On Asymptotically Exact Probability of $k$-Connectivity in Random Key Graphs

Intersecting Erdős–Rényi Graphs

Jun Zhao, Member, IEEE, Osman Yağan, Member, IEEE, and Virgil Gligor, Senior Member, IEEE

Abstract—Random key graphs have originally been introduced in the context of a random key predistribution scheme for securing wireless sensor networks (WSNs). Since then, they have appeared in applications spanning recommender systems, social networks, clustering and classification analysis, and cryptanalysis of hash functions [2], trust networks [15], modeling “small-world” networks [31], and recommender systems using collaborative filtering [19]. They belong to a larger class of random graphs known as random intersection graphs [4, 10, 26]; in fact, they are referred to as uniform random intersection graphs by some authors [1, 3, 16, 24–26].

A random key graph, denoted $G(n; K, P)$, can be described as follows: Let $V_n = \{v_1, \ldots, v_n\}$ denote the set of vertices in the graph, and assume available a pool of $P$ keys. Each vertex $v_i$ is assigned $K$ distinct keys that are selected uniformly at random from a key pool of size $P$. An undirected edge is then drawn between any pair of distinct vertices $v_i$ and $v_j$ if $S_i \cap S_j \neq \emptyset$. In this paper, we consider random key graphs with unreliable (i.e., randomly deleted) edges. Namely, let $\mathbb{E}(n; p)$ denote an Erdős–Rényi graph on vertices $V_n = \{v_1, \ldots, v_n\}$, where an edge exists between any distinct pair of vertices $v_i$ and $v_j$ with probability $p$, independently from all other edges. The intersection of a random key graph and an Erdős–Rényi graph, denoted $\mathbb{G}_{on}(n; K, P, p) = G(n; K, P) \cap \mathbb{E}(n; p)$, corresponds to a random key graph with unreliable (Bernoulli) links, and can be a useful model in various real-world applications; e.g., with secure WSN application in mind, link unreliability can be attributed to harsh environmental conditions severely impairing transmissions. With parameters $K, P$, and $p$ scaling with the number of vertices $n$, we derive asymptotically exact probabilities for three related graph properties in $\mathbb{G}_{on}(n; K, P, p)$: i) $k$-vertex-connectivity, ii) $k$-edge-connectivity, and iii) the minimum vertex degree being at least $k$, where a graph is $k$-vertex-connected (resp. $k$-edge-connected) if it remains connected despite the deletion of any $(k−1)$ vertices (resp. edges). Our results extend the literature on random key graphs in several directions, in particular providing the first analysis on the asymptotically exact probability of the connectivity of $\mathbb{G}_{on}(n; K, P, p)$.

Index Terms—Random key graphs, Erdős–Rényi graphs, $k$-connectivity, Poisson approximation, network reliability.

I. INTRODUCTION

A. Problem Statement

Random key graphs are naturally induced by the Eschenauer-Gligor random key predistribution scheme [12], which is a widely accepted solution for securing wireless sensor network (WSN) communications. Recently, they received significant interest with applications spanning key predistribution in secure wireless sensor networks [1, 5, 7–9, 15, 24, 28–33, 35, 37, 38], clustering and classification analysis [16], cryptanalysis of hash functions [2], trust networks [15], modeling “small-world” networks [31], and recommender systems using collaborative filtering [19]. They belong to a larger class of random graphs known as random intersection graphs [4, 10, 26]; in fact, they are referred to as uniform random intersection graphs by some authors [1, 3, 16, 24–26].

A random key graph, denoted $G(n; K, P)$, can be described as follows: Let $V_n = \{v_1, \ldots, v_n\}$ denote the set of vertices in the graph, and assume available a pool of $P$ keys. Each vertex $v_i$ is assigned $K$ distinct keys that are selected uniformly at random from a key pool of size $P$. An undirected edge is then drawn between any pair of distinct vertices $v_i$ and $v_j$ if $S_i \cap S_j \neq \emptyset$. In this paper, we consider random key graphs with unreliable (i.e., randomly deleted) edges. Namely, let $\mathbb{E}(n; p)$ denote an Erdős–Rényi graph [4], on vertices $V_n = \{v_1, \ldots, v_n\}$, where an edge exists between any distinct pair of vertices $v_i$ and $v_j$ with probability $p$, independently from all other edges. The intersection of a random key graph and an Erdős–Rényi graph, denoted $\mathbb{G}_{on}(n; K, P, p) = G(n; K, P) \cap \mathbb{E}(n; p)$, corresponds to a random key graph with unreliable (Bernoulli) links, and can be a useful model in various real-world applications; e.g., with secure WSN application in mind, link unreliability can be attributed to harsh environmental conditions severely impairing transmissions. We refer the reader to [38] for another application of $\mathbb{G}_{on}(n; K, P, p)$ on large scale, distributed publish-subscribe services in online social networks.

Our main goal in this paper is to reveal the relationship between the parameters $(n; K, P, p)$ and the connectivity properties of the corresponding graph $\mathbb{G}_{on}(n; K, P, p)$. In particular, we wish to answer the following three questions: With parameters $K, P$, and $p$ scaling with the number of vertices $n$, i.e., when they are functions of $n$, what are the asymptotic
behavior of the probabilities that \( G_{on}(n; K_n, P_n, p_n) \) is i) \( k \)-vertex-connected; ii) \( k \)-edge-connected; and iii) has minimum vertex degree at least \( k \), as \( n \) grows large? We say that a graph is \( k \)-vertex-connected if it remains connected despite the deletion of any \( (k - 1) \) vertices, and \( k \)-edge-connectivity is defined similarly for the deletion of edges; with \( k = 1 \), these definitions reduce to the standard notion of graph connectivity. The degree of a vertex is defined as the number of edges incident on it. The three graph properties considered here are related to each other in that \( k \)-vertex-connectivity implies \( k \)-edge-connectivity, which in turn implies that the minimum vertex degree is at least \( k \). \(^{20}\)

### B. Main Results

Under mild conditions on the scalings \( K_n, P_n, p_n \), we establish the asymptotically exact probabilities for the three aforementioned graph properties for \( G_{on}(n; K_n, P_n, p_n) \). Our main result can be summarized as follows: With mappings \( K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0 \) and a mapping \( p : \mathbb{N}_0 \rightarrow [0,1] \), let the sequence \( \alpha : \mathbb{N}_0 \rightarrow \mathbb{R} \) be defined through

\[
p_n \cdot \left[ 1 - \frac{P_n - K_n}{P_n} \right] = \frac{\ln n + (k - 1) \ln \ln n + \alpha_n}{n}, \tag{1}
\]

If \( \lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty) \), then we have the following convergence results under the conditions that \( P_n = \Omega(n) \) and \( K_n = o(1) \):

i) \( \lim_{n \to \infty} \mathbb{P} \left[ G_{on}(n; K_n, P_n, p_n) \right. \) has a minimum vertex degree at least \( k \). \]

\[
e^{-\frac{\alpha^* + \alpha}{\ln n}}.
\]

ii) \( \lim_{n \to \infty} \mathbb{P} \left[ G_{on}(n; K_n, P_n, p_n) \right. \) is \( k \)-edge-connected. \]

\[
e^{-\frac{\alpha^*}{\ln n}}
\]

iii) \( \lim_{n \to \infty} \mathbb{P} \left[ G_{on}(n; K_n, P_n, p_n) \right. \) is \( k \)-vertex-connected. \]

\[
e^{-\frac{\alpha}{\ln n}}
\]

A detailed discussion on this result is provided in Section 12-8. For the moment, we find it useful to note that the left hand side of (1) corresponds to the probability that an edge exists between any pair of vertices in \( G_{on}(n; K_n, P_n, p_n) \). In particular, \( 1 - \left( \frac{P_n - K_n}{P_n} \right) / (P_n) \) gives the probability that two vertices have a key in common in their key sets, and hence have an edge in between in the random key graph \( G(n; K_n, P_n) \). With this in mind, the reader familiar with the literature on random graphs will already realize that our main results are analogous to the classical results by Erdős and Rényi \([11]\) and the asymptotic properties of the same three properties for Erdős–Rényi graphs \( G(n; p_n) \); more on this later in Section 12-8.

Along the way to proving the main result given above, we also establish a Poisson convergence result for the number of vertices in \( G_{on}(n; K_n, P_n, p_n) \) with degree \( h - 1 \). Let \( \phi_h(n; K_n, P_n, p_n) \) denote the number of vertices in \( G_{on} \) that have degree \( h \); i.e., number of vertices with \( h \) edges incident on them. Then, with \( \alpha : \mathbb{N}_0 \rightarrow \mathbb{R} \) still defined through (1) and

\[\lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty) \]

still in effect, we establish that

\[
\lim_{n \to \infty} \mathbb{P} \left[ \phi_{k-1}(n; K_n, P_n, p_n) = \ell \right] = e^{-\lambda \ell \ell},
\]

\[
\ell = 0, 1, 2, \ldots, \quad \text{with} \quad \lambda = e^{-\alpha^* / (k-1)}.
\]

In other words, we show that \( \phi_{k-1}(n; K_n, P_n, p_n) \) converges in distribution to a Poisson random variable with parameter \( \lambda \). This result provides a little bit more information than part i) of the main result described above for the topology of \( G_{on} \), and constitutes an analog of the celebrated Poisson approximation result for Erdős–Rényi graphs \([4, 11]\).

### C. Significance of the Results

The problem studied in this paper has close ties with the popular network reliability problem \([4\) Section 7.5\], described as follows: Starting with a fixed, deterministic graph \( \mathbb{J} \), obtain \( \mathbb{G}(\mathbb{J}; p) \) by deleting each edge of \( \mathbb{J} \) independently with probability \( 1 - p \). Network reliability problem is interested in finding the probability that \( \mathbb{G}(\mathbb{J}; p) \) is connected as a function of \( p \). For an arbitrary graph \( \mathbb{J} \), this problem is shown \([23, 27]\) to be \(\#P\)-complete, meaning that no polynomial algorithm exists for its solution, unless \( P = NP \). With \( k = 1 \), our results given above constitute an asymptotic solution of the network reliability problem for random key graphs; as explained below our results provide the first asymptotical probability analysis for the 1-connectivity of \( G_{on} \). Although asymptotic in nature, these results can still provide useful insights about the reliability properties of random key graphs with number of vertices \( n \) being on the order of thousands; see Section 11 for numerical experiments.

From an application point of view, our results can be helpful in ensuring the desired level of network reliability in various applications where random key graphs are utilized. For example reliability against the failure of sensors or links is particularly important in WSN applications where sensors are deployed in hostile environments (e.g., battlefield surveillance), or, are unattended for long periods of time (e.g., environmental monitoring), or, are used in life-critical applications (e.g., patient monitoring). Moreover, the \( k \)-vertex-connectivity property studied in this paper is expected to be desirable in various network domains since it ensures the existence of at least \( k \) mutually disjoint paths between any two nodes in the network; see Menger’s Theorem \([4]\). For wireless networks, this provides communication security against an adversary that is able to compromise up to \( k - 1 \) links by launching a node capture attack \([5]\); i.e., two nodes can communicate securely as long as at least one of the \( k \) disjoint paths connecting them consists of links that are not compromised by the adversary. Furthermore, it enables flexible communication-load balancing across multiple paths so that network energy consumption is distributed without penalizing any access path \([13]\).

With respect to the literature available, our results provide extensions in several directions; see the paragraph below for details. In particular, our results complement the zero-one laws established in \([37, 38]\) for the \( k \)-connectivity of \( G_{on}(n; K_n, P_n, p_n) \). With \( \alpha_n \) defined through (1), the authors

---

\(^{20}\) Throughout the paper, \( k \) is a positive integer and does not scale with \( n \); \( \mathbb{N}_0 \) stands for the set of all positive integers; \( \mathbb{R} \) is the set of all real numbers; and \( e \) is the base of the natural logarithm function, \( ln \). We use the standard Landau asymptotic notation \( o(\cdot), O(\cdot), \omega(\cdot), \Omega(\cdot), \Theta(\cdot) \).
established in [37], [38] that
\[
\lim_{n \to \infty} P\left[ G_{on}(n; K_n, P_n, p_n) \text{ is } k\text{-vertex-connected.} \right] = \begin{cases} 
1, & \text{if } \lim_{n \to \infty} \alpha_n = +\infty, \\
0, & \text{if } \lim_{n \to \infty} \alpha_n = -\infty.
\end{cases}
\]
The same result was obtained for the two other graph properties as well, namely the \( k\)-edge-connectivity and minimum vertex degree being at least \( k \). Put differently, the results in [37], [38] cover the case where \( \alpha^* = \pm \infty \); whereas the results of the current paper cover the range \( \alpha^* \in (-\infty, +\infty) \).

We now discuss the practical importance of going beyond the zero-one laws and obtaining the asymptotically exact probability for all three properties. First, with zero-one laws, we are only provided with parameter choices which lead to \( k\)-connectivity almost surely or to a network that is not \( k\)-connected almost surely. For WSN applications, given the trade-offs involved between connectivity, security and memory load [12], [29], it would be more useful to have a complete picture, e.g., by obtaining the exact probability of \( k\)-connectivity for all parameter choices. In addition, there may be situations where the network designer is interested in having a guaranteed level of reliability (one-laws would provide conditions for that) but may also be interested in having a higher level of reliability without such guarantees (one-laws would fall short in providing this). Our results fill this gap. Finally, it is not possible to determine the width of the phase transition from zero-one laws; the width of the phase transition is often calculated by the difference in parameters that it takes to increase the probability of \( k\)-connectivity from \((1 - q)\) to \( q\), for some \( q < 0.5\). In other words, it is not clear from zero-one laws how sensitive the probability of \( k\)-connectivity is to the variations in the parameters \( K_n, P_n, \) and \( p_n \). By providing exact asymptotic probabilities, our findings provide a clear picture of these intricate relationships.

### D. Comparison with Related Work

Our results extend the literature on random key graphs in many directions. For random key graphs with unreliable links, i.e., for \( G_{on}(n; K_n, P_n, p_n) \), we provide the first analysis on the probability of \( k\)-connectivity as well as on the probability of 1-connectivity. For random key graphs \( G(n; K_n, P_n) \), we provide the first results on the asymptotically exact probability for \( k\)-connectivity with \( k \geq 2 \). Our results also constitute an important milestone in the limited literature on the intersection of random graphs, by providing the first analysis on the asymptotically exact probabilities for the property of minimum vertex degree being at least \( k \), \( k\)-edge-connectivity, and \( k\)-vertex-connectivity. Much work in the broad area of random graphs focuses on a single model with the notion of adjacency requiring only a single condition to be satisfied. Recently, there has been considerable attention on intersecting different random graphs [17], [18], [21], [22], [29], [33], [34], [37], [38]. However, there has not been any work reporting result similar to ours on the asymptotically exact probability for any of the three properties above – of course, excluding the trivial case of intersecting an Erdős–Rényi graph with another Erdős–Rényi graph as the resulting intersection is still an Erdős–Rényi graph.

Table I-C on the next page gives a more detailed comparison of our work with the literature.

### E. Roadmap

We organize the rest of the paper as follows. We present the main results in Section III together with a discussion and numerical experiments. In Section III we detail the steps of establishing Theorem 1 through Lemma 2. Afterwards, Section IV reduces proving Lemma 2 to establishing Propositions 1 and 2. Section V provides useful lemmas, which are used to demonstrate Propositions 1 and 2 in Sections VI and VII, respectively. Finally, we conclude the paper in Section VIII.

## II. MAIN RESULTS AND DISCUSSION

We introduce the main results in Theorem 1 below.

**Theorem 1.** In graph \( G_{on}(n; K_n, P_n, p_n) \) with \( P_n = \Omega(n) \) and \( K_n = o(1) \), let the sequence \( \alpha_n \) for all \( n \) be defined through
\[
p_n \cdot \left[ 1 - \left( \frac{P_n - K_n}{P_n} \right) \right] = \frac{\ln n + (k - 1) \ln n + \alpha_n}{n},
\]
If \( \lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty) \), then
i) \( \lim_{n \to \infty} P\left[ G_{on}(n; K_n, P_n, p_n) \text{ has a minimum vertex degree at least } k \right] = e^{-\frac{\alpha^*}{k - \alpha^*}} \)
ii) \( \lim_{n \to \infty} P\left[ G_{on}(n; K_n, P_n, p_n) \text{ is } k\text{-edge-connected} \right] = e^{-\frac{\alpha^*}{k - \alpha^*}} \), and
iii) \( \lim_{n \to \infty} P\left[ G_{on}(n; K_n, P_n, p_n) \text{ is } k\text{-vertex-connected} \right] = e^{-\frac{\alpha^*}{k - \alpha^*}} \).

<table>
<thead>
<tr>
<th>Graph</th>
<th>Property</th>
<th>Results</th>
<th>Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>( G_{on}(n; K_n, P_n, p_n) )</td>
<td>( k)-connectivity &amp; Min. vertex degree ( \geq k )</td>
<td>exact probability</td>
<td>this paper</td>
</tr>
<tr>
<td>( G(n; K_n, P_n) )</td>
<td>( k)-connectivity &amp; Min. vertex degree ( \geq k )</td>
<td>exact probability</td>
<td>this paper</td>
</tr>
<tr>
<td></td>
<td>1-connectivity &amp; Absence of isolated vertices</td>
<td>exact probability</td>
<td>this paper</td>
</tr>
</tbody>
</table>

**Comparison of our main results with related work.** For convenience, we write \( k\)-vertex connectivity and \( k\)-edge connectivity together as \( k\)-connectivity.
Theorem 2 presents asymptotically exact probabilities for three properties in graph $G_{on}$: the property of minimum vertex degree being at least $k$, $k$-vertex connectivity, and $k$-edge-connectivity. With $p_n = 1$ for all $n$, $G_{on}(n; K_n, P_n, p_n)$ becomes a random key graph $G(n, K, P)$. Therefore, setting $p_n = 1$, Theorem 2 provides asymptotically exact probabilities for all three properties in a random key graph. Furthermore, setting $k = 1$, we obtain from Theorem 2 the asymptotically exact probabilities of 1-vertex-connectivity, of 1-edge-connectivity, and of minimum vertex degree being at least one (i.e., of absence of isolated vertices) for $G_{on}$.

The extra conditions $P_n = \Omega(n)$ and $K/n = o(1)$ are enforced in Theorem 1 merely for technical reasons. Similar conditions appear in several other works on random key graphs; e.g., see [9], [17], [32]. In the context of secure WSNs, these conditions are deemed practical as they hold trivially in most implementations. In particular, it is noted [9], [14], [29] that the key pool size $P_n$ needs to be larger than the number of sensors $n$, and the number of keys $K_n$ per sensor needs to be several orders of magnitude smaller than $P_n$ for feasible operation of the WSN.

Our second main result establishes a Poisson convergence result for the number of vertices in $G_{on}(n; K_n, P_n, p_n)$ with degree $h$, for each $h = 0, 1, \ldots$.

**Theorem 2.** In $G_{on}(n; K_n, P_n, p_n)$ with $P_n = \Omega(n)$ and $K/n = o(1)$, let the sequence $\alpha_n$ be defined through (2). If \( \lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty) \), then

$$
\lim_{n \to \infty} \mathbb{P}(\phi_{k-1}(n; K_n, P_n, p_n) = \ell) = e^{-\lambda} \frac{\lambda^\ell}{\ell!},
$$

for $\ell = 0, 1, 2, \ldots$, with $\lambda = e^{-\alpha^*} / [(k - 1)!]$. In other words, as $n \to \infty$, $\phi_{k-1}(n; K_n, P_n, p_n)$ tends to a Poisson distribution with parameter $\lambda$.

This result implies part i) of Theorem 1 and tells a little bit more about the topology of $G_{on}$. With $k = 1$, it also shows that under suitable conditions, the number of isolated vertices (i.e., number of vertices with no incident edges) converges in distribution to a Poisson random variable. These results are analogs of the celebrated Poisson approximation results for Erdős–Rényi graphs; e.g., see [11] Theorem 3 and [12] Theorem 3.1.

### A. Numerical Experiments

To check our analytical results in the non-asymptotic regime, we run simulations and illustrate the numerical results in Figure 1. In all set of experiments, we fix the number of vertices at $n = 2,000$ and the key pool size at $P = 10,000$. For the link reliaibility probability $p$, we consider $p = 0.2, 0.5, 0.8$, while varying the parameter $K$ from 3 to 21 in Figure 1 (a) and from 5 to 23 in Figure 1 (b). For each pair $(K, p)$, we generate 1,000 independent samples of $G_{on}(n; K, P, p)$ and count the number of times that the obtained graphs are $k$-vertex-connected, $k$-edge-connected, or have minimum vertex degree at least $k$, where $k = 1$ in Figure 1 (a) and $k = 2$ in Figure 1 (b). Then, the counts divided by 1,000 give the empirical probabilities for the properties of interest. In all simulations, we observe that the empirical probabilities for all three properties are very close to each other, in accordance with Theorem 1. In Figure 1 (a) (resp. 1 (b)), the curves with legend “simulation” correspond to each other, in accordance with Theorem 1. In Figure 1 (a) and (b), we first determine $\alpha$ from (2): i.e., from the equation

$$
p \left[ 1 - \left( \frac{p-K}{K} \right)^{n} \right] = \ln n + (k-1) \ln n + \alpha.
$$

Then, the analytical approximation for the probability of $k$-vertex-connectivity is obtained from $e^{-e^{-\alpha}}$. We conclude that although our results are asymptotic in nature, they can already provide useful predictions for the probabilities of $k$-connectivity and 1-connectivity with the number of vertices $n$ being on the order of a thousand.
B. Intuition behind the Main Result

The intuition behind our main results can easily be understood by observing that the left hand side of the scaling condition (2) is in fact the edge probability of the graph \(G_{on}(n; K_n, P_n, p_n)\) as explained below.

Recall that \(V_n = \{v_1, \ldots, v_n\}\) is the set of vertices. We let \(E_{ij}\) (resp., \(\Gamma_{ij}\) and \(C_{ij}\)) denote the event that vertices \(v_i\) and \(v_j\) are adjacent in the graph \(G_{on}(n; K_n, P_n, p_n)\) (resp., the random key graph \(G(n; K_n, P_n)\) and the Erdős–Rényi graph \(\mathbb{H}(n; p_n)\)). Clearly, \(E_{ij}\) takes place if and only if \(\Gamma_{ij}\) and \(C_{ij}\) both occurs, and \(\Gamma_{ij}\) means that vertices \(v_i\) and \(v_j\) have at least one key in common. Since each vertex independently selects \(K_n\) keys uniform at random from a pool of \(P_n\) keys, and we have \(P_n \geq 2K_n\) for all \(n\) sufficient large from the condition \(K_n = o(1)\), it is straightforward to derive \(P[\Gamma_{ij}] = 1 - \frac{(p_n - K_n)^2}{K_n} \), which we denote by \(p_s\); i.e.,

\[
p_s = 1 - \frac{(p_n - K_n)^2}{K_n}.
\]

Then \(p_s\) is the edge probability of the random key graph \(G(n; K_n, P_n)\). Given \(P[C_{ij}] = p_n\) for \(i \neq j\), the independence of \(C_{ij}\) and \(\Gamma_{ij}\), and \(E_{ij} = C_{ij} \cap \Gamma_{ij}\), we know \(P[E_{ij}] = \frac{P[C_{ij}]}{P[\Gamma_{ij}]} = p_s p_n\). Therefore, with \(p_e\) denoting the edge probability of \(G_{on}(n; K_n, P_n, p_n)\), we obtain

\[
p_e = p_n \cdot p_s = p_n \cdot \left[1 - \frac{(p_n - K_n)^2}{K_n}\right].
\]

With the above in mind, our main results are exact analogs of the "classical" results by Erdős and Rényi [11, Theorems 2 and 3] for Erdős–Rényi graphs. In particular, they have shown [14] that with a sequence \(\alpha_n\) defined through \(p_n = \frac{\ln n + (k-1) \ln \ln n + \alpha_n}{n}\), the Erdős–Rényi graph \(\mathbb{H}(n; p_n)\) satisfies

\[
\lim_{n \to \infty} P[\mathbb{H}(n; p_n) \text{ is } k\text{-vertex-connected}] = e^{-\frac{\alpha^*}{\alpha^* - 1}}, \\
\text{if } \lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, \infty).
\]

Similar results have been obtained for \(k\)-edge-connectivity and minimum vertex degree being at least \(k\). To this end, although Erdős–Rényi graphs and random key graphs are not in general equivalent (e.g., they have vastly different behaviors for clustering coefficient and number of triangles [30, 31]), our results indicate that they have analogous behaviors for \(\ell\)-connectivity when they are matched through their edge probabilities. Our results also indicate an analogous \(k\)-connectivity behavior between random key graphs with unreliable links and Erdős–Rényi graphs.

III. Establishing Theorems [1] and [2]

We write \(G_{on}(n; K_n, P_n, p_n)\) as \(G_{on}\) at some places for simplicity. Also, for clarity, Table III on the next page summarizes several notation that will be used below and their meaning.

We will establish Theorems [1] and [2] by proving results on the number of vertices with a certain degree in graph \(G_{on}\). With \(\phi_h\) counting the number of vertices with degree \(h\) in \(G_{on}\), \(h = 0, 1, \ldots, \) we will show that for any \(\ell \geq 0\), probability \(P[\phi_h = \ell] \) is asymptotically equivalent to the probability that a Poisson random variable with mean \(\lambda_h\) (defined below) takes the value of \(\ell\); specifically,

\[
P[\phi_h = \ell] \sim (\ell)!^{-1} \lambda_h^\ell e^{-\lambda_h}, \quad \ell = 0, 1, \ldots; \quad h = 0, 1, \ldots,
\]

where

\[
\lambda_h = n(h!)^{-1}(np_e)^h e^{-np_e}.
\]

To prove [5], we will use the method of moments as given by the following lemma taken from [6, Theorem 2.13]. Throughout the paper, for two positive sequences \(f_n\) and \(g_n\), the relation \(f_n \sim g_n\) means \(\lim_{n \to \infty} f_n / g_n = 1\).

Lemma 1 [6, Theorem 2.13]). Let \(X_{n,i}\) \((i = 1, 2, \ldots, n)\) be Bernoulli random variables. Define \(J_n\) as \(\sum_{i=1}^n X_{n,i}\) and \(\Psi_{n,m}\) as the \(m\)-th binomial moment of \(J_n\); i.e.,

\[
\Psi_{n,m} = \sum_{j=m}^n \binom{j}{m} P[J_n = j].
\]

If \(\Psi_{n,m} \sim \frac{\alpha}{m^r}\), then \(P[J_n = \ell] \sim (\ell!)^{-1} \nu^\ell e^{-\nu}\) for \(\ell = 0, 1, \ldots, n\).

In view of Lemma 1, we introduce the following for graph \(G_{on}\). We let \(\Psi_{n,h}\) be the number of vertices with degree \(h\) in \(G_{on}\). With \(I_{n,h,i}\) defined by

\[
I_{n,h,i} = \begin{cases} 1, & \text{Vertex } v_i \text{ has degree } h, \\ 0, & \text{Vertex } v_i \text{ has degree } h', \end{cases}
\]

we have \(\Phi_{n,h} = \sum_{i=1}^n I_{n,h,i}\). Let \(\Psi_{n,m,h}\) denote the \(m\)-th binomial moment of \(\Phi_{n,h}\). Then \(\Psi_{n,m,h}\) is \(\sum_{j=m}^n \binom{j}{m} P[\Phi_{n,h} = j]\), which equals the probability that in graph \(G_{on}\) there are at least \(m\) vertices, each of which has degree \(h\). We have

\[
\Psi_{n,m,h} = \begin{cases} \text{In graph } G_{on}, \text{there are at least } m \text{ vertices,} \\ \text{each of which has degree } h. \end{cases}
\]

If Lemma 2 below holds, we substitute [5] into [7] and obtain

\[
\Psi_{n,m,h} \sim \left(\frac{n}{m}\right) \cdot \frac{\lambda_h^m}{m^m} \sim \frac{\lambda_h^m}{m^m},
\]

which with Lemma 1 gives rise to the desired result [5].

Lemma 2. Given \(P_n \geq 3K_n\) for all \(n\) sufficiently large, \(K_n = \omega(1)\), and [2] with \(\lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty)\), then for any integers \(m \geq 1\) and \(h \geq 0\), we have

\[
P[\text{Each of vertices } v_1, v_2, \ldots, v_m \text{ has degree } h. ] \sim \frac{\lambda_h^m}{m^m}.
\]

where \(p_e\) is given by [44] (i.e., \(p_e = p_n \cdot \left[1 - \frac{(p_n - K_n)^2}{K_n}\right]\)), and \(\lambda_h\) is given by [6] (i.e., \(\lambda_h = n(h!)^{-1}(np_e)^h e^{-np_e}\)).

Remark 1. From the expression of \(\lambda_h\) in [6], we know that [8] is equivalent to

\[
P[\text{Each of vertices } v_1, v_2, \ldots, v_m \text{ has degree } h. ] \sim (h!)^{-m} (np_e)^h e^{-np_e}.
\]
TABLE II

Several notation and their meaning.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>number of vertices</td>
</tr>
<tr>
<td>$P_n$</td>
<td>size of the key pool</td>
</tr>
<tr>
<td>$K_n$</td>
<td>number of keys with each vertex</td>
</tr>
<tr>
<td>$G(n; K_n, P_n)$</td>
<td>random key graph</td>
</tr>
<tr>
<td>$p_n$</td>
<td>probability of each edge in $G(n; K_n, P_n)$ being reliable to consider graph intersection $G_{on}$ below</td>
</tr>
<tr>
<td>$H(n; p_n)$</td>
<td>Erdős–Rényi graph</td>
</tr>
<tr>
<td>$G_{on}(n; K_n, P_n)$ or $G_{on}$</td>
<td>$G(n; K_n, P_n) \cap H(n; p_n)$</td>
</tr>
<tr>
<td>$V_n = { v_1, \ldots, v_n }$</td>
<td>the common vertex set of graphs $G_{on}(n; K_n, P_n), G(n; K_n, P_n)$, and $H(n; p_n)$</td>
</tr>
<tr>
<td>$S_i$</td>
<td>the key set of vertex $v_i$, constructed by selecting $K_n$ keys uniformly at random from the pool of $P_n$ keys, for $i = 1, 2, \ldots, n$</td>
</tr>
<tr>
<td>$S_i^*$</td>
<td>a specific realization of $S_i$</td>
</tr>
<tr>
<td>$S_{ij}^*$</td>
<td>$S_i^* \cap S_j^*$</td>
</tr>
<tr>
<td>$\Gamma_{ij}$</td>
<td>event $S_i \cap S_j \neq \emptyset$; i.e., event that vertices $v_i$ and $v_j$ have at least one key in common (event that vertices $v_i$ and $v_j$ are adjacent in random key graph $G(n; K_n, P_n)$)</td>
</tr>
<tr>
<td>$C_{ij}$</td>
<td>event that vertices $v_i$ and $v_j$ are adjacent in Erdős–Rényi graph $H(n; p_n)$</td>
</tr>
<tr>
<td>$E_{ij}$</td>
<td>$\Gamma_{ij} \cap C_{ij}$; i.e., event that vertices $v_i$ and $v_j$ are adjacent in $G_{on}(n; K_n, P_n)$</td>
</tr>
<tr>
<td>$p_s$</td>
<td>edge probability of random key graph $G(n; K_n, P_n)$ (i.e., $p_s = P(\Gamma_{ij})$)</td>
</tr>
<tr>
<td>$p_e$</td>
<td>edge probability of $G_{on}(n; K_n, P_n)$ (i.e., $p_e = p_s \cdot p_n$)</td>
</tr>
<tr>
<td>$\phi_h$</td>
<td>number of vertices with degree $h$ in $G_{on}(n; K_n, P_n)$ for $h = 0, 1, \ldots$</td>
</tr>
<tr>
<td>$\lambda_h$</td>
<td>$n(h!)^{-1}(np)^h e^{-np}$</td>
</tr>
<tr>
<td>$1[C_{ij}]$</td>
<td>the indicator variable of event $C_{ij}$; i.e., $1[C_{ij}] = \begin{cases} 1, &amp; \text{if there is an edge between } v_i \text{ and } v_j \text{ in } H(n; p_n); \ 0, &amp; \text{if there is no edge between } v_i \text{ and } v_j \text{ in } H(n; p_n). \end{cases}$</td>
</tr>
<tr>
<td>$\mathcal{C}_m$</td>
<td>a $(\frac{m}{2})$-tuple consisting of all possible $1[C_{ij}]$ with $1 \leq i &lt; j \leq m$; i.e., $\mathcal{C}<em>m = {1[C</em>{12}], \ldots, 1[C_{1m}], 1[C_{23}], \ldots, 1[C_{2m}], \ldots, 1[C_{(m-1)m}], 1[C_{(m-2)(m-1)}]}$</td>
</tr>
<tr>
<td>$\mathcal{T}_m$</td>
<td>a $m$-tuple $\mathcal{T}_m = (S_1, S_2, \ldots, S_m)$, where $S_i$ is the key set on vertex $v_i$</td>
</tr>
<tr>
<td>$\mathcal{L}_m$</td>
<td>$\mathcal{L}_m = (\mathcal{C}_m, \mathcal{T}_m)$</td>
</tr>
<tr>
<td>$\mathcal{C}_m$</td>
<td>the set of all possible $\mathcal{C}_m$; see $[19]$</td>
</tr>
<tr>
<td>$\mathcal{T}_m$</td>
<td>the set of all possible $\mathcal{T}_m$; see $[20]$</td>
</tr>
<tr>
<td>$\mathcal{L}_m$</td>
<td>the set of all possible $\mathcal{L}_m$; see $[21]$</td>
</tr>
<tr>
<td>$\mathcal{L}_m^{(0)}$</td>
<td>$\mathcal{L}_m \in \mathcal{L}<em>m^{(0)}$ is the event that there is no edge between any two of vertices $v_1, v_2, \ldots, v_m$ in graph $G</em>{on}$, i.e., $\mathcal{L}_m^{(0)} := { \mathcal{L}<em>m : (S_i \cap S_j = \emptyset) \text{ or } (1[C</em>{ij}] = 0), \forall i, j \text{ with } 1 \leq i &lt; j \leq m }$.</td>
</tr>
<tr>
<td>$N_i$</td>
<td>the neighborhood set of vertex $v_i$ in graph $G_{on}$ for $i = 1, 2, \ldots, m$</td>
</tr>
<tr>
<td>$M_{j_1j_2\ldots j_m}$</td>
<td>$M_{j_1j_2\ldots j_m} = \left{ v_w : v_w \in {v_{m+1}, v_{m+2}, \ldots, v_n}; \text{ and } \begin{cases} v_w \in N_i &amp; \text{if } j_i = 1, \ v_w \notin N_i &amp; \text{if } j_i = 0. \end{cases} \right}$ for $j_1, j_2, \ldots, j_m \in {0, 1}$</td>
</tr>
<tr>
<td>$\mathcal{M}_m$</td>
<td>a $2^m$-tuple $\mathcal{M}_m = (</td>
</tr>
<tr>
<td>$\mathcal{M}_m(\mathcal{L}_m)$</td>
<td>given $\mathcal{L}_m \in \mathcal{L}_m$, $\mathcal{M}_m(\mathcal{L}_m)$ is the set of $\mathcal{M}_m$ under the condition that each of $v_1, v_2, \ldots, v_m$ has a degree of $h$</td>
</tr>
<tr>
<td>$\mathcal{M}_m^{(0)}$</td>
<td>$\mathcal{M}_m^{(0)}$ satisfies $</td>
</tr>
<tr>
<td>$\mathcal{M}_m^{*}$</td>
<td>a specific realization of $\mathcal{M}_m$</td>
</tr>
<tr>
<td>$\mathcal{L}_m^{*}$</td>
<td>a specific realization of $\mathcal{L}_m$</td>
</tr>
<tr>
<td>$\mathcal{C}_m^<em>$ and $\mathcal{T}_m^</em>$</td>
<td>$\mathcal{C}_m^<em>$ and $\mathcal{T}_m^</em>$ are defined such that $\mathcal{L}_m^* = (\mathcal{C}_m^<em>, \mathcal{T}_m^</em>)$</td>
</tr>
<tr>
<td>$V_m$</td>
<td>$V_m = { v_1, v_2, \ldots, v_m }$</td>
</tr>
<tr>
<td>$V_m^{w}$</td>
<td>$V_m^{w} = V_m \setminus {v_1, v_2, \ldots, v_m} = {v_{m+1}, v_{m+2}, \ldots, v_n}$</td>
</tr>
<tr>
<td>$f(n - m, \mathcal{M}_m^*)$</td>
<td>see $[39]$</td>
</tr>
<tr>
<td>L.H.S.</td>
<td>the left hand side</td>
</tr>
<tr>
<td>R.H.S.</td>
<td>the right hand side</td>
</tr>
</tbody>
</table>
We now explain why conditions of Theorem 1 imply Lemma 2; conditions \( K_n = \omega(1) \) and \( P_n \geq 3K_n \) for all \( n \) sufficiently large, respectively. First, as given in [38, Lemma 7], from \( P_n = \Omega(n) \) and (2) with \( |\alpha_n| = O(1) \), we obtain \( K_n = \Omega(\sqrt{\ln n}) = \omega(1) \); note that \( \lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty) \) implies \( |\alpha_n| = O(1) \). Second, \( K_n = \omega(1) \) clearly leads to \( P_n \geq 3K_n \) for all \( n \) sufficiently large.

The proof of Lemma 2 starts in Section IV. The key difficulty in establishing this result lies in the calculation of the probability term appearing in (8) and in obtaining efficient bounds for it. This is because, unlike Erdős–Rényi graphs, edge appearances are not independent [30, 32] in the random key graph \( G(n; K_n, P_n) \), and hence in \( G_{\infty,n} \). In a nutshell, these intricate correlations between the degrees of vertices \( v_1, \ldots, v_m \) makes the calculation of the aforementioned probability term, and hence establishing our main results, difficult.

We now show Theorems 1 and 2 by Lemma 2 (or (5)).

### A. Proving Theorem 1

In graph \( G_{\infty,n} \), let \( \delta \) be the minimum vertex degree, \( \kappa_v \) be the edge connectivity, \( \kappa_e \) be the vertex connectivity, respectively. The vertex connectivity of a graph is defined as the minimum number of vertices that need to be deleted to make it disconnected, and edge connectivity is defined similarly for the deletion of edges. Thus, the property of minimum vertex degree being at least \( k \), \( k \)-edge-connectivity, \( k \)-vertex-connectivity are given by events \( \delta \geq k \), \( \kappa_v \geq k \), and \( \kappa_e \geq k \), respectively. For any graph, it holds [4] that \( \delta \geq \kappa_v \geq \kappa_e \). Therefore, we have

\[
P[\delta \geq k] \geq P[\kappa_e \geq k] \geq P[\kappa_v \geq k],
\]

and

\[
P[\kappa_v \geq k] = P[\delta \geq k] - P[(\kappa_v < k) \cap (\delta \geq k)] \geq P[\delta \geq k] - \sum_{h=0}^{k-1} P[(\kappa_v = h) \cap (\delta > h)].
\]

In [38, Lemma 6], under \( P_n = \Omega(n) \), \( \frac{K}{P_n} = o(1) \), Equation (4) with \( |\alpha_n| = o(\ln \ln n) \) (this clearly holds for Theorem 1 since we have \( |\alpha_n| = O(1) \) from \( \lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty) \)), we have shown

\[
P[(\kappa_v = h) \cap (\delta > h)] = o(1), \quad \text{for each } h = 0, 1, \ldots, k - 1.
\]

In view of (9), (10), and (11), Theorem 1 will be completed once we show

\[
\lim_{n \to \infty} P[\delta \geq k] = e^{-\frac{\alpha^*}{(k-1)!}},
\]

i.e., result i) in Theorem 1.

We now demonstrate (12). Clearly, event \( (\delta \geq k) \) is equivalent to event \( \bigcap_{h=0}^{k-1} (\phi_h = 0) \) (i.e., no vertex has a degree falling in \( \{0, 1, \ldots, k - 1\} \)). Hence, we obtain

\[
P[\delta \geq k] = P\left[ \bigcap_{h=0}^{k-1} (\phi_h = 0) \right] \leq P[\phi_{k-1} = 0];
\]

and by the union bound, it holds that

\[
P[\delta \geq k] = \mathbb{P}\left[ (\phi_{k-1} = 0) \cap \bigcup_{h=0}^{k-2} (\phi_h \neq 0) \right] \geq \mathbb{P}[\phi_{k-1} = 0] - \sum_{h=0}^{k-2} \mathbb{P}[\phi_h \neq 0].
\]

In order to evaluate the bounds obtained (13) and (14), we now use (5). First, we recall the expression of \( p_e \) in (4) and calculate \( \lambda_h \) specified in (6). From (2) and (4), we have

\[
p_e = \frac{\ln n + (k - 1) \ln \ln n + \alpha_n}{n}.
\]

Since \( k \) does not scale with \( n \), given \( |\alpha_n| = O(1) \) from \( \lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty) \), we obtain from (15) that

\[
p_e = \frac{\ln n + \alpha}{n} \sim 0,
\]

Applying \( p_e \sim \frac{\ln n}{n} \) and (15) to (6), and considering \( \lim_{n \to \infty} \alpha_n = \alpha^* \in (-\infty, +\infty) \), we establish

\[
\begin{align*}
\lambda_h & \sim (h!)^{-1}(\ln n)^h e^{-\ln n - (k-1)\ln \ln n - \alpha_n} = (h!)^{-1}(\ln n)^h e^{h\alpha_n} \\
& \sim \left\{ \begin{array}{ll}
0, & \text{for } h = 0, 1, \ldots, k - 2; \\
\frac{e^{-\alpha^*}}{(k-1)!}, & \text{for } h = k - 1; \\
\alpha^*, & \text{for } h = k, k + 1, \ldots.
\end{array} \right.
\end{align*}
\]

By (5) and (17), we conclude that as \( n \to \infty \),

\[
P[\phi_h = 0] \to \left\{ \begin{array}{ll}
1, & \text{for } h = 0, 1, \ldots, k - 2; \\
e^{-\alpha^*}, & \text{for } h = k - 1; \\
0, & \text{for } h = k, k + 1, \ldots.
\end{array} \right.
\]

Finally, (12) follows from (13), (14), and (18). Hence, as explained before, Theorem 1 is proved.

### B. Proving Theorem 2

As given in (17), it holds that \( \lim_{n \to \infty} \lambda_k = e^{-\alpha^*} \), which along with (5) yields

\[
P[\phi_{k-1} = \ell] \sim (\ell!)^{-1} \frac{e^{-\alpha^*}}{(k-1)!} e^{-\alpha^*} \sim (\ell!)^{-1} \frac{e^{-\alpha^*}}{(k-1)!} e^{-\alpha^*},
\]

for each \( \ell = 0, 1, 2, \ldots \)

Hence, Theorem 2 is established.

### IV. The Proof of Lemma 2

To start with, we recall several notation that will be used throughout. \( V_n = \{v_1, \ldots, v_n\} \) is the vertex set in the three graphs \( H(n; p_n) \), \( G(n; K_n, P_n) \), and \( G_{\infty,n}(n; K_n, P_n, p_n) \). Recall that \( C_{ij} \) denotes the event that an edge between vertices \( v_i \) and \( v_j \) exists in the Erdős–Rényi graph \( H(n; p_n) \). Then we set \( 1[C_{ij}] \) as the indicator variable of event \( C_{ij} \) by

\[
1[C_{ij}] := \begin{cases} 
1, & \text{if there is an edge between } v_i \text{ and } v_j \text{ in } H(n; p_n); \\
0, & \text{if there is no edge between } v_i \text{ and } v_j \text{ in } H(n; p_n).
\end{cases}
\]
We denote by $C_m$ a $m$-tuplet consisting of all possible $1[C_{ij}]$ with $1 \leq i < j \leq m$ as follows:

$$C_m := \{1[C_{ij}] \mid 1 \leq i < j \leq m\} \cup \{1[C_{12}, \ldots, 1[C_{1m}], 1[C_{23}, \ldots, 1[C_{2m}], \ldots, 1[C_{(m-1,m)}]\}.$$ 

Recalling $S_i$ as the key set on vertex $v_i$, we define a $m$-tuple $T_m$ through $T_m := (S_1, S_2, \ldots, S_m)$. Then we define $L_m$ as $L_m := (C_m, T_m)$. With $L_m$, we have the states of all edges between vertices $v_1, v_2, \ldots, v_m$ in $\mathbb{H}(n; p)$, and the key sets $S_1, S_2, \ldots, S_m$ on $v_1, v_2, \ldots, v_m$, so all edges between $v_1, v_2, \ldots, v_m$ in graph $G_{on}$ are determined.

Let $C_m, T_m$ and $L_m$ be the sets of all possible $C_m, T_m$ and $L_m$, respectively. In other words, we have

$$C_m := \{1[C_{ij}] \in \{0, 1\} \mid 1 \leq i < j \leq m\} = \{(0, 0, \ldots, 0, 1), (0, 0, \ldots, 0, 1), \ldots, (0, 1, 1, \ldots, 1)\},$$

$$T_m = \{S_i \mid S_i \text{ consists of } K_i \text{ keys, selected uniformly at random from the key pool of } P_i \}.$$ 

and

$$L_m = \{(C_m, T_m) \mid C_m \in C_m, T_m \in T_m\}.\tag{21}$$

We define $L_m^0 := \{1[C_{ij}] \in \{0, 1\} \mid 1 \leq i < j \leq m\}$ is the event that there is no edge between any two of vertices $v_1, v_2, \ldots, v_m$ in graph $G_{on}$, i.e.,

$$L_m^0 := \{L_m \mid \forall i, j \text{ with } 1 \leq i < j \leq m\}.\tag{22}$$

In graph $G_{on}$, we define $N_i$ as the neighborhood set of vertex $v_i$ for $i = 1, 2, \ldots, m$, and define the vertex set $M_{j_1, j_2, \ldots, j_m} = \{v_{m+1}, v_{m+2}, \ldots, v_n\}$, we obtain

$$\bigcup_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1, j_2, \ldots, j_m}| = \mathcal{V}_m,\tag{23}$$

and

$$\bigcup_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1, j_2, \ldots, j_m}| = \left(\bigcup_{i=1}^{m} N_i\right) \cap \mathcal{V}_m.\tag{24}$$

We define a $2^m$-tuplet $M_m$ through $M_m := \{M_{j_1, j_2, \ldots, j_m} \mid j_1, j_2, \ldots, j_m \in \{0, 1\}\}$

$$= \{M_0^{(0)}, M_0^{(1)}, M_0^{(-1, 1)}, M_0^{(-2, 1)}, M_0^{(-3, 1)}, \ldots, M_0^{(-m, 1)}\}.$$ 

Let $E$ be the event that each of $v_1, v_2, \ldots, v_m$ has a degree of $h$. Given $L_m \in L_m^0$, we define $M_m^*(L_m)$ as the set of $M_m$ under the condition that $E$ occurs. Then it’s straightforward to compute $\mathbb{P}[E]$ via

$$\mathbb{P}[E] = \sum_{L_m \in L_m^0, M_m^*(L_m) \in M_m^*(L_m^0)} \mathbb{P}[\{L_m = L_m^* \cap (M_m = M_m^*)\}].\tag{26}$$

Given event $L_m^0 \in L_m^0$ (i.e., there is no edge between vertices in $V_m := \{v_1, v_2, \ldots, v_m\}$), one choice of $M_m$ to have $E$ happen is the following $M_m^0$, which results in that each vertex $v_1, v_2, \ldots, v_m$ has $h$ neighbors in $\mathcal{V}_m = V_m \setminus \{v_{m+1}, v_{m+2}, \ldots, v_n\}$, and that any two of vertices $v_1, v_2, \ldots, v_m$ do not have any common neighbor in $\mathcal{V}_m$. $M_m^0$ satisfies

$$|M_0^{(i, 0-i)}| = h, \quad \text{for } i = 1, 2, \ldots, m;$$

$$|M_{j_1, j_2, \ldots, j_m}| = 0, \quad \text{for } \sum_{i=1}^{m} j_i > 1;$$

$$|M_0| = n - m - hm.$$ 

By (26), we further write $\mathbb{P}[E]$ as the sum of

$$\sum_{L_m \in L_m^0, M_m^*(L_m) \in M_m^*(L_m^0): (L_m^* \notin L_m^0) \text{ or } (L_m^0 \notin M_m^0)} \mathbb{P}[\{L_m = L_m^* \cap (M_m = M_m^*)\}]$$

and

$$\mathbb{P}[\{L_m \in L_m^0 \cap (M_m = M_m^0)\}].\tag{29}$$

From Remark [1 after Lemma 2] we will establish Lemma 2 once proving the following Propositions [1 and 2]. In the rest of the paper, we will often use $1 + x \leq e^x$ for any $x \in \mathbb{R}$ and $1 - xy \leq (1 - x^y) \leq 1 - xy + \frac{x^2y^2}{2}$ for $0 \leq x < 1$ and $y = 0, 1, 2, \ldots, (\text{Fact 2 in } \mathbb{R})$.

**Proposition 1.** Given $P_n \geq 3K_n$ for all $n$ sufficiently large, for a non-negative integer $x$, the term $0^x$ is short for $00\ldots 0$ , and the term $1^x$ is short for $\underbrace{11\ldots 1}_{"x" \text{ number of } 1}$.
with $|\alpha_n| = O(1)$, and $K_n = \omega(1)$, we have
$$\mathbb{P}[v \in M_0 \mid T_m = T_m^*] = o\left(\frac{1}{n}\right).$$

Proposition 2. Given $P_n \geq 3K_n$ for all $n$ sufficiently large,
$$\mathbb{P}[v \in M_0 \mid \{S_{ij}\} = u]\leq K_n^{-1}p_n u + 2p_n^2.$$

V. USEFUL LEMMAS AND THEIR PROOFS

In proving Propositions 1 and 2, we will use the following

Lemma 3. If $P_n \geq 3K_n$, then for any three distinct vertices $v_i, v_j$ and $v_k$ in graph $G_m$, and for any $u = 0, 1, \ldots, K_n$, we have
$$\mathbb{P}[(v_i \cap v_j) \mid (v_i = u)] \leq K_n^{-1}p_n u + 2p_n^2.$$

Lemma 4. Under $P_n \geq 3K_n$ and any $T_m^* = (S_1, S_2, \ldots, S_m) \in T_m$ (i.e., the key set $S_i$ of vertex $v_i$ is specified as $S_i^*$ for $i = 1, 2, \ldots, m$), the following results hold for any vertex $v_i \in T_m$ (i.e., for any $u \in \{m+1, m+2, \ldots, n\}$): we have
$$\mathbb{P}[v_i \in M_{0^m} \mid T_m = T_m^*] \geq 1 - mp_n,$$
and
$$\mathbb{P}[v_i \in M_{0^m} \mid T_m = T_m^*] \leq e^{-mp_n} + mp_n \sum_{1 \leq i \leq n} |S_i^*|,$$
and for any $i = 1, 2, \ldots, m$, we have
$$\mathbb{P}[v_i \in M_{0^m-1,0^m-i} \mid T_m = T_m^*] \leq p_n,$$
and
$$\mathbb{P}[v_i \in M_{0^m-1,0^m-i} \mid T_m = T_m^*] \geq p_n \left(1 - 2mp_n - K_n^{-1}p_n \sum_{j \in \{1, 2, \ldots, m\}\setminus\{i\}} |S_{ij}^*|\right),$$
where $S_{ij}^* = S_i^* \cap S_j^*.$

A. The Proof of Lemma 3

We establish Lemma 3 given
$$\mathbb{P}[\Gamma_v \cap \Gamma_{jt} \mid (v_i = u)] = \mathbb{P}[\Gamma_v = u] + \mathbb{P}[\Gamma_{jt} = u] - \mathbb{P}[\Gamma_v \cap \Gamma_{jt} = u]$$
$$= 2p_n - 1 + \left(\frac{p_n - (2K_n - u)}{K_n}\right) \left(\frac{p_n}{K_n}\right)$$
$$\leq 2p_n - 1 + \left(1 - p_n\right) \frac{2K_n}{K_n}$$
(by Lemma 5.1)
$$\leq 2p_n - p_n(2K_n - u)/K_n + p_n^2[(2K_n - u)/K_n]^2/2$$
$$\leq K_n^{-1}p_n u + 2p_n^2.$$

B. The Proof of Lemma 4

Event $v_i \in M_{0^m}$ equals $\bigcup_{i=1}^m E_{v_i}$, where $E_{v_i}$ is the event that there exists an edge between vertices $v_i$ and $v_j$ in $G_m$. Therefore, by a union bound, the left hand side (L.H.S.) of (30) is no less than $1 - \sum_{i=1}^m \mathbb{P}[E_{v_i} \mid T_m = T_m^*] = 1 - mp_n$, and given Lemma 3, we establish (31) by
$$\mathbb{P}[v_i \in M_{0^m} \mid T_m = T_m^*] \leq 1 - \sum_{i=1}^m \mathbb{P}[E_{v_i} \mid T_m = T_m^*] + \sum_{1 \leq i < j \leq m} \mathbb{P}[E_{v_i} \cap E_{v_j} \mid T_m = T_m^*]$$
$$\leq 1 - mp_n + p_n^2 \sum_{1 \leq i < j \leq m} (K_n^{-1}p_n |S_{ij}^*| + 2p_n^2)$$
$$\leq e^{-mp_n + p_n^2} + K_n^{-1}p_n \sum_{1 \leq i < j \leq m} |S_{ij}^*|.$$

Since event $v_i \in M_{0^m}$ equals the intersection of $E_{v_i}$ and $\bigcup_{j \in \{1, 2, \ldots, m\} \setminus \{i\}} E_{v_j}$, L.H.S. of (32) is at most
$$\mathbb{P}[E_{v_i} \mid T_m = T_m^*] = \mathbb{P}[E_{v_i} \mid T_m = T_m^*] = p_n,$$
and we obtain (33) by
$$\mathbb{P}[v_i \in M_{0^m-1,0^m-i} \mid T_m = T_m^*] \geq p_n \left(1 - 2mp_n - K_n^{-1}p_n \sum_{j \in \{1, 2, \ldots, m\}\setminus\{i\}} |S_{ij}^*|\right).$$

VI. THE PROOF OF PROPOSITION 1

We embark on the evaluation of (28) by computing
$$\mathbb{P}[\{M_m = M_{m^*} \mid \mathcal{L}_m = \mathcal{L}_m^*\}.$$

With $C_m$ and $T_m^*$ defined such that $C_m = (C_m, T_m^*)$, event $(\mathcal{L}_m = \mathcal{L}_m^*)$ is the intersection of events $(\mathcal{C}_m = \mathcal{C}_m^*)$ and $(\mathcal{T}_m = \mathcal{T}_m^*)$. Since $(\mathcal{C}_m = \mathcal{C}_m^*)$ and $(\mathcal{M}_m = \mathcal{M}_m^*)$ are independent, we obtain
$$\mathbb{P}[\{M_m = M_{m^*} \mid \mathcal{T}_m = \mathcal{T}_m^*\}].$$

For any $j_1, j_2, \ldots, j_m \in \{0, 1\}$, for any distinct vertices $v_{w_1} \in T_m$ and $v_{w_2} \in T_m$, events ($v_{w_1} \in M_{j_1,j_2,\ldots,j_m}$) and ($v_{w_2} \in M_{j_1,j_2,\ldots,j_m}$) are not independent but are conditionally independent given $(T_m = T_m^*)$ (with the key sets $S_1, S_2, \ldots, S_m$ specified as $S_1^*, S_2^*, \ldots, S_m^*$, respectively). Therefore,
$$f(n - m, \mathcal{M}_m) \mathbb{P}[v_i \in M_{0^m} \mid T_m = T_m^*] \mathbb{P}[v_i \in M_{0^m} \mid T_m = T_m^*] \times$$
$$\prod_{j_1,j_2,\ldots,j_m \in \{0, 1\}} \mathbb{P}[v_{w_i} \in M_{j_1,j_2,\ldots,j_m} \mid T_m = T_m^*] \mathbb{P}[v_{w_i} \in M_{j_1,j_2,\ldots,j_m} \mid T_m = T_m^*],$$

$$= f(n - m, \mathcal{M}_m) \mathbb{P}[v_i \in M_{0^m} \mid T_m = T_m^*] \mathbb{P}[v_i \in M_{0^m} \mid T_m = T_m^*] \times$$
$$\prod_{j_1,j_2,\ldots,j_m \in \{0, 1\}} \mathbb{P}[v_{w_i} \in M_{j_1,j_2,\ldots,j_m} \mid T_m = T_m^*] \mathbb{P}[v_{w_i} \in M_{j_1,j_2,\ldots,j_m} \mid T_m = T_m^*],$$

(36)
where \( f(\sum_{i=1}^{\ell} x_i, (x_1, x_2, \ldots, x_\ell)) \) is determined via

\[
f(\sum_{i=1}^{\ell} x_i, (x_1, x_2, \ldots, x_\ell)) := \left( \begin{array}{c} \sum_{i=1}^{\ell} x_i \\ x_1 \\ \vdots \\ x_\ell \end{array} \right) \times \left( \begin{array}{c} \sum_{i=1}^{\ell} x_i \\ x_1 \\ \vdots \\ x_\ell \end{array} \right) = \frac{1}{(x_1!x_2!\ldots x_\ell)!} \prod_{i=1}^{\ell} x_i!
\]

for integers \( \ell \geq 1 \) and \( x_i \geq 0, \ i = 1, 2, \ldots, \ell \).

To bound \( \Delta \), we evaluate the right hand side (R.H.S.) of \( \Delta \). First, from \( \Delta \) and

\[
\sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1 j_2 \ldots j_m}^*| = |\mathcal{V}_m| = n - m
\]

which holds by \( \Delta \), we have

\[
f(n - m, M_m^*) = \frac{(\sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1 j_2 \ldots j_m}^*|)!}{\prod_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1 j_2 \ldots j_m}^*|!} \leq \frac{n - m - \sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1 j_2 \ldots j_m}^*|!}{\prod_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1 j_2 \ldots j_m}^*|!} \leq \frac{n}{\sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1 j_2 \ldots j_m}^*|!} \leq n.
\]

Second, for any \( j_1, j_2, \ldots, j_m \in \{0, 1\} \) with \( \sum_{i=1}^{m} j_i \geq 1 \), there exists \( t \in \{0, 1, \ldots, m\} \) such that \( j_t = 1 \), so

\[
P[v_w \in M_{j_1 j_2 \ldots j_m} \mid T_m = T_m^*] \leq P[E_{wt} \mid T_m = T_m^*] = P[E_{wt} \mid S_t = S_t^*] = p_e,
\]

where \( E_{wt} \) is the event that there exists an edge between vertices \( v_w \) and \( v_t \) in graph \( G_m^t \).

Defining \( \Lambda \) by

\[
\Lambda = \sum_{j_1, j_2, \ldots, j_m \in \{0, 1\}} |M_{j_1 j_2 \ldots j_m}^*|,
\]

we obtain from \( \Delta \) that

\[
|M_{0^m}^*| = n - m - \Lambda.
\]

Applying \( \Delta \) to \( |c_m| = 1 \), we derive

\[
\sum_{T_m} \sum_{c_m} \left\{ |P[c_m = c_m^* \mid T_m = T_m^*]| n^{-m-L} \right\} \leq (n^{m-L}) |c_m| = 1, \text{ we derive}
\]

\[
< (h + 1)^{2m-1} \times \sum_{T_m} \sum_{c_m} \left\{ P[c_m = c_m^* \mid T_m = T_m^*] \right\} \times \sum_{c_m} \left\{ P[c_m = c_m^* \mid T_m = T_m^*] \right\} = (h + 1)^{2m-1} |c_m| = 1, \text{ we derive}
\]

\[
< (h + 1)^{2m-1} (n^{m-L}) \times \sum_{T_m} \sum_{c_m} \left\{ P[c_m = c_m^* \mid T_m = T_m^*] \right\} \times \sum_{c_m} \left\{ P[c_m = c_m^* \mid T_m = T_m^*] \right\} = (h + 1)^{2m-1} (n^{m-L}) \times \sum_{T_m} \sum_{c_m} \left\{ P[c_m = c_m^* \mid T_m = T_m^*] \right\} \times \sum_{c_m} \left\{ P[c_m = c_m^* \mid T_m = T_m^*] \right\}.
\]

From \( \Delta \) and \( \lim_{n \to \infty} n p_e = \infty \) by \( \Delta \), the proof of
Proposition 1 is completed once we show
\[
\sum_{T_m \in T_m} \left\{ \mathbb{P}[T_m = T_m'] \mathbb{P}[v_w \in M_0^m \mid T_m = T_m'] \right\} 
\leq e^{-mnpe} \cdot [1 + o(1)]. \tag{51}
\]

A. Establishing \[\text{Lemma 2}\]
From (30) and (31) (viz., Lemma 4), it holds that
\[
\mathbb{P}[\forall v_w \in M_0^m \mid T_m = T_m'] \leq \sum_{i \leq j \leq m} |S'_{ij}| (1 - mp_e)^{-m-h-m}.
\]
where \(S'_{ij} = S'_i \cap S'_j\). With (16) (i.e., \(p_e \sim \frac{\ln n}{n}\)), we have \(m^2 np^2 = o(1)\) and \(mp_e = o(1)\), which are substituted into (52) to induce (51) once we prove
\[
\sum_{T_m \in T_m} \mathbb{P}[T_m = T_m'] e^{\frac{npe}{\ln n} \sum_{i \leq j \leq m} |S'_{ij}|} \leq 1 + o(1). \tag{53}
\]
L.H.S. of (53) is denoted by \(H_{n,m}\) and evaluated below.
For each fixed and sufficiently large \(n\), we consider: a) \(p_n < n^{-\delta} (\ln n)^{-1}\) and b) \(p_n \geq n^{-\delta} (\ln n)^{-1}\), where \(\delta\) is an arbitrary constant with \(0 < \delta < 1\).

a) \(p_n < n^{-\delta} (\ln n)^{-1}\)
From \(p_n < n^{-\delta} (\ln n)^{-1}\), (54) (namely, \(p_e \leq \frac{2 \ln n}{n}\) and \(|S'_n| \leq K_n\) for \(1 \leq i < j \leq m\), it holds that
\[
e^{\frac{npe}{\ln n} \sum_{i \leq j \leq m} |S'_{ij}|} < e^{2 \ln n - n^{-\delta} (\ln n)^{-1} (\gamma)} < e^{m^2 n^{-\delta}},
\]
which is substituted into \(H_{n,m}\) to bring about
\[
H_{n,m} < e^{m^2 n^{-\delta}} \sum_{T_m \in T_m} \mathbb{P}[T_m = T_m'] = e^{m^2 n^{-\delta}}, \tag{53}
\]

b) \(p_n \geq n^{-\delta} (\ln n)^{-1}\)
We relate \(H_{n,m}\) to \(H_{n,m-1}\) and assess \(H_{n,m}\) iteratively. First, with \(T_m = (S'_1, S'_2, \ldots, S'_m)\), event \((T_m = T_m')\) is the intersection of independent events: \((T_{m-1} = T_{m-1}')\) and \((S_m = S'_{m})\).
Then we have
\[
H_{n,m} = \sum_{T_m \in T_m} \mathbb{P}[(T_m-1 = T_{m-1}') \cap (S_m = S'_m)] \cdot e^{\frac{npe}{\ln n} \sum_{i \leq j \leq m-1} |S'_{ij}|} e^{\frac{npe}{\ln n} \sum_{i \leq j \leq m} |S'_{ij}|}.
\]
By \(\sum_{i \leq j \leq m} |S'_{ij}| = \sum_{i \leq j \leq m} |S'_i \cap S'_j| \leq m |S'_m| \cap (\bigcup_{i=1}^{m-1} S'_i)\)
and \(34\) (i.e., \(p_e \leq \frac{2 \ln n}{n}\)), we get
\[
e^{\frac{npe}{\ln n} \sum_{i \leq j \leq m} |S'_{ij}|} \leq e^{2 m^2 n^{-\delta} (\ln n)^{-1} |S'_m|}.
\]
Further leading to
\[
H_{n,m} / H_{n,m-1} \leq \sum_{u=0}^{K_n} \left[ \mathbb{P} \left[ S_m \cap \bigcup_{i=1}^{m-1} S'_i \right] = u \right] e^{2 m^2 n^{-\delta} (\ln n)^{-1} u}.
\]
Since \(S_m\) is a set of \(K_n\) keys, selected uniformly at random from a pool of \(P_n\) keys, denoting \(\bigcup_{i=1}^{m-1} S'_i\) by \(v\), then we obtain that for \(u \in [\max\{0, K_n + v - P_n\}, K_n]\),
\[
\mathbb{P} \left[ |S_m \cap \bigcup_{i=1}^{m-1} S'_i| = u \right] = \frac{\binom{K_n-v}{u} \binom{P_n}{u}}{\binom{P_n}{K_n}}. \tag{56}
\]
From \(v \geq |S'_1| \geq K_n\) and \(v \leq \sum_{i=1}^{m-1} |S'_i| \leq (m-1)K_n < mK_n\), we have \(K_n \leq v < mK_n\), which together with (56)

L.H.S. of (56)
\[
= \prod_{t=0}^{K_n-v-1} (v-t) \cdot \prod_{t=0}^{K_n-u-1} (P_n-v-t) \cdot \frac{K_n!}{(K_n-u)!} \cdot \frac{1}{(P_n-K_n)!} \cdot \frac{1}{(mK_n)^u} \cdot \frac{(mK_n)^u}{(P_n-K_n)K_n}.
\]

R.H.S. of (55)
\[
\leq \sum_{u=0}^{K_n} \frac{1}{u!} \left( \frac{mK_n^2}{P_n-K_n} \cdot e^{2 m^2 n^{-\delta}(\ln n)^{-1}} \right) u \leq e^{m^2 n^{-\delta}(\ln n)^{-1}}.
\]
From (3), we have
\[
1 - p_s = \frac{(P_n-K_n)}{K_n} \frac{P_n}{P_n} \cdot \frac{1}{P_n-K_n} \cdot \frac{K_n-1}{K_n} \leq \frac{1}{P_n-K_n} e^{-K_n^2 n^{-\delta}} / P_n.
\]
For \(n\) sufficiently large, from \(p_n \geq n^{-\delta} (\ln n)^{-1}\) and (54) (i.e., \(p_e = p_n p_n \leq \frac{2 \ln n}{n}\)), we obtain
\[
p_s = p_n^{-1} p_e \leq p_n^{-1} \cdot 2 n^{-1} \ln n \leq 2 n^{-1} (\ln n)^{-2}.
\]
Hence, for \(n\) sufficiently large, we apply (59), (60) and \(P_n \geq 3K_n > 2K_n\) to get
\[
K_n^2 / (P_n - K_n) < 2K_n^2 / P_n \leq -2 \ln (1 - p_s) \leq -2 \ln (1 - 2 \cdot 2 n^{-1} (\ln n)^{-2}) \leq 2 \sqrt{2n} \frac{\ln n}{\ln n} \leq \ln n.
\]
In view of \(-\ln (1 - x) \leq \sqrt{x} \leq 0 \leq 0.4\), which can be proved by analyzing the derivative of \(-\ln (1 - x) - \sqrt{x}\).

Given \(K_n = \omega(1)\), for arbitrary constant \(c > 2\) and for all \(n\)
sufficiently large, $\frac{K_m}{p_m} \geq \frac{4e^{-m}}{(c^2-1)}$ holds. Then
\[ e^{2m \log n - n} \leq e^{\frac{(c^2-1)\log n}{2}} \cdot n = n^{\frac{(c^2-1)\log n}{2}}. \]  (62)

Using (58), (61), and (62) in (55) yields
\[
H_{n,m} / H_{n,m-1} 
\leq \text{R.H.S. of (55)} 
\leq e^{\frac{2\sqrt{2m} - 1}{2} \cdot n - \frac{(c^2-1-\epsilon) \log n}{2}} 
\leq e^{3 \log n n^{\frac{c-1}{c}}} \cdot n^m. \]  (63)

To derive $H_{n,m}$ iteratively based on (63), we compute $H_{n,2}$ below. By definition, setting $m = 2$ in L.H.S. of (53) and considering the independence between events $(S_1 = S_1^*)$ and $(S_2 = S_2^*)$, we obtain
\[
H_{n,2} = \sum_{S_1^* \in S_2^*} P[S_1 = S_1^*] \sum_{S_2^* \in S_2^*} P[S_2 = S_2^*] e^{\frac{p_m \log n_1}{K_m} |S_1^* \cap S_2^*|}. \]  (64)

Clearly, $\sum_{S_2^* \in S_2^*} P[S_2 = S_2^*] e^{\frac{p_m \log n_1}{K_m} |S_1^* \cap S_2^*|}$ equals R.H.S. of (53) with $m = 2$. Then from (63) and (64),
\[
H_{n,2} \leq \sum_{S_1^* \in S_2^*} P[S_1 = S_1^*] e^{6n^{\frac{c-1}{c}}} \cdot n = e^{6n^{\frac{c-1}{c}}} \cdot n. \]  (65)

Therefore, it holds via (63) and (65) that
\[
H_{n,m} \leq e^{6n^{\frac{c-1}{c}}} \cdot n \leq e^{\frac{3}{2}(m^2+m-2)n^{-\frac{1}{c}}} \cdot n. \]
Finally, summarizing cases a) and b), we report
\[
H_{n,m} \leq \max \left\{ e^{m^2n^{-\delta}} \cdot n, e^{\frac{3}{2}(m^2+m-2)n^{-\frac{1}{c}}} \cdot n \right\}. \]
With $n \to \infty$, $H_{n,m} \leq 1 + o(1)$ (i.e., (53)) follows.

VII. THE PROOF OF PROPOSITION 2
We define $C_m^{(0)}$ and $T_m^{(0)}$ by
\[
C_m^{(0)} = \left\{ \begin{array}{ll} 0, 0, \ldots, 0, \\
\text{2 number of “0”} \end{array} \right. 
\]
and
\[
T_m^{(0)} = \{ T_m \mid S_i \cap S_j = \emptyset, \forall i, j \} \text{\ with } 1 \leq i < j \leq m \}. \]
Clearly, $(C_m = C_m^{(0)})$ or $(T_m \in T_m^{(0)})$ each implies $(L_m \in L_m^{(0)})$. Also, $(C_m = C_m^{(0)})$ and $(M_m = M_m^{(0)})$ are independent with each other. Therefore, with (29) = $P(\{L_m \in L_m^{(0)} \cap (M_m = M_m^{(0)})\})$, we get
\[
(29) \geq P[C_m = C_m^{(0)}] P[M_m = M_m^{(0)}], \]  (66)
and
\[
(29) \geq P[T_m \in T_m^{(0)}] P[(M_m = M_m^{(0)}) | (T_m \in T_m^{(0)})]. \]  (67)

Given $(C_m = C_m^{(0)}) = \bigcup_{1 \leq i < j \leq m} C_{ij}$ and $(T_m \in T_m^{(0)}) = \bigcup_{1 \leq i < j \leq m} T_{ij}$, applying the union bound, we obtain
\[
P[C_m = C_m^{(0)}] \geq 1 - \sum_{1 \leq i < j \leq m} P[C_{ij}] \geq 1 - m^2 p_n / 2, \]  (68)
and
\[
P[T_m \in T_m^{(0)}] \geq 1 - \sum_{1 \leq i < j \leq m} P[T_{ij}] \geq 1 - m^2 p_s / 2. \]  (69)

In the following two subsections, we will prove
\[
P[ M_m = M_m^{(0)} ] \sim (h!)^{-m} (np_e)^{hm} e^{-mnp}, \]  (70)
and
\[
P[ (M_m = M_m^{(0)}) \mid (T_m \in T_m^{(0)}) ] \geq (h!)^{-m} (np_e)^{hm} e^{-mnp} \cdot [1 - o(1)]. \]  (71)

Substituting (68) and (70) into (66), and applying (69) and (71) to (66), we have
\[
(29) \geq \frac{(h!)^{-m} (np_e)^{hm} e^{-mnp}}{1 - \min \{ p_s, p_n \} \cdot m^2 / 2 \cdot [1 - o(1)]. \]  (72)

From (70), we get
\[
(29) \leq P[ M_m = M_m^{(0)} ] \leq (h!)^{-m} (np_e)^{hm} e^{-mnp} \cdot [1 + o(1)]. \]  (73)
Combining (72) and (73), and using
\[
\min \{ p_s, p_n \} \leq \sqrt{p_s p_n} = \sqrt{p_e} \leq \sqrt{\frac{2 \log n}{n}} = o(1) \]
which holds from $p_e = p_s p_n$ and (34), Proposition 2 follows. Below we detail the proofs of (70) and (71).

A. Establishing (70)
We write $P[ M_m = M_m^{(0)} ]$ as
\[
\sum_{T_m \in T_m^{(0)}} \{ P[T_m = T_m^{(0)}] P[(M_m = M_m^{(0)}) | (T_m = T_m^{(0)})] \}; \]
where $P[(M_m = M_m^{(0)}) | (T_m = T_m^{(0)})]$ equals
\[
f(n-m, M_m^{(0)}) P[v_{i} \in M_{i-m} \mid T_m = T_m^{*}]^{n-m-h_m} \]
\[
\times \prod_{i=1}^{m} P[v_{i} \in M_{i-1,0}^{*} \mid T_m = T_m^{*}]^{h_i}, \]
with function $f$ specified in (37). From (27) and (40),
\[
f(n-m, M_m^{(0)}) = \frac{(n-m)!}{(n-m-h_m)!(h!)^m} \sim (h!)^{-m} n^{hm}. \]  (74)
We will establish
\[
\sum_{T_m \in T_m^{*}} \{ P[T_m = T_m^{*}] \prod_{i=1}^{m} P[v_{i} \in M_{i-1,0}^{*} \mid T_m = T_m^{*}]^{h_i} \} \]
\[
\geq p_e^{hm} \cdot [1 - o(1)]. \]  (75)
We use (74) and (75) as well as (30) (viz., Lemma 3) in evaluating \( P[M_m = M_m^{(0)}] \) above. Then
\[
P[M_m = M_m^{(0)}] \\
\geq (h!)^{-m}n^{-hm} \cdot [1 - o(1)] \cdot (1 - m p_e)^n \times \\
\sum_{T_m \in T_m^{(0)}} P[T_m = T_m^{(h)}] \prod_{i=1}^m \left\{ P[v_w \in M_{0^{i-1},1,0^{m-i}} \mid T_m = T_m^{(h)}] \right\} \\
\geq (h!)^{-m} (n p_e)^{hm} e^{-mp_e} \cdot [1 - o(1)]. \tag{76}
\]
Substituting (51) (74) above and (32) in Lemma 3 into the computation of \( P[M_m = M_m^{(0)}] \) yields
\[
P[M_m = M_m^{(0)}] \\
\leq (h!)^{-m} n^{-hm} p_e^{hm} \times [1 + o(1)] \times \\
\sum_{T_m \in T_m^{(0)}} P[T_m \in M_{0^{m-1}} \mid T_m = T_m^{n-m-hm}} \\
\sim (h!)^{-m} (n p_e)^{hm} e^{-mp_e}. \tag{77}
\]
Then (70) follows from (76) and (77). Namely, (70) holds upon the establishment of (75), which is proved below. First, from (33) in Lemma 4 with \( T_m = (S_{1j}^*, S_2^*, \ldots, S_m^*) \) and \( S_{ij}^* = S_i^* \cap S_j^* \), we get
\[
\prod_{i=1}^m P[v_w \in M_{0^{i-1},1,0^{m-i}} \mid T_m = T_m^{(h)}] \\
\geq p_e^{hm} \prod_{i=1}^m \left[ 1 - \left( 2 m p_e + \frac{m n}{K_n} \sum_{j \in \{1,2,\ldots,m\} \backslash \{i\}} \frac{|S_{ij}^*|}{m} \right) \right]^h \\
\geq p_e^{hm} \left[ 1 - 2 h m p_e^2 - \frac{2 h m p_e n}{K_n} \sum_{1 \leq i < j \leq m} |S_{ij}^*| \right].
\]
With \( p_e = o(1) \) by (16), we obtain (75) once proving
\[
\frac{p_n}{K_n} \sum_{T_m^{(0)}} P[T_m = T_m^{*}] \sum_{1 \leq i < j \leq m} |S_{ij}^*| = o(1). \tag{78}
\]
If \( T_m^{*} \in T_m^{(0)} \), then \( |S_{ij}^*| = 0 \). Consequently, from (69), the proof of (78) becomes evident by
\[
\text{L.H.S. of (73)} \\
\leq p_n \cdot m (m - 1)/2 \cdot P[T_m^{*} \in T_m^{(0)}] \\
\leq p_n \cdot m^2/2 \cdot m^2 p_s/2 \leq m^4 n^{-1} \ln n/2 = o(1).
\]
B. Establishing (77)
\[
P[M_m = M_m^{(0)}] \mid (T_m \in T_m^{(0)}) \\
\text{is equivalent to } P[M_m = M_m^{(0)}] \mid (T_m = T_m^{*}) \text{ for any } T_m \in T_m^{(0)}, \text{ so it follows that}
\]
\[
\Delta = f(n - m, M_m^{(0)}) \cdot P[v_w \in M_{0^{n-1}}, T_m = T_m^{*}]^{n-m-hm} \\
\times \prod_{i=1}^m \left\{ P[v_w \in M_{0^{i-1},1,0^{m-i}} \mid T_m = T_m^{(h)}] \right\}, \tag{79}
\]
with \( f(n - m, M_m^{(0)}) \) given by (74). For \( T_m \in T_m^{(0)} \), from \( |S_{ij}^*| = 0 \) and (33) in Lemma 4 we derive
\[
P[v_w \in M_{0^{i-1},1,0^{m-i}} \mid T_m = T_m^{*}] \geq p_e (1 - 2m p_e). \tag{80}
\]
Substituting (74) (80) above and (30) in Lemma 4 into (75), we conclude that
\[
\Delta \geq (h!)^{-m} n^{-hm} \cdot [1 - o(1)] \\
\times (p_e)^{hm} (1 - 2 m p_e)^{hm} \cdot (1 - m p_e)^{n-m-hm} \\
\sim (h!)^{-m} (n p_e)^{hm} e^{-mp_e}.
\]
VIII. Conclusion
Random key graphs have received considerable attention recently and been used in a wide range of applications ranging from key predistribution in wireless sensor networks to modeling social networks. In this paper, for the intersection of an Erdős–Rényi graph and a random key graph, we derive asymptotically exact probabilities for k-edge-connectivity, k-vertex-connectivity, and the property of minimum vertex degree being at least \( k \). Our results are new even with \( k \) set as 1 for the graph intersection, and also new with general \( k \) for random key graphs without intersecting Erdős–Rényi graphs.

References


