THE INSTITUTE FOR SYSTEMS RESEARCH

ISR TECHNICAL REPORT 2009-1

Zero-One Laws for Connectivity in Random Key Graphs

Osman Yagan and Armand Makowski

Zero-one laws for connectivity in random key graphs *

Osman Yağan and A.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.

February 9, 2009

Abstract

The random key graph, also known as the *uniform random intersection graph*, is a random graph induced by the random key predistribution scheme of Eschenauer and Gligor under the assumption of full visibility. We report on recent results concerning a conjectured zero-one law for graph connectivity.

Keywords: Wireless sensor networks, Key predistribution, Secure connectivity, Absence of isolated nodes, Zero-one laws, Poisson convergence.

1 Introduction

1.1 Background

A Wireless Sensor Network (WSN) is a collection of spatially distributed sensors with limited capabilities for computations and wireless communications. WSNs are being used in many areas including military applications such as battlefield surveillance, and civilian applications such as environment monitoring and traffic control. In general, sensors are deployed in a hostile area so that they are likely to be captured and used by an adversary, which makes the security a key issue for the success of these networks. Since the traditional methods for security have been found inadequate for such networks, the following random key predistribution scheme proposed by Eschenauer and Gligor [7] has instead received some attention: Before network deployment, each sensor is independently assigned K distinct cryptographic keys which are selected at random from a pool of P keys. These K keys constitute the key ring of the node and

*This work was supported by NSF Grant CCF-07290.

are inserted into its memory. 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 [7] for implementation details.

Under the assumption of *full visibility*, namely that nodes are all within communication range of each other, the constraint of being within transmission range is always in effect and a secure link can be established between two nodes whenever their key rings have at least one key in common. This notion of adjacency induces the *random key* graph $\mathbb{K}(n;(K,P))$ on the vertex set $\{1,\ldots,n\}$ where n is the number of sensor nodes; see Section 2 for precise definitions.

A basic question concerning the EG scheme is its ability to achieve *secure connectivity* among participating nodes in the sense that a *secure path* exists between any pair of nodes. Therefore, it is natural to seek conditions on n, K and P under which $\mathbb{K}(n;(K,P))$ is a connected graph with high probability – The availability of such conditions would provide an encouraging indication as to the feasibility of this distribution scheme in the context of wireless sensor networks. As explained in Section 3, this search has lead to *conjecturing* the following zero-one law for graph connectivity in $\mathbb{K}(n;(K.P))$: If we scale the parameters K and P with n according to

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{1}$$

for some sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$, then

$$\begin{aligned} &\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n;(K_n,P_n)) \text{ is connected}\right] \\ = &\begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty. \end{cases} \end{aligned} \tag{2}$$

This conjecture appeared independently in [1, 18].

To the best of the authors knowledge, the conjecture (1)-(2) proved to hold only for the cases where $P_n \ll n$; see Section 4 for a brief review of the recent work. In this paper, we complement the existing results concerning the conjecture by providing a proof for the case where $P_n = \Omega(n)$, i.e., when $P_n \geq \sigma n$ for some $\sigma > 0$.

The rest of the paper is organized as follows: In Section 2 we formally introduce the class of random key graphs. Section 4 is devoted to a brief review of recent results followed in Section 5 by the main result of the paper summarized as Theorem 5.1. A basic roadmap of the proof of Theorem 5.1 is provided in Section 6 where we identify the terms that need to become vanishingly small as n grows large. The needed bounding arguments to do so are developed in Sections 9, 10 and 11 and the final steps of the proof are then outlined in Section 12.

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 $\mathbb{E}$. Also, we use the notation $=_{st}$ to indicate distributional equality. 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 $K < P$. To lighten the notation we often group the integers P and K into the ordered pair $\theta \equiv (P, K)$.

For each node $i = 1, \ldots, n$, let $K_i(\theta)$ denote the random set of K distinct keys assigned to node i. We can think of $K_i(\theta)$ as an $\mathcal{P}_K$-valued rv where $\mathcal{P}_K$ denotes the collection of all subsets of $\{1, \ldots, P\}$ which contain exactly K elements – Obviously, we have $|\mathcal{P}_K| = \binom{P}{K}$. The rvs $K_1(\theta), \ldots, K_n(\theta)$ are assumed to be *i.i.d.* rvs, each of which is *uniformly* distributed over $\mathcal{P}_K$ with

$$\mathbb{P}[K_i(\theta) = S] = \binom{P}{K}^{-1}, \quad S \in \mathcal{P}_K \tag{3}$$

for all $i = 1, \ldots, n$. 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

$$K_i(\theta) \cap K_j(\theta) \neq \emptyset, \tag{4}$$

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 by $\mathbb{K}(n; \theta)$. For distinct $i, j = 1, \ldots, n$, it is a simple matter to check that

$$\mathbb{P}[K_i(\theta) \cap K_j(\theta) = \emptyset] = q(\theta) \tag{5}$$

with

$$q(\theta) = \begin{cases} 0 & \text{if } P < 2K \\ \frac{\binom{P-K}{K}}{\binom{P}{K}} & \text{if } 2K \leq P. \end{cases} \tag{6}$$

This expression and others given later are simple consequences of the often used fact that

$$\mathbb{P}[S \cap K_i(\theta) = \emptyset] = \frac{\binom{P-|S|}{K}}{\binom{P}{K}}, \quad i = 1, \ldots, n \tag{7}$$

for every subset S of $\{1, \ldots, P\}$ with $|S| \leq P - K$. The case $P < 2K$ is clearly not interesting: It corresponds to an edge existing between every pair of nodes, so that $\mathbb{K}(n; \theta)$ coincides with the completely regular graph $K_{n,n}$.

Random key graphs form a subclass in the family of *random intersection* graphs. However, the model adopted here differs from the random intersection

graphs discussed by Singer-Cohen et al. in [12, 16] where each node is assigned a key ring, one key at a time according to a Bernoulli-like mechanism (so that each key ring has a random size and has positive probability of being empty). Random key graphs are also called *uniform random intersection* graphs by some authors [1]. They have been discussed recently in several application contexts, e.g., security of wireless sensor networks [1] [5], clustering analysis [9] [10] and recommender systems using global filtering [13].

Throughout, with $n = 2, 3, \ldots$, and positive integers K and P such that $K \leq P$, let $P(n; \theta)$ denote the probability that the random key graph $\mathbb{K}(n; \theta)$ is connected, namely

$$P(n; \theta) := \mathbb{P}\left[\mathbb{K}(n; \theta) \text{ is connected}\right]$$

where it is understood that $\theta = (K, P)$.

3 Origins of the conjecture

As indicated earlier, we wish to select P and K so that $P(n; \theta)$ is as large (i.e., as close to one) as possible. In their original work, Eschenauer and Gligor [7] approached this issue as follows:
(i) Let $\mathbb{G}(n; p)$ denote the Erdős-Renyi graph on n vertices with edge probability p $(0 < p \leq 1)$ [2, 11]. Despite strong similarities, the random graph $\mathbb{K}(n; \theta)$ is *not* an Erdős-Renyi graph $\mathbb{G}(n; p)$. This is so because edge assignments are correlated in $\mathbb{K}(n; \theta)$ but independent in $\mathbb{G}(n; p)$. Yet, setting aside this fact, they boldly replaced $\mathbb{K}(n; \theta)$ by a proxy Erdős-Renyi graph $\mathbb{G}(n; p)$ with p and θ are related through

$$p = 1 - q(\theta). \tag{8}$$

This constraint ensures that link assignment probabilities in $\mathbb{K}(n; \theta)$ and $\mathbb{G}(n; p)$ coincide.
(ii) In Erdős-Renyi graphs the property of graph connectivity is known to exhibit the following zero-one law [2]: If we scale the edge assignment probability p according to

$$p_n = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{9}$$

for some sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$, then

$$\lim_{n \to \infty} \mathbb{P}\left[\mathbb{G}(n; p_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } \lim_{n \to \infty} \alpha_n = -\infty \\ \\ 1 & \text{if } \lim_{n \to \infty} \alpha_n = +\infty. \end{cases} \tag{10}$$

(iii) Under the substitution (8), these classical results suggest scaling the parameters K and P with n according to

$$1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{11}$$

for some sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$. In view of (10) it is then not too unreasonable to expect that the following zero-one law

$$\lim_{n\to\infty} P(n;\theta_n) = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty \end{cases} \tag{12}$$

should hold (possibly under some additional assumptions).

Of course, for this approach to be operationally useful, a good approximation to the right handside of (8) is needed. Eschenauer and Gligor provided such an approximation with the help of Stirling's formula. However, as already indicated by DiPietro et al. [4], [5], it is easy to check that

$$1 - \frac{\binom{P-K}{K}}{\binom{P}{K}} \simeq \frac{K^2}{P} \tag{13}$$

under reasonable assumptions. Thus, if instead of scaling the parameters according to (11), we scale them according to

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{14}$$

it is natural to conjecture that the zero-one law (12) should still hold.

4 Related work

Recent results concerning the conjectured zero-one law (1)-(2) are now surveyed: Di Pietro et al. have shown [5, Thm. 4.6] that for large n, the random key graph will be connected with very high probability if P_n and K_n are selected such that

$$K_n \geq 5, \ P_n \geq n \quad \text{and} \quad \frac{K_n^2}{P_n} \sim c \ \frac{\log n}{n} \tag{15}$$

as soon as $c \geq 16$.[1] They also observe that for large n, the random key graph will be disconnected with very high probability if the scaling satisfies

$$\frac{K_n^2}{P_n} = o\left(\frac{\log n}{n}\right).$$

In [1] Blackburn and Gerke have recently obtained a generalization of the results by Di Pietro et al.. They showed [1, Thm. 5] under the conditions

$$K_n \geq 2 \quad \text{and} \quad n \leq P_n, \quad n = 1, 2, \ldots \tag{16}$$

that

$$\lim_{n\to\infty} P(n;\theta_n) = 0 \quad \text{if} \quad \limsup_{n\to\infty} \frac{K_n^2}{P_n} \frac{n}{\log n} < 1 \tag{17}$$

[1] In the conference version of this work [4, Thm. 4.6] the result is claimed to hold for $c > 8$.

and

$$\lim_{n\to\infty} P(n;\theta_n) = 1 \quad \text{if} \quad \liminf_{n\to\infty} \frac{K_n^2}{P_n}\frac{n}{\log n} > 1. \tag{18}$$

In the process of establishing (17)-(18), they also showed [1, Thm. 3] that the conjectured zero-one law (1)-(2) indeed holds in the special case $K_n = 2$ for all $n = 1, 2, \ldots$ *without* any constraints on the size of the key pools. Equipped with this result, it is now a small step to conclude (as they do) that (1)-(2) does hold when $P_n = o\left(\frac{n}{\log n}\right)$ with $2 \le K_n \le P_n$. In fact, a little more than that can be said: If for some $\epsilon \in (0, 4)$ it holds that $P_n \le \frac{(4-\epsilon)n}{\log n}$, we get (with $K_n = 2$)

$$\frac{4n}{P_n} - \log n \ge \frac{\epsilon}{4-\epsilon}\log n.$$

With ϵ in the given range, the last expression tends to ∞ as n grows large and we conclude that the conjecture (1)-(2) does hold whenever

$$P_n \le \frac{(4-\epsilon)n}{\log n}$$

for some ϵ in $(0, 4)$.

5 The main result

Any pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ defines a *scaling*, and we can always associate with it a sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ through the relation

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{19}$$

Just set

$$\alpha_n := n\frac{K_n^2}{P_n} - \log n, \quad n = 1, 2, \ldots$$

We refer to this sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ as the *deviation function* associated with the scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$. As the terminology suggests, the deviation function measures by how much the scaling deviates from the critical scaling $\frac{\log n}{n}$.

A scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ is said to be *admissible* if

$$K_n \le P_n, \quad n = 1, 2, \ldots \tag{20}$$

and

$$2 \le K_n \tag{21}$$

for *all* $n = 1, 2, \ldots$ *sufficiently* large. The main result of this paper can now be stated as follows.

Theorem 5.1 *Consider an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ with deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ determined through (19). We have*

$$\lim_{n\to\infty} P(n;\theta_n) = 0 \quad \textit{if } \lim_{n\to\infty} \alpha_n = -\infty. \tag{22}$$

On the other hand, if there exists some $\sigma > 0$ such that

$$\sigma n \le P_n \tag{23}$$

for all $n = 1, 2, \ldots$ sufficiently large, we have

$$\lim_{n\to\infty} P(n;\theta_n) = 1 \quad \textit{if } \lim_{n\to\infty} \alpha_n = \infty. \tag{24}$$

The condition (23) is sometimes expressed as $P_n = \Omega(n)$ and is weaker than the growth condition at (16) used by Blackburn and Gerke [1]. It is also easy to check that Theorem 5.1 implies the zero-one law (17)-(18).

The one-law in Theorem 5.1 cannot hold if the condition (21) fails. This is a simple consequence of the following observation.

Lemma 5.2 *For any mapping $P : \mathbb{N}_0 \to \mathbb{N}_0$ for which the limit $\lim_{n\to\infty} P_n$ exists (possibly infinite), we have*

$$\lim_{n\to\infty} P(n;(1,P_n)) = \begin{cases} 0 & \textit{if } \lim_{n\to\infty} P_n > 1 \\ \\ 1 & \textit{if } \lim_{n\to\infty} P_n = 1. \end{cases} \tag{25}$$

Proof. For $n = 2, 3, \ldots$ and any positive integer P_n, the graph $\mathbb{K}(n;(1,P_n))$ is connected if and only if all nodes choose the *same* key. This event happens with probability $P_n^{-(n-1)}$. The conclusion is now immediate once we observe that the condition $\lim_{n\to\infty} P_n = 1$ (resp. $\lim_{n\to\infty} P_n > 1$) requires $P_n = 1$ (resp. $P_n \ge 2$) for all $n = 1, 2, \ldots$ sufficiently large owing to P_n being integer. ■

A typical example where condition (21) fails can be constructed as follows: With $c > -1$, take

$$K_n = 1, \; P_n = \left\lceil \frac{1}{c+1} \frac{n}{\log n} \right\rceil, \quad n = 1, 2, \ldots.$$

In that case $\alpha_n \sim c \log n$.

6 A roadmap for the proof of Theorem 5.1

Fix $n = 2, 3, \ldots$ and consider positive integers K and P such that $2 \leq K \leq P$. We define the events

$$C_n(\theta) := [\mathbb{K}_n(\theta) \text{ is connected}]$$

and

$$I_n(\theta) := [\mathbb{K}_n(\theta) \text{ contains no isolated nodes}] .$$

If the random key graph $\mathbb{K}(n;\theta)$ is connected, then it does not contain isolated nodes, whence $C_n(\theta)$ is a subset of $I_n(\theta)$, and the conclusions

$$\mathbb{P}[C_n(\theta)] \leq \mathbb{P}[I_n(\theta)] \tag{26}$$

and

$$\mathbb{P}[C_n(\theta)^c] = \mathbb{P}[C_n(\theta)^c \cap I_n(\theta)] + \mathbb{P}[I_n(\theta)^c] \tag{27}$$

obtain.

In [18], we established the following zero-one law for the absence of isolated nodes by the method of first and second moments applied to the number of isolated nodes. This result was also obtained independently by Blackburn and Gerke [1].

Theorem 6.1 *For any admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$, it holds that*

$$\lim_{n\to\infty} \mathbb{P}[I_n(\theta_n)] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty \end{cases} \tag{28}$$

where the deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ is determined through (19).

Taken together with Theorem 6.1, the relations (26) and (27) pave the way to proving Theorem 5.1. Indeed, pick an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ with deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$. If $\lim_{n\to\infty} \alpha_n = -\infty$, then $\lim_{n\to\infty} \mathbb{P}[I_n(\theta_n)] = 0$ by the zero-law for the absence of isolated nodes, whence $\lim_{n\to\infty} \mathbb{P}[C_n(\theta_n)] = 0$ with the help of (26). If $\lim_{n\to\infty} \alpha_n = \infty$, then $\lim_{n\to\infty} \mathbb{P}[I_n(\theta_n)] = 1$ by the one-law for the absence of isolated nodes, and the desired conclusion $\lim_{n\to\infty} \mathbb{P}[C_n(\theta_n)] = 1$ (or equivalently, $\lim_{n\to\infty} \mathbb{P}[C_n(\theta_n)^c] = 0$) will follow via (27) if we show that

$$\lim_{n\to\infty} \mathbb{P}[C_n(\theta_n)^c \cap I_n(\theta_n)] = 0. \tag{29}$$

We shall do this by finding a sufficiently tight upper bound on the probability in (29) and then showing that it goes to zero as well. While the additional condition (23) plays a crucial role in carrying out this argument, a number of additional assumptions will be imposed on the admissible scaling under consideration. This is done mostly for technical reasons in that it leads to simpler proofs. Eventually these additional conditions will be removed to ensure the desired final result, namely (24) under (23), e.g., see Section 7 for details.

With this in mind, the admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ is said to be *strongly admissible* if its deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies the additional growth condition

$$\alpha_n = o(n). \tag{30}$$

Strong admissibility has the following useful implications: Under (30) it is always the case from (19) that

$$\lim_{n\to\infty} \frac{K_n^2}{P_n} = 0. \tag{31}$$

Since $1 \leq K_n \leq K_n^2$ for all $n = 1, 2, \ldots$, this last convergence implies

$$\lim_{n\to\infty} \frac{K_n}{P_n} = 0 \tag{32}$$

and

$$\lim_{n\to\infty} P_n = \infty. \tag{33}$$

As a result,

$$2K_n \leq P_n \tag{34}$$

for all $n = 1, 2, \ldots$ sufficiently large, and the random key graph does not degenerate into a completely regular graph under a strongly admissible scaling. We shall also make use of the fact that (32) is equivalent to

$$\lim_{n\to\infty} \frac{P_n}{K_n} = \infty. \tag{35}$$

Finally in Lemma 8.3 we show that (31) suffices to imply

$$1 - q(\theta_n) \sim \frac{K_n^2}{P_n}. \tag{36}$$

This is discussed in Section 8, and provides the appropriate version of (13).

7 A reduction step

The relevance of the notion of strong admissibility flows from the following fact.

Lemma 7.1 *Consider an admissible scaling $K, P : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation sequence $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies*

$$\lim_{n\to\infty} \alpha_n = \infty. \tag{37}$$

Assume there exists some $\sigma > 0$ such that

$$\sigma n \leq P_n \tag{38}$$

for all $n = 1, 2, \ldots$ sufficiently large. Then, there always exists an admissible scaling $\tilde{K}, \tilde{P} : \mathbb{N}_0 \to \mathbb{N}_0$ with

$$\tilde{K}_n \leq K_n \quad \text{and} \quad \tilde{P}_n = P_n, \quad n = 1, 2, \ldots \tag{39}$$

whose deviation function $\tilde{\alpha} : \mathbb{N}_0 \to \mathbb{R}$ satisfies both conditions

$$\lim_{n \to \infty} \tilde{\alpha}_n = \infty \tag{40}$$

and

$$\tilde{\alpha}_n = o(n). \tag{41}$$

Proof. For each $n = 1, 2, \ldots$, we set

$$K_n^\star := \sqrt{P_n \cdot \frac{\log n + \alpha_n^\star}{n}}.$$

where

$$\alpha_n^\star := \min(\alpha_n, \log n)$$

The properties

$$\lim_{n \to \infty} \alpha_n^\star = \infty \tag{42}$$

and

$$\alpha_n^\star = o(n) \tag{43}$$

are immediate by construction.

Now define the scaling $\tilde{K}, \tilde{P} : \mathbb{N}_0 \to \mathbb{N}_0$ by

$$\tilde{K}_n := \lceil K_n^\star \rceil, \ \tilde{P}_n = P_n, \quad n = 1, 2, \ldots \tag{44}$$

We get $K_n^\star \leq K_n$ for all $n = 1, 2, \ldots$ since $\alpha_n^\star \leq \alpha_n$, whence $\tilde{K}_n \leq K_n$ by virtue of the fact that K_n is always an integer. This establishes (39).

Next, observe that $\tilde{K}_n = 1$ if and only $K_n^\star \leq 1$, a condition which occurs only when

$$P_n (\log n + \alpha_n^\star) \leq n. \tag{45}$$

This last inequality can only hold for a finite number of values of n. Otherwise, there would exist a countably infinite subset N of $\mathbb{N}_0$ such that both (38) and (45) simultaneously hold on N. In that case, we conclude that

$$\sigma (\log n + \alpha_n^\star) \leq 1, \quad n \in N$$

and this is a clear impossibility in view of (42) (which implies $\alpha_n^\star > 0$ for all n suffiiciently large). Together with (39) this establishes the admissibility of the scaling $\tilde{K}, \tilde{P} : \mathbb{N}_0 \to \mathbb{N}_0$.

Fix $n = 1, 2, \ldots$. The definitions imply $K_n^\star \le \tilde{K}_n < 1 + K_n^\star$ and upon squaring we get the inequalities

$$P_n \cdot \frac{\log n + \alpha_n^\star}{n} \le \tilde{K}_n^2 \tag{46}$$

and

$$\tilde{K}_n^2 < 1 + 2\sqrt{P_n \cdot \frac{\log n + \alpha_n^\star}{n}} + P_n \cdot \frac{\log n + \alpha_n^\star}{n}. \tag{47}$$

The deviation sequence $\tilde{\alpha} : \mathbb{N}_0 \to \mathbb{R}$ of the newly defined scaling is determined through

$$\frac{\tilde{K}_n^2}{\tilde{P}_n} = \frac{\log n + \tilde{\alpha}_n}{n}, \quad n = 1, 2, \ldots.$$

By comparing with (46) and (47) we conclude that

$$\alpha_n^\star \le \tilde{\alpha}_n \tag{48}$$

and

$$\frac{\log n + \tilde{\alpha}_n}{n} < \frac{1}{P_n} + 2\sqrt{\frac{1}{P_n} \cdot \frac{\log n + \alpha_n^\star}{n}} + \frac{\log n + \alpha_n^\star}{n},$$

whence

$$\frac{\alpha_n^\star}{n} \le \frac{\tilde{\alpha}_n}{n} < \frac{1}{P_n} + 2\sqrt{\frac{1}{P_n} \cdot \frac{\log n + \alpha_n^\star}{n}} + \frac{\alpha_n^\star}{n}. \tag{49}$$

It is now plain from (42) and (48) that (40) holds. Next, letting n go to infinity in (49) and using (43) we conclude to (41) since $\lim_{n\to\infty} P_n = \infty$ by virtue of (38). ■

This construction also works with

$$\alpha_n^\star = \min\left(\alpha_n, \omega_n\right), \quad n = 1, 2, \ldots$$

for any sequence $\omega : \mathbb{N}_0 \to \mathbb{R}_+$ such that $\lim_{n\to\infty} \omega_n = \infty$ and $\omega_n = o(n)$, e.g., $\omega_n = n^\delta$ for some $0 < \delta < 1$.

We close with a key technical consequence of Lemma 7.1: By construction the scaling $\tilde{K}, \tilde{P} : \mathbb{N}_0 \to \mathbb{N}_0$ *is* a strongly admissible scaling and an easy coupling argument based on (39) implies

$$P(n; \tilde{\theta}_n) \le P(n; \theta_n), \quad n = 2, 3, \ldots$$

Thus, we need only show (24) under (23) for strongly admissible scalings. As a result, in view of the discussion leading to (29) it suffices to establish the following result, to which the remainder of the paper is devoted.

Proposition 7.2 *Consider any strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. Then, it holds that*

$$\lim_{n\to\infty} \mathbb{P}\left[C_n(\theta_n)^c \cap I_n(\theta_n)\right] = 0 \tag{50}$$

under the condition (23).

Proposition 7.2 shows that in random key graphs, graph connectivity is asymptotically equivalent to the absence of isolated nodes under any strongly admissible scaling whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$ under the condition (23).

8 The equivalence (36)

To establish the equivalence (36) we start with simple bounds which prove useful in a number of places.

Lemma 8.1 *For positive integers K, L and P such that $K + L \leq P$, we have*

$$\left(1 - \frac{L}{P - K}\right)^K \leq \frac{\binom{P-L}{K}}{\binom{P}{K}} \leq \left(1 - \frac{L}{P}\right)^K, \tag{51}$$

whence

$$\frac{\binom{P-L}{K}}{\binom{P}{K}} \leq e^{-K \cdot \frac{L}{P}}. \tag{52}$$

Proof. Under the condition $K + L \leq P$, the relation

$$\frac{\binom{P-L}{K}}{\binom{P}{K}} = \frac{(P-L)!}{(P-L-K)!} \cdot \frac{(P-K)!}{P!} \tag{53}$$

holds with

$$\frac{(P-jL)!}{(P-jL-K)!} = \prod_{\ell=0}^{K-1} (P - jL - \ell), \quad j = 0, 1.$$

Upon substituting we find

$$\frac{\binom{P-L}{K}}{\binom{P}{K}} = \prod_{\ell=0}^{K-1} \left(1 - \frac{L}{P-\ell}\right) \tag{54}$$

and a straightforward bounding argument yields the bounds (51). The passage to (52) follows from the inequality $1 - x \leq e^{-x}$ valid for $0 \leq x \leq 1$. ■

Applying Lemma 8.1. to the expression (6) yields the following bounds.

Lemma 8.2 *With positive integers K and P such that $2K \leq P$, we have*

$$1 - e^{-\frac{K^2}{P}} \leq 1 - q(\theta) \leq \frac{K^2}{P - K}. \tag{55}$$

Proof. Lemma 8.1 (with $L = K$) yields the bounds

$$1 - e^{-\frac{K^2}{P}} \leq 1 - q(\theta) \leq 1 - \left(1 - \frac{K}{P-K}\right)^K. \tag{56}$$

The conclusion (55) is now immediate once we note that

$$1 - \left(1 - \frac{K}{P-K}\right)^K = \int_{1-\frac{K}{P-K}}^1 Kt^{K-1}dt \leq \frac{K^2}{P-K}$$

by a crude bounding argument. ■

A little bit more than (36) can be said.

Lemma 8.3 *Consider a scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ such that*

$$2K_n \leq P_n \tag{57}$$

for all n sufficiently large. Then, we have

$$\lim_{n\to\infty} q(\theta_n) = 1 \tag{58}$$

if and only if

$$\lim_{n\to\infty} \frac{K_n^2}{P_n} = 0, \tag{59}$$

and under either condition the asymptotic equivalence

$$1 - q(\theta_n) \sim \frac{K_n^2}{P_n} \tag{60}$$

holds.

As noted already at the end of Section 6, condition (57) is automatically implied by (59), a condition which itself holds for any strongly admissible scaling.

On several occasions, we will rely on (60) through the following equivalent formulation: For every δ in $(0, 1)$ there exists a finite integer $n^\star(\delta)$ such that

$$(1-\delta)\frac{K_n^2}{P_n} \leq 1 - q(\theta_n) \leq (1+\delta)\frac{K_n^2}{P_n} \tag{61}$$

whenever $n \geq n^\star(\delta)$.

Proof. On the range where (57) holds, Lemma 8.2 yields

$$1 - e^{-\frac{K_n^2}{P_n}} \leq 1 - q(\theta_n) \leq \frac{K_n^2}{P_n - K_n}. \tag{62}$$

Multiply (62) by $\frac{P_n}{K_n^2}$ and let n go to infinity in the resulting set of inequalities. Under (59), we get

$$\lim_{n\to\infty} \frac{P_n}{K_n^2} \cdot \left(1 - e^{-\frac{K_n^2}{P_n}}\right) = 1 \tag{63}$$

from the elementary fact $\lim_{t\downarrow 0} \frac{1-e^{-t}}{t} = 1$, while

$$\lim_{n\to\infty} \frac{P_n}{K_n^2} \cdot \frac{K_n^2}{P_n - K_n} = \lim_{n\to\infty} \frac{P_n}{P_n - K_n} = 1 \tag{64}$$

by virtue of (32). (which is implied by (59)). The asymptotic equivalence (60) follows, and the validity of (58) is immediate.

Conversely, if $\lim_{n\to\infty} q(\theta_n) = 1$, then (62) readily implies $\lim_{n\to\infty} e^{-\frac{K_n^2}{P_n}} = 1$, and we obtain (59). ■

9 A basic union bound

Proposition 7.2 will be established with the help of a union bound for the probability appearing at (50) – The approach is similar to the one used for proving the one-law for connectivity in Erdős-Renyi graphs graphs [2, p. 164] [17, p. 304]:

Fix $n = 2, 3, \ldots$ and consider positive integers K and P such that $2K \leq P$. For any non-empty subset S of nodes, i.e., $S \subseteq \{1, \ldots, n\}$, we define the graph $\mathbb{K}(n;\theta)(S)$ (with vertex set S) as the subgraph of $\mathbb{K}(n;\theta)$ restricted to the nodes in S. We say that S is *isolated* in $\mathbb{K}(n;\theta)$ if there there are no edges (in $\mathbb{K}(n;\theta)$) between the nodes in S and the nodes in the complement $S^c = \{1, \ldots, n\} - S$. This is characterized by

$$K_i(\theta) \cap K_j(\theta) = \emptyset, \quad i \in S,\ j \in S^c.$$

With each non-empty subset S of nodes, we associate several events of interest: Let $C_n(\theta; S)$ denote the event that the subgraph $\mathbb{K}(n;\theta)(S)$ is itself connected. The event $C_n(\theta; S)$ is completely determined by the rvs $\{K_i(\theta),\ i \in S\}$. We also introduce the event $B_n(\theta; S)$ to capture the fact that S is isolated in $\mathbb{K}(n;\theta)$, i.e.,

$$B_n(\theta; S) := \left[K_i(\theta) \cap K_j(\theta) = \emptyset, \quad i \in S,\ j \in S^c\right].$$

Finally, we set

$$A_n(\theta; S) := C_n(\theta; S) \cap B_n(\theta; S).$$

The starting point of the discussion is the following basic observation: If $\mathbb{K}(n;\theta)$ is *not* connected and yet has no isolated nodes, then there must exist a non-empty subset S of nodes with $|S| \geq 2$ such that $\mathbb{K}(n;\theta)(S)$ is connected while S is isolated in $\mathbb{K}(n;\theta)$. This is captured by the inclusion

$$C_n(\theta)^c \cap I_n(\theta) \subseteq \cup_{S\in\mathcal{N}:\ |S|\geq 2}\ A_n(\theta; S). \tag{65}$$

with $\mathcal{N}$ denoting the collection of all non-empty subsets of $\{1,\ldots,n\}$. A moment of reflection should convince the reader that this union need only be taken over all non-empty subsets S of $\{1,\ldots,n\}$ with $2 \leq |S| \leq \lfloor \frac{n}{2} \rfloor$. Then, a standard union bound argument immediately gives

$$\begin{aligned} \mathbb{P}\left[C_n(\theta)^c \cap I_n(\theta)\right] &\leq \sum_{S\in\mathcal{N}:2\leq|S|\leq\lfloor\frac{n}{2}\rfloor} \mathbb{P}\left[A_n(\theta;S)\right] \\ &= \sum_{r=2}^{\lfloor\frac{n}{2}\rfloor}\left(\sum_{S\in\mathcal{N}_r}\mathbb{P}\left[A_n(\theta;S)\right]\right). \end{aligned} \tag{66}$$

Now, for each $r = 1,\ldots,n$, we simplify the notation by writing $A_{n,r}(\theta) := A_n(\theta;\{1,\ldots,r\})$, $B_{n,r}(\theta) := B_n(\theta;\{1,\ldots,r\})$ and $C_r(\theta) := C_n(\theta;\{1,\ldots,r\})$. For $r = n$ this notation is consistent with $C_n(\theta)$ as defined in Section 6. Under the enforced assumptions, it is a simple matter to check by exchangeability that

$$\mathbb{P}\left[A_n(\theta;S)\right] = \mathbb{P}\left[A_{n,r}(\theta)\right], \quad S \in \mathcal{N}_r$$

where $\mathcal{N}_r$ denotes the collection of all subsets of $\{1,\ldots,n\}$ with exactly r elements, and the expression

$$\sum_{S\in\mathcal{N}_r}\mathbb{P}\left[A_n(\theta;S)\right] = \binom{n}{r}\mathbb{P}\left[A_{n,r}(\theta)\right] \tag{67}$$

follows as we recall that $|\mathcal{N}_r| = \binom{n}{r}$. Substituting into (66) we obtain the key bound

$$\mathbb{P}\left[C_n(\theta)^c \cap I_n(\theta)\right] \leq \sum_{r=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\theta)\right]. \tag{68}$$

Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ as in the statement of Proposition 7.2. In the right hand side of (68) we substitute θ by θ_n by means of this strongly admissible scaling. The proof of Proposition 7.2 will be completed once we show that

$$\lim_{n\to\infty}\sum_{r=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{r}\mathbb{P}\left[A_{n,r}(\theta_n)\right] = 0 \tag{69}$$

under the appropriate conditions. This approach was used to establish the one-law in Erdős-Renyi graphs [2] [17] where simple bounds can be derived for the probability terms in (69). Our situation is technically more involved and requires more delicate bounding arguments as becomes apparent in the forthcoming sections.

10 Bounding the probabilities $\mathbb{P}\left[A_{n,r}(\theta)\right]$ $(r = 1,\ldots,n)$

Again consider positive integers K and P such that $2K \leq P$. Fix $n = 2,3,\ldots$ and pick $r = 1,\ldots,n-1$. In the course of evaluating $\mathbb{P}\left[A_{n,r}(\theta)\right]$, we shall make

use of the rv $U_r(\theta)$ given by

$$U_r(\theta) := \left|\cup_{i=1}^{r} K_i(\theta)\right|. \tag{70}$$

It is always the case that $U_r(\theta) \leq P$. However, the equivalence

$$B_{n,r}(\theta) = [(\cup_{i=1}^{r} K_i(\theta)) \cap K_j(\theta) = \emptyset,\ j = r+1, \ldots n]$$

implies that the set of nodes $\{1, \ldots, r\}$ *cannot* be isolated in $\mathbb{K}(n;\theta)$ if $P - U_r(\theta) < K$, i.e.,

$$B_{n,r}(\theta) \cap [P - U_r(\theta) < K] = \emptyset.$$

Hence, under the enforced assumptions on the rvs $K_1(\theta), \ldots, K_n(\theta)$, we readily obtain the expression

$$\mathbb{P}\left[B_{n,r}(\theta) | K_i(\theta),\ i = 1, \ldots, r\right] = \left(\frac{\binom{P-U_r(\theta)}{K}}{\binom{P}{K}}\right)^{n-r} \qquad a.s.$$

on the event $[U_r(\theta) \leq P - K]$.

As mentioned earlier, the event $C_r(\theta)$ is determined by the rvs $K_1(\theta), \ldots, K_r(\theta)$. Upon conditioning on these rvs, we then conclude that

$$\begin{aligned} \mathbb{P}\left[A_{n,r}(\theta)\right] &= \mathbb{P}\left[C_r(\theta) \cap B_{n,r}(\theta)\right] \\ &= \mathbb{E}\left[\mathbf{1}\left[C_r^{\star}(\theta)\right] \cdot \left(\frac{\binom{P-U_r(\theta)}{K}}{\binom{P}{K}}\right)^{n-r}\right] \end{aligned}$$

with

$$C_r^{\star}(\theta) := C_r(\theta) \cap [U_r(\theta) \leq P - K].$$

The bound

$$\mathbb{P}\left[A_{n,r}(\theta)\right] \leq \mathbb{E}\left[\mathbf{1}\left[C_r^{\star}(\theta)\right] \cdot e^{-(n-r)\frac{K}{P} \cdot U_r(\theta)}\right] \tag{71}$$

follows by applying (52) in Lemma 8.1.

The constraints

$$K \leq U_r(\theta) \leq \min\left(rK, P\right) \tag{72}$$

automatically imply $U_r(\theta) \leq P - K$ whenever $rK \leq P - K$, i.e., $(r+1)K \leq P$. Thus,

$$C_r^{\star}(\theta) = C_r(\theta), \quad r = 1, \ldots, r_n(\theta) \tag{73}$$

where we have set

$$r_n(\theta) := \min\left(r(\theta), \left\lfloor \frac{n}{2} \right\rfloor\right) \quad \text{with} \quad r(\theta) := \left\lfloor \frac{P}{K} \right\rfloor - 1.$$

This discussion already brings out a number of items that are likely to require some attention: We will need to device good bounds for the probabilities $\mathbb{P}\left[C_r(\theta)\right]$ and $\mathbb{P}\left[C_r^{\star}(\theta)\right]$. Also some of the distributional properties of the rv $U_r(\theta)$ are expected to play a role. Finally, different arguments are probably needed for the ranges $1 \leq r \leq r_n(\theta)$ and $r_n(\theta) < r \leq \lfloor \frac{n}{2} \rfloor$.

The next result shows that the probability of $C_r(\theta)$ can indeed be bounded in terms of known quantities.

Lemma 10.1 *For each $r = 2, \ldots, n$, we have*

$$\mathbb{P}\left[C_r(\theta)\right] \leq r^{r-2}\left(1 - q(\theta)\right)^{r-1}. \tag{74}$$

The basic idea behind this bound is as in Erdős-Renyi graphs [2] where the analog of (74) holds with $1 - q(\theta)$ playing the role of probability of link assignment.

Proof. If $\mathbb{K}(n;\theta)(S)$ (with $S = \{1, \ldots, r\}$) is a connected graph, then it must contain a spanning tree on S. As a result, with $\mathcal{T}_r$ denoting the collection of all trees on the vertex set $\{1, \ldots, r\}$, we find

$$\mathbb{P}\left[C_r(\theta)\right] \leq \sum_{T \in \mathcal{T}_r} \mathbb{P}\left[T \subset \mathbb{K}(n;\theta)(S)\right] \tag{75}$$

by a union bound argument where the notation $T \subset \mathbb{K}(n;\theta)(S)$ indicates that the tree T is a subgraph of $\mathbb{K}(n;\theta)(S)$.

Each tree T in $\mathcal{T}_r$ is uniquely determined by $r - 1$ edges. Edge assignments being *pairwise* independent in $\mathbb{K}(n;\theta)$ [18, **?**], we readily conclude that

$$\mathbb{P}\left[T \subset \mathbb{K}(n;\theta)(S)\right] = \left(1 - q(\theta)\right)^{r-1}, \quad T \in \mathcal{T}_r. \tag{76}$$

This can be done by an easy induction argument on r. By Cayley's formula there are r^{r-2} trees on r vertices, i.e., $|\mathcal{T}_r| = r^{r-2}$, and (74) follows from (75) via (76). ■

The bound (71) and the inequality $U_r(\theta) \geq K$ together imply

$$\begin{aligned} \mathbb{P}\left[A_{n,r}(\theta)\right] &\leq \mathbb{P}\left[C_r(\theta)\right] \cdot e^{-(n-r)\frac{K^2}{P}} \\ &\leq r^{r-2}\left(1 - q(\theta)\right)^{r-1} \cdot e^{-(n-r)\frac{K^2}{P}} \end{aligned} \tag{77}$$

as we make use of Lemma 10.1 in the last step. Unfortunately, this bound turns out to be too loose for our purposes. As this can be traced to the crude lower bound used for $U_r(\theta)$, we expect that these bounds can be improved by taking into account the distributional properties of the rv $U_r(\theta)$. This step is taken in the next section.

11 The tail of the rv $U_r(\theta)$ and improved bounds

Consider positive integers K and P such that $K \leq P$. Rough estimates will suffice to get the needed information regarding the distribution of the rv $U_r(\theta)$. This is the content of the next result.

Lemma 11.1 *For all $r = 1, 2, \ldots$, the bound*

$$\mathbb{P}\left[U_r(\theta) \leq x\right] \leq \binom{P}{x} \left(\frac{\binom{x}{K}}{\binom{P}{K}} \right)^r \tag{78}$$

holds whenever $x = K, \ldots, \min(rK, P)$.

Proof. For a given x in the prescribed range, we note that $U_r(\theta) \leq x$ implies that $\cup_{i=1}^r K_i(\theta)$ is contained in some set S of size x, so that

$$[U_r(\theta) \leq x] \subseteq \bigcup_{S \in \mathcal{P}_x} [\cup_{i=1}^r K_i(\theta) \subseteq S].$$

A standard union bound argument gives

$$\begin{aligned} \mathbb{P}\left[U_r(\theta) \leq x\right] &\leq \sum_{S \in \mathcal{P}_x} \mathbb{P}\left[\cup_{i=1}^r K_i(\theta) \subseteq S\right] \\ &= \sum_{S \in \mathcal{P}_x} \mathbb{P}\left[K_i(\theta) \subseteq S,\ i = 1, \ldots, r\right] \\ &= \sum_{S \in \mathcal{P}_x} \prod_{i=1}^r \mathbb{P}\left[K_i(\theta) \subseteq S\right] \\ &= \sum_{S \in \mathcal{P}_x} \left(\mathbb{P}\left[K_1(\theta) \subseteq S\right]\right)^r \end{aligned} \tag{79}$$

under the enforced assumptions on the rvs $K_1(\theta), \ldots, K_n(\theta)$.

Since every subset of size x contain $\binom{x}{K}$ further subsets of size K, we get

$$\mathbb{P}\left[K_1(\theta) \subseteq S\right] = \frac{\binom{x}{K}}{\binom{P}{K}}, \quad S \in \mathcal{P}_x.$$

Reporting this fact into (79) we readily obtain (78) from the fact $|\mathcal{P}_x| = \binom{P}{x}$. ■

Under the conditions of validity for (78) we note that

$$\frac{\binom{x}{K}}{\binom{P}{K}} = \prod_{\ell=0}^{K-1} \left(\frac{x - \ell}{P - \ell} \right) \leq \left(\frac{x}{P} \right)^K$$

since $\frac{x-\ell}{P-\ell}$ decreases as ℓ increases from $\ell = 0$ to $\ell = K - 1$. Reporting into (78) we conclude to a somewhat looser but simpler bound.

Lemma 11.2 *For all $r = 1, 2, \ldots$, the bounds*

$$\mathbb{P}\left[U_r(\theta) \leq x\right] \leq \binom{P}{x} \left(\frac{x}{P} \right)^{rK} \tag{80}$$

holds whenever $x = K, \ldots, \min(rK, P)$.

The bounds (78) and (80) trivially hold with $\mathbb{P}[U_r(\theta) \le x] = 0$ when $x = 1, \ldots, K-1$ since we always have $U_r(\theta) \ge K$. We shall make repeated use of this fact as follows: For all $n, r = 1, 2, \ldots$, with $r < n$, we have

$$\begin{aligned} \binom{n}{r} \mathbb{P}[U_r(\theta) \le x] &\le \binom{n}{r}\binom{P}{x}\left(\frac{x}{P}\right)^{rK} \\ &\le \binom{\lfloor P/\sigma \rfloor}{r}\binom{P}{x}\left(\frac{x}{P}\right)^{rK} \end{aligned} \tag{81}$$

on the range $x = 1, \ldots, \min(rK, P)$ *whenever* $\sigma n \le P$ for some $\sigma > 0$ (a condition needed only for the last step). Note that the condition $n\sigma \le P$ also implies $n \le \lfloor \frac{P}{\sigma} \rfloor$ owing to n being an integer.

We are now in a position to improve on the bound (77): Fix $n = 2, 3, \ldots$ and pick $r = 2, \ldots, n-1$. For each positive integer x, the decomposition

$$\begin{aligned} \mathbb{P}[A_{n,r}(\theta)] &= \mathbb{P}[C_r(\theta) \cap B_{n,r}(\theta)] \\ &= \mathbb{P}[C_r(\theta) \cap B_{n,r}(\theta) \cap E_r(\theta; x)] \\ &\quad + \mathbb{P}[C_r(\theta) \cap B_{n,r}(\theta) \cap E_r(\theta; x)^c] \end{aligned} \tag{82}$$

holds where the event $E_r(\theta; x)$ is given by

$$E_r(\theta; x) := [U_r(\theta) \le x].$$

The arguments leading to (71) also yield

$$\begin{aligned} & \mathbb{P}[C_r(\theta) \cap B_{n,r}(\theta) \cap E_r(\theta; x)] \\ = \; & \mathbb{E}\left[\mathbf{1}[C_r^\star(\theta)]\,\mathbf{1}[E_r(\theta; x)]\left(\frac{\binom{P-U_r(\theta)}{K}}{\binom{P}{K}}\right)^{n-r}\right] \\ \le \; & \mathbb{E}\left[\mathbf{1}[C_r^\star(\theta)]\,\mathbf{1}[E_r(\theta; x)]\, e^{-(n-r)\frac{K}{P}U_r(\theta)}\right] \\ \le \; & \mathbb{P}[C_r^\star(\theta) \cap E_r(\theta; x)]\, e^{-(n-r)\frac{K^2}{P}} \end{aligned} \tag{83}$$

given that $U_r(\theta) \ge K$. In a similar way we obtain

$$\mathbb{P}[C_r(\theta) \cap B_{n,r}(\theta) \cap E_r(\theta; x)^c] \le \mathbb{P}[C_r^\star(\theta) \cap E_r(\theta; x)^c]\, e^{-(n-r)\frac{K}{P}(x+1)} \tag{84}$$

since $U_r(\theta) \ge x + 1$ on the complement $E_r(\theta; x)^c$. Reporting (83) and (84) into (82) leads to the following fact.

Lemma 11.3 *Consider positive integers K and P such that $K \le P$. With $n = 2, 3, \ldots$ and $r = 1, \ldots, n$, we have*

$$\mathbb{P}[A_{n,r}(\theta)] \le \mathbb{P}[E_r(\theta; x)]\, e^{-(n-r)\frac{K^2}{P}} + \mathbb{P}[C_r(\theta)]\, e^{-(n-r)\frac{K}{P}(x+1)} \tag{85}$$

for each positive integer x.

Combining this decomposition with Lemma 10.1 will provide bounds which are tighter than (77).

12 Outlining the proof of Proposition 7.2

It is now clear how to proceed: Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ as in the statement of Proposition 7.2. Under (30) we necessarily have $\lim_{n\to\infty} \frac{P_n}{K_n} = \infty$ as discussed at the end of Section 6. As a result, $\lim_{n\to\infty} r_n(\theta_n) = \infty$, and for any given integer $R \geq 2$ we have

$$R < r_n(\theta_n), \quad n \geq n^\star(R) \tag{86}$$

for some finite integer $n^\star(R)$.

For the time being, pick an integer $R \geq 2$ (as specified in Section 14), and on the range $n \geq n^\star(R)$ consider the decomposition

$$\begin{aligned} \sum_{r=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] &= \sum_{r=2}^{R} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] \\ &+ \sum_{r=R+1}^{r_n(\theta)} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] \\ &+ \sum_{r=r_n(\theta_n)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right]. \end{aligned} \tag{87}$$

Let n go to infinity: The desired convergence (69) will be established if we show

$$\lim_{n\to\infty} \sum_{r=2}^{R} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] = 0, \tag{88}$$

$$\lim_{n\to\infty} \sum_{r=R+1}^{r_n(\theta_n)} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] = 0 \tag{89}$$

and

$$\lim_{n\to\infty} \sum_{r=r_n(\theta_n)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[A_{n,r}(\theta_n)\right] = 0. \tag{90}$$

The next sections are devoted to proving the validity of (88), (89) and (90) with the help of the bounds (85). Throughout, we make repeated use of the standard bounds

$$\binom{n}{r} \leq \left(\frac{en}{r}\right)^r \tag{91}$$

valid for all $r, n = 1, 2, \ldots$ with $r \leq n$. Also, we note by convexity that the inequality

$$(x+y)^p \leq 2^{p-1}(x^p + y^p), \quad x, y \geq 0 \tag{92}$$

holds for each $p \geq 1$.

13 Establishing (88)

Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. According to this scaling, for each $r = 2, 3, \ldots$ and $n = r+1, r+2, \ldots$, replace θ by θ_n in Lemma 11.3 with $x = \lfloor (1+\varepsilon) K_n \rfloor$ for some ε in $(0, \frac{1}{2})$. For an arbitrary integer $R \geq 2$, the convergence (88) will follow if we show that

$$\lim_{n\to\infty} \binom{n}{r} \mathbb{P}\left[C_r(\theta_n)\right] e^{-(n-r)\frac{K_n}{P_n}(\lfloor (1+\varepsilon)K_n \rfloor + 1)} = 0 \tag{93}$$

and

$$\lim_{n\to\infty} \binom{n}{r} \mathbb{P}\left[E_r\left(\theta_n; \lfloor (1+\varepsilon)K_n \rfloor\right)\right] e^{-(n-r)\frac{K_n^2}{P_n}} = 0 \tag{94}$$

for *each* $r = 2, 3, \ldots$. These two convergence statements are established below in Proposition 13.1 and Proposition 13.2, respectively.

Proposition 13.1 *Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. With $\varepsilon > 0$, the convergence (93) holds for each $r = 2, 3, \ldots$.*

Proof. Pick $r = 2, 3, \ldots$ and $\varepsilon > 0$, and consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$. We combine the bounds (74) and (91) to write

$$\begin{aligned}
& \binom{n}{r} \mathbb{P}\left[C_r(\theta_n)\right] e^{-(n-r)\frac{K_n}{P_n}(\lfloor (1+\varepsilon)K_n \rfloor + 1)} \\
\leq\ & \left(\frac{en}{r}\right)^r r^{r-2} \left(1 - q(\theta_n)\right)^{r-1} e^{-(n-r)\frac{K_n}{P_n}(\lfloor (1+\varepsilon)K_n \rfloor + 1)} \\
\leq\ & \left(\frac{e^r}{r^2}\right) n^r \left(1 - q(\theta_n)\right)^{r-1} e^{-(n-r)\frac{K_n^2}{P_n}(1+\varepsilon)}
\end{aligned} \tag{95}$$

for all $n = r+1, r+2, \ldots$.

In view of Lemma 8.3 (via (60)), the convergence (93) will be established if we show that

$$\lim_{n\to\infty} n^r \left(\frac{K_n^2}{P_n}\right)^{r-1} e^{-(n-r)\frac{K_n^2}{P_n}(1+\varepsilon)} = 0. \tag{96}$$

This follows by the strong admissibility of the scaling.

On the range where (95) holds, we find via (19) that

$$\begin{aligned}
& n^r \left(\frac{K_n^2}{P_n}\right)^{r-1} e^{-(n-r)\frac{K_n^2}{P_n}(1+\varepsilon)} \\
=\ & n^r \left(\frac{\log n + \alpha_n}{n}\right)^{r-1} e^{-(n-r)\frac{\log n + \alpha_n}{n}(1+\varepsilon)} \\
=\ & n(\log n + \alpha_n)^{r-1} e^{-(1+\varepsilon)(1-\frac{r}{n})\log n} e^{-(1+\varepsilon)(1-\frac{r}{n})\alpha_n} \\
=\ & n^{1-(1+\varepsilon)(1-\frac{r}{n})} (\log n + \alpha_n)^{r-1} e^{-(1+\varepsilon)(1-\frac{r}{n})\alpha_n} \\
=\ & n^{-\varepsilon+(1+\varepsilon)\frac{r}{n}} (\log n + \alpha_n)^{r-1} e^{-(1+\varepsilon)(1-\frac{r}{n})\alpha_n}.
\end{aligned} \tag{97}$$

Under the condition $\lim_{n\to\infty}\alpha_n=\infty$ it is plain that

$$\lim_{n\to\infty} n^{-\varepsilon+(1+\varepsilon)\frac{r}{n}}(\log n)^{r-1}e^{-(1+\varepsilon)(1-\frac{r}{n})\alpha_n}=0$$

and

$$\lim_{n\to\infty} n^{-\varepsilon+(1+\varepsilon)\frac{r}{n}}\alpha_n^{r-1}e^{-(1+\varepsilon)(1-\frac{r}{n})\alpha_n}=0.$$

Letting n go to infinity in (97) we readily get (96) by making use of (92). ■

Proposition 13.2 *Consider a strongly admissible scaling $P,K:\mathbb{N}_0\to\mathbb{N}_0$ whose deviation function $\alpha:\mathbb{N}_0\to\mathbb{R}$ satisfies $\lim_{n\to\infty}\alpha_n=\infty$. For every ε in $(0,\frac{1}{2})$, the convergence (94) holds for each $r=2,3,\ldots$.*

Proof. Pick $r=2,3,\ldots$ and ε in $(0,\frac{1}{2})$, and consider a strongly admissible scaling $P,K:\mathbb{N}_0\to\mathbb{N}_0$. For n sufficiently large, we use (80) with $x=\lfloor(1+\varepsilon)K_n\rfloor$ to obtain

$$\begin{aligned}
&\binom{n}{r}\mathbb{P}\left[E_r(\theta_n;\lfloor(1+\varepsilon)K_n\rfloor)\right]\\
\leq\ &\binom{n}{r}\binom{P_n}{\lfloor K_n(1+\varepsilon)\rfloor}\left(\frac{\lfloor K_n(1+\varepsilon)\rfloor}{P_n}\right)^{rK_n}\\
\leq\ &n^r\left(\frac{eP_n}{\lfloor K_n(1+\varepsilon)\rfloor}\right)^{\lfloor K_n(1+\varepsilon)\rfloor}\left(\frac{\lfloor K_n(1+\varepsilon)\rfloor}{P_n}\right)^{rK_n}\\
\leq\ &n^r\left(e^{\frac{\lfloor K_n(1+\varepsilon)\rfloor}{rK_n-\lfloor K_n(1+\varepsilon)\rfloor}}\frac{\lfloor K_n(1+\varepsilon)\rfloor}{P_n}\right)^{rK_n-\lfloor K_n(1+\varepsilon)\rfloor}.
\end{aligned}$$

The condition $r\geq 2$ implies the inequalities

$$\frac{\lfloor K_n(1+\varepsilon)\rfloor}{rK_n-\lfloor K_n(1+\varepsilon)\rfloor}\leq\frac{1+\varepsilon}{r-(1+\varepsilon)}\leq\frac{1+\varepsilon}{1-\varepsilon}$$

and

$$rK_n-\lfloor K_n(1+\varepsilon)\rfloor\geq K_n\left(r-(1+\varepsilon)\right)>0.$$

Thus, upon setting

$$\Gamma(\varepsilon):=(1+\varepsilon)e^{\frac{1+\varepsilon}{1-\varepsilon}},$$

we conclude by strong admissibility (in view of (32)) that

$$\Gamma(\varepsilon)\cdot\frac{K_n}{P_n}<1$$

for all n sufficiently large. Therefore,

$$e^{\frac{\lfloor K_n(1+\varepsilon)\rfloor}{rK_n-\lfloor K_n(1+\varepsilon)\rfloor}}\frac{\lfloor K_n(1+\varepsilon)\rfloor}{P_n}\leq\Gamma(\varepsilon)\cdot\frac{K_n}{P_n}<1$$

on that range.

There, armed with these facts we can write

$$\begin{aligned}
&\binom{n}{r}\mathbb{P}\left[E_r(\theta_n;\lfloor(1+\varepsilon)K_n\rfloor)\right] \\
\leq\ & n^r\left(\Gamma(\varepsilon)\cdot\frac{K_n}{P_n}\right)^{rK_n-\lfloor K_n(1+\varepsilon)\rfloor} \\
\leq\ & n^r\left(\Gamma(\varepsilon)\cdot\frac{K_n}{P_n}\right)^{K_n(r-1-\varepsilon)} \\
\leq\ & n^r\left(\Gamma(\varepsilon)\cdot\frac{K_n}{P_n}\right)^{2(r-1-\varepsilon)} \qquad (98)\\
\leq\ & n^r\left(\Gamma(\varepsilon)\cdot\frac{K_n^2}{P_n}\right)^{2(r-1-\varepsilon)} \\
=\ & n^r\left(\Gamma(\varepsilon)\cdot\frac{\log n+\alpha_n}{n}\right)^{2(r-1-\varepsilon)} \\
=\ & n^{-r+2+2\varepsilon}\left(\Gamma(\varepsilon)\cdot(\log n+\alpha_n)\right)^{2(r-1-\varepsilon)} \qquad (99)
\end{aligned}$$

where we made use of $K_n \geq 2$ to obtain (98). On the other hand we also have

$$e^{-(n-r)\frac{K_n^2}{P_n}} = e^{-(n-r)\frac{\log n+\alpha_n}{n}} = n^{-(1-\frac{r}{n})}\cdot e^{-\frac{n-r}{n}\alpha_n}. \qquad (100)$$

Therefore, upon multiplying (99) and (100) we see that Proposition 13.1 will follow if we show that

$$\lim_{n\to\infty} n^{-r+1+2\varepsilon+\frac{r}{n}}\left(\log n+\alpha_n\right)^{2(r-1-\varepsilon)} e^{-\frac{n-r}{n}\alpha_n} = 0. \qquad (101)$$

The choice of ε and r ensures that $r-1-\varepsilon > 0$ and $-r+1+2\varepsilon+\frac{r}{n} < 0$ for all n sufficiently large. The condition $\lim_{n\to\infty}\alpha_n = \infty$ now yields

$$\lim_{n\to\infty} n^{-r+1+2\varepsilon+\frac{r}{n}}\left(\log n\right)^{2(r-1-\varepsilon)} e^{-\frac{n-r}{n}\alpha_n} = 0 \qquad (102)$$

and

$$\lim_{n\to\infty} n^{-r+1+2\varepsilon+\frac{r}{n}}\alpha_n^{2(r-1-\varepsilon)} e^{-\frac{n-r}{n}\alpha_n} = 0. \qquad (103)$$

The desired conclusion (101) follows by making use of (102) and (103) with the help of the inequality (92). ■

Neither of these two results made use of the condition (23).

14 Establishing (89)

In order to establish (89) we will need two technical facts which are presented in Proposition 14.1 and Proposition 14.2.

Proposition 14.1 *Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. Then, with $0 < \lambda < 1$ and integer $R \geq 2$, we have*

$$\lim_{n\to\infty} \sum_{r=R+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[C_r(\theta_n)\right] e^{-(n-r)\frac{K_n}{P_n}(\lfloor \lambda r K_n \rfloor + 1)} = 0 \tag{104}$$

whenever λ and R are selected so that

$$2 < \lambda(R+1). \tag{105}$$

Proposition 14.1 is proved in Section 16. Next, with λ in $(0, \frac{1}{2})$ and $\sigma > 0$, we write

$$C(\lambda; \sigma) := \left(\frac{e^2}{\sigma}\right)^{\frac{\lambda}{1-2\lambda}}. \tag{106}$$

Proposition 14.2 *Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. If there exists some $\sigma > 0$ such that (23) holds for all $n = 1, 2, \ldots$ sufficiently large, then we have*

$$\lim_{n\to\infty} \sum_{r=1}^{r_n(\theta_n)} \binom{n}{r} \mathbb{P}\left[E_r(\theta_n; \lfloor \lambda r K_n \rfloor)\right] e^{-(n-r)\frac{K_n^2}{P_n}} = 0 \tag{107}$$

whenever λ in $(0, \frac{1}{2})$ is selected small enough so that

$$\max\left(2\lambda\sigma, \lambda^{1-2\lambda}, \lambda C(\lambda; \sigma)\right) < 1. \tag{108}$$

A proof of Proposition 14.2 can be found in Section 17. Note that for any $\sigma > 0$, $\lim_{\lambda \downarrow 0} \lambda C(\lambda; \sigma) = 0$ and that $\lim_{\lambda \downarrow 0} \lambda^{1-2\lambda} = 0$ so that the condition (108) can always be met by suitably selecting $\lambda > 0$.

We now turn to the proof of (89): Keeping in mind Propositions 14.1 and 14.2, we select λ sufficiently small in $(0, \frac{1}{2})$ to meet the condition (108) and then pick any integer $R \geq 2$ sufficiently large to ensure

$$2 < \lambda(R+1). \tag{109}$$

Next consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies the condition $\lim_{n\to\infty} \alpha_n = \infty$. Then, for each $n \geq n^\star(R)$ (with $n^\star(R)$ as specified at (86)), replace θ by θ_n according to this scaling, and for each $r = R+1, \ldots, r_n(\theta_n)$, set $x = \lfloor \lambda r K_n \rfloor$ in Lemma 11.3 with λ as specified by (108).

With these preliminaries in place, we see from Lemma 11.3 that (89) holds if both limits

$$\lim_{n\to\infty} \sum_{r=R+1}^{r_n(\theta_n)} \binom{n}{r} \mathbb{P}\left[C_r(\theta_n)\right] e^{-(n-r)\frac{K_n}{P_n}(\lfloor \lambda r K_n \rfloor + 1)} = 0$$

and

$$\lim_{n\to\infty} \sum_{r=R+1}^{r_n(\theta_n)} \binom{n}{r} \mathbb{P}\left[E_r(\theta_n; \lfloor \lambda r K_n \rfloor)\right] e^{-(n-r)\frac{K_n^2}{P_n}} = 0$$

hold. However, under the selections (108) and (109), these two convergence statements are immediate from Proposition 14.1 and Proposition 14.2, respectively. ■

15 Establishing (90)

The following two results are needed to establish (90). The first of these results is given next with a proof available in Section 18.

Proposition 15.1 *Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. If there exists some $\sigma > 0$ such that (23) holds for all $n = 1, 2, \ldots$ sufficiently large, then we have*

$$\lim_{n\to\infty} \sum_{r=r_n(\theta_n)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[E_r(\theta_n; \lfloor \mu P_n \rfloor)\right] e^{-(n-r)\frac{K_n^2}{P_n}} = 0 \tag{110}$$

whenever μ in $(0, \frac{1}{2})$ is selected so that

$$\max\left(2\left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^{\sigma}, \sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right) < 1. \tag{111}$$

Note that $\lim_{\mu\downarrow 0}\left(\frac{e}{\mu}\right)^{\mu} = 1$, whence $\lim_{\mu\downarrow 0}\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu} = 0$, and (111) can be made to hold for any $\sigma > 0$ by taking $\mu > 0$ sufficiently small. The next proposition is established in Section 19.

Proposition 15.2 *Consider an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. If there exists some $\sigma > 0$ such that (23) holds for all $n = 1, 2, \ldots$ sufficiently large, then we have*

$$\lim_{n\to\infty} \sum_{r=r_n(\theta_n)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[C_r(\theta_n)\right] e^{-(n-r)\frac{K_n}{P_n}(\lfloor \mu P_n \rfloor + 1)} = 0 \tag{112}$$

for each μ in $(0, 1)$.

The proof of (90) is now within easy reach: Consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. On the range where (23) holds, for each $n \geq n^\star(R)$ (with

$n^\star(R)$ as specified at (86)), replace θ by θ_n according to this scaling, and set $x = \lfloor \mu P_n \rfloor$ in Lemma 11.3 with μ as specified by (111). We get (90) as a direct consequence of Proposition 15.1 and Proposition 15.2. ■

16 A proof of Proposition 14.1

Let λ and R be as in the statement of Proposition 14.1, and pick a positive integer n such that $2(R+1) < n$. Arguments similar to the ones leading to (95) yield

$$\binom{n}{r} \mathbb{P}\left[C_r(\theta_n)\right] e^{-(n-r)\frac{K_n}{P_n}(\lfloor \lambda r K_n \rfloor + 1)} \leq \left(\frac{e^r}{r^2}\right) n^r e^{-\lambda r(n-r)\frac{K_n^2}{P_n}} \left(1 - q(\theta_n)\right)^{r-1}$$

for all $r = 1, \ldots, n$. Thus, in order to establish (104), we need only show

$$\lim_{n\to\infty} \sum_{r=R+1}^{\lfloor \frac{n}{2} \rfloor} \frac{e^r}{r^2} n^r e^{-\lambda r(n-r)\frac{K_n^2}{P_n}} \left(1 - q(\theta_n)\right)^{r-1} = 0. \tag{113}$$

As in the proof of Proposition 13.2, by the strong admissibility of the scaling (with the help of (61)), it suffices to show

$$\lim_{n\to\infty} \sum_{r=R+1}^{\lfloor \frac{n}{2} \rfloor} \frac{e^r}{r^2} n^r e^{-\lambda r(n-r)\frac{K_n^2}{P_n}} \left((1+\delta)\frac{K_n^2}{P_n}\right)^{r-1} = 0 \tag{114}$$

with $0 < \delta < 1$.

For each $r = 1, \ldots, \lfloor \frac{n}{2} \rfloor$, we get

$$\begin{aligned}
& \left(\frac{e^r}{r^2}\right) n^r e^{-\lambda r(n-r)\frac{K_n^2}{P_n}} \left((1+\delta)\frac{K_n^2}{P_n}\right)^{r-1} \\
= \; & \left(\frac{e^r}{r^2}\right) n^r e^{-\lambda r(n-r)\frac{\log n + \alpha_n}{n}} \left((1+\delta)\frac{\log n + \alpha_n}{n}\right)^{r-1} \\
= \; & n\left(\frac{e^r}{r^2}\right) e^{-\lambda r(n-r)\frac{\log n + \alpha_n}{n}} \left((1+\delta)(\log n + \alpha_n)\right)^{r-1} \\
\leq \; & n e^r e^{-\lambda r(1-\frac{r}{n})(\log n + \alpha_n)} \left((1+\delta)(\log n + \alpha_n)\right)^{r-1} \\
\leq \; & n e^r e^{-\frac{\lambda}{2} r(\log n + \alpha_n)} \left((1+\delta)(\log n + \alpha_n)\right)^{r-1} \\
= \; & n\left(e^{1-\frac{\lambda}{2}(\log n + \alpha_n)}\right)^r \left((1+\delta)(\log n + \alpha_n)\right)^{r-1}
\end{aligned} \tag{115}$$

as we note that

$$1 - \frac{r}{n} \geq \frac{1}{2}, \quad r = 1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor \tag{116}$$

since on that range we have $n - r \geq n - \lfloor \frac{n}{2} \rfloor \geq \frac{n}{2}$.

Next, for all $n = 1, 2, \ldots$ we set

$$\Gamma_n(\lambda) := ne^{1-\frac{\lambda}{2}(\log n+\alpha_n)}$$

and

$$a_n(\lambda) := e^{1-\frac{\lambda}{2}(\log n+\alpha_n)}(1+\delta)(\log n + \alpha_n).$$

With this notation we conclude that

$$\begin{aligned}
&\sum_{r=R+1}^{\lfloor \frac{n}{2} \rfloor} \left(\frac{e^r}{r^2}\right) n^r e^{-\lambda r(n-r)\frac{K_n^2}{P_n}} \left((1+\delta)\frac{K_n^2}{P_n}\right)^{r-1} \\
\leq\ & \Gamma_n(\lambda) \sum_{r=R+1}^{\lfloor \frac{n}{2} \rfloor} a_n(\lambda)^{r-1} \\
\leq\ & \Gamma_n(\lambda) \sum_{r=R}^{\infty} a_n(\lambda)^r. \qquad (117)
\end{aligned}$$

Obviously, $\lim_{n\to\infty} a_n(\lambda) = 0$ under the condition $\lim_{n\to\infty} \alpha_n = \infty$, so that $a_n(\lambda) < 1$ for all n sufficiently large. On that range, the geometric series at (117) converges to a finite limit with

$$\sum_{r=R}^{\infty} a_n(\lambda)^r = \frac{a_n(\lambda)^R}{1-a_n(\lambda)}.$$

Thus,

$$\begin{aligned}
&\sum_{r=R+1}^{\lfloor \frac{n}{2} \rfloor} \frac{e^r}{r^2} \cdot n^r e^{-\lambda r(n-r)\frac{K_n^2}{P_n}} \left((1+\delta)\frac{K_n^2}{P_n}\right)^{r-1} \\
\leq\ & \Gamma_n(\lambda) \cdot \frac{a_n(\lambda)^R}{1-a_n(\lambda)} \\
=\ & C_{n,R}(\delta) \cdot n^{1-\frac{\lambda}{2}(R+1)} e^{-\frac{\lambda}{2}(R+1)\alpha_n} (\log n + \alpha_n)^R
\end{aligned}$$

with

$$C_{n,R}(\delta) := \frac{e^{R+1}(1+\delta)^R}{1-a_n(\lambda)}.$$

Under (105), the condition $\lim_{n\to\infty} \alpha_n = \infty$ implies

$$\lim_{n\to\infty} n^{1-\frac{\lambda}{2}(R+1)} e^{-\frac{\lambda}{2}(R+1)\alpha_n} (\log n)^R = 0$$

and

$$\lim_{n\to\infty} n^{1-\frac{\lambda(R+1)}{2}} e^{-\frac{\lambda(R+1)}{2}\alpha_n} \alpha_n^R = 0.$$

The desired conclusion (114) is now immediate with the help of the inequality (92). ■

Condition (23) played no role.

17 A proof of Proposition 14.2

We begin by providing bounds on the probabilities of interest entering (107). Recall the definitions of the quantities introduced before the statement of Proposition 14.2.

Proposition 17.1 *Consider positive integers K, P and n such that $2 \leq K \leq P$ and $\sigma n \leq P$ for some $\sigma > 0$. For any λ in $(0, \frac{1}{2})$ small enough to ensure*

$$\max\left(2\sigma\lambda, \lambda C(\lambda;\sigma)\right) < 1, \tag{118}$$

we have

$$\binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \leq B(\lambda;\sigma;K)^r \tag{119}$$

for all $r = 1, \ldots, r_n(\theta)$ where we have set

$$B(\lambda;\sigma;K) := \max\left(\lambda^{1-2\lambda}, \lambda^{1-2\lambda}\left(\frac{e^2}{\sigma}\right)^{\lambda}, \frac{e^2}{\sigma K^{K-2}}\right). \tag{120}$$

Proof. Pick positive integers K, P and n as in the statement of Proposition 17.1. For each $r = 1, 2, \ldots, n$, we use (81) with $x = \lfloor \lambda r K \rfloor$ to find

$$\binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \leq \binom{\lfloor \frac{P}{\sigma} \rfloor}{r} \binom{P}{\lfloor \lambda r K \rfloor} \left(\frac{\lfloor \lambda r K \rfloor}{P}\right)^{rK}. \tag{121}$$

On the range

$$r = 1, \ldots, r_n(\theta), \tag{122}$$

the inequalities

$$r \leq \left\lfloor \frac{P}{K} \right\rfloor - 1 < \frac{P}{K} \tag{123}$$

hold, whence $r < \frac{P}{2}$ since $K \geq 2$. Now if λ is selected in $(0, \frac{1}{2})$ such that $2\lambda\sigma < 1$, it then follows from (123) that $\lambda r K < \lambda P < \frac{P}{2\sigma}$ so that

$$\lfloor \lambda r K \rfloor \leq \left\lfloor \frac{P}{2\sigma} \right\rfloor \leq \frac{1}{2}\left\lfloor \frac{P}{\sigma} \right\rfloor. \tag{124}$$

Under these circumstances, we also note that

$$rK - \lfloor 2\lambda r K \rfloor \geq (1 - 2\lambda) rK > 0. \tag{125}$$

Two possibilities arise:

Case I: $r \leq \lfloor \lambda r K \rfloor$ – Since $r \leq \lfloor \lambda r K \rfloor \leq \frac{\lfloor \frac{P}{\sigma} \rfloor}{2}$ via (124), we can use (121) to get

$$\begin{aligned}
& \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \\
\leq & \binom{\lfloor \frac{P}{\sigma} \rfloor}{\lfloor \lambda r K \rfloor} \binom{P}{\lfloor \lambda r K \rfloor} \left(\frac{\lfloor \lambda r K \rfloor}{P}\right)^{rK} \\
\leq & \left(\frac{e\lfloor \frac{P}{\sigma} \rfloor}{\lfloor \lambda r K \rfloor}\right)^{\lfloor \lambda r K \rfloor} \left(\frac{eP}{\lfloor \lambda r K \rfloor}\right)^{\lfloor \lambda r K \rfloor} \left(\frac{\lfloor \lambda r K \rfloor}{P}\right)^{rK} \\
\leq & \left(\frac{e}{\sigma}\frac{P}{\lfloor \lambda r K \rfloor}\right)^{\lfloor \lambda r K \rfloor} \left(\frac{eP}{\lfloor \lambda r K \rfloor}\right)^{\lfloor \lambda r K \rfloor} \left(\frac{\lfloor \lambda r K \rfloor}{P}\right)^{rK} \\
= & \left(\frac{e^2}{\sigma}\right)^{\lfloor \lambda r K \rfloor} \left(\frac{\lfloor \lambda r K \rfloor}{P}\right)^{rK - 2\lfloor \lambda r K \rfloor} \\
= & \left(\left(\frac{e^2}{\sigma}\right)^{\frac{\lfloor \lambda r K \rfloor}{rK - 2\lfloor \lambda r K \rfloor}} \cdot \frac{\lfloor \lambda r K \rfloor}{P}\right)^{rK - 2\lfloor \lambda r K \rfloor} \\
\leq & \left(\max\left(1, C(\lambda;\sigma)\right) \cdot \frac{\lfloor \lambda r K \rfloor}{P}\right)^{rK - 2\lfloor \lambda r K \rfloor} \qquad (126)
\end{aligned}$$

with $C(\lambda;\sigma)$ given by (106) – In the last step we made use of (125) together with the fact that

$$\frac{\lfloor \lambda r K \rfloor}{rK - 2\lfloor \lambda r K \rfloor} \leq \frac{\lambda r K}{rK - 2\lambda r K} = \frac{\lambda}{1 - 2\lambda}$$

since $\lfloor \lambda r K \rfloor \leq \lambda r K$.

On the range (122), we have $rK \leq P$ from (123) and using this fact into (126) we find

$$\binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \leq \left(\lambda \cdot \max\left(1, C(\lambda;\sigma)\right)\right)^{rK - 2\lfloor \lambda r K \rfloor}.$$

In particular, if λ in $(0, \frac{1}{2})$ were selected such that $\lambda C(\lambda;\sigma) < 1$, then we have $\lambda \max\left(1, C(\lambda;\sigma)\right) < 1$ and it follows that

$$\binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \leq \left(\lambda \cdot \max\left(1, C(\lambda;\sigma)\right)\right)^{(1-2\lambda)rK}$$

by recalling (125). Such a selection will also imply that the quantity

$$\left(\lambda \cdot \max\left(1, C(\lambda;\sigma)\right)\right)^{(1-2\lambda)K} = \left(\lambda^{1-2\lambda} \max\left(1, \left(\frac{e^2}{\sigma}\right)^{\lambda}\right)\right)^{K}$$

is largest when $K = 1$ and the conclusion

$$\binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \leq \left(\max\left(\lambda^{1-2\lambda}, \lambda^{1-2\lambda} \left(\frac{e^2}{\sigma} \right)^{\lambda} \right) \right)^r . \tag{127}$$

follows.

Case II: $\lfloor \lambda r K \rfloor \leq r$ – On the range (122), we have $\lfloor \lambda r K \rfloor \leq r \leq \frac{P}{2}$ by virtue of (123). Using (121) we find

$$\begin{aligned} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] &\leq \binom{\lfloor \frac{P}{\sigma} \rfloor}{r} \binom{P}{r} \left(\frac{\lfloor \lambda r K \rfloor}{P} \right)^{rK} \\ &\leq \left(\frac{e}{r} \left\lfloor \frac{P}{\sigma} \right\rfloor \right)^r \left(\frac{eP}{r} \right)^r \left(\frac{\lfloor \lambda r K \rfloor}{P} \right)^{rK} \\ &\leq \left(\frac{eP}{r\sigma} \right)^r \left(\frac{eP}{r} \right)^r \left(\frac{\lfloor \lambda r K \rfloor}{P} \right)^{rK} . \end{aligned} \tag{128}$$

The condition $\lfloor \lambda r K \rfloor \leq r$ now implies via (128) that

$$\begin{aligned} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] &\leq \left(\frac{eP}{r\sigma} \right)^r \left(\frac{eP}{r} \right)^r \left(\frac{r}{P} \right)^{rK} . \\ &= \left(\frac{e^2}{\sigma} \right)^r \left(\frac{r}{P} \right)^{r(K-2)} \\ &= \left(\frac{e^2}{\sigma} \left(\frac{r}{P} \right)^{(K-2)} \right)^r \\ &\leq \left(\frac{e^2}{\sigma K^{K-2}} \right)^r \end{aligned} \tag{129}$$

since $r \leq \frac{P}{K}$ via (123). Proposition 17.1 is now established by combining the inequalities (127) and (129). ■

We can now turn to the proof of Proposition 14.2: Consider positive integers K, P and n as in the statement of Proposition 17.1. Pick λ in $(0, \frac{1}{2})$ which satisfies (108) and note that (118) is also valid under this selection. In the usual manner we get

$$\begin{aligned} & \sum_{r=1}^{r_n(\theta)} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \cdot e^{-(n-r)\frac{K^2}{P}} \\ \leq & \sum_{r=1}^{r_n(\theta)} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \cdot e^{-\left(n - \lfloor \frac{n}{2} \rfloor\right)\frac{K^2}{P}} \\ = & \; e^{-\frac{n}{2}\frac{K^2}{P}} \sum_{r=1}^{r_n(\theta)} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \lambda r K \rfloor)\right] \end{aligned}$$

$$\leq \quad e^{-\frac{n}{2}\frac{K^2}{P}} \sum_{r=1}^{r_n(\theta)} B(\lambda;\sigma;K)^r \tag{130}$$

as we invoke Proposition 17.1. If it is the case that $B(\lambda;\sigma;K) < 1$, the geometric series is summable and

$$\sum_{r=1}^{r_n(\theta)} B(\lambda;\sigma;K)^r \leq \sum_{r=1}^{\infty} B(\lambda;\sigma;K)^r = \frac{B(\lambda;\sigma;K)}{1-B(\lambda;\sigma;K)}$$

so that

$$\sum_{r=1}^{r_n(\theta)} \binom{n}{r} \mathbb{P}\left[E_r(\theta;\lfloor \lambda r K \rfloor)\right] \cdot e^{-(n-r)\frac{K^2}{P}} \leq e^{-\frac{n}{2}\frac{K^2}{P}} \frac{B(\lambda;\sigma;K)}{1-B(\lambda;\sigma;K)}. \tag{131}$$

Now, consider a strongly admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. On the range where (23) holds, replace θ by θ_n in the last inequality according to this admissible scaling. We see from (19) that

$$K_n^2 = \frac{P_n}{n}(\log n + \alpha_n) \geq \sigma(\log n + \alpha_n)$$

so that $\lim_{n\to\infty} K_n = \infty$, hence

$$\lim_{n\to\infty} \left(\frac{e^2}{\sigma K_n^{K_n-2}}\right) = 0$$

Also, any λ in the interval $(0, \frac{1}{2})$ satisfying (108) also satisfies the condition $\lambda C(\lambda;\sigma) < 1$, so that

$$\lambda^{1-2\lambda}\left(\frac{e^2}{\sigma}\right)^{\lambda} = (\lambda C(\lambda;\sigma))^{1-2\lambda} < 1.$$

As a result, under (108) we see that $B(\lambda;\sigma;K_n) < 1$ for all n sufficiently large and (131) is therefore valid under the enforced assumptions. Now replacing θ by θ_n in (131), we find

$$\begin{aligned} & \sum_{r=1}^{r_n(\theta)} \binom{n}{r} \mathbb{P}\left[E_r(\theta_n;\lfloor \lambda r K_n \rfloor)\right] \cdot e^{-(n-r)\frac{K_n^2}{P_n}} \\ \leq \quad & e^{-\frac{n}{2}\frac{\log n+\alpha_n}{n}} \left(\frac{B(\lambda;\sigma;K_n)}{1-B(\lambda;\sigma;K_n)}\right) \\ = \quad & n^{-\frac{1}{2}} e^{-\frac{\alpha_n}{2}} \left(\frac{B(\lambda;\sigma;K_n)}{1-B(\lambda;\sigma;K_n)}\right). \end{aligned}$$

Finally, let n go to infinity in this last expression: The condition $\lim_{n\to\infty} \alpha_n = \infty$ implies $\lim_{n\to\infty} n^{-\frac{1}{2}} e^{-\frac{\alpha_n}{2}} = 0$ and this completes the proof. ■

18 A proof of Proposition 15.1

Proposition 15.1 is an easy consequence of the following bound.

Proposition 18.1 *Consider positive integers K and P such that $2 \le K$ and $2K \le P$. For each μ in $(0, \frac{1}{2})$, we have*

$$\sum_{r=r_n(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \mu P \rfloor)\right] e^{-(n-r)\frac{K^2}{P}} \le \left(2e^{-\frac{K^2}{2P}}\right)^n \left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^P \tag{132}$$

for all $n = 2, 3, \ldots$.

Proof. Fix $n = 2, 3, \ldots$. In establishing (132) we need only consider the case $r_n(\theta) < \lfloor \frac{n}{2} \rfloor$ (for otherwise (132) trivially holds), so that $r_n(\theta) = r(\theta)$ and $r_n(\theta) + 1 = \lfloor \frac{P}{K} \rfloor$. The constraint $r_n(\theta) < r \le \lfloor \frac{n}{2} \rfloor$ is then equivalent to

$$\left\lfloor \frac{P}{K} \right\rfloor \le r \le \left\lfloor \frac{n}{2} \right\rfloor,$$

hence

$$rK \ge \left(\frac{P}{K} - 1\right) K \ge \frac{P}{2}$$

as we make use of the fact that $2K \le P$ in the last step.

With μ in the interval $(0, \frac{1}{2})$ it follows that

$$\lfloor \mu P \rfloor \le \frac{P}{2} \le \min(rK, P) \tag{133}$$

and the bound (80) applies with $x = \lfloor \mu P \rfloor$ for all $r = r(\theta) + 1, \ldots, \lfloor \frac{n}{2} \rfloor$.

With this in mind, recall (116). We then get

$$\begin{aligned}
& \sum_{r=r_n(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \mu P \rfloor)\right] e^{-(n-r)\frac{K^2}{P}} \\
\le & \sum_{r=r(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \binom{P}{\lfloor \mu P \rfloor} \left(\frac{\lfloor \mu P \rfloor}{P}\right)^{rK} e^{-(n-r)\frac{K^2}{P}} \\
\le & e^{-\lfloor \frac{n}{2} \rfloor \frac{K^2}{P}} \sum_{r=r(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \left(\frac{eP}{\lfloor \mu P \rfloor}\right)^{\lfloor \mu P \rfloor} \left(\frac{\lfloor \mu P \rfloor}{P}\right)^{rK} \\
\le & e^{-\frac{n}{2}\frac{K^2}{P}} \sum_{r=r(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} e^{\lfloor \mu P \rfloor} \left(\frac{\lfloor \mu P \rfloor}{P}\right)^{rK - \lfloor \mu P \rfloor} \\
\le & e^{-\frac{n}{2}\frac{K^2}{P}} \sum_{r=r(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} e^{\lfloor \mu P \rfloor} \mu^{rK - \lfloor \mu P \rfloor}
\end{aligned} \tag{134}$$

$$\leq \quad e^{-\frac{n}{2}\frac{K^2}{P}} \left(\frac{e}{\mu}\right)^{\lfloor \mu P \rfloor} \left(\sum_{r=r(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \right) \mu^{\frac{P}{2}}$$

since $\frac{P}{2} \leq rK$ for all $r = r(\theta)+1, \ldots, \lfloor \frac{n}{2} \rfloor$ as pointed out earlier. The passage to (134) made use of the fact that $rK - \lfloor \mu P \rfloor \geq 0$. The binomial formula now implies

$$\sum_{r=r(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \leq 2^n, \tag{135}$$

so that

$$\sum_{r=r_n(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \mu P \rfloor)\right] e^{-(n-r)\frac{K^2}{P}} \leq \left(2e^{-\frac{K^2}{2P}}\right)^n \left(\frac{e}{\mu}\right)^{\mu P} \mu^{\frac{P}{2}}$$

and the desired conclusion (132) follows. ■

Now, if in Proposition 18.1, we assume that $\sigma n \leq P$ for some $\sigma > 0$, then the inequality

$$\left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^P \leq \left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^{\sigma n}$$

follows as soon as

$$\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu} < 1, \tag{136}$$

and (132) takes the more compact form

$$\sum_{r=r_n(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[E_r(\theta; \lfloor \mu P \rfloor)\right] e^{-(n-r)\frac{K^2}{P}} \leq \left(2e^{-\frac{K^2}{2P}} \left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^{\sigma}\right)^n. \tag{137}$$

To conclude the proof of Proposition 15.1, observe that (136) is implied by selecting μ in $(0, \frac{1}{2})$ according to (111). In that case, consider a strongly admissible scaling scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$. On the range where (38) holds, replace θ by θ_n in (137) according to this scaling. This yields

$$\begin{aligned} & \sum_{r=r_n(\theta_n)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[E_r(\theta_n; \lfloor \mu P_n \rfloor)\right] e^{-(n-r)\frac{K_n^2}{P_n}} \\ \leq & \left(2e^{-\frac{K_n^2}{2P_n}} \left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^{\sigma}\right)^n \\ \leq & \left(2\left(\sqrt{\mu}\left(\frac{e}{\mu}\right)^{\mu}\right)^{\sigma}\right)^n \end{aligned} \tag{138}$$

As we let n go to infinity in this last inequality, we readily get the desired conclusion (110) from (111). ■

This result does not make use of the fact that $\lim_{n\to\infty} \alpha_n = \infty$.

19 A proof of Proposition 15.2

Consider positive integers K and P such that $2 \leq K \leq P$, and pick μ in the interval $(0,1)$. For each $n = 2, 3, \ldots$, crude bounding arguments yield

$$\begin{aligned}
\sum_{r=r_n(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[C_r(\theta)\right] \cdot e^{-(n-r)\frac{K}{P}(\lfloor \mu P \rfloor + 1)} &\leq \sum_{r=r_n(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} e^{-(n-r)\frac{K}{P}(\mu P)} \\
&\leq \left(\sum_{r=r_n(\theta)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \right) e^{-\left(n - \lfloor \frac{n}{2} \rfloor\right) K\mu} \\
&\leq 2^n e^{-\frac{n}{2} K\mu} \qquad (139)
\end{aligned}$$

where in the last step we used (135).

To complete the proof of Proposition 15.2, consider an admissible scaling $P, K : \mathbb{N}_0 \to \mathbb{N}_0$ whose deviation function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies $\lim_{n\to\infty} \alpha_n = \infty$. Replace θ by θ_n in (139) according to this admissible scaling so that

$$\sum_{r=r_n(\theta_n)+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{r} \mathbb{P}\left[C_r(\theta_n)\right] e^{-(n-r)\frac{K_n}{P_n}\lfloor \mu P_n \rfloor} \leq \left(2e^{-\frac{\mu K_n}{2}}\right)^n. \qquad (140)$$

The condition (23) implies

$$K_n^2 = \frac{\log n + \alpha_n}{n} \cdot P_n \ \geq \sigma\left(\log n + \alpha_n\right)$$

for $n = 1, 2, \ldots$ sufficiently large, whence $\lim_{n\to\infty} K_n = \infty$ since the assumed condition $\lim_{n\to\infty} \alpha_n = \infty$ ensures that eventually $\alpha_n \geq 0$ for all n sufficiently large. Consequently,

$$\lim_{n\to\infty} \left(2e^{-\frac{\mu K_n}{2}}\right) = 0$$

and the desired conclusion (112) follows upon letting n go to infinity in (140). ■

References

[1] S.R. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," May 2008. arXiv:0805.2814v2 [math.CO]

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

[3] A. Cayley, "A theorem on trees," *Quarterly Journal of Mathematics* **23** (1889), pp. 376-378.

[4] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Sensor networks that are provably secure," in Proceedings of SecureComm 2006, the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks, Baltimore (MD), August 2006.

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

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

[7] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), Washington (DC), November 2002, pp. 41-47.

[8] J. Fill, E.R. Schneinerman and K.B. Cohen-Singer, "Random intersection graphs when $m = \omega(n)$: An equivalence theorem relating the evolution of the $G(n, m, p)$ and $G(n, p)$ models, *Random Structures and Algorithms* **16** (2000), pp. 249-258.

[9] 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.

[10] 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, Eds., Springer, Berlin (2007), pp. 67-74.

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

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

[13] P. Marbach, "A lower-bound on the number of rankings required in recommender systems using collaborativ filtering," Forty second Conference on Information Systems and Science (CISS 2008), Princeton University, Princeton (NJ), March 2008.

[14] G.E. Martin, *Counting: The Art of Enumerative Combinatorics*, Springer Verlags New York, 2001.

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

[16] K.B. Singer, *Random Intersection Graphs*, Ph.D. Thesis, Department of Mathematical Sciences, The Johns Hopkins University, Baltimore (MD), 1995.

[17] J. Spencer, "Nine Lectures on Random Graphs," in Ecole d'Eté de Probabilités de saint Flour XXI - 1991, Editor P.L. Hennequin, Springer Lecture Notes in Mathematics **1541**, Springer-Verlag Berlin Heidelberg 1993. pp. 293-347.

[18] O. Yağan and A.M. Makowski, "On the random graph induced by a random key predistribution scheme under full visibility," In Proceedings of the IEEE International Symposium on Information Theory (ISIT 2008), Toronto (ON), June 2008.

[19] O. Yağan and A.M. Makowski, "On the random graph induced by a random key predistribution scheme under full visibility (Extended version)," Available online at http://hdl.handle.net/1903/7498, January 2008.

[20] O. Yağan and A.M. Makowski, "Connectivity results for random key graphs," submitted for inclusion in the program of the IEEE International Symposium on Information Theory (ISIT 2009), Seoul (S. Korea).