AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **36** (2006), Pages 231–239

A lower bound for the size of a critical set in the back circulant latin square

Nicholas J. Cavenagh*

Institute for Theoretical Computer Science ITI, Charles University
Malostranské Naměsti 25
11800 Praha 1
Czech Republic

Abstract

The back circulant latin square of order n is the latin square based on the addition table for the integers modulo n. A critical set is a partial latin square that has a unique completion to a latin square, and is minimal with respect to this property. In this note we show that the size of a critical set in the back circulant latin square of order n is at least $n^{4/3}/2 - n - n^{2/3}/2 + 2n^{1/3} - 1$.

1 Introduction

We define $\mathrm{scs}(n)$ 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 ([7]) showed that if $n > 20$, $\mathrm{scs}(n) \geq \lfloor (7n-3)/6 \rfloor$. Horak, Aldred and Fleischner showed that if $n \geq 8$, $\mathrm{scs}(n) \geq \lfloor (4n-8)/3 \rfloor$ ([8]). Very recently, this bound was improved by the author to $\mathrm{scs}(n) \geq n(\log n)^{1/3}/2$ (for all $n \geq 1$) ([3]). Bate and van Rees ([2]) showed that the size of the smallest strong critical set (a critical set with a certain type of completion) is $\lfloor n^2/4 \rfloor$. 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. Some computational results for critical sets in small latin squares are given in [1]. See [9] for a survey paper on critical sets in latin squares, or [10] for more general results on defining sets and trades in combinatorial structures.

The lower bound in this paper is essentially a refinement of the result in [3], exploiting the cyclic structure of back circulant latin squares.

* Supported by Ministry of Education of the Czech Republic as project LN00A056

2 Definitions

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

Let $N = \{0, 1, 2, \ldots, n-1\}$. A *partial latin square* 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 $i = i'$.

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). A partial latin square has the property that each entry occurs at most once in each row and at most once in each column.

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 $N = \{0, 1, 2, \ldots, n-1\}$ in such a way that each element of N occurs precisely once in each row and precisely once in each column of the array.

We define the *back circulant latin square* B_n to be the latin square based on the addition table for the integers modulo n. That is,

$$B_n = \{(i, j; i + j \pmod n) \mid 0 \leq i, j \leq n-1\}.$$

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 there exists a latin trade T in L such that $P \cap T = \emptyset$, then P is also contained in the latin square $(L \setminus T) \cup T'$, where T' is a disjoint mate of T. Therefore if P is a critical set in a latin square L, P must intersect every latin trade in L. It comes as no surprise, then, that the study of latin squares is closely related to the study of critical sets in latin squares. Other applications of latin trades include the compact storage of large catalogues of latin squares (see Wanless, [11]).

3 Latin trade constructions

In this section we construct latin trades that are used later in our proof on critical sets. The following theorem first appeared in [4]. We omit the proof in this paper. However, an example follows to illustrate the construction.

Theorem 1 (Theorem 2.4, [4]) *Let $x, y \geq 1$. Consider the subrectangle in the back circulant latin square B_{x+y} cornered by the following elements:*

$$(0, 0; 0), (0, y; y), (x, 0; x) \text{ and } (x, y; 0).$$

Then there exists a latin trade, denoted by $I_{x,y}$, with the following properties:

1. *$I_{x,y}$ is contained within the above subrectangle.*
2. *$I_{x,y}$ includes the above four elements.*
3. *The disjoint mate of $I_{x,y}$, denoted by $I'_{x,y}$, includes the elements $(0, y; 0)$ and $(x, 0; 0)$.*

Example 2 *Figure* 1 *shows the latin trade $I_{5,8}$, together with its disjoint mate $I'_{5,8}$, constructed as in Theorem* 1.

0					5			8
					8		10	11
							11	12
5					10		12	0

$I_{5,8}$

5					8			0
					10		11	8
							12	11
0					5		10	12

$I'_{5,8}$

Figure 1

4 Main Results

Note that since a back circulant square of even order n can be partitioned into 2×2 subsquares (which are latin trades), the smallest size of a critical set when n is even is $n^2/4$. The results in this section apply for both n even and n odd.

Because of the cyclic nature of B_n, partial latin squares may be "shifted" by translation to different positions in B_n. We assume throughout this section that row, column and entry values are calculated modulo n. We describe the process more precisely in the next definition.

Definition 3 *Let I be a partial latin square in the back circulant latin square of order n. We define $I \oplus (i,j)$ to be the partial latin square in B_n given by:*

$$I \oplus (i,j) = \{(\alpha + i, \beta + j; \gamma + i + j (\text{mod } n)) \mid (\alpha, \beta, \gamma) \in I\}.$$

The next lemma exploits the latin trades constructed in the previous section.

Lemma 4 *Let C be a critical set in B_n, a and b integers such that $a + b < n - 1$ and $a, b \geq 1$. Suppose that every cell in C of the form (i,j) is empty, where $r \leq i \leq r + a - 1$ and $c \leq j \leq c + b - 1$. Then:*

1. *Columns c through to $c + b - 1$ (mod n) in C must contain at least*

$$min\ (\lfloor b^2/4 \rfloor, a\lfloor b/2 \rfloor)$$

   entries, and

2. *rows r through to $r + a - 1$ (mod n) in C must contain at least*

$$min\ (\lfloor a^2/4 \rfloor, b\lfloor a/2 \rfloor)$$

   entries.

Proof Because of the cyclic structure of B_n, we may assume, without loss of generality, that $r = c = 0$. Let $B = \lceil b/2 \rceil$. Consider column 0 and column B in B_n. For each i, $0 \leq i < \min(a, B)$, we construct a latin trade T_i that intersects columns 0 and B only within rows a through to $n - 1$. All other elements of T_i will lie within the first a rows and the first b columns. Informally, we find i in column B, then zig-zag between columns B and 0 until we reach an element that lies between rows 0 to $a - 1$. We then adjoin this zig-zagging sequence of elements with one of the trades from Theorem 1 (pasted in the first a rows) to create a new latin trade.

Formally, we construct T_i as follows. Let x be the least positive integer such that

$$i + B \leq i - xB (\text{mod } n) \leq B + (a - 1).$$

Let $\gamma = (i - xB) \pmod{n}$.

Suppose first that $B|n$. In this case, $x = n/B$, $\gamma = i$ and our latin trade T_i is equal to:

$$\{(i - \alpha B - B, B; i - \alpha B), (i - \alpha B, 0; i - \alpha B) \mid 0 \leq \alpha < x\}.$$

The disjoint mate T_i', obtained by exchanging the entries in each row, is:

$$\{(i - \alpha B - B, B; i - \alpha B - B), (i - \alpha B, 0; i - \alpha B + B) \mid 0 \leq \alpha < x\}.$$

Clearly T_i and T_i' occupy the same shape and are disjoint. Also, since we are just swapping entries in the same row, T_i and T_i' are row-balanced. Finally,

$$\mathcal{C}^0_{T_i} = \mathcal{C}^0_{T_i'} = \mathcal{C}^B_{T_i} = \mathcal{C}^B_{T_i'} = \{i - \alpha B \mid 0 \leq i < x\}.$$

Thus T_i is a latin trade with disjoint mate T_i'.

Otherwise B does not divide n. We have two subcases: $\gamma > i + B$ and $\gamma < i + B$. For the first subcase, our latin trade T_i is:

$$\begin{gathered}(I_{\gamma-(i+B),B} \setminus \{(\gamma - (i + B), B; 0)\}) \oplus (i, 0) \cup \{(\gamma - B, B; \gamma)\} \\ \cup\{(i - \alpha B - B, B; i - \alpha B), (i - \alpha B - B, 0; i - \alpha B - B) \mid 0 \leq \alpha < x\}.\end{gathered}$$

The disjoint mate of this latin trade, T_i', is equal to:

$$\begin{gathered}(I'_{\gamma-(i+B),B} \setminus \{(\gamma - (i + B), 0; 0)\}) \oplus (i, 0) \cup \{(\gamma - B, 0; \gamma)\} \\ \cup\{(i - \alpha B - B, 0; i - \alpha B), (i - \alpha B - B, B; i - \alpha B - B) \mid 0 \leq \alpha < x\},\end{gathered}$$

where $I'_{\gamma-(i+B),B}$ is the disjoint mate of latin trade $I_{\gamma-(i+B),B}$.

We next verify that T_i is a latin trade with disjoint mate T_i'. Since $I_{\gamma-(i+B),B}$ and $I'_{\gamma-(i+B),B}$ are latin trades (from Theorem 1), they have the same shape and are disjoint. It follows that T_i and T_i' have the same shape and are disjoint. Now, let $(d, e; f)$ be some element of T_i. If we can show that there exists d' and e' such that $(d', e; f), (d, e'; f) \in T_i'$, it follows that T_i' is a disjoint mate of T_i. First suppose that $(d, e; f) \in (I_{\gamma-(i+B),B} \setminus \{(\gamma - (i + B), B; 0)\}) \oplus (i, 0)$. Then $(d - i, e; f - i) \in I_{\gamma-(i+B),B} \setminus \{(\gamma - (i + B), B; 0)\})$. Thus, there exists $d' \neq d - i$ and $e' \neq e$ such that $(d - i, e'; f - i), (d', e; f - i) \in I'_{\gamma-(i+B),B}$. So clearly $(d, e'; f), (d', e; f) \in T_i'$ unless $(d - i, e'; f - i)$ or $(d', e; f - i) = (\gamma - (i + B), 0; 0)$. Since column B is the unique column for which row $\gamma - (i + B)$ contains entry 0 within $I_{\gamma-(i+B),B}$ (see Theorem 1), the former implies that $(d - i, e; f - i) = (\gamma - (i + B), B; 0)$; a contradiction to the definition of T_i. Similarly, the latter implies that $(d - i, e; f - i) = (0, 0; 0)$, or, equivalently, $(d, e; f) = (i, 0; i)$. For this case observe that $(\gamma, 0; i) \in T_i'$.

Next suppose that $(d, e; f) = (\gamma - B, B; \gamma)$. Then $(\gamma - B, 0; \gamma), (i - xB, B; \gamma) \in T_i'$. In the remaining rows we are simply swapping entries between column 0 and column B, so these rows are clearly balanced. For $(d, e; f) = (i - xB, 0; i - xB)$, observe that $(\gamma - B, 0; \gamma) \in T_i'$. Otherwise if $(d, e; f) = (i - \alpha B - B, 0; i - \alpha B - B)$ for some

$0 \leq \alpha < x-1$, then observe that $(i-(\alpha+1)B-B, 0; i-\alpha B-B) \in T_i'$. It follows that column 0 is balanced.

To see that column B is balanced, first consider $(i-B, B; i) \in T_i$. From Theorem 1, $(0, B; 0) \in I'_{\gamma-(i+B),B}$. Thus $(i, B; i) \in T_i'$. Otherwise $(d, e; f) = (i-\alpha B-B, B; i-\alpha B)$ for some $0 < \alpha < x$ and $(i-\alpha B, B; i-\alpha B) \in T_i'$.

For the second subcase, our latin trade T_i is:

$$(I_{i+B-\gamma,B} \setminus \{(i+B-\gamma, B; 0)\}) \oplus (\gamma - B, 0) \cup \{(i, B; i+B)\}$$
$$\cup \{(i-\alpha B-B, B; i-\alpha B), (i-\alpha B-B, 0; i-\alpha B-B) \mid 0 \leq \alpha < x\}.$$

The disjoint mate of this latin trade, T_i', is equal to:

$$(I'_{i+B-\gamma,B} \setminus \{(i+B-\gamma, 0; 0)\}) \oplus (\gamma - B, 0) \cup \{(i, 0; i)\}$$
$$\cup \{(i-\alpha B-B, 0; i-\alpha B), (i-\alpha B-B, B; i-\alpha B-B) \mid 0 \leq \alpha < x\},$$

where $I'_{i+B-\gamma,B}$ is the disjoint mate of latin trade $I_{\gamma-(i+B),B}$. (All rows, columns and entries are calculated modulo n.) The proof that T_i is indeed a latin trade with disjoint mate T_i' is very similar to the previous subcase.

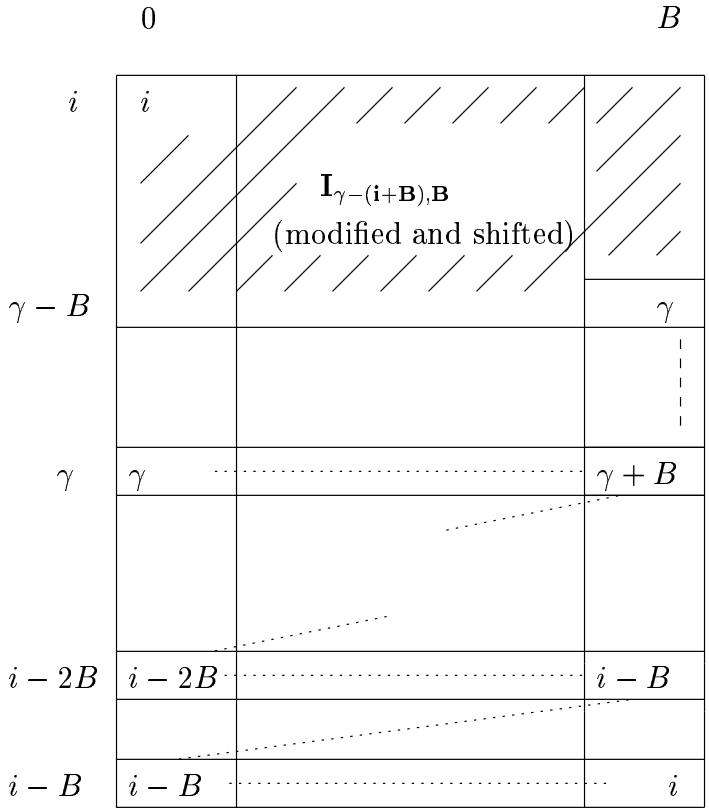

Figure 2: The latin trade T_i, where $\gamma > i + B$.

We will next show that if $i \neq j$, T_i and T_j intersect only within rows 0 through to $a-1$. First observe that each T_i intersects rows a through to $n-1$ exactly in rows

$i - B$, $i - 2B, \ldots i - xB = i - x(i)B$. For the sake of a contradiction, assume that $i - k_1 B = j - k_2 B \pmod{n}$ for some $k_1 \leq x(i)$ and $k_2 \leq x(j)$. If $k_1 = k_2$, then $i = j$. Otherwise suppose that $i \neq j$ and let $k_2 < k_1$. Then $i - (k_1 - k_2)B = j \pmod{n}$. But since $0 \leq j < a$, $B \leq j + B < B + a$, implying $B \leq i - (k_1 - k_2 - 1)B \pmod{n} < B + a$, contradicting the minimality of $x(i)$. The case $k_1 < k_2$ is analagous.

Thus, since C is a critical set, and C contains no entries in the intersection of the first a rows and the first b columns, C must intersect each latin trade T_i separately. Thus C has at least $\min(B, a) - 1$ entries in columns 0 and B.

Because of the cyclic nature of B_n, C must have at least $\min(B, a) - 1$ entries in every pair of columns of the form $i, B + i$, where $0 \leq i \leq \lfloor b/2 \rfloor - 1$. Thus if $B \leq a$, C has at least $\lfloor b^2/4 \rfloor$ elements in columns 0 through to $B - 1$. Otherwise $B > a$, and C has at least $a\lfloor b/2 \rfloor$ elements in columns 0 through to $b - 1$.

Similarly, by considering latin trades in the rows rather than the columns, we have: that C has at least

$$\min\left(\lfloor a^2/4 \rfloor, b\lfloor a/2 \rfloor\right)$$

entries in rows 0 through to $a - 1$. □

Example 5 *This example illustrates a latin trade constructed by the proof of the previous theorem. Here* $n = b = 15$, $i = r = c = 0$, $B = 8$ *and* $\beta = 13$. *Essentially, we have taken the latin trade* $I_{5,8}$ *from Example* 2, *removed the element* $(5, 8; 0)$, *embedded the resultant partial latin square in* B_{15}, *and finally added a zig-zagging sequence between columns* 0 *and* 8 *to create a latin trade in* B_{15}.

0					5			8
					8		10	11
							11	12
5					10		12	13
6								14
7								0
13								6
14								7

The latin trade

5					8			0
					10		11	8
							12	11
13					5		10	12
14								6
0								7
6								13
7								14

Its disjoint mate

Figure 3

Theorem 6 *Let* $n \geq 8$. *The size of a critical set in* B_n *is at least* $n^{4/3}/2 - n - n^{2/3}/2 + 2n^{1/3} - 1$.

Proof Consider a set of a contiguous rows in B_n; call them a "strip" of width a. Either, a strip of width a contains an $a \times b$ rectangle with no elements from the critical set C, or it doesn't. If it does then from the previous lemma there must be at least $\min(\lfloor a^2/4 \rfloor, b\lfloor a/2 \rfloor)$ elements of C in that strip of width a. If B_n does not contain an $a \times b$ rectangle with no entries from C, there must be at least $\lceil n/b \rceil$ entries from C in the strip to prevent it. So there are at least $\min(\lfloor a^2/4 \rfloor, b\lfloor a/2 \rfloor, \lceil n/b \rceil)$ elements of C in a strip of width a. Since B_n contains $\lfloor n/a \rfloor$ strips of width a, then $|C| \geq \lfloor n/a \rfloor \min(\lfloor a^2/4 \rfloor, b\lfloor a/2 \rfloor, \lceil n/b \rceil)$.

Let $a = 2\lfloor n^{1/3} \rfloor$ and $b = \lfloor n^{1/3} \rfloor$. We get

$$|C| \geq \left\lfloor \frac{n}{2\lfloor n^{1/3} \rfloor} \right\rfloor \min((\lfloor n^{1/3} \rfloor)^2, \left\lceil \frac{n}{\lfloor n^{1/3} \rfloor} \right\rceil).$$

But

$$\left\lceil \frac{n}{\lfloor n^{1/3} \rfloor} \right\rceil \geq \frac{n}{n^{1/3}} = n^{2/3} \geq (\lfloor n^{1/3} \rfloor)^2.$$

Therefore,

$$\begin{aligned} |C| &\geq \left\lfloor \frac{n}{2\lfloor n^{1/3} \rfloor} \right\rfloor (\lfloor n^{1/3} \rfloor)^2 \\ &\geq \left(\frac{n}{2(n^{1/3} - \epsilon)} - \delta\right)(n^{1/3} - \epsilon)^2 \text{ where } \epsilon, \delta \in \mathbb{R} \text{ and } 0 \leq \epsilon, \delta < 1 \\ &\geq \left(\frac{n}{2n^{1/3}} - 1\right)(n^{1/3} - 1)^2 \\ &= \frac{n^{4/3}}{2} - n - \frac{n^{2/3}}{2} + 2n^{1/3} - 1. \end{aligned}$$

□

Corollary 7 *If $n = a^3$ for some even integer a, then the size of a critical set in B_n is at least $n^{4/3}/2$.*

Proof If n is the product of an even cube, ϵ and δ are 0 in the proof of the above theorem. □

Acknowledgments I would like to thank Professor John van Rees whose comments were very helpful in writing the final theorem.

References

[1] 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.

[2] J. A. Bate and G. H. J. van Rees, The size of the smallest strong critical set in a latin square, *Ars Combinatoria* 53 (1999), 73–83.

[3] N. J. Cavenagh, A superlinear bound for the size of a critical set in a latin square, submitted.

[4] N. J. Cavenagh and A. Khodkar, Balanced critical sets in latin squares, *Utilitas Math.* 64 (2003), 229–249.

[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] C-M. Fu, H-L. Fu and C. A. Rodger, The minimum size of critical sets in latin squares, *J. Stat. Plan. Inference* 62 (1997), 333–337.

[8] P. Horak, R. E. L. Aldred and H. Fleischner, Completing latin squares: critical sets, *J. Combin. Designs* 10 (2002), 419–432.

[9] A. D. Keedwell, Critical sets in latin squares and related matters: an update, *Utilitas Math.* 65 (2004), 97–131.

[10] A. P. Street, "Trades and defining sets," CRC Handbook of Combinatorial Designs, C. J. Colbourn and J. H. Dinitz (Editors), CRC Press, New York, 1996, pp. 474–478.

[11] I. Wanless, Cycle switches in latin squares, *Graphs and Combin.* 20 (2004), 545–570.

(Received 19 July 2005; revised 18 Oct 2005)