THE INSTITUTE FOR SYSTEMS RESEARCH

ISR TECHNICAL REPORT 2011-11

A zero-one law for the existence of triangles in random key graphs

Osman Yagan and Armand M. Makowski

A zero-one law for the existence of triangles in random key graphs

Osman Yağan and Armand M. Makowski
oyagan@umd.edu, armand@isr.umd.edu
Department of Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland, College Park, MD 20742.

September 3, 2011

Abstract

Random key graphs are random graphs induced by the random key predistribution scheme of Eschenauer and Gligor under the assumption of full visibility. For this class of random graphs we show the existence of a zero-one law for the appearance of triangles, and identify the corresponding critical scaling. This is done by applying the method of first and second moments to the number of triangles in the graph.

Keywords: Random key graphs, Uniform intersection graphs, Existence of triangles, Zero-one laws, Critical scalings

1 Introduction

Random key graphs are random graphs that belong to the class of random intersection graphs [13]; in fact they are sometimes called uniform random intersection graphs by some authors [1, 6, 7]. They have appeared recently in application areas as diverse as clustering analysis [6, 7], collaborative filtering in recommender systems [10] and random key predistribution for wireless sensor networks (WSNs) [5]. In this last context, random key graphs naturally occur in the study of the following random key predistribution scheme introduced by Eschenauer and Gligor [5]: Before deployment, each sensor in a WSN is independently assigned K distinct cryptographic keys which are selected at random from a very large pool of P keys. These K keys

constitute the key ring of the node and are inserted into its memory module. Two sensor nodes can then establish a secure link between them if they are within transmission range of each other and if their key rings have at least one key in common; see [5] for implementation details. If we assume *full visibility*, namely nodes are all within communication range of each other, then secure communication between two nodes requires only that their key rings share at least one key. The resulting notion of adjacency defines the class of random key graphs; see Section 2 for precise definitions.

Much efforts have recently been devoted to developing zero-one laws for the property of connectivity in random key graphs. A key motivation can be found in the need to obtain conditions under which the scheme of Eschenauer and Gligor guarantees secure connectivity with high probability in large networks. An interesting feature of this work lies in the following fact: Although random key graphs are *not* stochastically equivalent to the classical Erdős-Rényi graphs [4], it is possible to transfer well-known zero-one laws for connectivity in Erdős-Rényi graphs to random key graphs by asymptotically matching their edge probabilities. This approach, which was initiated by Eschenauer and Gligor in their original analysis [5], has now been validated rigorously; see the papers [1, 3, 12, 14, 15] for recent developments. Furthermore, Rybarczyk [12] has shown that this transfer from Erdős-Rényi graphs also works for a number of issues related to the giant component and its diameter.

In view of these developments, it is natural to wonder whether this transfer technique applies to other graph properties. In particular, in the literature on random graphs there is a long standing interest [2, 4, 8, 9, 11, 13] in the containment of certain (small) subgraphs, the simplest one being the *triangle*. This last case is of some practical relevance since the number of triangles in a graph is closely related to its clustering properties [17]. With this in mind, in the present paper we study the zero-one law for the existence of triangles in random key graphs and identify the corresponding critical scaling.

From these findings we conclude that in the many node regime, the expected number of triangles in random key graphs is always at least as large as the corresponding quantity in asymptotically matched Erdős-Rényi graphs. For the parameter range of practical relevance in WSNs, this expected number of triangles can be orders of magnitude larger in random key graphs than in Erdős-Rényi graphs, a fact also observed earlier via simulations by Di Pietro et al. [3]. As a result, transferring results from Erdős-Rényi graphs by matching their edge probabilities is not a valid approach in general, and can be quite misleading in the context of WSNs.

The zero-one laws obtained here were announced in the conference paper [16] with much longer proofs. In line with results currently available for other classes of graphs, e.g., Erdős-Rényi graphs [8, Chap. 3] and geometric random graphs [11, Chap. 3], it would be interesting to consider the containment problem for small subgraphs other than triangles in the context of random key graphs.

The paper is organized as follows: In Section 2 we formally introduce the class of random key graphs while in Section 3 we present the main results of the paper given as Theorem 3.1 and Theorem 3.2. Section 4 compares these results with the corresponding zero-one law in Erdős-Rényi graphs. The zero-one laws are established by an application of the method of first and second moments, respectively [2, p. 2] [8, p. 55]. Before we begin, several asymptotic results are collected in Section 5 for easy reference. In Section 6, we give a proof of the zero-law (Theorem 3.1). A proof of the one-law (Theorem 3.2) is presented in Sections 7 and 8. An additional technical derivation is given in Appendix A.

A word on the notation and conventions in use: All limiting statements, including asymptotic equivalences, are understood with n going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation operator by $\mathbb{E}$. The indicator function of an event E is denoted by $\mathbf{1}[E]$. For any discrete set S we write $|S|$ for its cardinality.

2 Random key graphs

The model is parametrized by the number n of nodes, the size P of the key pool and the size K of each key ring with $K \leq P$. We group the integers P and K into the ordered pair $\theta \equiv (K, P)$ in order to simplify the notation. Now, for each node $i = 1, \ldots, n$, let $K_i(\theta)$ denote the random set of K distinct keys assigned to node i – Thus, under the convention that the P keys are labelled $1, \ldots, P$, the random set $K_i(\theta)$ is a subset of $\{1, \ldots, P\}$ with $|K_i(\theta)| = K$. The rvs $K_1(\theta), \ldots, K_n(\theta)$ are assumed to be *i.i.d.* rvs, each of which is *uniformly* distributed with

$$\mathbb{P}[K_i(\theta) = S] = \binom{P}{K}^{-1}, \qquad i = 1, \ldots, n \tag{1}$$

for any subset S of $\{1, \ldots, P\}$ with $|S| = K$. This corresponds to selecting keys randomly and *without* replacement from the key pool.

Distinct nodes $i, j = 1, \ldots, n$ are said to be adjacent if they share at least one key in their key rings, namely

$$K_i(\theta) \cap K_j(\theta) \neq \emptyset, \tag{2}$$

in which case an undirected link is assigned between nodes i and j. The resulting random graph defines the *random key graph* on the vertex set $\{1, \ldots, n\}$, hereafter denoted $\mathbb{K}(n; \theta)$.

For distinct $i, j = 1, \ldots, n$, it is easy to check that

$$\mathbb{P}\left[K_i(\theta) \cap K_j(\theta) = \emptyset\right] = q(\theta) \tag{3}$$

with

$$q(\theta) := \begin{cases} 0 & \text{if } \; P < 2K \\ \\ \frac{\binom{P-K}{K}}{\binom{P}{K}} & \text{if } \; 2K \leq P. \end{cases} \tag{4}$$

The probability of edge occurrence between any two nodes is therefore equal to $1 - q(\theta)$. If $P < 2K$ there exists an edge between any pair of nodes, and $\mathbb{K}(n; \theta)$ coincides with the complete graph on the vertex set $\{1, \ldots, n\}$. Also, we always have $0 \leq q(\theta) < 1$, and $q(\theta) > 0$ if and only if $2K \leq P$. The expression (4) is a simple consequence of the often used fact that

$$\mathbb{P}\left[S \cap K_i(\theta) = \emptyset\right] = \frac{\binom{P-|S|}{K}}{\binom{P}{K}}, \quad i = 1, \ldots, n \tag{5}$$

for every subset S of $\{1, \ldots, P\}$ with $|S| \leq P - K$.

3 The main results

Pick positive integers K and P such that $K \leq P$. Fix $n = 3, 4, \ldots$ and for distinct $i, j, k = 1, \ldots, n$, define the indicator function

$$\chi_{n,ijk}(\theta) := \mathbf{1}\left[\text{Nodes } i, j \text{ and } k \text{ form a triangle in } \mathbb{K}(n; \theta)\right].$$

The number of (unlabelled) triangles in $\mathbb{K}(n; \theta)$ is simply given by

$$T_n(\theta) := \sum_{(ijk)} \chi_{n,ijk}(\theta) \tag{6}$$

where $\sum_{(ijk)}$ denotes summation over all distinct triples ijk with $1 \leq i < j < k \leq n$. The event that there exists at least one triangle in $\mathbb{K}(n; \theta)$ is then characterized by $T(n, \theta) := [T_n(\theta) > 0] = [T_n(\theta) = 0]^c$.

The main result of the paper is a zero-one law for the existence of triangles in random key graphs. To state the results we find it convenient to make use of the quantity

$$\tau(\theta) := \frac{K^3}{P^2} + \left(\frac{K^2}{P}\right)^3, \qquad \begin{array}{c}\theta = (K, P) \\ K, P = 1, 2, \ldots\end{array} \tag{7}$$

For simplicity of exposition we refer to any pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* provided the natural condition $K_n \leq P_n$ holds for all $n = 2, 3, \ldots$. The zero-law is given first.

Theorem 3.1 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$, we have the zero-law $\lim_{n\to\infty} \mathbb{P}\left[T_n(\theta_n) > 0\right] = 0$ under the condition*

$$\lim_{n\to\infty} n^3 \tau(\theta_n) = 0. \tag{8}$$

The one-law given next assumes a more involved form.

Theorem 3.2 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ for which the limit $\lim_{n\to\infty} q(\theta_n) = q^\star$ exists, we have the one-law $\lim_{n\to\infty} \mathbb{P}\left[T_n(\theta_n) > 0\right] = 1$ either if $0 \leq q^\star < 1$ or if $q^\star = 1$ under the condition*

$$\lim_{n\to\infty} n^3 \tau(\theta_n) = \infty. \tag{9}$$

Theorem 3.1 and Theorem 3.2 will be established by the method of first and second moments, respectively [2, p. 2], [8, p. 55], applied to the count variables defined at (6). To facilitate comparison with Erdős-Rényi graphs, we combine Theorem 3.1 and Theorem 3.2 into the symmetric statement.

Theorem 3.3 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ for which $\lim_{n\to\infty} q(\theta_n)$ exists, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[T_n(\theta_n) > 0\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} n^3 \tau(\theta_n) = 0 \\ \\ 1 & \text{if } \lim_{n\to\infty} n^3 \tau(\theta_n) = \infty. \end{cases} \tag{10}$$

It follows from Lemma 5.1 that the condition $\lim_{n\to\infty} n^3 \tau(\theta_n) = 0$ implies $\lim_{n\to\infty} q(\theta_n) = 0$ (hence $q^\star = 0$).

4 Comparing with Erdős-Rényi graphs

In this section we compare Theorem 3.3 with its analog for Erdős-Rényi graphs. First some notation: For each p in $[0,1]$ and $n = 2, 3, \ldots$, let $\mathbb{G}(n;p)$ denote the Erdős-Rényi graph on the vertex set $\{1, \ldots, n\}$ with edge probability p. In analogy with (6) let $T_n(p)$ denote the number of (unlabelled) triangles in $\mathbb{G}(n;p)$, and consider the event that there exists at least one triangle in $\mathbb{G}(n;p)$, i.e., $[T_n(p) > 0]$. We also refer to any mapping $p : \mathbb{N}_0 \to [0,1]$ as a scaling for Erdős-Rényi graphs. The following zero-one law for triangle containment in Erdős-Rényi graphs is well known [2, Chp. 4], [4, Thm. 1], [8, Thm. 3.4, p. 56].

Theorem 4.1 *For any scaling $p : \mathbb{N}_0 \to [0,1]$, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[T_n(p_n) > 0\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} n^3\tau^\star(p_n) = 0 \\ \\ 1 & \text{if } \lim_{n\to\infty} n^3\tau^\star(p_n) = \infty \end{cases} \tag{11}$$

where we have set $\tau^\star(p) := p^3$, $0 \le p \le 1$.

As this result is also established by the method of first and second moments, its form is easily understood once we note that

$$\mathbb{E}\left[T_n(p)\right] = \binom{n}{3}\tau^\star(p), \qquad \begin{matrix} 0 \le p \le 1 \\ n = 3, 4, \ldots \end{matrix} \tag{12}$$

As mentioned earlier, random key graphs are *not* equivalent to Erdős-Renyi graphs even when their edge probabilities are matched, i.e., as graph-valued rvs, the random graphs $\mathbb{G}(n;p)$ and $\mathbb{K}(n;\theta)$ have different distributions with $p = 1 - q(\theta)$; see [16] for a discussion of (dis)similarities. However, in order to meaningfully compare the zero-one laws of Theorem 3.3 and Theorem 4.1, the scaling $p : \mathbb{N}_0 \to [0,1]$ (for Erdős-Rényi graphs) is said to be *asymptotically matched* to the scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ (for random key graphs) if $p_n \sim 1 - q(\theta_n)$. This is equivalent to requiring that the expected degrees in $\mathbb{K}(n;\theta_n)$ and $\mathbb{G}(n;p_n)$ be asymptotically equivalent. Under the natural condition $\lim_{n\to\infty} q(\theta_n) = 1$, the asymptotic matching condition amounts to

$$p_n \sim \frac{K_n^2}{P_n} \tag{13}$$

by virtue of Lemma 5.1.

The definitions readily yield

$$\frac{\tau(\theta_n)}{\tau^\star(p_n)} = \frac{1}{p_n^3} \cdot \left(\frac{K_n^3}{P_n^2}\right) + \frac{1}{p_n^3} \cdot \left(\frac{K_n^2}{P_n}\right)^3, \quad n = 2, 3, \ldots$$

whence

$$\frac{\tau(\theta_n)}{\tau^\star(p_n)} \sim 1 + \frac{P_n}{K_n^3} \tag{14}$$

under (13). This suggests that the existence of a triangle is always reached *earlier* in the evolution of a random key graph as compared to the Erdös-Rényi graph asymptotically matched to it. By Proposition 5.2, (14) is equivalent to

$$\frac{\mathbb{E}\left[T_n(\theta_n)\right]}{\mathbb{E}\left[T_n(p_n)\right]} \sim 1 + \frac{P_n}{K_n^3} \tag{15}$$

as we make use of the expressions (12) and (28). In other words, for large n the expected number of triangles in random key graphs is always at least as large as the corresponding quantity in asymptotically matched Erdős-Rényi graphs.

In the context of WSNs, it is natural to select the parameters K_n and P_n such that the induced random key graph is *connected*. However, there is a tradeoff between connectivity and security [3], requiring $\frac{K_n^2}{P_n}$ to be kept as close as possible to the critical scaling $\frac{\log n}{n}$ for connectivity; see the papers [1, 3, 12, 14, 15]. In the desired regime near the boundary, this amounts to

$$\frac{K_n^2}{P_n} \sim c \cdot \frac{\log n}{n} \tag{16}$$

with $c > 1$ but close to one, and from (15) we see then that

$$\frac{\mathbb{E}\left[T_n(\theta_n)\right]}{\mathbb{E}\left[T_n(p_n)\right]} \sim 1 \quad \text{if and only if} \quad K_n \gg \frac{n}{\log n}. \tag{17}$$

In that case the expected number of triangles in random key graphs is of the same order as the corresponding quantity in asymptotically matched Erdős-Rényi graphs with $\mathbb{E}\left[T_n(\theta_n)\right] \sim \mathbb{E}\left[T_n(p_n)\right] \sim \frac{c^3}{6}\left(\log n\right)^3$ – This is a direct consequence of (13) and (16). This conclusion holds regardless of the value of c in (16).

However, given the limited memory and computational power of the sensor nodes, the key ring sizes at (17) are not practical. In addition, they will lead to *high* node degrees and this in turn will decrease network *resiliency* against node capture attacks. Indeed, it was proposed by Di Pietro et al. [3, Thm. 5.3] that security in WSNs be ensured by selecting K_n and P_n such that $\frac{K_n}{P_n} \sim \frac{1}{n}$. Under (16) this additional requirement then leads to $K_n \sim c \cdot \log n$ so that $P_n \sim c \cdot n \log n$, and (15) now implies

$$\lim_{n\to\infty} \frac{\mathbb{E}\left[T_n(\theta_n)\right]}{\mathbb{E}\left[T_n(p_n)\right]} = \lim_{n\to\infty} \left(1 + \frac{n}{(c \cdot \log n)^2}\right) = \infty. \tag{18}$$

Hence, for realistic WSN scenarios the expected number of triangles in the induced random key graphs can be orders of magnitude larger than in Erdős-Rényi graphs. This provides a clear example where transferring known results for Erdős-Rényi graphs to random key graphs by asymptotically matching their edge probabilities can be misleading.

5 Some useful asymptotics

In this section we collect a number of asymptotic results that prove useful in establishing the results derived in this paper. The first result was already obtained in [15, 18].

Lemma 5.1 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$, we have*

$$\lim_{n\to\infty} q(\theta_n) = 1 \quad \textit{if and only if} \quad \lim_{n\to\infty} \frac{K_n^2}{P_n} = 0, \tag{19}$$

and under either condition the asymptotic equivalence

$$1 - q(\theta_n) \sim \frac{K_n^2}{P_n} \tag{20}$$

holds.

Since $1 \le K_n \le {K_n}^2$ for all $n = 1, 2, \ldots$, the condition (19) implies

$$\lim_{n\to\infty} \frac{K_n}{P_n} = 0 \tag{21}$$

and

$$\lim_{n\to\infty} P_n = \infty, \tag{22}$$

so that for any $c > 0$, we have $cK_n < P_n$ for all n sufficiently large in $\mathbb{N}_0$ (dependent on c).

With positive integers K and P such that $K \le P$, we define

$$\beta(\theta) := (1 - q(\theta))^3 + q(\theta)^3 - q(\theta)r(\theta) \tag{23}$$

where we have set

$$r(\theta) := \begin{cases} 0 & \text{if } \; P < 3K \\ \frac{\binom{P-2K}{K}}{\binom{P}{K}} & \text{if } \; 3K \le P. \end{cases} \tag{24}$$

Note that $r(\theta)$ corresponds to the probability (5) when $|S| = 2K$, and a probabilistic interpretation for $\beta(\theta)$ is given in Lemma 6.1. Direct inspection shows that $r(\theta) \leq q(\theta)^2$, whence

$$\beta(\theta) \geq (1 - q(\theta))^3 > 0. \tag{25}$$

The following asymptotic equivalence will be crucial to stating the results in a more explicit form.

Proposition 5.2 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (19), we have the asymptotic equivalence $\beta(\theta_n) \sim \tau(\theta_n)$.*

Proof. Under the enforced assumptions, we have $3K_n < P_n$ for all n sufficiently large in $\mathbb{N}_0$, and on that range we can use the expression (23) to write

$$\beta(\theta_n) = (1 - q(\theta_n))^3 + q(\theta_n)^3 \left(1 - \frac{r(\theta_n)}{q^2(\theta_n)}\right), \quad n = 1, 2, \ldots.$$

As Lemma 5.1 already implies $q(\theta_n)^3 \sim 1$ and $(1 - q(\theta_n))^3 \sim \left(\frac{K_n^2}{P_n}\right)^3$, the asymptotic equivalence $\beta(\theta_n) \sim \tau(\theta_n)$ will be established if we show that

$$1 - \frac{r(\theta_n)}{q(\theta_n)^2} \sim \frac{K_n^3}{P_n^2}. \tag{26}$$

This key technical fact is discussed in Appendix A. ■

6 A proof of Theorem 3.1

We begin by computing the expected number of triangles in random key graphs.

Lemma 6.1 *Fix $n = 3, 4, \ldots$. For positive integers K and P such that $K \leq P$, we have*

$$\mathbb{E}\left[\chi_{n,123}(\theta)\right] = \beta(\theta) \tag{27}$$

with $\beta(\theta)$ defined at (23), so that

$$\mathbb{E}\left[T_n(\theta)\right] = \binom{n}{3} \beta(\theta). \tag{28}$$

Proof. Fix positive integers K and P such that $K \leq P$. As exchangeability yields

$$\mathbb{E}\left[T_n(\theta)\right] = \binom{n}{3}\mathbb{E}\left[\chi_{n,123}(\theta)\right], \quad n = 3, 4, \ldots \tag{29}$$

we need only show the validity of (27).

In the discussion that follows we omit the explicit dependence on θ when no confusion arises from doing so. Also, we make repeated use of the fact that for any pair of events, say E and F, we have

$$\mathbb{P}\left[E \cap F\right] = \mathbb{P}\left[E\right] - \mathbb{P}\left[E \cap F^c\right]. \tag{30}$$

Thus,

$$\begin{aligned}
\mathbb{E}\left[\chi_{n,123}(\theta)\right] &= \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_1 \cap K_3 \neq \emptyset, K_2 \cap K_3 \neq \emptyset\right] \\
&= \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_1 \cap K_3 \neq \emptyset\right] \\
&\quad - \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_1 \cap K_3 \neq \emptyset, K_2 \cap K_3 = \emptyset\right] \\
&= \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_1 \cap K_3 \neq \emptyset\right] \\
&\quad - \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_2 \cap K_3 = \emptyset\right] \\
&\quad + \mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_1 \cap K_3 = \emptyset, K_2 \cap K_3 = \emptyset\right].
\end{aligned}$$

By independence, with the help of (5), we readily obtain the expressions

$$\mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_1 \cap K_3 \neq \emptyset\right] = \left(1 - q(\theta)\right)^2$$

and

$$\mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_2 \cap K_3 = \emptyset\right] = \left(1 - q(\theta)\right) q(\theta).$$

Next, as we use (30) one more time, we get

$$\begin{aligned}
&\mathbb{P}\left[K_1 \cap K_2 \neq \emptyset, K_1 \cap K_3 = \emptyset, K_2 \cap K_3 = \emptyset\right] \\
&\quad = \mathbb{P}\left[K_1 \cap K_3 = \emptyset, K_2 \cap K_3 = \emptyset\right] \\
&\qquad - \mathbb{P}\left[K_1 \cap K_2 = \emptyset, K_1 \cap K_3 = \emptyset, K_2 \cap K_3 = \emptyset\right].
\end{aligned}$$

Again, by independence, with the help of (5) we conclude that

$$\mathbb{P}\left[K_1 \cap K_3 = \emptyset, K_2 \cap K_3 = \emptyset\right] = q(\theta)^2 \tag{31}$$

and

$$\begin{aligned}
&\mathbb{P}\left[K_1 \cap K_2 = \emptyset, K_1 \cap K_3 = \emptyset, K_2 \cap K_3 = \emptyset\right] \\
&\quad = \mathbb{P}\left[K_1 \cap K_2 = \emptyset, K_3 \cap (K_1 \cup K_2) = \emptyset\right] \\
&\quad = \mathbb{E}\left[\mathbf{1}\left[K_1 \cap K_2 = \emptyset\right] r(\theta)\right] \\
&\quad = q(\theta) r(\theta)
\end{aligned} \tag{32}$$

since $|K_1 \cup K_2| = 2K$ when $K_1 \cap K_2 = \emptyset$. Collecting these facts we find

$$\mathbb{E}\left[\chi_{n,123}(\theta)\right] = (1 - q(\theta))^2 - (1 - q(\theta))\, q(\theta) + q(\theta)^2 - q(\theta) r(\theta)$$

and the conclusion (27) follows by elementary algebra. ■

We now turn to proving Theorem 3.1: Consider a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$. For each $n = 3, 4, \ldots$, the elementary bound $\mathbb{P}\left[T_n(\theta_n) > 0\right] \leq \mathbb{E}\left[T_n(\theta_n)\right]$ implies

$$\mathbb{P}\left[T_n(\theta_n) > 0\right] \leq \binom{n}{3} \beta(\theta_n)$$

by virtue of Lemma 6.1. Theorem 3.1 thus follows if under (8) we show that $\lim_{n\to\infty} \binom{n}{3} \beta(\theta_n) = 0$. By Proposition 5.2 this convergence is clearly equivalent to the assumed condition $\lim_{n\to\infty} n^3 \tau(\theta_n) = 0$, and the proof of Theorem 3.1 is now complete. ■

7 Proving Theorem 3.2

The case $0 \leq q^\star < 1$ is discussed in the conference paper [16]. To handle the case $q^\star = 1$, we use a standard bound which forms the basis of the method of second moment [8, Remark 3.1, p. 55]. Here this bound takes the form

$$\frac{\left(\mathbb{E}\left[T_n(\theta_n)\right]\right)^2}{\mathbb{E}\left[T_n(\theta_n)^2\right]} \leq \mathbb{P}\left[T_n(\theta_n) > 0\right], \quad n = 3, 4, \ldots \tag{33}$$

Theorem 3.2 will be established in the case $q^\star = 1$ if we show the following result.

Proposition 7.1 *For any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (19), we have*

$$\lim_{n\to\infty} \frac{\mathbb{E}\left[T_n(\theta_n)^2\right]}{\left(\mathbb{E}\left[T_n(\theta_n)\right]\right)^2} = 1 \tag{34}$$

under the condition (9).

The remainder of the paper is devoted to establishing Proposition 7.1. A natural first step towards establishing Proposition 7.1 consists in computing the second moment of the count variables (6).

Proposition 7.2 *For positive integers K and P such that $K \leq P$, we have*

$$\begin{aligned}\mathbb{E}\left[T_n(\theta)^2\right] = \mathbb{E}\left[T_n(\theta)\right] &+ \left(\frac{\binom{n-3}{3}}{\binom{n}{3}} + 3\frac{\binom{n-3}{2}}{\binom{n}{3}}\right) \cdot \mathbb{E}\left[T_n(\theta)\right]^2 \\ &+ \binom{n}{3}\binom{3}{2}\binom{n-3}{1} \cdot \mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right]\end{aligned} \tag{35}$$

for all $n = 3, 4, \ldots$.

Proof. Fix positive integers K and P such that $K \leq P$, and $n = 3, 4, \ldots$. By exchangeability and the binary nature of the rvs involved we readily obtain

$$\begin{aligned}\mathbb{E}\left[T_n(\theta)^2\right] = \mathbb{E}\left[T_n(\theta)\right] &+ \binom{n}{3}\binom{3}{2}\binom{n-3}{1}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right] \\ &+ \binom{n}{3}\binom{3}{1}\binom{n-3}{2}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,145}(\theta)\right] \\ &+ \binom{n}{3}\binom{n-3}{3}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,456}(\theta)\right].\end{aligned} \tag{36}$$

Under the enforced independence assumptions the rvs $\chi_{n,123}(\theta)$ and $\chi_{n,456}(\theta)$ are independent and identically distributed. As a result,

$$\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,456}(\theta)\right] = \mathbb{E}\left[\chi_{n,123}(\theta)\right]\mathbb{E}\left[\chi_{n,456}(\theta)\right] = \beta(\theta)^2$$

so that

$$\binom{n}{3}\binom{n-3}{3}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,456}(\theta)\right] = \frac{\binom{n-3}{3}}{\binom{n}{3}} \cdot \mathbb{E}\left[T_n(\theta)\right]^2 \tag{37}$$

as we make use of the relation (28).

On the other hand, with the help of (5) we check that the indicator rvs $\chi_{n,123}(\theta)$ and $\chi_{n,145}(\theta)$ are independent and identically distributed *conditionally* on $K_1(\theta)$ with

$$\mathbb{P}\left[\chi_{n,123}(\theta) = 1 | K_1(\theta)\right] = \mathbb{P}\left[\chi_{n,123}(\theta) = 1\right] = \beta(\theta). \tag{38}$$

As a similar statement applies to $\chi_{n,145}(\theta)$, we conclude that the rvs $\chi_{n,123}(\theta)$ and $\chi_{n,145}(\theta)$ are (unconditionally) independent and identically distributed with

$$\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,145}(\theta)\right] = \mathbb{E}\left[\chi_{n,123}(\theta)\right]\mathbb{E}\left[\chi_{n,145}(\theta)\right] = \beta(\theta)^2.$$

Again by virtue of (28), this last observation yields

$$\binom{n}{3}\binom{3}{1}\binom{n-3}{2}\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,145}(\theta)\right] = 3\frac{\binom{n-3}{2}}{\binom{n}{3}}\cdot\left(\mathbb{E}\left[T_n(\theta)\right]\right)^2. \tag{39}$$

Substituting (37) and (39) into (36) establishes Proposition 7.2. ■

8 A proof of Proposition 7.1

Consider any scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (19). As pointed out earlier, the equivalent conditions (19) imply $3K_n < P_n$ for all n sufficiently large in $\mathbb{N}_0$. On that range, with θ replaced by θ_n, Proposition 7.2 yields

$$\begin{aligned}\frac{\mathbb{E}\left[T_n(\theta_n)^2\right]}{\left(\mathbb{E}\left[T_n(\theta_n)\right]\right)^2} = \frac{1}{\mathbb{E}\left[T_n(\theta_n)\right]} &+ \left(\frac{\binom{n-3}{3}}{\binom{n}{3}} + 3\frac{\binom{n-3}{2}}{\binom{n}{3}}\right) \\ &+ \frac{3(n-3)}{\binom{n}{3}}\cdot\frac{\mathbb{E}\left[\chi_{n,123}(\theta_n)\chi_{n,124}(\theta_n)\right]}{\left(\mathbb{E}\left[\chi_{n,123}(\theta_n)\right]\right)^2}\end{aligned} \tag{40}$$

as we make use of (29) in the last term.

Let n go to infinity in the resulting expression: By Proposition 5.2 we have $\lim_{n\to\infty} n^3\beta(\theta_n) = \infty$ under condition (9), whence $\lim_{n\to\infty}\mathbb{E}\left[T_n(\theta_n)\right] = \infty$ by virtue of (29). Since

$$\lim_{n\to\infty}\left(\frac{\binom{n-3}{3}}{\binom{n}{3}} + 3\frac{\binom{n-3}{2}}{\binom{n}{3}}\right) = 1 \quad \text{and} \quad \frac{\binom{n}{3}}{3(n-3)} \sim \frac{n^2}{18},$$

the convergence (34) will hold if we show that

$$\lim_{n\to\infty}\frac{1}{n^2}\frac{\mathbb{E}\left[\chi_{n,123}(\theta_n)\chi_{n,124}(\theta_n)\right]}{\left(\mathbb{E}\left[\chi_{n,123}(\theta_n)\right]\right)^2} = 0 \tag{41}$$

under the foregoing conditions on the scaling.

We proceed as follows: Given positive integers K and P such that $K \le P$, fix $n = 3, 4, \ldots$. It is immediate that

$$\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right] \le \mathbb{E}\left[\chi_{n,123}(\theta)\mathbf{1}\left[K_1(\theta)\cap K_4(\theta)\neq\emptyset\right]\right]. \tag{42}$$

From (5) it follows that the rvs $\chi_{n,123}(\theta)$ and $\mathbf{1}\left[K_1(\theta)\cap K_4(\theta)\neq\emptyset\right]$ are independent conditionally on $K_1(\theta)$, and an easy conditioning argument yields

$$\mathbb{E}\left[\chi_{n,123}(\theta)\mathbf{1}\left[K_1(\theta)\cap K_4(\theta)\neq\emptyset\right]\right] = \beta(\theta)(1-q(\theta)) \tag{43}$$

as we recall (4) and (38). Using (42) together with (27) and (43) we readily obtain the inequalities

$$\frac{\mathbb{E}\left[\chi_{n,123}(\theta)\chi_{n,124}(\theta)\right]}{\left(\mathbb{E}\left[\chi_{n,123}(\theta)\right]\right)^2} \leq \frac{\beta(\theta)(1-q(\theta))}{\beta(\theta)^2} \leq \beta(\theta)^{-2/3} \tag{44}$$

where in the last step we noted that $1-q(\theta) \leq \beta(\theta)^{1/3}$ by appealing to (25).

Now consider a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying (19), and replace θ by θ_n in the bound (44) according to this scaling. The convergence (41) will be established if we show that

$$\lim_{n\to\infty} n^2\beta(\theta_n)^{2/3} = \infty. \tag{45}$$

As Proposition 5.2 yields

$$n^2\beta(\theta_n)^{2/3} \sim n^2\tau(\theta_n)^{2/3} = \left(n^3\tau(\theta_n)\right)^{2/3},$$

the desired conclusion (45) follows under the condition (9). ■

Acknowledgments

This work was supported by NSF Grant CCF-07290 and part of this material was presented in [16]. The authors thank the reviewer for a very careful reading of the manuscript, and for comments which greatly improved its presentation and significantly shortened the proof of Theorem 3.2.

References

[1] S.R. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," *Discrete Mathematics* **309** (2009), pp. 5130-5140.

[2] B. Bollobás, *Random Graphs*, Second Edition, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (UK), 2001.

[3] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information Systems Security* **TISSEC 11** (2008), pp. 1-22.

[4] P. Erdős and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci.* **5** (1960), pp. 17-61.

[5] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the ACM Conference on Computer and Communications Security (2002), Washington (DC), November 2002.

[6] E. Godehardt and J. Jaworski "Two models of random intersection graphs for classification," in *Studies in Classification, Data Analysis and Knowledge Organization* **22**, Eds. O. Optiz and M. Schwaiger, Springer, Berlin (2003), pp. 67-82.

[7] E. Godehardt, J. Jaworski and K. Rybarczyk, "Random intersection graphs and classification," in *Studies in Classification, Data Analysis and Knowledge Organization* **33**, Eds. H.J. Lens and R,. Decker, Springer, Berlin (2007), pp. 67-74.

[8] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 2000.

[9] M.K. Karoński, E.R. Scheinerman, and K.B. Singer-Cohen, "On random intersection graphs: The subgraph problem," *Combinatorics, Probability and Computing* **8** (1999), pp. 131-159.

[10] P. Marbach, "A lower-bound on the number of rankings required in recommender systems using collaborative filtering," Proceedings of the 42nd Annual Conference on Information Sciences and Systems (CISS 2008), Princeton University, Princeton (NJ), March 2008.

[11] M.D. Penrose, *Random Geometric Graphs*, Oxford Studies in Probability **5**, Oxford University Press, New York (NY), 2003.

[12] K. Rybarczyk, "Diameter, connectivity, and phase transition of the uniform random intersection graph," *Discrete Mathematics* **311** (2011), pp. 1998-2019.

[13] K.B. Singer, *Random Intersection Graphs*, Ph.D. Thesis, The Johns Hopkins University, Baltimore (MD), 1995.

[14] O. Yağan and A. M. Makowski, "Connectivity results for random key graphs," Proceedings of the IEEE International Symposium on Information Theory (ISIT 2009), Seoul (Korea), June 2009.

[15] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs," Submitted to *IEEE Transactions on Information Theory*, November 2009. Under second review. Available online at arXiv:0908.3644v1 [math.CO]. Earlier draft available online (with a different title) at http://hdl.handle.net/1903/8716, January 2009.

[16] O. Yağan and A. M. Makowski, "On the existence of triangles in random key graphs," in Proceedings of the 47th Annual Allerton Conference on Communication, Control and Computing, Monticello (IL), September 2009.

[17] O. Yağan and A. M. Makowski, "Random key graphs – Can they be small worlds?," in Proceedings of the First Workshop on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (GRAPH-HOC 2009), Chennai (India), December 2009.

[18] O. Yağan, *Random Graph Modeling of Random Key Distribution Schemes in Wireless Sensor Networks*, Ph.D. Thesis, Department of Electrical and Computer Engineering, University of Maryland, College Park (MD), June 2011.

A Establishing (26)

With positive integers K, P such that $3K \leq P$, we note that

$$\begin{aligned}
\frac{r(\theta)}{q(\theta)^2} &= \left(\frac{(P-2K)!}{(P-K)!}\right)^2 \cdot \frac{(P-2K)!}{(P-3K)!} \cdot \frac{P!}{(P-K)!} \\
&= \prod_{\ell=0}^{K-1} \left(\frac{P-2K-\ell}{P-K-\ell}\right) \cdot \prod_{\ell=0}^{K-1} \left(\frac{P-\ell}{P-K-\ell}\right) \\
&= \prod_{\ell=0}^{K-1} \left(1 - \left(\frac{K}{P-K-\ell}\right)^2\right),
\end{aligned}$$

and elementary bounding arguments yield

$$1 - \left(1 - \left(\frac{K}{P-K}\right)^2\right)^K \leq 1 - \frac{r(\theta)}{q(\theta)^2} \leq 1 - \left(1 - \left(\frac{K}{P-2K}\right)^2\right)^K.$$

Pick a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying the equivalent conditions (19) and consider n sufficiently large in $\mathbb{N}_0$ so that $3K_n < P_n$. On that range, we replace θ by θ_n in the last chain of inequalities according to this scaling.

A standard sandwich argument will yield the desired equivalence (26) if we show that

$$1-\left(1-\left(\frac{K_n}{P_n-cK_n}\right)^2\right)^{K_n} \sim \frac{K_n^3}{P_n^2}, \quad c=1,2. \tag{A.1}$$

To do so we proceed as follows: Fix $c=1,2$. With

$$A_n(c) := \left(\frac{K_n}{P_n-cK_n}\right), \quad n=1,2,\dots$$

standard calculus yields

$$1-\left(1-\left(\frac{K_n}{P_n-cK_n}\right)^2\right)^{K_n} = K_n A_n(c)^2 \int_0^1 \left(1-A_n(c)^2 t\right)^{K_n-1} dt$$

on the appropriate range. The asymptotics

$$A_n(c)^2 = \left(\frac{K_n}{P_n-cK_n}\right)^2 \sim \left(\frac{K_n}{P_n}\right)^2 \quad \text{and} \quad K_n A_n(c)^2 \sim \frac{K_n^3}{P_n^2} \tag{A.2}$$

follow from (21), so that (A.1) will hold if we show that

$$\lim_{n\to\infty} \int_0^1 \left(1-A_n(c)^2 t\right)^{K_n-1} dt = 1. \tag{A.3}$$

By the first part of (A.2) we conclude from (21) that for all n sufficiently large in $\mathbb{N}_0$ we have $\sup_{0\le t\le 1}\left|1-A_n(c)^2 t\right| \le 1$. Therefore, the Bounded Convergence Theorem will yield (A.3) as soon as we establish

$$\lim_{n\to\infty} \left(1-A_n(c)^2 t\right)^{K_n-1} = 1, \quad 0\le t\le 1. \tag{A.4}$$

To that end, recall the decomposition

$$\log(1-x) = -\int_0^x \frac{1}{1-t}dt = -x-\Psi(x), \quad 0\le x<1 \tag{A.5}$$

where

$$\Psi(x) := \int_0^x \frac{t}{1-t}dt.$$

It is easy to check that

$$\lim_{x\downarrow 0} \frac{\Psi(x)}{x^2} = \frac{1}{2}. \tag{A.6}$$

Fix n sufficiently large in $\mathbb{N}_0$ as required above. For each t in the interval $(0,1]$, we use (A.5) to write

$$\begin{aligned}\big(1-A_n(c)^2t\big)^{K_n-1} &= e^{(K_n-1)\log\left(1-A_n(c)^2t\right)}\\ &= e^{-(K_n-1)A_n(c)^2t-(K_n-1)\Psi(A_n(c)^2t)}. \qquad \text{(A.7)}\end{aligned}$$

Returning to the second part of (A.2), we now use (19) and (21) to find

$$\lim_{n\to\infty} K_nA_n(c)^2 = \lim_{n\to\infty}\left(\frac{K_n^2}{P_n}\cdot\frac{K_n}{P_n}\right) = 0.$$

We immediately conclude $\lim_{n\to\infty}(K_n-1)A_n(c)^2 = 0$, whence

$$\lim_{n\to\infty}(K_n-1)\Psi(A_n(c)^2t) = \lim_{n\to\infty}(K_n-1)A_n(c)^2t\cdot\frac{\Psi(A_n(c)^2t)}{A_n(c)^2t} = 0$$

with the help of (A.6) in the last step. Finally, letting n go to infinity in (A.7), we readily get (A.4) as desired. ■