The Strange Logic of Random Graphs

0-1 Laws for Random Graphs

Jonathan Hermon

Weizmann Institute of Science

December 13, 2011

Lecture material by Joel Spencer

Motivation

Problems

- Large graphs are very hard to analyze.
- Analyzing a large graph “manually” is rather primitive.
- Large graphs are everywhere: social networks, actors playing together in movies, biology, etc.
- Sometimes we want to show that there is some graph with a certain property but we do not know how to construct such a graph.

A Possible Solution

Analyzing the typical behaviour of a random graph with “similar properties”. There are several known models for doing this. Today we discuss a simple model that capture just a little of the reality of real life large networks, but is easy to analyze, so we can say a lot about this model

Motivation

Proving existence of a certain graph

- Let A be some graph property.
- We pick a graph randomly with distribution D such that D gives positive weight to any simple graph with n vertices.
- If $\mathbb{P}$[the graph we pick has property A] > 0, then there must be some simple graph with n vertices that has property A

The Erdös—Rényi Model

Definition

$G \sim G(n,p)$ if V(G)=[n], G is a simple undirected graph, and every edge $\{$i,j$\}$ is included in the graph with probability p, and this event is independent for different edges.

Remark

- This is exactly bond percolation on K_n - the complete graph on n vertices.
- $\Omega = \{G \mid$ V(G)=[n], G is a simple undirected graph$\}$.
- For any H in Ω if $G \sim G(n,p)$ $Pr[G = H] = p^{|E(H)|}(1-p)^{\binom{n}{2}-|E(H)|}$.

Example Application

Definition

The k'th diagonal Ramsey number R_k is
$min\{n \,|$for any 2 coloring of the edges of K_n there is a monochromatic copy of $K_k\}$

Theorem

Let R_k be the k'th diagonal Ramsey number. Then: $R_k > 2^{k/2}$.

Proof.

Let $G \sim G(n, \frac{1}{2})$, $n \leq 2^{k/2}$. We calculate:

$$\mathbb{P}[\text{G has } K_k \text{ as a subgraph}] \leq_1 \mathbb{P}[\cup\{v_{i_1}, ..., v_{i_k} \text{ form a copy of } K_k\}]$$

$$\leq_2 \binom{n}{k} 2^{-\binom{k}{2}} \leq_3 \left(\frac{n}{2 \cdot 2^{-(k-1)/2}}\right)^k \leq_4 \left(\frac{\sqrt{2}}{2}\right)^k < \frac{1}{2}$$

1) The union is taken over all disjoint k-tuples of vertices.
2) Union bound. 3) Since $2^k \leq k!$. 4) By our assumption on n. □

We color all edges of K_n randomly. Each edge, independently from the other edges, is colored either in red or blue with probability $\frac{1}{2}$ for each color. We obtain 2 graphs G_{red}, G_{blue} both of them $\sim G(n, \frac{1}{2})$.
$\mathbb{P}$[in our random coloring there is a monochromatic copy of K_k] $=$ $\mathbb{P}[G_{red}$ has K_k as a subgraph $\cup$ G_{blue} has K_k as a subgraph] $< \frac{1}{2} + \frac{1}{2} = 1$. So with positive probability there is no monochromatic copy of K_k, i.e. there is some 2-coloring of the

Graph properties

Examples

- Being connected.
- Hamiltonicity
- Having a giant component
- Having a specific graph as a subgraph.
- Having a radius of length 2.

How to define graph properties?

Suggestion 1

We can identify a property A with the set of graphs that satisfy the property.

Suggestion 2

Define a language for graphs and write the property as a sentence in that language (i.e. describe the property by some formula). We will soon do that.

Monotone Properties

Definition

A property B is said to be monotone if whenever G has property B and $G < G'$ (i.e. G' is obtained from G by adding edges to G), then G' also has property B.

Claim

Let A be a monotone property. If $p < q$, then $\mathbb{P}_p(A) < \mathbb{P}_q(A)$ (Where $\mathbb{P}_p(A) := \mathbb{P}_p(G(n,p) \models A) :=$ the probability that $G \sim G(n,p(n))$ has property A).

Proof

Proof.

We couple $G \sim G(n,p)$ and $H \sim G(n,q)$ in the same probability space such that always $G \leq H$.
For each edge $\{i,j\}$ we take $e(i,j) \sim U(0,1)$, such that all these random variables are independent. The edge $\{i,j\}$ exists in G iff $e(i,j) < p$, and it exists in H iff $e(i,j) < q$ ☐

Threshold Functions

Definition

A function $f(n)$ is said to be a threshold function for property B if the following hold:

- If $p(n) \ll f(n)$ then $\lim_{n\to\infty} \mathbb{P}_{p(n)}(G(n,p(n)) \models B) = 0$
- If $f(n) \ll p(n)$ then $\lim_{n\to\infty} \mathbb{P}_{p(n)}(G(n,p(n)) \models B) = 1$
  Where $G(n,p(n)) \models B$ is notation for $G \sim G(n,p(n))$ has property B.

Remark

- The threshold function is not defined uniquely. It is defined up to constant and addition/substraction of negligible terms
- The threshold function plays a similar roll to the critical value phenomena we encounter in percolation on infinite graphs; But usually there is a small window around $c \cdot f(n)$ in which the probability goes from nearly 0 to nearly 1, so there is no immediate phase transition.

Monotone properties have threshold functions

Claim

Any monotone property A has a threshold function.

Proof.

For a fixed n, $\mathbb{P}_p(A) = \sum_{\{H\in\Omega \,|\, H\models A\}} \mathbb{P}_p(H)$. This is a polynomial in p so by the intermediate value theorem $\exists p(n)$ s.t. $\mathbb{P}_{p(n)}(A) = \epsilon$. We check that $p(n)$ satisfies the first condition of a threshold function. the second direction is verified similarly.
Let $C \in \mathbb{N}$ s.t $(1-\epsilon)^C \leq \epsilon$. By Bernoulli inequality $1-(1-p(n))^C \leq C \cdot\ p(n)$. But if $H \sim G_1 \cup G_2 \cup ... \cup G_C$ where each $G_i \sim G(n, p(n))$ independently from the others, then $H \sim G(n, 1-(1-p(n))^C)$. So by monotonicity of A we have:

$$\mathbb{P}_{c\cdot p(n)}(A) \geq \mathbb{P}_{1-(1-p(n))^C}(A) = \mathbb{P}(H \models A) \geq \mathbb{P}(\cup_{i=1}^{C}\{G_i \models A\})$$

$$= 1-(1-\epsilon)^C \geq 1-\epsilon$$

□

The Evolution of G(n,p)

The Evolution of G(n,p)

When p=0 G(n,p) has no edges, and when p=1 G(n,p)=k$_n$. As p gradually increases G(n,p) becomes denser and we see more and more monotone properties appearing.

- Around $p(n) = n^{-2}$ edges start appearing.
- Around $p(n) = n^{(-1-\frac{1}{k})}$ all trees with k+1 vertices appear.
- Around $p(n) = \frac{1}{n}$ triangles appear, a giant component appears and the graph becomes nonplanar.
- Around $p(n) = \frac{ln(n)}{n}$ the graph becomes connected.
- Let H be some graph. Denote $c(H) = max\{\frac{|E(H')|}{|V(H')|} \mid H' \subseteq H\}$. Then H appears as a subgraph around $p(n) = n^{-c(H)}$

The main Theorem

Observation

Non of the threshold functions above are constant or of the form $n^{-\alpha}$, where α is irrational.

Theorem (Fagin 1976 - 0-1 Law)

Let $p(n)$ be a sequence s.t. for any fixed s $[p(n)(1-p(n))]^s n \gg ln(n)$, then for any property, A, expressible in the language of graphs (which will be defined soon) we have exactly one of the following:

- $\lim_{n\to\infty} \mathbb{P}_{p(n)}(G(n,p(n)) \models A) = 1$
- $\lim_{n\to\infty} \mathbb{P}_{p(n)}(G(n,p(n)) \models A) = 0$

And the value of the limit for any fixed A is the same for all such sequences!

Interpretation of the theorem

Immediate corollaries

- For any fixed p we have the zero one law.
- Since the value of the limit (0 or 1) is the same for all p, no constant p is a threshold functions and there are no phase transitions!

Spencer Shelah 0-1 Law

Theorem (J. Spencer S. Shelach 0-1 Law 1988)

For any irrational $0 < \alpha < 1$, $p(n) = n^{-\alpha}$ satisfies the 0-1 law: That is, for any property, A, expressible in the language of random graphs (which will be defined soon) we have exactly one of the following:

- $\lim_{n\to\infty} \mathbb{P}_{p(n)}(G(n, p(n)) \models A) = 1$
- $\lim_{n\to\infty} \mathbb{P}_{p(n)}(G(n, p(n)) \models A) = 0$

Moreover, p(n) is not a threshold function for A.

The Graph Language

First-Order Logic: Our Language

- variables: $x_1, x_2, \ldots$
- two binary relations: $=$ and $\sim$
- quantifiers: $\forall$ and $\exists$
- connectives: $\vee, \wedge, \rightarrow, \neg$

Note

We will assume the following two axioms:

- $\forall x \ \neg(x \sim x)$ ("there are no loops")
- $\forall x \forall y \ (x \sim y) \rightarrow (y \sim x)$ ("the graph is undirected")
- This language has no constants, function symbols and relation symbols.

Models

Definition

A model for over a language L is a couple (M, σ), where M is a set, and σ is an "interpretation function" that satisfies:

- $\forall$ constant $c \in L$, $\sigma(c) \in M$
- $\forall$ relation symbol with n entries, P, $\sigma(P) \subseteq M^n$ is a relation
- $\forall$ function symbol with n entries, f, $\sigma(f) : M^n \to M$.

Basically it is a set in which the strings of L have some actual meaning.

Remark

- Any simple graph is a model over L (the relation $\sim$ is just the adjacency relation).
- Any model, M, over L can be interpreted as a graph by thinking of the points in M as vertices, and saying v is adjacent to u iff $v \sim u$ in the model M.

Example

Example

Let $A =$ "$\exists x \exists y \exists z (x \sim y) \wedge (y \sim z) \wedge (z \sim x)$". In that case, $G \models A$ if and only if G (thought of as a graph) contains a triangle.

Proposition

$\lim_{n \to \infty} \mathbb{P}(G(n, \frac{1}{2}) \models A) = 1.$

Proof.

Partition the vertices of G into disjoint $3 - tuples$. Each tuple forms a triangle with probability $1/8$, hence the probability that G does not contain a triangle is no higher than the probability that none of the disjoint $3 - tuples$ form a triangle which is $\left(\frac{7}{8}\right)^{n/3} \to 0$. ☐

Remark

The previous proof works for any fixed p, not just $p = \frac{1}{2}$. Moreover one can copy the idea of the prove and show that if H is some specific graph, and A is the property ”the graph contains H as a subgraph” (which can be written as a sentence in L) then $\lim_{n\to\infty} \mathbb{P}(G(n,p) \models A) = 1$.

Furmulas Sentences

Definition

- $X_i = X_j$ and $X_i \sim X_j$ are called atomic formulas.
- If Q,P are formulas then so are: $\neg Q, P \wedge\ Q, P \vee Q, P \rightarrow Q, \exists x Q(x), \forall x Q(x)$.
- The formulas over L are all formulas that can be constructed in finite number of steps from the atomic formulas, which are the building blocks of the language.

Remark

We do not really need $\forall$ in our language as it can be represented by $\exists$ and $\neg$.

Furmulas Sentences

Definition

- All the variables in atomic formulas are free-variables.
- If Q,P are formulas then: $F.V(\neg Q) = F.V(Q)$ $F.V(P \rightarrow Q) = F.V(P \wedge\ Q) = F.V(P \vee Q) = F.V(P) \cup F.V(Q)$, $F.V(\exists x Q(x)) = F.V(\forall x Q(x)) = F.V(Q) \setminus \{x\}$.
- A sentence is a formula with no free variables.

Remark

A formula with free variables, whose meaning in any model depends on the values we choose to give the free variables, and accordingly its truth value may change for different values we give the free variables. However if M is a model and φ is a sentence then either $M \models \varphi$ or $M \not\models \varphi$.

Theories

Definition

- A Theory (over L) is a set of sentences (over L)
- $\mathfrak{M}$ is a model of a theory T (denoted $\mathfrak{M} \models T$) if for any sentence $\varphi \in T$, $\mathfrak{M} \models \varphi$
- A theory T is said to be consistent if it has a model.

Compactness Theorem

A Theory T is consistent iff any finite $T' \subset T$ is consistent.
(i.e. if T does not have a model then there is a finite $T' \subset T$ that does not have a model. This is similar to the "finite intersection property", thus the name of the theorem is justified.)

Gödel's Completeness Theorem

Let T be a theory. A sentence φ is provable by T (i.e. there is a finite proof for φ, that uses only the axioms in T, tautologies and some natural deduction roles: modus ponens and modus tollens) iff for any model of T, $\mathfrak{M} \models T$, we have $\mathfrak{M} \models \varphi$

Definition

A theory T is said to be complete if for any sentence φ either T proves φ ($T \vdash \varphi$) or T proves $\neg\varphi$ ($T \nvdash \varphi$).
By Gödel's Completeness Theorem this is equivalent to:
Either $\forall \mathfrak{M} \models T$ we have $\mathfrak{M} \models \varphi$ or $\forall \mathfrak{M} \models T$ we have $\mathfrak{M} \nvDash \varphi$.

Lowenheim-Skolem Theorem

If a theory T (over L) is consistent, then T has a model $\mathfrak{M}$, s.t. $|\mathfrak{M}| \leq |L| + \aleph_0$

Theorem

Let T be a consistent theory over L, s.t. $|L| \leq \aleph_0$, with no finite models. If any 2 countable models of T (which exist by previous theorem) agree on all formulas (i.e. are elementary equivalent), then T is complete

Proof.

Assume otherwise, then by the equivalent definition of complete theory, which is obtained by Gödel's Completeness Theorem, this means that there is a sentence A s.t. both $T \cup \{A\}, T \cup \{\neg A\}$ are consistent. By L-S we have m_1, m_2 countable or finite models for $T \cup \{A\}, T \cup \{\neg A\}$. But since m_1, m_2 are also models for T (they satisfy T and at least one additional sentence), they can not be finite. Thus m_1, m_2 are 2 countable models of T, which disagree on A.
A contradiction! □

Almost Sure Theories

Definition

An almost sure theory is the set of all sentences A holding w.h.p (with respect to some $p = p(n)$), meaning: $\lim_{n\to\infty} \mathbb{P}_{p(n)}(G(n, p(n)) \models A) = 1$.

Theorem

An almost sure theory is a closed under logical inference.

Proof.

Suppose B is deduced from an almost sure theory T; hence, it can be deduced from a finite subset of T, $A_1, \ldots, A_k$ (since any proof has to be finite).
$\mathbb{P}(G(n,p) \models (\neg A_1) \vee \ldots \vee (\neg A_k)) \leq \sum_{i=1}^{k} \mathbb{P}(G(n,p) \models \neg A_i) \to 0.$
If T satisfies all sentences in a proof, it will also satisfy the conclusion of the proof $\square$

Almost Sure Theories

Theorem

An almost sure theory T is consistent.

Proof.

Use the definition of T and the compactness theorem $\square$

The Zero-One Law

Definition

We say that $p = p(n)$ satisfies the Zero-One Law if for every first-order sentence A, the following holds: $\lim_{n\to\infty} \mathbb{P}[G(n, p(n)) \models A] \in \{0, 1\}$.

Theorem (Fagin)

Any sequence $p(n)$ s.t. for any fixed s $[p(n)(1 - p(n))]^s n \gg ln(n)$, satisfies the Zero-One Law. In particular ay fixed sequence p(n)=p satisfies the 0-1 Law.

Alice's Restaurant Property

Definition

For any non-negative integers r, s, let $A_{r,s}$ be the following statement: "For any distinct $x_1, \ldots, x_r$ and $y_1, \ldots, y_s$ there exists a vertex z such that $z \sim x_i$ for all i and $\neg z \sim y_i$ for all i."
Note: This is a first-order sentence. z is called a witness

Alice's Restaurant Property

Proposition

$\forall r, s \geq 0$, *$A_{r,s}$ holds almost surely.*

Proof.

For given r, s and $x_1, \dots, x_r, y_1, \dots, y_s$, let Noz be the event "there is no witness z satisfying …". It is easy to see that $P\text{Noz} = [1 - p^r \cdot (1-p)^s]^{n-r-s}$. The union bound gives the following:
$\mathbb{P}(\neg A_{r,s}) \leq \binom{n}{r}\binom{n-r}{s}\left(1 - [1 - p^r \cdot (1-p)^s]^{n-r-s}\right)^{n-r-s} \leq_1 n^{r+s} e^{-[p^r(1-p)^s(n-r-s)]} \rightarrow 0$. By our assumption on p(n).
1) is true since $\forall x \in \mathbb{R}, 1 + x \leq e^x$.

□

Alice's Restaurant Property

Definition

A graph is said to have the Alice's Restaurant Property if it satisfies $A_{r,s}$ for all $r, s \geq 0$.

Theorem

There is a unique graph G (up to isomorphism) for which $G \models ARP$*.*

Alice's Restaurant Property

Proof of existence.

The theory generated by $A_{r,s}$ is partial to the almost sure theory, so it is consistent. Hence, by L-S theorem it has a countable or finite model (in our case, countable since $A_{n,0}$ can be satisfied only by a graph with at least n+1 vertices).
Notice that this countable graph G is in fact a graph limit of G(n,p(n)) and is in fact independent of p(n) as long as it is in our range!
A direct construction: label the vertices 1,2,3,.... It is enough to say for each j which of 1,....,j-1 are neighbors of j in order to define the graph. Write $j = \sum_{i=1}^{j} \epsilon_i(j) 2^i$ (its binary representation, $\epsilon_i(j) \in \{0, 1\}$). Then $j \sim i$ iff $\epsilon_i(j) = 1$ ☐

Proof of uniqueness.

On the board! ☐

Proof of Fagin's Theorem

Proof.

Consider the theory *ARP*. We have shown that this theory has a unique countable model. Hence, by a previous theorem *ARP* is complete. But since $ARP \subseteq T =$ the Almost Sure Theory, we get that T is complete. Let B be a first-order sentence. Suppose $T \vdash B$. Then since T is closed to logic inference (we showed this), $B \in T =$ The Almost Sure Theory thus B holds w.h.p. Otherwise $T \vdash (\neg B)$; switching the roles of B and $\neg B$ yields the desired result. ☐