

# The size of the smallest latin trade in a back circulant latin square

Nicholas J. Cavenagh  
Centre for Discrete Mathematics and Computing  
Department of Mathematics  
The University of Queensland  
Queensland 4072  
Australia  
Email: njc@maths.uq.edu.au

Abstract: Drapal and Kepka (1989) proved that if  $I$  is a latin trade in the back circulant latin square of order  $n$ , then  $|I| \geq O(\log p)$ , where  $p$  is the smallest prime that divides  $n$ . We give an alternative proof of this result.

Keywords: latin square, latin trade.

## 1. BACKGROUND INFORMATION

The concept of intersections between latin squares and the concept of latin trades are closely related. Given two distinct latin squares  $L_1$  and  $L_2$  of the same order, the set of elements of  $L_1$  which differ from  $L_2$  is a latin trade. Conversely, any latin trade may be constructed in this way.

Drapal and Kepka [6] proved that if  $L$  is a latin square of order  $n \geq 3$  then the intersection between  $L$  and  $B_n(\neq L)$ , the back circulant latin square, is at least 4 if  $n$  is even, or at least  $e \log p + 3$ , where  $p$  is the least prime that divides  $n$ , if  $n$  is odd. Equivalently, the size of the smallest latin trade in  $B_n$  is at least  $O(\log p)$ . This note presents an alternative proof of this result. The approach taken is accessible to readers with a combinatorics background.

It is conjectured that we can construct a latin trade of order bounded by  $O(\log n)$  in  $B_n$  for any  $n$ . Drapal ([4]) has shown that for any  $n \geq 3$  there exists a latin trade of size at most  $O(\log n^2)$  in the back circulant latin square of order  $n$ . In doing so he proves that certain triangulations of the integral plane correspond to latin trades in  $B_n$ .

Latin trades are essential for constructions of critical sets in latin squares (see, for example, [2] and [3]).

The linear algebraic notation used in this paper is consistent with [1]. Let  $N = \{0, 1, 2, \dots, n-1\}$ . A *partial latin square*  $P$  of order  $n$  is a set of ordered triples of elements of  $N$  such that

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

If  $(i, j, k) \in P$  we say that the *entry*  $k$  occurs in *row*  $i$  and *column*  $j$  (or *cell*  $(i, j)$ ) of  $P$ . Thus we may think of  $P$  as an  $n \times n$  array of integers chosen from  $N$  in such a way that each element of  $N$  occurs at most once in each row and at most once in each column of the array.

If every cell of the array contains an entry 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  $N = \{0, 1, \dots, n-1\}$  in such a way that each element of  $N$  occurs precisely once in each row and precisely once in each column of the array. Let  $B_n$  denote the back circulant latin square of order  $n$ . That is, if the rows and columns are labelled zero to  $n-1$ , then for all positive integers  $n$ ,  $B_n = \{(i, j, i + j \pmod{n}) \mid 0 \leq i, j \leq n-1\}$ .

Two partial latin squares are said to be *isotopic* if there exist three permutations  $\alpha, \beta, \gamma$  of the set  $N$  such that  $(i, j, k) \in P$  if and only if  $(\alpha(i), \beta(j), \gamma(k)) \in Q$ .

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. For each  $i$ ,  $0 \leq i \leq n-1$ , let  $\mathcal{R}_P^i$  denote the set of entries occurring in row  $i$  of  $P$ . Formally,  $\mathcal{R}_P^i = \{k \mid \text{there exists } j, (i, j, k) \in P\}$ . Similarly, for each  $j$ ,  $0 \leq j \leq n-1$ , we define  $\mathcal{C}_P^j = \{k \mid \text{there exists } i, (i, j, k) \in P\}$ . We will also need  $\mathcal{E}_P^k = \{(i, j) \mid (i, j, k) \in P\}$  and  $\mathcal{E}(P) = \{k \mid \text{there exists } i, j, (i, j, k) \in P\}$ .

**Definition 1.** A partial latin square  $I (\neq \emptyset)$  of order  $n$  is said to be a *latin trade* if there exists a partial latin square  $I'$  (called a *disjoint mate* of  $I$ ) of order  $n$ , such that

1.  $\mathcal{S}_I = \mathcal{S}_{I'}$ ,
2. for each  $k \in \mathcal{E}(I)$ ,  $\mathcal{E}_I^k \cap \mathcal{E}_{I'}^k = \emptyset$ . (Or if  $(i, j, k) \in I$  and  $(i, j, k') \in I'$ , then  $k \neq k'$ .)
3. for each  $i$ ,  $0 \leq i \leq n-1$ ,  $\mathcal{R}_I^i = \mathcal{R}_{I'}^i$ , and
4. for each  $j$ ,  $0 \leq j \leq n-1$ ,  $\mathcal{C}_I^j = \mathcal{C}_{I'}^j$ .

**Example 2.** Figure 1 shows a latin trade  $I$  in  $B_7$ , together with the latin square formed by replacing  $I$  with its disjoint mate  $I'$ . The entries of  $I$

and  $I'$  are shown in italics. Nine is the smallest possible size for a latin trade in  $B_7$  [7].

<i>0</i>	1	2	3	<i>4</i>	5	6
1	2	3	4	5	6	0
2	3	<i>4</i>	5	<i>6</i>	0	1
3	4	5	<i>6</i>	0	1	2
<i>4</i>	5	<i>6</i>	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

<i>4</i>	1	2	3	0	5	6
1	2	3	4	5	6	0
2	3	<i>6</i>	5	<i>4</i>	0	1
3	4	5	0	<i>6</i>	1	2
0	5	<i>4</i>	<i>6</i>	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

Figure 1

### 3. A LOWER BOUND

The size of the smallest latin trade found in *any* latin square is four. Such latin trades are called *intercalates*, and exist in  $B_n$  whenever  $n$  is even.

In this section we establish a lower bound for the size of a latin trade in  $B_n$ , for any odd  $n \geq 3$ . To do so we take an arbitrary latin trade  $I$  in  $B_n$  and exploit the group properties of  $(\mathbb{Z}, +)$  to establish a set of equations involving the entries of  $I$ . We then make use of some linear algebra, and later on even some calculus! But first of all we need a couple of small lemmas.

**Lemma 3.** If  $I$  is a latin trade and if  $|\mathcal{E}_I^k| \geq 1$ , for some  $k \in N$ , then  $|\mathcal{E}_I^k| \geq 2$ .

*Proof.* Suppose there exists a latin trade  $I$  and entry  $k$  with  $|\mathcal{E}_I^k| = 1$ . Let  $I'$  be a disjoint mate of  $I$ . Then by conditions 2 and 3 of Definition 1,  $\mathcal{R}_I^i = \mathcal{R}_{I'}^i$ , and there exists  $j' \neq j$  such that  $(i, j', k) \in I'$ . But from condition 4 of Definition 1,  $\mathcal{C}_I^{j'} = \mathcal{C}_{I'}^{j'}$ , and there exists  $i' \neq i$  such that entry  $(i', j', k) \in I$ , and  $|\mathcal{E}_I^k| \geq 2$ .  $\square$

**Lemma 4.** If  $I$  is a latin trade then  $|\mathcal{E}(I)| \geq 2$ .

*Proof.* Suppose that  $I$  is a latin trade and  $|\mathcal{E}(I)| = 1$ . Let  $\mathcal{E}(I) = \{k\}$ , and  $(i, j) \in \mathcal{E}_I^k$ . Let  $I'$  be a disjoint mate of  $I$ . Conditions 1 and 2 of Definition 1 tells us that there exists  $k' \neq k$ , with  $(i, j, k') \in I'$ . But from conditions 2 and 3 of Definition 1,  $(i, j', k') \in I$ , for some  $j' \neq j$ . This contradicts our original assumption.  $\square$

The following procedure indicates how a matrix equation may be derived from a given latin trade in  $B_n$ . This is the first step in obtaining the lower bound given in Theorem 9. An example of this procedure is given in Example 11.

Consider a latin trade  $I$  in a back circulant latin square of order  $n$ , together with a disjoint mate  $I'$ . Let  $\mathcal{E}(I) = \{x_1, x_2, \dots, x_{m+1}\} \subseteq N$ . We know from Lemma 4 that  $m \geq 1$ . Because of the cyclic structure of  $B_n$ , the set

$$\{(i - x_{m+1}, j, k - x_{m+1} \pmod{n}) \mid (i, j, k) \in I\}$$

is also a latin trade in  $B_n$ , and is isotopic to  $I$ . Thus we can assume without loss of generality that  $x_{m+1} = 0$ .

Now, let  $b = |\mathcal{E}_I^{x_1}|$  (the number of occurrences of  $x_1$  as an *entry* in  $I$ ). From Lemma 3,  $b \geq 2$ . Let  $S = \mathcal{E}_I^{x_1}$  and  $S' = \mathcal{E}_{I'}^{x_1}$ . Then

$$S = \{(i_1, j_1), (i_2, j_2), \dots, (i_b, j_b)\},$$

for some integers  $i_1, i_2, \dots, i_b, j_1, j_2, \dots, j_b$ . Also,

$$S' = \{(i_1, j_{\alpha(1)}), (i_2, j_{\alpha(2)}), \dots, (i_b, j_{\alpha(b)})\},$$

where  $\alpha$  is some devolution of the set  $\{1, 2, \dots, b\}$ .

Observe that:

$$\sum_{y=1}^b (i_y + j_y) = \sum_{y=1}^b (i_y + j_{\alpha(y)}).$$

But each  $(i_y + j_y) \equiv x_1 \pmod{n}$ , and each  $(i_y + j_{\alpha(y)}) \equiv x_k \pmod{n}$ , for some  $k$ , where  $2 \leq k \leq m+1$ . This gives us an equation

$$(1) \quad bx_1 \equiv b_{12}x_2 + \dots + b_{1m}x_m + b_{1m+1}x_{m+1} \pmod{n},$$

where  $\sum_{i=2}^{m+1} b_{1i} = b \geq 2$ , and  $x_{m+1} = 0$ . (Let  $Q \subset I$  be the partial latin square with the same shape as  $S'$ . Then  $b_{1i} = |\mathcal{E}_Q^{x_i}|$ .) From the definition of congruence modulo  $n$ , we may rewrite equation (1) as:

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m = c_1n,$$

where  $a_{11} = b$ ,  $a_{1i} = -b_{1i} \leq 0$  and  $c_1$  is some integer. Observe that  $\sum_{i=1}^m a_{1i} = b - \sum_{i=2}^m b_{1i} = b_{1m+1} \geq 0$ .

We repeat this process for the entries  $x_i$ ,  $1 \leq i \leq m$ , to obtain equations of the form:

$$a_{i1}x_1 + a_{i2}x_2 + \dots + a_{im}x_m = c_in.$$

In each case  $a_{ii} = |\mathcal{E}_I^{x_i}| \geq 2$  (by Lemma 3),  $a_{ij} \leq 0$  if  $i \neq j$ , and  $\sum_{j=1}^m a_{ij} \geq 0$ . Let  $A \in M_{m \times m}(\mathbb{Z})$  be the matrix given by  $A = [a_{ij}]$  (where  $1 \leq i, j \leq m$ ),  $X$  the column vector  $(x_1, x_2, \dots, x_m)^t$  and  $B$  the vector  $(c_1, c_2, \dots, c_m)^t$ . We say that  $A$  is a matrix *derived* from the latin trade  $I$ . Then  $AX = nB$ , or equivalently

$$X = \frac{n}{\det(A)} \text{adj}(A)B,$$

where  $\text{adj}(A)$  is the adjoint of  $A$ , a matrix with integer entries. Next we explore some properties of  $\det(A)$ .

**Lemma 5.** If  $I$  is a latin trade in the back circulant latin square of order  $n$ , then  $\gcd(n, \det(A)) > 1$ , where  $A$  is any matrix derived from  $I$ .

*Proof.* Let  $I$  be a latin trade in  $B_n$ , and let  $A$  be a matrix derived from  $I$ . Then, as above, we have a matrix equation  $X = n \times \text{adj}(A)B/\det(A)$ , where  $\text{adj}(A)$  is the adjoint of  $A$ , a matrix with integer entries. The elements of  $X$  are the non-zero entries that occur in cells of  $I$ , so they must lie between 1 and  $n - 1$ . However, if  $\gcd(n, \det(A)) = 1$ , each entry of  $X$  is divisible by  $n$ , contradicting the previous statement.  $\square$

**Definition 6.** Let  $A = [a_{ij}]$  be a matrix in  $M_{m \times m}(\mathbb{R})$ . We say that  $A$  is a *trade matrix* if it satisfies the following properties, for all  $1 \leq i, j \leq m$ :

1.  $a_{ii} > 0$ ,
2.  $a_{ij} \leq 0$  ( $i \neq j$ ),
3.  $\sum_{j=1}^m a_{ij} \geq 0$ .

Any matrix  $A$  derived from a latin trade  $I$  is a trade matrix. The following lemma gives an upper bound on the determinant of a trade matrix, in terms of its diagonal elements.

**Lemma 7.** If  $A = [a_{ij}] \in M_{m \times m}(\mathbb{R})$  is a trade matrix, then  $\det(A) \leq \prod_{i=1}^m a_{ii}$ .

*Proof.* The proof is by induction on  $m$ , and essentially involves row reduction of  $A$ .

If  $m = 1$ ,  $\det(A) = a_{11}$ , so the lemma is true in this case. Otherwise assume that  $m \geq 2$ , and that for any trade matrix with  $m - 1$  rows and columns, its determinant is no greater than the product of its diagonal elements. Let  $B = [b_{ij}]$  be the  $(m - 1) \times (m - 1)$  matrix obtained from  $A$  as follows. For all  $i, j$ ,  $1 \leq i, j \leq m - 1$ :

$$b_{ij} = a_{i+1, j+1} - a_{i+1, 1}a_{1, j+1}/a_{11}.$$

Observe that  $\det(A) = a_{11}\det(B)$ . We will show that  $B$  is a trade matrix.

Firstly, if  $i \neq j$  then  $a_{ii} \geq |a_{ij}|$ . (This is a consequence of conditions 1, 2 and 3 in Definition 6.) It follows that  $a_{i1}a_{1i} \leq a_{ii}a_{11}$ , for all  $i$ ,  $2 \leq i \leq m$ . If equality holds for any  $i$ , then  $\det(A) = 0$ , and certainly  $\det(A) \leq \prod_{i=1}^m a_{ii}$  in this case. Otherwise for all  $i$ ,  $1 \leq i \leq m - 1$ ,  $a_{i+1, 1}a_{1, i+1} < a_{i+1, i+1}a_{11}$ , and

$$b_{ii} = a_{i+1, i+1} - \frac{a_{i+1, 1}a_{1, i+1}}{a_{11}} > 0.$$

Therefore condition 1 of Definition 6 holds for  $B$ .

Now we check condition 2. If  $i \neq j$  and  $1 \leq i, j \leq m - 1$ ,

$$b_{ij} = a_{i+1, j+1} - \frac{a_{i+1, 1}a_{1, j+1}}{a_{11}} \leq a_{i+1, j+1} \leq 0,$$

since  $a_{i+1,1}$  and  $a_{1,j+1}$  are both non-positive. Thus  $b_{ij} \leq 0$  and condition 2 holds.

Next,

$$\begin{aligned} \sum_{j=1}^{m-1} b_{ij} &= \sum_{j=2}^m (a_{i+1,j} - a_{i+1,1}a_{1j}/a_{11}) \\ &= \sum_{j=2}^m a_{i+1,j} - \frac{a_{i+1,1}}{a_{11}} \sum_{j=2}^m a_{1j}. \end{aligned}$$

But  $\sum_{j=1}^m a_{i+1,j} \geq 0$  and  $\sum_{j=1}^m a_{1j} \geq 0$ , so

$$\sum_{j=1}^{m-1} b_{ij} \geq -a_{i+1,1} - \frac{a_{i+1,1}}{a_{11}}(-a_{11}) = 0.$$

Thus condition 3 holds, and we have that  $B$  is a trade matrix.

But from our inductive hypothesis,

$$\det(B) \leq \prod_{i=1}^{m-1} b_{ii} \leq \prod_{i=2}^m a_{ii},$$

and so  $\det(A) \leq \prod_{i=1}^m a_{ii}$ . □

**Lemma 8.** For all integers  $m \geq 1$  and  $p \geq 2$ ,  $mp^{1/m} \geq e \log p$ .

*Proof.* Consider the derivative of  $mp^{1/m}$  with respect to  $m$ :

$$\begin{aligned} \frac{d}{dm}(mp^{1/m}) &= p^{1/m} + m \frac{d}{dm}(e^{\log p/m}) \\ &= p^{1/m} - \frac{\log p}{m} e^{\log p/m} \\ &= p^{1/m}(1 - \log p/m). \end{aligned}$$

Setting the first derivative to zero gives us  $m = \log p$ . The second derivative is:  $p^{1/m} \log p/m^2$ . This is always positive, so  $m = \log p$  gives us a minimum value for the expression  $mp^{1/m}$ . Thus,

$$\begin{aligned} mp^{1/m} &\geq \log p \times p^{1/\log p} \\ &= \log p \times (e^{\log p})^{1/\log p} = e \log p. \end{aligned}$$

□

**Theorem 9.** If  $I$  is a latin trade in  $B_n$ , then  $|I| \geq \lceil e \log p + 2 \rceil$ , where  $p$  is the smallest prime that divides  $n$ .

*Proof.* Let  $I$  be a latin trade in  $B_n$ , let  $A$  a matrix derived from  $I$  and let  $\gcd(n, \det(A)) = g$ . From Lemma 5,  $g > 1$  and thus  $g \geq p$ , where  $p$  is the least prime that divides  $n$ . Suppose that the number of distinct entries in

$I$  is  $m + 1$ , and that the diagonal entries of  $A$  are  $a_{11}, a_{22}, \dots, a_{mm}$ . Then, together with Lemma 7, we have that

$$p \leq g \leq \det(A) \leq \prod_{i=1}^m a_{ii}.$$

Under this constraint,

$$|I| \geq 2 + \sum_{i=1}^m a_{ii} \geq 2 + mp^{1/m}.$$

(Since  $\sum_{i=1}^m a_{ii}$  is minimized when  $a_{11} = a_{22} = a_{33} = \dots = a_{mm}$ , which implies that each  $a_{ii} \geq p^{1/m}$ . Also, there are at least two cells of  $I$  containing the  $(m+1)$ th entry.) But Lemma 8 shows that  $mp^{1/m} \geq e \log p$  and we have  $|I| \geq e \log p + 2$ .  $\square$

**Corollary 10.** If  $L$  is a latin square of order  $n$  and  $L \neq B_n$ , then  $|L \cap B_n| \geq \lceil e \log p + 2 \rceil$ , where  $p$  is the smallest prime that divides  $n$ .

*Proof.* This corollary follows from the relationship between latin trades and intersections between latin squares.  $\square$

**Example 11.** Consider the latin trade  $I$  and its disjoint mate  $I'$  given in Figure 2.

	$j_1$	$j_2$	$j_3$	$j_4$	$j_5$
$i_1$	$x_3$	$x_2$	$x_4$	$x_1$	
$i_2$	$x_2$	$x_4$			$x_3$
$i_3$			$x_1$		$x_4$
$i_4$				$x_3$	$x_1$

$I$

	$j_1$	$j_2$	$j_3$	$j_4$	$j_5$
$i_1$	$x_2$	$x_4$	$x_1$	$x_3$	
$i_2$	$x_3$	$x_2$			$x_4$
$i_3$			$x_4$		$x_1$
$i_4$				$x_1$	$x_3$

$I'$

**Figure 2**

Suppose that  $I$  is contained in the latin square  $B_n$ . We shall derive a matrix  $A$  from the latin trade  $I$ , as in the procedure that follows Lemma 4. We may let  $x_4 = 0$  without loss of generality.

The sets of cells containing the entry  $x_1$  in  $I$  and  $I'$  are given by:

$$S = \{(i_1, j_4), (i_3, j_3), (i_4, j_5)\} \text{ and } S' = \{(i_1, j_3), (i_3, j_5), (i_4, j_4)\}$$

respectively. Observe that

$$(i_1 + j_4) + (i_3 + j_3) + (i_4 + j_5) = (i_1 + j_3) + (i_3 + j_5) + (i_4 + j_4).$$

By considering each of these sums within the latin trade  $I$  in  $B_n$ , we get  $3x_1 \equiv x_3 + 2x_4 \pmod{n}$ , or equivalently  $3x_1 - x_3 = b_1 n$  for some integer  $b_1$ . Following the same procedure for entries  $x_2$  and  $x_3$  we obtain equations

$2x_2 - x_3 = b_2n$  and  $3x_3 - 2x_1 - x_2 = b_3n$ , for some integers  $b_2$  and  $b_3$ . Then  $AX = nB$ , where  $X = (x_1, x_2, x_3)^t$ ,  $B = (b_1, b_2, b_3)^t$  and

$$A = \begin{pmatrix} 3 & 0 & -1 \\ 0 & 2 & -1 \\ -2 & -1 & 3 \end{pmatrix}.$$

The determinant of  $A$  is 11. (Note that this is no greater than the product of the diagonal entries of  $A$ , as per Lemma 7.) In fact, a solution to  $AX = 11B$  is given by  $X = (1, 7, 3)^t$  and  $B = (0, 1, 0)^t$ , and  $I$  can be embedded in  $B_{11}$ . A corresponding latin trade in  $B_{11}$  is given in Figure 3, together with its disjoint mate.

0	1		3			7			
1									0
	3								1
			7			0			3

The latin trade  $I$  embedded in  $B_{11}$ .

1	3		7			0			
0									1
	1								3
			3			7			0

The disjoint mate of the above latin trade.

**Figure 3**

#### REFERENCES

- [1] H. Anton, "Elementary Linear Algebra," John Wiley & Sons, Inc., Canada, 1981.
- [2] D. Curran and G. H. J. van Rees, Critical sets in latin squares, *Congr. Numer.* **22** (1978), 165–168.
- [3] D. Donovan and J. Cooper, Critical sets in back circulant latin squares, *Aequationes Math.* **52** (1996), 157–179.
- [4] A. Drapal, On a planar construction of quasigroups, *Czechoslovak Math. J.* **41** (1991), 538–548.
- [5] A. Drapal, Non-isomorphic 2-groups coincide at most in three quarters of their multiplication tables, *European J. Combinatorics* **21** (2000), 301–321.
- [6] A. Drapal and T. Kepka, On a distance of groups and latin squares, *Comment. Math. Univ. Carolinae* **30**, 4 (1989), 621–626.
- [7] A. Howse, "Latin interchanges, critical sets and associated structures," Ph.D. thesis, University of Queensland, 1998.