

# On the forced matching numbers of bipartite graphs

Peter Adams<sup>a,1</sup>, Mohammad Mahdian<sup>b</sup>, E.S. Mahmoodian<sup>c</sup>

<sup>a</sup>*Department of Mathematics, The University of Queensland, Brisbane 4072, Australia*

<sup>b</sup>*Department of Mathematics, MIT, Cambridge, MA 02139, USA*

<sup>c</sup>*Department of Mathematical Sciences, Sharif University of Technology,  
P.O. Box 11365-9415, Tehran, I.R. Iran*

## Abstract

Let  $G$  be a graph that admits a perfect matching. A *forcing set* for a perfect matching  $M$  of  $G$  is a subset  $S$  of  $M$ , such that  $S$  is contained in no other perfect matching of  $G$ . This notion has arisen in the study of finding resonance structures of a given molecule in chemistry. Similar concepts have been studied for block designs and graph colorings under the name *defining set*, and for Latin squares under the name *critical set*. There is some study of forcing sets of hexagonal systems in the context of chemistry, but only a few other classes of graphs have been considered. For the hypercubes  $Q_n$ , it turns out to be a very interesting notion which includes many challenging problems.

In this paper we study the computational complexity of finding the forcing number of graphs, and we give some results on the possible values of forcing number for different matchings of the hypercube  $Q_n$ . Also we show an application to critical sets in back circulant Latin rectangles.

AMS SUBJECT CLASSIFICATION: 05C70

KEYWORDS: forcing number; matching in graphs; unique matchings; hypercubes.

## 1 Introduction and preliminaries

Let  $G$  be a graph that admits a perfect matching. A *forcing set* for a perfect matching  $M$  of  $G$  is a subset  $S$  of  $M$ , such that  $S$  is contained in no other perfect matching of  $G$ . The cardinality of a forcing set of  $M$  with the smallest size is called

---

<sup>1</sup>Research supported by Australian Research Council Grant A49937047.

*E-mail addresses:* pa@maths.uq.edu.au, mahdian@mit.edu, emahmood@sharif.ac.ir

the *forcing number* of  $M$ , and is denoted by  $f(G, M)$ . Also let  $f(G, \mathcal{M})$  denote the minimum of  $f(G, M)$  for  $M$  in a prescribed set  $\mathcal{M}$  of matchings of  $G$ .

This notion has arisen in the study of finding resonance structures of a given molecule in chemistry [9]. Later, Harary et al. [8] introduced the concept of *forcing number* of a perfect matching in graphs; see also [7]. Similar concepts have been studied under the name *defining set* for block designs (see [5] and [16]) for graph colorings (see [11]), and under the name *critical set* for Latin squares (see [3] and [1]). There is some study of forcing sets of hexagonal systems in the context of chemistry, but only few other classes of graphs have been considered ([13], [14], [10], [15]). For the hypercubes,  $Q_n$ , it turns out to be a very interesting notion which includes many challenging problems.

In this section we state some preliminaries, in Section 2 we discuss the computational complexity of finding the forcing number of matchings for graphs, and in Section 3 we give some results on the possible values of  $f(Q_n, M)$ ; for different matchings  $M$  of the hypercube  $Q_n$ . In particular, we give a matching  $N_5$  in  $Q_5$  for which  $f(Q_5, N_5) = 9$ , which is the first known example of a matching in any  $Q_n$  with forcing number greater than  $2^{n-2}$ . We then use this result in a construction which gives, for each  $n \geq 6$  and each  $r \in \{2^{n-2}, 2^{n-2} + 1, \dots, 2^{n-2} + 2^{n-5}\}$ , a matching in  $Q_n$  whose forcing number is  $r$ . Finally, in Section 4 we discuss an application to critical sets in Latin rectangles.

For a matching  $S$  in a graph  $G$  we denote by  $V(S)$  the set of all endpoints of the edges in  $S$ . As most of the graphs that we are dealing with here are bipartite, the following proposition shows a significant property of the forcing sets of matchings in such graphs. This proposition can also be found in [15].

**Proposition 1** *Let  $M$  be a matching in a bipartite graph  $G$  and  $S \subset M$  be a forcing set for  $M$ . Then there is a vertex in  $G$  that is forced immediately by  $S$ , that is, there is an edge  $uv$  of  $M \setminus S$  such that all of the neighbors of  $v$  except  $u$  are in  $V(S)$ .*

**Proof.** If this is not the case, after removing the set of all endpoints of the edges in  $S$  from  $G$ , we will obtain a bipartite graph in which every vertex has degree at least two. Therefore, by a generalization of the marriage theorem of Philip Hall (by M. Hall, see [6]), this graph has more than one matching. Thus  $S$  can be completed in more than one way, which is a contradiction. ■

Clearly, this proposition only goes one way: there may be a vertex in  $G$  that is forced immediately even if  $S$  is not a forcing set. Note that in the case of bipartite graphs, Proposition 1 makes finding completion (or non-completion) linear in the number of edges. This is similar to searches for strong critical sets in Latin squares (but not weak critical sets). Note also that if we remove the assumption that  $G$  is bipartite, then the proposition above is no longer true. For example, see the graph in Figure 1. It is easy to see that this graph has a unique perfect matching  $M$  that is marked by the dark edges in the figure, so the empty set is a forcing set for  $M$ . But it is clear that no vertex is forced immediately by this forcing set.

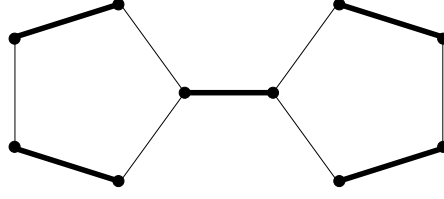


Figure 1: A non-bipartite graph in which no vertex is forced immediately

Let  $G$  be a graph and  $M$  be a matching in  $G$ . A cycle  $C$  which has alternate edges in  $M$  is called an  $M$ -alternating cycle. The following very useful proposition which is easy to prove is mentioned in [14].

**Proposition 2** *Let  $G$  be a graph and  $M$  be a perfect matching in  $G$ . A subset  $S$  of  $M$  is a forcing set for  $M$  if and only if it contains at least one edge from each  $M$ -alternating cycle.*

Actually, if  $M$  is a perfect matching in  $G$  and  $S$  is a minimal forcing set for  $M$ , then for each edge  $e \in S$  there exists an  $M$ -alternating cycle  $C$  such that  $C \cap S = \{e\}$ .

## 2 Algorithmic results

In this section we discuss the complexity of finding forcing numbers of matchings of a graph. For every bipartite graph  $G$  and perfect matching  $M$  of  $G$ , a digraph  $D(G, M)$  may be defined as follows [14].

**Definition.** Let  $G$  be a bipartite graph with bipartition  $X$  and  $Y$  and let  $M = \{x_1y_1, x_2y_2, \dots, x_ny_n\}$  be a perfect matching in  $G$  ( $x_i \in X$  and  $y_i \in Y$ , for  $i = 1, \dots, n$ ). The digraph  $D(G, M)$  is defined as follows: the vertex set of  $D(G, M)$  is  $M$ , and a vertex  $x_iy_i$  is joined to another vertex  $x_jy_j$  if and only if  $y_i$  is joined to  $x_j$  in  $G$ .

By the definition above and Proposition 2 we have the following.

**Proposition 3** *Let  $G$  be a bipartite graph,  $M$  a perfect matching in  $G$ , and  $S$  a subset of  $M$ . Then  $S$  is a forcing set for  $M$  if and only if  $D(G, M) \setminus S$  is an acyclic digraph.*

**Remark 1** Proposition 3 yields an efficient algorithm for recognizing forcing sets of matchings in bipartite graphs. It is not difficult to modify this method to obtain an algorithm for recognizing forcing sets of matchings in general graphs.

**Remark 2** By Proposition 3, finding the smallest forcing set for a given matching  $M$  in a graph  $G$  is equivalent to finding the smallest number of vertices of  $D(G, M)$

whose removal leaves no directed cycle in  $D(G, M)$ . This problem is known as the *feedback vertex set* problem, and is **NP**-complete for graphs with no in- or out-degree exceeding 2, see [4]. We use this idea to prove that the smallest forcing set problem is **NP**-complete. The problems are defined below.

- **FEEDBACK VERTEX SET**

INSTANCE:  $(D, k)$ , where  $D$  is a digraph and  $k$  is an integer.

QUESTION: Is there any subset  $S$  of at most  $k$  vertices of  $D$  such that  $D \setminus S$  does not contain any directed cycle?

- **SMALLEST FORCING SET**

INSTANCE: A graph  $G$ , a perfect matching  $M$  in  $G$ , and an integer  $k$ .

QUESTION: Is there any subset  $S$  of at most  $k$  edges in  $M$  such that  $S$  is a forcing set for  $M$ ?

**Theorem 1** *SMALLEST FORCING SET is **NP**-complete for bipartite graphs with maximum degree 3.*

**Proof.** It is clear from Remark 1 that the problem is in **NP**. We prove the **NP**-completeness by reducing **FEEDBACK VERTEX SET** to **SMALLEST FORCING SET**. Let  $D$  and  $k$  be an instance of **FEEDBACK VERTEX SET**. We construct a bipartite graph  $G$  as follows: corresponding to each vertex  $u$  of  $D$  we assign two vertices  $u_x$  and  $u_y$  in  $G$ , and if  $(u, v)$  is a directed edge in  $D$ , we join  $u_y$  and  $v_x$  in  $G$ . Also, for every vertex  $u \in V(D)$ , we join  $u_x$  and  $u_y$  in  $G$ . It is clear that the set  $M = \{(u_x, u_y) : u \in V(D)\}$  is a perfect matching in  $G$ . Also, it is not difficult to see that  $D = D(G, M)$ . Therefore, by Proposition 3,  $(D, k)$  is a yes-instance of **FEEDBACK VERTEX SET** if and only if there is a forcing set of size at most  $k$  for  $M$  in  $G$ . Also notice that if no in- or out-degree in  $D$  exceeds 2, then the maximum degree of the vertices of  $G$  is at most 3. Therefore, the **NP**-completeness of **FEEDBACK VERTEX SET** for graphs with no in- or out-degree more than 2 implies that **SMALLEST FORCING SET** is **NP**-complete for bipartite graphs of maximum degree 3. ■

Determining the computational complexity of the following remains open:

- **SMALLEST FORCING NUMBER OF GRAPH**

INSTANCE: A graph  $G$  and an integer  $k$ .

QUESTION: Is there any matching in  $G$  with the forcing number of at most  $k$ ?

### 3 Spectrum of forcing numbers for hypercubes

In a given graph  $G$ , different matchings may have different forcing numbers. The study of these possible numbers is of interest.

**Definition.** The *spectrum* of the forcing numbers for a graph  $G$  is defined as  $\text{Spec}(G) = \{k \mid \text{there exists a perfect matching } M \text{ of } G \text{ such that } f(G, M) = k\}$ .

In this section we discuss the spectrum of forcing numbers of matchings in hypercubes  $Q_n$ . In [13] it is conjectured that for each  $n$ , and for every matching  $M$ ,  $f(Q_n, M) \geq \frac{2^n}{4}$ . This conjecture is proved to be true for each even number  $n$  by M.E. Riddle [15]. Here we denote the vertices of a hypercube  $Q_n$  by the set  $\{0, 1, 2, \dots, 2^n - 1\}$ , where each vertex is viewed as a  $(0, 1)$  sequence of length  $n$  consisting of its binary representation. Two vertices are adjacent if and only if their sequence representations differ in exactly one component. For a given value  $k$ ,  $1 \leq k \leq n$ , a set of edges of the form  $\{a_n, b_n\}$ , where  $a_n$  is any sequence having 0 in the  $k$ -th component and  $b_n$  is obtained from  $a_n$  by changing the  $k$ -th component to 1, is called a set of *parallel edges*, and the edges are said to be in the *same direction*.

**Proposition 4** *Let  $M$  be a perfect matching of the hypercube  $Q_n$  consisting of edges all in the same direction. Then  $f(Q_n, M) = \frac{2^n}{4}$ .*

**Proof.** Without loss of generality, define  $P_n$  to be the set of edges of the form  $\{0a_{n-1}, 1a_{n-1}\}$ , where  $a_{n-1}$  is any binary sequence of length  $n - 1$ . Then  $P_n^*$ , the set of edges of the form  $\{0b_{n-1}, 1b_{n-1}\}$ , where  $b_{n-1}$  is any binary sequence with an *even* number of 1's, is a forcing set for  $P_n$ . Since  $P_n$  can be decomposed into a set of  $\frac{2^n}{4}$  disjoint  $P_n$ -alternating cycles, by Proposition 2,  $P_n^*$  is a smallest forcing set for  $P_n$ . ■

**Remark 3** As in the proof of Proposition 4,  $\overline{P_n^*}$ , the set of edges of the form  $\{0c_{n-1}, 1c_{n-1}\}$ , where  $c_{n-1}$  is any binary sequence with an *odd* number of 1's, is also a smallest forcing set for  $P_n$ .

The hypercube  $Q_n$  consists of two copies of  $Q_{n-1}$ , with a set  $\mathcal{P}$  of parallel edges in between. We use the notation  $Q_{n-1} \oplus Q_{n-1}$  to show this, and by  $M_1 \oplus M_2$  we mean a matching in  $Q_n$  which consists of the edges of a matching  $M_1$  in the first copy of  $Q_{n-1}$  and the edges of a matching  $M_2$  in the second copy of  $Q_{n-1}$ .

**Lemma 1** *If there exists a perfect matching  $M_n$  of  $Q_n$  with forcing number  $d$ , then we can construct a perfect matching in  $Q_{n+1}$  with forcing number at least  $2d$ .*

**Proof.** Consider  $Q_{n+1}$  as two copies of  $Q_n$ , with a set  $\mathcal{P}$  of parallel edges in between. Let  $M_{n+1}$  be the perfect matching formed as  $M_n \oplus M_n$ . Assume that  $S$  is a minimum forcing set for  $M_{n+1}$ . Then  $S = S_1 \oplus S_2$ , where  $S_1$  is the set of edges of  $S$  in the first copy of  $Q_n$ , and  $S_2$  is the set of edges in the second copy. Note that since any forcing set is a subset of matching  $M_{n+1}$ , and  $M_{n+1}$  does not contain any edge from  $\mathcal{P}$ , thus  $S$  does not contain any of those edges either.

Now, if  $|S_1| < d$ , then by Proposition 2, there is an alternating cycle in the first copy of  $Q_n$  that does not contain any of the edges of  $S_1$ , and therefore the alternating cycle does not contain any of the edges of  $S$ . Thus, we can switch the edges of that alternating cycle to obtain another matching which contains  $S$ . This

is in contradiction with the assumption that  $S$  is a forcing set. Thus  $|S_1| \geq d$ . Similarly, we must have  $|S_2| \geq d$ . Therefore,  $|S| \geq 2d$ . ■

The argument used in the last lemma may be used to give a more general result:

**Lemma 2** *Let  $G$  be a graph and  $V_1 \cup V_2 \cup \dots \cup V_k$  be a partition of its vertex set. Suppose that  $M_1, M_2, \dots, M_k$  are perfect matchings in the induced subgraphs  $G[V_1], G[V_2], \dots, G[V_k]$ , respectively. Then  $f(G, M_1 \cup M_2 \cup \dots \cup M_k) \geq f(G[V_1], M_1) + f(G[V_2], M_2) + \dots + f(G[V_k], M_k)$ .*

In [13] it is shown that for sufficiently large  $n$ , there exists a perfect matching  $M$  of  $Q_n$  with  $f(Q_n, M) > \frac{2^n}{4}$ . The proof is by existence and not by construction. Our computer searches show that for each  $n \leq 4$  we have  $f(Q_n, M) = \frac{2^n}{4}$ , for every perfect matching  $M$  of  $Q_n$ . However, we have  $\text{Spec}(Q_5) = \{8, 9\}$ . The following example gives a matching of  $Q_5$  with forcing number 9. This represents the first known perfect matching of  $Q_n$  with forcing number greater than  $\frac{2^n}{4}$ .

**Example 1** *In  $Q_5$ , the set of edges*

$$N_5^* = \{\{0, 1\}, \{2, 10\}, \{5, 13\}, \{9, 11\}, \{20, 22\}, \{16, 17\}, \{19, 23\}, \{24, 28\}, \{30, 31\}\}$$

*is a smallest forcing set for the matching*

$$N_5 = N_5^* \cup \{\{3, 7\}, \{4, 6\}, \{18, 26\}, \{21, 29\}, \{8, 12\}, \{14, 15\}, \{25, 27\}\}.$$

*This is shown in Figure 2, with the edges of  $N_5^*$  highlighted. To make the picture*

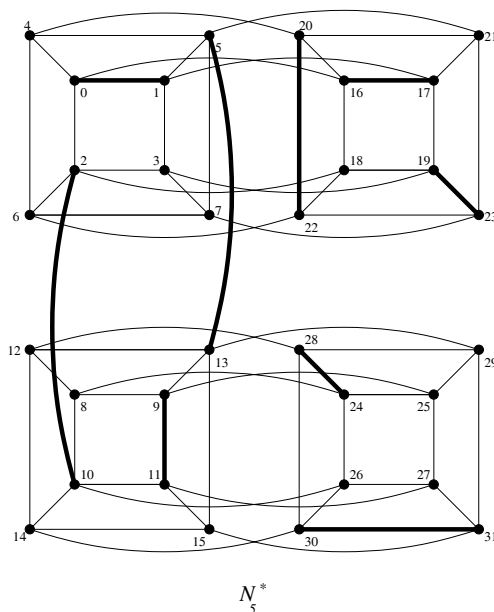


Figure 2: A smallest forcing set of size 9 for  $Q_5$

*clearer we have omitted parallel edges between the two copies of  $Q_4$ .*

The forcing set  $N_5^*$  in Example 1 may be generalized. First we note that the set  $\overline{N}_5^* = \{\{0, 1\}, \{3, 7\}, \{4, 6\}, \{16, 17\}, \{18, 26\}, \{21, 29\}, \{8, 12\}, \{14, 15\}, \{25, 27\}\}$  is also a smallest forcing set for the same matching  $N_5$ . The edges of  $N_5$  can be put into eight disjoint alternating cycles of length 4. The edges of each of these cycles are partitioned by the elements of  $\mathcal{D}_5 = \{P_5^*, \overline{P}_5^*, N_5^*, \overline{N}_5^*\}$ , with one exception, which has two edges in both  $N_5^*$  and  $\overline{N}_5^*$ . This property of  $\mathcal{D}_5$  is very useful in our general construction. To make the general construction clear we state the following lemma.

**Lemma 3** *We have  $\{16, 17, 18\} \subseteq \text{Spec}(Q_6)$ .*

**Proof.** Consider  $Q_6$  as  $Q_5 \oplus Q_5$ . We call these two copies of  $Q_5$  the *first* and *second* pieces of  $Q_6$ . To obtain perfect matchings in  $Q_6$  with smallest forcing sets of sizes 16, 17, and 18, we consider the following perfect matchings, respectively:  $M_1 = P_5 \oplus P_5$ ;  $M_2 = P_5 \oplus N_5$ ; and  $M_3 = N_5 \oplus N_5$ . To see this, first by Lemma 1 we know that in each case the forcing set is *at least* of the indicated size, respectively. Next, consider the following forcing sets, respectively:  $S_1 = P_5^* \oplus \overline{P}_5^*$ ,  $S_2 = P_5^* \oplus \overline{N}_5^*$ , and  $S_3 = N_5^* \oplus \overline{N}_5^*$ ; see Figures 3, 4, and 5. To make the pictures clearer, in each case we have omitted parallel edges between the copies of  $Q_4$  which correspond to each  $Q_5$ , and between the copies of each  $Q_5$  which correspond to  $Q_6$ .

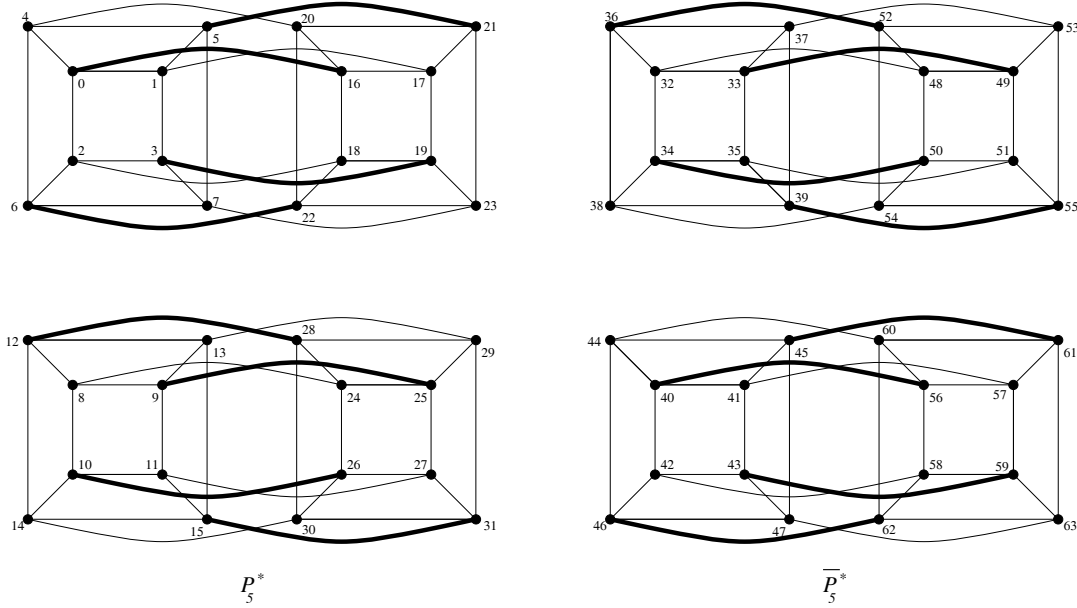


Figure 3:  $S_1 = P_5^* \oplus \overline{P}_5^*$

We note that each of the given sets is indeed a forcing set for the corresponding perfect matching. For example, consider  $S_2$ : each edge  $uv$  in the first piece which belongs to  $P_5 \setminus P_5^*$  has at least one vertex, say  $u$ , which is *forced*, because all of its neighbors, except  $v$ , are saturated by  $S_2$ . The same argument holds for the second piece. It is even easier to see this for  $S_1$  and  $S_3$ . ■

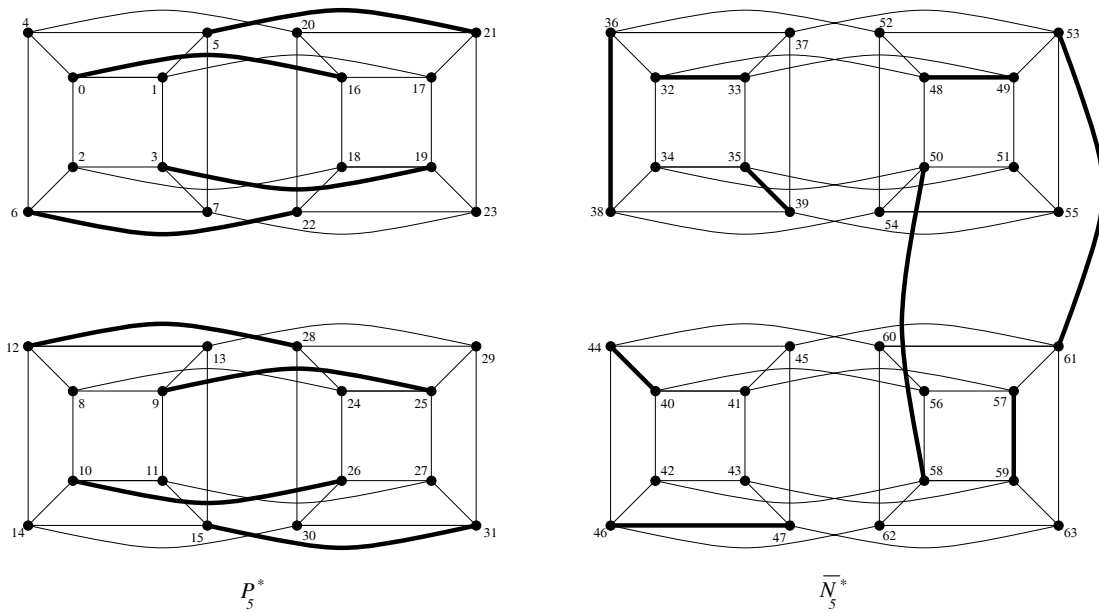


Figure 4:  $S_2 = P_5^* \oplus \overline{N}_5^*$

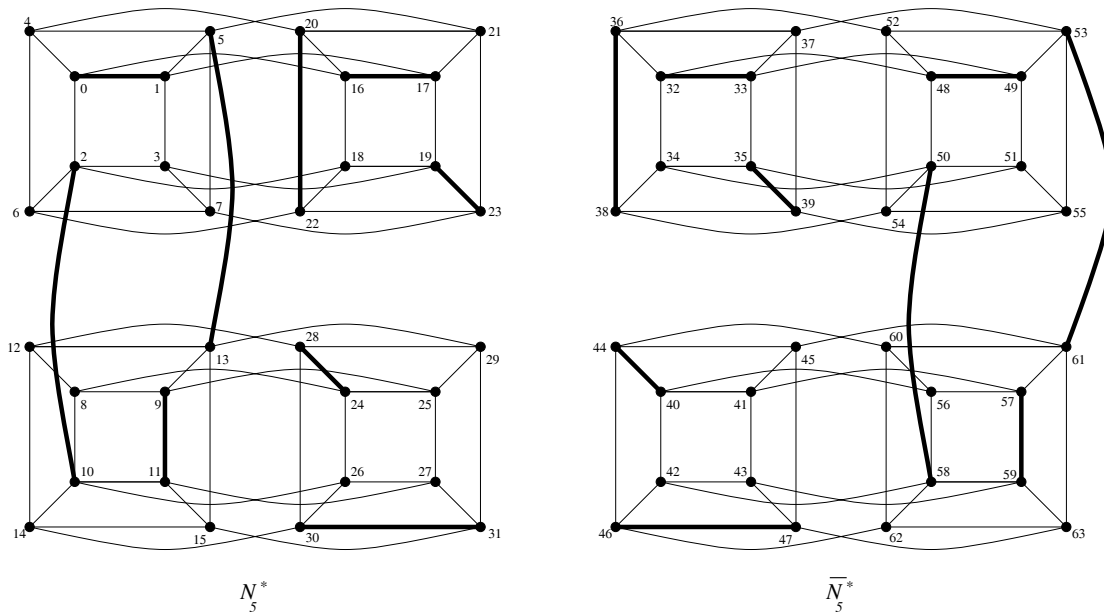


Figure 5:  $S_3 = N_5^* \oplus \overline{N}_5^*$

Note that using the same proof as in Lemma 3, the set  $S'_2 = \overline{P}_5^* \oplus N_5^*$  is another forcing set of size 17 for  $M_2$ .

By considering the  $(0, 1)$  sequence of each vertex of  $Q_{m+n}$ , it can easily be seen that  $Q_{m+n} = Q_m \times Q_n$ . In the following theorem, we consider  $Q_n$  as  $Q_5 \times Q_{n-5}$ . In other words,  $Q_n$  consists of  $2^{n-5}$  copies of  $Q_5$ , say  $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{2^{n-5}}$ , and every vertex in  $\mathcal{C}_i$  is connected to its corresponding vertex in  $\mathcal{C}_j$  if and only if  $i$  and  $j$  are connected in  $Q_{n-5}$ . We call each  $\mathcal{C}_i$  a *piece* of  $Q_n$ .

**Theorem 2** *Let  $n \geq 5$ , and consider  $Q_n$  as  $Q_5 \times Q_{n-5}$ . Let  $M$  be the matching obtained by considering the matching  $N_5$  in  $r$  pieces of  $Q_n$ , and  $P_5$  in the remaining pieces. Then  $f(Q_n, M) = 2^{n-2} + r$ .*

**Proof.** By Lemma 2, the forcing number of  $M$  is at least  $2^{n-2} + r$ . Next we construct a forcing set of size  $2^{n-2} + r$ . As  $Q_{n-5}$  is a bipartite graph, let  $A$  and  $B$  be its two parts. For any vertex of  $Q_{n-5}$  to which an  $N_5$  is assigned, consider  $N_5^*$ , if it is in part  $A$ , and  $\overline{N}_5^*$  if it is in part  $B$ . Similarly for any vertex of  $Q_{n-5}$  to which a  $P_5$  is assigned, consider  $P_5^*$  if it is in part  $A$  and  $\overline{P}_5^*$  if it is in part  $B$ . Let  $S$  be the union of these sets of edges. We claim that  $S$  is a forcing set for  $M$ . To see this, consider a vertex  $v$  in  $Q_{n-5}$ . Suppose that  $M_v$  is the matching in  $M$  for the copy of  $Q_5$  which corresponds to  $v$ . Further, suppose that the corresponding assigned forcing set for  $M_v$  in  $S$  is  $S_v$ . If  $S_v$  is  $P_5^*$ , each of its neighbors either has  $\overline{P}_5^*$  or  $\overline{N}_5^*$  as the corresponding assigned forcing set. Therefore, for every edge in  $M_v \setminus S_v$ , at least one of its endpoints forced, because all of its other neighbors are saturated by  $S$  (compare with the forcing sets in Lemma 3). Therefore, all of the edges of  $M_v \setminus S_v$  are forced. Similarly, for all other vertices in  $Q_{n-5}$  all of the edges are forced. Thus,  $S$  is a forcing set of size  $2^{n-2} + r$  for  $M$ . ■

By using the forcing sets of size 8 and 9 of  $Q_5$  and Theorem 2, we obtain,

**Corollary 1** *For every  $n \geq 5$ ,  $\{2^{n-2}, 2^{n-2} + 1, \dots, 2^{n-2} + 2^{n-5}\} \subseteq \text{Spec}(Q_n)$ .*

**Remark 4** We had hoped to computationally find a perfect matching in  $Q_6$  with forcing number greater than 18. The approach we used was: find each non-isomorphic perfect matching in  $Q_6$  (in a canonical ordering), and search for the smallest forcing set in that matching. This was a very large computational task, which we were able to improve significantly by using a probabilistic search for a forcing set of size 18, and not checking smaller sizes. Most matchings in  $Q_6$  have forcing number smaller than 18, so it was usually very easy to find a forcing set of size 18.

There were over 350,000,000 non-isomorphic perfect matchings in  $Q_6$ . Even with the improvements to efficiency noted above, an exhaustive search ran for about 4 months on a cluster of 30 computers. We showed that no matching in  $Q_6$  has forcing number greater than 18.

In [13] there is a probabilistic proof that if  $n$  is large, then there is a matching  $M$  in  $Q_n$  such that the size of the smallest forcing set for  $M$  is more than  $2^n/4$ . Using

the same method, it is possible to prove a more general result for bipartite graphs. Let  $F(G, \mathcal{M})$  denote the maximum of  $f(G, M)$  over the set of all perfect matchings  $M$  in  $G$ .

**Theorem 3** *For any  $k$ -regular bipartite graph  $G$  with  $N$  vertices in each part, we have*

$$F(G, \mathcal{M}) \geq \left(1 - \frac{\log(2e)}{\log k}\right) N,$$

where  $e$  is the base of the natural logarithm.

**Proof.** We estimate the number of perfect matchings of  $G$  in two ways. Since we know that the number of perfect matchings is equal to the permanent of  $A$ , where  $a_{ij}$  is the number of edges between vertex  $i$  in one part and vertex  $j$  in the other part, then van der Warden's theorem can be used to prove that the number of perfect matchings of  $G$  is at least

$$\left(\frac{k}{N}\right)^N N! \geq \left(\frac{k}{N}\right)^N \left(\frac{N}{e}\right)^N = \left(\frac{k}{e}\right)^N. \quad (1)$$

On the other hand, for every perfect matching of  $G$ , there is a forcing set of size  $F(G, \mathcal{M})$ . Therefore, the number of perfect matchings of  $G$  cannot exceed the number of matchings of size  $F(G, \mathcal{M})$  in  $G$ . Now, we count the number of matchings of size  $F(G, \mathcal{M})$  in  $G$ . Any matching of size  $F(G, \mathcal{M})$  in  $G$  can be constructed by the following process: we choose  $F(G, \mathcal{M})$  different vertices from the first part of  $G$  (there are  $\binom{N}{F(G, \mathcal{M})} \leq 2^N$  different ways to do this), and then for any of the selected vertices, we choose one of its neighbors (since the graph is  $k$ -regular, there are at most  $k^{F(G, \mathcal{M})}$  ways to select them). Therefore, the total number of matchings of size  $F(G, \mathcal{M})$  in  $G$  is at most

$$2^N k^{F(G, \mathcal{M})}. \quad (2)$$

Thus, Equations (1) and (2) imply

$$\left(\frac{k}{e}\right)^N \leq 2^N k^{F(G, \mathcal{M})}.$$

Taking the logarithm of both sides, we get

$$N \log\left(\frac{k}{e}\right) \leq N \log 2 + F(G, \mathcal{M}) \log k,$$

which completes the proof of the theorem. ■

The following corollary is immediate.

**Corollary 2** ([15]) *For any  $\alpha < 1$ , if  $n$  is sufficiently large, then there is a matching  $M$  of  $Q_n$  with forced matching number at least  $\alpha 2^{n-1}$ .*

This result means that if  $n$  is large enough, there are matchings in  $Q_n$  such that any forcing set for them needs to contain almost all the edges of the matching! This last statement holds for any  $k$ -regular bipartite graph as long as  $k$  and  $n$  are large enough. This happens with many of the graphs  $G(L, r)$  which are introduced in next section.

## 4 Some applications

The concept of forcing sets for perfect matchings may be applied to the construction of certain cryptographic schemes, as is done for the critical sets of Latin squares (see for example [2]). For example, as we noted above, there are over 350,000,000 non-isomorphic perfect matchings in  $Q_6$ , while certain perfect matchings can be specified with as few as 16 edges.

Another application arises in the discussion of critical sets in Latin rectangles. A *critical set* in an  $m \times n$  array is a set  $S$  of given entries, chosen from the set  $\{1, 2, \dots, n\}$ , such that there exists a unique extension of  $S$  to a Latin rectangle of size  $m \times n$  and no proper subset of  $S$  has this property.

Let  $L$  be an  $m \times n$  Latin rectangle ( $m < n$ ), with entries drawn from  $\{1, 2, \dots, n\}$ . For each  $r = 1, \dots, m$ , we construct a bipartite graph  $G(L, r)$  corresponding to the  $r$ -th row of  $L$  as follows: each part of  $G(L, r)$  consists of  $n$  vertices. The first part corresponds to the columns of  $L$ , and the second part corresponds to the entries  $1, \dots, n$ . We connect the vertex  $i$  in the first part to the vertex  $j$  in the second part if  $j$  does not occur in the  $i$ -th column of  $L$ , except possibly in the cell  $(r, i)$ . In other words, we connect  $i$  to  $j$  if, given all of the entries of the Latin rectangle except the entries in the  $r$ -th row, one could write  $j$  in the cell  $(r, i)$ .

Now, assume that all of the entries of  $L$  are given, except the entries in the  $r$ -th row. We can fill the  $r$ -th row in several ways, each way corresponds to a matching in the graph  $G(L, r)$ . Therefore, if the forcing number of  $G(L, r)$  is  $k$ , then at least  $k$  entries of the  $r$ -th row of  $L$  must be present in any critical set of  $L$ .

With this relation it may be possible to improve results on critical sets in back circulant Latin rectangles. For example, in [12] it is shown that the size of the smallest critical set in a back circulant Latin rectangle of size  $m \times n$ , with  $4m \leq 3n$ , is equal to  $m(n - m) + \lfloor (m - 1)^2/4 \rfloor$ ; see also [11]. Applying the forced matching approach may improve the condition  $4m \leq 3n$ , which is the subject of further research. In fact, some computational searches show that the above bound also holds for  $(m, n) = (5, 6), (8, 10), (11, 14), (14, 18),$  and  $(17, 22)$ .

## Acknowledgements

The third author (ESM) appreciates the hospitality of the Department of Mathematics at the University of Queensland, while working on this paper.

## References

- [1] 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.
- [2] J. COOPER, D. DONOVAN AND J. SEBERRY, *Secret sharing schemes arising from Latin squares*, *Bull. Inst. Combin. Appl.* **12** (1994), 33–43.
- [3] D. CURRAN AND G.H.J. VAN REES, *Critical sets in Latin squares*, *Proceedings of the Eighth Manitoba Conference on Numerical Mathematics and Computing* (Univ. Manitoba, Winnipeg, Man., 1978), 165–168, *Congress. Numer.*, XXII, Utilitas Math. Publ., Winnipeg, Man., 1979.
- [4] M.R. GAREY AND D.S. JOHNSON, *Computers and intractability. A guide to the theory of NP-completeness*, *A Series of Books in the Mathematical Sciences*, W.H. Freeman and Co., San Francisco, Calif., 1979.
- [5] K. GRAY, *On the minimum number of blocks defining a design*, *Bull. Austral. Math. Soc.* **41** (1990), 97–112.
- [6] M. HALL, JR., *Combinatorial theory*, Second edition, John Wiley & Sons, Inc., New York, 1986.
- [7] F. HARARY, *Three new directions in graph theory*, *Proceedings of the First Estonian Conference on Graphs and Applications* (Tartu-Kääriku, 1991), 15–19, Tartu Univ., Tartu, 1993.
- [8] F. HARARY, D.J. KLEIN AND T.P. ZIVKOVIĆ, *Graphical properties of polyhexes: perfect matching vector and forcing*, *J. Math. Chem.* **6** (1991), 295–306.
- [9] D.J. KLEIN AND M. RANDIĆ, *Innate degree of freedom of a graph*, *J. Comput. Chem.* **8** (1987) 516–521.
- [10] F. LAM AND L. PACTER, *Forcing numbers for stop signs*, Preprint.
- [11] E.S. MAHMOODIAN, R. NASERASR AND M. ZAKER, *Defining sets in vertex colorings of graphs and Latin rectangles*, *Discrete Math.* **167/168** (1997), 451–460.
- [12] E.S. MAHMOODIAN AND G.H.J. VAN REES, *Critical sets in back circulant Latin rectangles*, *Australas. J. Combin.* **16** (1997), 45–50.
- [13] L. PACTER, *Domino tiling, gene recognition, and mice*, Ph.D. thesis, 1999, MIT.
- [14] L. PACTER AND P. KIM, *Forcing matchings on square grids*, *Discrete Mathematics* **190** (1998), 287–294.

- [15] M.E. RIDDLE, *The minimum forcing number for the torus and hypercubes*, Preprint.
- [16] A.P. STREET, *Defining sets for block designs: an update*, in *Combinatorics Advances*, C.J. Colbourn and E.S. Mahmoodian, eds., *Mathematics and Its Applications*, Kluwer Academic Publishers, Dordrecht, Boston, London, 1995, 307–320.