22 Algorithms and Combinatorics

The Strange Logic of Random Graphs

J. Spencer

Springer

Joel Spencer

The Strange Logic of Random Graphs

With 13 Figures

Springer

Joel Spencer
Courant Institute
New York University
251 Mercer Street
New York, NY 10012-1110
USA
e-mail: spencer@cs.nyu.edu

Library of Congress Cataloging-in-Publication Data applied for
Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Spencer, Joël:
The strange logic of random graphs / Joel Spencer. – Berlin; Heidelberg; New York; Barcelona; Hong Kong; London; Milan; Paris; Singapore; Tokyo: Springer, 2001
(Algorithms and combinatorics; 22)
ISBN 3-540-41654-4

Mathematics Subject Classification (2000): 05C80, 03B10

ISSN 0937-5511
ISBN 3-540-41654-4 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typeset in LaTeX by the author. Edited and reformatted by Johannes Küster, typoma, www.typoma.com, using a Springer LaTeX macro package.
Printed on acid-free paper SPIN 10774693 46/3142LK - 5 4 3 2 1 0

To MaryAnn

Contents

Part I

Beginnings

0. Two Starting Examples

The core of our work is the study of Zero-One Laws for sparse random graphs. We may think of this study as having two sources. The first is the Zero-One Law for random graphs with constant probability, as given in Section 0.1. The second is the notion of evolution of random graph as discussed in Section 1.1.1. In that evolution it is central that the edge probability p be taken not just as a constant but as a function $p = p(n)$ of the total number of vertices. In Section 0.2 we examine such an evolution in the much easier case of a random unary predicate. To allow an easy introduction we avoid a plethora of notation in this chapter, the technical preliminaries – including many key definitions – are left for Chapter 1 and beyond.

0.1 A Blend of Probability, Logic and Combinatorics

We will be looking at labelled graphs G on n vertices. For convenience we'll call the vertices $\{1, \ldots, n\}$. The number of such graphs is precisely $2^{\binom{n}{2}}$ as each of the $\binom{n}{2}$ pairs i, j can be either adjacent or not adjacent. Consider a graph property – for example, the property of containing a triangle. Call the property A. We set $\mu_n(A)$ equal the proportion of labelled graphs on n vertices that have the property A. A precise evaluation of $\mu_n(A)$ might be very difficult. We start slowly.

Claim 0.1.1 $\lim_{n\to\infty} \mu_n(A) = 1$

Rather than proportion, it will be easier to work [throughout this book] with probabilities. Imagine that every pair i, j of vertices flips a fair coin to decide whether or not to be adjacent. We call the outcome the random graph $G(n, \frac{1}{2})$, which is defined in Section 1.1. We can and shall interpret $\mu_n(A)$ as the probability that this random graph has property A.

With this interpretation we give a simple argument (one of many) for Claim 0.1.1. Split the vertices into $s = \lfloor n/3 \rfloor$ disjoint triples. A triple i, j, k forms a triangle with probability precisely $\frac{1}{8}$. These are independent events as they involve distinct coin flips. Thus the probability that none of the s triples form a triangle is $(7/8)^s$. This goes to zero as n, and therefore s, goes to infinity. But this is an upper estimate (in some sense a very poor one but it suffices for our purposes) of the probability that there is no triangle whatsoever. When a nonnegative sequence is bounded from above by a sequence going to zero it must itself go to zero. So the probability that there is no triangle goes to zero.

Definition 0.1 *When* $\lim_{n\to\infty} \mu_n(A) = 1$ *holds we say that property* A *occurs* almost surely, *or, equivalently, that almost all graphs have property* A. *When* $\lim_{n\to\infty} \mu_n(A) = 0$ *we say that property* A *holds* almost never, *or, equivalently, that almost no graphs have property* A.

We note that this notation is not standard. A number of authors use the term *asymptotically almost surely* for the above concept and reserve almost surely for events that have probability one.

Let's consider, without proofs, some other examples of properties A. Almost all graphs are connected. Almost no graphs are planar. Almost no graphs have an isolated vertex. Almost all graphs have an induced pentagon. Is there a strict dichotomy (what we'll later call a Zero-One Law) between almost all and almost no? Of course not. The average graph will have $\frac{1}{2}\binom{n}{2}$ edges. Let A be the event that the graph G has more than $\frac{1}{2}\binom{n}{2}$ edges. It is not difficult to show $\lim_{n\to\infty} \mu_n(A) = \frac{1}{2}$, that asymptotically half the graphs have more than $\frac{1}{2}\binom{n}{2}$ edges. Sometimes a "silly" example can be instructive. Let A be the event that n itself is even. Then $\mu_n(A)$ is one when n is even and zero when n is odd, we aren't even looking at the graph. Here $\mu_n(A)$ does not approach a limit as $n \to \infty$! Still, these properties that avoid the strict dichotomy are somewhat suspect, the earlier properties have much more of a naturalness to them.

We would like to say that natural properties hold either almost surely or almost never. But what properties shall we call natural? For most of this book we shall deal with *first order properties*, as defined in Section 1.2. This is a notion long studied by logicians. How well it captures "naturalness" is discussed in Section 8.1.3 with some less than positive comments but our reason for using it is quite pragmatic: we can prove something remarkable.

Theorem 0.1.2 (Fagin-GKLT). *Let* A *be any first order property. Then*

$$\lim_{n\to\infty} \mu_n(A) = 0 \text{ or } 1$$

That is, every first order sentence holds either almost surely or almost never.

GKLT refers to Glebskii, Kogan, Liagonkii and Talanov [8]. The proof of this theorem we give here, basically from Fagin [7], is a blend of combinatorics, probability and logic. For every pair of nonnegative integers r, s we define a particular property of special importance.

Definition 0.2 *The* r, s *extension statement, denoted* $A_{r,s}$, *is that for all distinct vertices* $x_1, \ldots, x_r$ *and* $y_1, \ldots, y_s$ *there exists a vertex* z *distinct from them all which is adjacent to all of the* $x_1, \ldots, x_r$ *and to none of the* $y_1, \ldots, y_s$.

We naturally include the cases $r = 0$ and $s = 0$ so that, for example, $A_{1,0}$ is that every vertex has a neighbor. When z is adjacent to all the x's and none of the y's we call z a *witness*, a term that will appear in later contexts as well. The probability part of the proof consists of showing that

Claim 0.1.3 *For all $r, s \geq 0$ the r, s extension statement $A_{r,s}$ holds almost surely.*

For a given $x_1, \ldots, x_r$ and $y_1, \ldots, y_s$ let $\text{NOZ}[x_1, \ldots, y_s]$ be the event that there is no witness z. (The notation NOZ is meant to suggest "no z.")

Claim 0.1.4 $\Pr[\text{NOZ}] = (1 - 2^{-r-s})^{n-r-s}$.

Proof: There are $n - r - s$ potential witnesses z's. Each has probability 2^{-r-s} of being a witness, as $r + s$ coin tosses must come up in a particular way. But the events "z is not a witness" are mutually independent over the z's as they involve disjoint sets of coin tosses. Thus the probability the no z is a witness is $(1 - 2^{-r-s})^{n-r-s}$.

While $\Pr[\text{NOZ}] \to 0$ that by itself only shows that for a particular $x_1, \ldots, x_r$ and $y_1, \ldots, y_s$ there is almost surely a witness z. The event $A_{r,s}$ is logically equivalent to saying NOZ fails for all choices of x's and y's. Turning things around, the event $\neg A_{r,s}$ is the disjunction of the events NOZ over all possible $x_1, \ldots, x_r$ and $y_1, \ldots, y_s$. There are a total of $\binom{n}{r}\binom{n-r}{s}$ choices for the x's and y's.

Now we need an absolutely elementary fact: The probability of the disjunction of events is *at most* the sum of the probabilities of the events. Equality occurs only when the events are disjoint, which will not be the case here. The actual calculation of the probability of a disjunction can be quite complicated (involving, e.g., the Inclusion-Exclusion laws) but it is surprising how often the above fact will suffice for our purposes.

In applying our fact all the events have the same probability so the sum is actually a product and

$$\Pr[\neg A_{r,s}] \leq \binom{n}{r}\binom{n-r}{s}(1 - 2^{-r-s})^{n-r-s} \tag{1}$$

Now, recalling r, s are fixed, we take the limit of the right hand side of 1 as $n \to \infty$. The term $\binom{n}{r}\binom{n-r}{s}$ is a polynomial in n. The term $(1 - 2^{-r-s})^{n-r-s}$ is an exponential in n, going to zero as $1 - 2^{-r-s} < 1$. Polynomial growth times exponential decay goes to zero. We've bounded $\Pr[\neg A_{r,s}]$ from above by a function going to zero and hence $\neg A_{r,s}$ holds almost never. But then $A_{r,s}$ hold almost surely, giving Claim 0.1.3.

Now our argument makes a surprising turn into the infinite.

Definition 0.3 *A graph G is said to have the* Alice's Restaurant *property if it satisfies the r, s extension statement $A_{r,s}$ for all nonnegative integers r, s. Equivalently: if for all pairs of disjoint finite sets X, Y of vertices there* *exists z not in their union which is adjacent to all $x \in X$ and no $y \in Y$. Equivalently: given any finite set X of size, say, s there are witnesses $z \notin X$ with all 2^s possible adjacency patterns to X.*

This colorful term was first used by Peter Winkler. It refers to a popular song by Arlo Guthrie whose refrain – you can get anything you want at Alice's Restaurant – captures the spirit of the property. No finite graph G can have the Alice's Restaurant property since one could take X to be the entire vertex set and $Y = \emptyset$ and then there would be no witness z. The surprise comes when we look at countable graphs.

Theorem 0.1.5. *There is a unique (up to isomorphism) countable graph G satisfying the Alice's Restaurant property.*

Proof of Uniqueness: Let G_1, G_2 be countable graphs satisfying the Alice's Restaurant property, label their vertices $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ respectively. We will find a bijection $\phi\colon G_1 \to G_2$ in an infinite number of stages, which shall alternate between LeftStep and RightStep, beginning with a LeftStep. At the beginning ϕ is nowhere defined. At each step we will define one more value of ϕ. (While the first (left) step can be considered part of the general procedure below we note it always consists of setting $\phi(a_1) = b_1$.) Say that after s steps we have defined $\phi(x_i) = y_i$ for $1 \leq i \leq s$. We shall require inductively that ϕ is an isomorphism between its domain and range, i.e., that x_i, x_j are adjacent if and only if y_i, y_j are adjacent.

We define a RightStep. Let y_{s+1} be the first vertex of G_2 (by which we mean that vertex with the smallest index when written b_j) which is not one of the $y_1, \ldots, y_s$. We define, and this is the critical point, x_{s+1} to be the first vertex of G_1 which is not one of the $x_1, \ldots x_s$ and so that defining $\phi(x_{s+1}) = y_{s+1}$ retains the inductive property – i.e., that x_{s+1} is adjacent to x_i (with $1 \leq i \leq s$) if and only if y_{s+1} is adjacent to y_i. We are looking for an x_{s+1} with a particular set of adjacencies to the $x_1, \ldots, x_s$. The existence of such an x_{s+1} follows from the Alice's Restaurant property of the graph G_1.

A LeftStep is similar, taking x_{s+1} to be the first vertex of G_1 which is not one of the $x_1, \ldots, x_s$ and then y_{s+1} to be the first vertex of G_2 which is not one of the $y_1, \ldots, y_s$ which is adjacent to y_i (with $1 \leq i \leq s$) if and only if x_{s+1} is adjacent to x_i. The Alice's Restaurant for the graph G_2 guarantees the existence of y_{s+1} and we set $\phi(x_{s+1}) = y_{s+1}$.

The final ϕ obtained by this procedure will be an isomorphism between its domain and range. But any vertex in G_1 has some label, say a_u, and so will be in the domain after at most u LeftSteps, since at each LeftStep the least vertex of G_1 not already taken is placed in the domain. Similarly, any vertex in G_2 has some label, say b_v, and so will be in the range after at most v RightSteps, since at each RightStep the least vertex of G_2 not already taken is placed in the range. Thus ϕ is a bijection from G_1 to G_2 which preserves adjacency and hence G_1, G_2 are isomorphic.

An Example: In the partial picture below we first set $\phi(a_1) = b_1$. The next step is a RightStep and b_2 is the first unused vertex of G_2. It is adjacent to b_1. The first unused vertex of G_1 adjacent to a_1 is a_4 so we set $\phi(a_4) = b_2$. The next step is a LeftStep and a_2 is the first unused vertex of G_1. It is adjacent to a_1 and not a_4 so we seek an unused vertex of G_2 adjacent to b_1 and not b_2, the first one is b_6 and we set $\phi(a_2) = b_6$. The next step is a RightStep and b_3 is the first unused vertex of G_2. It is adjacent to b_2 and not to b_1 nor b_6 so we seek an unused vertex of G_1 adjacent to a_4 and not to a_1 nor a_2. The Alice's Restaurant property of G_1 assures us that such a vertex exists, if the first one is a_{17} we set $\phi(a_{17}) = b_3$ and continue.

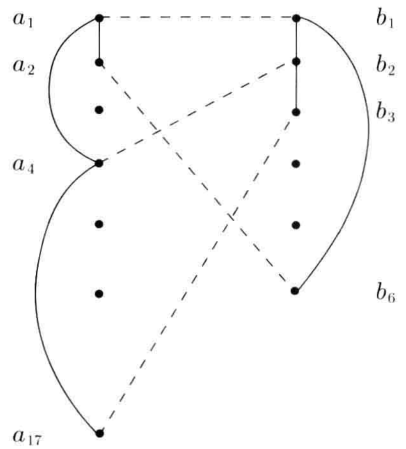

Fig. 0.1.

Existence (Proof 1): Let the vertices be $0, 1, 2, \ldots$. For $s \geq 1$ let the 2^s vertices $2^s \leq i < 2^{s+1}$ have all possible adjacency patterns with $0, \ldots, s-1$. Explicitly, when $2^s \leq i < 2^{s+1}$ write $i = 2^s + \sum_{j=0}^{s-1} \epsilon_j 2^j$. For $0 \leq j < s$ have i, j adjacent if and only if $\epsilon_j = 1$. (Not all adjacencies have been specified by this procedure, those that have not can be filled in arbitrarily.) Any finite set X has a maximal value s and so there will be a witness $i \in [2^s, 2^{s+1})$ with any desired adjacency pattern to X.

Existence (Proof 2): Start with a countable vertex set on which no adjacencies have been determined. Make a countable list (X_i, Y_i) of pairs of disjoint finite sets from the vertex set. At step i take a vertex z_i not previously used (not in $X_1, \ldots, X_i, Y_1, \ldots, Y_i$ nor $z_1, \ldots, z_{i-1}$) and make it adjacent to all of X_i and none of Y_i. At the end of the countable procedure some pairs have not had their adjacency determined, they can be set arbitrarily. But any finite pair (X, Y) appeared in the countable list as some position i and so has its witness $z = z_i$.

Existence (Proof 3): Since each $A_{r,s}$ holds almost surely the theory T generated by them is consistent and hence has a countable model, as discussed more generally in Sections 1.5 and 1.6.

The final portion of Theorem 0.1.2 uses Logic. Consider the theory T of graphs with the sentences $A_{r,s}$. (That is, add the $A_{r,s}$ as axioms.) This theory has no finite models (that is, graphs satisfying the axioms) and has a unique (up to isomorphism) countable model. From the Gödel Completeness Theorem, a basic but very deep result in logic, we deduce (as described in more detail in Section 1.5) that the theory T is complete. This means that for any sentence B either B or $\neg B$ is deducible in the theory - provable from the axioms $A_{r,s}$.

Suppose B is provable in T. Proof is finite and so there is a proof using only finitely many of the axioms, call them A^i for $1 \leq i \leq u$, each being of the form $A_{r,s}$. (This reduction to a finite number of axioms is critical and sometimes referred to as the Compactness Principle.) Any G that satisfies the conjunction $\wedge_i A^i$ must satisfy B. Complementing, any G satisfying $\neg B$ must satisfy the disjunction $\vee_i \neg A^i$. The probability of a disjunction is at most the sum of the probabilities and so for any n

$$\mu_n(\neg B) \leq \sum_{i=1}^{s} \mu_n(\neg A^i)$$

The limit of a *finite* sum of sequences is the sum of their limits so

$$\lim_{n\to\infty} \sum_{i=1}^{s} \mu_n(\neg A^i) = \sum_{i=1}^{s} \lim_{n\to\infty} \mu_n(\neg A^i) = \sum_{i=1}^{s} 0 = 0$$

Therefore $\neg B$ holds almost never. Therefore B holds almost surely.

The only other case is when $\neg B$ is provable in T. The roles of B and $\neg B$ are now reversed. We deduce B holds almost never. So either B holds almost surely or almost never, completing the proof of Theorem 0.1.2.

The Fagin-GKLT Theorem 0.1.2 deals with asymptotics but speaks only about finite graphs, infinite graphs never appear in the statement. Yet this proof involves "going to the infinite and coming back". It was that aspect that first convinced this author (among many) of the beauties of the subject. A rough analogy can be made to the use of the complex numbers to prove statements about the reals. Mathematics works in strange ways. We shall explore a number of techniques that lead to Zero-One Laws but the use of infinite graphs shall remain a strong motif throughout this work.

0.2 A Random Unary Predicate

We turn now away from graphs to a rather easier random model which illustrates many of the concepts we shall deal with. We call it the simple unary predicate with parameters n, p and denote it by $\mathrm{SU}(n, p)$. The model is over a universe Ω of size n, a positive integer. We imagine each $x \in \Omega$ flipping a coin to decide if $U(x)$ holds, and the coin comes up heads with probability p. Here we have p real, $0 \leq p \leq 1$. Formally we have a probability space on the possible U over Ω defined by the properties $\Pr[U(x)] = p$ for all $x \in \Omega$ and the events $U(x)$ being mutually independent. We consider sentences in the first order language. In this language we have only equality (we shall always assume we have equality) and the unary predicate U. The cognescenti should note that Ω has no further structure and in particular is not considered an ordered set as in Section 10.7.

This is a spartan language. One thing we can say is

$$\text{YES} := \exists_x U(x),$$

that U holds for some $x \in \Omega$. Simple probability gives

$$\Pr[\mathrm{SU}(n,p) \models \text{YES}] = 1 - (1-p)^n$$

As p moves from zero to one $\Pr[\text{YES}]$ moves monotonically from zero to one. We are interested in the asymptotics as $n \to \infty$. At first blush this seems trivial: for $p = 0$, $\mathrm{SU}(n,p)$ never models YES while for any constant $p > 0$,

$$\lim_{n\to\infty} \Pr[\mathrm{SU}(n,p) \models \text{YES}] = \lim_{n\to\infty} 1 - (1-p)^n = 1$$

In an asymptotic sense YES has already almost surely occurred by the time p reaches any positive constant.

This leads us to a critical notion. *We do not restrict ourselves to p constant but rather consider $p = p(n)$ as a function of n.* What is the parametrization $p = p(n)$ that best enables us to see the transformation of $\Pr[\mathrm{SU}(n,p(n)) \models \text{YES}]$ from zero to one. Some reflection leads to the parametrization $p(n) = c/n$. If c is a positive constant then

$$\lim_{n\to\infty} \Pr[\mathrm{SU}(n,p(n)) \models \text{YES}] = \lim_{n\to\infty} 1 - \left(1 - \frac{c}{n}\right)^n = 1 - e^{-c}$$

(Technically, as $p \leq 1$ always, this parametrization is not allowable for $n < c$ – but since our interest is only with limits as $n \to \infty$ this will not concern us.) If we think of c going from zero to infinity then the limit probability is going from zero to one. We shall not look at the actual limits here but only in whether the limits are zero or one.

Repeating the notation of Section 0.1 we say that a property A holds *almost always* if $\lim_{n\to\infty} \Pr[\mathrm{SU}(n,p(n)) \models A] = 1$. We say that A holds *almost never* if the above limit is zero or, equivalently, if $\neg A$ holds almost surely. Note, however, that these notions depend on the particular function $p(n)$. This notion is extremely general. Whenever we have for all sufficiently large positive integers n a probability space over models of size n then we can speak of a property A holding almost surely or almost never. For the particular property YES the exact results above have the following simple consequences: