

# Zero forcing number of graphs

Thomas Kalinowski \*

Nina Kamčev †

Benny Sudakov ‡

## Abstract

A subset  $S$  of initially infected vertices of a graph  $G$  is called *forcing* if we can infect the entire graph by iteratively applying the following process. At each step, any infected vertex which has a unique uninfected neighbour, infects this neighbour. The *forcing number* of  $G$  is the minimum cardinality of a forcing set in  $G$ . In the present paper, we study the forcing number of various classes of graphs, including graphs of large girth,  $H$ -free graphs for a fixed bipartite graph  $H$ , random and pseudorandom graphs.

## 1 Introduction

Let  $G$  be a simple, undirected graph on the vertex set  $V$ . The *zero forcing process* on  $G$  is defined as follows. Initially, there is a subset  $S$  of black vertices, while all other vertices are said to be white. At each time step, a black vertex with exactly one white neighbour will *force* its white neighbour to become black. The set  $S$  is said to be a *zero forcing set* if, by iteratively applying the forcing step, all of  $V$  becomes black. The *zero forcing number* of  $G$  is the minimum cardinality of a zero forcing set in  $G$ , denoted by  $Z(G)$ . Note that given an initial set of black vertices, the set of black vertices obtained by applying the colour-change rule until no more changes are possible is unique. We will often use the adjective ‘forcing’ instead of ‘zero forcing’.

The forcing process is an instance of a propagation process on graphs (in particular, it is a cellular automaton). Such processes are a common topic across mathematics and computer science (see, e.g., [14], [8], [29], [18]). In other fields (statistical mechanics [13], physics [7], social network analysis [24]), diverse graph processes are used to model technical or societal processes. For an overview of the different models and applications, refer to the book [9].

The zero forcing process was introduced in [10] and used in [11] as a criterion for quantum controllability of a system. Independently, [1] have introduced it to bound the minimum rank, or equivalently, the maximum nullity of a graph  $G$ . Given an  $n$ -vertex graph  $G$ , let  $M(G)$  denote the maximum nullity over all symmetric real-valued matrices  $A$  whose zero-nonzero pattern of the off-diagonal entries is described by the graph  $G$ . This means that for  $i \neq j$ , the entry  $A_{ij}$  is non-zero if and only if  $ij$  is an edge in  $G$ , whereas the diagonal entries are chosen freely. The minimum rank of  $G$  is  $n - M(G)$ . This parameter has been extensively studied in the last fifteen years, largely due to its connection to inverse eigenvalue problems for graphs, singular graphs, biclique partitions and other problems. Among several tools introduced to study the minimum rank, the zero forcing number has the advantage that its definition is purely combinatorial. In [1], it was shown that  $Z(G) \geq M(G)$  for all graphs  $G$ . To see this, suppose that  $A$  is a matrix whose zero pattern is described by  $G$ , and  $S$  is a zero forcing set of cardinality  $|S|$  smaller than the nullity of  $A$ . This guarantees that we can construct a vector  $x \neq 0$  such that  $Ax = 0$  and  $x|_S = 0$ . But then by iteratively applying the forcing step to the components of  $x$ , we can show  $x = 0$ , which is a contradiction. The minimum rank and forcing number of some specific families of graphs have also been computed in [1]. As a simple example, a complete graph  $K_n$  on  $n$  vertices has  $Z(K_n) = M(K_n) = n - 1$ , whereas the  $n$ -vertex path  $P_n$  has  $Z(P_n) = M(P_n) = 1$ . More results on this topic can be found in [2] and [17].

---

\*School of Mathematical and Physical Sciences, University of Newcastle, Callaghan, NSW 2308, Australia.  
Email: thomas.kalinowski@newcastle.edu.au.

†Department of Mathematics, ETH, 8092 Zurich. Email: nina.kamcev@math.ethz.ch.

‡Department of Mathematics, ETH, 8092 Zurich. Email: benjamin.sudakov@math.ethz.ch.

Recently, there has been a lot of interest in studying the forcing number of graphs for its own sake, and its relation to other graph parameters, such as the path cover number [21], connected domination number [6], and the chromatic number [32]. Among others, [12] and [22] contain upper bounds on the zero forcing number of a graph in terms of its degrees. It is easy to see that the trivial lower bound on the zero forcing number of a graph is  $Z(G) \geq \delta - 1$ . Improving this trivial upper bound, and confirming the earlier conjecture of Davila and Kenter, [16], the authors of [15] showed that

$$Z(G) \geq \delta + (\delta - 2)(g - 3),$$

for a graph  $G$  with minimum degree  $\delta \geq 2$  and girth  $g \geq 3$  (the *girth* is the length of the shortest cycle in a graph). Our first result substantially improves on this bound, with the exception of very small values of  $\delta$ .

**Theorem 1.1.** *Let  $G$  be a graph of girth  $g$  with minimum degree  $\delta$ .*

- (i) *If  $g = 2k + 1$  for  $k \in \mathbb{N}$ , then  $Z(G) \geq e^{-1} \left( \frac{\delta^k}{k+1} - \delta^{k-1} \right)$ .*
- (ii) *If  $g = 2k + 2$  for  $k \in \mathbb{N}$ , then  $Z(G) \geq 2e^{-1} \left( \frac{\delta^k}{k+1} - \delta^{k-1} \right)$ .*

The crucial ingredient of the proof is an upper bound on the density of a graph which contains no cycles  $C_3, C_4, \dots, C_{g-1}$ . This is an instance of the so-called Turán problem (see, e.g., [20]). Given a graph  $H$ , we define the Turán number  $\text{ex}(n, H)$  to be the maximum number of edges  $e(G)$  over all the  $n$ -vertex graphs  $G$  not containing a subgraph isomorphic to  $H$ . In general, if a graph  $G$  does not contain  $H$  as a subgraph, we refer to it as  $H$ -free. The Turán numbers of graphs have been extensively studied, and the asymptotic value of  $\text{ex}(n, H)$  is known for all non-bipartite graphs  $H$ . Denote the complete bipartite graph with vertex classes of order  $a$  and  $b$  by  $K_{a,b}$ . A celebrated theorem of Kövari, Sós and Turán [30] says that for  $a \leq b$ ,  $\text{ex}(n, K_{a,b}) = O\left(n^{2-\frac{1}{a}}\right)$ . This implies that for every bipartite graph  $H$ , there exists  $c_H < 1$  such that  $\text{ex}(n, H) = O\left(n^{1+c_H}\right)$ . Using our approach based on the Turán numbers, we can extend Theorem 1.1 to  $H$ -free graphs  $G$ , substantially improving the trivial bound  $Z(G) \geq \delta - 1$ .

**Theorem 1.2.** *Suppose that for a graph  $H$  and all  $n \geq n_0(H)$ ,  $\text{ex}(n, H) \leq \beta_H n^{1+c_H}$ . Let  $G$  be an  $H$ -free graph of minimum degree  $\delta \geq 2n_0$ . Then*

$$Z(G) \geq 2^{-1-\frac{2}{c_H}} \left( \frac{\delta}{\beta_H} \right)^{\frac{1}{c_H}}.$$

The authors of [1] report that somewhat surprisingly,  $M(G) = Z(G)$  for many graphs for which  $M(G)$  was known. Our next theorem shows that for most graphs,  $M(G)$  and  $Z(G)$  are actually far apart. We consider the random graph model  $G_{n,p}$ . This is an  $n$ -vertex graph in which every pair of vertices is adjacent randomly and independently with probability  $p$ . With an abuse of notation, we write  $G_{n,p}$  for the sampled graph, as well as the underlying probability space. The model  $G_{n,\frac{1}{2}}$  is particularly interesting since it assigns the same probability to all the  $2^{\binom{n}{2}}$  graphs, thus allowing us to make statements about a typical graph. We say that an event in  $G_{n,p}$  holds *with high probability* if its probability tends to 1 as  $n$  tends to infinity. The standard  $O$ -notation is used for the asymptotic behaviour of the relative order of magnitude of two sequences, depending on a parameter  $n \rightarrow \infty$ . Hall et al. [25] have shown that with high probability, the maximum nullity of a random graph  $G_{n,\frac{1}{2}}$  lies between  $0.49n$  and  $0.86n$ . On the other hand, we will show that the zero forcing number of a typical graph is almost as high as  $n$ .

**Theorem 1.3.** *Let  $p = p(n)$  satisfy  $\frac{\log^2 n}{\sqrt{n}} \leq p \leq \frac{2}{3}$ , then with high probability*

$$Z(G_{n,p}) = n - \left(2 + \sqrt{2} + o(1)\right) \cdot \frac{\log(np)}{-\log(1-p)}.$$

In particular, for  $p = \frac{1}{2}$  we have  $Z(G_{n,\frac{1}{2}}) = n - \left(2 + \sqrt{2} + o(1)\right) \log_2 n$ , whereas for  $p = o(1)$  the formula simplifies to  $Z(G_{n,p}) = n - \left(2 + \sqrt{2} + o(1)\right) p^{-1} \log(np)$ .

There is a natural trend in probabilistic combinatorics to explore the possible extensions of results about random graphs to the pseudorandom setting. A graph is pseudorandom if its edge distribution resembles the one of  $G_{n,p}$ . There are several formal approaches to pseudorandomness. Here, we will use the one based on the spectral properties of the graph. The *adjacency matrix* of a graph  $G = (V, E)$  with vertex set  $V = [n]$  is an  $n \times n$  matrix whose entry  $a_{ij}$  is 1 if  $\{i, j\} \in E$ , and 0 otherwise. The *eigenvalues of a graph*  $G$  are the eigenvalues of its adjacency matrix. An  $(n, d, \lambda)$  graph is a  $d$ -regular  $n$ -vertex graph in which all eigenvalues but the largest one are at most  $\lambda$  in absolute value. If  $G$  is an  $(n, d, \lambda)$  graph, its largest eigenvalue is  $\lambda_1 = d$ , and the difference  $d - \lambda$  is called the *spectral gap*. It is well known (see, e.g., [31]) that the larger this gap is, the more closely the edge distribution of a regular graph  $G$  approaches that of the random graph with the corresponding edge density. We prove a theorem which provides spectral bounds on the zero forcing number of a graph. The lower bound is given in terms of the smallest eigenvalue of  $G$ , akin to the celebrated result of Hoffman on the independence number [26], whereas the previously defined  $\lambda$  is used for the upper bound.

**Theorem 1.4.** *Let  $G$  be an  $(n, d, \lambda)$ -graph with smallest eigenvalue  $\lambda_{\min}$ . Then*

- (i)  $Z(G) \geq n \left( 1 + \frac{2\lambda_{\min}}{d - \lambda_{\min}} \right).$
- (ii)  $Z(G) \leq n \left( 1 - \frac{1}{2(d - \lambda)} \log \left( \frac{d - \lambda}{2\lambda + 1} \right) \right).$

The first bound on  $n - Z(G)$  is tight, whereas (ii) is tight up to a multiplicative constant.

The rest of this paper is organised as follows. The second section contains results on  $H$ -free graphs with a forbidden bipartite graph  $H$ . In the third section, we asymptotically determine the zero forcing number of  $G_{n,p}$ . Section 4 contains bounds based on the spectral properties of a graph.

## 2 Graphs with forbidden subgraphs

In this section, we bound the forcing number of graphs with a forbidden bipartite subgraph. First we consider graphs with large girth  $g$  and minimum degree  $\delta$ , showing that

- (i)  $Z(G) \geq e^{-1} \left( \frac{\delta^k}{k+1} - \delta^{k-1} \right)$  for  $g = 2k + 1, k \in \mathbb{N}$ , and
- (ii)  $Z(G) \geq 2e^{-1} \left( \frac{\delta^k}{k+1} - \delta^{k-1} \right)$  for  $g = 2k + 2, k \in \mathbb{N}$ .

*Proof of Theorem 1.1.* We will use the result of Alon, Hoory and Linial [3], which says that a graph  $G_1$  of girth  $g$  and average degree  $d$  has to satisfy

$$|V(G_1)| \geq \begin{cases} (d-1)^k, & g = 2k + 1 \\ 2(d-1)^k, & g = 2k + 2. \end{cases} \quad (1)$$

Let  $G$  be an  $n$ -vertex graph with girth  $g = 2k + 1$  and minimum degree  $\delta$ . The proof for the case of even girth is the same. Let  $S$  be a zero forcing set in  $G$  of order  $s$ . Assume that  $s \leq \frac{n}{(k+1)}$ , otherwise we can apply (1) to the entire graph  $G$  and obtain

$$s > \frac{n}{k+1} \geq \frac{(\delta-1)^k}{k+1} > e^{-1} \frac{\delta^k}{k+1},$$

so we are done. Starting from  $S$ , we run the zero forcing process until we have reached a set of black vertices  $T$  with  $|T| = (k+1)s$ . Let  $U$  be the set of vertices which forced some vertex of  $T \setminus S$  during our process. Then, since each vertex can force only one of its neighbours,  $|U| \geq ks$ . Moreover, all the edges with an endpoint in  $U$  lie inside  $T$ . Denoting the number of edges with both endpoints in  $T$  by  $e(T)$ , we have

$$e(T) \geq \frac{|U|}{2} \cdot \delta \geq \frac{k|S|}{2} \cdot \delta.$$

The graph  $G[T]$  has average degree at least  $\frac{k\delta}{k+1}$ . Applying (1) to the graph  $G[T]$  gives

$$(k+1)s \geq \left( \frac{k\delta}{k+1} - 1 \right)^k = \delta^k \left( \frac{k}{k+1} \right)^k \left( 1 - \frac{k+1}{k\delta} \right)^k \geq \delta^k e^{-1} \left( 1 - \frac{k(k+1)}{k\delta} \right)$$

$$s \geq e^{-1} \left( \frac{\delta^k}{k+1} - \delta^{k-1} \right),$$

as required. For the second inequality, we used  $\left( \frac{k}{k+1} \right)^k \geq e^{-1}$  and  $(1-\alpha)^k \geq 1-k\alpha$  for  $\alpha < 1, k \in \mathbb{N}$ .  $\square$

It is worth mentioning that already for rather small values of  $\delta$ , our lower bound exceeds the value  $\delta + (\delta - 2)(g - 3)$  conjectured in [16]. Even for girth five, by taking  $k = 2$ , we obtain  $Z(G) \geq \frac{1}{3} \left( \frac{2\delta}{3} - 1 \right)^2$ , which implies the conjecture of Davila and Kenter for  $\delta \geq 22$ .

The previous approach will now be used to establish a bound which applies to  $H$ -free graphs for any bipartite graph  $H$ . We do not try to optimise the constants in this proof.

*Proof of Theorem 1.2.* It will be useful to rearrange our hypothesis on the Turán number of  $H$ , which is that for  $n \geq n_0$ ,  $\text{ex}(n, H) \leq \beta_H n^{1+c_H}$ . Suppose that  $G_1$  is an  $H$ -free graph with average degree  $d \geq n_0$ . In particular,  $G_1$  has at least  $n_0$  vertices. Denoting  $n_1 = |V(G_1)|$ , the hypothesis gives

$$\frac{1}{2}dn_1 = e(G_1) \leq \beta_H n_1^{1+c_H}$$

$$\left( \frac{d}{2\beta_H} \right)^{\frac{1}{c_H}} \leq n_1.$$

The proof reduces to the following claim, which we state formally because we will use it to prove Corollary 2.2.

**Claim 2.1.** *Suppose that any  $H$ -free graph  $G_1$  with average degree  $d \geq n_0$  satisfies*

$$|V(G_1)| \geq \left( \frac{d}{2\beta_H} \right)^{\frac{1}{c_H}}. \quad (2)$$

*Let  $G$  be an  $H$ -free graph with minimum degree  $\delta \geq 2n_0$ . Then  $Z(G) \geq \frac{1}{2} \left( \frac{\delta}{4\beta_H} \right)^{\frac{1}{c_H}}$ .*

To see this, let  $S$  be a zero forcing set in  $G$  of order  $s$ . Assume that  $s < \frac{n}{2}$ , since otherwise we can apply (2) to the entire graph  $G$  to get

$$s \geq \frac{n}{2} \geq \frac{1}{2} \left( \frac{\delta}{2\beta_H} \right)^{\frac{1}{c_H}} \geq \frac{1}{2} \left( \frac{\delta}{4\beta_H} \right)^{\frac{1}{c_H}}.$$

Starting from  $S$ , we run the zero forcing process until we have reached a set of black vertices  $T$  with  $|T| = 2s$ . Let  $U$  be the set of vertices which forced some vertex of  $T \setminus S$  during our process. Since each vertex can force only one of its neighbours,  $|U| = s$ . Moreover, all the edges with an endpoint in  $U$  lie inside  $T$ . Hence

$$e(T) \geq \frac{|U|}{2} \cdot \delta = \frac{s}{2} \delta.$$

We conclude that the average degree in  $G[T]$  is at least  $\frac{\delta}{2}$ . Now we can apply (2) to  $G[T]$ .

$$|T| = 2s \geq \left( \frac{\delta}{4\beta_H} \right)^{\frac{1}{c_H}},$$

as required.  $\square$

Recall that  $K_{a,b}$  denotes the complete bipartite graph with parts of order  $a$  and  $b$ . Using the well-known result of [30], we give explicit bounds for  $K_{a,b}$ -free graphs.

**Corollary 2.2.** *Let  $G$  be a  $K_{a,b}$ -free graph with minimum degree  $\delta \geq 4a - 4$ . Then*

$$Z(G) \geq \frac{1}{2} \left( \frac{\delta}{4(b-1)^{\frac{1}{a}}} \right)^{\frac{a}{a-1}}.$$

*Proof.* The aforementioned theorem of Kövari, Sós and Turán [30] states that for an  $n$ -vertex  $K_{a,b}$ -free graph with average degree  $d$ ,

$$d \leq (b-1)^{\frac{1}{a}} n^{1-\frac{1}{a}} + a - 1. \quad (3)$$

It follows that  $K_{a,b}$  satisfies (2) with  $n_0 = 2a - 2$  and  $c_H = \frac{a-1}{a}$ . For, let  $G_1$  be an  $n$ -vertex  $K_{a,b}$ -free graph with average degree  $d \geq 2a - 2$ . If the second summand in (3) is strictly larger than the first one, then we have  $d < 2a - 2$ , which is a contradiction. Therefore the first summand is larger, so

$$d \leq 2(b-1)^{\frac{1}{a}} n^{1-\frac{1}{a}}.$$

Rearranging, we get  $n \geq \left( \frac{d}{2(b-1)^{\frac{1}{a}}} \right)^{\frac{a}{a-1}}$ . Our bound on the zero forcing number of  $K_{a,b}$ -free graphs follows from Claim 2.1.  $\square$

Since for  $b > (a-1)!$ , there are constructions of  $K_{a,b}$ -free graphs with minimum degree  $\delta$  and  $O(\delta^{\frac{a}{a-1}})$  vertices (see, e.g., [4]), the result of Corollary 2.2 is tight up to a constant factor.

### 3 The random graph

Here we prove that for  $\frac{\log^2 n}{\sqrt{n}} \leq p = o(1)$ , with high probability

$$Z(G_{n,p}) = n - \left(2 + \sqrt{2} + o(1)\right) \cdot \frac{\log(np)}{p}.$$

Since for  $p = o(1)$ ,  $-\log(1-p) = (1 + o(1))p$ , this establishes the bound of Theorem 1.3. Restricting to  $p = o(1)$  in this section keeps the calculations clearer. The case of constant  $p$  is easier (as we explain below) and can be proved similarly. In what follows, we mostly omit floor and ceiling signs for the sake of clarity of presentation. The logarithms are in base  $e$  unless stated otherwise. All the inequalities will hold for large enough  $n$ . In a graph  $G$ , we denote the set of edges between vertex sets  $S$  and  $T$  by  $E(S, T)$ . We write  $u \sim v$  if the vertices  $u$  and  $v$  are adjacent in  $G$ , and  $u \not\sim v$  otherwise.

Our approach combines the first and the second moment method, and is somewhat similar to the argument used to determine the independence number of  $G_{n,p}$  (see, e.g. [27, Section 7]). However, the proof contains some delicate points, which we try to explain before giving the formal argument. We start this discussion by considering only the uniform model  $G_{n, \frac{1}{2}}$ .

The zero forcing number of the random graph is governed by the occurrence of a specific substructure called a witness. In a graph  $G$  on the vertex set  $V$ , a  $k$ -witness (or a witness of order  $k$ ) is a pair of ordered vertex  $k$ -tuples  $((s_i)_{i \in [k]}, (t_i)_{i \in [k]})$  such that  $s_i, t_i \in V$ ,  $s_i \sim t_i$  for each  $i$ , and  $s_i \not\sim t_j$  for  $i < j$ . The definition requires  $s_i \neq s_j$  for  $i \neq j$ , but it might happen that  $s_i = t_j$  for some  $i > j$ . The adjacency matrix of a  $k$ -witness, where the rows and columns are indexed by  $(s_i)$  and  $(t_i)$  respectively, can be found in Figure 1a. For any pair of  $k$ -tuples  $((s_i)_{i \in [k]}, (t_i)_{i \in [k]})$ , we define the set of *superdiagonal* pairs to be  $\{(s_i, t_j) : i, j \in [k], i < j\}$ , and the set of *diagonal* pairs to be  $\{(s_i, t_i) : i \in [k]\}$ . It is easy to see that if  $G$  has a forcing set  $S$  of order at most  $n - k$ , then it contains a  $k$ -witness (Lemma 3.1). Therefore, our aim is to find the order of the largest witness in  $G_{n, \frac{1}{2}}$ . The first subtlety arises in trying to use the first moment computation to guess the forcing number of  $G_{n, \frac{1}{2}}$ . Let  $R_k$  be the random variable counting the

$k$ -witnesses in  $G_{n, \frac{1}{2}}$ . For fixed  $k$ -tuples  $(s_i)$  and  $(t_i)$ , the probability that they form a witness is  $2^{-\binom{k+1}{2}}$  since they determine  $\binom{k+1}{2}$  superdiagonal and diagonal pairs. Using linearity of expectation, we can multiply this probability with the number of choices for  $(s_i)$  and  $(t_i)$  to obtain

$$\mathbb{E}[R_k] \leq \left( \frac{n!}{(n-k)!} \right)^2 \cdot 2^{-\binom{k+1}{2}} \leq n^{2k} 2^{-\frac{k^2}{2}} = (n^2 2^{-\frac{k}{2}})^k.$$

For  $k \geq (4 + \epsilon) \log_2 n$ , it holds that  $\mathbb{E}[R_k] = o(1)$ , so Markov's inequality implies that with high probability  $G_{n, \frac{1}{2}}$  contains no such  $k$ -witness. On the other hand, if  $k \leq (4 - \epsilon) \log_2 n$  the expected number of  $k$ -witnesses tends to infinity with  $n$ , so it is reasonable to take  $(4 + o(1)) \log_2 n$  as the first guess for the order of the largest witness. For example, in finding the independence number of  $G_{n, p}$ , the first moment computation gives the correct value throughout the range of  $p$ . However, in our case, the actual asymptotic order of a witness,  $k_c := (2 + \sqrt{2}) \log_2 n$ , is smaller than  $4 \log_2 n$ .

The reason for this is that a substructure of a  $k$ -witness  $((s_i)_{i \in [k]}, (t_i)_{i \in [k]})$  obtained by discarding a final segment of  $(s_i)$  and an initial segment of  $(t_i)$  has a lower expected number of copies inside  $G_{n, \frac{1}{2}}$  than the witness itself, and therefore gives a stronger bound on  $k$ . The correct asymptotic value is obtained by taking  $\ell = \ell(k) = \frac{\sqrt{2}}{2} k$ , and counting substructures called  $k$ -subwitnesses. The adjacency matrix of a subwitness is depicted in Figure 1b. For integers  $a \leq b$ , define the interval  $[a .. b] = \{a, a+1, \dots, b\}$ . A  $k$ -subwitness in  $G$  is a pair of  $\ell$ -tuples  $((s'_i)_{i \in [\ell]}, (t'_i)_{i \in [k-\ell+1 .. k]})$  such that  $s'_i, t'_i \in V$ ,  $s'_i \sim t'_i$  for each  $i \in [k-\ell+1 .. \ell]$ , and  $s'_i \not\sim t'_j$  for  $1 \leq i < j \leq k$ . Clearly, if  $((s_i)_{i \in [k]}, (t_i)_{i \in [k]})$  is a witness in  $G$ , then the restrictions  $(s_1, \dots, s_\ell)$  and  $(t_{k-\ell+1}, \dots, t_k)$  form a subwitness.

In Lemma 3.2, we will count  $k$ -subwitnesses for  $k = (1 + \epsilon)k_c = (1 + \epsilon)(2 + \sqrt{2}) \log_2 n$ , and show that with high probability,  $G_{n, \frac{1}{2}}$  contains no such  $k$ -subwitness. An intuition on why we can discard those segments of  $(s_i)$  and  $(t_i)$  is that given a  $(1 - \epsilon)k_c$ -subwitness in  $G_{n, \frac{1}{2}}$ , we can extend it to a  $(1 - \epsilon)k_c$ -witness with high probability. Indeed, to find the remaining columns  $t_1, \dots, t_{k-\ell}$ , we only need to consider their adjacencies with  $s_1, \dots, s_{k-\ell}$ . But  $k - \ell = (1 - \epsilon) \log_2 n$ , and therefore a short computation shows that for any choice of  $s_1, \dots, s_{k-\ell}$ , with high probability, there will be at least  $n^{\frac{\epsilon}{2}}$  vertices in  $G_{n, \frac{1}{2}}$  satisfying any adjacency restriction with  $s_1, \dots, s_{k-\ell}$ . Of course, the same property of  $G_{n, \frac{1}{2}}$  implies that we can find the missing rows  $s_{\ell+1}, \dots, s_k$ .

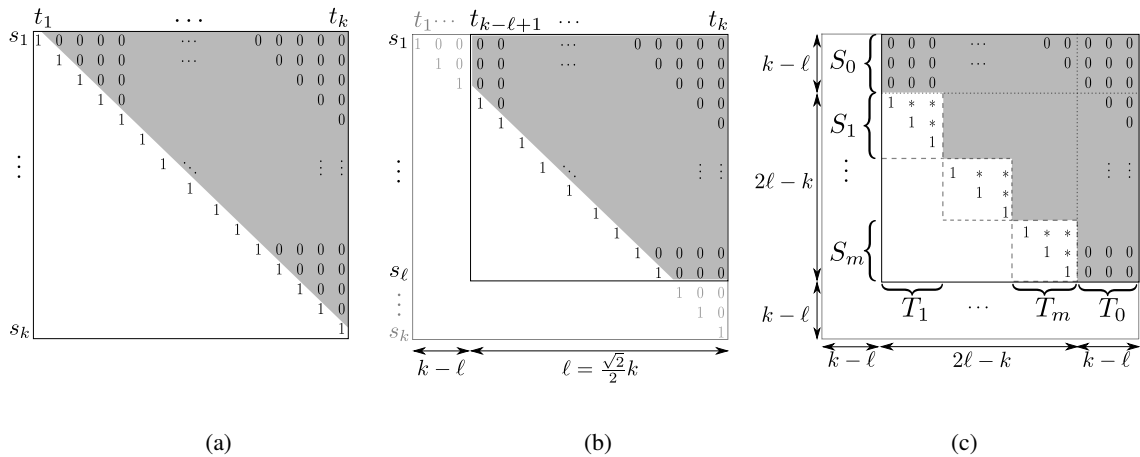


Figure 1: Adjacency matrices of a  $k$ -witness,  $k$ -subwitness and a loose  $k$ -subwitness respectively. The regions which are required to contain only zeros are shaded. In Figure (c), the stars mark the entries which are superdiagonal in this particular ordering of the vertices, but not required to contain zeros.

This intuition gives the correct answer for  $G_{n, \frac{1}{2}}$ , but when  $p = o(1)$  the computation of the expected

number of  $k$ -subwitnesses contains another caveat. In a subwitness,  $(s'_i)_{i \in [\ell]}$  and  $(t'_i)_{i \in [k-\ell+1..k]}$  are orderings of the corresponding vertex sets. In the first moment computation, the ordering contributes a factor of  $(\ell!)^2 = k^{2\ell+o(k)}$ . This factor was negligible when  $p = \frac{1}{2}$  and  $k_c = \Theta(\log n)$ , but for  $p = o(1)$ ,  $G_{n,p}$  contains witnesses whose order is polynomial in  $n$ , so we need to be more careful. Next, we explain how to shave off a factor of  $k^{k+o(k)}$ . A subwitness is modified so that the adjacency matrix is invariant under reordering large subsets of the vertices, at the price of discarding a small number of its zero entries. Figure 1c illustrates this tradeoff.

In a graph  $G$ , we define a *loose  $k$ -subwitness* (or just *loose subwitness*) to be a substructure labelled by sets  $S_0, S_1, \dots, S_m, T_0, T_1, \dots, T_m \subseteq V$  and bijections  $f_i : S_i \rightarrow T_i$  for  $i = 1, \dots, m$ , where  $m = (2\ell - k)p = (\sqrt{2} - 1)kp$  and the following conditions are satisfied.

- (i) The sets  $S_i$  are pairwise disjoint for  $i = 0, \dots, m$ , as well as the sets  $T_i$ . Denoting  $S = \bigcup_{i=0}^m S_i$  and  $T = \bigcup_{i=0}^m T_i$ , we have  $|S| = |T| = \ell$  and  $|S_0| = k - \ell = \left(1 - \frac{\sqrt{2}}{2}\right)k$ . The sets  $S \setminus S_0$  and  $T \setminus T_0$  are partitioned *equitably* into  $S_i$ , and  $T_i$ , that is,  $0 \leq |S_i| - |T_i| \leq 1$  for  $1 \leq i \leq m$ . Therefore,  $\frac{1}{p} - 1 \leq |S_i| = |T_i| \leq \frac{1}{p} + 1$  and the orders of  $S_i$  are non-increasing for  $i \in [m]$ .
- (ii) For the edges between  $S$  and  $T$ , we require  $E(S_0, T) = E(T_0, S) = \emptyset$ , and  $E(S_i, T_j) = \emptyset$  for  $i < j$ . For each bijection  $f_i$  and  $v \in S_i$ , there is an edge in  $G$  between  $v$  and  $f_i(v)$ . In other words, the bijections  $f_i$  determine a matching between  $S_i$  and  $T_i$ .

The key point is that any graph that contains a  $k$ -witness, also contains a loose  $k$ -subwitness, which we use to get an improved bound. Since the sets  $S_i$  and  $T_i$  are not ordered, but only paired by the bijections  $f_i$  for  $i \in [m]$ , we gain a factor of  $k^{-k+o(k)}$  in the first moment computation. On the other hand, for  $i \in [m]$ , we do not care about the adjacency relation between  $S_i$  and  $T_i$  apart from the diagonal vertex pairs, but that costs us a much less significant factor  $(1-p)^{|S_i|^2 m} = (1-p)^{(2\ell-k)/p}$ . In words, the definition of a loose subwitness allows a large number of vertex permutations. However, since those permutations preserve most of the superdiagonal pairs, the adjacency matrix of a loose subwitness still contains most of the zeros which were previously required.

Estimating the expected number of loose subwitnesses in  $G_{n,p}$ , we can match the bound obtained from the second moment method (Lemma 3.3). This computation requires some additional understanding of how two witnesses can interact, but the ideas are explicit in the argument. We are now ready to present the formal proof. We first establish the relationship between the zero forcing number of a graph and the occurrence of a witness. We will be using the shortened notation  $\mathbf{s} = (s_i)_{i \in [k]}$ , and denote the image of this  $k$ -tuple by  $\mathbf{s}[k] = \{s_i : i \in [k]\}$ .

**Lemma 3.1.** *Let  $G$  be an  $n$ -vertex graph. If  $Z(G) \leq n - k$ , then  $G$  contains a  $k$ -witness. Moreover, if  $G$  contains a  $k$ -witness  $(\mathbf{s}, \mathbf{t})$  with  $\mathbf{s}[k] \cap \mathbf{t}[k] = \emptyset$ , then  $Z(G) \leq n - k$ .*

*Proof.* Assume that  $Z(G) \leq n - k$ , that is,  $G$  has a forcing set  $S$  with  $n - |S| \geq k$ . Index the vertices of  $V(G) \setminus S$  according to the order in which they were forced, so  $t_1$  is the first forced vertex,  $t_2$  the second, and so on, up to  $t_k$ . For  $1 \leq i \leq k$ , let  $s_i$  be a vertex which forced  $t_i$ . Then by the definition of a zero forcing set,  $((s_i)_{i \in [k]}, (t_i)_{i \in [k]})$  is a witness.

Conversely, let  $(\mathbf{s}, \mathbf{t})$  be a  $k$ -witness with  $\mathbf{s}[k] \cap \mathbf{t}[k] = \emptyset$ . Then  $V(G) \setminus \mathbf{t}[k]$  is a forcing set in  $G$ , since the vertices  $t_1, \dots, t_k$  can be forced by the vertices  $s_1, \dots, s_k$  respectively.  $\square$

We now formalise the ideas outlined in the previous discussion.

**Lemma 3.2.** *Let  $\frac{C}{n} < p(n) < 1$  for a large constant  $C$ , and define  $k = \frac{(2+\sqrt{2})}{p} (\log(np) + \log \log(np))$ . With high probability,  $G_{n,p}$  contains no  $k$ -witness, and therefore  $Z(G_{n,p}) \geq n - k$ .*

*Proof.* For a graph  $G$  on the vertex set  $V$ , a  $k$ -witness and a loose  $k$ -subwitness have been defined in the previous section. We set  $k = \frac{(2+\sqrt{2})}{p} (\log(np) + \log \log(np))$  and  $\ell = \frac{\sqrt{2}}{2}k$ ,  $r = 2\ell - k = \frac{(\sqrt{2}+o(1))}{p} \log(np)$ ,  $m = pr = (\sqrt{2} + o(1)) \log(np)$ . The crucial fact is that if  $G$  contains a witness  $((s_i)_{i \in [k]}, (t_i)_{i \in [k]})$ , then a loose

subwitness can be found as follows.  $S_0$  consists of the first  $k - \ell$  rows of the witness,  $S_0 := \{s_1, \dots, s_{k-\ell}\}$ , and  $T_0$  of the last  $k - \ell$  columns,  $T_0 := \{t_{\ell+1}, \dots, t_k\}$ . The sets  $S_1, \dots, S_m$  are constructed by ordering the vertices  $s_{k-\ell+1}, s_{k-\ell+2}, \dots, s_\ell$  and partitioning them into  $m$  equitable intervals. Naturally,  $T_1, \dots, T_m$  are the corresponding columns,  $T_j = \{t_i : s_i \in S_j\}$ , and the bijections  $f_j$  map  $s_i$  to  $t_i$  for  $i \in [k - \ell + 1 \dots \ell]$ .

Let  $Y_k$  denote the number of loose  $k$ -subwitnesses in  $G_{n,p}$ . Our aim is to show  $\mathbb{E}[Y_k] \rightarrow 0$ . Fix the sets  $S_j, T_j$  and bijections  $f_j$  which satisfy (i). In particular,  $|S_1 \cup \dots \cup S_m| = |T_1 \cup \dots \cup T_m| = 2\ell - k = r$  and  $|S_i| = |T_i| \in \left[\frac{1}{p} - 1, \frac{1}{p} + 1\right]$  for  $i \in [m]$ . For  $S_j, T_j$  and  $f_j$  to span a loose subwitness, i.e. for (ii) to be satisfied, we require  $(\ell^2 - r^2) + \left(\binom{r}{2} - m \cdot \binom{r/m}{2}\right)$  pairs to be non-edges in  $G_{n,p}$ . The first summand,  $\ell^2 - r^2 = 2(k - \ell)\ell - (k - \ell)^2$ , comes from  $E(S_0, T) = E(T_0, S) = \emptyset$ , and the second from  $E(S_i, T_j) = \emptyset$  for  $i < j$ . The  $m \cdot \binom{r/m}{2}$  pairs have been subtracted since we do not impose any restrictions on  $E(S_i, T_i)$ , and they will turn out to be negligible. Moreover, (ii) requires  $r$  diagonal edges to be present in  $G_{n,p}$ , so the probability that our fixed  $S_j, T_j$  and bijections  $f_j$  satisfy (ii) is at most

$$p^r (1 - p)^{\ell^2 - \frac{r^2}{2} - \frac{r^2}{2m}}.$$

Now we will take the union bound over all the potential loose subwitnesses. There are at most  $\binom{n}{\ell-r}^2$  choices for  $S_0, T_0$ , and  $\left(\frac{n}{\frac{r}{m}}\right)^m$  choices for the sets  $S_j, j \in [m]$ . Each vertex  $v \in S_j$  gets assigned a vertex  $f_j(v)$ , which can be done in at most  $n^r$  ways. This assignment also determines the sets  $T_j = f_j(S_j)$  for  $j \in [m]$ .

$$\mathbb{E}[Y_k] \leq \binom{n}{\ell-r}^2 \left(\frac{n}{\frac{r}{m}}\right)^m n^r p^r (1-p)^{\ell^2 - \frac{r^2}{2} - \frac{r^2}{2m}} \leq \left(\frac{en}{\ell-r}\right)^{2\ell-2r} \left(\frac{enm}{r}\right)^r n^r p^r e^{-p\left(\ell^2 - \frac{r^2}{2} - \frac{r^2}{2m}\right)}.$$

We use the inequalities  $\ell - r \geq \frac{k}{4}$  and  $r \geq \frac{k}{4}$  to obtain

$$\mathbb{E}[Y_k] \leq \left(\frac{4en}{k}\right)^{2\ell-2r} \left(\frac{4en}{k}\right)^r m^r n^r p^r e^{-p\left(\ell^2 - \frac{r^2}{2} - \frac{r^2}{2m}\right)} \leq C_1^k (np)^{2\ell} (kp)^{-2\ell+r} m^r e^{-p\left(\ell^2 - \frac{r^2}{2}\right)},$$

where  $C_1 = 4e^2$ . For the second inequality, we used  $m = pr$ , so that  $e^{\frac{pr^2}{2m}} = e^{r/2} \leq e^k$ . Finally, substituting  $\ell = \frac{\sqrt{2}}{2}k$ ,  $\ell^2 - \frac{r^2}{2} = (\sqrt{2} - 1)k^2$ , and noting that  $(kp)^{-2\ell+r} m^r \leq (kp)^{-2\ell+2r} < 1$ , we obtain

$$\mathbb{E}[Y_k] < C_1^k (np)^{\sqrt{2}k} e^{-pk^2(\sqrt{2}-1)}.$$

Taking  $np$  sufficiently large and recalling that  $pk = (2 + \sqrt{2})(\log(np) + \log \log(np))$ , we get  $\mathbb{E}[Y_k] < 2^{-k}$ . With high probability,  $G_{n,p}$  contains no loose  $k$ -subwitnesses, and therefore no  $k$ -witnesses. By Lemma 3.1,  $Z(G) \geq n - k$  with high probability.  $\square$

To show that with high probability,  $G_{n,p}$  contains a  $k$ -witness  $(\mathbf{s}, \mathbf{t})$  with  $\mathbf{s}[k] \cap \mathbf{t}[k] = \emptyset$ , we use a well-known consequence of Chebyshev's inequality. Let  $X_n$  be a sequence of non-negative random variables indexed by some parameter  $n$  going to infinity. If  $\mathbb{E}[X_n] \rightarrow \infty$  and  $\frac{\text{Var}[X_n]}{(\mathbb{E}[X_n])^2} \rightarrow 0$ , then with high probability  $X_n > 0$ . The proof can be found for example in [5, Corollary 4.3.2].

**Lemma 3.3.** *Let  $p = p(n)$  satisfy  $\frac{\log^2 n}{\sqrt{n}} < p = o(1)$  and  $\epsilon > 0$ . With high probability*

$$Z(G_{n,p}) \leq n - (1 - \epsilon) \cdot \frac{(2 + \sqrt{2}) \log(np)}{p}.$$

*Proof.* Partition the vertex set  $V$  of  $G_{n,p}$  into  $V_1$  and  $V_2$  with  $|V_1| = \lfloor \frac{n}{2} \rfloor$  and  $|V_2| = \lceil \frac{n}{2} \rceil$ . Fix  $k = (1 - \epsilon) \cdot \frac{(2 + \sqrt{2}) \log(np)}{p}$ . We say that a pair  $(\mathbf{s}, \mathbf{t})$  (or the corresponding  $k$ -witness) is *divided* if  $s_i \in V_1$  and  $t_i \in V_2$



for  $i \in [k]$ . We will show that with high probability,  $G_{n,p}$  contains a divided  $k$ -witness. Let  $X_k$  denote the number of such  $k$ -witnesses in  $G_{n,p}$ . Furthermore, for a pair of  $k$ -tuples  $(\mathbf{s}, \mathbf{t})$ , we denote the event that  $(\mathbf{s}, \mathbf{t})$  is a  $k$ -witness by  $W_{\mathbf{s}, \mathbf{t}}$ . Let us first estimate the expectation of  $X_k$ . We will denote  $n' = \frac{n}{2}$ , and define the falling factorial power

$$(n')_k = \frac{n'!}{(n' - k)!}. \quad (4)$$

We crudely bound  $(n')_k \geq \left(\frac{n'}{2}\right)^k$  for  $k \leq \frac{n'}{2}$ . We also use  $1 - p \geq e^{-(p+p^2)} \geq e^{-1.1p}$  for  $0 \leq p \leq 0.1$ . In the following equation, the sum runs over all divided pairs of  $k$ -tuples  $(\mathbf{s}, \mathbf{t})$ .

$$\begin{aligned} \mathbb{E}[X_k] &= \sum_{\mathbf{s}, \mathbf{t}} \mathbb{P}[W_{\mathbf{s}, \mathbf{t}}] = ((n')_k)^2 p^k (1-p)^{\binom{k}{2}} \geq \left(\frac{n}{4}\right)^{2k} p^k e^{-1.1p \frac{k^2}{2}} \\ &\geq \left(\frac{1}{16} n^2 p e^{-1.1 \left(1 + \frac{\sqrt{2}}{2}\right) \log(np)}\right)^k > \left(\frac{1}{16} n^2 p (np)^{-1.9}\right)^k \end{aligned}$$

where in the second line, we used  $pk \leq (2 + \sqrt{2}) \log(np)$ . It follows that  $\mathbb{E}[X_k] \geq (n^{0.1})^k \rightarrow \infty$ .

To use Chebyshev's inequality, we will need second moment estimates. Fix a specific divided pair  $(\mathbf{s}, \mathbf{t})$ . The events  $W_{\mathbf{s}', \mathbf{t}'}$  are symmetric over all the divided pairs  $(\mathbf{s}', \mathbf{t}')$ , so the standard computation (see, e.g. [5, Section 4.3]) gives

$$\text{Var}[X_k] \leq \mathbb{E}[X_k] \sum_{\substack{\mathbf{s}', \mathbf{t}' \\ \mathbf{s}[k] \cap \mathbf{s}'[k] \neq \emptyset \\ \mathbf{t}[k] \cap \mathbf{t}'[k] \neq \emptyset}} \mathbb{P}[W_{\mathbf{s}', \mathbf{t}'} \mid W_{\mathbf{s}, \mathbf{t}}].$$

Note that the sum includes the case  $(\mathbf{s}', \mathbf{t}') = (\mathbf{s}, \mathbf{t})$ , so we do not need the additional summand  $\mathbb{E}[X_k]$  which often appears in the formula. For any pair of  $k$ -tuples  $(\mathbf{s}', \mathbf{t}')$ , we have defined the set of *superdiagonal* pairs to be  $\{(s'_i, t'_j) : i, j \in [k], i < j\}$ , and the set of *diagonal pairs* to be  $\{(s'_i, t'_i) : i \in [k]\}$ . We now partition the pairs  $(\mathbf{s}', \mathbf{t}')$ . Let  $P_{a,b,d}$  denote the set of divided pairs  $(\mathbf{s}', \mathbf{t}')$  such that

- $|\mathbf{s}[k] \cap \mathbf{s}'[k]| = a$ ,  $|\mathbf{t}[k] \cap \mathbf{t}'[k]| = b$ , and
- the number of vertex pairs which are diagonal in both  $(\mathbf{s}, \mathbf{t})$  and  $(\mathbf{s}', \mathbf{t}')$  is  $d$ .

Moreover, we define the term  $T_{a,b,d} = \frac{1}{\mathbb{E}[X_k]} \sum_{(\mathbf{s}', \mathbf{t}') \in P_{a,b,d}} \mathbb{P}[W_{\mathbf{s}', \mathbf{t}'} \mid W_{\mathbf{s}, \mathbf{t}}]$ . If  $d > a$  or  $d > b$ ,  $T_{a,b,d} = 0$ , so we let  $d$  run up to  $a$  for simplicity. Using this partition, our sum can be written as

$$\frac{\text{Var}[X_k]}{(\mathbb{E}[X_k])^2} \leq \sum_{a,b=1}^k \sum_{d=0}^a T_{a,b,d}. \quad (5)$$

We now analyse the term  $T_{a,b,d}$ . We start by counting the divided pairs in  $P_{a,b,d}$ . There are at most  $(n' - k)_{k-a} (n' - k)_{k-b}$  ways of selecting and indexing the vertices of  $\mathbf{s}'[k] \setminus \mathbf{s}[k]$  and  $\mathbf{t}'[k] \setminus \mathbf{t}[k]$ . Then we select  $d$  distinct pairs  $(s_i, t_i)$  which are diagonal in  $(\mathbf{s}, \mathbf{t})$  and will also be diagonal in  $(\mathbf{s}', \mathbf{t}')$ , which can be done in at most  $\binom{k}{d}$  ways. The number of ways to place those pairs into  $(\mathbf{s}', \mathbf{t}')$ , i.e. to choose the index  $j$  such that  $s'_j = s_i$  and  $t'_j = t_i$  is at most  $(k)_d$ . Similarly, we choose  $a - d$  of the remaining vertices in  $\mathbf{s}[k]$ , and assign them any preimage under  $\mathbf{s}'$ , which gives an additional factor of  $\binom{k-d}{a-d} (k-d)_{a-d}$ . Finally, we do the same for  $\mathbf{t}$  and  $\mathbf{t}'$ . Altogether,

$$|P_{a,b,d}| \leq (n' - k)_{k-a} (n' - k)_{k-b} \binom{k}{d} (k)_d \binom{k-d}{a-d} (k-d)_{a-d} \binom{k-d}{b-d} (k-d)_{b-d}. \quad (6)$$

We will later use the fact that  $\frac{(n'-k)_{k-a}}{(n')_k} \leq \frac{(n'-a)_{k-a}}{(n')_k} = \frac{(n'-a)!(n'-k)!}{(n'-k)!n'!} = \frac{1}{(n')_a}$ . To bound the probability of  $(\mathbf{s}', \mathbf{t}') \in P_{a,b,d}$  being a  $k$ -witness, we first bound the number of pairs which are superdiagonal for both  $(\mathbf{s}, \mathbf{t})$  and  $(\mathbf{s}', \mathbf{t}')$ . We can even forget about how the overlap vertices are placed in  $(\mathbf{s}', \mathbf{t}')$ , that is, the number of common superdiagonal pairs is bounded above by  $\Phi(a, b)$ , where

$$\Phi(a, b) = \max_{A, B \subseteq [k], |A|=a, |B|=b} |\{(i, j) \in A \times B : i < j\}|.$$

Note that trivially  $\Phi(a, b) \leq ab$ . By definition of  $\Phi$ ,  $\mathbb{P}[W_{s',t} \mid W_{s,t}] \leq p^{k-d}(1-p)^{\binom{k}{2}-\Phi(a,b)}$ . Dividing by  $\mathbb{E}[X_k]$  and using (6), we get

$$T_{a,b,d} \leq \frac{1}{(n')_a(n')_b} k^{a+b-d} \binom{k}{d} \binom{k}{a-d} \binom{k}{b-d} p^{-d} (1-p)^{-\Phi(a,b)}. \quad (7)$$

The following lemma is essential to our argument.

**Lemma 3.4.** *For any  $k \in \mathbb{N}$  and  $a, b \in [k]$ ,  $\frac{\Phi(a,b)}{k(a+b)} \leq 1 - \frac{\sqrt{2}}{2}$ .*

From its proof, which we defer to the end of this section, it will be clear that the maximum value of  $T_{a,b,d}$  is achieved at  $a = b = \frac{\sqrt{2}}{2}k$ .

We now split into two cases according to the value of  $a + b$ . Firstly, assume that  $a + b \geq \frac{24}{\epsilon p}$ . In this case, we trivially bound the product of the three remaining binomial coefficients in (7) by  $2^{3k}$ . The whole purpose of analysing the term  $T_{a,b,d}$  was to gain an extra factor of  $k^{-d}$  compared to the trivial bound on the number of vertex orderings in  $(s, t)$ . This gives

$$\begin{aligned} T_{a,b,d} &\leq 4^{a+b} 2^{3k} (np)^{-(a+b)} (kp)^{a+b-d} e^{(p+p^2)\Phi(a,b)}, \\ \sum_{d=0}^a T_{a,b,d} &\leq 4^{a+b+1} \cdot 2^{3k} (np)^{-(a+b)} (kp)^{a+b} e^{(p+p^2)\Phi(a,b)}. \end{aligned}$$

For the second inequality, we just summed over  $d$  and used  $\sum_{d=0}^a (kp)^{-d} \leq \sum_{d=0}^a (2 \log(np))^{-d} < 4$ . Using Lemma 3.4 and  $\frac{k}{a+b} \leq \frac{\epsilon}{6} \log(np)$ , we get

$$\sum_{d=0}^a T_{a,b,d} \leq \left( 8kp \cdot 2^{\frac{\epsilon}{6} \log(np)} (np)^{-1} e^{\left(1 - \frac{\sqrt{2}}{2}\right)k(p+p^2)} \right)^{a+b}.$$

Let  $n$  be large enough so that  $p \leq 0.1\epsilon$ . Now  $kp = (1 - \epsilon)(2 + \sqrt{2}) \log(np)$  gives  $e^{\left(1 - \frac{\sqrt{2}}{2}\right)k(p+p^2)} \leq e^{(1-\epsilon)(1+0.1\epsilon) \log(np)} \leq (np)^{(1-0.9\epsilon)}$ , and hence

$$\sum_{d=0}^a T_{a,b,d} \leq \left( 8(1 - \epsilon)(2 + \sqrt{2}) \log(np) (np)^{\left(\frac{1}{2} \log 2 - 0.9\right)\epsilon} \right)^{a+b} \leq (np)^{-\frac{\epsilon}{4}(a+b)}$$

for large enough  $n$ . Summing over  $a, b$ , we get

$$\sum_{\substack{a,b \in [k] \\ a+b \geq \frac{24}{\epsilon p}}} \sum_{d=0}^a T_{a,b,d} \leq \sum_{a=1}^k \sum_{b=1}^k (np)^{-\frac{\epsilon}{4}(a+b)} \leq \left( \sum_{a=1}^k (np)^{-\frac{\epsilon a}{4}} \right)^2 \rightarrow 0. \quad (8)$$

In the second case,  $a + b < \frac{24}{\epsilon p}$ , we bound the binomial coefficients by  $\binom{k}{i} \leq k^i$ ,  $i \in \{d, a-d, b-d\}$ . Then

$$T_{a,b,d} \leq 4^{a+b} n^{-(a+b)} k^{2a+2b-2d} p^{-d} (1-p)^{-ab}.$$

Assuming  $p < \frac{1}{2}$ , we use the inequality  $(1-p) \geq e^{-p-p^2} \geq e^{-2p}$ , which implies  $(1-p)^{-ab} \leq e^{2pab} \leq e^{\frac{p(a+b)^2}{2}}$ . Furthermore,  $kp > 1$ , so

$$T_{a,b,d} \leq \left( 4n^{-1} k^2 e^{\frac{p(a+b)}{2}} \right)^{a+b}.$$

From the condition  $p \geq \frac{\log^2 n}{\sqrt{n}}$ , it follows that  $n^{-1} k^2 \leq n^{-1} \cdot \frac{16n}{\log^4 n} \log^2(np) \leq \frac{16}{\log^2 n}$ . Moreover,  $e^{\frac{p(a+b)}{2}} \leq e^{\frac{12}{\epsilon}}$ , so altogether,  $T_{a,b,d} \leq \left( \frac{1}{\log n} \right)^{a+b}$  for large enough  $n$ . Summing up,

$$\sum_{\substack{a,b \in [k] \\ a+b < \frac{24}{\epsilon p}}} \sum_{d=0}^a T_{a,b,d} \leq \sum_{a=1}^k \sum_{b=1}^k (a+1)(\log n)^{-(a+b)} \leq \left( \sum_{a=1}^k (a+1)(\log n)^{-a} \right) \left( \sum_{b=1}^k (\log n)^{-b} \right) \rightarrow 0.$$

We conclude that  $\frac{\text{Var}[X_k]}{(\mathbb{E}[X_k])^2} = o(1)$ , and hence  $X_k > 0$  with high probability. Upon this event, Lemma 3.1 implies  $Z(G) \leq n - k$ .  $\square$

Now we prove Lemma 3.4, which is essentially finding the induced subgraph of a  $k$ -witness with a minimum expected number of copies in  $G_{n,p}$ .

*Proof of Lemma 3.4.* Let  $k$  be fixed. Recall that we are trying to maximise  $\frac{\Phi(a,b)}{k(a+b)}$  over all  $a, b$ , where  $\Phi(a, b) = \max_{A, B \subseteq [k], |A|=a, |B|=b} |\{(i, j) \in A \times B : i < j\}|$ .

We first fix  $|A| = a$ ,  $|B| = b$  and  $|A \cap B| = g$ . If  $A$  and  $B$  are a selection of rows and columns of a  $k \times k$  matrix, then  $g$  denotes the number of diagonal entries at the intersection of selected rows and columns. Define  $\phi(A, B) = |\{(i, j) \in A \times B : i < j\}|$ . We claim that  $\phi(A, B) \leq ab - \frac{(g+1)g}{2}$ . To see this, note that each element  $(c_1, c_2)$  with  $c_1, c_2 \in A \cap B$  and  $c_1 \geq c_2$  is contained in  $A \times B$ , but not counted by  $\phi$ . There are  $\frac{(g+1)g}{2}$  such pairs (in fact, such  $(c_1, c_2)$  are indices of the subdiagonal matrix entries selected by  $A$  and  $B$ ).

Now we minimise  $g$  for fixed  $a$  and  $b$ . From the identity  $|A \cup B| + |A \cap B| = |A| + |B|$  and  $|A \cup B| \subseteq [k]$ , we get  $g \geq a + b - k$ , so  $\phi(A, B) \leq ab - \frac{(a+b-k+1)(a+b-k)}{2}$ . Taking the maximum over  $A$  and  $B$  and using the AM-GM inequality, we get

$$\begin{aligned} \Phi(a, b) &\leq ab - \frac{(a+b-k+1)(a+b-k)}{2} \leq \left(\frac{a+b}{2}\right)^2 - \frac{(a+b-k)^2}{2} \\ \frac{\Phi(a, b)}{k(a+b)} &\leq \frac{1}{k(a+b)} \left( \left(\frac{a+b}{2}\right)^2 - \frac{(a+b-k)^2}{2} \right). \end{aligned}$$

We substitute  $a+b = 2\alpha k$ , so that the problem reduces to maximising the function  $f(\alpha) = \frac{1}{4\alpha} (2\alpha^2 - (2\alpha - 1)^2)$  for  $0 < \alpha \leq 1$ . This is a simple calculus exercise, but we provide details for the sake of transparency.  $f'(\alpha) = \frac{1}{4\alpha^2} (-2\alpha^2 + 1)$ , so  $f$  attains its local maximum at  $\alpha_0 = \frac{\sqrt{2}}{2}$ . Evaluating  $f$  at  $\alpha_0$ , we get

$$\Phi(a, b) \leq \max_{\alpha} f(\alpha) = f(\alpha_0) = 1 - \frac{\sqrt{2}}{2}$$

for all  $a, b \subseteq [k]$ . Note that the equality is asymptotically attained when  $A = [\ell]$ ,  $B = [k - \ell + 1, k]$  with  $\ell = \lfloor \frac{\sqrt{2}k}{2} \rfloor$ , which we have used in Lemma 3.2 (the 0-statement of Theorem 1.3).  $\square$

## 4 Spectral bounds

In this section we discuss the bounds on the zero forcing number in terms of the graph eigenvalues. The study of spectral properties and their relation to other graph parameters is an established area of research with many diverse techniques and applications, surveyed for example in the monograph of Godsil and Royle [23]. One of the earliest results of this type is Hoffman's bound on the independence number of a graph. Namely, let  $G$  be an  $n$ -vertex  $d$ -regular graph, and let  $\lambda_{\min}$  denote its smallest eigenvalue. Hoffman proved that then  $G$  contains no independent set of order larger than  $\frac{-\lambda_{\min}n}{d-\lambda_{\min}}$ . Note that since the trace of the adjacency matrix of a graph is zero,  $\lambda_{\min}$  is negative. There are many examples showing the bound to be tight.

We establish an analogue of Hoffman's bound for the zero forcing number, showing that  $Z(G) \geq n \left(1 + \frac{2\lambda_{\min}}{d-\lambda_{\min}}\right)$ . To prove this result we use the following well-known estimate on the edge distribution of a graph in terms of its eigenvalues. Part (ii) is provided in, e.g., [31], whereas the variant (i) follows from the same proof. For a graph  $G = (V, E)$  and two sets  $U, W \subseteq V$ , denote the number of edges with one endpoint in  $U$  and the other one in  $W$  by  $e(U, W)$ . Any edge with both endpoints in  $U \cap W$  is counted twice. Recall that an  $(n, d, \lambda)$  graph is a  $d$ -regular  $n$ -vertex graph in which all eigenvalues but the largest one are at most  $\lambda$  in absolute value.

**Theorem 4.1.** Let  $G$  be an  $(n, d, \lambda)$ -graph, and denote its smallest eigenvalue by  $\lambda_{\min}$ . Then for any two vertex subsets  $U, W$  of  $G$ ,

$$(i) \quad \frac{d|U||W|}{n} - e(U, W) \leq -\lambda_{\min} \sqrt{|U||W| \left(1 - \frac{|U|}{n}\right) \left(1 - \frac{|W|}{n}\right)}.$$

$$(ii) \quad \left| \frac{d|U||W|}{n} - e(U, W) \right| \leq \lambda \sqrt{|U||W| \left(1 - \frac{|U|}{n}\right) \left(1 - \frac{|W|}{n}\right)}.$$

*Proof of Theorem 1.4 (i).* Let  $(\mathbf{s}, \mathbf{t})$  be a  $k$ -witness in  $G$ , and  $k = 2\mu n$ . Note that there are no edges between the sets  $U = \{s_1, s_2, \dots, s_{\mu n}\}$  and  $W = \{t_{\mu n+1}, \dots, t_k\}$ . Hence, using Theorem 4.1, we get

$$0 = e(U, W) \geq d\mu^2 n + \lambda_{\min} \mu n(1 - \mu) \\ -\lambda_{\min} \geq d\mu - \lambda_{\min} \mu \\ \mu \leq \frac{-\lambda_{\min}}{d - \lambda_{\min}}.$$

Hence the largest witness in  $G$  has order at most  $\frac{-2\lambda_{\min}n}{d - \lambda_{\min}}$ , which by Lemma 3.1 implies

$$Z(G) \geq n \left(1 + \frac{2\lambda_{\min}}{d - \lambda_{\min}}\right). \quad \square$$

Surprisingly, the additional factor of two in the above-mentioned bound that looks like an artefact of the proof, turns out to be necessary, and the result of Theorem (i) is shown to be tight by the following example.

**Proposition 4.2.** For any  $D \geq 2$ , and for infinitely many values of  $N$ , there exists an  $N$ -vertex  $D$ -regular graph  $G^*$  whose smallest eigenvalue is  $\lambda_{\min} = -2$ , and which satisfies  $N - Z(G^*) \geq \frac{4N}{D+2} - 2$ .

*Proof.* Let  $G$  be an  $n$ -vertex  $d$ -regular graph which contains a Hamilton cycle consisting of edges  $e_1, e_2, \dots, e_n$  in this order. Clearly, such graphs do exist. Let  $G^*$  be the line graph of  $G$ , that is,  $G^*$  has the vertex set  $E(G)$  with two vertices adjacent if the corresponding edges in  $G$  share a vertex. Then  $G^*$  has  $N = \frac{nd}{2}$  vertices and is  $D$ -regular with  $D = 2d - 2$ . Moreover, Hoffman [26] has observed that the smallest eigenvalue of  $G^*$  is  $-2$ .

Note that the vertices in  $G^*$  corresponding to  $e_1, e_2, \dots, e_n$  form an induced cycle. This implies that  $V(G^*) \setminus \{e_3, e_4, \dots, e_n\}$  is a zero forcing set in  $G^*$ . Namely, the vertex  $e_i$  forces  $e_{i+1}$  for  $i = 2, 3, \dots, n-1$ . This zero forcing set has order  $N - (n-2)$ . Finally, notice that in  $G^*$ , we have

$$-\frac{2\lambda_{\min}N}{d - \lambda_{\min}} = \frac{4 \cdot \frac{nd}{2}}{2d - 2 + 2} = n. \quad \square$$

Next, we turn our attention to the second part of Theorem 1.4, which says that any  $(n, d, \lambda)$ -graph  $G$  satisfies

$$Z(G) \leq n \left(1 - \frac{1}{2(d - \lambda)} \log \left( \frac{d - \lambda}{2\lambda + 1} \right)\right).$$

In particular, if  $\lambda = d^{1-\epsilon}$  for some  $\epsilon > 0$ , then  $n - Z(G) = \Omega\left(\frac{n \log d}{d}\right)$ .

*Proof of Theorem 1.4 (ii).* We greedily construct a witness. In each step  $i$ , we will select vertices  $s_i, t_i \in U_{i-1}$  and a set  $U_i \subseteq U_{i-1}$ . Start with  $U_0 = V$ , the vertex set of  $G$ . Assuming that the steps  $1, \dots, i-1$  were executed, let  $s_i$  be any vertex in  $U_{i-1}$  satisfying  $1 \leq \deg_{G[U_{i-1}]}(s_i) \leq (d - \lambda) \frac{|U_{i-1}|}{n} + \lambda$ . We fix  $t_i$  to be any neighbour of  $s_i$ , and set  $U_i = U_{i-1} \setminus N_G(s_i)$  (note that  $N_G(s_i)$  contains  $s_i$ ). The algorithm continues as long as  $|U_i| > \frac{\lambda n}{d + \lambda}$ . Denote the final number of steps by  $k$ .

It is clear that such  $k$ -tuples  $(\mathbf{s}, \mathbf{t})$  form a witness. We will show that there is a choice for  $s_i$  throughout the algorithm, and that  $k \geq \frac{n}{2(d - \lambda)} \log \left( \frac{d - \lambda}{2\lambda + 1} \right)$ .

**Claim 4.3.** *If  $|U_i| > \frac{\lambda n}{d+\lambda}$ , then the induced subgraph  $G[U_i]$  contains a vertex  $u$  satisfying  $1 \leq \deg_{G[U_i]}(u) \leq (d-\lambda)\frac{|U_i|}{n} + \lambda$ .*

Suppose that some set  $U_i$  does not satisfy the Claim. Since  $|U_i| > \frac{\lambda n}{d+\lambda}$ , it is not an independent set by Theorem 4.1. Therefore, removing all the isolated vertices in  $G[U_i]$ , we get a non-empty set of vertices  $W \subseteq U_i$  in which every vertex  $u$  satisfies  $\deg_{G[W]}(u) > (d-\lambda)\frac{|U_i|}{n} + \lambda$ . In particular,

$$e(W, W) > 2 \cdot \frac{|W|}{2} \left( (d-\lambda)\frac{|U_i|}{n} + \lambda \right),$$

recalling that we are counting each edge in  $E(W, W)$  twice. On the other hand, Theorem 4.1 implies that

$$e(W, W) \leq |W| \left( \frac{d|W|}{n} + \lambda \left( 1 - \frac{|W|}{n} \right) \right) \leq |W| \left( (d-\lambda)\frac{|U_i|}{n} + \lambda \right).$$

We reached a contradiction, which completes the proof of the Claim.

Now denote  $a_i = \frac{|U_i|}{n}$ . By construction,  $a_0 = 1$  and

$$a_{i+1} \geq a_i - \frac{d-\lambda}{n} \cdot a_i - \frac{\lambda+1}{n}.$$

**Claim 4.4.** *For  $i \leq \frac{n}{2(d-\lambda)} \log \frac{d-\lambda}{2\lambda+1}$ ,  $a_i \geq \frac{\lambda}{d+\lambda}$ .*

It is not hard to show by induction that for all  $i$ ,

$$a_i \geq \left( 1 + \frac{\lambda+1}{d-\lambda} \right) \left( 1 - \frac{d-\lambda}{n} \right)^i - \frac{\lambda+1}{d-\lambda}.$$

Now we estimate  $a_i$ , ignoring the constant  $\left( 1 + \frac{\lambda+1}{d-\lambda} \right)$  and using the inequality  $1 - \frac{d-\lambda}{n} \geq e^{-\frac{2(d-\lambda)}{n}}$  for  $\frac{d-\lambda}{n} < \frac{1}{2}$ . This gives

$$a_i \geq e^{-\frac{2(d-\lambda)}{n} \cdot \frac{n}{2(d-\lambda)} \log \left( \frac{d-\lambda}{2\lambda+1} \right)} - \frac{\lambda+1}{d-\lambda} = \frac{2\lambda+1}{d-\lambda} - \frac{\lambda+1}{d-\lambda} = \frac{\lambda}{d+\lambda},$$

as required. We get that the algorithm continues for at least  $k = \frac{n}{2(d-\lambda)} \log \frac{d-\lambda}{2\lambda+1}$  steps, so

$$Z(G) \leq n \left( 1 - \frac{1}{2(d-\lambda)} \log \frac{d-\lambda}{2\lambda+1} \right). \quad \square$$

To show that this bound is tight up to a constant factor, we exhibit a sequence of  $(n, d, \lambda)$ -graphs  $G_m$  with  $\lambda = O(\sqrt{d})$  whose forcing number is at least  $n \left( 1 - \frac{\log_2 d}{2d} + o(1) \right)$ . We use the following construction from [31, Section 3]. For an odd integer  $m$ , the vertices of  $G_m$  are all binary vectors of length  $m$  with an odd number of ones except for the all-one vector. Two distinct vertices are adjacent iff the inner product of the corresponding vectors is 1 modulo 2. This graph has  $n_m = 2^{m-1} - 1$  vertices, degree  $d_m = \frac{n_m-3}{2}$ , and second largest eigenvalue  $\lambda(G_m) = 1 + 2^{\frac{m-3}{2}} = O(\sqrt{d_m})$ . It is easy to check that if  $(\mathbf{s}, \mathbf{t})$  is a  $k$ -witness in  $G_m$ , then the vectors corresponding to  $t_1, t_2, \dots, t_k$  are linearly independent, and therefore  $k \leq m = (1 + o(1)) \log_2 n_m = \frac{(1+o(1))n_m}{2d_m} \log_2 d_m$ . This implies the required bound on  $Z(G_m)$ .

## 5 Concluding Remarks

- Theorem 1.3 can be extended to  $p = \omega(n^{-1})$ . The proof combines our second moment estimates with Talagrand's inequality, along the lines of [27, Theorem 7.4], which finds independent sets of order  $p^{-1} \log(np)$  in  $G_{n,p}$ . Since this proof gives no additional insight, we put it into the appendix.

- It would be interesting to study the minimum rank of quasirandom graphs. Recall that the minimum rank of the random graph  $G_{n, \frac{1}{2}}$  is bounded away from 0, that is,  $mr(G_{n, \frac{1}{2}}) \geq 0.14n$  with high probability (see, e.g. [25]). We wonder if this also holds for  $(n, d, \lambda)$ -graphs when  $d$  is linear in  $n$  and  $\lambda = o(n)$ .
- Another question would be to find the zero forcing number of the random regular graph  $G_{n,d}$ , which is a graph chosen uniformly at random from all  $n$ -vertex  $d$ -regular graphs. We are interested in  $G_{n,d}$  for a large constant  $d$  and  $n \rightarrow \infty$ . A greedy argument (see, e.g. [6]) shows that  $Z(G_{n,d}) \leq n(1 - \frac{1}{d-1})$  deterministically, whereas Theorem 1.4 (ii) implies that for large  $d$ , with high probability,  $Z(G_{n,d}) \leq n(1 - \frac{\log d}{4d})$ . This follows from the fact that with high probability,  $G_{n,d}$  is an  $(n, d, \lambda)$ -graph with  $\lambda \leq 3\sqrt{d}$  (see, e.g., [19]). The lower bound,  $Z(G_{n,d}) \geq n(1 - \frac{40 \log d}{d})$ , is an immediate consequence of the fact that with high probability,  $G_{n,d}$  contains edges between any two sets  $S, T$  with  $|S|, |T| \geq \frac{20n \log d}{d}$  (see, e.g., [28, Lemma 3.6]). It would be interesting to find the correct constant.

## References

- [1] AIM minimum rank – special graphs work group, Zero forcing sets and the minimum rank of graphs, *Linear Algebra Appl.* 428.7 (2008), 1628–1648.
- [2] A dynamic catalog of spectral data for families of graphs, <http://aimath.org/pastworkshops/catalog2.html>. Accessed on 1 May 2017.
- [3] N. Alon, S. Hoory, and N. Linial, The Moore bound for irregular graphs, *Graphs Combin.* 18 (2002), 53 – 57.
- [4] N. Alon, L. Rónyai, and T. Szabó, Norm-graphs: variations and applications, *J. Combin. Theory Ser. B* 76 (1999), 280–290.
- [5] N. Alon and J.H. Spencer, **The probabilistic method**, Second Edition, John Wiley & Sons, Inc., New York, 2000.
- [6] D. Amos, Y. Caro, R. Davila, R. Pepper, Upper bounds on the  $k$ -forcing number of a graph, *Discrete Appl. Math.* 181 (2015), 1–10.
- [7] A. Arenas, A. Diaz-Guilera, J. Kurths, Y. Moreno, and C. Zhou, Synchronization in complex networks. *Phys. Rep.* 469 (2008), 93 – 153.
- [8] J. Balogh, B. Bollobás and R. Morris, Graph bootstrap percolation, *Random Structures Algorithms* 41 (4) (2012), 413 – 444.
- [9] A. Barrat, M. Barthélemy and A. Vespignani, **Dynamical processes in complex networks**, Cambridge University Press, Cambridge, UK, 2008.
- [10] D. Burgarth and V. Giovannetti, Full control by locally induced relaxation, *Phys. Rev. Lett.* 99 (2007), 100501.
- [11] D. Burgarth, S. Bose, C. Bruder and V. Giovannetti, Local controllability of quantum networks, *Phys. Rev. A* 79 (2009), 060305 (R).
- [12] Y. Caro and R. Pepper, Dynamic approach to  $k$ -forcing, Preprint available on <http://arxiv.org/abs/1405.7573v1> (2014).
- [13] J. Chalupa, P.L. Leath and G.R. Reich, Bootstrap percolation on a Bethe lattice, *J. Phys. C: Solid State Phys.* 12 (1979), L31.
- [14] A. Coja-Oghlan, U. Feige, M. Krivelevich, D. Reichman, Contagious sets in expanders, *Proceedings of the 26th Symposium on Discrete Algorithms (SODA 2015)*, 1953 – 1987.

- [15] R. Davila, T. Kalinowski, and S. Stephen, Proof of a conjecture of Davila and Kenter regarding a lower bound for the forcing number in terms of girth and minimum degree, arXiv preprint. Preprint available on <http://arxiv.org/abs/1611.06557> (2016).
- [16] R. Davila, and F. Kenter. Bounds for the zero forcing number of a graph with large girth, *Theory Appl. Graphs* 2 (2015).
- [17] S.M. Fallat and L. Hogben, Minimum Rank, Maximum Nullity, and Zero Forcing Number of Graphs, **Handbook of Linear Algebra**, second edition (ed L. Hogben), CRC Press, Boca Raton, FL, 2014.
- [18] M. Freidlin and A. Wentzell, Diffusion processes on graphs and the averaging principle, *Ann. Probab.* 21 (1993), 2215 – 2245.
- [19] J. Friedman, A Proof of Alon’s Second Eigenvalue Conjecture and Related Problems, *Mem. Amer. Math. Soc.* (2008).
- [20] Z. Füredi and M. Simonovits, The history of degenerate (bipartite) extremal graph problems, **Erdős Centennial** (eds L. Lovász, I. Ruzsa and V. T.-Sós), vol. 25 of Bolyai Soc. Math. Stud., Springer, 2013, 169 – 264.
- [21] M. Gentner, L.D. Penso, D. Rautenbach and U.S. Souza, Extremal values and bounds for the zero forcing number, *Discrete Appl. Math.* 214 (2016), 196 – 200.
- [22] M. Gentner and D. Rautenbach, Some bounds on the zero forcing number of a graph, Preprint available on <http://arxiv.org/abs/1608.00747> (2016).
- [23] C. Godsil and G. Royle, **Algebraic graph theory**, Springer Verlag, New York 2001.
- [24] M. Granovetter, Threshold models of collective behavior, *Am. J. Sociol.* 83, 1420 – 1443 (1978).
- [25] T. Hall, L. Hogben, R.R. Martin and B. Shader, Expected values of parameters associated with the minimum rank of a graph, *Linear Algebra Appl.* 433.1 (2010), 101–117.
- [26] A.J. Hoffman, Some recent results on spectral properties of graphs, *Beiträge zur Graphentheorie* (1968), 75 – 80.
- [27] S. Janson, T. Łuczak and A. Ruciński, **Random Graphs**, Wiley – Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, New York, 2000.
- [28] N. Kamčev, T. Łuczak, B. Sudakov, Anagram-free colorings of graphs, *Combin. Probab. Comput.*, to appear.
- [29] D. Kempe, J. Kleinberg and E. Tardos. Maximizing the spread of influence in a social network. In *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)* (2003), 137 – 146.
- [30] T. Kövári, V. T. Sós, and P. Turán, On a problem of K. Zarankiewicz, *Colloq. Math.* 3 (1954), 50 – 57.
- [31] M. Krivelevich and B. Sudakov, Pseudo-random graphs, **More Sets, Graphs and Numbers** (eds E. Gyori, G.O.H. Katona and L. Lovász), vol. 15 of Bolyai Soc. Math. Stud., Springer, 2006 , 199 – 262.
- [32] F.A. Taklimi, Zero Forcing Sets for Graphs, University of Regina, 2013. Diss. Ph.D. thesis.

## A The random graph with small $p$

To extend Lemma 3.3 for small  $p$  we use Talagrand’s Inequality (see, e.g., [27, Theorem 2.29]).

**Lemma A.1.** Assume  $\omega(n^{-1}) = p < \frac{\log^2 n}{\sqrt{n}}$ . Let the vertex set  $V$  of  $G_{n,p}$  be partitioned into  $V_1$  and  $V_2$  with  $|V_1| = \lfloor \frac{n}{2} \rfloor$  and  $|V_2| = \lceil \frac{n}{2} \rceil$ , and let  $k_{-\epsilon} = \frac{(1-\epsilon)(2+\sqrt{2})}{p} \cdot \log(np)$  with  $0 < \epsilon < \frac{1}{2}$ . With high probability,  $G_{n,p}$  contains a divided  $k_{-\epsilon}$ -witness.

*Proof.* Denote by  $w(G)$  the order of the largest divided witness. For a given  $\epsilon$ , we will actually show that  $w(G_{n,p}) \geq k_{-2\epsilon} = \frac{(1-2\epsilon)(2+\sqrt{2})}{p} \cdot \log(np)$  whp. The first step is a second moment lower bound on the probability  $\mathbb{P}[w(G_{n,p}) \geq k_{-\epsilon}]$ . For now, we write  $k = k_{-\epsilon}$ . The proof is identical to the proof of Lemma 3.3 down to equation (8). The case  $a + b \geq \frac{24}{\epsilon p}$  remains unchanged (and that is the case which determines  $k$ ). Hence we assume  $a + b < \frac{24}{\epsilon p}$ . Equation (7) from the proof of Lemma 3.3 implies

$$\begin{aligned} T_{a,b,d} &\leq \left(\frac{2}{n}\right)^{a+b} k^{a+b-d} p^{-d} \binom{k}{d} \binom{k}{a-d} \binom{k}{b-d} (1-p)^{-ab} \\ &\leq \left(\frac{2k}{n}\right)^{a+b} \binom{k}{d} \binom{k}{a} \binom{k}{b} (1-p)^{-ab}. \end{aligned}$$

Denote  $a + b = 2u$  and define  $S_u := \left(\frac{2k}{n}\right)^{2u} \binom{k}{u}^3 (1-p)^{-u^2}$ . It is clear that  $T_{a,b,d} \leq S_{\frac{a+b}{2}} = S_u$ , so we will maximise  $S_u$  for  $u \in [1, \frac{12}{\epsilon p}]$ . We compute

$$\frac{S_{u+1}}{S_u} = \left(\frac{2k}{n}\right)^2 \cdot \left(\frac{k-u}{u+1}\right)^3 (1-p)^{-2u-1}.$$

We will use the following two claims.

**Claim A.2.**  $\frac{S_{u+1}}{S_u}$  has at most one local extremum on  $[1, \frac{12}{\epsilon p}]$ .

**Claim A.3.** For  $u_1 = 2k \left(\frac{k}{n}\right)^{\frac{2}{3}}$ ,  $\frac{S_{u_1+1}}{S_{u_1}} < 1$ . Moreover,  $\frac{S_2}{S_1} \geq 1$ .

The two claims imply that the maximum of  $S_u$  lies in the interval  $[1, u_1]$ . For, there is at most one point  $u$  where  $\frac{S_{u+1}}{S_u}$  switches from larger than one to smaller than one. The second claim implies that such a point lies in the interval  $[1, u_1]$ . We will prove the two claims later. Now we finish the proof assuming the claims, that is, we bound  $S_u$  for  $u \leq u_1$ .

$$S_u = \left(\frac{2k}{n}\right)^{2u} \binom{k}{u}^3 (1-p)^{-u^2} \leq \left(\frac{4k^2}{n^2} \cdot \frac{e^3 k^3}{u^3}\right)^u e^{2pu^2}.$$

We use the fact that

- (i)  $2pu_1 \leq 2pk \leq 4 \log(np)$ , and
- (ii) the function  $u \mapsto \left(\frac{4e^3 k^3}{n^2 u^3}\right)^u$  is increasing for  $u^3 \leq \frac{4e^2 k^5}{n^2}$ , and in particular on  $[1, u_1]$ .

$$\log S_u \stackrel{(ii)}{\leq} u_1 \left( \log \left( \frac{4k^2}{n^2} \cdot \frac{e^3 n^2}{8k^2} \right) + 2pu_1 \right) \stackrel{(i)}{\leq} u_1 (3 + 4 \log(np)) \leq k \cdot 10 \log(np) \cdot \left(\frac{k}{n}\right)^{\frac{2}{3}} \leq k(np)^{-\frac{1}{2}}.$$

The third inequality, where  $u_1 \ll k$  is really used, is crucial in the calculation. We conclude that for all  $a, b, d$  such that  $a + b < \frac{24}{\epsilon p}$ ,

$$T_{a,b,d} \leq e^{k(np)^{-\frac{1}{2}}}.$$

Summing over all such  $a, b, d$  and using (8) we get

$$\frac{\text{Var}[X_k]}{(\mathbb{E}[X_k])^2} \leq \sum_{\substack{a,b \in [k] \\ a+b \geq \frac{24}{\epsilon p}}} \sum_{d=0}^a T_{a,b,d} + \sum_{\substack{a,b \in [k] \\ a+b < \frac{24}{\epsilon p}}} \sum_{d=0}^a T_{a,b,d} \leq k^3 e^{k(np)^{-\frac{1}{2}}} + o(1) \leq e^{2k(np)^{-\frac{1}{2}}}.$$



We will apply a stronger form of Chebyshev's inequality, which reads  $\mathbb{P}[X_k > 0] \geq \frac{(\mathbb{E}[X_k])^2}{\mathbb{E}[X_k^2]}$ . For details, refer to [27, Remark 3.1].

$$\frac{\mathbb{E}[X_k^2]}{(\mathbb{E}[X_k])^2} = \frac{\text{Var}[X_k]}{(\mathbb{E}[X_k])^2} + 1 \leq e^{4k(np)^{-\frac{1}{2}}}, \quad \text{so}$$

$$\mathbb{P}[X_k > 0] \geq e^{-4k(np)^{-\frac{1}{2}}}.$$

To show concentration of the order of the largest divided witness  $w(G_{n,p})$ , we apply Talagrand's Inequality. The random graph  $G_{n,p}$  is modelled using vertex exposure. Formally, we fix an ordering of the vertices  $v_1, v_2, \dots, v_n$ , and define mutually independent random variables  $(Z_i)_{i \in [n]}$ , where  $Z_i$  exposes the backward edges from the vertex  $v_i$ . Then the  $w(G_{n,p})$  is a function of  $Z_1, \dots, Z_n$ . This function is 1-Lipschitz, that is, if graphs  $G$  and  $G'$  differ only at the vertex  $v_i$ , then  $|w(G) - w(G')| \leq 1$ . Moreover, whenever  $w(G_{n,p}) \geq k$ , there exist  $2k$  certificate vertices, namely the vertices of a divided  $k$ -witness, which are responsible for the fact that  $w(G_{n,p}) \geq k$ . Hence we may apply [27, Theorem 2.29] with  $\psi(k) = 2k$  in their notation. Recalling that  $k_{-\epsilon} = \frac{(1-\epsilon)(2+\sqrt{2})}{p} \cdot \log(np)$ , we have

$$\mathbb{P}[w(G) \leq k_{-2\epsilon}] \mathbb{P}[w(G) \geq k_{-\epsilon}] \leq e^{-\frac{(k_{-\epsilon} - k_{-2\epsilon})^2}{8k_{-\epsilon}}} \leq e^{-\frac{\epsilon^2 k_{-\epsilon}}{8}}.$$

We have shown that  $\mathbb{P}[w(G) \geq k_{-\epsilon}] \geq e^{-4k_{-\epsilon}(np)^{-\frac{1}{2}}}$ . Putting this together with the previous inequality and taking  $np > \left(\frac{10}{\epsilon}\right)^4$ ,

$$\mathbb{P}[w(G) \leq k_{-2\epsilon}] \leq e^{-\frac{\epsilon^2 k_{-\epsilon}}{8} + 4k_{-\epsilon}(np)^{-\frac{1}{2}}} \leq e^{-\frac{\epsilon^2 k_{-\epsilon}}{16}} \rightarrow 0,$$

as required.

*Proof of Claim A.2.* We differentiate  $f(u) = \left(\frac{k-u}{u+1}\right)(1-p)^{-2u/3}$ , the part of  $\frac{S_{u+1}}{S_u}$  which is dependent on  $u$ , raised to power  $\frac{1}{3}$  to simplify the calculation. This is valid since the function  $x \mapsto x^3$  is increasing. Let us replace  $(1-p)$  by  $e^{-q}$ , where  $q = -\log(1-p)$ .

$$f'(u) = e^{2qu/3} \left( \frac{-1}{u+1} - \frac{k-u}{(u+1)^2} + \frac{k-u}{u+1} \cdot \frac{2q}{3} \right)$$

$$f'(u) = 0 \quad \Leftrightarrow \quad k+1 + \frac{2q}{3}(-ku - k + u^2 + u) = 0$$

This is a quadratic equation in  $u$ . Viète's formulae give that if  $u_-$  and  $u_+$  are solutions, then  $u_- + u_+ = k-1$ . Therefore the larger solution, say  $u_+$ , is at least  $\frac{k-1}{2}$ . Since  $\frac{12}{\epsilon p} < \frac{k-1}{2}$  provided that  $np$  is sufficiently large,  $u_-$  is the only potential local extremum in  $\left[1, \frac{12}{\epsilon p}\right]$ .  $\square$

*Proof of Claim A.3.* Take  $u_1$  as in the statement. Then  $\frac{k^3}{u_1^3} = \frac{1}{8} \left(\frac{n}{k}\right)^2$

$$\frac{S_{u+1}}{S_u} \leq \left(\frac{2k}{n}\right)^2 \cdot 2^{-3} \cdot \frac{n^2}{k^2} \cdot e^{8pk\left(\frac{k}{n}\right)^{2/3}} = (1+o(1))\frac{1}{2}.$$

Furthermore,

$$\frac{S_2}{S_1} = \left(\frac{2k^2}{n}\right) \left(\frac{k-1}{2}\right)^3 (1-p)^{-2} \geq \frac{k^5}{10n^2} \cdot \frac{1}{4} > 1. \quad \square$$

This concludes the proof of the lemma.  $\square$