On the intersection of random graphs with an application to random key pre-distribution[ab]

Armand M. Makowski

ECE & ISR/HyNet
University of Maryland at College Park
armand@isr.umd.edu

[a]Supported by NSF Grants CCF-0830702 and CCF-1217997.
[b]Joint work with N. Prasanth Anthapadmanabhan and O. Yağan

The big picture

Intersecting graphs

Assume given two graphs with vertex set V, say

$$G_1 \equiv (V, E_1) \quad \text{and} \quad G_2 \equiv (V, E_2)$$

The **intersection** of the two graphs $G_1 \equiv (V, E_1)$ and $G_2 \equiv (V, E_2)$ is the graph (V, E) with

$$E := E_1 \cap E_2$$

We write

$$G_1 \cap G_2 := (V, E_1 \cap E_2)$$

Capturing multiples constraints

Adjacency expresses constraints/relationships which can be **physical**, **logical**, **sociological**, etc.

E.g., for two constraints:

- Communication constraint and link quality (e.g., fading)
- Communication constraint and secure link (e.g., via shared key)
- Membership in two different social networks

Random graphs

For vertex set V, let $\mathcal{E}(V)$ denote the collection of all sets of (undirected) edges on V. A **random graph** with vertex set V is simply an $\mathcal{E}(V)$-valued rv defined on some probability triple $(\Omega, \mathcal{F}, \mathbb{P})$, say $\mathbb{E} : \Omega \to \mathcal{E}(V)$.

We write

$$\mathbb{G} \equiv (V, \mathbb{E})$$

Erdős-Rényi graphs, generalized random graphs, geometric random graphs, random key graphs, small worlds, random threshold graphs, multiplicative attribute graphs, growth models (e.g., preferential attachment models, fitness-based models)

Constructing (undirected) random graphs

Convenient to write

$$V \equiv \{1, \ldots, n\}.$$

Random link assignments encoded through $\{0, 1\}$-valued rvs

$$\{L_{ij},\ 1 \leq i < j \leq n\}$$

with

$$L_{ij} = \begin{cases} 1 & \text{if } (i,j) \text{ up} \\ \\ 0 & \text{if } (i,j) \text{ down} \end{cases}$$

Distinct nodes $i, j = 1, \ldots, n$ are **adjacent** if $L_{ij} = 1$, and an **undirected** link is assigned between nodes i and j.

Examples:

- Erdős-Renyi (Bernoulli) graphs
- Geometric random graphs – Disk models
- Random key graphs

Intersecting random graphs

Assume given two random graphs with **same** vertex set V, say

$$\mathbb{G}_1 \equiv (V, \mathbb{E}_1) \quad \text{and} \quad \mathbb{G}_2 \equiv (V, \mathbb{E}_2)$$

The **intersection** of the two random graphs $\mathbb{G}_1 \equiv (V, \mathbb{E}_1)$ and $\mathbb{G}_2 \equiv (V, \mathbb{E}_2)$ is the random graph $(V, \mathbb{E})$ where

$$\mathbb{E} := \mathbb{E}_1 \cap \mathbb{E}_2$$

We write

$$\mathbb{G}_1 \cap \mathbb{G}_2 = (V, \mathbb{E}_1 \cap \mathbb{E}_2)$$

Equivalently,

$$L_{ij} = L_{1,ij} \cdot L_{2,ij}, \quad 1 \leq i < j \leq n$$

Throughout the **component** random graphs $\mathbb{G}_1$ and $\mathbb{G}_2$ are assumed to be **independent**:

The collections $\{L_{1,ij},\ 1 \leq i < j \leq n\}$ and $\{L_{2,ij},\ 1 \leq i < j \leq n\}$ are independent.

A basic objective

Inheritance – Understand how the structural properties of the random graph $\mathbb{G}_1 \cap \mathbb{G}_2$ are shaped by those of the **component** random graphs $\mathbb{G}_1$ and $\mathbb{G}_2$

Focus on graph **connectivity** and on the **absence** of isolated nodes – Easier and hopefully asymptotically equivalent

---

After all

$$2^{\frac{n(n-1)}{2}} \text{ possible graphs on } V$$

and **typical** behavior explored **asymptotically** via

Zero-one Laws

A basic source of difficulty

$$\mathbb{G}_1 \cap \mathbb{G}_2 \text{ connected}$$

implies

$$\mathbb{G}_1 \text{ and } \mathbb{G}_2 \textbf{ both} \text{ connected}$$

But the converse is **false!**

$$V = \{1, 2, 3\}: \qquad \begin{aligned} E_1 &: 1 \sim 2 \sim 3 \\ E_2 &: 1 \sim 3 \sim 2 \\ E_1 \cap E_2 &: 2 \sim 3 \end{aligned}$$

Similar comment when considering the absence of isolated nodes

Examples of random graphs and their zero-one laws

Erdős-Renyi (ER) graphs $\mathbb{G}(n;p)$

Random link assignment encoded through **i.i.d.** $\{0,1\}$-valued rvs

$$\{L_{ij},\ 1 \leq i < j \leq n\}$$

with

$$\mathbb{P}\left[L_{ij} = 1\right] = p$$

for some $0 < p < 1$.

Also known as Bernoulli graphs

Strong zero-one law for graph connectivity in ER graphs $\mathbb{G}(n;p)$ $(0<p<1)$ [**Erdős and Renyi**]: Whenever

$$p_n \sim c\,\frac{\log n}{n}$$

for some $c>0$, we have

$$\lim_{n\to\infty}\mathbb{P}\left[\mathbb{G}(n;p_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } 0<c<1 \\ \\ 1 & \text{if } 1<c \end{cases}$$

Same zero-one law for absence of isolated nodes

Critical scaling for graph connectivity:

$$p_n^\star := \frac{\log n}{n}, \quad n=1,2,\ldots$$

We also have the **weak** zero-one law:

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n;p_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \frac{p_n}{p_n^\star} = 0 \\ \\ 1 & \text{if } \lim_{n\to\infty} \frac{p_n}{p_n^\star} = \infty \end{cases}$$

Simple consequence of strong zero-one law by the **monotonicity** of the mapping

$$p \to \mathbb{P}\left[\mathbb{G}(n;p) \text{ is connected}\right]$$

Geometric random graphs $\mathbb{G}(n;\rho)$

Population of n nodes located at $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ in a bounded convex region $\mathbb{A} \subset \mathbb{R}^2$.

With $\rho > 0$, nodes i and j are adjacent if

$$\|\boldsymbol{X}_i - \boldsymbol{X}_j\| \leq \rho$$

so that

$$L_{ij} = \mathbf{1}\left[\|\boldsymbol{X}_i - \boldsymbol{X}_j\| \leq \rho\right]$$

Usually, **i.i.d.** node locations $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ which are **uniformly** distributed on unit square or unit disk – Disk model

Strong zero-one law for graph connectivity in geometric random graphs $\mathbb{G}(n;\rho)$ $(\rho > 0)$ [**Penrose, Gupta and Kumar**]: Whenever

$$\pi \rho_n^2 \sim c \, \frac{\log n}{n}$$

for some $c > 0$, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n;\rho_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } \ 0 < c < 1 \\ \\ 1 & \text{if } \ 1 < c \end{cases}$$

Same zero-one law for absence of isolated nodes

Critical scaling for graph connectivity:

$$\pi \left(\rho_n^\star\right)^2 = \frac{\log n}{n}, \quad n = 1, 2, \ldots$$

A random key pre-distribution scheme (Eschenauer and Gligor 2002)

For integers P and K with $1 \leq K < P$, let $\mathcal{P}_K$ denote the collection of all subsets of $\{1, \ldots, P\}$ with exactly K elements

---

For each node $i = 1, \ldots, n$, with $\theta = (P, K)$, let $K_i(\theta)$ denote the **random** set of K **distinct** keys assigned to node i

---

Under the EG scheme, 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

$$\mathbb{P}\left[K_i(\theta) = S\right] = \binom{P}{K}^{-1}, \quad S \in \mathcal{P}_K, \ i = 1, \ldots, n$$

The random key graph $\mathbb{K}(n;\theta)$

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

$$K_i(\theta) \cap K_j(\theta) \neq \emptyset.$$

In other words,

$$L_{ij}(\theta) := \mathbf{1}\left[K_i(\theta) \cap K_j(\theta) \neq \emptyset\right]$$

For distinct $i, j = 1, \ldots, n$,

$$q(\theta) = \mathbb{P}\left[K_i(\theta) \cap K_j(\theta) = \emptyset\right] = \frac{\binom{P-K}{K}}{\binom{P}{K}}.$$

Strong zero-one law for graph connectivity in random key graphs $\mathbb{K}(n;\theta)$ $(K < P)$ [**Di Pietro et al., Burbank and Gerke, Rybarczyk, YM**]: Whenever

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

for some $c > 0$, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n;\theta_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } 0 < c < 1 \\ \\ 1 & \text{if } 1 < c \end{cases}$$

Same zero-one law for absence of isolated nodes

Observation: With $\lim_{n\to\infty} q(\theta_n) = 1$,

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

Observation

All cases discussed so far are "**homogeneous**" with a well-defined **link probability** $p(\mathbb{G})$:

$$p(\mathbb{G}) = \text{Probability that two nodes are adjacent in } \mathbb{G}$$

Zero-one laws for connectivity and absence of isolated nodes are determined by conditions on $p(\mathbb{G})$, or **proxy** thereof:

$$p(?(n, ?_n) \sim c\ \frac{\log n}{n}$$

for some $c > 0$

ER graphs $\mathbb{G}(n;p)$:	p
Random geometric graphs $\mathbb{G}(n;\rho)$:	$\ldots$ but $\pi\rho^2$
Random key graphs $\mathbb{K}(n;\theta)$:	$1-q(\theta)$ but $\frac{K^2}{P}$

Intersecting random graphs and their zero-one laws

Three examples

Secure links via key sharing under partial visibility with an on-off communication model:

$$\mathbb{G}(n;p) \cap \mathbb{K}(n;\theta)$$

Disk model with possibility of defective links due to fading:

$$\mathbb{G}(n;\rho) \cap \mathbb{G}(n;p)$$

Disk model with possibility of secure links via key sharing:

$$\mathbb{G}(n;\rho) \cap \mathbb{K}(n;\theta)$$

With $n \to \infty$,

In all cases mentioned earlier, elements of a limiting theory are available for the **component** random graphs: Zero-one laws hold for graph **connectivity** and **absence** of isolated nodes when the parameters are properly scaled with n

---

Inheritance – For a given random intersection graph,

- Zero-one laws for graph **connectivity** and for the **absence** of isolated nodes?
- Critical thresholds?
- Width of phase transitions?

A silly detour: Intersecting ER graphs

With $\mathbb{G}_1 \equiv \mathbb{G}(n, p_1)$ and $\mathbb{G}_2 \equiv \mathbb{G}(n, p_2)$, then

$$\mathbb{G}_1 \cap \mathbb{G}_2 =_{st} \mathbb{G}(n, p) \quad \text{with} \quad p := p_1 \cdot p_2$$

under the **independence** of the components.

Whenever

$$p_n = p_{1,n} \cdot p_{2,n} \sim c \, \frac{\log n}{n}$$

for some $c > 0$, we have

$$\lim_{n \to \infty} \mathbb{P}\left[\mathbb{G}(n; p_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } \; 0 < c < 1 \\ \\ 1 & \text{if } \; 1 < c \end{cases}$$

Zero-law holds for $\mathbb{G}(n, p_1) \cap \mathbb{G}(n, p_2)$ whenever

$$p_n = p_{1,n} \cdot p_{2,n} = \frac{1}{2}\frac{\log n}{n}, \quad n = 1, 2, \ldots$$

Yet one-law holds for $\mathbb{G}(n, p_1)$ and $\mathbb{G}(n, p_2)$ with

$$p_{1,n} = p_{2,n} = \sqrt{\frac{1}{2}\frac{\log n}{n}}, \quad n = 1, 2, \ldots$$

since

$$\lim_{n\to\infty} \frac{\sqrt{\frac{1}{2}\frac{\log n}{n}}}{\frac{\log n}{n}} = \lim_{n\to\infty} \sqrt{\frac{1}{2}} \cdot \sqrt{\frac{n}{\log n}} = \infty$$

Easy to understand what is going on here **because**

$$\mathbb{G}(n; p_1) \cap \mathbb{G}(n; p_2) =_{st} \mathbb{G}(n, p) \quad \text{with} \quad p := p_1 \cdot p_2$$

but this yields so little **insight**! Yet ...

Intersecting ER graphs is trivial but what about other situations?

Natural question: Might it still be the case that zero-one laws are determined by conditions on the link assignment probability

$$p(\mathbb{G}_1 \cap \mathbb{G}_2) = p(\mathbb{G}_1) \cdot p(\mathbb{G}_2) \quad [\textbf{Independence}]$$

Remember in "one dimension"!

Intersecting $\mathbb{G}(n;p)$ and $\mathbb{K}(n;\theta)$

This time,

$$\mathbb{G}(n;p) \cap \mathbb{K}(n;\theta) \neq_{st} \mathbb{G}(n;p') \quad \text{for some } p' = p'(p,\theta)$$

$$\mathbb{G}(n;p) \cap \mathbb{K}(n;\theta) \neq_{st} \mathbb{K}(n;\theta') \quad \text{for some } \theta' = \theta'(p,\theta)$$

But not all is lost!

$$p\left(\mathbb{G}(n;p)\right) = p$$

and

$$p\left(\mathbb{K}(n;\theta)\right) = (1 - q(\theta))$$

so that

$$p\left(\mathbb{G}(n;p) \cap \mathbb{K}(n;\theta)\right) = p \cdot (1 - q(\theta))$$

Conjecture?

Strong zero-one law for connectivity and absence of isolated nodes in $\mathbb{G}(n;p) \cap \mathbb{K}(n;\theta)$: Whenever

$$p_n \left(1 - q(\theta_n)\right) \sim c \, \frac{\log n}{n}$$

for some $c > 0$, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n;p_n) \cap \mathbb{K}(n;\theta_n) \ldots\right] = \begin{cases} 0 & \text{if } \; 0 < c < 1 \\ \\ 1 & \text{if } \; 1 < c \end{cases}$$

Indeed correct ...

Connectivity:

Yağan (2012) provided $\lim_{n\to\infty} p_n \log n$ exists and there exists $\sigma > 0$ such that

$$\sigma n \leq P_n, \quad n = 1, 2, \ldots$$

Absence of isolated nodes:

Makowski and Yağan (2013) without any additional condition!

Let $I_n(p, \theta)$ denote the **number** of isolated nodes in the intersection graph $\mathbb{G}(n; p) \cap \mathbb{K}(n; \theta)$, so that

$$\mathbb{P}\left[\mathbb{G}(n; p) \cap \mathbb{K}(n; \theta) \text{ has no isolated node}\right] = \mathbb{P}\left[I_n(p, \theta) = 0\right]$$

Method of **first** and **second moments** via the standard bounds

---

$$1 - \mathbb{E}\left[I_n(p, \theta)\right] \leq \mathbb{P}\left[I_n(p, \theta) = 0\right]$$

and

$$\mathbb{P}\left[I_n(p, \theta) = 0\right] \leq 1 - \frac{\left(\mathbb{E}\left[I_n(p, \theta)\right]\right)^2}{\mathbb{E}\left[I_n(p, \theta)^2\right]}$$

Need to figure out whether

$$\lim_{n\to\infty} \mathbb{E}\left[I_n(p_n, \theta_n)\right] = 0$$

and

$$\lim_{n\to\infty} \frac{\left(\mathbb{E}\left[I_n(p_n, \theta_n)\right]\right)^2}{\mathbb{E}\left[I_n(p_n, \theta_n)^2\right]} = 1$$

under the appropriate conditions

Easy to see that

$$\mathbb{E}\left[I_n(p,\theta)\right] = n\left(1-p(1-q(\theta))\right)^{n-1}$$

so that

$$\begin{aligned}\lim_{n\to\infty}\mathbb{E}\left[I_n(p_n,\theta_n)\right] &= \lim_{n\to\infty} n\left(1-c_n\frac{\log n}{n}\right)^{n-1}\\ &= \begin{cases}\infty & \text{if } 0<c<1 - \textbf{Beware}\\ \\ 0 & \text{if } 1<c\end{cases}\end{aligned}$$

with $\lim_{n\to\infty} c_n = c$

$$n\left(1-c_n\frac{\log n}{n}\right)^{n-1} = e^{\log n-(n-1)c_n\frac{\log n}{n}+\ldots}$$

Expression available for

$$\frac{\left(\mathbb{E}\left[I_n(\theta)\right]\right)^2}{\mathbb{E}\left[I_n(p,\theta)^2\right]}$$

but far more complicated!

Zero-law for connectivity follows. One-law handled by arguments similar to the ones used by Yağan and Makowski (2012)

Additional results

$$\mathbb{G}(n, \rho) \cap \mathbb{G}(n, p)$$

Yi et al (2006), Prasanth Anthapadmanabhan and Makowski (2010), Penrose (2013)

$$\mathbb{G}(n, \rho) \cap \mathbb{K}(n, \theta)$$

Yi et al (2006), Santhana Krishnan et al. (2013)