2n - 4$ . Moreover, in this case these three rows in  $L$  are isoptopic to three adjacent rows in the back circulant Latin square. In our proof new algorithms for Latin trades in arbitrary Latin squares are given.

## 1. INTRODUCTION

In any combinatorial configuration it is possible to identify a subset which uniquely determines the structure of the configuration and in some cases is minimal with respect to this property. Examples of such subsets can be found by studying the literature on critical sets in Latin squares (see Donovan and Howse [8]) and defining sets in block designs (see Street [10]). The recent research in these areas has focused on building a bank of knowledge which may be used to determine the spectrum of the prescribed subsets. With this current paper we restrict ourselves to a discussion of critical sets in Latin squares.

We define  $scs(n)$  to be the size of the smallest critical set in any Latin square of order  $n$ . The problem of determining this value exactly for every  $n$  remains unsolved. However, progress has been made on upper and lower bounds.

Fu, Fu and Rodger ([9]) showed that if  $n > 20$ ,  $scs(n) \geq \lfloor (7n-3)/6 \rfloor$ . The smallest critical set so far constructed for any Latin square of size  $n$  has size  $\lfloor n^2/4 \rfloor$  ([6], [5]). A critical set of such size is known to exist in back circulant Latin squares, namely those Latin squares based on the addition table for the integers modulo  $n$ .

Donovan, Cooper, Nott and Seberry ([7]) examined lower bounds for critical sets of Latin squares based on certain groups. Bate and van Rees ([3]) showed that the size of the smallest strong critical set (a critical set with a certain type of completion) is  $\lfloor n^2/4 \rfloor$ .

Proving the existence of critical sets often involves the construction of many Latin trades (see, for example [4] and [8]). In this paper we give algorithms that construct Latin trades in sets of 3 rows in Latin squares.

We then use these Latin trades to show that if  $P$  is a critical set with one empty row (or column or entry), there are at most two rows (or columns or entries) of  $P$  with exactly

one element. It follows that if  $P$  has an empty row (or column or entry),  $|P| \geq 2n - 4$ . Next, if  $P$  has one empty row (or column or entry) and two rows (or columns or entries) with exactly one element, these three columns are isotopic to three adjacent columns in the back circulant Latin square. This result adds further weight to the conjecture that the back circulant Latin square yields the smallest possible critical set for a given order.

## 2. DEFINITIONS

We start with basic definitions which allow us to state and prove our main results.

Let  $N = \{0, 1, 2, \dots, n - 1\}$ . A *partial Latin square* (*partial quasigroup*)  $P$  of order  $n$  is a set of ordered triples of the form  $(i, j, k)$ , where  $i, j, k \in N$  with the following properties:

- if  $(i, j, k) \in P$  and  $(i, j, k') \in P$  then  $k = k'$ ,
- if  $(i, j, k) \in P$  and  $(i, j', k) \in P$  then  $j = j'$  and
- if  $(i, j, k) \in P$  and  $(i', j, k) \in P$  then  $i = i'$ .

If  $(i, j, k) \in P$  we say that  $i \circ j = k$ ,  $j = i \setminus k$  and  $i = k / j$ . We may also represent a partial Latin square  $P$  as an  $n \times n$  array with entries chosen from the set  $N$  such that if  $(i, j, k) \in P$ , the *entry*  $k$  occurs in cell  $(i, j)$ . At any given point in this paper we endeavour to use the representation that makes our explanation clearest.

It is important for the reader to note that an *element* of  $P$  is a triple  $(i, j, k) \in P$ , whereas an *entry* in  $P$  is an integer  $k \in N$  such that  $(i, j, k) \in P$ , for some  $i$  and  $j$ . A partial Latin square has the property that each entry occurs at most once in each row and at most once in each column.

Every partial Latin square has six *conjugates* (five and itself). In this paper we will make use of the conjugates

- $\{(k, j, i) \mid (i, j, k) \in P\}$ , and
- $\{(i, k, j) \mid (i, j, k) \in P\}$ .

Because of the existence of these conjugates, statements made about the columns of a partial Latin square may also be made about its rows, and in turn, entries.

If all the cells of the array are filled then the partial Latin square is termed a Latin square. That is, a *Latin square*  $L$  of order  $n$  is an  $n \times n$  array with entries chosen from the set  $N = \{0, 1, 2, \dots, n - 1\}$  in such a way that each element of  $N$  occurs precisely once in each row and precisely once in each column of the array.

For a given partial Latin square  $P$  the set of cells  $\mathcal{S}_P = \{(i, j) \mid (i, j, k) \in P, \text{ for some } k \in N\}$  is said to determine the *shape* of  $P$  and  $|\mathcal{S}_P|$  is said to be the *size* of the partial Latin square. That is, the size of  $P$  is the number of non-empty cells in the array. For each  $r$ ,  $1 \leq r \leq n$ , let  $\mathcal{R}_P^r$  denote the set of entries occurring in row  $r$  of  $P$ . Formally,  $\mathcal{R}_P^r = \{k \mid (r, j, k) \in P\}$ . Similarly, for each  $c$ ,  $1 \leq c \leq n$ , we define  $\mathcal{C}_P^c = \{k \mid (i, c, k) \in P\}$ .

A partial Latin square  $T$  of order  $n$  is said to be a *Latin trade* (or *Latin interchange*) if  $T \neq \emptyset$  and there exists a partial Latin square  $T'$  (called a *disjoint mate* of  $T$ ) of order  $n$ , such that

- $\mathcal{S}_T = \mathcal{S}_{T'}$ ,
- if  $(i, j, k) \in T$  and  $(i, j, k') \in T'$ , then  $k \neq k'$ ,
- for each  $r$ ,  $1 \leq r \leq n$ ,  $\mathcal{R}_T^r = \mathcal{R}_{T'}^r$ , (the row  $r$  is *balanced*) and
- for each  $c$ ,  $1 \leq c \leq n$ ,  $\mathcal{C}_T^c = \mathcal{C}_{T'}^c$  (the column  $c$  is *balanced*).

A *critical set* in a Latin square  $L$  (of order  $n$ ) is a partial Latin square  $P \subseteq L$ , such that

- (1)  $L$  is the only Latin square of order  $n$  which has element  $k$  in cell  $(i, j)$  for each  $(i, j, k) \in P$ ; and  
(2) no proper subset of  $P$  satisfies (1).

If  $P$  is a critical set in a Latin square  $L$ ,  $P$  must intersect every Latin trade in  $L$ . (For if there exists a Latin trade  $T$  in  $L$  such that  $P \cap T = \emptyset$ ,  $P$  is also contained in the Latin square  $(L \setminus T) \cup T'$ , where  $T'$  is a disjoint mate of  $T$ . Every pair of rows, columns or entries in a Latin square gives rise to at least one Latin trade (formed by exchanging the row, column or entry symbols respectively). Thus any critical set may have at most one empty column, at most one empty row, and at most one missing entry.

If  $P$  is a critical set in a Latin square  $L$ , the partial Latin square given by  $L \setminus P$  is called the *compliment* of  $P$  and is denoted by  $P^C$ .

We define  $P_n$  to be the following partial Latin square contained in the back circulant square  $B_n$ :

$$P_n = \{(i, j, i + j) \mid n - 1 - i \geq j > n/2\} \cup \{(i, j, i + j - n) \mid n/2 \geq j \geq n - i\}.$$

It is shown in ([6],[5]) that  $P_n$  is a critical set in  $B_n$ . Observe that  $|P_n| = \lfloor n^2/4 \rfloor$ .

**Example 1.** The partial Latin square  $P_7$  is given in Figure 1, together with the Latin square  $B_7$ .

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

$P_7$

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

$B_7$

**Figure 1**

Two partial Latin squares  $P$  and  $Q$  are said to be *isotopic* if there exist three permutations  $\alpha, \beta$  and  $\gamma$  of the set  $N$  such that  $(i, j, k) \in P$  if and only if  $(\alpha(i), \beta(j), \gamma(k)) \in Q$ . Many properties of partial Latin squares are preserved under isotopism. For example if  $P$  is a critical set and  $Q$  is isotopic to  $P$ , then  $Q$  is also a critical set. We make use of this fact in this paper.

### 3. LATIN TRADE CONSTRUCTIONS

Consider the following Latin trade  $T$ , with disjoint mate  $T'$ :

0	1	2					8	9	3
1	2	3	0	5	6	7			
			5	6	7	3	0	8	9

1	2	3					0	8	9
0	1	2	5	6	7	3			
			0	5	6	7	8	9	3

Note that it is made up of three “zig-zagging” sequences between pairs of rows, each beginning with entry 0 and ending with entry 3. It is this simple idea we extend in this section to construct Latin trades from sets of three rows in Latin squares.

We begin with a convenient lemma on Latin trades.

**Lemma 2.** Let  $x \in N$ , and let  $P$  and  $P'$  be two partial Latin squares with the same shape, the same size and with the following properties:

- if  $(i, j, k) \in P$  and  $(i, j, k') \in P'$  then  $k \neq k'$ ;
- for every  $c$ ,  $1 \leq c \leq n - 1$ , column  $c$  is balanced;
- for every  $r$ ,  $r \in \{0, 1, \dots, n - 1\} \setminus \{x\}$ , row  $r$  is balanced.

Then  $P$  is a Latin trade with disjoint mate  $P'$ .

*Proof.* Let  $(x, j, k) \in P$ . Because column  $j$  is balanced, there exists  $(x', j, k) \in P'$ . Now suppose there are  $m$  occurrences of the entry  $k$  in  $P$ . Then there will also be  $m$  occurrences of  $k$  in  $P'$ , since every column is balanced. There are  $m - 1$  occurrences of the entry  $k$  in  $P$  in the set of rows excluding  $x$ , so there must be  $m - 1$  occurrences of the entry  $k$  in the same set of rows in  $P'$ . Thus there must be an element  $(x, j', k) \in P'$ .  $\square$

Any two rows (or columns or entries)  $x$  and  $y$  in a Latin square  $L$  of order  $n$  give rise to a permutation  $\rho_{x,y}$  of the set  $N = \{0, 1, \dots, n - 1\}$ , defined as follows. If there exists column  $c$  such that  $x \circ c = i$  and  $y \circ c = j$ , then  $\rho_{x,y}(i) = j = (y \circ (x \setminus i))$ . From this point we focus on three rows which we label arbitrarily 0, 1 and  $n - 1$ . (The reason for this labelling becomes apparent in Theorem 6.) Let  $\alpha = \rho_{0,1}$ ,  $\beta = \rho_{1,n-1}$  and  $\gamma = \rho_{n-1,0}$ . In this section we often use an asterisk “\*” to denote an arbitrary column. In these cases the column is uniquely determined by a row and entry. (In the ordered triple  $(i, j, k)$ ,  $j = i \setminus k$ .)

**Theorem 3.** Suppose there exist distinct entries  $e_1$  and  $e_2$  such that

1.  $\alpha^p(e_1) = e_2$  and  $\beta^q(e_1) = e_2$  where  $1 \leq p, q, \leq n - 1$ , and
2.  $\alpha^g(e_1) \neq \beta^h(e_1)$ , for all  $0 \leq g < p$ ,  $0 \leq h < q$ , except  $(g, h) = (0, 0)$ .

(Note that  $\alpha^0$  and  $\beta^0$  are the identity permutation.) Then there exist two Latin trades  $T_1$  and  $T_2$  such that  $T_1 \cap T_2 = S$ , where

$$S = \{(0, *, \alpha^g(e_1)), (1, *, \alpha^{g+1}(e_1)) \mid 0 \leq g < p\} \\ \cup \{(1, *, \beta^h(e_1)), (n - 1, *, \beta^{h+1}(e_1)) \mid 0 \leq h < q\},$$

and if  $(r, c, e) \in (T_1 \cup T_2) \setminus S$ , then  $r \neq 1$ .

*Proof.* We first illustrate the set  $S$  as a partial Latin square in the following diagram. (Note that because of Condition 2 there are  $p + q$  distinct columns altogether.)

0	$e_1$	$\alpha(e_1)$	.....	$\alpha^{p-1}(e_1)$				
1	$\alpha(e_1)$	$\alpha^2(e_1)$	.....	$\alpha^p(e_1) = e_2$	$e_1$	$\beta(e_1)$	.....	$\beta^{q-1}(e_1)$
$n - 1$					$\beta(e_1)$	$\beta^2(e_1)$	.....	$\beta^q(e_1) = e_2$

We write algorithms to construct Latin trades  $T_1$  and  $T_2$  in pseudo-code.

**Algorithm to construct  $T_1$ .**

- (1) let  $x = e_1$  and  $T_1 = S$ .
- (2) while  $x \neq e_2$  :
- (3) let  $T_1 := T_1 \cup \{(n-1, *, x)\}$ .
- (4) if  $\gamma(x) = \alpha^y(e_1)$ , for some  $y$  where  $0 \leq y \leq p-1$ ,
- (5) then let  $x = \alpha(\gamma(x))$ .
- (6) else
- (7) let  $T_1 := T_1 \cup \{(0, *, \gamma(x))\}$  and let  $x := \gamma(x)$ .
- (8) while  $x = \beta^y(e_1)$  for some  $y$  where  $1 \leq y \leq q-1$ ,
- (9) let  $T_1 := T_1 \cup \{(0, *, \gamma(\beta(x)))\}$  and
- (10) let  $x := \gamma(\beta(x))$ .

**Algorithm to construct  $T_2$ .**

To construct  $T_2$ , we begin at line 7 of the algorithm for  $T_1$  with  $T_1 = S$  and  $x = \beta(e_1)$  and proceed as above.

We now justify why these algorithms meet the conditions of the theorem. (Readers are encouraged to look ahead to Example 4 to analyse a specific construction.) We make the following claims:

- Claim 1. Let  $(i, j, k) \in (T_1 \cup T_2) \setminus (S \cup \{(n-1, *, e_1), (0, *, \gamma(\beta(e_1)))\})$ . Then the triple  $(i', j', k')$  inserted directly before  $(i, j, k)$  in either algorithm is unique.
- Claim 2. The triple  $(n-1, *, e_1)$  is inserted only once in the algorithm for  $T_1$  and never in the algorithm for  $T_2$ .
- Claim 3. The triple  $(0, *, \gamma(\beta(e_1)))$  is inserted only once in the algorithm for  $T_2$  and never in the algorithm for  $T_1$ .
- Claim 4. The algorithms for  $T_1$  and  $T_2$  both terminate.
- Claim 5.  $T_1 \cap T_2 = S$ .
- Claim 6. The partial Latin squares  $T_1$  and  $T_2$  are Latin trades.

Observe that both algorithms only add entries to row 0 or row  $n-1$ .

**Claim 1** Let  $(i', j', k')$  be inserted directly before  $(i, j, k)$  in the algorithm.

**Case 1:**  $i = n-1$ . Then  $(i, j, k)$  is added at line 3 of the algorithm. If  $k = \alpha^g(e_1)$ , for some  $1 \leq g \leq p-1$ , then  $(i', j', k') = (n-1, *, \beta(\alpha^g(e_1)))$ . Otherwise  $(i', j', k') = (0, *, k)$ .

**Case 2:**  $i = 0$ . Then  $(i, j, k)$  is added at either line 7 or line 9 of the algorithm. If  $k = \gamma(\beta^h(e_1))$ , for some  $2 \leq h \leq q-1$ , then  $(i', j', k') = (0, *, \beta^{h-1}(e_1))$ . Otherwise  $(i', j', k') = (n-1, *, \beta(\alpha(k)))$ .

**Claim 2** Suppose that Claim 2 is false, and there is a triple  $(i', j', k')$  added directly before  $(n-1, *, e_1)$  in either the algorithm for  $T_1$  or the algorithm for  $T_2$ . By Case 1 of Claim 1, either  $e_1 = \alpha^g(e_1)$  for some  $1 \leq g \leq p-1$ , or  $(i', j', k') = (0, *, e_1)$ . The former is

impossible by Condition 2 of our theorem, so we must have  $(i', j', k') = (0, *, e_1)$ . Now, we can't have  $e_1 = \gamma(\beta^h(e_1))$  for some  $2 \leq h \leq q-1$  because this implies that  $\alpha(e_1) = \beta^{h-1}(e_1)$  which contradicts Condition 2 of our theorem. Therefore  $(i'', j'', k'') = (n-1, *, \beta(\alpha(e_1)))$ . But let's look at the algorithm in a forward direction for a moment. We add the triple  $(n-1, *, \beta(\alpha(e_1)))$  at line 3, which means we are interrupted by line 4 because  $\gamma(\beta(\alpha(e_1))) = e_1$ . So the *next* element added is  $(n-1, *, \alpha(e_1))$ . In other words,  $(i', j', k') = (n-1, *, \alpha(e_1))$ , a contradiction to the fact that our algorithm is well-defined.

**Claim 3** Suppose the ordered triple  $(0, *, \gamma(\beta(e_1)))$  is preceded by some triple  $(i', j', k')$  inserted at line 3, 7 or 9 of the algorithm. Then  $(0, *, \gamma(\beta(e_1)))$  is inserted at either line 7 or line 9. In the latter case, it is preceded by the triple  $(0, *, e_1)$ . Then we must have  $e_1 = \beta^y(e_1)$  for some  $1 \leq y \leq q-1$ , which contradicts Condition 2 of the theorem. In the former case  $(0, *, \gamma(\beta(e_1)))$  is preceded by the triple  $(n-1, *, \beta(e_1))$  at line 3. This is also impossible as since  $x = \beta(e_1)$ , we are still at line 8 of the algorithm.

**Claim 4** This claim follows directly from Claims 1, 2 and 3.

**Claim 5** We first show that no elements of  $S$  are added to  $T_1$  at lines 3, 7 or 9.

**Case 1:** Suppose we are at line 3 of the algorithm for  $T_1$ . If the triple  $(n-1, *, x) \in S$ , then  $x = \beta^g(e_1)$  for some  $1 \leq g \leq q$ . But if  $g < q$  we are at line 9 rather than line 3, and if  $g = p$ ,  $x = e_2$  and the algorithm has terminated at line 2.

**Case 2:** Next suppose we are at line 7. We cannot have  $\gamma(x) = \alpha^g(e_1)$ , for some  $0 \leq g \leq p-1$  for the following reasons. If  $g = 0$  we will have  $x = e_1$  at the next line 2, contradicting Claim 1b. If  $g > 0$  we are at line 4.

**Case 3:** If we are at line 9 we cannot have  $\gamma(\beta^h(e_1)) = \alpha^g(e_1)$  for some  $0 \leq g \leq p-1$ ,  $2 \leq h \leq q$  because this is equivalent to  $\beta^{h-1}(e_1) = \alpha^{g+1}(e_1)$ , contradicting condition 2 of this theorem.

Next suppose that  $(i, j, k) \in (T_1 \cup T_2) \setminus S$ . Either  $(i, j, k) = (n-1, *, e_1)$ ,  $(i, j, k) = (0, *, \gamma(\beta(e_1)))$ , or by Claim 1 there exists a unique  $(i', j', k')$  inserted directly before  $(i, j, k)$  in the algorithm for  $T_1$ . Let  $f(i, j, k) = (i', j', k')$ . Since the algorithms for  $T_1$  and  $T_2$  terminate (Claim 4) there exist distinct integers  $m_1$  and  $m_2$  such that  $f^{m_1}(i, j, k) = (n-1, *, e_1)$ , and  $f^{m_2}(i, j, k) = (0, *, \gamma(\beta(e_1)))$ . If  $m_1 < m_2$  Claim 2 is contradicted; otherwise  $m_1 > m_2$  and Claim 3 is contradicted.

Therefore  $T_1$  and  $T_2$  intersect only at  $S$ .

**Claim 6** We now prove that  $T_1$  and  $T_2$  are Latin trades by constructing disjoint mates. Let  $T'_1$  ( $T'_2$ ) be a partial Latin square with the same size and shape as  $T_1$  ( $T_2$ ). We fill the cells of  $T'_1$  and  $T'_2$  in the following way. (Note that  $\circ, \setminus$ , are operations corresponding to the quasigroup  $L$  of which  $T_1$  and  $T_2$  are subsets.)

Every column of  $T_1$  ( $T_2$ ) has either 0, 2 or 3 entries. If a column  $j$  has two entries in  $T_1$  ( $T_2$ ), we swap these entries in  $T'_1$  ( $T'_2$ ). Otherwise column  $j$  has three entries. In this case either:

1.  $(0, j, \alpha^{g-1}(e_1)), (1, j, \alpha^g(e_1)), (n-1, j, n-1 \circ j) \in T_1$  ( $T_2$ ) for some  $1 \leq g \leq p$ , or
2.  $(0, j, 0 \circ j), (1, j, \beta^h(e_1)), (n-1, j, \beta^{h+1}(e_1)) \in T_1$  ( $T_2$ ) for some  $0 \leq h \leq q-1$ .

We permute entries as to have the elements

1.  $(0, j, (n-1) \circ j), (1, j, \alpha^{g-1}(e_1)), (n-1, j, \alpha^g(e_1)) \in T'_1 (T'_2)$  or
2.  $(0, j, \beta^h(e_1)), (1, j, \beta^{h+1}(e_1)), (n-1, j, 0 \circ j) \in T'_1 (T'_2)$ ,

respectively. Note that in both  $T'_1$  and  $T'_2$ , in cells of the form  $(1, 1 \setminus \alpha^g(e_1))$  we have the entry  $\alpha^{g-1}(e_1)$  and in cells of the form  $(1, 1 \setminus \beta^h(e_1))$  we have entry  $\beta^{h+1}(e_1)$ .

Now we show that  $T'_1$  is in fact the disjoint mate of  $T_1$ . From the way we have constructed the partial Latin square  $T'_1$  it is clear that  $\mathcal{C}_{T'_1}^c = \mathcal{C}_{T_1}^c$  for every column  $c$  (every column is balanced), and  $\mathcal{R}_{T'_1}^1 = \mathcal{R}_{T_1}^1$  (row 1 is balanced). (Recall that the only elements with row equal to 1 are elements of  $S$ .) So we only need to show that  $\mathcal{R}_{T'_1}^0 = \mathcal{R}_{T_1}^0$  and  $\mathcal{R}_{T'_1}^{n-1} = \mathcal{R}_{T_1}^{n-1}$ . Consider the former. We will prove that if  $(0, j, k) \in T_1$ , then  $(0, j', k) \in T'_1$  for some  $j' \neq j$ . Now, if  $(0, j, k) \in T_1$  then either  $(0, j, k) \in S$  or we insert  $(0, j, k)$  at line 7 or at line 9 of the algorithm. Suppose we have just added the triple  $(0, j, k)$ . Then we either jump to line 2 or (re-)enter the while loop at line 7. In summary there are three cases to consider. Either:

- (a)  $(0, j, k) \in S \setminus \{(0, *, e_1)\}$ ; or
- (a) We have  $x = k$  at the beginning of line 2 in the algorithm; or
- (c)  $k = \beta^h(e_1)$  for some  $h, 1 \leq h \leq q-1$ .

First consider case (a). If  $(0, j, k) \in S \setminus \{(0, *, e_1)\}$  then  $k = \alpha^g(e_1)$  for some  $1 \leq g \leq p-1$ .

If there exists an  $x$  at some occurrence of line 2 of the algorithm such that  $\gamma(x) = \alpha^{g-1}(e_1)$ , then the triple  $(n-1, j', k) \in T_1$ , and by the construction of  $T'_1$ , we have  $(0, j', k) \in T'_1$ . Otherwise there is a column  $j'$  such that  $(0, j', \alpha^{g-1}(e_1)), (1, j', \alpha^g(e_1)) \in T_1$  with cell  $(n-1, j')$  empty, and  $(0, j', k) \in T'_1$ .

Next case (b). If  $\gamma(k) = \alpha^g(e_1)$  for some  $0 \leq g \leq p-1$ , then the ordered triples  $(0, j', \alpha^g(e_1)), (1, j', \alpha^{g+1}(e_1)), (n-1, j', k) \in T_1$  for some column  $j'$ . Therefore  $(0, j', k), (1, j', \alpha^g(e_1)), (n-1, j', \alpha^{g+1}(e_1)) \in T'_1$ . In particular  $(0, j', k) \in T'_1$ . Otherwise  $(n-1, j', k), (0, j', \gamma(k)) \in T_1$  for some column  $j'$  (with cell  $(1, j')$  empty), and thus  $(0, j', k) \in T'_1$ .

Finally if case (c) occurs, then there is a column  $j'$  such that

$$(0, j', \gamma(\beta^{y+1}(e_1))), (1, j', \beta^y(e_1)), (n-1, j', \beta^{y+1}(e_1)) \in T_1,$$

and so

$$(0, j', \beta^y(e_1)), (1, j', \beta^{y+1}(e_1)), (n-1, j', \gamma(\beta^{y+1}(e_1))) \in T'_1$$

and in particular  $(0, j', k) \in T'_1$ .

To prove that  $\mathcal{R}_{T'_1}^{n-1} = \mathcal{R}_{T_1}^{n-1}$ , simply apply Lemma 2. Because the algorithms for  $T_1$  and  $T_2$  have little difference, similar arguments can also be used to prove that  $T_2$  is a Latin trade. □

**Example 4.** Here we construct non-trivial Latin trades that exist in rows 0, 1 and 6 in the back circulant square  $B_{17}$ . We start with  $S$  as shown in bold.

<b>0</b>	<b>1</b>	<b>2</b>	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<b>1</b>	<b>2</b>	<b>3</b>	4	<b>5</b>	6	7	8	9	<b>10</b>	11	12	13	14	<b>15</b>	16	<b>0</b>
6	7	8	9	<b>10</b>	11	12	13	14	<b>15</b>	16	0	1	2	<b>3</b>	4	<b>5</b>

Here is the trade  $T_1$ , constructed using the above algorithm,

<b>0</b>	<b>1</b>	<b>2</b>	3	<b>4</b>	<b>5</b>	6	7	<b>8</b>	9	10	<b>11</b>	12	13	<b>14</b>	<b>15</b>	16
<b>1</b>	<b>2</b>	<b>3</b>	4	<b>5</b>	6	7	8	9	<b>10</b>	11	12	13	14	<b>15</b>	16	<b>0</b>
6	7	<b>8</b>	9	<b>10</b>	<b>11</b>	12	13	<b>14</b>	<b>15</b>	16	<b>0</b>	1	2	<b>3</b>	4	<b>5</b>

and the disjoint mate of trade  $T_1$ :

<b>1</b>	<b>2</b>	<b>8</b>	3	<b>5</b>	<b>11</b>	6	7	<b>14</b>	9	10	<b>0</b>	12	13	<b>15</b>	4	16
<b>0</b>	<b>1</b>	<b>2</b>	4	<b>10</b>	6	7	8	9	<b>15</b>	11	12	13	14	<b>3</b>	16	<b>5</b>
6	7	<b>3</b>	9	4	<b>5</b>	12	13	<b>8</b>	<b>10</b>	16	<b>11</b>	1	2	<b>14</b>	<b>15</b>	<b>0</b>

Here is the trade  $T_2$ , constructed using the above algorithm,

<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	4	5	6	7	8	<b>9</b>	<b>10</b>	11	12	13	14	15	<b>16</b>
<b>1</b>	<b>2</b>	<b>3</b>	4	<b>5</b>	6	7	8	9	<b>10</b>	11	12	13	14	<b>15</b>	16	<b>0</b>
6	7	8	<b>9</b>	<b>10</b>	11	12	13	14	<b>15</b>	<b>16</b>	0	1	2	<b>3</b>	4	<b>5</b>

and the disjoint mate of trade  $T_2$ :

<b>1</b>	<b>2</b>	<b>3</b>	<b>9</b>	4	5	6	7	8	<b>10</b>	<b>16</b>	11	12	13	14	15	<b>0</b>
<b>0</b>	<b>1</b>	<b>2</b>	4	<b>10</b>	6	7	8	9	<b>15</b>	11	12	13	14	<b>3</b>	16	<b>5</b>
6	7	8	<b>3</b>	<b>5</b>	11	12	13	14	<b>9</b>	<b>10</b>	0	1	2	<b>15</b>	4	<b>16</b>

Note that  $T_1$  and  $T_2$  intersect only at  $S$ .

Because of the existence of conjugates, it should be noted that the previous theorem may also be applied to sets of three columns or sets of three entries in a Latin square.

**Corollary 5.** In any set of three rows  $r_1, r_2, r_3$  in any Latin square of order  $n$ , there exists a Latin trade  $T$  and triples of the form  $(r_i, c, r_i \circ c) \in L$  such that  $(r_i, c, r_i \circ c) \notin T$  for each  $1 \leq i \leq 3$ .

*Proof.* Consider the permutations  $\alpha = \rho_{r_1, r_2}$ ,  $\beta = \rho_{r_2, r_3}$  and  $\gamma = \rho_{r_3, r_1}$ . If any of these permutations may be decomposed into disjoint cycles then we have a trade  $T$  with the desired properties.

Otherwise let  $e_1 = r_1 \circ j$  and  $e_2 = r_2 \circ j$  for some column  $j$ . (Thus  $\alpha(e_1) = e_2$ .) Since  $\rho_{r_2, r_3}$  cannot be split into disjoint cycles there exists  $1 \leq q \leq n - 1$  such that  $\beta^q(e_1) = e_2$  and  $e_1 \neq \beta^h(e_1)$ , for all  $0 \leq h < q$ .

But if  $q = n - 1$ , the entry  $e_1$  in row  $r_3$  must be in column  $j$ , which means that  $e_1$  occurs twice in column  $j$ , a contradiction to  $L$  being a Latin square. Thus  $q < n - 1$ . From Theorem 3, there exist Latin trades  $T_1$  and  $T_2$  such that  $T_1 \cap T_2 = S$ , where

$$S = \{(r_1, *, e_1), (r_2, *, \alpha(e_1))\} \\ \cup \{(r_2, *, \beta^h(e_1)), (r_3, *, \beta^{h+1}(e_1)) \mid 0 \leq h < q\},$$

and if  $(r, c, e) \in (T_1 \cup T_2) \setminus S$ , then  $r \neq r_2$ .

Now, suppose that  $T_1$  contains all of row  $r_3$ . Then since  $q < n - 1$  and  $T_1 \cap T_2 = S$ , there exists a column  $c$  in  $T_2$  with no entries. Otherwise  $T_1$  does not contain all of row  $r_3$ , and there exists a column  $c$  in  $T_1$  with no entries. So either  $T_1$  or  $T_2$  is a Latin trade with the required properties.  $\square$

#### 4. MAIN RESULT

**Theorem 6.** Suppose that  $P$  is a critical set in a Latin square  $L$  of order  $n$ , and there is a row  $a$  such that  $|\mathcal{R}_P^a| = 0$ . (In other words, row  $a$  is empty in  $P$ .) Let

$$S = \{c \mid |\mathcal{R}_P^c| = 1\}.$$

Then  $|S| \leq 2$  (there are at most two rows with exactly one entry in  $P$ ) and thus  $|P| \geq 2n - 4$ . Without loss of generality let  $a = 0$  and  $S = \{n - 1, 1\}$ . Then the rows  $n - 1, 0$  and  $1$  in  $P$  are isotopic to rows  $n - 1, 0$  and  $1$  in  $P_n$ . Thus rows  $n - 1, 0$  and  $1$  in  $L$  are isotopic to three adjacent rows in the back circulant Latin square.

*Proof.* Given critical set  $P$  in Latin square  $L$ , we can form a relation  $\theta_{x,y}$  on the set  $\{0, 1, \dots, n - 1\}$  as follows. We say that  $(e_1, e_2) \in \theta_{x,y}$  if and only if

1.  $\rho_{x,y}^m(e_1) = e_2$ , for some integer  $m \geq 1$ ,
2. each element of the form  $(x, *, \rho_{x,y}^k(e_1))$  is in  $P^C$ , where  $0 \leq k \leq m - 1$ , and
3. each element of the form  $(y, *, \rho_{x,y}^k(e_1))$  is in  $P^C$ , where  $1 \leq k \leq m$ .

In other words,  $(e_1, e_2) \in \theta_{x,y}$  if and only if there is a sequence of elements in  $P^C$  of the form  $(x, c_1, e_1), (y, c_1, y \circ e_1), (x, c_2, y \circ e_1), (y, c_2, y \circ e_2), \dots, (x, c_m, y \circ c_{m-1}), (y, c_m, e_2)$ .

**Claim:** If  $(e_1, e_2) \in \theta_{0,1} \cap \theta_{1,n-1}$ , then there exists a Latin trade  $T$  in  $L$  in columns  $0, 1$  and  $n - 1$  that does not intersect  $P$ .

Let  $\alpha = \rho_{0,1}$ ,  $\beta = \rho_{1,n-1}$  and  $\gamma = \rho_{n-1,0}$  as in the previous section.

Suppose that  $l$  and  $m$  are the least positive integers such that  $\alpha^l(e_1) = e_2$  and  $\beta^m(e_1) = e_2$ . Choose the least  $q$  such that  $\alpha^p(e_1) = \beta^q(e_1) (= e_3)$ , where  $p \leq l$  and  $q \leq m$ . Then  $(e_1, e_3) \in \theta_{0,1}$  and  $(e_1, e_3) \in \theta_{1,n-1}$  and

$$e_1, e_3, \alpha(e_1), \alpha^2(e_1), \dots, \alpha^{p-1}(e_1), \beta(e_1), \beta^2(e_1), \dots, \beta^{q-1}(e_1)$$

are all distinct.

From Theorem 3 we can construct two Latin trades,  $T_1$  and  $T_2$  in rows  $0, 1$  and  $n - 1$  so that  $T_1 \cap T_2 = S$ , where

$$\begin{aligned} S = & \{(0, *, \alpha^g(e_1)), (1, *, \alpha^{g+1}(e_1)) \mid 0 \leq g < p\} \\ & \cup \{(1, *, \beta^h(e_1)), (n - 1, *, \beta^{h+1}(e_1)) \mid 0 \leq h < q\}, \end{aligned}$$

and  $T_1$  and  $T_2$  contain no other elements in row 1. Because  $(e_1, e_3) \in \theta_{0,1} \cap \theta_{1,n-1}$ , the set  $S$  does not intersect  $P$ . But since  $|\mathcal{R}_P^0 \cup \mathcal{R}_P^{n-1}| = 1$ , at least one of  $T_1$  and  $T_2$  will not intersect  $P$ , and our claim is proven. So since  $P$  is a critical set,  $\theta_{0,1} \cap \theta_{1,n-1}$  must be empty.

Next we show that this implies that our three rows are isotopic to adjacent rows in  $B_n$ . Observe that each cycle in the permutation  $\alpha$  gives rise to a Latin trade in rows  $0$  and  $1$ . However since there is only one element in  $\mathcal{R}_P^0 \cup \mathcal{R}_P^1$ , the permutation  $\alpha$  may not be split into disjoint cycles. So without loss of generality, we may assume that  $\alpha$  is the permutation that maps  $i$  to  $i + 1$  modulo  $n$ , for each  $i$  between  $0$  and  $n - 1$ . Furthermore we may label the columns so that  $(0, i, i) \in L$  for each  $i$  between  $0$  and  $n - 1$ . What we have so far is

represented in the following diagram.

	0	1	2	.....	$n - 1$
$n - 1$	$\beta(1)$	$\beta(2)$	$\beta(3)$	.....	$\beta(0)$
0	0	1	2	.....	$n - 1$
1	1	2	3	.....	0

Without loss of generality let  $\mathcal{R}_P^1 = \{0\}$  and  $\mathcal{R}_P^{n-1} = \{a\}$  for some  $a \in N$ . Thus the ordered pair  $(x, y)$  is in  $\theta_{0,1}$  if and only if  $x < y$ .

So for  $\theta_{0,1} \cap \theta_{1,n-1}$  to be empty, if  $(x, y) \in \theta_{1,n-1}$  then we must have  $x > y$ . But  $(x, \beta(x)) \in \theta_{1,n-1}$  if and only if  $x \neq 0$  and  $\beta(x) \neq a$ . So we have  $x > \beta(x)$  unless  $x = 0$  or  $\beta(x) = a$ . Now  $\beta(1)$  cannot equal 0 as  $\alpha^{-1}(1) = 0$ , or in other words 0 already occurs as an entry in that column. Thus we must have  $\beta(1) = a$ . Next,  $\beta(2)$  cannot equal 1, so we must have  $\beta(2) = 0$ . Similarly  $\beta(3) = 1$ ,  $\beta(4) = 2$  and continuing in this way we have  $\beta(i) = i - 2$ , for each  $i$  between 2 and  $n - 1$ . Now there are only two cells left to fill in column  $n - 1$ , and since  $\beta(0) \neq n - 1$ , we have  $\beta(0) = n - 2$  and  $\beta(1) = n - 1 (= a)$ . Thus columns  $n - 1, 0$ , and 1 in  $L$  together are isotopic to three adjacent columns of  $B_n$ , and moreover columns  $n - 1, 0$  and 1 in  $P$  are isotopic to the columns  $n - 1, 0$  and 1 in  $P_n$ .

Since the column  $n - 1$  is uniquely determined in our argument, we have the following. If  $C$  is a critical set with an empty row, then at most two columns have exactly one element. Moreover if  $C$  is a critical set with an empty row,  $|C| \geq 2n - 4$ .

□

We should stress that the conjugate arguments of the previous theorem also hold. For example, if  $P$  is a critical set with an empty column, or if  $P$  is a critical set with no occurrences of an entry  $k$ , then  $|P| \geq 2n - 4$ .

Possibly the results in this paper will be extended with the development of more sophisticated Latin trades. Eventually this may lead to proving that  $scs(n) = \lfloor n^2/4 \rfloor$ . If this paper is the first step to such a proof, the following conjectures (which are not disproved by heuristic evidence in [1], [2]) may be the next steps.

**Conjecture 7.** If  $P$  is a critical set with one empty column (or row or entry), there are at most four other columns (or rows or entries) with at most two elements.

**Conjecture 8.** In any critical set  $P$ , there are at most three columns (or rows or entries) with at most one element.

A corollary of the previous conjecture and the results of this paper would be that  $|P| \geq 2n - 3$  for any critical set  $P$  of order  $n$ . This would be an improvement on known bounds (see Introduction).

The algorithms given in this paper find Latin trades quickly and efficiently in Latin squares. They may be useful when testing computationally whether partial Latin squares are in fact critical sets.

## REFERENCES

- [1] P. Adams, R. Bean and A. Khodkar, A census of critical sets in the Latin squares of order at most six, submitted.
- [2] P. Adams and A. Khodkar, Smallest critical sets for the Latin squares of orders six and seven, J. Combin. Math. Combin. Comput. **37** (2001), 287–300.

- [3] J.A. Bate and G.H.J. van Rees, The size of the smallest strong critical set in a Latin square, *Ars Combin.*, 53 (1999), 73–83.
- [4] N.J. Cavenagh and A. Khodkar, Balanced critical sets in Latin squares, *Utilitas Math.* (to appear).
- [5] J. Cooper, D. Donovan and J. Seberry, Latin squares and critical sets of minimal size, *Australas. J. Combin.*, 4 (1991), 113–120.
- [6] 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, pp. 165–168.
- [7] D. Donovan, J. Cooper, D.J. Nott and J. Seberry, Latin squares: critical sets and their lower bounds, *Ars Combin.*, 39 (1995), 33–48.
- [8] D. Donovan and A. Howse, Towards the spectrum of critical sets, *Australas. J. Combin.*, 21 (2000), 107–130.
- [9] C-M. Fu, H-L. Fu and C.A. Rodger, The minimum size of critical sets in Latin squares, *J. Statist. Plann. Inference.*, 62, No. 2 (1997), 333–337.
- [10] A.P. Street, “Trades and defining sets,” *CRC Handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz (Editors), CRC Publishing Co., 1996, pp. 474–478.