ELSEVIER Discrete Mathematics 167/168 (1997) 451–460

DISCRETE MATHEMATICS

Defining sets in vertex colorings of graphs and latin rectangles

E.S. Mahmoodian*, Reza Naserasr, Manouchehr Zaker

Department of Mathematical Sciences, Sharif University of Technology, P.O. Box 11365-9415, Tehran, Iran

Received 7 July 1995; revised 30 January 1996

Abstract

In a given graph G, a set of vertices S with an assignment of colors is said to be a *defining set of the vertex coloring of* G, if there exists a unique extension of the colors of S to a $\chi(G)$-coloring of the vertices of G. The concept of a defining set has been studied, to some extent, for block designs and also under another name, a *critical set*, for latin squares. In this note we extend this concept to graphs, and show its relationship with the critical sets of latin rectangles. The size of smallest defining sets for some classes of graphs are determined and a lower bound is introduced for an arbitrary graph G. The size of smallest critical sets of a back circulant latin rectangle of size $m \times n$, with $2m \leqslant n$, is also determined.

1. Introduction

A *latin rectangle* is an $m \times n$ array, $m \leqslant n$, from the numbers $1,2,\dots,n$ 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 $m \times n$. There are some papers on critical sets of latin squares. The interested reader may start with [4] and its references. In [4], application of critical sets in latin squares to secret sharing schemes is shown. If we index the rows and columns of an $m \times n$ array, $m \leqslant n$, by the sets $M = \{1,2,\dots,m\}$ and $N = \{1,2,\dots,n\}$, 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*. The following important result can be found in [3].

Theorem A (Cooper et al. [3]). *Let L be a back circulant latin square of order n. Then L contains a minimal critical set of size $\lfloor n^2/4 \rfloor$.*

* Corresponding author. E-mail: emahmood@vax.ipm.ac.ir.

PII S0012-365X(96)00247-6

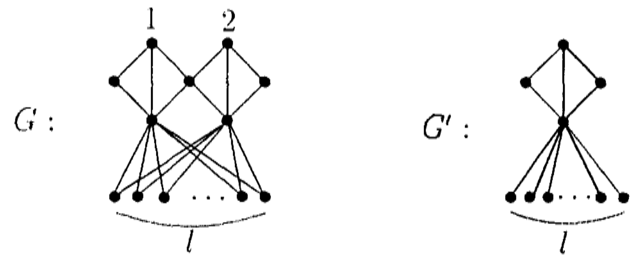

Fig. 1. $d_v(G) < d_v(G')$.

The problem of finding critical sets in latin squares with minimum cardinality is an open question. We study a similar concept for graphs and show that the critical sets of latin squares are just defining sets of some special graphs.

We consider (simple) graphs which are finite, undirected, with no loops or multiple edges. We will use standard notations such as K_n for the complete graph on n vertices, C_n for the cycle of size n, and P_n for the path with n vertices. For the necessary definitions and other notations we refer the reader to texts, such as [2]. In this section we mention some of the definitions and results which are referred to throughout the paper. A *k-coloring* of a graph G is an assignment of k different colors to the vertices of G, such that no two adjacent vertices receive the same color. The *vertex chromatic number* of a graph G, denoted by $\chi(G)$, is the minimum number k, for which there exists a k-coloring for G. In a given graph G, a set of vertices S with an assignment of colors is said to be a *defining set of vertex coloring*, if there exists a unique extension of the colors of S to a $\chi(G)$-coloring of the vertices of G. A defining set with minimum cardinality is called a *minimum defining set* (of vertex coloring) and its cardinality is denoted by $d_v(G)$. For example this parameter in the case of a connected bipartite graphs is equal to 1, and for $K_4 - e$ is equal to 2. As an another interesting example, one may check that $d_v(P) = 4$, for the Petersen graph P. Also $d_v(C_{2n+1}) = n + 1$; for, from every two adjacent vertices in C_{2n+1}, one must be included in any defining set. Note that for any graph G we have $d_v(G) \geqslant \chi(G) - 1$.

The following example shows that, in general, $d_v(G') \leqslant d_v(G)$ when G' is a subgraph of G, is not true; even if $\chi(G) = \chi(G')$.

In the graph G the set of vertices with the color numbers given as in Fig. 1, is a defining set. So $d_v(G) = 2$, but clearly $d_v(G') \geqslant l$.

The concept of defining sets is defined for block designs. See [7] for a survey.

Since any $m \times n$ latin rectangle, $m \leqslant n$, is equivalent to an n-coloring of the graph $K_m \times K_n$, it is of interest to explore the concept of defining sets of vertex colorings of graphs. In Section 2 we state some results on this problem. Any defining set of a vertex coloring of $K_m \times K_n$, is a critical set for an $m \times n$ latin rectangle. In Section 3 we find critical sets of some back circulant latin rectangles.

The following theorem of M. Hall, which is a corollary of the celebrated Marriage Theorem of P. Hall, is very useful in our proofs.

Theorem B (Hall [5]). *If n sets $S_1,\dots,S_n$ have a system of distinct representatives — SDR — and the smallest of these sets contains t objects, then if $t \geqslant n$, there are at least $t(t-1)\cdots(t-n+1)$ different SDRs, and if $t<n$, there are at least $t!$ different SDRs.*

2. Defining sets in vertex colorings

In the following theorem a lower bound for the size of a defining set in a graph G is given.

Theorem 1. *For every graph G we have*

$$d_{\mathrm{v}}(G) \geqslant |V(G)| - \frac{|E(G)|}{\chi(G)-1}.$$

Proof. Let S be a defining set of size $d_{\mathrm{v}}(G)$ and consider the extension of the coloring of S to a $\chi(G)$-coloring of the vertices of G. Denote the number of vertices with color i in S by r_i, and in G by v_i. Let G_{ij} be the induced subgraph of G over the vertices with color i and j. We claim that S contains at least one vertex from each component of G_{ij}. Suppose a component of G_{ij} does not intersect S, then by permuting the colors i and j in that component, one obtains a new $\chi(G)$-coloring for G. Thus, the number of components in G_{ij} is at most r_i+r_j. Therefore there are at least $(v_i+v_j)-(r_i+r_j)$ edges in G_{ij}. Now, if we sum up this for all i and j such that $1 \leqslant i < j \leqslant \chi(G)$, we obtain

$$|E(G)| \geqslant (\chi(G)-1)(|V(G)| - d_{\mathrm{v}}(G));$$

from which the assertion follows. □

Corollary. *The size of a minimum defining set of the cartesian product of K_2 by C_{2n+1} is*

$$d_{\mathrm{v}}(K_2 \times C_{2n+1}) = n+1.$$

Proof. Let $G = K_2 \times C_{2n+1}$. From Theorem 1 we obtain $d_{\mathrm{v}}(G) \geqslant n+\frac{1}{2}$. Thus, $d_{\mathrm{v}}(G) \geqslant n+1$. To show equality we give a defining set, S, of size $n+1$ as in Fig. 2. Note that all the vertices in S are labeled by their colors. The colors a and b depend on n, where:

$$2n+1 = 3k; \quad a=1,\ b=2$$

$$2n+1 = 3k+1; \quad a=2,\ b=2$$

$$2n+1 = 3k+2; \quad a=3,\ b=3. \qquad \square$$

The following theorem on defining sets of $G \times K_n$ will be useful in the discussion of critical sets in latin rectangles.

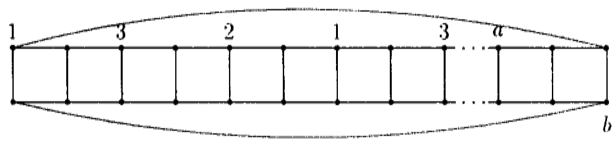

Fig. 2. $G = K_2 \times C_{2n+1}$.

Theorem 2. *For any graph G, such that* $\chi(G) \leqslant n$ *we have*

$$d_v(G \times K_n) \geqslant |V(G)|(n-1) - 2|E(G)|.$$

Proof. By [1], we have $\chi(G \times K_n) = n$. Let $|V(G)| = m$, $V(K_n) = \{1,2,\ldots,n\}$, and $V(G) = \{1,2,\ldots,m\}$. We note that $G \times K_n$ which is isomorphic to $K_n \times G$, has mn vertices, which contains m 'horizontal' copies of K_n, say $K_n^{(1)}, K_n^{(2)}, \ldots, K_n^{(m)}$, (ordered from top to bottom), and n 'vertical' copies $G^{(1)}, G^{(2)}, \ldots, G^{(n)}$ (ordered from left to right) of G. A horizontal copy $K_n^{(i)}$ and a vertical copy $G^{(j)}$ have only one vertex (i,j) in common. Now let S be a defining set for $G \times K_n$ and let $d_1, d_2, \ldots, d_m$ be the degree sequence of G. We show that for each i, at least $n - d_i - 1$ vertices of $K_n^{(i)}$ belong to S. Suppose on the contrary, there exists an i such that fewer than $n - d_i - 1$ vertices of $K_n^{(i)}$ belong to S. In other words, the colors of at least $d_i + 2$ vertices, say $T = \{t_1, t_2, \ldots, t_{d_i+2}\}$, of $K_n^{(i)}$ are not given. Assume that the colors of all vertices of $G \times K_n$, except the ones in T are given. Let T_j be the set of colors available for the vertex t_j, $j = 1,2,\ldots,d_i + 2$; that is the set of colors which do not appear in the neighborhood of t_j in S. Since S is a defining set, there exists an *SDR* for T_j's. We have

$$|T_j| \geqslant n - ((n - d_i - 2) + d_i) = 2, \quad j = 1,2,\ldots,d_i + 2.$$

By Theorem 1, there exist at least two *SDR*s. This contradicts the assumption that the set S is a defining set. Now, since S contains at least $n - d_i - 1$ vertices from each horizontal copy,

$$|S| \geqslant \sum_{i=1}^{m} (n - d_i - 1) = m(n-1) - 2|E(G)|. \qquad \square$$

If in Theorem 2 we let $G = K_m$ then we have

Corollary. *For* $n \geqslant m$,

$$d_v(K_m \times K_n) \geqslant m(n-m).$$

Next we discuss defining sets of cartesian products of cycles by complete graphs. The results of Theorems 3–5 show that the lower bound in Theorem 2 is a good bound.

Theorem 3. *For* $n \geqslant 6$ *we have*

$$d_v(C_m \times K_n) = m(n-3).$$

Proof. If in Theorem 2 we let $G = C_m$, we obtain

$$d_v(C_m \times K_n) \geqslant m(n-3).$$

To show equality, we need the following notation. For an ordered triple *abc* we denote the three permutations *abc* (the identity permutation), *bca*, and *cab* by σ_1, σ_2, and σ_3, respectively. Note that in the latin square

$$\begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix},$$

given any two rows, the remaining row can be determined uniquely. To proceed, we note that if the vertices of $C_m \times K_n$ are in an $m \times n$ array in each row of which we have a subgraph K_n, then as in the proof of Theorem 2 any defining set must contain at least $n-3$ vertices of each row.

We consider two cases for m:

(i) *m even*. For $n = 6$, a defining set is given as follows,

(σ_1)	1	2	3	*	*	*	
	*	*	*	4	5	6	(σ_1)
(σ_2)	2	3	1	*	*	*	
	*	*	*	5	6	4	(σ_2)
		⋮			⋮		
(σ_1 or σ_2)	⊙	⊙	⊙	*	*	*	
	*	*	*	⊙	⊙	⊙	(σ_1 or σ_2)
(σ_3)	3	1	2	*	*	*	
	*	*	*	6	4	5	(σ_3)

In the above table in the first three columns we use only the colors 1, 2, and 3. And in this coloring, for example in the third row, we have used the permutation σ_2 of $\{1,2,3\}$, which is 231. Here a ⊙ sign, means that the color in that entry is given, while a $*$ sign, means that the color of that entry is not given.

For $n \geqslant 8$, a defining set can be given such a way that only the colors $1, 2, \ldots, 6$ are used in the first six columns of $C_m \times K_n$, similar to the case of $n = 6$, and the colors of the vertices in the last $n-6$ columns are all given.

For $n = 7$, we treat $K_7 \times C_m$ in arrays of $m \times 3$ and $m \times 4$. The first array will be the same as the first $m \times 3$ array in the case of $n = 6$. For the second array, the following arrays can be used for $m = 4$ and $m = 6$, respectively,

*	*	*	4
7	6	4	5
*	4	*	*
4	5	6	7

*	*	7	*
5	7	6	4
7	*	*	*
5	6	4	7
*	*	7	*
4	5	6	7

Since the last row of first array is the same as the last row of second array, to obtain a defining set for any other even number m, one can use a suitable combinations of these two arrays.

(ii) *m odd.* For $n = 6$, the following are defining sets for $C_3 \times K_6$ and $C_5 \times K_6$, respectively,

1	2	3	*	*	*
*	*	5	4	*	3
2	*	*	6	4	*

5	3	1	*	*	*
*	*	*	5	6	4
1	2	3	*	*	*
*	*	5	4	*	3
2	*	*	6	4	*

To obtain a defining set for $C_m \times K_6$, where $m \geqslant 7$, since $m-3$ is even, one can combine the above array for $C_3 \times K_6$ with the one in the case of m even and $n = 6$.

For $n \geqslant 9$, as in the case of m even, one can use the defining set of $C_m \times K_6$, given above, to obtain a defining set for $C_m \times K_n$.

For $n = 7$, the following are defining sets for $C_3 \times K_7$ and $C_5 \times K_7$, respectively:

2	3	5	*	*	*	6
3	5	*	1	4	*	*
*	*	*	4	5	6	7

5	3	1	*	*	*	7
7	*	*	5	6	4	*
1	2	3	*	7	*	*
*	*	5	4	*	3	7
2	*	*	6	4	7	*

For $n = 8$, the following are defining sets for $C_3 \times K_8$ and $C_5 \times K_8$, respectively:

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

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

For $m \geqslant 7$, both of these cases ($n = 7$ and $n = 8$) can be dealt within the same way as in the case of $n = 6$. □

Theorem 4. *For* $n \geqslant 6$ *we have,*

$$d_v(P_m \times K_n) = m(n-3) + 2.$$

Proof. For $m = 1, 2$, it is trivial; and for $m \geqslant 3$ it is similar to Theorem 3. □

3. Critical sets in back circulant latin rectangles

As we noted earlier, an $m \times n$ latin rectangle, $m \leqslant n$, is equivalent to an n-coloring of graph $K_m \times K_n$. In the following, we first show that equality is possible in the corollary to Theorem 2, thus there exists $m \times n$ latin rectangles with $n \geqslant m^2$ and a critical set of size $m(n-m)$, but there is no such rectangle with a smaller critical set.

Theorem 5. *If* $n \geqslant m^2$, *then*

$$d_v(K_m \times K_n) = m(n-m).$$

Proof. We consider the following $m \times n$ latin rectangle,

$$L = [A_1 A_2 \ldots A_{m-1} A_m];$$

where each A_i, $i = 1, 2, \ldots, m-1$, is an $m \times m$ back circulant latin square, generated by the row,

$$(i-1)m+1 \quad (i-1)m+2 \quad \ldots \quad (i-1)m+m;$$

and A_m is an $m \times (n - m^2 + m)$ back circulant latin rectangle, generated by the row,

$$m^2 - m + 1 \quad m^2 - m + 2 \quad \ldots \quad n.$$

Now a critical set can be given which consists of all the entries of L, except the entries of the ith row of A_i, $i = 1, \ldots, m-1$, and the entries of the last row of A_m which are $m^2 - m + 1$, $m^2 - m + 2, \ldots,$ and m^2. It is easy to check that S is a critical set of $K_m \times K_n$, and $|S| = m(n-m)$. □

Next, we find the smallest critical set for back circulant latin rectangles of size $m \times n$, where $2m \leqslant n$. We use some graph theoretical methods. To understand the method, first we will show it in an example. The following lemma on cyclic graphs is very useful in our proof. A *cyclic* graph G on n vertices is one with an automorphism group containing the cyclic group $(\mathbf{Z}_n, +)$ as a subgroup.

Lemma 1. *Let n and d be two natural numbers such that $n - d$ is odd. Let G be a d-regular cyclic graph with vertex set $V(G) = \{1, 2, \ldots, n\}$ and $ij \in E(G)$, if $i - j \equiv r+1, r+2, \ldots,$* or *$r + d \bmod n$; where $r = (n-d-1)/2$. Then $\beta(G)$, the covering number of G, is equal to $n - r - 1$.*

Proof. An example of a cyclic graph with the conditions of the lemma where $n = 11$, $d = 2$, $r = 4$, is given in Fig. 3.

Since $\alpha(G) + \beta(G) = n$, where $\alpha(G)$ is the independence number of G, it is sufficient to show that $\alpha(G) = r + 1$. Suppose S is an independent set of vertices in G with maximum size. Without loss of generality, we can assume that $1 \in S$. We have $S \subseteq T = V(G) - \{r+2, r+3, \ldots, r+d+1\}$. But T contains r parallel edges $\{j, r+d+j\}$, $j = 2, 3, \ldots, r+1$. Therefore, $|S| \leqslant r + 1$. The set of vertices $\{1, 2, 3, \ldots, r+1\}$ is an independent set; thus $|S| = \alpha(G) = r + 1$. □

Example 1. Let L be a 5×11 back circulant latin rectangle. Then L contains a critical set of size 34, which is the smallest critical set for such a latin rectangle.

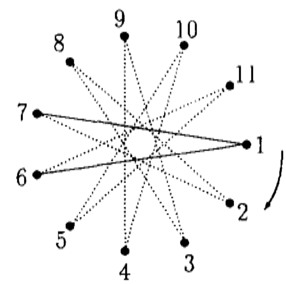

Fig. 3. G_1, a cyclic graph of Example 1.

Proof. In the following table a critical set with size 34 is shown for the back circulant latin rectangle of size 5×11:

(1)	(2)	(3)	(4)	(5)	(6)	7	8	9	10	11
(2)	(3)	(4)	(5)	(6)	(7)	(8)	9	10	11	1
(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	11	1	2
4	5	6	7	(8)	(9)	(10)	(11)	(1)	(2)	(3)
5	6	7	8	9	(10)	(11)	(1)	(2)	(3)	(4)

Now we prove that, this is the smallest critical set for that latin rectangle. Note that in each row there are some pairs that can be permuted. For example, in the first row if we permute 1 and 7, the resulting rectangle is still a latin rectangle. So any critical set must contain at least one of these entries. We associate a graph G_1 with the first row, with $V(G_1) = \{1,2,\ldots,11\}$, and $ij \in E(G_1)$ if the entries i and j can be permuted in the first row (see Fig. 3).

Let S be a critical set for L. The set of elements of S in the first row is a covering set for G_1. The graph G_1 satisfies the conditions of Lemma 1, where $n = 11$, $d = 2$, $r = 4$, and $\beta(G_1) = 6$. Thus, S contains at least 6 entries from the first row. Similarly we associate a graph G_2 with the second row. The set of elements of S in the second row is a covering set for G_2. The graph G_2 satisfies the conditions of Lemma 1, where $n = 11$, $d = 4$, $r = 3$, and $\beta(G_2) = 7$. Thus, S contains at least 7 elements from the second row. Similarly S must contain 8 elements from the third row. If G_k is the graph associated with the kth row, it can easily be checked that $G_1 = G_5$ and $G_2 = G_4$. Thus S must contain at least $6+7+8+7+6 = 34$ elements. □

Theorem 6. *Let L be an $m \times n$ back circulant latin rectangle, where $2m \leqslant n$. 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.*

Proof. As in Example 1, we associate a graph G_k with the kth row of L as follows. The set of vertices of G_k, is $V(G_k) = \{1,2,3,\ldots,n\}$, and $ij \in E(G_k)$ if and only if the entries i and j can be permuted in the kth row of L such that the resulting rectangle is still a latin rectangle.

First, we show that G_k, for $k \leqslant \lceil m/2 \rceil$, satisfies the hypotheses of Lemma 1. Indeed, since L is back circulant it follows that G_k is cyclic. As can be observed from the back circulant latin rectangle given below, in G_k, since $2m \leqslant n$, the neighborhood of vertex k is $\{m+1, m+2, \dots, n-m+2k-1\}$.

$$
\begin{array}{ccccccccccccccccccccc}
1 & 2 & \cdot & \cdot & \cdot & k & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & n \\
2 & \cdot & \cdot & \cdot & k & \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 & k & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
k & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot & m & \cdot & \cdot & \cdot & b & c & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & e \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & m & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & k \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & k & \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 & k & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
m & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & e & k & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
\end{array}
$$

Here, $a = 2k-1$, $b = n-m+2k-1$, $c = n-m+2k$, and $e = k-1$. So we have $d = n-2m+2k-1$ and $r = m-k$. Thus by Lemma 1, $\beta(G_k) = n-m+k-1$, $k \leqslant \lceil m/2 \rceil$.

Next, we show that $G_k = G_{m-k+1}$. This can be seen by noting that the neighborhood of vertex l in G_l, for $l \geqslant \lceil m/2 \rceil$ is $\{2l, \dots, n\}$. Now suppose that S is a critical set for L. Then the elements of S in row k must be a covering set for G_k. Therefore,

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

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

$$S = \{(i,j) | i \leqslant \lceil m/2 \rceil,\ 1 \leqslant j \leqslant n-m+i-1\} \cup \{(i,j) | i > \lceil m/2 \rceil,\ i+1 \leqslant j \leqslant n\},$$

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

In [3] it is proved that the smallest critical set for a back circulant latin square of order n is $n^2/4$, for n even. The following conjecture is made in [6].

Conjecture (*Mahmoodian* [6]). For any latin square of order n the cardinality of any critical set is greater than or equal to $\lfloor n^2/4 \rfloor$.

Acknowledgements

The authors are very grateful to Ali Asghar Khanban for his invaluable comments. This research is supported by the Sharif University of Technology.

References

[1] M. Behzad and E.S. Mahmoodian, On topological invariants of the product of graphs, Canad. Math. Bull. 12 (1969) 157–166.

[2] J.A. Bondy and U.S.R. Murty, Graph Theory with Applications (Elsevier, New York, 1976).

[3] J. Cooper, D. Donovan and J. Seberry, Latin squares and critical sets of minimal size, Austral. J. Combin. 4 (1991) 113–120.

[4] J. Cooper, D. Donovan and J. Seberry, Secret sharing schemes arising from latin squares, Bull. Inst. Combin. Appl. 12 (1994) 33–43.

[5] M. Hall, Combinatorial Theory (Wiley, New York, 2nd ed., 1986).

[6] E.S. Mahmoodian, Some problems in graph colorings, in: S. Javadpour and M. Radjabalipour, eds., Proc. 26th Ann. Iranian Math. Conf., Kerman, Iran, March 1995 (Iranian Math. Soc., University of Kerman, 1995, 215–218.

[7] A.P. Street, Defining sets for block designs: an update, in: C.J. Colbourn and E.S. Mahmoodian, eds., Combinatorics Advances, Mathematics and Its Applications (Kluwer, Dordrecht, 1995) 307–320.