Combinatorics, Probability and Computing (2015) 24, 457–479.
doi:10.1017/S0963548314000194

Randomized Rumour Spreading: The Effect of the Network Topology

KONSTANTINOS PANAGIOTOU[1†],
XAVIER PÉREZ-GIMÉNEZ[2], THOMAS SAUERWALD[3†] and HE SUN[4]

[1]Mathematisches Institut, Universität München, Theresienstr. 39, 80333 München, Germany
(e-mail: kpanagio@math.lmu.de)

[2]Max Planck Institute for Informatics, Campus E1.4, 66123 Saarbrücken, Germany
(e-mail: xperez@mpi-inf.mpg.de)

[3]Computer Laboratory, University of Cambridge, 15 JJ Thomson Avenue, Cambridge CB3 0FD, UK
(e-mail: thomas.sauerwald@cl.cam.ac.uk)

[4]Cluster of Excellence "Multimodal Computing and Interaction", Computer Science, Saarland University, 66123 Saarbrücken, Germany
(e-mail: hsun@mpi-inf.mpg.de)

Received 31 January 2013; revised 25 February 2014; first published online 6 May 2014

We consider the popular and well-studied push model, which is used to spread information in a given network with n vertices. Initially, some vertex owns a rumour and passes it to one of its neighbours, which is chosen randomly. In each of the succeeding rounds, every vertex that knows the rumour informs a random neighbour. It has been shown on various network topologies that this algorithm succeeds in spreading the rumour within $O(\log n)$ rounds. However, many studies are quite coarse and involve huge constants that do not allow for a direct comparison between different network topologies. In this paper, we analyse the push model on several important families of graphs, and obtain tight runtime estimates. We first show that, for any almost-regular graph on n vertices with small spectral expansion, rumour spreading completes after $\log_2 n + \log n + o(\log n)$ rounds with high probability. This is the first result that exhibits a general graph class for which rumour spreading is essentially as fast as on complete graphs. Moreover, for the random graph $G(n, p)$ with $p = c \log n/n$, where $c > 1$, we determine the runtime of rumour spreading to be $\log_2 n + \gamma(c) \log n$ with high probability, where $\gamma(c) = c \log(c/(c-1))$. In particular, this shows that the assumption of almost regularity in our first result is necessary. Finally, for a hypercube on $n = 2^d$ vertices, the runtime is with high probability at least $(1+\beta) \cdot (\log_2 n + \log n)$, where $\beta > 0$. This reveals that the push model on hypercubes is slower than on complete graphs, and thus shows that the assumption of small spectral expansion in our first result is also necessary. In addition, our results combined with the upper bound of $O(\log n)$ for the hypercube

† Part of this work was done while the author was affiliated with the Max Planck Institute for Informatics.

(see [11]) imply that the push model is faster on hypercubes than on a random graph $G(n, c\log n/n)$, where c is sufficiently close to 1.

2010 *Mathematics subject classification*: Primary 05C85
Secondary 68Q87, 68W20

1. Introduction

Randomized broadcasting is one of the most important communication primitives in large networks. A classical and well-studied protocol is the following algorithm, which is known in the literature as the *push model* or *randomized rumour spreading*. Initially, some rumour is placed on one of the n vertices of a given network G. Then, in succeeding rounds, every vertex that knows the rumour selects one of its neighbours uniformly at random, and passes the information to it. The crucial question is: How many rounds are needed until every vertex becomes informed?

The push model has been studied in many works, and its performance on several different families of graphs is well understood. In one of the first papers dealing with this topic, Frieze and Grimmett [15] proved that if the underlying graph is the complete graph with n vertices, then asymptotically almost surely (a.a.s.) (with probability tending to 1 as $n \to \infty$) the broadcast is completed within $(1 + o(1))(\log_2 n + \log n)$ rounds, where $\log n$ will denote the natural logarithm. The problem has been subsequently studied on a number of graph classes, such as hypercubes, bounded-degree graphs, and Erdős–Rényi random graphs: see, *e.g.*, [11, 21]. In particular, for hypercubes and Erdős–Rényi random graphs $G(n, p)$ with $p = c\log n/n$, $c > 1$, a runtime bound of $O(\log n)$ was shown in [11]. In [9], the authors proved a lower bound of $\log_2 n + \log n - o(\log n)$ which holds for any regular graph. Neglecting low-order terms, this implies that complete graphs have the fastest broadcast time among regular graphs.

Most of the existing bounds for the performance of the push model on general graphs show that a.a.s. the number of rounds needed is $O(f(G)\,\mathrm{polylog}(n))$, where $f(G)$ is some graph parameter. In particular, Giakkoupis and Sauerwald [18] showed that $f(G)$ can be chosen as the inverse vertex expansion of G. Moreover, Giakkoupis [17] and Chierichetti, Lattanzi and Panconesi [5] proved, among other things, that $f(G) \leqslant c_\alpha \phi^{-1}$, where ϕ is the conductance of G and c_α is a quantity depending on the ratio α of the maximum and minimum degree (see also [26] for a result for regular graphs). All the above results imply that if the parameter in question is within reasonable bounds, then we obtain a guaranteed logarithmic broadcast time. However, almost no work addresses the issue of *how exactly* the network topology affects the performance of the push model. In other words, we are interested in the structural properties that may have a favourable or a disadvantageous effect on the broadcast time. Resolving such questions is a fundamental issue in network design, and for practical applications, it is important to study the constants that are hidden in the $O(\cdot)$-notation. Unfortunately, many theoretical analyses are rough, so the constants involved are typically huge.

In this context, a precise analysis of the push model was performed by Fountoulakis, Huber and Panagiotou [13], who studied the case where G is an Erdős–Rényi random graph. We will denote by $G(n, p)$ a graph on n vertices that is obtained by including each

possible edge independently with probability p. Among other results, they showed that if the average degree is $\omega(\log n)$, then a.a.s. the broadcast time coincides asymptotically with the broadcast time on the complete graph. So, the performance of the push model remains essentially unaffected by the fact that most edges are missing. Moreover, Fountoulakis and Panagiotou studied in [12] the case where $G(n,d)$ is a random d-regular graph, where $d = O(1)$, and determined the exact effect of d on the broadcast time.

Our results. In this paper we perform a precise analysis of the push protocol on several graphs. Our first result addresses the broadcast time of the push model on *expander graphs*, which have found numerous applications in computer science and mathematics: see the survey [19]. The crucial property of an expander graph is that every set of vertices is connected to the rest of the graph by a large number of edges. Here we focus on a spectral characterization of such graphs, which is related to the spectral gap of their adjacency matrices.

Let G be a connected graph with n vertices that has minimum degree equal to δ and maximum degree equal to Δ. Let $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$ be the eigenvalues of the adjacency matrix of G, and set $\lambda = \max_{2 \leqslant i \leqslant n} |\lambda_i|$. We will say that G is an $(n, \delta, \Delta, \lambda)$-*graph*. Our statements about G should be interpreted in the context of a sequence of graphs indexed by n, where Δ, δ and λ are functions of n. We are interested in asymptotic results as n tends to infinity. Our main result about expander graphs states that the broadcast time of the push model is asymptotically the same as on the complete graph. In other words, expander graphs belong to the same "universality class" with respect to the performance of the push model. Henceforth we will let $T(G)$ denote the (random) broadcast time if the underlying graph is G, and the rumour is placed initially on the vertex with label 1 (or equivalently, the rumour is placed on a vertex chosen uniformly at random).

Theorem 1.1. *Let G be an $(n, \delta, \Delta, \lambda)$-graph, where $\Delta/\delta = 1 + o(1)$ and $\lambda = o(\Delta)$, as $n \to \infty$. Then, a.a.s.*

$$|T(G) - (\log_2 n + \log n)| = o(\log n).$$

Note that the above theorem, together with some well-known facts about random graphs (see [16, 27]), also implies (up to the magnitude of the error term) the main result in [13], where the same bounds on the broadcast time were shown for the special case that $G = G(n,p)$ and $p = \omega(\log n/n)$. Moreover, Theorem 1.1 also applies to random d-regular graphs, where d can be any increasing function of n such that $d = o(\sqrt{n})$, as for this range of d, $\lambda = O(\sqrt{d})$ was shown in Broder, Frieze, Suen and Upfal [4].

We now demonstrate that the two conditions in Theorem 1.1 are best possible in the sense that if we replace any of two $o(.)$ terms in the statement by $O(.)$, then there are graphs that do not satisfy the conclusion. For instance, consider a random d-regular graph with constant d. It trivially satisfies the first condition, but satisfies only $\lambda \leqslant 3\sqrt{d}$ [4]. Since G is a constant-degree, regular graph, it follows by Theorem 1 and Lemma 1 of [9] that $T(G(n,d)) = \log_2 n + \log n + \Omega(\log n)$, a.a.s. Let us now address the condition on Δ/δ. It is well known ([16, 27]; see Lemmas A.1 and 3.2) that a random graph $G(n,p)$ with

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Table 1. Overview of the previous and our new results concerning the push model

Graph	Asymptotic broadcast time	Reference
complete graph	$\log_2 n + \log n$	[15]
$G(n,p)$, $p = \omega(\log n)/n$	$\log_2 n + \log n$	[13]
$G(n,d)$, $d = O(1)$	$\log_{2(1-1/d)} n + \log_{(1-1/d)^{-d}} n$	[12]
d-reg. graph, $\lambda = O(\sqrt{d})$, $d = \omega(\sqrt{n})$	$\log_2 n + \log n$	[12]
hypercube	$O(\log n)$	[11]
$G(n,p)$, $p = c \log n/n, c > 1$	$\log_2 n + \gamma(c) \log n, \gamma(c) > 1$	Theorem 1.2
$G(n,d)$, $d = \omega(1)$	$\log_2 n + \log n$	Theorem 1.1
graph with $\Delta/\delta = 1 + o(1)$, $\lambda = o(\Delta)$	$\log_2 n + \log n$	Theorem 1.1
hypercube	$\log_2 n + \log n + \Omega(\log n)$	Theorem 1.3

$p = (c \log n)/n$ for $c > 1$ satisfies $\lambda = o(\Delta)$ and $\Delta/\delta = \Theta(1)$. However, the next theorem implies that $T(G(n,p)) = \log_2 n + \log n + \Omega(\log n)$ a.a.s.

Theorem 1.2. *Let $c > 1$ be any constant and $p = (c \log n)/n$. Set $\gamma(c) = c \log(c/(c-1)) > 1$. Then, a.a.s.*

$$|T(G(n,p)) - (\log_2 n + \gamma(c) \log n)| = o(\log n).$$

Moreover, this result settles an important question that was left open by the previous results by extending the analysis of the performance of the push model to sparser random graphs with $p = (c \log n)/n$ for a constant $c > 1$ (see [11, 13] and Table 1). In particular, it shows that the broadcast time for a constant $c > 1$ is larger than for $c = \omega(1)$. Moreover, if $c < 1$, then $G(n,p)$ is a.a.s. not connected: see, *e.g.*, [20]. So, a complete broadcast is not possible in this case. Observe that $\gamma(c) \to 1$ when $c \to \infty$, which nicely matches the result of Theorem 1.1. On the other hand, $\gamma(c) \to \infty$ when $c \to 1$.

Our final result addresses the performance of the push model on hypercubes, which constitute popular topologies for the analysis of algorithms in distributed systems. We show that the push model on the hypercube is slower than on the complete graph, but faster than on a random graph $G(n,p)$ with $p = c \log n/n$ where c is sufficiently close to 1. In other words, the regular degree distribution of the hypercube seems to be of more help for rumour spreading than the higher expansion of a random graph. Interestingly, our analysis reveals that on random graphs, the number of informed vertices nearly doubles in each round, as long as their number is $o(n)$. In contrast to that, the growth is significantly smaller on the hypercube for the same range. However, to inform the remaining vertices, the random graph suffers from its heterogeneous structure, that is, there are too many vertices of small degree that are connected to higher-degree vertices.

Theorem 1.3. *Let H_n be a hypercube with n vertices, where n is a power of 2. Then there is a constant $\beta > 0$ such that a.a.s. $T(H_n) \geqslant (1+\beta) \cdot (\log_2 n + \log n)$.*

Our results, together with some earlier bounds, are summarized in Table 1.

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Techniques and methods. One of the most fundamental results in spectral graph theory is the famous *expander mixing lemma*: see [1]. Let G be an n-vertex d-regular graph such that the adjacency matrix has eigenvalues $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$. Then, roughly speaking, the expander mixing lemma guarantees that the number of edges between any two subsets of the vertices is close to what one would expect in a *random* d-regular graph, if $\lambda = \max_{2 \leqslant i \leqslant n} |\lambda_i|$ is not too large. Unfortunately, we cannot apply this lemma directly to support us in the proof of Theorem 1.1, as the relevant graphs are only close to being regular. In order to overcome this limitation, we prove in Section 2 a general statement, which provides similarly sharp bounds for almost regular graphs. Based on this, we perform a tight analysis of the push model by separating the evolution of the set of informed vertices into phases, and controlling the growth in each phase individually.

In Section 3 we prove Theorem 1.2. The proof is based mainly on techniques from the theory of random graphs, which allow us to prove various facts about the degree sequence and the distribution of the edges in certain structures. The most challenging aspect in this proof is that $G(n,p)$, for the range of parameters considered here, is quite far from being a regular graph. This introduces a significant bias in the actual evolution of the set of informed vertices. However, also in this case it is possible to perform a tight analysis of the push model, by using our knowledge of the degree sequence and from the fact that a.a.s. all vertices have the property that most of their neighbours have degree close to average. We hope that similar methods might be useful for studying randomized broadcasting on other classes of random graphs with stronger fluctuations in their degree sequences.

Finally, a further important ingredient in our proofs is a general-purpose technique that we use for obtaining lower bounds for the broadcast time in terms of *random walks*. While the relation between random walks and rumour spreading has been studied before (*e.g.*, [3, 10, 26]), all the obtained relations are of asymptotic nature. Our new approach establishes a direct link between rumour spreading and the transition probabilities of random walks, which is described in more detail in Section 4. Theorem 1.3 is a consequence of this general principle.

Notation. In order to avoid ambiguities we will introduce some notation that will be used throughout the paper. Let $G = (V, E)$ be a graph, v a vertex of G, and U, W two subsets of its vertices. We will write $N_G(v)$ for the set of neighbours of v in G, and $\deg_G(v) = |N_G(v)|$ for its degree. For any vertex set S, let $N(S) = \cup_{v \in S} N(v)$. Moreover, we will write $E_G(U, W)$ for the set of edges with one endpoint in U and one in W, and $e_G(U, W) = |E_G(U, W)|$. We will abbreviate $E_G(U, U) = E_G(U)$. Finally, we will omit the subscript if the graph in question is clear from the context. For any round t, we denote by I_t the set of informed vertices at the end of round t. Similarly, $U_t := V \setminus I_t$ is the set of uninformed vertices. Recall that $\log x$ denotes the logarithm of x to the base e.

2. Rumour spreading on expander graphs

Throughout this section, let $d = 2|E|/n$ be the average degree of G. Our main goal here is to prove Theorem 1.1.

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

2.1. Expansion lemmas

The first ingredient in our proofs addresses the structure of regular graphs. The following statement is a strengthened version of the famous expander mixing lemma, where in comparison to the bound below, the factors $(1-|U|/n)(1-|W|/n)$ do not occur.

Lemma 2.1 ([22, Theorem 2.11]). *Let $G=(V,E)$ be an (n,d,d,λ)-graph. Then for any two subsets $U,W\subseteq V$, we have*

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

Remark. An inspection of the proof of Theorem 2.11 in [22] shows that the statement continues to hold for graphs (possibly with loops) that correspond to adjacency matrices $\mathbf{A}$ where each row sum equals d, but the diagonal elements $A_{i,i}$ can be any non-negative integer, provided that the sets U and W are disjoint.

Let us now turn our attention to non-regular graphs.

Lemma 2.2 ([22]). *Let $G=(V,E)$ be any graph with average degree d and spectral expansion $\lambda<d$. Then, for any subsets $U,W\subseteq V$ we have*

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

We prove the following generalization of Lemma 2.1 to almost regular graphs.

Lemma 2.3. *Let $G=(V,E)$ be an $(n,\delta,\Delta,\lambda)$-graph. Then, for any two disjoint subsets $U,W\subseteq V$, we have*

$$\left|e(U,W)-\frac{\Delta|U||W|}{n}\right|\leqslant(\lambda+(\Delta-\delta))\sqrt{|U||W|\left(1-\frac{|U|}{n}\right)\left(1-\frac{|W|}{n}\right)}.$$

Proof. Define a matrix $\mathbf{B}:=\mathbf{A}+\mathbf{D}$, where $\mathbf{D}$ is the diagonal matrix defined by $\mathbf{D}_{i,i}=\Delta-\deg(i)$, and $\mathbf{A}$ is the adjacency matrix of G. The eigenvalues of $\mathbf{D}$ are $\varepsilon_1\geqslant\varepsilon_2\geqslant\cdots\geqslant\varepsilon_n$. The matrix $\mathbf{B}$ is an integer-valued, symmetric matrix with eigenvalues $\Delta=\beta_1\geqslant\beta_2\geqslant\cdots\geqslant\beta_n$. This allows us to apply Lemma A.2, which yields $\lambda_2\leqslant\beta_2\leqslant\lambda_2+\varepsilon_1$ and $\lambda_n\leqslant\beta_n\leqslant\lambda_n+\varepsilon_1$ (as all eigenvalues of $\mathbf{D}$ are positive). Therefore, with $\beta:=\max_{2\leqslant i\leqslant n}|\beta_i|$, we have

$$\begin{aligned}\beta&=\max\{|\beta_2|,|\beta_n|\}\\&\leqslant\max\{|\lambda_2|+|\beta_2-\lambda_2|,|\lambda_n|+|\beta_n-\lambda_n|\}\\&\leqslant\max\{|\lambda_2|,|\lambda_n|\}+\varepsilon_1\leqslant\lambda+(\Delta-\delta).\end{aligned}$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Since every row (and column) sum of **B** equals Δ, we can apply Lemma 2.1 to the graph induced by the matrix **B** to conclude that

$$\left|e_B(U,W) - \frac{\Delta|U||W|}{n}\right| \leqslant \beta\sqrt{|U||W|\left(1-\frac{|U|}{n}\right)\left(1-\frac{|W|}{n}\right)}$$
$$\leqslant (\lambda + (\Delta-\delta))\sqrt{|U||W|\left(1-\frac{|U|}{n}\right)\left(1-\frac{|W|}{n}\right)}.$$

As U and W are disjoint, we have $e_B(U,W) = e(U,W)$, which proves the claim. □

Corollary 2.4. *Let $G=(V,E)$ be an $(n,\delta,\Delta,\lambda)$-graph satisfying the preconditions of Theorem 1.1. Then, for any subset $U \subseteq V$ of size $1 \leqslant |U| \leqslant n/2$, it holds that*

$$\left|e(U, V\setminus U) - \frac{\Delta|U|(n-|U|)}{n}\right| = o(\Delta)\cdot|U|, \tag{2.1}$$

2.2. Analysis of the algorithm (upper bound)

Lemma 2.5. *Let G be a graph that satisfies the preconditions of Theorem 1.1. Then all the following statements are a.a.s. true.*

(I) *Suppose $1 \leqslant |I_t| \leqslant n/\log n$. Then there exists $\tau = \log_2 n + o(\log n)$ such that $|I_{t+\tau}| > n/\log n$.*

(II) *Suppose $n/\log n \leqslant |I_t| \leqslant n - n/\log n$. Then there exists $\tau = o(\log n)$ such that $|I_{t+\tau}| > n - n/\log n$.*

(III) *Suppose $|I_t| \geqslant n - n/\log n$. Then there exists $\tau = \log n + o(\log n)$ such that $|I_{t+\tau}| = n$.*

Proof. **(I)** $|I_t| \in [1, n/\log n]$. By Corollary 2.4, we know that

$$e(I_t, V\setminus I_t) \geqslant \frac{\Delta|I_t|(n-|I_t|)}{n} - o(\Delta)|I_t| \geqslant \left(1 - \frac{1}{\log n} - o(1)\right)\Delta|I_t|. \tag{2.2}$$

Define

$$\tilde{\lambda} := \frac{\lambda}{d} + \frac{1}{\log n}.$$

Let

$$A = \{v \in N(I_t)\setminus I_t : |N(v)\cap I_t| \geqslant 2d\sqrt{\tilde{\lambda}}\}.$$

Then, by definition of A,

$$e(A, I_t) \geqslant |A|\cdot 2d\sqrt{\tilde{\lambda}}.$$

By Lemma 2.2, we have

$$e(A, I_t) \leqslant \frac{d|A||I_t|}{n} + \lambda\sqrt{|A||I_t|} < \frac{d|A||I_t|}{n} + d\tilde{\lambda}\sqrt{|A||I_t|}.$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Thus

$$|A| \cdot 2d\sqrt{\tilde{\lambda}} < \frac{d|A||I_t|}{n} + d\tilde{\lambda}\sqrt{|A||I_t|} \quad \Longleftrightarrow \quad 2\sqrt{\tilde{\lambda}} - \frac{|I_t|}{n} < \tilde{\lambda}\sqrt{\frac{|I_t|}{|A|}},$$

which implies that

$$\begin{aligned} |A| &< \tilde{\lambda}^2 \cdot |I_t| \cdot \left(\frac{n}{2n\sqrt{\tilde{\lambda}} - |I_t|}\right)^2 \leqslant \tilde{\lambda}^2 \cdot |I_t| \cdot \left(\frac{n}{2n\sqrt{\tilde{\lambda}} - n/\log n}\right)^2 \\ &\leqslant \tilde{\lambda}^2 \cdot |I_t| \cdot \left(\frac{1}{2\sqrt{\tilde{\lambda}} - 1/\log n}\right)^2 < \tilde{\lambda} \cdot |I_t|. \end{aligned}$$

Define $B = (N(I_t) \setminus I_t) \setminus A$. Using (2.2), we can bound $e(I_t, B)$ by

$$\begin{aligned} e(I_t, B) &= e(I_t, V \setminus I_t) - e(I_t, A) \\ &\geqslant (1 - o(1))\Delta|I_t| - \frac{d|A||I_t|}{n} - d\tilde{\lambda}\sqrt{|A||I_t|} \\ &\geqslant (1 - o(1))\Delta|I_t| - d\left(\frac{\lambda}{d} + \frac{1}{\log n}\right)|I_t| \\ &\geqslant (1 - o(1))\Delta|I_t|. \end{aligned}$$

With the above estimate at hand, we compute the expected value of $|I_{t+1} \cap B|$. Note that for any $v \in B$, the probability that it gets informed is at least

$$1 - \prod_{u \in N(v) \cap I_t} \left(1 - \frac{1}{\Delta}\right).$$

We have

$$\mathbb{E}[|I_{t+1} \cap B|] \geqslant \sum_{v \in B} \left[1 - \prod_{u \in N(v) \cap I_t} \left(1 - \frac{1}{\Delta}\right)\right] = \sum_{v \in B} 1 - \left(1 - \frac{1}{\Delta}\right)^{|N(v) \cap I_t|}.$$

Using the inequality that $(1 - x)^n \leqslant 1 - nx + n^2x^2$, we get

$$\begin{aligned} \mathbb{E}[|I_{t+1} \cap B|] &\geqslant \sum_{v \in B} 1 - \left(1 - \frac{|N(v) \cap I_t|}{\Delta} + \frac{|N(v) \cap I_t|^2}{\Delta^2}\right) \\ &= \sum_{v \in B} \frac{|N(v) \cap I_t|}{\Delta}\left(1 - \frac{|N(v) \cap I_t|}{\Delta}\right) \geqslant \left(1 - \frac{2d\sqrt{\tilde{\lambda}}}{\Delta}\right)\frac{e(I_t, B)}{\Delta}. \end{aligned}$$

Since the last expression is at least

$$\left(1 - \frac{2d\sqrt{\tilde{\lambda}}}{\Delta}\right)\frac{e(I_t, B)}{\Delta} \geqslant (1 - o(1))(1 - o(1))|I_t| = (1 - o(1))|I_t|,$$

we obtain

$$\mathbb{E}[|I_{t+1} \setminus I_t|] \geqslant \mathbb{E}[|I_{t+1} \cap B|] \geqslant (1 - o(1))|I_t|.$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Since $|I_{t+1} \setminus I_t| \leqslant |I_t|$, it follows by using Markov's inequality (applied to $|I_t| - |I_{t+1} \setminus I_t|$) that

$$\mathbb{P}[|I_{t+1}| \geqslant (2 - f(n))|I_t|] \geqslant 1 - g(n),$$

where $f(n)$ and $g(n)$ are both functions that tend to zero. Hence the time to reach $|I_t| \geqslant n/\log n$ can be upper-bounded by the sum of $\log_{2-f(n)} n$ independent, identically distributed geometric random variables with expectation at most $1 + o(1)$ each. Using the Chernoff bound from Theorem A.4 yields for $\tau := \log_2 n + o(\log n)$ that $\mathbb{P}[|I_{t+\tau}| > n/\log n] = 1 - o(1)$.

(II) $|I_t| \in [n/\log n, n - n/\log n]$. We further divide this phase into the two cases

$$|I_t| \in [n/\log n, n/2] \quad \text{and} \quad |I_t| \in [n/2, n - n/\log n].$$

We start with the first case, $|I_t| \in [n/\log n, n/2]$. By Lemma 2.3, we have

$$\begin{aligned} e(I_t, V \setminus I_t) &\geqslant \frac{\Delta |I_t||V \setminus I_t|}{n} - (\lambda + \Delta - \delta) \cdot \frac{|I_t||V \setminus I_t|}{n} \\ &\geqslant \frac{1}{2}(\delta - \lambda)|I_t| > \frac{1}{4}\delta |I_t|, \end{aligned}$$

where in the last inequality we used the assumptions that $\lambda = o(\Delta)$ and $\Delta/\delta = 1 + o(1)$. Similar to the analysis of phase (I), we can lower-bound the expected number of vertices that become informed in round $t + 1$:

$$\begin{aligned} \mathbb{E}[|I_{t+1} \setminus I_t|] &\geqslant \sum_{u \in N(I_t) \setminus I_t} \left[1 - \prod_{v \in N(u) \cap I_t} \left(1 - \frac{1}{\Delta}\right)\right] \geqslant \sum_{u \in N(I_t) \setminus I_t} 1 - \mathrm{e}^{-|N(u) \cap I_t|/\Delta} \\ &\geqslant \sum_{u \in N(I_t) \setminus I_t} \frac{|N(u) \cap I_t|}{2\Delta} = \frac{e(I_t, V \setminus I_t)}{2\Delta} \geqslant \frac{\delta}{8\Delta}|I_t|, \end{aligned}$$

where the third inequality used the fact that $\mathrm{e}^{-x} \leqslant 1 - x/2$ for any $x \in (0, 1)$.

Since $|I_{t+1}| \leqslant 2|I_t|$, we obtain as long as $|I_t| \leqslant n/2$ that there are constants $\alpha, \beta > 0$ so that $\mathbb{P}[|I_{t+1}| \geqslant (1 + \alpha)|I_t|] \geqslant \beta$. Hence the time to reach $|I_t| \geqslant n/2$ can be upper-bounded by the sum of $\log_{1+\alpha}(\log n)$ independent, identically distributed geometric random variables with expectation at most $1/\beta$ each. Using a Chernoff bound for the sum of geometric random variables (see Theorem A.4) yields that with probability $1 - o(1)$, we reach $|I_t| \geqslant n/2$ within at most $o(\log n)$ additional rounds.

Consider now the case $|I_t| \in [n/2, n - n/\log n]$. To analyse this case, we examine the shrinking of $U_t := V \setminus I_t$. Again, as $|U_t| \leqslant n/2$, by Lemma 2.3 we have

$$e(U_t, I_t) > \frac{1}{4}\delta |U_t|.$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Let us now compute the expected number of uninformed vertices after one additional round:

$$\mathbb{E}[|U_{t+1}|] = \sum_{u\in U_t} \prod_{v\in N(u)\cap I_t} \left(1-\frac{1}{\deg(v)}\right) \leqslant \sum_{u\in U_t} \mathrm{e}^{-|N(u)\cap I_t|/\Delta}$$
$$\leqslant \sum_{u\in U_t} 1-\frac{|N(u)\cap I_t|}{2\Delta} \leqslant |U_t| - \frac{\delta}{8\Delta}|U_t| = \left(1-\frac{\delta}{8\Delta}\right)|U_t|.$$

A simple inductive argument yields for any integer $\tau \geqslant 1$ that

$$\mathbb{E}[|U_{t+\tau}|] \leqslant \left(1-\frac{\delta}{8\Delta}\right)^{\tau}|U_t|,$$

so for

$$\tau := 2\log\log n/\log\left(1/\left(1-\frac{\delta}{8\Delta}\right)\right) = o(\log n)$$

we have

$$\mathbb{E}[|U_{t+\tau}|] \leqslant |U_t|/\log^2 n = o(n/\log n).$$

Hence, by Markov's inequality, $\mathbb{P}[|U_{t+\tau}| \geqslant n/\log n] = o(1)$.

(III) $|I_t| \in [n - n/\log n, n]$. Again, we analyse the shrinking of the set U_t. Recall from (2.2) that $e(I_t, U_t) \geqslant (1-f(n))\cdot\Delta\cdot|U_t|$, where $f(n)$ is any function with $f(n) = o(1)$. Let $A \subseteq U_t$ be the set of vertices $v \in U_t$ for which $|N(v)\cap I_t| \leqslant (1-\sqrt{f(n)}/2)\cdot\Delta$. We assume for a contradiction that $|A| > 2\sqrt{f(n)}\cdot|U_t|$ and conclude

$$\begin{aligned} e(I_t, U_t) &= \sum_{v\in A}|N(v)\cap I_t| + \sum_{v\in U_t\setminus A}|N(v)\cap I_t| \\ &\leqslant |A|\cdot(1-\sqrt{f(n)}/2)\cdot\Delta + |U_t\setminus A|\cdot\Delta \\ &= |U_t|\cdot\Delta - |A|\cdot\sqrt{f(n)}\cdot\Delta/2 \\ &< (1-f(n))\cdot\Delta\cdot|U_t|, \end{aligned}$$

which yields the desired contradiction. Now define $B := U_t \setminus A$ so that for each $u \in B$,

$$|N(v)\cap I_t| > (1-\sqrt{f(n)}/2)\cdot\Delta \quad \text{and} \quad |B| \geqslant (1-2\sqrt{f(n)})\cdot|U_t|.$$

Using linearity of expectations,

$$\mathbb{E}[|U_{t+1}|] \leqslant \sum_{v\in B}\mathbb{P}[v\notin I_{t+1}] + \sum_{v\in A}\mathbb{P}[v\notin I_{t+1}]$$
$$\leqslant \sum_{v\in B}\left(1-\frac{1}{\Delta}\right)^{|N(v)\cap I_t|} + \sum_{v\in A}1$$

Using the inequality $(1-1/\Delta) \leqslant \mathrm{e}^{-1/\Delta}$, we get

$$\mathbb{E}[|U_{t+1}|] \leqslant \sum_{v\in B}\mathrm{e}^{-|N(v)\cap I_t|/\Delta} + |A|$$
$$< \left(\mathrm{e}^{-1}\cdot\mathrm{e}^{\sqrt{f(n)}/2}\right)\cdot|B| + 2\sqrt{f(n)}\cdot|U_t|$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

$$\leqslant \left(\mathrm{e}^{-1} \cdot \left(1 + \mathrm{e}\sqrt{f(n)}/2\right)\right) \cdot |B| + 2\sqrt{f(n)} \cdot |U_t|$$
$$\leqslant \left(\mathrm{e}^{-1} + 3\sqrt{f(n)}\right) \cdot |U_t|,$$

where the third inequality used the fact that $\mathrm{e}^x \leqslant 1 + \mathrm{e} \cdot x$ for any $x \in [0, 1]$. By induction, it follows that for any round $\tau > t$,

$$\mathbb{E}[|U_\tau|] \leqslant \left(\mathrm{e}^{-1} + 3\sqrt{f(n)}\right)^{\tau - t} \cdot |U_t|.$$

We choose

$$\tau := t + \log_{\mathrm{e}^{-1} + 3\sqrt{f(n)}}(n) = t + \log n + o(\log n)$$

and obtain that

$$\mathbb{E}[|U_{t+\tau}|] \leqslant \frac{1}{n} \cdot |U_t|.$$

Since by assumption $|U_t| \leqslant n/\log n$, this implies $\mathbb{E}[|U_{t+\tau}|] \leqslant 1/\log n$, so that

$$\mathbb{P}[|U_{t+\tau}| \geqslant 1] \leqslant \mathbb{E}[|U_{t+\tau}|] \leqslant 1/\log n. \qquad \square$$

2.3. Analysis of the algorithm (lower bound)

We first note that if the graph G is regular, then the lower bound follows directly from Theorem 1 and Lemma 1 of [9]. If the graph G is not regular, then it must hold that $\delta = \omega(1)$. For the proof of the lower bound, observe that after $t := \log_2 n - 1$ rounds we have $|I_t| \leqslant n/2$. For a lower bound on the running time of the algorithm, we may assume that each vertex $u \in U_t$ may get the rumour from any of its neighbours at any time. So we can forget about who actually knows the rumour but consider the model in which at each round each vertex in V picks a neighbour. We want a lower bound on the probability that some vertex in U_t never gets selected in

$$\tau := (\log n - h(n)) \cdot \frac{\delta - 3/4}{\Delta} = \log n - o(\log n)$$

rounds, where $h(n)$ is any slow growing function satisfying $h(n) = o(\log n)$ and $h(n) = \omega(1)$. For each $u \in U_t$, let E_u denote the event that u is never selected within those rounds. We compute

$$\mathbb{P}[E_u] = \prod_{v \in N(u)} \left(1 - \frac{1}{|N(v)|}\right)^{\tau} \geqslant \left(1 - \frac{1}{\delta}\right)^{\Delta\tau} \geqslant \mathrm{e}^{\Delta\tau/(\delta - 3/4)} = \mathrm{e}^{-\log n + \omega(1)},$$

where we used the fact that $(1 - 1/x)^{x - 3/4} \geqslant \mathrm{e}^{-1}$ for any $x \geqslant 2$. Summing over all vertices in U_t, we obtain

$$\sum_{u \in U_t} \mathbb{P}[E_u] \geqslant n/2 \cdot \mathrm{e}^{-\log n + \omega(1)} \to \infty.$$

By construction, the events $\{\overline{E_u} : u \in U_t\}$ are negatively correlated in the sense that, for any set of different vertices $u, u_1, \cdots, u_k \in U_t$, we have that $\mathbb{P}[\overline{E_u} \mid \overline{E_{u_1}} \wedge \cdots \wedge \overline{E_{u_k}}] \leqslant \mathbb{P}[\overline{E_u}]$.

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Therefore,

$$\mathbb{P}\left[\bigwedge_{u\in U_t}\overline{E_u}\right] \leqslant \prod_{u\in U_t}\mathbb{P}[\overline{E_u}] \leqslant \mathrm{e}^{-\sum_{u\in U_t}\mathbb{P}[E_u]} = o(1).$$

To conclude, we have shown that $\mathbb{P}[T(G) \geqslant \log_2 n + \log n - o(\log n)] \geqslant 1 - o(1)$. This lower bound together with the upper bound obtained in Lemma 2.5 immediately yields Theorem 1.1.

3. Rumour spreading on $G(n,p)$

In this section we analyse the push protocol on the classical Erdős–Rényi random graphs, and prove Theorem 1.2. We let $G(n,p)$ denote the random graph on vertex set $V = \{1,\dots,n\}$ where each edge is selected independently with probability p. Throughout this section, we will write $f(n) \sim g(n)$ if $\lim_{n\to\infty} f(n)/g(n) = 1$.

3.1. Properties of $G(n,p)$

In this subsection we collect some basic facts about $G(n,p)$, which will be useful in the forthcoming proofs. We begin by computing tight bounds for the degree sequence of $G(n,p)$, where $p = \Theta(\log n/n)$. The next two lemmas provide us with the required information.

Lemma 3.1. *Let $x_1 > x_0 > 0$ and $c > 1$ be constants, and let $p \sim c\log n/n$. Fix $V' \subseteq V$ with $|V'| = n - o(n)$ (where $V' = V$ is allowed). Let N_i be the number of vertices in V' with degree i in $G(n,p)$. Then, uniformly for all $i \in [x_0\log n, x_1\log n]$ we have that $\mathbb{E}[N_i] = n^{g(i/\log n)\pm o(1)}$, where $g(x) = x(1+\log(c/x)) - c + 1$. Moreover, the variance satisfies*

$$\mathbb{V}[N_i] \leqslant o(\mathbb{E}[N_i]^2) + \mathbb{E}[N_i].$$

Proof. The degree $\deg(v)$ of any given vertex $v \in V'$ is distributed as $\mathrm{Bin}(n-1,p)$. Then, Stirling's formula implies that

$$\begin{aligned}\mathbb{E}[N_i] &= |V'|\mathbb{P}[\deg(v) = i]\\ &= (n - o(n))\binom{n-1}{i}p^i(1-p)^{n-1-i}\\ &= n^{1-o(1)}\left(\frac{\mathrm{e}n}{i}\right)^i p^i(1-p)^{n-1-i}.\end{aligned}$$

Hence, writing $x = i/\log n$, we get

$$\mathbb{E}[N_i] = n^{1-o(1)}\left(\frac{\mathrm{e}c \pm o(1)}{x}\right)^i \mathrm{e}^{-pn\pm o(1)} = n^{\log((\mathrm{e}c/x)^x)-c+1\pm o(1)} = n^{g(x)\pm o(1)}.$$

Next, we estimate the probability that two different vertices v and w in V' have the same degree i. To compute that, we take into account whether or not v and w share a common edge, which occurs with probability p, and then rearrange the expression obtained in

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

terms of $\mathbb{P}[\deg(v) = i]$:

$$\begin{aligned}
&\mathbb{P}[\deg(v) = i \cap \deg(w) = i] \\
&\quad = p\binom{n-2}{i-1}^2 p^{2i-2}(1-p)^{2n-2-2i} + (1-p)\binom{n-2}{i}^2 p^{2i}(1-p)^{2n-4-2i} \\
&\quad = \left(\frac{i^2}{p(n-1)^2} + \frac{(n-1-i)^2}{(1-p)(n-1)^2}\right)(\mathbb{P}[\deg(v) = i])^2 \sim (\mathbb{P}[\deg(v) = i])^2.
\end{aligned}$$

Finally, we have

$$\begin{aligned}
\mathbb{V}[N_i] &= |V'|\mathbb{P}[\deg(v) = i] + |V'|(|V'| - 1)\mathbb{P}[\deg(v) = i \cap \deg(w) = i] - \mathbb{E}[N_i]^2 \\
&= \mathbb{E}[N_i] + (1 \pm o(1))\mathbb{E}[N_i]^2 - \mathbb{E}[N_i]^2 \\
&\leqslant o(\mathbb{E}[N_i]^2) + \mathbb{E}[N_i].
\end{aligned}$$

□

Lemma 3.2. *Let $c > 1$ be any constant and $p = c\log n/n$. Let δ and Δ be the minimum and maximum degrees of $G(n,p)$. Then there exist constants c_0, c_1 with $0 < c_0 < c - 1 < c < c_1$ such that a.a.s.*

$$(1 - o(1))c_0 \log n \leqslant \delta \leqslant \Delta \leqslant (1 + o(1))c_1 \log n.$$

Proof. Define

$$c_0 = -\frac{c-1}{W_0(-\mathrm{e}^{-1}(c-1)/c)} \quad \text{and} \quad c_1 = -\frac{c-1}{W_1(-\mathrm{e}^{-1}(c-1)/c)},$$

where W_0 and W_1 are respectively the lower and upper branch of the Lambert W function on $[-\mathrm{e}^{-1}, 0]$ (recall that each branch of the Lambert W function satisfies $W(y)\mathrm{e}^{W(y)} = y$). Let $g(x)$ be defined as in the statement of Lemma 3.1. By direct substitution and easy computations, we can check that $g(c_0) = g(c_1) = 0$, $g(c-1) > 0$ and $g(c) > 0$. Moreover, by looking at the derivative $g'(x) = \log(c/x)$ we see that $g(x)$ is increasing in $(0, c)$ and decreasing in (c, ∞). Thus we can conclude that the only positive solutions of $g(x) = 0$ are precisely $x = c_0$ and $x = c_1$, and moreover $0 < c_0 < c - 1 < c < c_1$.

Given any constant $\varepsilon > 0$, for each vertex v we have

$$\begin{aligned}
\mathbb{P}[\deg(v) \leqslant (c_0 - \varepsilon)\log n] &= \sum_{j=0}^{\lfloor (c_0-\varepsilon)\log n \rfloor} \binom{n-1}{j} p^j (1-p)^{n-1-j} \\
&= O(\mathbb{P}[\deg(v) = \lfloor (c_0 - \varepsilon)\log n \rfloor]),
\end{aligned}$$

since the ratio between any two consecutive terms in the above sum is at most $c_0/c < 1$. Similarly,

$$\begin{aligned}
\mathbb{P}[\deg(v) \geqslant (c_1 + \varepsilon)\log n] &= \sum_{j=\lceil (c_1+\varepsilon)\log n \rceil}^{n-1} \binom{n-1}{j} p^j (1-p)^{n-1-j} \\
&= O(\mathbb{P}[\deg(v) = \lceil (c_1 + \varepsilon)\log n \rceil]),
\end{aligned}$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

since the corresponding ratio is at least $c_1/c > 1$. In view of these facts and by Lemma 3.1, the expected number of vertices of degree at most $(c_0 - \varepsilon)\log n$ is

$$O\big(n \cdot \mathbb{P}[\deg(v) = \lfloor (c_0 - \varepsilon)\log n \rfloor]\big) = n^{g(c_0-\varepsilon)\pm o(1)} = o(1),$$

since $g(c_0 - \varepsilon) < 0$. A totally analogous argument shows that the expected number of vertices of degree at least $(c_1 + \varepsilon)\log n$ is $o(1)$. Since the choice of ε was arbitrary, we conclude that the required bounds on δ and Δ hold a.a.s. □

We will also use the following property of $G(n,p)$, which essentially says that the neighbourhood of all vertices contains many vertices with actual degree close to the expected degree.

Lemma 3.3. *Let $c > 1$ be any constant and $p = c\log n/n$. For each vertex u in $G(n,p)$, define*

$$\tilde{N}(u) = \{v \in N(u) : |\,|N(v)| - pn\,| \leqslant \log^{3/4} n\}. \tag{3.1}$$

Then, a.a.s. for every vertex u we have $|N(u) \setminus \tilde{N}(u)| \leqslant \log^{3/4} n$.

Proof. In view of Lemma 3.2, there is a constant $x_1 > c$ such that a.a.s. $\Delta \leqslant x_1 \log n$. We call this event E, and restrict our analysis to that case. Let us fix a vertex $u \in V$. Put $N = N(u)$ and $N' = N(u) \setminus \tilde{N}(u)$. To prove the lemma, it suffices to show that $\mathbb{P}\big[(|N'| > \log^{3/4} n) \cap E\big] = o(1/n)$, and then apply a union bound over all the vertices $u \in V$.

First, we expose the neighbours of u, and condition upon the particular N obtained. We use a subscript star to denote probabilities in the conditional space. We assume that $|N| \leqslant x_1 \log n$ (as implied by event E). Then we expose all internal edges in N, and let X be the number of them. Since there are at most $|N|^4 \leqslant (x_1 \log n)^4$ possible pairs of internal edges, we have that

$$\mathbb{P}_*[X \geqslant 2] \leqslant (x_1 \log n)^4 p^2 = n^{-2+o(1)}. \tag{3.2}$$

Next we expose the edge set $E(N, V_0)$, where $V_0 = V \setminus (N \cup \{u\})$. For each $v \in N$, consider the number $X_v = |N(v) \cap V_0|$ of neighbours of v which lie in V_0. Note that each X_v is distributed as $\mathrm{Bin}(|V_0|, p)$, so a version of the Chernoff bounds (see, *e.g.*, Alon and Spencer [2, Theorems A.1.11 and A.1.13]) yields

$$\mathbb{P}_*\big[|X_v - pn| > \log^{3/4} n - 2\big] = \mathrm{e}^{-\Omega(\log^{1/2} n)}.$$

Let B be the event that there are more than $\log^{3/4} n$ vertices $v \in N$ for which $|X_v - pn| > \log^{3/4} n - 2$ holds. Note that by definition, the random variables $\{X_v : v \in N(u)\}$ are mutually independent. Hence,

$$\mathbb{P}_*[B] \leqslant |N| \binom{|N|}{\lceil \log^{3/4} n \rceil} \exp\big(-\Omega(\log^{1/2} n)\lceil \log^{3/4} n \rceil\big) = \mathrm{e}^{-\Omega(\log^{5/4} n)}. \tag{3.3}$$

Since the bounds in (3.2) and (3.3) hold uniformly for all N satisfying $|N| \leqslant x_1 \log n$, we deduce that

$$\mathbb{P}\big[((X \geqslant 2) \cup B) \cap (|N| \leqslant x_1 \log n)\big] \leqslant n^{-2+o(1)} = o(1/n).$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Note that if $X < 2$ then $X_v \leqslant \deg(v) \leqslant X_v + 1$ for each $v \in N$. We conclude the proof by observing that the event $(|N'| > \log^{3/4} n) \cap E$ implies $((X \geqslant 2) \cup B) \cap (|N| \leqslant x_1 \log n)$ by construction, and thus we get the desired bound $\mathbb{P}\big[(|N'| > \log^{3/4} n) \cap E\big] = o(1/n)$. □

The lemma below bounds the number of edges contained in small subsets of the vertices. The first statement follows immediately from Lemma 5.3 in [7], while the second statement is from [6, Property 3].

Lemma 3.4. *Let $c > 1$ be any constant and $p = c \log n/n$. A.a.s. for every subset $S \subseteq V$ of $G(n,p)$ of size $|S| = O(n/\log n)$ we have that $e(S) = o(|S| \log n)$. Moreover, for any set S with $1 \leqslant |S| \leqslant n/2$, $e(S, V \setminus S) = \Omega(|S|np)$.*

Finally, we include a lemma that addresses the typical structure of the neighbourhoods of small sets.

Lemma 3.5. *Let $c > 1$ be any constant and $p = c \log n/n$. There is a function $f(n) = o(1)$ such that the following is a.a.s. true. For every set S of vertices of $G(n,p)$ such that $|S| \leqslant n/\log n$, there are at most $f(n)|S|$ vertices outside of S that have more than $f(n) \log n$ neighbours in S.*

Proof. We will show the claim for $f(n) = (\log\log n)^{-1/3}$. Let H be a fixed subset of the vertex set of $G(n,p)$, and let $v \in V \setminus H$. Then, if $|H| \leqslant n/\log n$,

$$\begin{aligned}\mathbb{P}[|N(v) \cap H| \geqslant f(n)\log n] &\leqslant \binom{|H|}{\lceil f(n)\log n\rceil} p^{\lceil f(n)\log n\rceil} \\ &\leqslant \left(\frac{\mathrm{e}n}{f(n)\log^2 n} \cdot \frac{c\log n}{n}\right)^{\lceil f(n)\log n\rceil} = n^{-\Omega((\log\log n)^{2/3})}.\end{aligned}$$

Hence, the probability that there are at least $f(n)s$ vertices v in $V \setminus H$ with $|N(v) \cap H| \geqslant f(n)\log n$ (*i.e.*, set H contradicts the claim in the statement) is at most

$$n^{f(n)s} \cdot n^{-\Omega((\log\log n)^{2/3}) \cdot f(n)s} = n^{-\Omega((\log\log n)^{2/3}) \cdot f(n)s}.$$

By linearity of expectation, the expected number of subsets of $G(n,p)$ with $1 \leqslant s \leqslant n/\log n$ vertices having the property above is at most

$$n^s n^{-\Omega((\log\log n)^{2/3}) \cdot f(n)s} = o(1/n),$$

and the proof is completed by summing for all s and applying Markov's inequality. □

3.2. Analysis of the algorithm

We first analyse the evolution of I_t as long as $1 \leqslant |I_t| \leqslant n - n/\log^2 n$. The following lemma proves that as long as $|I_t|$ is not too large, $|I_t|$ almost doubles in each round.

Lemma 3.6. *Let $c > 1$ be any constant and set $p = c \log n/n$. Then there is some $t = \log_2 n + o(\log n)$ such that we have a.a.s. that $|I_t| \geqslant n - n/\log^2 n$.*

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Proof. Before we proceed with the actual proof, let us recall some basic properties of $G(n,p)$. First, by applying Lemma 3.2 we infer that there are constants $0 < c_0 < c_1$ such that a.a.s. the minimum degree δ of $G_{n,p}$ satisfies $\delta = (1-o(1))c_0 \log n$ and the maximum degree satisfies $\Delta = (1+o(1))c_1 \log n$. Moreover, let $f(n) = o(1)$ be the function guaranteed to exist by Lemma 3.5. Set

$$A := \{v \in N(I_t) \setminus I_t : |N(v) \cap I_t| \geqslant f(n) \log n\}.$$

Then, a.a.s. we may assume that $|A| \leqslant f(n)|I_t|$.

Let us first consider the case where $1 \leqslant |I_t| \leqslant n/\log n$. By applying Lemma 3.4 we infer that a.a.s. the set I_t spans $o(|I_t| \log n)$ edges, that is, $e(I_t) = o(|I_t| \log n)$. From now on we will assume that $G(n,p)$ has all these properties without further reference.

Let $B := (N(I_t) \setminus I_t) \setminus A$. Define for any vertex $u \in I_t$ an indicator random variable X_u, which is one if u sends the rumour to a vertex $v \in B$ and no other vertex sends a rumour to v. We have

$$\begin{aligned}\mathbb{P}[X_u = 1] &= \sum_{v \in B} \mathbb{P}[u \text{ is the only vertex that informs } v] \\ &\geqslant \sum_{v \in B \cap N(u)} \frac{1}{\deg(u)} \cdot \left(1 - \frac{1}{\delta}\right)^{f(n)\log n} = (1-o(1))\frac{|N(u) \cap B|}{\deg(u)}.\end{aligned}$$

Let $X := \sum_{u \in I_t} X_u$. By linearity of expectation,

$$\begin{aligned}\mathbb{E}[X] &= \sum_{u \in I_t} \mathbb{E}[X_u] \geqslant (1-o(1)) \cdot \sum_{u \in I_t} \frac{\deg(u) - |N(u) \cap I_t| - |N(u) \cap A|}{\deg(u)} \\ &\geqslant (1-o(1))\left(|I_t| - \frac{1}{\delta}\sum_{u \in I_t} |N(u) \cap I_t| - \frac{1}{\delta}\sum_{u \in I_t} |N(u) \cap A|\right).\end{aligned}$$

Note that $\sum_{u \in I_t} |N(u) \cap I_t| = 2e(I_t) = o(|I_t| \log n)$. Moreover, a simple double-counting argument implies $\sum_{u \in I_t} |N(u) \cap A| \leqslant |A|\Delta$. As $|A| \leqslant f(n)|I_t|$ and $\delta, \Delta = \Theta(\log n)$ we infer that $\mathbb{E}[X] \geqslant (1-o(1))|I_t|$, and we infer that $\mathbb{E}[|I_{t+1}| \mid |I_t| \leqslant n/\log n] \geqslant (2-o(1)) \cdot |I_t|$. As in Lemma 2.5, we can prove that for $t = \log_2 n + o(\log n)$ a.a.s. $|I_t| \geqslant n/\log n$.

Now consider the case where $n/\log n \leqslant |I_t| \leqslant n - n/\log^2 n$. We can do exactly the same analysis as in Lemma 2.5 and use the fact that the ratio Δ/δ is a constant. Here, the second statement of Lemma 3.4 provides a sufficiently large lower bound on the expansion. Therefore, after $\tau := O(\log \log n)$ additional rounds a.a.s. $|I_{t+\tau}| \geqslant n - n/\log^2 n$. □

The next proposition analyses the last stages of the rumour spreading algorithm when $|I_t|$ is large. Its conclusion, combined with Lemma 3.6, provides us with an upper bound on the broadcast time for $G(n,p)$.

Proposition 3.7 (upper bound). *Let $\varepsilon > 0$, $c > 1$ be any constants, and $p = c \log n/n$. Let t be such that $|I_t| \geqslant n - n/\log^2 n$. Then, all the remaining vertices will a.a.s. get informed within additional $\lceil(\gamma + \varepsilon)\log n\rceil$ rounds, where*

$$\gamma = \gamma(c) = c \log\left(\frac{c}{c-1}\right).$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Proof. Recall from Lemma 3.2 that there exist constants $x_1 > x_0 > 0$ such that a.a.s. $x_0 \log n < \delta \leqslant \Delta < x_1 \log n$. Call this event E_1. Let V_i denote the set of vertices of degree i. By Markov's inequality, the event $|V_i| \geqslant \log^2 n\, \mathbb{E}[|V_i|]$ has probability at most $1/\log^2 n$. Therefore, we can apply a union bound and also Lemma 3.1 to deduce that a.a.s. all degrees $i \in [x_0 \log n, x_1 \log n]$ satisfy $|V_i| < \log^2 n\, \mathbb{E}[|V_i|] \leqslant n^{g(i/\log n)+o(1)}$. Call this event E_2. Let E_3 be the event that $|N(u) \setminus \tilde{N}(u)| \leqslant \log^{3/4} n$ for every vertex u, where $\tilde{N}(u)$ is defined as in (3.1). By Lemma 3.3, E_3 holds a.a.s.

Let us write $I = I_t$ and $U = U_t$ for simplicity, and note that the internal edges of U were not exposed during the rumour spreading, so each one still occurs independently with probability p. For any vertex u in U, using the inequality $\binom{m}{k} \leqslant (em/k)^k$, we obtain

$$\mathbb{P}\left[|N(u) \cap U| \geqslant \frac{\log n}{\log\log n}\right] \leqslant \binom{|U|}{\lceil \frac{\log n}{\log\log n} \rceil} p^{\lceil \frac{\log n}{\log\log n} \rceil} \leqslant \left(\frac{ec \log\log n}{\log^2 n}\right)^{\frac{\log n}{\log\log n}} \leqslant n^{-2+o(1)}.$$

Thus taking the union bound over all vertices in U, we obtain that a.a.s. each vertex in U has at most $\log n/\log\log n$ neighbours in U. Call this event E_4.

Henceforth, assume that E_1, E_2, E_3 and E_4 hold together. We can partition U into the sets $U_i = U \cap V_i$, for $i \in [x_0 \log n, x_1 \log n]$, which must satisfy $|U_i| \leqslant |V_i| \leqslant n^{g(i/\log n)+o(1)}$ (since E_1 and E_2 hold). Pick an i in that range and a vertex $u \in U_i$. Set $x = i/\log n$. Define $N_1 = \tilde{N}(u) \cap I$ and $N_2 = (N(u) \setminus \tilde{N}(u)) \cap I$, and observe that events E_3 and E_4 imply $|N_1| \sim i = x \log n$ and $|N_2| = o(\log n)$. We can upper-bound the probability that u does not receive the rumour in $\lceil (\gamma + \varepsilon) \log n \rceil$ rounds from any vertex in I by

$$\prod_{v \in N(u) \cap I} \left(1 - \frac{1}{|N(v)|}\right)^{\lceil (\gamma+\varepsilon)\log n \rceil} \leqslant \prod_{v \in N_1} \mathrm{e}^{-\frac{(\gamma+\varepsilon)\log n}{|N(v)|}} \prod_{v \in N_2} \mathrm{e}^{-\frac{(\gamma+\varepsilon)\log n}{|N(v)|}} \leqslant n^{-(\gamma+\varepsilon)x/c+o(1)},$$

and therefore the expected number of vertices in U_i not being informed in that time is at most $n^{g(x)-(\gamma+\varepsilon)x/c+o(1)}$. Standard analysis shows that the function $cg(x)/x$ maximizes at $x = c - 1$ and takes the value γ. Therefore, $g(x) \leqslant \gamma x/c$, and the expectation above is at most

$$n^{-\varepsilon x/c+o(1)} \leqslant n^{-\varepsilon x_0/c+o(1)}.$$

Hence taking a union bound over all degrees $i \in [x_0 \log n, x_1 \log n]$, we obtain that a.a.s. all vertices get informed. □

Finally, we bound from below the time it takes to inform the last uninformed vertices of the graph, when $|I_t|$ is not too large. This will be used to obtain a lower bound on the broadcast time for $G(n, p)$.

Proposition 3.8 (lower bound). *Let $c > 1$ and $p = c \log n/n$. Let us assume that t is such that $|I_t| \leqslant n/\log^2 n$. Then, given any $\varepsilon > 0$, a.a.s. after $\lceil (\gamma - \varepsilon) \log n \rceil$ rounds there are still some uninformed vertices in $G(n, p)$, where*

$$\gamma = \gamma(c) = c \log\left(\frac{c}{c-1}\right).$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

Proof. Let us write $I = I_t$ for brevity. In view of Lemma 3.2, we assume that all vertices in I have degree at most $x_1 \log n$, for some constant $x_1 > c$, and in particular $|N(I)| \leqslant x_1 n/\log n$. We define $U = V \setminus I$ and $U' = U \setminus N(I)$, which must satisfy $|U| \geqslant n - n/\log^2 n$ and $|U'| \geqslant n - x_1 n/\log n$. Moreover, observe that the internal edges of U have not been exposed yet by the rumour spreading algorithm.

Let $i = \lceil (c-1)\log n \rceil$, and let U_i be the set of vertices in U' with exactly i neighbours. We wish to estimate the size of U_i. Since there are no crossing edges between U' and I, henceforth we confine our attention only to $G(n,p)$ restricted to U, which can be regarded as $G(|U|,p)$. We apply Lemma 3.1 to $G(|U|,p)$ and to the subset U', and infer that

$$\mathbb{E}[|U_i|] \geqslant n^{g(c-1)-o(1)} \to \infty \quad \text{and} \quad \sqrt{\mathbb{V}[|U_i|]} = o(\mathbb{E}[|U_i|]),$$

so as a consequence of Chebyshev's inequality we deduce that a.a.s. $|U_i| \geqslant n^{g(c-1)-o(1)}$.

Summarizing, we obtained a.a.s. a set U_i of at least $n^{g(c-1)-o(1)}$ uninformed vertices with degree i. In view of Lemma 3.3, for every vertex $u \in U_i$ we have $|N(u) \setminus \tilde{N}(u)| \leqslant \log^{3/4} n$, where $\tilde{N}(u)$ is defined as in (3.1). We may assume for our lower bound on the running time of the algorithm that each vertex $u \in U_i$ may get the rumour from any of its neighbours at any time. So we can forget about who actually knows the rumour at a given time but consider the model in which in each round each vertex in U picks a neighbour. We want a lower bound on the probability that some vertex in U_i never gets selected in $\lceil (\gamma - \varepsilon)\log n \rceil$ rounds. For each $u \in U_i$ let E_u denote the event that u is never selected within those rounds. We compute

$$\begin{aligned}\mathbb{P}[E_u] &= \prod_{v \in N(u)} \left(1 - \frac{1}{|N(v)|}\right)^{\lceil (\gamma-\varepsilon)\log n \rceil} \geqslant \prod_{v \in N(u)} \mathrm{e}^{-\frac{(\gamma-\varepsilon)\log n}{|N(v)|} - o(1)} \\ &= \prod_{v \in \tilde{N}(u)} \mathrm{e}^{-\frac{(\gamma-\varepsilon)\log n}{|N(v)|} - o(1)} \prod_{v \in N(u) \setminus \tilde{N}(u)} \mathrm{e}^{-\frac{(\gamma-\varepsilon)\log n}{|N(v)|} - o(1)} \geqslant n^{-(\gamma-\varepsilon)(c-1)/c - o(1)},\end{aligned}$$

and summing over all vertices in U_i,

$$\sum_{u \in U_i} \mathbb{P}[E_u] \geqslant n^{g(c-1)-(\gamma-\varepsilon)(c-1)/c-o(1)} = n^{\varepsilon(c-1)/c-o(1)} \to \infty.$$

As in Section 2.3, we arrive at

$$\mathbb{P}\left[\bigwedge_{u \in U_i} \overline{E_u}\right] \leqslant \prod_{u \in U_i} \mathbb{P}[\overline{E_u}] \leqslant \mathrm{e}^{-\sum_{u \in U_i} \mathbb{P}[E_u]} = o(1),$$

and in particular we will a.a.s. have some uninformed vertices after $\lceil (\gamma - \varepsilon)\log n \rceil$ rounds. □

At this stage, we have all the ingredients we need to prove Theorem 1.2. The upper bound on $T(G(n,p))$ follows immediately from Lemma 3.6 and Proposition 3.7. For the lower bound, we simply observe that after $t = \lfloor \log_2(n/\log^2 n) \rfloor = \log_2 n - o(\log n)$ rounds we still have $|I_t| \leqslant n/\log^2 n$, and combine this fact with Proposition 3.8.

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

4. Lower-bounding rumour spreading time by random walks

In this section, we develop a new technique for lower-bounding the rumour spreading time in terms of random walk matrices. We consider (lazy) random walks on G based on the transition matrix $\mathbf{P} := \frac{1}{2} \cdot (\mathbf{I} + \mathbf{D}^{-1}\mathbf{A})$, where $\mathbf{D}$ is the $(n \times n)$-diagonal matrix with $\deg(u)$ at entry (u,u). Note that in each step, the random walk stays at the current vertex with probability $1/2$ and otherwise moves to a neighbour chosen uniformly at random.

We first derive a general lemma that relates the probability of informing a vertex to the corresponding entry of the transition matrix $\mathbf{P}$. Then we apply this lemma to the hypercube and show that after $\log_2 n$ rounds, less than $5n^{0.9} \log n$ nodes are informed. Once we have established this, the lower bound of $\log_2 n + \log n + \Omega(\log n)$ is almost immediate.

Lemma 4.1. *For any round t and any pair of vertices u, v, we have*

$$\mathbb{P}[v \in I_t \mid I_0 = \{u\}] \leqslant 2^t \cdot \mathbf{P}^t_{u,v}.$$

Proof. Consider the matrix $\mathbf{M} := \mathbf{I} + \mathbf{D}^{-1}\mathbf{A}$. Clearly, $\mathbf{M} = 2 \cdot \mathbf{P}$. Fix a vertex $u \in V$, which originates the rumour. We now prove the statement by induction on t. To this end, let p^0 be the unit-vector with $p^0_u = 1$ and $p^0_v = 0$ for any $v \neq u$. Define $p^t := p^{t-1} \cdot \mathbf{M}$. Clearly, $p^t = p^0 \mathbf{M}^t$, and for any vertex v,

$$p^t_v = \sum_{w \in V} p^0_w \cdot \mathbf{M}^t_{w,v} = \mathbf{M}^t_{u,v}.$$

Hence it suffices to prove that for any step t, $\mathbb{P}[v \in I_t \mid I_0 = \{u\}] \leqslant p^t_v$. This holds for $t = 0$ by definition. For the induction step,

$$\begin{aligned}
&\mathbb{P}[v \in I_{t+1} \mid I_0 = \{u\}] \\
&\quad \leqslant \sum_{w \in N(v)} \mathbb{P}[w \text{ sends rumour to } v \text{ in round } t+1 \mid I_0 = \{u\}] + \mathbb{P}[v \in I_t \mid I_0 = \{u\}] \\
&\quad \leqslant \sum_{w \in N(v)} \mathbb{P}[w \in I_t \mid I_0 = \{u\}] \cdot \frac{1}{\deg(w)} + p^t_v \\
&\quad \leqslant \sum_{w \in N(v)} p^t_w \cdot \frac{1}{\deg(w)} + p^t_v = [p^t \cdot \mathbf{M}]_v = p^{t+1}_v,
\end{aligned}$$

where the last two inequalities hold due to the induction hypothesis. □

We now use the above lemma to prove Theorem 1.3.

Proof of Theorem 1.3. Assume that the rumour starts at the vertex $0 = (0)^d$, where $d := \log_2 n$. Our aim is to use Lemma 4.1, so we have to analyse $\mathbf{P}^t_{u,v}$. Recall that a random walk according to the matrix $\mathbf{P}$ stays at the current vertex with probability $1/2$ or moves to a randomly chosen neighbour. This is equivalent to saying that in each step the random walk chooses a coordinate $\{1, \ldots, d\}$ uniformly at random and flips the bit with probability $1/2$. Our aim is to prove that for $t := d = \log_2 n$, the random walk is

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

unlikely to reach a vertex which has approximately $(1/2)d$ or more ones in its binary representation. To this end, we let C_t denote the number of coordinates that are chosen at least once within the first t steps of the random walk. Moreover, F_t denotes the number of coordinates that are set to 1 at step t. Then, F_t has distribution $\mathrm{Bin}(C_t, 1/2)$. The idea is now to prove that C_t can be approximated by $\mathrm{Bin}(d, 1-1/\mathrm{e})$, which implies that $F_t \approx \mathrm{Bin}(d,p)$, where $p := (1-1/\mathrm{e})/2$.

To make this more formal, let us first consider C_t. Note that C_t can be seen as the number of non-empty bins when throwing $t = d$ balls into d bins, where each bin is chosen independently and uniformly at random (we refer to [25, Chapter 5] for more on balls-into-bins). Now consider a setting where the number of balls in each bin is an independent Poisson random variable with expected value 1. Then, if Y is the number of non-empty bins in this setting, Y has distribution $\mathrm{Bin}(d, 1-1/\mathrm{e})$. From [25, Theorem 5.10] we know that for any $0 \leqslant k \leqslant d$,

$$\mathbb{P}[C_t \geqslant k] \leqslant 2 \cdot \mathbb{P}[Y \geqslant k] = 2 \cdot \mathbb{P}[\mathrm{Bin}(d, 1-1/\mathrm{e}) \geqslant k].$$

Since $\mathbb{P}[\mathrm{Bin}(i,1/2) \geqslant r]$ is increasing in i, we apply [14, Lemma A.1] to conclude that

$$\begin{aligned}\mathbb{P}[F_t \geqslant r] &= \sum_{i=0}^{d} \mathbb{P}[C_t = i] \cdot \mathbb{P}[\mathrm{Bin}(i,1/2) \geqslant r] \\ &\leqslant \sum_{i=0}^{d} 2 \cdot \mathbb{P}[\mathrm{Bin}(d,1-1/\mathrm{e}) = i] \cdot \mathbb{P}[\mathrm{Bin}(i,1/2) \geqslant r] \\ &= 2 \cdot \mathbb{P}[\mathrm{Bin}(d,p) \geqslant r],\end{aligned}$$

so that $\mathbb{P}[F_t \geqslant r] \leqslant 2 \cdot \mathbb{P}[\mathrm{Bin}(d,p) \geqslant r]$. By the Chernoff bound,

$$\mathbb{P}[F_t \geqslant (1+\delta)pd] \leqslant 2 \cdot \mathbb{P}[\mathrm{Bin}(d,p) \geqslant (1+\delta)pd] \leqslant 2 \cdot \left(\frac{\mathrm{e}^{\delta}}{(1+\delta)^{1+\delta}}\right)^{pd}$$

Denoting by $|v|_1$ the number of ones in the binary representation of a vertex $v \in \{0,1\}^d$, we can now upper-bound the expected number of informed nodes after $t = \log_2 n$ rounds with the help of Lemma 4.1 as follows:

$$\begin{aligned}\mathbb{E}[|I_t|] &\leqslant 1 + \sum_{v \in V \setminus \{0\}} \min\{1, 2^t \cdot \mathbf{P}^t_{0,v}\} \\ &\leqslant 1 + \sum_{\substack{v \in V\setminus\{0\} \\ |v|_1 \leqslant (1+\delta)pd}} 1 + \sum_{\substack{v \in V\setminus\{0\} \\ |v|_1 > (1+\delta)pd}} 2^t \cdot \mathbf{P}^t_{0,v} \\ &\leqslant 1 + \sum_{k=1}^{(1+\delta)pd} \binom{d}{k} + 2^t \cdot 2 \cdot \left(\frac{\mathrm{e}^{\delta}}{(1+\delta)^{1+\delta}}\right)^{dp} \\ &\leqslant 1 + n^{H((1+\delta)p)} + 2n \cdot \left(\frac{\mathrm{e}^{\delta}}{(1+\delta)^{1+\delta}}\right)^{dp},\end{aligned}$$

where $H(x)$ is the binary entropy of $x \in (0,1)$. By choosing $\delta = 0.315$, we infer that the last expression is at most $3n^{0.98}$. Using Markov's inequality, $\mathbb{P}[|I_t| \geqslant \log n \cdot \mathbb{E}[|I_t|]] = o(1)$. But if $|I_t| \leqslant 3n^{0.98} \log n$, we need at least additional $0.02 \log_2 n - o(\log n)$ rounds to reach

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

a step $\tau = t + 0.02\log_2 n - o(\log n)$ with $|I_\tau| \in [n/4, n/2]$, since $|I_t|$ can at most double in each round.

It only remains to prove that the probability that all the $|U_\tau| \geqslant n/2$ uninformed nodes become informed within $\log n - o(\log n)$ additional rounds goes to 0. This follows from the argument in [9, Proof of Theorem 1] setting $p = 1/\log n$ and $\Delta = \log_2 n$ (see also the end of the proof of Proposition 3.8). This completes the proof. □

Appendix: Auxiliary lemmas

Lemma A.1 ([16, 27]). *Let A be the adjacency matrix of $G(n,p)$, where $0 < p < 1/2$. Then with probability $1 - o(1)$, for every $2 \leqslant i \leqslant n$, we have $|\lambda_i| = O(\sqrt{pn})$.*

Lemma A.2 ([24, Example 7.5.2, p. 551]). *Let $\mathbf{A}$ and $\mathbf{E}$ be the two $n \times n$, symmetric and real-valued matrices, and let $\mathbf{B} := \mathbf{A} + \mathbf{E}$. Let $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$ be the n eigenvalues of $\mathbf{A}$, let $\varepsilon_1 \geqslant \varepsilon_2 \geqslant \cdots \geqslant \varepsilon_n$ be the n eigenvalues of $\mathbf{E}$ and let $\beta_1 \geqslant \beta_2 \geqslant \cdots \geqslant \beta_n$ be the n eigenvalues of $\mathbf{B}$. Then, for every i, the following double inequality holds:*

$$\lambda_i + \varepsilon_1 \geqslant \beta_i \geqslant \lambda_i + \varepsilon_n.$$

The following concentration inequalities are used to analyse the evolution of the informed nodes over time.

Theorem A.3 (method of bounded differences [23, Lemma 1.2]). *Let $X_1, X_2, \ldots, X_n$ be independent random variables, with X_i taking values in a set A_i for each i. Suppose that the function $f : \prod_{i=1}^n A_i \to \mathbb{R}$ satisfies $|f(x) - f(x')| \leqslant c_k$, whenever the vectors x and x' differ only in the kth coordinate. Let $Y := f(X_1, X_2, \ldots, X_n)$. Then, for any $\rho > 0$,*

$$\mathbb{P}[|Y - \mathbb{E}[Y]| \geqslant \rho] \leqslant 2 \cdot \exp\left(-2\rho^2 \Big/ \sum_{k=1}^n c_k^2\right).$$

We note the following standard Chernoff bound for sum of geometric random variables which can be easily derived by using a Chernoff bound for a sum of Bernoulli random variables.

Theorem A.4 ([8]). *Suppose that $X_1, \ldots, X_n$ are independent geometric random variables on $\mathbb{N}$ with parameter δ, so $\mathbb{E}[X_i] = 1/\delta$ for each i. Let*

$$X := \sum_{i=1}^n X_i, \quad \mu = \mathbb{E}[X] = n/\delta.$$

Then, for any $\varepsilon > 0$,

$$\mathbb{P}[X \geqslant (1+\varepsilon)\mu] \leqslant \mathrm{e}^{-\varepsilon^2 n/2(1+\varepsilon)}.$$

https://doi.org/10.1017/S0963548314000194 Published online by Cambridge University Press

References

[1] Alon, N. and Chung, F. R. K. (1988) Explicit construction of linear sized tolerant networks. *Discrete Math.* **72** 15–19.

[2] Alon, N. and Spencer, J. (2008) *The Probabilistic Method*, third edition, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley.

[3] Boyd, S., Ghosh, A., Prabhakar, B. and Shah, D. (2006) Randomized gossip algorithms. *IEEE Trans. Inform. Theory* **52** 2508–2530.

[4] Broder, A. Z., Frieze, A. M., Suen, S. and Upfal, E. (1998) Optimal construction of edge-disjoint paths in random graphs. *SIAM J. Comput.* **28** 541–573.

[5] Chierichetti, F., Lattanzi, S. and Panconesi, A. (2010) Almost tight bounds for rumour spreading with conductance. In *42nd Annual ACM Symposium on Theory of Computing: STOC'10*, pp. 399–408.

[6] Cooper, C. and Frieze, A. M. (2007) The cover time of sparse random graphs. *Random Struct. Alg.* **30** 1–16.

[7] Doerr, B., Friedrich, T. and Sauerwald, T. (2008) Quasirandom rumor spreading. In *19th Annual ACM–SIAM Symposium on Discrete Algorithms: SODA'08*, pp. 773–781. `arXiv.1012.5351`

[8] Dubhashi, D. and Panconesi, A. (2009) *Concentration of Measure for the Analysis of Randomized Algorithms*, Cambridge University Press.

[9] Elsässer, R. and Sauerwald, T. (2009) On the runtime and robustness of randomized broadcasting. *Theoret. Comput. Sci.* **410** 3414–3427.

[10] Elsässer, R. and Sauerwald, T. (2009) Cover time and broadcast time. In *26th International Symposium on Theoretical Aspects of Computer Science: STACS'09*, pp. 373–384.

[11] Feige, U., Peleg, D., Raghavan, P. and Upfal, E. (1990) Randomized broadcast in networks. *Random Struct. Alg.* **1** 447–460.

[12] Fountoulakis, N. and Panagiotou, K. (2010) Rumor spreading on random regular graphs and expanders. In *14th International Workshop on Randomization and Computation: RANDOM'10*, pp. 560–573.

[13] Fountoulakis, N., Huber, A. and Panagiotou, K. (2010) Reliable broadcasting in random networks and the effect of density. In *29th IEEE Conference on Computer Communications: INFOCOM'10*, pp. 2552–2560.

[14] Friedrich, T., Gairing, M. and Sauerwald, T. (2012) Quasirandom load balancing. *SIAM J. Comput.* **41** 747–771.

[15] Frieze, A. and Grimmett, G. (1985) The shortest-path problem for graphs with random arc-lengths. *Discrete Appl. Math.* **10** 57–77.

[16] Füredi, Z. and Kómlos, J. (1981) The eigenvalues of random symmetric matrices. *Combinatorica* **3** 233–241.

[17] Giakkoupis, G. (2011) Tight upper bounds for rumor spreading in graphs of a given conductance. In *28th International Symposium on Theoretical Aspects of Computer Science: STACS'11*, pp. 57–68.

[18] Giakkoupis, G. and Sauerwald, T. (2012) Rumor spreading and vertex expansion. In *23rd Annual ACM–SIAM Symposium on Discrete Algorithms: SODA'12*, pp. 1623–1641.

[19] Hoory, S., Linial, N. and Wigderson, A. (2006) Expander graphs and their applications. *Bull. Amer. Math. Soc.* **43** 439–561.

[20] Janson, S., Łuczak, T. and Ruciński, A. (2000) *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley.

[21] Karp, R., Schindelhauer, C., Shenker, S. and Vöcking, B. (2000) Randomized rumor spreading. In *41st Annual IEEE Symposium on Foundations of Computer Science: FOCS'00*, pp. 565–574.

[22] Krivelevich, M. and Sudakov, B. (2006) Pseudo-random graphs. In *More Sets, Graphs and Numbers*, Vol. 15 of *Bolyai Society Mathematical Studies*, Springer, pp. 199–262.

[23] McDiarmid, C. (1989) On the method of bounded differences. In *Surveys in Combinatorics*, Vol. 141 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, pp. 148–188.
[24] Meyer, C. D. (2000) *Matrix Analysis and Applied Linear Algebra*, SIAM. `http://www.matrixanalysis.com/DownloadChapters.html`
[25] Mitzenmacher, M. and Upfal, E. (2005) *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*, Cambridge University Press.
[26] Mosk-Aoyama, D. and Shah, D. (2008) Fast distributed algorithms for computing separable functions. *IEEE Trans. Inform. Theory* **54** 2997–3007.
[27] Vu, V. H. (2007) Spectral norm of random matrices. *Combinatorica* **27** 721–736.