Critical Sets in Back Circulant Latin Rectangles

E.S. Mahmoodian*

Department of Mathematical Sciences, Sharif University of Technology
P.O. Box 11365–9415, Tehran, IRAN
emahmood@rose.ipm.ac.ir

G.H.J. van Rees†

Department of Computer Science, University of Manitoba
Winnipeg, Manitoba, R3T 2N2, CANADA
vanrees@cs.umanitoba.ca

Dedicated to the memory of Derrick Breach, 1933–1996

Abstract

A *latin rectangle* is an $m \times n$ array, $m \leq n$, from the numbers $1, 2, \ldots, n$ such that each of these numbers occur in each row and in each column at most once. A *critical set* in an $m \times n$ array is a set S of given entries, such that there exists a unique extension of S to a latin rectangle of size $m \times n$. If we index the rows and columns of an $m \times n$ array, $m \leq n$, by the sets $M = \{1, 2, \ldots, m\}$ and $N = \{1, 2, \ldots, n\}$, respectively, then the array with integer $i + j - 1 \pmod n$ in the position (i, j) is said to be a *back circulant latin rectangle.* We show that the size of smallest critical set in a back circulant latin rectangle of size $m \times n$, with $4m \leq 3n$ is equal to $m(n - m) + \lfloor (m - 1)^2/4 \rfloor$.

1 Introduction

A *latin rectangle* is an $m \times n$ array, $m \leq n$, from the numbers $1, 2, \ldots, n$ such that each of these numbers occur in each row and in each column at most once. *A critical set* in an $m \times n$ array is a set S of given entries, such that there exists a unique

*The first author would like to thank the Department of Computer Science at the University of Manitoba for their hospitality as the paper was extensively developed there when he was visiting the second author. Also he thanks Institute for Theoretical Physics and Mathematics (IPM) for partial support of this research.

†The research of the second author was supported by NSERC Grant OGP0003558.

extension of S to a latin rectangle of size $m \times n$. There are some papers on critical sets of latin squares. The interested reader may start with [2] and [5] and their references. If we index the rows and columns of an $m \times n$ array, $m \leq n$, by the sets $M = \{1, 2, \ldots, m\}$ and $N = \{1, 2, \ldots, n\}$, respectively, then the array with integer $i + j - 1 \pmod{n}$ in the position (i, j) is said to be a *back circulant latin rectangle.* A critical set which contains no proper subset as a critical set is called a *minimal critical set*, and the one with the minimum cardinality is called a *minimum critical set*. What we define as a "minimum critical set", other authors define as a "critical set". The following important result can be found in [1].

Theorem A. [1] *Let L be a back circulant latin square of order n. Then L contains a minimal critical set of size* $\lfloor n^2/4 \rfloor$.

A minimal critical set of size $\lfloor n^2/4 \rfloor$, given in [1] is easily seen to be a minimum critical set when n is even. But whether the size of minimum critical set is $\lfloor n^2/4 \rfloor$, in the case of n being odd is an open question. Mahmoodian, Naserasr and Zaker [4] proved the following,

Theorem B. [4] *Let L be an* $m \times n$ *back circulant latin rectangle, where* $2m \leq n$. *Then L contains a critical set of size* $m(n-m) + \lfloor (m-1)^2/4 \rfloor$, *which is the smallest critical set for such a latin rectangle.*

We prove further that the result of Theorem B holds when $4m \leq 3n$. We refer to [4] for further definitions and notation. We make two new definitions. A *circular movement* is a permutation, $(a_{i,1}, a_{i,2}, \cdots, a_{i,r})$ of the numbers from some row i of an $m \times n$ latin rectangle such that if the permutation is applied to the numbers in that row of the latin rectangle (i.e. if in the row i the element $a_{i,2}$ is replaced with $a_{i,1}$, $a_{i,3}$ with $a_{i,2}, \cdots$, and $a_{i,1}$ with $a_{i,r}$) then the result is also a latin rectangle. We let the set of allowable differences between successive elements in the permutation be called the *difference* of the circular movement. We call it the set D.

Example 1.

1	2	3	4	5	6	7	8	9
2	3	4	5	6	7	8	9	1
3	4	5	6	7	8	9	1	2
4	5	6	7	8	9	1	2	3
5	6	7	8	9	1	2	3	4
6	7	8	9	1	2	3	4	5
7	8	9	1	2	3	4	5	6

is a 7×9 back circulant latin rectangle.
$(2, 5, 8)$ is a circulant movement in row 2. If it is applied to the latin rectangle we get:

1	2	3	4	5	6	7	8	9
8	3	4	2	6	7	5	9	1
3	4	5	6	7	8	9	1	2
4	5	6	7	8	9	1	2	3
5	6	7	8	9	1	2	3	4
6	7	8	9	1	2	3	4	5
7	8	9	1	2	3	4	5	6

Also $(4, 9)$ is a circulant movement in row 4 of either latin rectangle. D for row 3 of the first latin rectangle is $\{3, 4\}$.

It is quite clear that any critical set must intersect a circular movement in at least one element.

2 Main Theorem

Mahmoodian, Naserasr and Zaker [4], proved the following which we state as the following lemmas.

Lemma 1. *In a back circulant $m \times n$ latin rectangle, if $n - 2m + 2i - 1 > 0$ and $i \leq \lceil m/2 \rceil$, then row i must intersect any critical set in at least $n-m+i-1$ elements.*

Proof. The latin rectangle must look like the following array, where all numbers are modulo n:

$$
\begin{array}{cccccccccccccccccc}
1 & 2 & \cdot & \cdot & \cdot & i & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & n \\
2 & \cdot & \cdot & \cdot & i & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & i & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
i & \cdot & \cdot & \cdot & \cdot & \cdot & 2i & \cdot & m & m+1 & \cdot & \cdot & n-m+2i-1 & n-m+2i & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & m & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
m & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & i-1 & i & \cdot & \cdot & \cdot & \cdot
\end{array}
$$

Then $(i, m + 1), (i, m + 2), \cdots, (i, n - m + 2i - 1)$ are $n - 2m + 2i - 1$ circular movements and by using Lemma 1 in [4], we find that row i and any critical set of the latin rectangle must intersect in $(n + (n - 2m + 2i - 1) - 1)/2 = n - m + i - 1$ elements. Note that $n - 2m + 2i - 1 > 0$, giving the stated hypothesis. $\square$

Lemma 2. *In a back circulant $m \times n$ latin rectangle, if* $\lceil m/2 \rceil < i \leq n/2$, *then row i must intersect any critical set in at least $n - i$ elements.*

Proof. It follows by symmetry and by previous lemma. □

Using Lemma 1 and 2, Mahmoodian, Naserasr and Zaker [4], proved Theorem B. They construct and prove that the following:

$$\{(i,j) \mid i \leq \lfloor m/2 \rfloor, 1 \leq j \leq n-m+i-1\} \cup \{(i,j) \mid i > \lfloor m/2 \rfloor, i+1 \leq j \leq n\}$$

is a set which uniquely completes to the back circulant latin rectangle. This set has $m(n-m) + \lfloor (m-1)^2/4 \rfloor$ elements and intersects row i in $n-m+i-1$ elements if $i \leq \lceil m/2 \rceil$ and in $n-i$ elements if $i > \lceil m/2 \rceil$. By previous lemmas, no critical set could be smaller.

In [4] they got their result by looking at circular movements that were transpositions. We will look at circular movements that are larger.

Lemma 3. *A row i in an $m \times n$ back circulant latin rectangle must intersect any critical set in at least $n - m$ consecutive numbers, where n is considered consecutive to 1 and wrap around is allowed.*

Proof. In row i of an $m \times n$ back circulant latin rectangle, the difference set D, which has $n-m$ elements, is $D = \{i, i+1, \ldots, n-m+i-1\}$. We associate a (directed) graph G_i to row i, where $V(G_i) = \{1, 2, \ldots, n\}$, and jk is an arc in G_i (starting from j and ending in k) if the element k, in the row i, can be replaced by j; i.e. $k - j \in D$. Note that any circuit (directed cycle) in G_i is a circular movement in row i. Thus, the intersection of any critical set with row i is a covering for the circuits of G_i. Suppose S is a covering for the circuits in row i. By removing the set of vertices in S from G_i, there will be no circuit left in the resulting subgraph. Thus there is at least one vertex v whose outdegree in the subgraph is equal to zero. In other words all of the vertices that v is adjacent to, in G_i, are removed. Therefore $|S| \geq n-m$. Hence there are $n-m$ consecutive numbers in row i that intersect with the critical set. □

Lemma 4. *In a back circulant $m \times n$ latin rectangle, if $i \leq n-m$ and $i \leq \lceil m/2 \rceil$, then row i must intersect any critical set in at least $n-m+i-1$ elements.*

Proof. For row i we have $D = \{i, i+1, \ldots, n-m+i-1\}$. Let S be a critical set of the latin rectangle. By Lemma 3 we know that there are at least $n-m$ (therefore at least $i-1$) consecutive elements in row i that intersect this critical set. Consider the last $i-1$ of these so that the next element is not in S. Without loss of generality let the $i-1$ consecutive elements in the critical set and row i be $n-i+2, n-i+3, \ldots, n-1, n$ and let 1 not be in the critical set. Then consider the following $n-m$ circular movements, all starting with 1 and the numbers from

$i+1$ to $n-i+1$, inclusive, written down in order in the columns of the circular movements:

$$
\begin{array}{lllllll}
(1, & i+1, & i+1+n-m, & i+1+2n-2m, & \ldots, & ., & a) \\
(1, & i+2, & i+2+n-m, & i+2+2n-2m, & \ldots, & ., & a+1) \\
(1, & i+3, & i+3+n-m, & i+3+2n-2m, & \ldots, & ., & a+2) \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\
(1, & ., & ., & ., & \ldots, & ., & n-i+1) \\
(1, & ., & ., & ., & \ldots, & n-i+2) & \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \\
(1, & i+n-m, & i+2n-2m\ , & i+3n-3m, & \ldots, & a-1) &
\end{array}
$$

Here we have $m-i+2 \leq a \leq n-i+1$. All the differences are $n-m$, expect for, perhaps, the wrap around differences and the difference between the first and second elements. Since $n-m \geq i$, so $n-m \in D$. The differences between the first and second elements are $i, i+1, \ldots, n-m+i-1$ from top to bottom. The wrap around differences are also from the set $\{i, i+1, \ldots, n-m+i-1\}$, but not necessarily in that order. Hence these are circular movements that must intersect S. Since 1 is not in S and the rest of the elements of the circular movements are disjoint, there must be $n-m$ intersections between S and the elements $i+1, i+2, \ldots, n-i+1$. But $n-i+2, n+i+3, \ldots, n$ are also in the critical set. Hence row i and S intersect in $n-m+i-1$ elements. □

Theorem. (MAIN) *Let L be an $m \times n$ back circulant latin rectangle, where $4m \leq 3n$. Then L contains a critical set of size $m(n-m) + \lfloor (m-1)^2/4 \rfloor$, which is the smallest critical set for such a latin rectangle.*

Proof. Suppose $i \leq \lceil m/2 \rceil$. Since $4m \leq 3n$ we have either $n-2m+2i-1 > 0$ or $i \leq n-m$. Thus by Lemma 4, row i and a critical set must intersect in at least $n-m+i-1$ elements. By symmetry, as in Lemma 2, if $\lceil m/2 \rceil < i \leq m$, then row i must intersect any critical set in at least $n-i$ elements. Hence, if S is a critical set, then

$$
\begin{aligned}
|S| \geq\ & [(n-m)+(n-m+1)+\cdots+(n-m+\lfloor m/2 \rfloor -1)] \\
& +\tfrac{1}{2}(1+(-1)^{m+1})(n-m+\lfloor m/2 \rfloor) \\
& +[(n-m+\lfloor m/2 \rfloor -1)+\cdots+(n-m+1)+(n-m)] \\
& = m(n-m)+\lfloor (m-1)^2/4 \rfloor .
\end{aligned}
$$

If in a back circulant latin rectangle of size $m \times n$ we take the entries of the set S, where

$$
\begin{aligned}
S \ =\ & \{(i,j) | i \leq \lfloor m/2 \rfloor,\ \lfloor m/2 \rfloor - (i-1) \leq j \leq n - \lceil m/2 \rceil - 1\} \\
& \cup \{(i,j) | i > \lfloor m/2 \rfloor,\ \lfloor m/2 \rfloor + 1 \leq j \leq n + \lfloor m/2 \rfloor - i\},
\end{aligned}
$$

then S is a critical set of size $m(n-m) + \lfloor (m-1)^2/4 \rfloor$. □

Remark 1. Note that the condition $4m \leq 3n$ is the best possible we can get with our method of using Lemma 3 and 4. For example in a 7×9 back circulant latin rectangle (see Example 1) we do not necessarily need 4 elements in any critical set from row 3. In fact, if we take all elements of that rectangle, except a set of 6 consecutive elements from row 3, we will get a critical set.
Remark 2. It is conjectured by both of the present authors, independently, that

Conjecture . ([3] and [5]) *For any latin square of order n the cardinality of any critical set is greater than or equal to* $\lfloor n^2/4 \rfloor$.

The results such as the one in the main theorem above, are attempts toward settling that conjecture.
Remark 3. We thank M. Mahdian for his comments on this paper.

References

[1] J. Cooper, D. Donovan, and J. Seberry, *Latin squares and critical sets of minimal size*, Australasian Journal of Combinatorics, 4 (1991), pp. 113–120.

[2] ——, *Secret sharing schemes arising from latin squares*, Bulletin of Institute of Combinatorics and its Applications, 12 (1994), pp. 33–43.

[3] E. S. Mahmoodian, *Some problems in graph colorings*, in Proc. 26th Annual Iranian Math. Conference, S. Javadpour and M. Radjabalipour, eds., Kerman, Iran, Mar. 1995, Iranian Math. Soc., University of Kerman, pp. 215–218.

[4] E. S. Mahmoodian, R. Naserasr, and M. Zaker, *Defining sets of vertex coloring of graphs and latin rectangles*, Discrete Mathematics, 1997 (to appear).

[5] G. H. J. van Rees and J. A. Bate, *The size of the smallest strong critical set in a latin square*, Ars Combin., (submitted).

(Received 26/2/97)