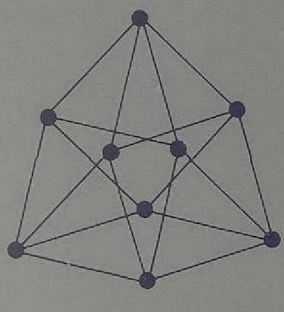
Cambridge studies in advanced mathematics 73

Random Graphs

Second Edition

BÉLA BOLLOBÁS



CAMBRIDGE STUDIES IN
ADVANCED MATHEMATICS 73

RANDOM GRAPHS

Already published

1 W.M.L. Holcombe *Algebraic automata theory*
2 K. Petersen *Ergodic theory*
3 P.T. Johnstone *Stone spaces*
4 W.H. Schikhof *Ultrametric calculus*
5 J.-P. Kahane *Some random series of functions, 2nd edition*
6 H. Cohn *Introduction to the construction of class fields*
7 J. Lambek & P.J. Scott *Introduction to higher-order categorical logic*
8 H. Matsumura *Commutative ring theory*
9 C.B. Thomas *Characteristic classes and the cohomology of finite groups*
10 M. Aschbacher *Finite group theory*
11 J.L. Alperin *Local representation theory*
12 P. Koosis *The logarithmic integral I*
13 A. Pietsch *Eigenvalues and s-numbers*
14 S.J. Patterson *An introduction to the theory of the Riemann zeta-function*
15 H.J. Baues *Algebraic homotopy*
16 V.S. Varadarajan *Introduction to harmonic analysis on semisimple Lie groups*
17 W. Dicks & M. Dunwoody *Groups acting on graphs*
18 L.J. Corwin & F.P. Greenleaf *Representations of nilpotent Lie groups and their applications*
19 R. Fritsch & R. Piccinini *Cellular structures in topology*
20 H. Klingen *Introductory lectures on Siegel modular forms*
21 P. Koosis *The logarithmic integral II*
22 M.J. Collins *Representations and characters of finite groups*
24 H. Kunita *Stochastic flows and stochastic differential equations*
25 P. Wojtaszczyk *Banach spaces for analysts*
26 J.E. Gilbert & M.A.M. Murray *Clifford algebras and Dirac operators in harmonic analysis*
27 A. Frohlich & M.J. Taylor *Algebraic number theory*
28 K. Goebel & W.A. Kirk *Topics in metric fixed point theory*
29 J.E. Humphreys *Reflection groups and Coxeter groups*
30 D.J. Benson *Representations and cohomology I*
31 D.J. Benson *Representations and cohomology II*
32 C. Allday & V. Puppe *Cohomological methods in transformation groups*
33 C. Soulé et al *Lectures on Arakelov geometry*
34 A. Ambrosetti & G. Prodi *A primer of nonlinear analysis*
35 J. Palis & F. Takens *Hyperbolicity, stability and chaos at homoclinic bifurcations*
37 Y. Meyer *Wavelets and operators I*
38 C. Weibel *An introduction to homological algebra*
39 W. Bruns & J. Herzog *Cohen-Macaulay rings*
40 V. Snaith *Explicit Brauer induction*
41 G. Laumon *Cohomology of Drinfield modular varieties I*
42 E.B. Davies *Spectral theory and differential operators*
43 J. Diestel, H. Jarchow & A. Tonge *Absolutely summing operators*
44 P. Mattila *Geometry of sets and measures in euclidean spaces*
45 R. Pinsky *Positive harmonic functions and diffusion*
46 G. Tenenbaum *Introduction to analytic and probabilistic number theory*
47 C. Peskine *An algebraic introduction to complex projective geometry I*
48 Y. Meyer & R. Coifman *Wavelets and operators II*
49 R. Stanley *Enumerative combinatories*
50 I. Porteous *Clifford algebras and the classical groups*
51 M. Audin *Spinning tops*
52 V. Jurdjevic *Geometric control theory*
53 H. Voelklein *Groups as Galois groups*
54 J. Le Potier *Lectures on vector bundles*
55 D. Bump *Automorphic forms*
56 G. Laumon *Cohomology of Drinfeld modular varieties II*
57 D.M. Clarke & B.A. Davey *Natural dualities for the working algebraist*
59 P. Taylor *Practical foundations of mathematics*
60 M. Brodmann & R. Sharp *Local cohomology*
61 J.D. Dixon, M.P.F. Du Sautoy, A. Mann & D. Segal *Analytic pro-p groups, 2nd edition*
62 R. Stanley *Enumerative combinatorics II*
64 J. Jost & X. Li-Jost *Calculus of variations*
68 Ken-iti Sato *Lévy processes and infinitely divisible distributions*
71 R. Blei *Analysis in integer and fractional dimensions*

Random Graphs

Second Edition

BÉLA BOLLOBÁS
University of Memphis
and
Trinity College, Cambridge

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011–4211, USA
10 Stamford Road, Oakleigh, VIC 3166, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 1985 by Academic Press
Second edition published 2001 by Cambridge University Press

Printed in the United Kingdom at the University Press, Cambridge

Typeface Times 11/14pt *System* LaTeX2e [UPH]

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data
Bollobás, Béla
Random graphs / Béla Bollobás. – 2nd ed.
p. cm. – (Cambridge mathematical library)
Includes bibliographical references and index.
ISBN 0 521 79722 5 (pbk.)
1. Random graphs. I. Title II. Series

QA166.17.B66 2001
511.'5–dc21 00-068952

IBSN 0 521 80920 7 hardback
ISBN 0 521 79722 5 paperback

To Gabriella and Mark

'I learn so as to be contented.'

After the inscription on 'Tsukubai', the stone wash-basin in Ryoanji temple.

Contents

Preface

The theory of random graphs was founded by Erdős and Rényi (1959, 1960, 1961a, b) after Erdős (1947, 1959, 1961) had discovered that probabilistic methods were often useful in tackling extremal problems in graph theory. Erdős proved, amongst other things, that for all natural numbers $g \geq 3$ and $k \geq 3$ there exist graphs with girth g and chromatic number k. Erdős did not construct such graphs explicitly but showed that most graphs in a certain class could be altered slightly to give the required examples.

This phenomenon was not entirely new in mathematics, although it was certainly surprising that probabilistic ideas proved to be so important in the study of such a simple finite structure as a graph. In analysis, Paley and Zygmund (1930a, b, 1932) had investigated random series of functions. One of their results was that if the real numbers c_n satisfy $\sum_{n=0}^{\infty} c_n^2 = \infty$ then $\sum_{n=0}^{\infty} \pm c_n \cos nx$ fails to be a Fourier–Lebesgue series for almost all choices of the signs. To exhibit a sequence of signs with this property is surprisingly difficult: indeed, no algorithm is known which constructs an appropriate sequence of signs from any sequence c_n with $\sum_{n=0}^{\infty} c_n^2 = \infty$. Following the initial work of Paley and Zygmund, random functions were investigated in great detail by Steinhaus (1930), Paley, Wiener and Zygmund (1932), Kac (1949), Hunt (1951), Ryll-Nardzewski (1953), Salem and Zygmund (1954), Dvoretzky and Erdős (1959) and many others. An excellent account of these investigations can be found in Kahane (1963, 1968). Probabilistic methods were also used by Littlewood and Offord (1938) to study the zeros of random polynomials and analytic functions. Some decades later, a simple but crucial combinatorial lemma from their work greatly influenced the study of random finite sets in vector spaces.

The first combinatorial structures to be studied probabilistically were tournaments, chiefly because random tournaments are intrinsically related to statistics. The study began with Kendall and Babington-Smith (1940) and a concise account of many of the results is given by Moon (1968*b*). Szele (1943) was, perhaps, the first to apply probabilistic ideas to extremal problems in combinatorics. He observed that some tournament of order n must have at least $n!/2^{n-1}$ Hamilton paths, because the expected number of Hamilton paths is $n!/2^{n-1}$. Once again, it is not easy to construct a tournament of order n with this many Hamilton paths. A little later, Erdős (1947) used a similar argument, based on the expected number of k-cliques in a graph of order n, to show that the Ramsey number $R(k)$ is greater than $2^{k/2}$.

Existence results based on probabilistic ideas can now be found in many branches of mathematics, especially in analysis, the geometry of Banach spaces, number theory, graph theory, combinatorics and computer science. Probabilistic methods have become an important part of the arsenal of a great many mathematicians. Nevertheless, this is only a beginning: in the next decade or two probabilistic methods are likely to become even more prominent. It is also likely that in the not too distant future it will be possible to carry out statistical analyses of more complicated systems. Mathematicians who are not interested in graphs for their own sake should view the theory of random graphs as a modest beginning from which we can learn a variety of techniques and can find out what kind of results we should try to prove about more complicated random structures.

As often happens in mathematics, the study of statistical aspects of graphs was begun independently and almost simultaneously by several authors, namely Ford and Uhlenbeck (1956), Gilbert (1957), Austin, Fagen, Penney and Riordan (1959) and Erdős and Rényi (1959). Occasionally all these authors are credited with the foundation of the theory of random graphs. However, this is to misconceive the nature of the subject. Only Erdős and Rényi introduced the methods which underlie the probabilistic treatment of random graphs. The other authors were all concerned with enumeration problems and their techniques were essentially deterministic.

There are two natural ways of estimating the proportion of graphs having a certain property. One may obtain exact formulae, using Pólya's enumeration theorem, generating functions, differential operators and the whole theory of combinatorial enumeration, and then either consider the task completed or else proceed to investigate the asymptotic behaviour of the exact but complicated formulae, which is often a daunting task.

This approach, whose spirit is entirely deterministic, was used in the first three papers mentioned above and has been carried further by numerous authors. Graphical enumeration is discussed in detail in the well known monograph of Harary and Palmer (1973) and the recent encyclopaedic treatise by Goulden and Jackson (1983). The connection between graphical enumeration and statistical mechanics is emphasized by Temperley (1981). The theory of enumeration is a beautiful, rich and rapidly developing area of combinatorics, but it has very little to do with the theory of random graphs.

The other approach was introduced by Erdős and Rényi and is expounded in this volume. It has only the slightest connection with enumeration. One is not interested in exact formulae but rather in approximating a variety of exact values by appropriate probability distributions and using probabilistic ideas, whenever possible. As shown by Erdős and Rényi, this probabilistic approach is often more powerful than the deterministic one.

It is often helpful to imagine a random graph as a living organism which evolves with time. It is born as a set of n isolated vertices and develops by successively acquiring edges at random. Our main aim is to determine at what stage of the evolution a particular property of the graph is likely to arise. To make this more precise, we shall consider the properties of a 'typical' graph in a probability space consisting of graphs of a particular type. The simplest such probability space consists of all graphs with a given set of n labelled vertices and M edges, and each such graph is assigned the same probability. Usually we shall write G_M for a random element of this probability space. Then, if H is any graph with the given vertex set and M edges, then $P(G_M = H) = 1/\binom{N}{M}$ where $N = \binom{n}{2}$.

In most cases we shall have a sequence of probability spaces. For each natural number n there will be a probability space consisting of graphs with exactly n vertices. We shall be interested in the properties of this space as $n \to \infty$. In this situation we shall say that a *typical element of our space has a property Q* when the probability that a random graph on n vertices has Q tends to 1 as $n \to \infty$. We also say that *almost every (a.e.)* graph has property Q. Thus almost every G_M has property Q if the proportion of graphs with this property tends to 1 as $n \to \infty$. Once we are given such probability spaces of graphs, numerous natural questions arise. Is a typical graph connected? Is it k-connected? Is the chromatic number at least k? Does almost every graph contain a triangle? Does it have diameter at most d? Is almost every graph Hamiltonian?

The greatest discovery of Erdős and Rényi was that many important properties of graphs appear quite suddenly. If we pick a function $M = M(n)$ then, in many cases, either almost every graph G_M has property Q or else almost every graph fails to have property Q. In this vague sense, we have a 0–1 law. The transition from a property being very unlikely to it being very likely is usually very swift. To make this more precise, consider a *monotone* (increasing) property Q, i.e. one for which a graph has Q whenever one of its subgraphs has Q. For many such properties there is a *threshold function* $M_0(n)$. If $M(n)$ grows somewhat slower than $M_0(n)$, then almost every G_M fails to have Q. If $M(n)$ grows somewhat faster than $M_0(n)$, then almost every G_M has the property Q. For example, $M_0(n) = \frac{1}{2}n \log n$ is a threshold function for connectedness in the following sense: if $\omega(n) \to \infty$, no matter how slowly, then almost every G is disconnected for $M(n) = \frac{1}{2}n(\log n - \omega(n))$ and almost every G is connected for $M(n) = \frac{1}{2}n(\log n + \omega(n))$.

As the proportion M/N of edges increases, where, as always, $N = \binom{n}{2}$ is the total number of possible edges, the shape of a typical graph G_M passes through several clearly identifiable stages, in which many of the important parameters of a typical graph are practically determined. When M is neither too small nor too large, then the most important property is that, for every fixed k, and k vertices in a typical graph have about the same number of neighbours. Thus a typical random graph is rather similar to an ideal regular graph whose automorphism group is transitive on small sets of vertices. Of course, there is no such non-trivial regular graph, and in many applications random graphs are used precisely because they approximate an ideal regular graph.

This book is the first systematic and extensive account of a substantial body of results from the theory of random graphs. Considerably shorter treatments of random graphs can be found in various parts of Erdős and Spencer (1974), in Chapter 8 of Marshall (1971), in Chapter 7 of Bollobás (1979*a*), and in the review papers by Grimmett (1980), Bollobás (1981*f*) and Karoński (1982). Despite over 750 references, several topics are not covered in any detail and we can make no claim to completeness. Perhaps the greatest omission is the extensive theory of random trees, about which the reader could get some idea by consulting the beautiful book by Moon (1970*a*) and the papers by Moon and Meir listed in the references. I might justify this particular omission because the tools used in its study are often those of enumeration rather than probability theory. However, here and in general, the choice of topics is mainly a reflection of my own interests.

The audience I had in mind when writing this book consisted mainly of research students and professional mathematicians. The volume should also be of interest to computer scientists. Random graphs are of ever increasing importance in this field and several of the sections have been written expressly for computer scientists.

The monograph was planned to be considerably shorter and was to be completed by early 1981. However, I soon realized that I had little control over the length which was dictated by the subject matter I intended to explore. Temptations to ease my load by adopting short-cuts have been rife but, for the reader's sake, I have tried to resist them. During its preparation I have given several courses on the material, notably for Part III for the University of Cambridge in 1980/81 and 1983/84. The first seven chapters were complete by the summer of 1982 and were circulated quite widely. I gave a series of lectures on these at the Waterloo Silver Jubilee Conference. These lectures were published only recently (1984*d*). I have written the book wherever I happened to be: the greatest part at Louisiana State University, Baton Rouge; a few chapters in Cambridge, Waterloo and São Paulo; and several sections in Tokyo and Budapest. I hope never again to travel with 200 lb of paper!

My main consideration in selecting and presenting the material was to write a book which I would like to read myself. In spite of this, the book is essentially self-contained, although familiarity with the basic concepts of graph theory and probability theory would be helpful. There is little doubt that many readers will use this monograph as a compendium of results. This is a pity, partly because a book suitable for that purpose could have been produced with much less effort than has gone into this volume, and also because proofs are often more important than results: not infrequently the reader will derive more benefit from knowing the methods used than from familiarity with the theorems. The list of contents describes fairly the material presented in the book.

The graph theoretic notation and terminology used in the book are standard. For undefined concepts and symbols the reader may consult Bollobás (1978*a*, 1979*a*).

The exercises at the end of each chapter vary greatly in importance and difficulty. Most are designed to clarify and complete certain points but a few are important results. The end of a proof, or its absence, is indicated by the symbol $\square$; the *floor* of x (i.e. the greatest integer less than, or equal to, x) is denoted by $\lfloor x \rfloor$; and the *ceiling* of x by $\lceil x \rceil$. With very few exceptions, the various parameters and random variables depend on the number n of vertices of graphs under consideration and the inequalities are only claimed to hold when n is sufficiently large. This is often stated but it is also implicit on many other occasions. The symbols $c_1, c_2, \ldots$ which appear without any explanation, are always independent of n. They may be absolute constants or may depend on other quantities which are independent of n. To assist the reader, it will often be stated which of these is the case.

It is a great pleasure to acknowledge the debt I owe to many people for their help. Several of my friends kindly read large sections of the manuscript. Andrew Thomason from Exeter, Istvan Simon from São Paulo, Masao Furuyama from Kyoto and Boris Pittel from Columbus were especially generous with their help. They corrected many errors and frequently improved the presentation. In addition, I benefited from the assistance of Andrew Barbour, Keith Carne, Geoff Eagleson, Alan Frieze and Jonathan Partington. Many research students, including Keith Ball, Graham Brightwell and Colin Wright, helped me find some of the mistakes; for the many which undoubtedly remain, I apologize. I am convinced that without the very generous help of Andrew Harris in using the computer the book would still be far from finished.

It was Paul Erdős and Alfréd Rényi who, just over 20 years ago, introduced me to the subject of random graphs. My active interest in the field was aroused by Paul Erdős some years later, whose love for it I found infectious; I am most grateful to him for firing my enthusiasm for the subject whose beauty has given me so much pleasure ever since.

Finally, I am especially grateful to Gabriella, my wife, for her constant support and encouragement. Her enthusiasm and patience survived even when mine failed.

Baton Rouge B.B.
December, 1984

Notation

$\beta_0(G)$	independence number	*page* 273, 282
$C(n, m)$	number of connected graphs	118
$\mathrm{cl}(G_n)$	clique number	282
$\mathrm{core}(G)$	core of G	150
$\mathrm{core}_k(G)$	k-core of G	150
$\delta(G)$	minimal degree	60
$\Delta(G)$	maximal degree	60
$(d_i)_1^n$	degree sequence	60
$\mathrm{diam}(G)$	diameter	251
E_M	expectation	34
E_p	expectation	35
E_r	rth factorial moment	3
$\mathrm{exc}(G)$	excess of G	148
$F = \mathbb{F}_q$	finite field	348
$G_M = G_{n,M}$	random graph	34
$G_p = G_{n,p}$	random graph	34
$G_r\text{-reg} = G_{n,r-\mathrm{reg}}$	random graph	50
$\widetilde{G} = (G_t)_0^N$	random graph process	42
$\widetilde{\mathscr{G}}$	space of graph processes	42
$\mathscr{G}(H; p)$	probability space of graphs	35
$\mathscr{G}(n; k\text{-out}) = \mathscr{G}_{k-\mathrm{out}}$	probability space of graphs	40
$\mathscr{G}(n, M) = \mathscr{G}_M$	probability space of graphs	34
$\mathscr{G}(n, p) = \mathscr{G}_p$	probability space of graphs	34
$\mathscr{G}(n, r\text{-reg}) = \mathscr{G}_{r-\mathrm{reg}}$	probability space of graphs	50
$\mathscr{G}\{n, P(\mathrm{edge})\}$	probability space of graphs	34
$\ker(G)$	kernel of G	150
$L_M = L_{nM}$	number of labelled graphs	229
$N(\mu, \sigma)$	normal distribution	9

P_k	property	44
P_λ	Poisson distribution	8
P_M	probability in $\mathscr{G}(n, M)$	34
P_p	probability in $\mathscr{G}(n, P)$	35
P_q	Paley graph	357
Q^n	n-dimensional cube	383
Q_p^n	random subgraph of Q^n	383
$R(s)$, $R(s, t)$	Ramsey numbers	320
$S_{n,p}$	binomial r.v.	5
$\tau = \tau_Q = \tau_Q(\widetilde{G}) = \tau(\widetilde{G}; Q)$	hitting time	42
$t(c)$	function concerning the number of vertices on tree components	102
$U_M = U_{n,M}$	number of unlabelled graphs	229
$u(c)$	function concerning the number of tree components	109
$\chi(G)$	chromatic number	296
$X_n \xrightarrow{d} X$	convergence in distribution	2
$\omega(n)$	function tending to ∞	43

1

Probability Theoretic Preliminaries

The aim of this chapter is to present the definitions, formulae and results of probability theory we shall need in the main body of the book. Although we assume that the reader has had only a rather limited experience with probability theory and, if somewhat vaguely, we do define almost everything, this chapter is not intended to be a systematic introduction to probability theory. The main purpose is to identify the facts we shall rely on, so only the most important—and perhaps not too easily accessible—results will be proved. Since the book is primarily for mathematicians interested in graph theory, combinatorics and computing, some of the results will not be presented in full generality. It is inevitable that for the reader who is familiar with probability theory this introduction contains too many basic definitions and familiar facts, while the reader who has not studied probability before will find the chapter rather difficult.

There are many excellent introductions to probability theory: Feller (1966), Breiman (1968), K. L. Chung (1974) and H. Bauer (1981), to name only four. The interested reader is urged to consult one of these texts for a thorough introduction to the subject.

1.1 Notation and Basic Facts

A *probability space* is a triple (Ω, Σ, P), where Ω is a set, Σ is a σ-field of subsets of Ω, P is a non-negative measure on Σ and $P(\Omega) = 1$. In the simplest case Ω is a finite set and Σ is $\mathscr{P}(\Omega)$, the set of all subsets of Ω. Then P is determined by the function $\Omega \to [0,1], w \to P(\{w\})$, namely

$$P(A) = \sum_{w \in A} P(\{w\}), A \subset \Omega.$$

A real valued *random variable* (r.v.) X is a measurable real-valued function on a probability space, $X : \Omega \to \mathbb{R}$.

Given a real valued r.v. X, its *distribution function* is $F(x) = P(X < x), -\infty < x < \infty$. Thus $F(x)$ is monotone increasing, continuous from the left, $\lim_{x\to-\infty} F(x) = 0$ and $\lim_{x\to\infty} F(x) = 1$. If there is a function $f(t)$ such that $F(x) = \int_{-\infty}^{x} f(t)\, dt$, then $f(t)$ is the *density function* of X. We say that a sequence of r.vs (Y_n) *tends to* X in *distribution* if $\lim_{n\to\infty} P(Y_n < x) = P(X < x) = F(x)$, whenever x is a point of continuity of $F(x)$. The notation for convergence in distribution is $X_n \xrightarrow{d} X$. Of course, convergence in distribution depends only on the distributions of the r.vs in question.

If h is any real-valued function on $\mathbb{R}$, the *expectation* of $h(X)$ is

$$E(h(X)) = \int_\Omega h(X) \mathrm{d}P = \int_{-\infty}^{\infty} h(x) \mathrm{d}F(x).$$

In particular, the *mean* of X, usually denoted by μ, is $E(X)$ and the *nth moment* of X is $E(X^n)$. Of course, these need not exist but, as they do exist for the r.vs we are going to consider, we shall assume that they exist. The *variance* of X is $\sigma^2(X) = E\{(X-\mu)^2\} = E(X^2) - \mu^2$ and the standard deviation is the non-negative square root of this.

If X is a non-negative r.v. with mean μ and $t > 0$, then

$$\mu \geq P(X \geq t\mu)t\mu.$$

Rewriting this slightly we get *Markov's inequality*:

$$P(X \geq t\mu) \leq 1/t. \tag{1.1}$$

Now let X be a real-valued r.v. with mean μ and variance σ^2. If $d > 0$, then clearly

$$E\{(X-\mu)^2\} \geq P(|X-\mu| \geq d)d^2$$

so we have *Chebyshev's inequality*:

$$P(|X-\mu| \geq d) \leq \sigma^2/d^2. \tag{1.2}$$

As a special case of this inequality we see that if $\mu \neq 0$, then

$$P(X=0) \leq P(|X-\mu| \geq \mu) \leq \sigma^2/\mu^2. \tag{1.2'}$$

In fact, one can do a little better, for by the Cauchy inequality with $\Omega_0 = \{w : X(w) \neq 0\}$ we have

$$E(X)^2 = \left(\int_{\Omega_0} X \mathrm{d}P\right)^2 \leq \left(\int_{\Omega_0} X^2 \mathrm{d}P\right)\left(\int_{\Omega_0} 1 \mathrm{d}P\right) = E(X^2)\{1 - P(X=0)\}.$$

Hence

$$P(X=0) \le 1 - E(X)^2/E(X^2) = \sigma^2/(\mu^2+\sigma^2). \tag{1.3}$$

Most of the r.vs we encounter are non-negative integer valued, so unless it is otherwise indicated (for example, by the existence of the density function), we assume that the r.v. takes only non-negative integer values. The distribution of such a r.v., X, is given by the sequence

$$p_k = P(X=k), k = 0, 1, \ldots.$$

Clearly $p_k \ge 0$ and $\Sigma_{k=0}^{\infty} p_k = 1$. Then the mean of X is $\Sigma_{k=1}^{\infty} k p_k$ and the nth moment is $E(X^n) = \Sigma_{k=1}^{\infty} k^n p_k$. If $X, X_1, X_2, \ldots$ are non-negative integer valued r.vs then $X_n \xrightarrow{d} X$ if

$$\lim_{n\to\infty} P(X_n = k) = P(X=k) = p_k$$

for every k.

Write $\mathscr{L}(X)$ for the distribution (*law*) of a r.v. X. Given integer-valued r.vs X and Y, the *total variation distance* of $\mathscr{L}(X)$ and $\mathscr{L}(Y)$ is

$$d(\mathscr{L}(X), \mathscr{L}(Y)) = \sup\{|P(X \in A) - P(Y \in A)| : A \subset \mathbb{Z}\}.$$

With a slight abuse of notation occasionally we write $d(X, Y)$ or $d(X, \mathscr{L}(Y))$ instead of $d(\mathscr{L}(X), \mathscr{L}(Y))$.

Clearly $X_n \xrightarrow{d} X$ iff $d(X_n, X) \to 0$. Of course, any information about the speed of convergence of $d(X_n, X)$ to 0 is more valuable than the fact that X_n tends to X in distribution.

Given a probability space (Ω, Σ, P) and a set $C \in \Sigma, P(C) > 0$, the *probability of a set* $A \in \Sigma$ *conditional on* C is defined as

$$P(A|C) = P(A \cap C)/P(C).$$

Then $P_C = P(\cdot|C)$ is a probability measure on (Ω, Σ). A r.v. X is said to be taken *condition on* C if it is considered as a function on (Ω, Σ, P_C); the expectation of this new r.v., denoted by $E(X|C)$, is said to be the expectation of X conditional on C.

Following Feller (1966) we use the notation $(x)_r = x(x-1)\ldots(x-r+1)$. Thus $(n)_n = (n)_{n-1} = n!$ and $\binom{n}{k} = (n)_k/(k)_k$. We define the *rth factorial moment* of a r.v. X as $E_r(X) = E\{(X)_r\}$. Thus if

$$P(X=k) = p_k,$$

then

$$E_r(X) = \sum_{k=r}^{\infty} p_k (k)_r.$$

Note that if X denotes the number of objects in a certain class then $E_r(X)$ is the expected number of *ordered r-tuples* of elements of that class.

The r.vs $X_1, X_2, \ldots$ are said to be *independent* if for each n

$$P(X_i = k_i, i = 1, \ldots, n) = \prod_{i=1}^{n} P(X_i = k_i)$$

for every choice of $k_1, k_2, \ldots, k_n$.

Note that $E(X+Y) = E(X) + E(Y)$ always holds and if $X_1, X_2, \ldots, X_n$ are independent, $E(X_i) = \mu_i$ and $E(X_i - \mu_i)^2 = \sigma_i^2$ then $E(\sum_i X_i) = \sum_i \mu_i$ and

$$\sigma^2\left(\sum_i X_i\right) = E\left[\left\{\sum_i (X_i - \mu_i)\right\}^2\right] = \sum_i \sigma_i^2.$$

In our calculations we shall often need the following rather sharp form of *Stirling's formula* proved by Robbins (1955):

$$n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n} e^{\alpha_n}, \tag{1.4}$$

where $1/(12n+1) < \alpha_n < 1/12n$.

Throughout the book we use Landau's notation $O\{f(n)\}$ for a term which, when divided by $f(n)$, remains bounded as $n \to \infty$. Similarly $h(n) = o\{g(n)\}$ means that $h(n)/g(n) \to 0$ as $n \to \infty$. Also, $h(n) \sim g(n)$ express the fact that $h(n)/g(n) \to 1$ as $n \to \infty$. Thus $h(n) \sim g(n)$ is equivalent to $h(n) - g(n) = o\{g(n)\}$. Note that a weak form of Stirling's formula (4) is $n! \sim (n/e)^n \sqrt{2\pi n}$. If the symbols o, O or $\sim$ are used without a variable, then we mean that the relation holds as $n \to \infty$.

An immediate consequence of (1.4) is that if $1 \leq m \leq n/2$, then

$$\begin{aligned} e^{-1/(6m)} \frac{1}{\sqrt{2\pi}} \left(\frac{n}{m}\right)^m \left(\frac{n}{n-m}\right)^{n-m} \left(\frac{n}{m(n-m)}\right)^{1/2} &\leq \binom{n}{m} \\ &\leq \frac{1}{\sqrt{2\pi}} \left(\frac{n}{m}\right)^m \left(\frac{n}{n-m}\right)^{n-m} \left(\frac{n}{m(n-m)}\right)^{1/2}. \end{aligned} \tag{1.5}$$

On putting $p = m/n$ and $q = 1-p$ we find that if $m \to \infty$ and $n-m \to \infty$, then

$$\binom{n}{m} \sim (2\pi)^{-1/2} (p^p q^q)^{-n} (pqn)^{-1/2}.$$

By writing the binomial coefficients as quotients of products of factorials we obtain some other useful inequalities. If $b \leq b + x < a$ and

$0 \le y < b \le a$, then

$$\left(\frac{a-b-x}{a-x}\right)^x \le \binom{a-x}{b}\binom{a}{b}^{-1} \le \left(\frac{a-b}{a}\right)^x \le e^{-(b/a)x} \tag{1.6}$$

and

$$\left(\frac{b-y}{a-y}\right)^y \le \binom{a-y}{b-y}\binom{a}{b}^{-1} \le \left(\frac{b}{a}\right)^y \le e^{-(1-b/a)y}. \tag{1.7}$$

For future reference we note some approximations of $\log(1+t)$. If $t > -1$, then

$$\log(1+t) \le \min\{t, t - \tfrac{1}{2}t^2 + \tfrac{1}{3}t^3\}, \tag{1.8}$$

if $t > 0$, then

$$\log(1+t) > t - \tfrac{1}{2}t^2, \tag{1.9}$$

if $0 < t < 0.45$, then

$$\log(1+t) > t - \tfrac{1}{2}t^2 + \tfrac{1}{4}t^3, \tag{1.9$'$}$$

if $0 < t < 0.69$, then

$$\log(1-t) > -t - t^2, \tag{1.10}$$

and if $0 < t < 0.431$, then

$$\log(1-t) > -t - \tfrac{1}{2}t^2 - \tfrac{1}{2}t^3. \tag{1.10$'$}$$

1.2 Some Basic Distributions

Throughout the book we shall keep to the convention that $0 < p < 1$ and $q = 1 - p$. We say that X is a *Bernoulli r.v. with mean p* if X takes only two values, 0 and 1, and $P(X = 1) = p$, $P(X = 0) = q$. Thus X can be thought of as the outcome of tossing a biased coin, with probability p of getting a head. Let $X^{(1)}, X^{(2)}, \ldots$ be a sequence of independent Bernoulli r.vs with each $X^{(i)}$ having mean p. Then the r.v. $S_{n,p} = \sum_{i=1}^n X^{(i)}$ satisfies

$$P(S_{n,p} = k) = b(k; n, p) = \binom{n}{k} p^k q^{n-k},$$

and we say that $S_{n,p}$ has a *binomial distribution with parameters n and p*. By definition $b(k; n, p)$ is the probability that we get k heads when tossing a coin n times, provided the probability of getting a head is p. Since $E(X^{(i)}) = p$ and $\sigma^2(X^{(i)}) = E\{(X^{(i)} - p)^2\} = pq$, the binomial distribution with parameters n and p has mean $E(S_{n,p}) = pn$ and variance $\sigma^2(S_{n,p}) = pqn$.

It is easily seen that $b(k; n, p)$ is largest when k approximates to pn, the expectation of $S_{n,p}$. Indeed, note that

$$\frac{b(k;n,p)}{b(k-1;n,p)} = 1 + \frac{(n+1)p-k}{kq}. \tag{1.11}$$

Hence, if m is the unique integer satisfying $p(n+1)-1 < m \le p(n+1)$, then the terms $b(k; n, p)$ strictly increase up to $k = m-1$ and strictly decrease from $k = m$; furthermore, $b(m-1; n, p) < b(m; n, p)$ unless $m = p(n+1)$, when equality holds. Consequently from Stirling's formula (4) it follows that if p is fixed then, as $n \to \infty$,

$$\max_k b(k;n,p) \sim \frac{1}{\sqrt{2\pi pqn}} = \frac{1}{\sigma\sqrt{2\pi}}.$$

Relations (1.11) and (1.5) imply the following simple but useful bound on the probability in the tail of the binomial distribution.

Theorem 1.1 *Let* $u > 1$ *and* $1 \le m = \lceil upn \rceil \le n-1$. *Then*

$$\begin{aligned} P(S_{n,p} \ge upn) &= P(S_{n,p} \ge m) < \frac{u}{u-1} b(m;n,p) \\ &\le \frac{1}{\sqrt{2\pi}} \frac{u}{u-1} \left(\frac{n}{m(n-m)} \right)^{1/2} u^{-upn} \left(\frac{1-p}{1-up} \right)^{(1-up)n}. \end{aligned}$$

Proof If $m \le k-1$ then, by (1.11),

$$\frac{b(k;n,p)}{b(k-1;n,p)} \le \frac{(n-m)p}{(m+1)q} < \frac{1}{u},$$

so

$$\sum_{k=m}^{n} b(k;n,p) < \frac{u}{u-1} b(m;n,p).$$

To see the second inequality, for $1 < x < 1/p$ set

$$f(x) = x^{-px} \left(\frac{1-p}{1-px} \right)^{1-px}.$$

Then

$$\frac{\mathrm{d}}{\mathrm{d}x} \log f(x) = -p \log x - p(1-px) \log \frac{1-p}{1-px} < 0,$$

so putting $v = m/(pn)$, by (1.5) we find that

$$\begin{aligned} b(m;n,p) &\le \frac{1}{\sqrt{2\pi}}\left(\frac{n}{m(n-m)}\right)^{1/2}\left(\frac{n}{m}\right)^m\left(\frac{n}{n-m}\right)^{n-m} p^m(1-p)^{n-m} \\ &= \frac{1}{\sqrt{2\pi}}\left(\frac{n}{m(n-m)}\right)^{1/2} f(v)^n \\ &\le \frac{1}{\sqrt{2\pi}}\left(\frac{n}{m(n-m)}\right)^{1/2} f(u)^n. \end{aligned}$$ □

The binomial distribution describes the number of successes among n trials, with the probability of a success being p. Now consider the number of failures encountered prior to the first success, and denote this by Y. Then clearly

$$P(Y = k) = q^k p, k = 0, 1, \ldots$$

The distribution defined above is said to be *geometric, with mean* q/p. It is easily checked that the mean is indeed q/p, the variance is q/p^2 and the rth factorial moment is $r!(q/p)^r$ (Ex. 3).

The number of failures prior to the rth success, say Z_r, is said to have a *negative binomial distribution.* The terminology is justified by the fact that

$$P(Z_r = k) = \binom{r+k-1}{k} p^r q^k, \quad k = 0, 1, \ldots$$

Since Z_r is the sum of r independent geometric r.vs, $E(Z_r) = rq/p$ and $\sigma^2(Z_r) = rq/p^2$.

A continuous version of the geometric distribution is the *exponential distribution* (or negative exponential distribution). A non-negative real valued r.v. L is said to have an exponential distribution with parameter $\lambda > 0$ is

$$P(L < t) = 1 - e^{-\lambda t} \text{ for } t > 0.$$

The density function of this distribution is $\lambda\, \mathrm{e}^{-\lambda t}$, and easy calculations show that $E(L) = 1/\lambda$ and $\sigma^2(L) = 1/\lambda^2$ (Ex. 4).

If Y is a geometric r.v. with mean $(1-p)/p$, where $p > 0$ is small, then the distribution of pY is close to the exponential distribution with mean 1 (Ex. 5).

The *hypergeometric distribution* with parameters N, R and $n (0 < n < N, 0 < R < N)$ is defined by

$$\begin{aligned} q_k &= P(X = k) = \binom{R}{k}\binom{N-R}{n-k} \Big/ \binom{N}{n} \\ &= \binom{n}{k}\binom{N-n}{R-k} \Big/ \binom{N}{R}, \quad k = 0, \ldots, s, \end{aligned}$$

where $s = \min\{n, R\}$. Thus q_k is the probability that if we select n balls at random from a pool of R red balls and $N-R$ blue balls then exactly k of the balls will be red. If n is fixed and, as $N \to \infty$, the ratio R/N converges to a constant $p, 0 < p < 1$, then the hypergeometric distribution tends to the binomial distribution $b(k; n, p)$. This is an immediate consequence of the inequality

$$\binom{n}{k}\left(p-\frac{k}{N}\right)^k\left(q-\frac{n-k}{N}\right)^{n-k} < q_k < \binom{n}{k}p^k q^{n-k}\left(1-\frac{k}{N}\right)^{-(n-k)}, \tag{1.12}$$

where $p = R/N$ and $q = 1-p$. As we are interested mostly in the upper bound for q_k, we show the second inequality. Consider the second expression for q_k and note that

$$\begin{aligned}\binom{N-n}{R-k}\Big/\binom{N}{R} &= \frac{(R)_k(N-n)_{R-k}}{(N)_R} = \frac{(R)_k(N-R)_{n-k}}{(N)_n} \\ &\le \left(\frac{R}{N}\right)^k\left(\frac{N-R}{N-k}\right)^{n-k} = p^k q^{n-k}\left(1-\frac{k}{N}\right)^{-n+k},\end{aligned}$$

since

$$\frac{N-R}{N-k} = \frac{N-R}{N}\frac{N}{N-k} = q\left(1-\frac{k}{N}\right)^{-1}.$$

A r.v. Y is said to have *Poisson distribution with mean* $\lambda > 0$ if

$$P(Y = k) = p(k; \lambda) = \mathrm{e}^{-\lambda}\lambda^k/k!, k = 0, 1, \ldots.$$

This distribution, which we shall denote by P_λ or $P(\lambda)$, is also closely related to the binomial distribution. Indeed, if $\lambda = pn$ and $0 < p < 1$, then

$$b(k; n, p) = \frac{(n)_k p^k}{k!}\left(1-\frac{\lambda}{n}\right)^{n-k} \le \frac{\lambda^k}{k!}\mathrm{e}^{\lambda(n-k)/n} = p(k;\lambda)\mathrm{e}^{pk}. \tag{1.13}$$

Also, if $\lambda = pn, 0 < p < \frac{1}{2}$ and $k \le n/2$, then, by (1.10),

$$\begin{aligned}b(k; n, p) &= \frac{\lambda^k}{k!}\left(1-\frac{\lambda}{n}\right)^{n-k}\Pi_{i=1}^{k-1}\left(1-\frac{i}{n}\right) \\ &\ge \frac{\lambda^k}{k!}\exp\left\{-\lambda-\lambda^2/n-\sum_{i=1}^{k-1}\left(\frac{i}{n}+\left(\frac{i}{n}\right)^2\right)\right\} \\ &\ge p(k;\lambda)\mathrm{e}^{-(\lambda^2+k^2)/n}.\end{aligned} \tag{1.14}$$

As a trivial consequence of (1.13) and (1.14) we find that if p depends on n in such a way that $pn \to \lambda$ as $n \to \infty$, where λ is a positive constant, then the binomial distribution with parameters n and p tends to the Poisson distribution with mean λ. In symbols: $S_{n,p} \xrightarrow{d} P_\lambda$.

The factorial moments of $S_{n,p}$ and P_λ are calculated without the slightest difficulty:

$$E_r(S_{n,p}) = p^r(n)_r \text{ and } E_r(P_\lambda) = \lambda^r.$$

1.3 Normal Approximation

In probabilistic graph theory we often need good estimates for the probability in the tail of the binomial distribution. The best known example of such an estimate is the DeMoivre–Laplace limit theorem [see Feller (1966, pp. 174–195) or Rényi (1970a, pp. 204–210)]. We shall give it here together with some bounds valid for all values in a given range.

A random variable is said to be *normally distributed with mean μ and variance σ^2* if it has density function

$$\frac{1}{\sigma\sqrt{2\pi}} e^{-(t-\mu)^2/2\sigma^2}.$$

This distribution is usually denoted by $N(\mu,\sigma)$. We shall reserve $\phi(t)$ and $\Phi(x)$ for the density function and distribution function of N (0, 1), respectively:

$$\phi(t) = (t)\frac{1}{\sqrt{2\pi}} e^{-t^2/2} \text{ and } \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt.$$

If $x > 0$ and $l \geq 0$, then (see Ex. 7)

$$1 + \sum_{m=1}^{2l+1} (-1)^m \frac{1 \cdot 3 \cdot \ldots \cdot (2m-1)}{x^{2m}} < \{1 - \Phi(x)\} \Big/ \left\{\frac{1}{x}\phi(x)\right\}$$
$$< 1 + \sum_{m=1}^{2l} (-1)^m \frac{1 \cdot 3 \cdot \ldots \cdot (2m-1)}{x^{2m}}. \quad (1.15)$$

In particular, as $x \to \infty$ we have

$$1 - \Phi(x) \sim \frac{1}{x}\phi(x) = \frac{1}{\sqrt{2\pi}} \frac{1}{x} e^{-x^2/2}. \quad (1.15')$$

Our first aim is to give upper bounds for the terms $b(k; n, p)$ of the binomial distribution. The restrictions in the theorem below are for the sake of convenience.

Theorem 1.2 *Suppose $pn \geq 1$ and $1 \leq hqn/3$. Then if $k \geq pn + h$, we have*

$$b(k; n, p) < \frac{1}{\sqrt{2\pi pqn}} \exp\left\{-\frac{h^2}{2pqn} + \frac{h}{qn} + \frac{h^3}{p^2n^2}\right\}.$$

Proof

We may and shall assume that $k = pn + h$. From inequality (1.5) we find

$$b(l; n, p) < \left(\frac{pn}{l}\right)^l \left(\frac{qn}{n-l}\right)^{n-l} [n/\{2\pi l(n-l)\}]^{1/2}$$

for every $l, 1 \leq 1 \leq n-1$. Hence

$$\begin{aligned}(2\pi pqn)^{1/2} b(k; n, p) &< \left(\frac{pn}{k}\right)^{k+1/2} \left(\frac{qn}{n-k}\right)^{n-k+1/2} \\ &= \left(\frac{pn}{pn+h}\right)^{pn+h+1/2} \times \left(\frac{qn}{qn-h}\right)^{qn-h+1/2} \\ &= \left(1 + \frac{h}{pn}\right)^{-pn-h-1/2} \left(1 - \frac{h}{qn}\right)^{-qn+h-1/2}.\end{aligned}$$

From inequalities (1.9) and (1.10′) we obtain that

$$\begin{aligned}(2\pi pqn)^{1/2} b(k; n, p) < \exp\Big\{&-(pn + h + \tfrac{1}{2})\left(\frac{h}{pn} - \frac{h^2}{2p^2n^2}\right) \\ &+ (qn - h + \tfrac{1}{2})\left(\frac{h}{qn} + \frac{h^2}{2q^2n^2} + \frac{h^3}{2q^3n^3}\right)\Big\}.\end{aligned}$$

The required inequality follows by expanding and simplifying the expression on the right and taking into account the conditions $pn \geq 1$ and $1 \leq h \leq qn/3$. □

Theorem 1.2 gives us the following upper bounds on the probability in the tail of the binomial distribution.

Theorem 1.3 *With the assumptions in Theorem 1.2 we have*

$$P(S_{n,p} \geq pn + h) < \left(\frac{pqn}{2\pi}\right)^{1/2} \frac{1}{h} \exp\left\{-\frac{h^2}{2pqn} + \frac{h}{pqn} + \frac{h^3}{p^2n^2}\right\}.$$

Proof By relation (1.11), if $m \geq pn + h$ then

$$\frac{b(m+1; n, p)}{b(m; n, p)} \leq 1 - \frac{h+q}{q(pn+h+1)} = \lambda < 1.$$

Hence

$$P(S_{n,p} \geq pn+h) = \sum_{m \geq pn+h} b(m;n,p) \leq \frac{1}{1-\lambda} b(\lceil pn+h \rceil; n,p).$$

It is easily checked that $(1-\lambda)^{-1} < (pqn/h)\{1+(h/pn)\} < (pqn/h)\mathrm{e}^{h/pn}$, so the result follows from Theorem 1.2.

It is often convenient to use the following weak but concise form of this result. □

Corollary 1.4 *(i) If* $1 \leq h < \min\{pqn/10, (pn)^{2/3}/2\}$, *then with* $h = x(pqn)^{1/2}$ *we have*

$$P(|S_{n,p} - pn| \geq h) < \frac{(pqn)^{1/2}}{h} \mathrm{e}^{-h^2/2pqn} = \frac{1}{x} \mathrm{e}^{-x^2/2}.$$

(ii) Suppose $0 < p < \frac{1}{2}$ *and* $(pn)^{-1/2} < \varepsilon < \frac{1}{6}$. *Then*

$$P(|S_{n,p} - pn| \geq \varepsilon pn) < \mathrm{e}^{-\varepsilon^2 pn/3q + \varepsilon/q}.$$

Proof (*i*) To deduce this from Theorem 1.2 we have to note simply that

$$\frac{h}{pqn} + \frac{h^3}{p^2n^2} < \frac{1}{2} \log \frac{\pi}{2} \approx 0.22579.$$

(*ii*) Theorem 1.2 gives that for $h = \varepsilon pn$ we have

$$\begin{aligned} P(S_{n,p} \geq pn+h) &< \left(\frac{pqn}{2\pi\varepsilon^2 p^2 n^2} \right)^{1/2} \mathrm{e}^{-\varepsilon^2 pn/3q} \exp\left(\frac{\varepsilon pn}{pqn} + \frac{\varepsilon^3 p^3 n^3}{p^2 n^2} - \frac{\varepsilon^2 pn}{6q} \right) \\ &< \frac{1}{2} \mathrm{e}^{-\varepsilon^2 pn/3q} \exp\left\{ \frac{\varepsilon}{q}(1 + \varepsilon^2 pqn - \varepsilon pn/6) \right\} \\ &< \frac{1}{2} \mathrm{e}^{-\varepsilon^2 pn/3q} \exp\left[\frac{\varepsilon}{q} \left\{ 1 - \frac{\varepsilon pn}{6}(1-6\varepsilon) \right\} \right] < \frac{1}{2} \mathrm{e}^{-\varepsilon^2 pn/3q + \varepsilon/q}. \end{aligned}$$

Analogous calculations yield

$$P(S_{n,p} \leq pn-h) < \tfrac{1}{2} \mathrm{e}^{-\varepsilon^2 q^3 n/3p^3 + \varepsilon/q} \leq \tfrac{1}{2} \mathrm{e}^{-\varepsilon^2 pn/3q + \varepsilon/q},$$

so the result follows. □

Another upper bound for the probability in the tail is due to Chernoff (1952). See also Okamoto (1958). For $0 < p < 1$ and $q = 1-p$, write $H_p(x)$ for the weighted entropy function: $H_p(x) = x \log(p/x) + (1-x) \log\{q/(1-x)\}, 0 < x < 1$. Note that $H_p(x) = H_q(1-x)$. Then we have

$$P(S_{n,p} \geq k) \leq \exp\{nH_p(k/n)\} \quad \text{for } k \geq pn$$

and, equivalently,

$$P(S_{n,p} \leq k) \leq \exp\{nH_p(k/n)\} \quad \text{for } k \leq pn.$$

To see these inequalities, simply note that for $u > 0$ and $k > pn$, by Markov's inequality (1.1) we have

$$P(S_{n,p} \geq k) \leq \mathrm{e}^{-uk}E(\mathrm{e}^{uS_{n,p}}) = \mathrm{e}^{-uk}(q + p\mathrm{e}^u)^n.$$

The right-hand side attains its minimum at $\mathrm{e}^u = qk/p(n-k)$ and so

$$P(S_{n,p} \geq k) \leq \left(\frac{p(n-k)}{qk}\right)^k \left(\frac{qn}{n-k}\right)^n = \left(\frac{pn}{k}\right)^k \left(\frac{qn}{n-k}\right)^{n-k} = \exp\{nH_p(k/n)\},$$

as claimed. For a different approach to proving Chernoff's inequalities, see Exercise 16.

In fact, the same inequalities hold for the sum X of n independent Bernoulli random variables $X_1, \dots, X_n$, with $P(X_i = 1) = E(X_i) = p_i$ and $\sum_1^n p_i = pn$. Indeed, by Jensen's inequality, for $pn < k$ and $u > O$ we have

$$P(X \geq k) \leq \mathrm{e}^{-uk}E(\mathrm{e}^{uX}) = \mathrm{e}^{-uk}\prod_{i=1}^n (q_i + p_i\mathrm{e}^u) \leq \mathrm{e}^{-uk}(q + p\mathrm{e}^u)^n.$$

As before, this implies that

$$P(X \geq k) \leq \exp\{nH_p(k/n)\}.$$

Janson (2001) pointed out that from this it is easy to deduce that if $X_1, \dots, X_n$ are independent Bernoulli random variables, $X = \sum_{i=1}^n X_i$ and $E(X) = \lambda$ then for $t \geq 0$ we have

$$P(X \geq \lambda + t) \leq \exp\left(-\frac{t^2}{2(\lambda + t/3)}\right)$$

and

$$P(X \leq \lambda - t) \leq \exp\left(-\frac{t^2}{2\lambda}\right).$$

As our next result shows, the bound in Theorem 1.2 is essentially best possible, provided $h = o\{(pqn)^{2/3}\}$.

Theorem 1.5 *Suppose $pn \geq 1$ and $k = pn + h < n$, where $h > 0$. Put*

$$\beta = \frac{1}{12k} + \frac{1}{12(n-k)}.$$

Then

$$b(k; n, p) > \frac{1}{\sqrt{2\pi pqn}} \exp\left(-\frac{h^2}{2pqn} - \frac{h^3}{2q^2n^2} - \frac{h^4}{3p^3n^3} - \frac{h}{2pn} - \beta\right).$$

Proof Stirling's formula (1.4) gives

$$b(k;n,p) > \left(\frac{pn}{k}\right)^k \left(\frac{qn}{n-k}\right)^{n-k} [n/\{2\pi k(n-k)\}]^{1/2} \mathrm{e}^{-\beta}.$$

Hence

$$\begin{aligned}(2\pi pqn)^{1/2} b(k;n,p) &> \mathrm{e}^{-\beta} \left(\frac{pn}{k}\right)^{k+1/2} \left(\frac{qn}{n-k}\right)^{n-k+1/2} \\ &= \mathrm{e}^{-\beta} \left(1+\frac{h}{pn}\right)^{-k-1/2} \left(1-\frac{h}{qn}\right)^{k-n-1/2}\end{aligned}$$

From inequality (1.8) it follows that

$$\begin{aligned}(2\pi pqn)^{1/2} b(k;n,p) > \exp\Bigg\{ &-\beta - (pn+h+\tfrac{1}{2}) \left(\frac{h}{pn} - \frac{h^2}{2p^2n^2} + \frac{h^3}{3p^3n^3}\right) \\ &+ (qn-h+\tfrac{1}{2}) \left(\frac{h}{qn} + \frac{h^2}{2q^2n^2} + \frac{h^3}{3q^3n^3}\right)\Bigg\}.\end{aligned}$$

The required inequality follows by expanding the expression on the right and noting that $h < qn$ and $pn \geq 1$. □

The estimates in Theorems 1.2 and 1.5 can be put together to give an approximation of the binomial distribution by the normal distribution. From the formulae so far it is clear that the most convenient measure of $k - pn$ is in multiples of the standard deviation $\sigma = (pqn)^{1/2}$.

Theorem 1.6 [DeMoivre–Laplace] *Suppose* $0 < p < 1$ *depends on* n *in such a way that* $pqn = p(1-p)n \to \infty as n \to \infty$.

(i) Suppose $h_1 < h_2, h_2 - h_1 \to \infty$ *as* $n \to \infty$ *and* $|h_1| + |h_2| = o\{(pqn)^{2/3}\}$. *Put* $h_i = x_i(pqn)^{1/2}, i = 1, 2$. *Then*

$$P(pn + h_1 \leq S_{n,p} \leq pn + h_2) \sim \Phi(x_2) - \Phi(x_1).$$

(ii) If $0 < h = x(pqn)^{1/2} = o\{(pqn)^{2/3}\}$, *then*

$$P(S_{n,p} \leq pn + h) \sim 1 - \Phi(x).$$

In particular, if $x \to \infty$, *then*

$$P(S_{n,p} \geq pn + h) \sim \frac{1}{x\sqrt{2\pi}} \mathrm{e}^{-x^2/2}.$$

Proof Let us assume for the moment that $1 \leq h_1 < h_2$. Then with

$\sigma = (pqn)^{1/2}$ from Theorem 1.2 we have

$$P(pn+h_1 \leq S_{n,p} \leq pn+h_2) \leq \frac{1}{\sigma\sqrt{2\pi}}\left(\sum_{h_1 \leq h \leq h_2} e^{-h^2/2\sigma^2}\right)\{1+o(1)\}$$
$$= \{1+o(1)\}\sum_{h_1 \leq h \leq h_2} \phi(h/\sigma)/\sigma \leq \{1+o(1)\}[\Phi(h_2/\sigma)-\Phi\{(h_1-1)/\sigma\}]$$
$$= \{1+o(1)\}\{\Phi(x_2)-\Phi(x_1)\},$$

where in the sums we assume that h runs over the values making $pn+h$ an integer. An analogous lower bound is obtained by Theorem 1.5, so (i) is proved. Now to lift the restriction $1 \leq h_1$, note simply that the omission of two terms from $\sum_{h_1 \leq h \leq h_2} b(pn+h; n, p)$ leaves a sum asymptotic to the original.

The second part can be proved analogously. It can also be deduced from the first part by putting $h_1 = h$ and $h_2 = h_1 + (pqn)^{5/8}$, say. The last assertion is a consequence of (1.15′). □

A weak version of Theorem 1.6(ii) is the assertion that if $pqn \to \infty$, then $(S_{n,p} - pn)/\sqrt{pqn} \xrightarrow{d} N(0,1)$. This is a special case of the Central Limit Theorem (see Theorem 1.23, below).

Occasionally we are interested in larger deviations than that covered by Theorem 1.6, and then the following easy bounds are rather useful. We leave the proof as an exercise.

Theorem 1.7 *(i) Suppose* $0 < p \leq \frac{1}{2}, \varepsilon\, pqn \geq 12$ *and* $0 < \varepsilon \leq 1/12$. *Then*

$$P(|S_{n,p} - pn| \geq \varepsilon\, pn) \leq (\varepsilon^2 pn)^{-1/2} e^{-\varepsilon^2 pn/3},$$

(ii) If $uq > 2$ *and* $pn \geq 1$, *then*

$$P(S_{n,p} \geq upn) < (e/u)^{upn},$$

and if $v \geq e$ *and* $v^2 pn \geq \log v$, *then*

$$P\left(S_{n,p} \geq \frac{ev}{\log v} pn\right) < e^{-vpn}.$$

The probability in the tail of the binomial distribution has attracted much attention; the best bounds to date (which are essentially the best possible) are due to Littlewood (1969), whose paper is highly recommended to those who think that the binomial distribution is too simple to deserve study.

1.4 Inequalities

One of the oldest tools in combinatorics is the inclusion-exclusion principle. Many extensions of this principle are useful in several branches of mathematics, especially in combinatorics, number theory and probability theory. Some of these extensions are used to estimate the number of primes less than a given numbers by going through the natural numbers and sieving out the multiples of numbers already found to be primes. In this section we establish several sieve formulae and deduce some probability theoretic consequences of them. For the rich theory of the general inclusion-exclusion principle, called the theory of Möbius inversion, the reader is referred to Rota (1964), Aigner (1980) and Goulden and Jackson (1983).

Suppose for every fixed r we are able to estimate the factorial moments $E_r(X_n)$ of a sequence of non-negative integer valued r.vs (X_n). Then, using certain sieve formulae, we may be able to conclude that the X_n tend in distribution to some known r.v. The aim of this section is to present the sieve formulae needed for this purpose. We start with the following beautiful and simple result of Rényi (1958). Related results are due to Galambos (1966) and Galambos and Rényi (1968); see also Comtet (1974, pp. 189–196).

Theorem 1.8 *Let $f_1, f_2, \ldots, f_k$ be Boolean polynomials in n variables A_1, $A_2, \ldots, A_n$ and let $b_1, b_2, \ldots, b_k$ be real constants. Suppose*

$$\sum_{i=1}^{k} b_i P\{f_i(B_1, B_2, \ldots, B_n)\} \geq 0 \tag{1.16}$$

whenever $B_1, B_2, \ldots, B_n$ are events in a probability space such that $P(B_i) =$ 0 or 1. Then (1.16) holds for every choice of events $B_1, B_2, \ldots, B_n$ in every probability space.

Proof A Boolean polynomial can be expressed as a union of complete products, that is polynomials of the form

$$g_J(A_1, \ldots, A_n) = \left(\bigcap_{i \in J} A_i \right) \cap \left(\bigcap_{i \notin J} \bar{A}_i \right), J \subset \{1, \ldots, n\}.$$

Here $\bar{A}_i$ denotes the complement of A_i. Hence (1.16) can be rewritten as

$$\sum_{J} c_J P\{g_J(B_1, \ldots, B_n)\} \geq 0, \tag{1.16$'$}$$

where the summation is over all 2^n subsets $J \subset \{1,\ldots,n\}$ and c_J depends only on J and the b_i.

Given a set $J_0 \subset \{1,\ldots,n\}$, choose $B_1,\ldots,B_n$ such that $P(B_i) = 1$ if $i \in J_0$ and $P(B_i) = 0$ if $i \notin J_0$. Then $P\{g_J(B_1,\ldots,B_n)\} = 0$ unless $J = J_0$ and $P\{g_{J_0}(B_1,\ldots,B_n)\} = 1$. Thus with this choice of the B_i the left-hand side of (16′) is c_{J_0}. Consequently $c_J \geq 0$ for every set J, so (16′) does hold for every choice of the events $B_1,\ldots,B_n$. □

An equivalent formulation of Theorem 1.8 is that every extreme point of the convex set

$$\{(P\{g_J(A_1,\ldots,A_n)\})_J : (A_i)_1^n \text{ are events}\} \subset \mathbb{R}^{2n}$$

has only 0 and 1 coordinates, with precisely one 1.

Corollary 1.9 *Suppose we have equality in (1.16) whenever $P(B_i) = 0$ or 1. Then equality holds for every choice of events $B_1,\ldots,B_n$.*

Let $A_1, A_2,\ldots,A_n$ be arbitrary events in a probability space (Ω, P). For $J \subset N = \{1,\ldots,n\}$ put

$$A_J = \bigcap_{j\in J} A_j \text{ and } A_\varnothing = \Omega.$$

Furthermore, set

$$p_J = P(A_J)$$

and

$$S_r = \sum_{|J|=r} p_J, \ r = 0,1,\ldots,n.$$

The usual *inclusion-exclusion formula* is an immediate consequence of Corollary 1.9:

$$P\left(\bigcup_{i=1}^n A_i\right) = \sum_{r=1}^n (-1)^{r+1} S_r. \tag{1.17}$$

Equivalently,

$$P\left(\bigcup_{i=1}^n A_i\right) + \sum_{|J|\geq 1} (-1)^{|J|} P(A_J) = 0. \tag{1.17′}$$

To see (1.17) note that if $P(A_1) = \ldots = P(A_l) = 1$ and $P(A_{l+1}) = \ldots = P(A_n) = 0$, where $l \geq 1$, then $S_r = \binom{l}{r}$ and

$$P\left(\bigcup_{i=1}^{n} A_i\right) - \sum_{r=1}^{n}(-1)^{r+1}S_r = 1 - \sum_{r=1}^{n}(-1)^{r+1}\binom{l}{r} = \sum_{r=0}^{n}(-1)^r\binom{l}{r} = 0.$$

Given sets $J \subset L \subset N = \{1,\ldots,n\}$, let us apply (1.17′) to the sets $A_i \cap A_J, i \in M = L - J$:

$$P\left\{\bigcup_{i\in M}(A_i \cap A_J)\right\} = \sum_{\substack{I\subset M\\ I\neq\emptyset}}(-1)^{|I|+1}P(A_I \cap A_J) = \sum_{\substack{I\subset M\\ I\neq\emptyset}}(-1)^{|I|+1}p_{I\cup J}.$$

Since the probability above is non-negative and at most p_J, we have

$$0 \leq \sum_{\substack{J\subset K\subset L\\ K\neq J}}(-1)^{|K-J|+1}p_K \leq p_J. \tag{1.18}$$

In fact, as shown in Rényi (1970*a*), the inequalities (1.18) together with $p_\emptyset = 1$ characterize the functions p_I. Thus if $p_I \in [0,1]$ for every set $I \subset N, p_\emptyset = 1$ and (1.18) holds for all $J \subset L \subset N$, then one can find a probability space (Ω, P) and events $A_1, A_2, \ldots, A_n$ such that $P(\bigcap_{i\in I} A_i) = p_I$ for every $I \subset N$.

A considerable strengthening of the inclusion-exclusion formula is due to Ch. Jordan (1926, 1927, 1934) [see also Fréchet (1940)]. This formula incorporates results of Poincaré and of Bonferroni (1936). In order to state it in a concise form, we shall say that a sum

$$s = \sum_{k=1}^{n}(-1)^{k+1}x_k$$

satisfies the *alternating inequalities* if

$$(-1)^l\left\{s + \sum_{k=1}^{l}(-1)^k x_k\right\} \geq 0$$

for every l, $l = 0, 1, \ldots, n$. (Note that in this case we have $x_k \geq 0$.)

Theorem 1.10 *Let $A_1, \ldots, A_n$ be events in a probability space, let $S_0, S_1, \ldots, S_n$ be as above, and denote by p_k the probability that exactly k of the A_i occur. Then*

$$p_k = \sum_{r=k}^{n}(-1)^{r+k}\binom{r}{k}S_r \tag{1.19}$$

and the sum satisfies the alternating inequalities.

Proof By Theorem 1.8 it suffices to prove the assertions in the case when for some $l, 0 \leq l \leq n, l$ of the sets A_i have probability 1 and the others have probability 0. Then $S_r = \binom{l}{r}$ and $p_k = \delta_{kl}$. If $l < k$ then all terms in (1.19) are 0 and if $l = k$ then (1.19) is of the form $1 = 1 - 0 + 0 - 0 + \ldots$.

Assume that $l > k$. Then $p_k = 0$ and

$$\sum_{r=k}^{k+m}(-1)^{k+r}\binom{r}{k}\binom{l}{r} = \sum_{r=k}^{k+m}(-1)^{k+r}\frac{(r)_k}{k!}\frac{(l)_r}{r!}$$
$$= \sum_{r=k}^{k+m}(-1)^{r+k}\frac{(l)_k}{k!}\frac{(l-k)_{r-k}}{(r-k)!} = \binom{l}{k}\sum_{r=k}^{k+m}(-1)^{r+k}\binom{l-k}{r-k}.$$

If $k + m \geq l$ then the sum is 0 and if $0 \leq m \leq l - k$ then it is

$$\binom{l}{k}+\binom{l}{k}\sum_{i=1}^{m}(-1)^i\left\{\binom{l-k-1}{i-1}+\binom{l-k-1}{i}\right\} = \binom{l}{k}(-1)^m\binom{l-k-1}{m}.$$

Hence the sum is positive if m is even and negative if m is odd. Thus (1.18) holds and the sum satisfies the alternating inequalities. □

Corollary 1.11 . *Let X be a r.v. with values in $\{0, 1, \ldots, n\}$ and let $E_r(X)$ be the rth factorial moment of X. Then*

$$P(X = k) = \left(\sum_{r=k}^{n}(-1)^{k+r}\frac{E_r(X)}{(r-k)!}\right)\Big/ k!$$

and the sum satisfies the alternating inequalities.

Proof Let A_i be the event $\{X \geq i\}, i = 1, \ldots, n$, and define the numbers $S_0, S_1, \ldots, S_n$ as above. Then clearly

$$S_r = E_r(X)/r! \tag{1.20}$$

and $\{X = k\}$ is the event that exactly k of the A_i occur. Hence the result follows from Theorem 1.10. □

In the proof above the value of X is the number of A_i's that occur. In fact (1.20) holds whenever X is defined from an arbitrary set of A_i's in this way.

Corollary 1.12 *Let X be a non-negative integer valued r.v. whose rth factorial moment $E_r(X) = E\{(X)_r\}$ is finite for $r = 1, \ldots, R$. Suppose s,*

$t \le R, k+s$ is odd and $k+t$ is even. Then

$$\left\{\sum_{r=k}^{s}(-1)^{k+r}E_r(X)/(r-k)!\right\}\Big/k! \le P(X=k)$$
$$\le \left\{\sum_{r=k}^{t}(-1)^{k+r}E_r(X)/(r-k)!\right\}\Big/k!.$$

Proof Set $X^{(n)} = \min\{X, n\}$. Then $\lim_{n\to\infty} E_r(X^{(n)}) = E_r(X)$ for $r = 1, \dots, R$, and for $n \ge k$ we have $P(X^{(n)} = k) = P(X = k)$. Therefore Corollary 1.11 implies our assertion. □

Corollary 1.13 *Let X be a non-negative integer valued r.v. with finite moments. If*

$$\lim_{r\to\infty} E_r(X)r^m/r! = 0$$

for all m, then

$$P(X=k) = \left\{\sum_{r=k}^{\infty}(-1)^{k+r}E_r(X)/(r-k)!\right\}\Big/k!$$

and the sum satisfies the alternating inequalities.

One has similar results for probabilities of the form $P(X \ge k)$. The following is the analogue of Corollary 1.11. The straightforward proof is omitted.

Corollary 1.14 *With the assumptions of Corollary 1.11*

$$P(X \ge k) = \sum_{r=k}^{n}(-1)^{k+r}\binom{r-1}{k-1}\frac{E_r(X)}{r!} = \sum_{r=k}^{n}(-1)^{k+r}\frac{E_r(X)}{(k-1)!(r-k)!r}$$

and the sum satisfies the alternating inequalities.

The results above can be extended to several sequences of events and to several random variables. We shall only state the analogue of Corollary 1.11. Let us say that a finite sum

$$s = \sum_{i_1=a_1}^{b_1}\cdots\sum_{i_m=a_m}^{b_m} x_{i_1,\dots,i_m}$$

satisfies the alternating inequalities if

$$\sum_{i_1=a_1}^{c_1}\cdots\sum_{i_m=a_m}^{c_m} x_{i_1,\dots,i_m} - s$$

is at least 0 if for each j either $c_j = b_j$ or $a_j \le c_j \le b_j$ and $c_j - a_j$ is even, and it is at most 0 if for each j either $c_j = b_j$ or $a_j \le c_j \le b_j$ and $c_j - a_j$ is odd.

Corollary 1.15 *Let $X_1, \dots, X_m$ be random variables with values in $\{0, 1, \dots, n\}$ and let*

$$E(r_1, \dots, r_m) = E\{(X_1)_{r_1} \dots (X_m)_{r_m}\}.$$

Then

$$P(X_1 = k_1, \dots, X_m = k_m) = \sum_{r_1=k_1}^{n} \cdots \sum_{r_m=k_m}^{n} (-1)^{k+r} \frac{E(r_1, \dots, r_m)}{\prod_1^m (r_i - k_i)!} \Big/ \prod_{i=1}^{m} k_i!$$

and the sum satisfies the alternating inequalities. Here $r = \sum_{i=1}^m r_i$ and $k = \sum_{i=1}^m k_i$.

If the random variables take non-negative integer values then the inequalities still hold.

In general, the inequalities appearing in the corollaries above are the best possible. However, if we know some relationships among the moments then we may be able to find better inequalities. The next result is an example of this.

Theorem 1.16 *Let X be a non-negative integer valued r.v. with moments $m_1 = E(X)$ and $m_2 = E(X^2)$.*

If $m_1 \le m_2 \le 2m_1 \le 2$, then

$$P(X = 0) \le 1 - (3m_1 - m_2)/2,$$

and if $2m_1 \le m_2 \le 3m_1 \le 6$, then

$$P(X = 0) \le 1 - (5m_1 - m_2)/6.$$

Both inequalities are best possible.

Proof Set $p_i = P(X = i), i = 0, 1, \dots$. Then

$$\sum_{i}^{\infty} (3i - i^2) p_i = 3m_1 - m_2,$$

so

$$1 - p_0 = \sum_{1}^{\infty} p_i = \frac{1}{2}(3m_1 - m_2) + \frac{1}{2} \sum_{1}^{\infty} (i^2 - 3i + 2) p_i.$$

Since

$$2i(i-2) \le 3(i-1)(i-2) = 3(i^2-3i+2), i = 1,2,\dots,$$

we have

$$\frac{1}{2}\sum_1^\infty (i^2-3i+2)p_i \ge \frac{1}{3}\sum_1^\infty (i^2-2i)p_i = \frac{1}{3}(m_2-2m_1).$$

Hence

$$1-p_0 \ge \tfrac{1}{2}(3m_1-m_2)+\max\left\{0, \tfrac{1}{3}(m_2-2m_1)\right\},$$

which implies our inequalities. It shows also that the first inequality in the theorem holds unconditionally—which is no surprise since it is a particular case of Corollary 1.12.

To see that the inequalities are best possible, in the first case define the distribution of X by $p_0 = 1-(3m_1-m_2)/2$, $p_1 = 2m_1-m_2$, $p_2 = (m_2-m_1)/2$, $0 = p_3 = p_4 = \dots$, and in the second case by $p_0 = 1-(5m_1-m_2)/6$, $p_1 = 0$, $p_2 = (3m_1-m_2)/2$, $p_3 = (m_2-2m_1)/3$, $0 = p_4 = p_5 = \dots$. The conditions on m_1 and m_2 imply that these choices are possible. It is easily checked that the moments are as required. □

The first inequality in Theorem 1.16 is exactly the inequality implied by Corollary 1.12. Note also that both inequalities are better than the Chebyshev type inequalities (1.2′) and (1.3).

Our next aim is to present a rather unusual but widely applicable inequality, the *Lovász Local Lemma.* Given independent events $A_1, A_2, \dots, A_m$ with $P(A_i) < 1$ we know that $P(\cap_{i=1}^m \overline{A}_i > 0)$ is not 0 since it is exactly $\Pi_{i=1}^m P(\overline{A}_i)$. Now, if the A_i are not independent but each A_i is independent of a system formed by 'most' of the A_j then a beautiful theorem of Erdős and Lovász (1975) may enable us to deduce that $P(\cap_{i=1}^m \overline{A}_i) > 0$. This result has become known as the *Lovász Local Lemma.* Extensions of the Lovás Local Lemma were proved by Spencer (1975, 1977); the next two theorems, which can be read out of the original proof in Erdős and Lovász (1975), are further slight extensions.

Theorem 1.17 *Let $A_1, A_2, \dots, A_m$ be events in a probability space, $J(1)$, $J(2), \dots, J(m)$ subsets of $\{1,2,\dots,m\}$ and $\gamma_1, \gamma_2, \dots, \gamma_m$ positive reals less than 1 such that for each $i, 1 \le i \le m$,*

(i) *A_i is independent of the system $\{A_j : j \notin J(i) \cup \{i\}\}$,*
(ii) *$P(A_i) \le \gamma_i \Pi_{j \in J(i)}(1-\gamma_j)$.*

Then

$$P\left(\bigcap_{j=1}^{m} \overline{A}_j\right) \geq \Pi_{j=1}^{m}(1-\gamma_j) \text{ and } P\left(A_1 \middle| \bigcap_{j=2}^{m} \overline{A}_j\right) \leq \gamma_1.$$

Proof We prove the assertions by induction on m. The case $m = 1$ is trivial, and in the proof of the induction step it suffices to show the second assertion for that implies

$$P\left(\bigcap_{j=1}^{m} \overline{A}_j\right) = P\left(\overline{A}_1 \middle| \bigcap_{j=2}^{m} \overline{A}_j\right) P\left(\bigcap_{j=2}^{m} \overline{A}_j\right) \geq (1-\gamma_1) P\left(\bigcap_{j=2}^{m} \overline{A}_j\right) \geq \prod_{j=1}^{m}(1-\gamma_j).$$

Assume that $J(1) = \{2, \ldots, d+1\}$ so A_1 is independent of A_{d+3}, $A_{d+3}, \ldots, A_m$. Since by the induction hypothesis $P(\cap_{j=2}^{m} \overline{A}_j) > 0$, the conditional probability $P(A_1 | \cap_{j=2}^{m} \overline{A}_j)$ is well defined and

$$\begin{aligned} P\left(A_1 \middle| \bigcap_{j=2}^{m} \overline{A}_j\right) &= \frac{P(A_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_m)}{P(\overline{A}_2 \cap \ldots \cap \overline{A}_m)} \\ &\leq \frac{P(A_1 \cap \overline{A}_{d+2} \cap \ldots \cap \overline{A}_m) P(\overline{A}_{d+2} \cap \ldots \cap \overline{A}_m)}{P(\overline{A}_{d+2} \cap \ldots \cap \overline{A}_m) P(\overline{A}_2 \cap \ldots \cap \overline{A}_m)} \\ &= \frac{P(A_1 | \overline{A}_{d+2} \cap \ldots \cap \overline{A}_m)}{P(\overline{A}_2 \cap \ldots \cap \overline{A}_{d+1} | \overline{A}_{d+2} \cap \ldots \cap \overline{A}_m)}. \end{aligned}$$

As A_1 is independent of $\{A_{d+2}, \ldots, A_m\}$, the numerator is precisely A_1. We can estimate the denominator as follows:

$$\begin{aligned} P(\overline{A}_2 \cap \ldots \cap \overline{A}_{d+1} | \overline{A}_{d+2} \cap \ldots \cap \overline{A}_m) &= P(\overline{A}_2 | \overline{A}_3 \cap \ldots \cap \overline{A}_m) P(\overline{A}_3 | \overline{A}_4 \cap \ldots \cap \overline{A}_m) \\ \ldots P(\overline{A}_{d+1} | \overline{A}_{d+2} \cap \ldots \cap \overline{A}_m) &\geq \prod_{j=2}^{d+1}(1-\gamma_j) = \prod_{j \in J(1)} (1-\gamma_j), \end{aligned}$$

where we applied the induction hypothesis to the systems $\{A_j, A_{j+1}, \ldots, A_m\}$, $j = 2, 3, \ldots$ Hence

$$P\left(A_1 \middle| \bigcap_{j=2}^{m} A_j\right) \leq P(A_1) \Big/ \prod_{j \in J(1)} (1-\gamma_j) \leq \gamma_1,$$

completing the proof. □

In most applications an event A_i is independent of a family $\{A_l : l \in L\}$ if A_i is independent of each $A_l, l \in L$. In that case the sets $J(i)$ in Theorem 1.17 are best defined by a *dependence graph*: a graph F on

$\{1,2,\ldots,m\}$ such that $J(i)$ is precisely $\Gamma(i)$, the set of neighbours of i in F. If, in addition, the sets $\Gamma(i)$ are fairly small (i.e. F has small maximal degree) then the following variant of Theorem 1.17 may be useful.

Theorem 1.18 *Let $A_1, A_2, \ldots, A_m$ be events with dependence graph F. Suppose $0 < \gamma < \frac{1}{2}$ and*

$$P(A_i) \le \gamma(1-\gamma)^{d(i)-1}$$

for every i, where $d(i)$ is the degree of i in F. Then

$$P\left(A_1 \,\middle|\, \bigcap_{j=2}^{m} \overline{A}_j\right) \le P(A_1)(1-\gamma)^{-d(1)} \le \gamma/(1-\gamma).$$

If F has maximal degree $\Delta \ge 3$ and

$$P(A_i) \le (\Delta-1)^{\Delta-1}/\Delta^{\Delta}$$

then

$$P\left(\bigcap_{j=1}^{m} \overline{A}_j\right) > 0.$$

Proof The first part follows by imitating the proof of Theorem 1.17, with $J(i) = \Gamma(i)$. Note that if j is a neighbour of vertex 1, then j has degree $d(j)-1$ in $F - \{1\}$, so with $d = d(1)$ and the notation of the proof of Theorem 1.17,

$$P(\overline{A}_j | \overline{A}_{j+1} \cap \ldots \cap \overline{A}_m) \ge 1 - P(A_j)(1-\gamma)^{-d(j)+1} \ge 1-\gamma.$$

for $2 \le j \le d+1$. Hence

$$P\left(A_1 \,\middle|\, \bigcap_{j=2}^{m} \overline{A}_j\right) \le P(A_1)(1-\gamma)^{-d(1)} \le \gamma/(1-\gamma),$$

as claimed.

The second part follows by putting $\gamma = 1/\Delta$. □

Note that $\{(\Delta-1)/\Delta\}^{\Delta-1} > 1/\mathrm{e}$ if $\Delta \ge 2$, so if $\Delta(G) = \Delta \ge 2$ and $P(A_i) \le 1/(\mathrm{e}\Delta)$ for every i, then $P(\cap_{i=1}^{m} \overline{A}_i) > 0$. In the original paper of Erdős and Lovász (1975) this was proved under the assumption that $P(A_i) \le 1/4\Delta$.

The Lovász Local Lemma enables us to show that certain unlikely events do occur with positive probability, even when this probability is exponentially small. In some applications, mere existence is frequently not sufficient and it is desirable to have a fast algorithm to locate 'rare' objects. This difficult and important problem was solved by Beck (1991), who showed that in some applications the Lemma can be converted into polynomial time sequential algorithms for finding desired 'rare' objects. With this breakthrough, Beck has greatly increased the importance of the Lovász Local Lemma to algorithms. Alon (1995) modified Beck's technique and constructed a parallelizable algorithmic version of the Lovász Local Lemma.

Having seen inequalities that guarantee that an event has positive probability even if this probability is exponentially small, we turn to inequalities that can be used to show that certain 'bad' events have exponentially small probabilities.

Given a probability triple $(\Omega, \mathcal{F}, \mathbb{P})$, let $\mathcal{F}_0 \subset \mathcal{F}, \subset \ldots$ be increasing sub-σ-fields of $\mathcal{F}$.

Let $X_0, X_1, \ldots$ be r.vs on Ω such that X_k is $\mathcal{F}_k$-measurable and $E(X_{k+1}|\mathcal{F}_k) = X_k$. The sequence (X_k) is a *martingale*. In combinational applications, more often than not, Ω is a finite set and so (X_k) is a finite sequence, each $\mathcal{F}_k$ is given by a partition of Ω into blocks (the atoms of $\mathcal{F}_k$), with the partition of $\mathcal{F}_k$ refining that of $\mathcal{F}_{k-1}$, and $X_k = E(X|\mathcal{F}_k) = E(X_{k+1}|\mathcal{F}_k)$ for some r.v. X on Ω. Furthermore, usually $\mathcal{F}_0$ is the σ-field $(\Omega, \emptyset)$ and so $X_0 = E(X_k) = E(X)$ for every k.

The following *Hoeffding–Azuma inequality* was proved by Hoeffding (1963) and Azuma (1967).

Theorem 1.19 *Let $(X_k)_0^l$ be a martingale such that $|X_k - X_{k-1}| \leq c_k, k = 1, \ldots, l$, for some constants $c_1, \ldots, c_l$. Then, for every $t \geq 0$,*

$$\mathbb{P}(X_l \geq X_0 + t) \leq \exp\left\{-t^2 \Big/ 2\sum_1^l c_k^2\right\}.$$

In combinatorics, it is often convenient to apply a variant of this inequality. The result below is due to Janson (2001), who proved the inequality with a particularly good constant in the exponent.

Theorem 1.20 *Let $Z_1, \ldots, Z_l$ be independent r.vs, with Z_k taking values in a set Ω_k. Let $f : \Omega = \Omega_1 \times \ldots \times \Omega_l \to \mathbb{R}$ be a measurable function such that if $\omega \in \Omega$ and $\omega' \in \Omega$ differ only in their kth coordinates then*

$$|f(\omega) - f(\omega')| \leq c_k$$

for some positive constants $c_1, \ldots, c_k$. Then the random variable $X =$

$f(Z_1,\dots,Z_l)$ *is such that, for every* $t \geq 0$,

$$\mathbb{P}(X \leq \mathbb{E}X - t) \leq \exp\left\{-2t^2 \Big/ \sum_1^l c_k^2\right\}.$$

Replacing f by $-f$, we see that $\mathbb{P}(X \geq \mathbb{E}X + t) \leq \exp\{-2t^2/\sum_1^l c_k^2\}$ holds as well.

Frequently, the set-up is even simpler: $\Omega_1,\dots,\Omega_k$ are finite probability spaces with product Ω, and $X : \Omega \to \mathbb{R}$ is a r.v. that satisfies the Lipschitz condition in Theorem 1.20:

$$|X(\omega) - X(\omega')| \leq c_k$$

if ω and ω' differ only in their kth coordinates. Then, as before,

$$\mathbb{P}(X \leq \mathbb{E}X - t) \leq \exp\left\{-2t^2 \Big/ \sum_1^l c_k^2\right\}$$

for every $t \geq 0$.

1.5 Convergence in Distribution

The sieve formulae of the previous section imply a number of results about convergence in distribution. In particular, Corollaries 1.12 and 1.13 have the following immediate consequence.

Theorem 1.21 *Let* $X_1, X_2, \dots$ *and* X *be non-negative integer-valued random variables. Suppose*

$$\lim_{n\to\infty} E_r(X_n) = E_r(X), \qquad r = 0, 1, \dots$$

and

$$\lim_{r\to\infty} E_r(X) r^m / r! = 0, m = 0, 1, \dots.$$

Then

$$X_n \xrightarrow{d} X.$$

If X is a Poisson r.v. with mean λ, then $E_r(X) = \lambda^r$ for every r. Hence, Theorem 1.21 implies the following result.

Theorem 1.22 *Let* $\lambda = \lambda(n)$ *be a non-negative bounded function on* $\mathbb{N}$. *Suppose the non-negative integer valued random variables* $X_1, X_2, \dots$ *are* *such that*

$$\lim_{n\to\infty}\{E_r(X_n)-\lambda^r\}=0, \qquad r=0,1,\ldots.$$

Then

$$d(X_n,P_\lambda)\longrightarrow 0.$$

This simple result will often be used in the main body of the book [see also Bender (1974*a*) for many other applications and refinements of the method]. We shall also need the analogue of Theorem 1.22 for several sequences of r.vs. The result below is implied by Corollary 1.15.

Theorem 1.23 *Let $\lambda_1=\lambda_1(n),\ldots,\lambda_m=\lambda_m(n)$ be non-negative bounded functions on $\mathbb{N}$. For each n let $X_1(n),\ldots,X_m(n)$ be non-negative integer valued random variables defined on the same space. Suppose for all $r_1,\ldots,r_m\in\mathbb{Z}^+$ we have*

$$\lim_{n\to\infty}(E\{(X_1(n))_{r_1}\ldots(X_m(n))_{r_m}-\lambda_1^{r_1}\ldots\lambda_m^{r_m}\})=0.$$

Then $X_1(n),\ldots,X_m(n)$ are asymptotically independent Poisson random variables with means $\lambda_1,\ldots,\lambda_m$, that is

$$\lim_{n\to\infty}\left[P\{X_1(n)=k_1,\ldots,X_m(n)=k_m\}-\prod_{i=1}^{m}(\mathrm{e}^{-\lambda_i}\lambda_i^{k_i}/k_i!)\right]=0$$

for all $k_1,\ldots,k_m\in\mathbb{Z}^+$.

We know that if $\lambda>0$ is a constant and $pn\to\lambda$, then $S_{p,n}\xrightarrow{d}P_\lambda$. Also, if $pqn\to\infty$ then $(S_{p,n}-pn)/\sqrt{pqn}\xrightarrow{d}N(0,1)$. Hence $(P_\lambda-\lambda)/\sqrt{\lambda}\xrightarrow{d}N(0,1)$ as $\lambda\to\infty$. [This is another special case of the Central Limit Theorem (see Theorem 1.25, below), since by Ex. 5 if $X_1,X_2,\ldots,X_n$ are independent Poisson r.vs with mean 1, then $\sum_{i=1}^n X_i$ has Poisson distribution with mean n.] We shall often need the assertion that similar convergence holds for r.vs which are not necessarily Poisson but are close to being Poisson r.vs.

Suppose X is a real-valued r.v. with a continuous distribution function F and absolute moments $M_1,M_2,\ldots$:

$$M_n=\int_{-\infty}^{\infty}|x|^n\mathrm{d}F.$$

If all moments exist and

$$\limsup_{n\to\infty}M_n^{1/n}/n<\infty,$$

then F is uniquely determined by its moments. In fact, by Carleman's theorem F is uniquely determined by its moments iff $\sum_{n=1}^{\infty} M_n^{-1/n} = \infty$ (see Feller, 1966, vol. II, p. 487). Since the nth absolute moment of $N(0,1)$ is asymptotic to $\sqrt{2}(n/e)^{n/2}$ (see Ex. 8), the normal distribution is determined by its moments. This implies that if (X_n) is a sequence of real valued r.vs such that for every fixed r the rth moment of X_n tends to the rth moment of $N(0,1)$, then $X_n \xrightarrow{d} N(0,1)$:

The observations above lead us to the following simple result.

Theorem 1.24 *Let (X_n) be a sequence of r.vs and let $\lambda_n \to \infty$. Suppose*

$$E_r(X_n) - \lambda_n^r = o(\lambda_n^{-s})$$

for all r and s, $1 \le r \le s$. Then

$$\frac{X_n - \lambda_n}{\sqrt{\lambda_n}} \xrightarrow{d} N(0,1).$$

Proof Clearly, for every $k \in \mathbb{N}$,

$$E\{(X_n - \lambda_n)^k \lambda_n^{-k/2}\} = \sum_{r=0}^{k}\sum_{t=0}^{k} c_{k,r,t} E_r(X_n)\lambda_n^{t-k/2}, \tag{1.21}$$

where $c_{k,r,t}$ depends only on k, r and t.

Let $Y_1, Y_2, \dots$ be Poisson r.vs, with Y_n having mean λ_n, and set $Z_n = (Y_n - \lambda_n)\lambda_n^{-1/2}$. Then $Z_n \xrightarrow{d} N(0,1)$ and so

$$E(Z_n^k) = \sum_{r=0}^{k}\sum_{t=0}^{k} c_{k,r,t}\lambda_n^{r+t-k/2} \longrightarrow m_k,$$

where m_k is the kth moment of $N(0,1)$. Therefore (1.21) and our assumption on $E_r(X_n)$ imply that the kth moments of the sequence $(X_n - \lambda_n)\lambda_n^{-1/2}$ also converge to m_k. □

Convergence to normal distribution holds under rather weak conditions. Here we shall just state two versions of the Central Limit Theorem holding for variable distributions. The following result, which is essentially the best possible, is due to Lindeberg (1922) (see also Feller, 1966, vol. II, p. 256).

Theorem 1.25 *Let $X_1, X_2, \dots$ be independent random variables with X_k having mean 0, variance $\sigma_k^2 > 0$ and distribution function*

$$s_n^2 = \sum_{k=1}^{n} \sigma_k^2.$$

Suppose

$$s_n^{-2} \sum_{k=1}^{n} \int_{|y| \geq t s_n} y^2 dF_k(y) \longrightarrow 0 \tag{1.22}$$

for every $t > 0$. Then

$$\sum_{k=1}^{n} X_k / s_n \xrightarrow{d} N(0,1).$$

It is not always easy to check whether (1.22, called the *Lindeberg condition*, is satisfied; often it is more convenient to check the *Ljapunov condition*, (1.23), given below (see Ex. 22).

Corollary 1.26 *Suppose (X_k) and (s_n) are as in Theorem 1.25, and for some $\delta > 0$*

$$\sum_{k=1}^{n} E(|X_k|^{2+\delta}) = o(s_n^{2+\delta}). \tag{1.23}$$

Then the Lindeberg condition (1.22 is satisfied and

$$\sum_{k=1}^{n} X_k / s_n \xrightarrow{d} N(0,1).$$

In combinatorial applications one usually checks (1.23) with $\delta = 1$.

In estimating joint probability distributions, the following simple result is often useful.

Theorem 1.27 *Let $f_1(x_1, \dots, x_N)$, $f_2(x_1, \dots, x_N)$, $\dots$, $f_r(x_1, \dots, x_N)$ be non-negative functions, non-decreasing in each variable x_i. Then if $X_1, \dots, X_N$ are independent r.vs, we have*

$$E\left\{\prod_{j=1}^{r} f_j(X_1, \dots, X_N)\right\} \geq \prod_{j=1}^{r} E\{f_j(X_1, \dots, X_N)\}.$$

It is easily seen that the general case follows from the case $r = 2$ and $N = 1$ (Ex. 21). By replacing $f_j(x_1, \dots, x_N)$ by $f_j(-x_1, \dots, -x_N)$ we see that the same inequality holds if the functions are non-increasing in each variable x_i.

Theorems 1.22 and 1.24 give rather simple-minded, though very useful, methods for showing approximations by Poisson and normal distributions. In the context of random graphs, a considerably more sophisticated method was used by Barbour (1982). This approach is based on that of C. Stein (1970) for the normal distribution and that of Chen (1975) and Barbour and Eagleson (1982) for the Poisson distribution.

The approximation by the Poisson distribution rests on an ingenious observation we shall state as a theorem. For $A \subset \mathbb{Z}^+$ and $\lambda > 0$ let $x = x_{\lambda,A}$ be the real-valued function on $\mathbb{Z}^+$ defined by $x(0) = 0$ and

$$x(m+1) = \lambda^{-m-1} e^{\lambda} m! \{P_\lambda(A \cap C_m) - P_\lambda(A) P_\lambda(C_m)\}, \qquad m \geq 0.$$

Here

$$C_m = \{0, 1, \ldots, m\},$$

and

$$P_\lambda(B) = e^{-\lambda} \sum_{k \in B} \lambda^k / k!$$

is the probability that a Poisson r.v. with mean λ has its value in B.

Theorem 1.28 *The function $x = x_{\lambda,A}$ has the following properties:*

(i) $\|x\| \equiv \sup_m |x(m)| \leq \min\{1, 2\lambda^{-1/2}\}$,
(ii) $\Delta x \equiv \sup_m |x(m+1) - x(m)| \leq 2 \min\{1, \lambda^{-1}\}$,
(iii) for any non-negative integer valued r.v. Y

$$E\{\lambda x(Y+1) - Y x(Y)\} = P(Y \in A) - P_\lambda(A).$$

Proof For a proof of (i) and (ii) we refer the reader to Barbour and Eagleson (1982). Although the proof of (iii) is even more straightforward, we give it here, since the significance of x is exactly that with the aid of x we can express the difference $P(Y \in A) - P_\lambda(A)$ in a pleasant form.

Assertion (iii) is equivalent to the relation

$$\lambda x(k+1) - k x(k) = \begin{cases} 1 - P_\lambda(A), & \text{if } k \in A, \\ -P_\lambda(A), & \text{if } k \notin A. \end{cases} \tag{1.24}$$

To see (1.24) note that if $k \geq 1$, then

$$\begin{aligned} \lambda x(k+1) - k x(k) &= \lambda^{-k} e^{\lambda} k! \{P_\lambda(A \cap C_k) - P_\lambda(A) P_\lambda(C_k) - P_\lambda(A \cap C_{k-1}) \\ &\quad + P_\lambda(A) P_\lambda(C_{k-1})\} \\ &= [P_\lambda(A \cap \{k\}) - P_\lambda(A) P_\lambda(\{k\})] / P_\lambda(\{k\}) \\ &= P_\lambda(A \cap \{k\}) / P_\lambda(\{k\}) - P_\lambda(A). \end{aligned}$$

and for $k = 0$ we have

$$\begin{aligned}\lambda x(1) &= e^{\lambda}[P_\lambda(A \cap \{0\}) - P_\lambda(A)P_\lambda(\{0\})] \\ &= P_\lambda(A \cap \{0\})/P_\lambda(\{0\}) - P_\lambda(A). \qquad \square\end{aligned}$$

Theorem 1.28 may enable us to estimate the total variation distance of a distribution from a Poisson distribution. In this way we may prove a convergence rate for $X_n \xrightarrow{d} P_\lambda$.

Exercises

1.1 Prove inequalities (1.8), (1.9) and (1.11).

1.2 Check that $\phi(x)$ is indeed a density function.

1.3 Let Y be a geometric r.v. with mean q/p, i.e. let $P(Y = k) = q^k p, k = 0, 1, \ldots$. Prove that $E(Y) = q/p, \sigma^2(Y) = q/p^2$ and $E_r(Y) = r!(q/p)^r$.

1.4 Show that an exponential r.v. with parameter $\lambda > 0$ has mean $1/\lambda$ and variance $1/\lambda^2$.

1.5 Let (Y_n) be a sequence of geometric r.vs with Y_n having mean $(1 - p_n)/p_n$. Show that if $p_n \to 0$, then $p_n Y_n \xrightarrow{d} L$, where L is an exponential r.v. with mean 1.

1.6$^-$ Let X and Y be independent Poisson r.vs with means λ and μ. Prove that $X + Y$ has Poisson distribution with mean $\lambda + \mu$.

1.7 Prove formula (1.15). [See Feller (1966, vol. I, p. 179) for a proof of the case $l = 0$.]

1.8 Prove that the rth absolute moment of $N(0,1)$ is $(r-1)!! = (r-1)(r-3)\ldots 3\cdot 1 \sim \sqrt{2}(r/e)^{r/2}$ if r is even, and $(1/\sqrt{\pi})2^{r/2}\{(r-1)/2\}! \sim \sqrt{2}(r/e)^{r/2}$ if r is odd. Indeed,

$$\begin{aligned}\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}|x|^r e^{-x^2/2}dx &= \sqrt{\frac{2}{\pi}}\int_0^{\infty} x^r e^{-x^2/2}dx \\ &= \frac{1}{\sqrt{\pi}}\int_0^{\infty} t^{-1/2}(2t)^{r/2}e^{-t}dt \\ &= \frac{1}{\sqrt{\pi}}2^{r/2}\int_0^{\infty} t^{(r-1)/2}e^{-t}dt \\ &= \frac{1}{\sqrt{\pi}}2^{r/2}\Gamma\left(\frac{r+1}{2}\right),\end{aligned}$$

where $t = x^2/2$. If r is even, then

$$\Gamma\left(\frac{r+1}{2}\right) = \frac{r-1}{2}\frac{r-3}{2}\cdots\frac{1}{2}\cdot\Gamma\left(\frac{1}{2}\right) = 2^{-r/2}\sqrt{\pi}(r-1)!!$$

and if r is odd then $\Gamma\{(r+1)/2\} = \{(r-1)/2\}!$ [See Gradshteyn and Ryzhik (1980, p. 337), Spiegel (1974, p. 268) or Titchmarsh (1964, p. 63.]

1.9$^-$. Deduce from Ex. 8 that for every natural number n we have

$$\int_0^\infty x^n e^{-x^2/2} dx \le (n!)^{1/2}.$$

1.10 Prove Theorem 1.7.

1.11$^-$. Let X be a non-negative integer-valued r.v.. Show that $E(X^2) \ge E(X)$ and $P(X = 0) \ge 1 - E(X)$.

1.12 Given $m_1 > 0, m_2^* > 0$ and $\varepsilon > 0$, construct a non-negative integer-valued r.v. X such that

$$E(X) = m_1, E(X^2) \ge m_2^* \text{and} P(X = 0) \le 1 - m_1 + \varepsilon.$$

[This shows that a large variance cannot improve the trivial lower bound on $P(X = 0)$ given in Ex. 10.]

1.13 Apply induction on the number of sets to show that inequalities (1.18) and $p_\varnothing = 1$ characterize the functions p_I defined after Corollary 1.9. (Rényi, 1970*a*.)

1.14 Let $g = g(A_1, \ldots, A_n) = \sum_{i=1}^N \sum_{j=1}^N c_{i,j} p(F_i) P(F_j)$, where the $c_{i,j}$ are real constants and $F_1, \ldots, F_N$ are Boolean functions of the variable events $A_1, \ldots, A_n$. Suppose $g(A_1, \ldots, A_n) = 0$ whenever each A_i has probability 0 or 1. Prove that

$$g(A_1, \ldots, A_n) \ge 0$$

holds in every probability space and for all choices of the A_i's iff it holds for all choices of the events in the space $\{x_1, x_2\}, P(x_1) = P(x_2) = \frac{1}{2}$. (Galambos and Rényi, 1968.)

1.15 Let L be the lattice of all subsets of $[n] = \{1, 2, \ldots, n\}$ and let $\mathscr{D}_n$ be the set of probability measures on $[n]$ such that no point gets measure 0. Then every $P \in \mathscr{D}_n$ can be considered as a lattice homomorphism $L \to [0,1]$, $A \to P(A)$. Finally, let us say that two maps $\phi, \psi : L \to [0,1]$ are *homotopic* if $\phi(A) < \phi(B)$ iff $\psi(A) < \psi(B)$.

Is it true that a lattice homomorphism $\psi : L \to [0,1]$ is homotopic to ϕ_P for some $p \in \mathscr{D}_n$ iff

$$\psi(A) < \psi(B) \text{iff} \psi(A \backslash B) < \psi(B \backslash A)$$

for all $A, B \in L$?

1.16 Note that for $m = \mu n$ and $\lambda = 1 - \mu$ the second inequality in (1.5) is of the form

$$\binom{n}{m} \leq \frac{1}{\sqrt{2\pi\lambda\mu n}} \lambda^{-\lambda n} \mu^{-mun}.$$

Prove that for $m = \mu n > pn$ we have

$$P(S_{n,p} \leq m) = \sum_{k=\mu n}^{n} \binom{n}{k} p^k q^{n-k} \leq (p/\lambda)^{\lambda n} (q/\mu)^{\mu n}.$$

[See Chernoff (1952) and Peterson (1961).]

1.17 Let A_i and $\Gamma(i)$ be as in Theorem 1.18 and suppose $|\Gamma(i)| = 1$ for every i. Show that if $P(A_i) < 1/2$ for every i, then $P(\bigcap_{i=1}^m \bar{A}_i) > 0$. [Note that one may have $P(A_i) = \frac{1}{2}$ for every i and $P(\bigcap_{i=1}^m \bar{A}_i) = 0$.]

1.18 Give an example of a system $\{A_i\}_1^m$ such that, with the notation of Theorems 1.17 and 1.18, $|\Gamma(i)| = d$ for every i but there is no dependence graph with maximal degree 1.

[Hint: Let $m = 2k + 1 \geq 3$ and let $A_1, A_2, \ldots, A_m$ be such that any $m - 1$ of the A_j's form an independent system, but the entire system is not independent.]

1.19 Show that if $A_1, A_2, \ldots, A_m$ are as in Theorem 1.17, $0 < \delta_i P(A_i) < 0.69$ and

$$\log \delta_i \geq \sum_{j \in J(i)} \{\delta_j P(A_j) + \delta_j^2 P(A_j)^2\},$$

$i = 1, \ldots, m$, then

$$P\left(\bigcap_{j=1}^m \bar{A}_j\right) \geq \prod_{j=1}^m (1 - \delta_j P(A_j)) > 0.$$

[Set $\gamma_i = \delta_i P(A_i)$ and apply (1.10) to show that the conditions of Theorem 1.17 are satisfied.]

1.20 Show that with the assumptions of Theorem 1.18, one has

$$P\left(\bigcap_{j=1}^m \bar{A}_j\right) \geq (1 - \gamma)^m.$$

1.21 Let f_1 and f_2 be non-negative and non-decreasing functions, and let X_1, X_2, be independent, identically distributed r.vs. Note that

$$E[\{f_1(X_1) - f_1(X_2)\}\{f_2(X_1) - f_2(X_2)\}] \geq 0$$

and so

$$E\{(f_1(X_1)f_2(X_1)\} \geq E\{f_1(X_1)\}E\{f_2(X_1)\}.$$

Show that this implies Theorem 1.27.

1.22 Prove that the Ljapunov conditions (1.23) imply the Lindeberg condition (1.22).

2

Models of Random Graphs

Throughout this book we shall concentrate on labelled graphs. This is partly because they are easier to handle and also because, as we shall see in Chapter IX, most assertions about labelled graphs can be carried over to unlabelled graphs without the slightest difficulty. For the sake of convenience in most cases we consider graphs with n vertices and take $V = \{1, 2, \ldots, n\}$ to be the vertex set. The set of all such graphs will be denoted by $\mathscr{G}^n$.

In the first section we introduce the most frequently encountered probability spaces (models) of random graphs. The following two sections contain basic properties of the models. The last section is devoted to the model of regular graphs. Unlike the case of the other models, a fair amount of effort is needed before one can prove even the simplest results about this natural and useful probability space.

2.1 The Basic Models

The two most frequently occurring models are $\mathscr{G}(n, M)$ and $\mathscr{G}\{n, P(\text{edge}) = p\}$. The first consists of all graphs with vertex set $V = \{1, 2, \ldots, n\}$ having M edges, in which the graphs have the same probability. Thus with the notations $N = \binom{n}{2}$, which we shall keep throughout the book, $0 \leq M \leq N, \mathscr{G}(n, M)$ has $\binom{N}{M}$ elements and every element occurs with probability $\binom{N}{M}^{-1}$. Almost always M is a function of n: $M = M(n)$. If we want to emphasize that the probability and expectation are taken in $\mathscr{G}\{n, M(n)\}$, then we shall write $P_M(\mathscr{A}) = P_{M(n)}(\mathscr{A})$ and $E_M(X) = E_{M(n)}(X)$ instead of $P(\mathscr{A})$ and $E(\mathscr{A})$.

In the model $\mathscr{G}\{n, P(\text{edge}) = p\}$ we have $0 < p < 1$, and the model consists of all graphs with vertex set $V = \{1, 2, \ldots, n\}$ in which the edges are chosen independently and with probability p. In other words, if G_0 is a graph with vertex set V and it has m edges, then

$$P(\{G_0\}) = P(G = G_0) = p^m q^{N-m}.$$

Here, as everywhere else in the book, q stands for $1 - p$. On the other hand, if we want to emphasize that the probability and expectation are taken in $\mathscr{G}\{n, P(\text{edge}) = p\}$, then we write P_p and E_p instead of P and E. This will be especially important if, as is often the case, $p = p(n)$ is a function of n.

Note that $\mathscr{G}\{n, P(\text{edge}) = \frac{1}{2}\}$ is exactly $\mathscr{G}^n$ with any two graphs being equiprobable.

When there is no danger of confusion, we shall use natural abbreviations. Often we write $\mathscr{G}_M, \mathscr{G}(M)$ or $\mathscr{G}\{M(n)\}$ for $\mathscr{G}\{n, M(n)\}$ and $\mathscr{G}(n,p), \mathscr{G}_p, \mathscr{G}(p)$ or $\mathscr{G}\{\mathrm{p(n)}\}$ for $\mathscr{G}\{n, P(\text{edge}) = p(n)\}$. Furthermore, G_p and G_M stand for random graphs from $\mathscr{G}(n,p)$ and $\mathscr{G}(n,M)$. Thus $P(G_p$ is disconnected) is the probability that a graph in $\mathscr{G}\{n, P(\text{edge}) = p\}$ is disconnected. If there is some danger of ambiguity, then we write $G_{n,p}$ and $G_{n,M}$, emphasizing that our graphs have n vertices. Finally, the expression 'random graph' is frequently abbreviated to 'r.g.'.

Occasionally we shall comment on a natural refinement of $\mathscr{G}\{n, P(\text{edge}) = p\}$. This is the model $\mathscr{G}\{n, (p_{ij})\}$; where $0 \leq p_{ij} \leq 1$ for $1 \leq i < j \leq n$. It consists of all graphs with vertex set $V = \{1, 2, \ldots, n\}$ in which the edges are chosen independently, and for $1 \leq i < j \leq n$ the probability of ij being an edge is exactly p_{ij}.

A special case of $\mathscr{G}\{n, (p_{ij})\}$ is $\mathscr{G}(H; p)$, where H is a fixed graph and $0 < p < 1$. In this case we select the edges of H with probability p independently of each other, and the edges not belonging to H are not selected. If $V(H) = V$, then with

$$p_{ij} = \begin{cases} p, & \text{if } ij \in E(H), \\ 0, & \text{otherwise,} \end{cases}$$

the space $\mathscr{G}(H; p)$ is identified with $\mathscr{G}\{n, (p_{ij})\}$.

Also, $\mathscr{G}(K^n; p)$ is the same as $\mathscr{G}(n,p)$. The space $\mathscr{G}\{K(n,m); p\}$ consists of bipartite labelled graphs with vertex sets U and W, $|U| = n$, $|W| = m$, in which each $U - W$ edge is selected with probability p.

We call a subset Q of $\mathscr{G}^n$ a *property of graphs of order* n if $G \in Q, H \in \mathscr{G}^n$ and $G \simeq H$ imply that $H \in Q$. In fact, in general all we shall use about a property Q is that it is a subset of $\mathscr{G}^n$. The statement 'G has Q' is then equivalent to '$G \in Q$'. Thus the property of being Hamiltonian is the set $\{G \in \mathscr{G}^n : G \text{ is Hamiltonian}\}$.

A property Q will be said to be *monotone increasing* or simply *monotone* if whenever $G \in Q$ and $G \subset H$ then also $H \in Q$. Thus the property of containing a certain subgraph, for instance a triangle, a complete graph of order five or a Hamilton cycle, is monotone increasing. We call Q *convex* if $F \subset G \subset H$ and $F \in Q, H \in Q$ imply that $G \in Q$. If Q is any property, then $P_M(Q)$ has the natural meaning: it is the probability that a graph of $\mathcal{G}(n, M)$ belongs to Q. Of course, $P_p(Q)$ is defined analogously.

Let Ω_n be a model of random graphs of order n. [Thus we usually have $\Omega_n = \mathcal{G}\{n, M(n)\}$ or $\Omega_n = \mathcal{G}(n, p)$.] We shall say that *almost every* (a.e.) graph in Ω_n has a certain property Q if $P(Q) \to 1$ as $n \to \infty$. Occasionally we shall write almost all (a.a.) instead of almost every.

It is perhaps worth noting that the assertion 'a.e. $G \in \mathcal{G}(n, \frac{1}{2})$ has Q' is the same as 'the proportion of all labelled graphs of order n that have Q tends to 1 as $n \to \infty$'.

Let us prove the heuristically obvious fact that a monotone increasing property is the more likely to occur the more edges we have or are likely to have.

Theorem 2.1 *Suppose Q is a monotone increasing property, $0 \leq M_1 < M_2 \leq N$ and $0 \leq p_1 < p_2 \leq 1$. Then*

$$P_{M_1}(Q) \leq P_{M_2}(Q) \text{ and } P_{p_1}(Q) \leq P_{p_2}(Q).$$

Proof (i) Let us select the M_2 edges one by one. The resulting graph will certainly have property Q if the graph formed by the first M_1 edges only has the property.

(ii) Put $p = (p_2 - p_1)/(1 - p_1)$. Choose independently $G_1 \in \mathcal{G}(n, p_1)$ and $G \in \mathcal{G}(n, p)$ and set $G_2 = G_1 \cup G$. Then the edges of G_2 have been selected independently and with probability $p_1 + p - p_1 p = p_2$, so G_2 is exactly an element of $\mathcal{G}(n, p_2)$. As Q is monotone increasing, if G_1 has Q so does G_2. Hence $P_{p_1}(Q) \leq P_{p_2}(Q)$, as claimed. □

Note that the argument above shows that if Q is a nontrivial monotone increasing property then

$$P_{p_2}(Q) \geq P_{p_1}(Q) + \{1 - P_{p_1}(Q)\}P_p(Q) \geq P_{p_1}(Q) + P_{p_1}(E^n)P_p(K^n) > P_{p_1}(Q).$$

In Theorem 2.1 it is irrelevant that we are dealing with graph properties. Let X be a set consisting of N elements and let Q be a *monotone increasing property* of subsets of X, i.e. let $Q \subset \mathcal{P}(X)$ be such that if $A \in Q$ and $A \subset B \subset X$ then $B \in Q$. For $0 \leq p \leq 1$ let $P_p(Q)$ be the probability that if the elements of X are selected independently and with probability p then the set formed by the chosen elements belongs to Q. Thus

$$P_p(Q) = \sum_{A \in Q} p^{|A|}(1-p)^{N-|A|}.$$

The second part of Theorem 2.1 says that $P_p(Q)$ is a monotone increasing function of p. Let us give another proof of this fact. This proof is somewhat pedestrian, but fairly informative. We may assume that Q is non-trivial, i.e. $\emptyset \notin Q$ and $X \in Q$. Set

$$H_k = \{A : A \in Q, |A| = k\} \text{ and } h_k = |H_k|.$$

Then $h_0 = 0, h_N = 1$,

$$P_p(Q) = \sum_{k=0}^{N} h_k p^k (1-p)^{N-k},$$

and so for $0 < p < 1$

$$\begin{aligned} \mathrm{d}P_p(Q)/\mathrm{d}p &= \sum_{k=1}^{N} k h_k p^{k-1}(1-p)^{N-k} - \sum_{k=1}^{N-1}(N-k)h_k p^k (1-p)^{n-k} \\ &= \sum_{k=1}^{N} p^{k-1}(1-p)^{N-k}\{k h_k - (N-k+1)h_{k-1}\}. \end{aligned}$$

Now each set $A \in H_{k-1}$ is contained in $N-k+1$ sets $B \in H_k$ and each set $B \in H_k$ contains at most k sets $A \in H_{k-1}$. Hence

$$k h_k \geq (N-k+1)h_{k-1},$$

so $\mathrm{d}P_p(Q)/\mathrm{d}p \geq 0$, showing that $P_p(Q)$ is an increasing function of p.

We shall find it extremely useful that in most investigations the models $\mathscr{G}(n, M)$ and $\mathscr{G}\{n, P(\text{edge}) = p\}$ are practically interchangeable, provided M is close to pN. The first two parts of the next theorem show that this is the case when we deal with properties holding for almost all graphs. The third part, essentially from Pittel (1982), allows us to replace $\mathscr{G}(n, M)$ by $\mathscr{G}(n, p)$, $p = M/N$, provided $P_p(Q) = o(M^{1/2})$.

Theorem 2.2 (*i*) *Let Q be any property and suppose $pqN \to \infty$. Then the following two assertions are equivalent.*

(*a*) *Almost every graph in $\mathscr{G}(n, p)$ has Q.*

(*b*) *Given* $x > 0$ *and* $\varepsilon > 0$, *if* n *is sufficiently large, there are*

$$
\begin{aligned}
l \geq (1-\varepsilon)2x(pqN)^{1/2} \textit{ integers } M_1, M_2, \ldots, M_l, \\
pN - x(pqN)^{1/2} < M_1 < M_2 < \ldots < M_l < pN + x(pqN)^{1/2} \\
\textit{such that } P_{M_i}(Q) > 1-\varepsilon \textit{ for every } i, i = 1, \ldots, l.
\end{aligned}
$$

(*ii*) *If* Q *is a convex property and* $pqN \to \infty$, *then almost every graph in* $\mathcal{G}(n,p)$ *has* Q *iff for every fixed* x *a.e. graph in* $\mathcal{G}(n,M)$ *has* Q, *where* $M = \lfloor pN + x(pqN)^{1/2} \rfloor$.

(*iii*) *If* Q *is any property and* $0 < p = M/N < 1$ *then*

$$P_M(Q) \leq P_p(Q) e^{1/6M} (2\pi pqN)^{1/2} \leq 3M^{1/2} P_p(Q).$$

Proof By the DeMoivre–Laplace theorem (Chapter 1, Theorem 2.6), for every fixed $x > 0$

$$P_p\{|e(G) - pN| < x(pqN)^{1/2}\} \sim \Phi(x) - \Phi(-x).$$

Since also

$$P_p\{e(G) = M\} = b(M; N, p) < (pqN)^{1/2}$$

for every M, the equivalence of (a) and (b) follows.

To see (ii), recall Theorem 2.1 and apply (i).

Finally, (iii) follows since by inequality (2.5) of Chapter 1 we have

$$
\begin{aligned}
P_p(Q) &= \sum_{m=0}^{N} \binom{N}{m} p^m q^{N-m} P_m(Q) \\
&\geq \binom{N}{M} p^M q^{N-M} P_M(Q) \\
&\geq P_M(Q)[\mathrm{e}^{1/6M}(2\pi pqN)^{1/2}]^{-1}. \qquad \square
\end{aligned}
$$

This result shows that if we know $P_M(Q)$ with a fair accuracy for every M close to pN, then we know $P_p(Q)$ with a comparable accuracy. The converse is far from being true for a general property. As a trivial example, let Q be the property that the graph has an even number of edges. Then $P_p(Q) \sim 1/2$ whenever $pqN \to \infty$. On the other hand, if $M = 2\lfloor pN/2 \rfloor$ then $0 \leq pN - M < 2$ and $P_M(Q) = 1$ for every n. However, as it is much more pleasant to work in $\mathcal{G}_p$ than in $\mathcal{G}_M$, let us note three cases when we can do so without losing much information about $\mathcal{G}_M$. First, Theorem 2.2 implies that if Q is a convex property and a.e. graph in $\mathcal{G}_p$ has Q then a.e. graph in $\mathcal{G}(\lfloor pN \rfloor)$ has Q, provided $pqN \to \infty$. Once again, it is obvious that the convexity restriction cannot be discarded. For example, if Q is the property that the number of edges is not a square, then if $pqN \to \infty$ then $P_p(Q) \to 1$ but $P_M(Q) = 0$ for $M = \lfloor (pN)^{1/2} \rfloor^2$. The second useful connection between $\mathcal{G}_p$ and $\mathcal{G}_M$ is only a little less trivial, though we state it as a theorem.

Theorem 2.3 *Suppose $a > 0$ and the function $X : \mathcal{G}^n \to [0, a]$ is such that $X(G) \le X(H)$ wherever $G \subset H$. Assume, furthermore, that $0 < p_1(n) < p_2(n) < 1, M(n) \in \mathbb{N}$,*

$$\lim_n p_1 q_1 N = \lim_n p_2 q_2 N = \infty$$

and

$$\lim_n (M - p_1 N)/(p_1 q_1 N)^{1/2} = \lim_n (p_2 N - M)/(p_2 q_2 N)^{1/2} = \infty,$$

where $q_i = 1 - p_i, i = 1, 2$. Then

$$E_{p_1}(X) + o(1) \le E_M(X) \le E_{p_2}(X) + o(1).$$

Finally, if we are interested in $\sum_{M=0}^{N} E_M(X)$, the sum of expectations of a r.v. X, then we do not need any assumptions on X to replace the model $\mathcal{G}(n, M)$ by $\mathcal{G}(n, p)$.

Theorem 2.4 *If $X : \mathcal{G}^n \to \mathbb{R}$ is any function, then*

$$\sum_{M=0}^{N} E_M(X) = (N+1) \int_0^1 E_p(X) dp.$$

Proof Since

$$E_p(X) = \sum_{M=0}^{N} \binom{N}{M} p^M q^{N-M} E_M(X),$$

we have

$$\int_0^1 E_p(X) \mathrm{d}p = \sum_{M=0}^{N} \binom{N}{M} E_M(X) \int_0^1 p^M (1-p)^{N-M} \mathrm{d}p = \frac{1}{N+1} \sum_{M=0}^{N} E_M(X).$$

The second equality above is based on the identity

$$\int_0^1 x^M (1-x)^{N-M} \mathrm{d}x = B(M+1, N-M+1) = \frac{1}{N+1} \binom{N}{M}^{-1},$$

where $B(\nu, \mu)$ is the beta function (see Gradshteyn and Ryzhik, 1980, p. 950). The identity is easily proved by partial integration. □

Erdős and Rényi (1959, 1960, 1961*a*) discovered the important fact that most monotone properties appear rather suddenly: for some $M = M(n)$ almost no G_M has Q while for 'slightly' larger M almost every G_M has Q. Given a monotone increasing property a function $M^*(n)$ is said to be a *threshold function* for Q if

$$M(n)/M^*(n) \to 0 \text{ implies that almost no } G_M \text{ has } Q,$$

and

$$M(n)/M^*(n) \longrightarrow \infty \text{ implies that almost every } G_M \text{ has } Q.$$

A priori there is no reason why a property should have a threshold function though this follows from an observation of Bollobás and Thomason (1987), noting that, with the natural definition, every monotone property of subsets of a set has a threshold function. Considerably deeper results were proved by Friedgut (1999): he gave necessary and sufficient conditions for the existence of sharp thresholds for monotone graph properties.

When we study a specific graph property Q, we do not rely on general results, and often succeed in doing more thick merely identifying a threshold function: for many a property Q we shall determine not just the threshold function but an exact probability distribution: for every $x, 0 < x < 1$, we shall find a function $M_x(n)$ such that $P(G_{M_x} \text{ has } Q) \to x$ as $n \to \infty$.

It is clear that threshold functions are not unique. However, threshold functions are unique within factors $m(n), 0 < \underline{\lim}\, m(n) \le \overline{\lim}\, m(n) < \infty$, that is if M_1^* is threshold function of Q then M_2^* is also a threshold function of Q iff $M_2^* = O(M_1^*)$ and $M_1^* = O(M_2^*)$. In this sense we shall speak of *the* threshold function of a property.

As mentioned earlier, the nearer our r.vs are to being independent, the easier it is to handle them. This is the reason why $\mathcal{G}_p$ is more pleasant to work with than $\mathcal{G}_M$. In $\mathcal{G}_p$ the edges are chosen independently, while in the model $\mathcal{G}_M$ the choice of an edge does have a (fortunately small) effect on the choice of another edge.

Another model with good independence properties is $\mathcal{G}(n; k\text{-out}) = \mathcal{G}_{k\text{-out}}$. A random graph $G_{k\text{-out}}$ is constructed as follows. The vertex set is $V = \{1, 2, \ldots, n\}$. For each vertex $x \in V$ select k other vertices, all $\binom{n-1}{k}$ choices being equiprobable, and all choices being independent, and for each selected vertex y direct an edge from x to y. Let $\vec{G} = \vec{G}_{k\text{-out}}$ be the *random directed graph* constructed in this way, with $\vec{\mathcal{G}} = \vec{\mathcal{G}}_{k\text{-out}}$ the probability space formed by them. Equivalently, $\vec{\mathcal{G}}_{k\text{-out}}$ is the probability space of all directed graphs with vertex set V in which every vertex has outdegree k.

It is fascinating to note that $\vec{\mathscr{G}}_{k\text{-out}}$ is mentioned in the Scottish Book: in 1935 Ulam asked for the probability of $\vec{G}_{k\text{-out}}$ being connected (see Mauldin, 1979; p. 107, Problem 2.38).

For $\vec{G} \in \vec{\mathscr{G}}$ let $G_{k\text{-out}} = \phi(\vec{G})$ be the random graph with vertex set V and edge set $\{xy$: at least one of $\vec{xy}$ and $\vec{yx}$ is an edge of $\vec{G}\}, \mathscr{G}_{k\text{-out}} = \phi(\vec{G})$: $\vec{G} \in \vec{\mathscr{G}}_{k\text{-out}}$. The probability of a graph H in $\mathscr{G}_{k\text{-out}}$ is the probability of the set of graphs $\phi^{-1}(H)$ in $\vec{\mathscr{G}}_{k\text{-out}}$. Note that every $G_{k\text{-out}}$ has at most kn edges but every vertex of it has degree at least k. As we shall see in Chapter 3, this is in sharp contrast with the graphs G_M, for a.e. G_M has isolated vertices unless M is not much smaller than $(n/2)\log n$.

The model $\mathscr{G}(n; p_1, p_2, \ldots, p_k)$ is also obtained by identifying edges obtained in different ways. The graphs of this model are obtained by first selecting edges of colour 1 with probability p_1, then edges of colour 2 with probability p_2, etc. This gives us a multigraph (graph with multiple edges) whose edges are coloured $1, 2, \ldots, k$. To obtain our r.g. we just forget the colours of the edges and identify multiple edges. Of course, the model we get in this way is nothing but $\mathscr{G}(n, p)$, where $p = 1 - \prod_1^k (1 - p_i)$. However, by selecting the edges in several stages we can work with independent graphs: the graph formed by the edges colour i is independent of the graph formed by the edges of colour j, $j \neq i$. This model was used in the second part of the proof of Theorem 2.1.

There are many other models of random graphs. By giving all graphs in a finite set the same probability we obtain a probability space. In this way we have random k-regular graphs, random trees, random forests, random planar graphs, etc. Of these, only random regular graphs will be investigated in detail. As regular graphs are not easily generated, we devote an entire section (§4) to the introduction of random regular graphs.

Let us conclude this section with two models which, in some sense, are refinements of $\mathscr{G}(n, p)$ and $\mathscr{G}(n, M)$.

Let $0 < p < 1$ be fixed. The model $\mathscr{G}(\mathbb{N}, p)$, studied in Bollobás and Erdös (1976), consists of all graphs with vertex set $\mathbb{N}$, whose edges are chosen independently and with probability p. In other words a r.g. $G \in \mathscr{G}(\mathbb{N}, p)$ is a collection $(X_{ij}) = \{X_{ij} : 1 \le i < j\}$ of independent r.vs with $P(X_{ij} = 1) = p$ and $P(X_{ij} = 0) = q$: a pair ij is an edge of G iff $X_{ij} = 1$. Clearly $G_n = G[1, 2, \ldots, n]$, the subgraph of G spanned by $1, 2, \ldots, n$, is exactly a r.g. G_p on $V = \{1, 2, \ldots, n\}$.

Note that the space $\mathscr{G}(\mathbb{N}, p)$ has uncountably many points and depends only on p. The definition of 'almost every' is then just the standard definition in measure theory: *almost every* (a.e.) $G \in \mathscr{G}(\mathbb{N}, p)$ is said to have a property Q if $P(G \text{ has } Q) = 1$. Note that if a.e. G is such that for some $n(G) \in \mathbb{N}$ every $G_n, n \geq n(G)$, has property Q, then a.e. G_p has Q. On the other hand, the converse is far from being true. Thus assertions concerning a.e. graph in $\mathscr{G}(\mathbb{N}, p)$ tend to be stronger than assertions about a.e. G_p.

A *random graph process on* $V = \{1, 2, \ldots, n\}$, or simply a *graph process*, is a Markov chain $\widetilde{G} = (G_t)_0^\infty$, whose states are graphs on V. The process starts with the empty graph and for $1 \leq t \leq \binom{n}{2}$ the graph G_t is obtained from G_{t-1} by the addition of an edge, all new edges being equiprobable. Then G_t has exactly t edges, so for $t = \binom{n}{2}$ we have $G_t = K^n$. For $t > \binom{n}{2}$ we take $G_t = K^n$ as well.

A slightly different approach to random graph processes goes as follows. A graph process is a sequence $(G_t)_t^N = 0$ such that

(i) each G_t is a graph on V,
(ii) G_t has t edges for $t = 0, 1, \ldots, N$ and
(iii) $G_0 \subset G_1 \subset \ldots$.

Let $\widetilde{\mathscr{G}}$ be the set of all $N!$ graph processes. Turn $\widetilde{\mathscr{G}}$ into a probability space by giving all members of it the same probability and write $\widetilde{G}$ for random elements of $\widetilde{\mathscr{G}}$. The term 'almost every' is used in its familiar meaning: *almost every* graph process $\widetilde{G}$ is said to have property Q if the probability that $\widetilde{G}$ has Q tends to 1 as $n \to \infty$. Furthermore, we call G_t *the state* of the process $\widetilde{G} = (G_t)_0^N$ at time t.

The map $\widetilde{\mathscr{G}} \to \mathscr{G}(n, M)$, defined by $\widetilde{G} = (G_t)_0^N \to G_M$, is measure preserving so the set of graphs obtained at time $t = M$ can be identified with $\mathscr{G}(n, M)$. Hence no contradiction will arise from the fact that G_M stands for two different objects: a random graph from $\mathscr{G}(n, M)$ and the state of a graph process $\widetilde{G}$ at time M.

Intuitively, $\widetilde{G}$ is an organism which develops by acquiring more and more edges in a random fashion. One of the main aims of the theory of random graphs is to determine when a given property is likely to appear. As mentioned earlier, Erdős and Rényi were the first to show that most monotone properties appear rather suddenly. In rather vague terms, a threshold function is a critical time, before which the property is unlikely and after which it is very likely.

Suppose Q is a monotone property of graphs. The time τ at which Q appears is the *hitting time* of Q:

$$\tau = \tau_Q = \tau_Q(\widetilde{G}) = \min\{t \geq 0 : G_t \text{ has } Q\}.$$

Thus $M^*(n)$ is the threshold function of Q if whenever $\omega(n) \to \infty$, the hitting time is almost surely between $M^*(n)/\omega(n)$ and $M^*(n)\omega(n)$:

$$P\{M^*(n)/\omega(n) < \tau_Q(n) < M^*(n)\omega(n)\} \longrightarrow 1.$$

Hitting times enable us to relate properties of r.gs more precisely than the model $\mathcal{G}(n, M)$. For example, let Q_1 be the property of having no isolated vertex and Q_2 the property of being connected. Then $\tau_{Q_1}(\widetilde{G}) \leq \tau_{Q_2}(\widetilde{G})$, i.e. Q_2 cannot occur before Q_1 since a connected graph (of order at least 2) has no isolated vertex. As we shall see in Chapter 7, a.e. G_M has Q_i ($i = 1$ or 2) iff $M = (n/2)\{\log n + \omega(n)\}$, where $\omega(n) \to \infty$. Thus a.e. G_M is connected iff a.e. G_M has minimum degree at least 1. However, considerably more is true. The main obstruction to connectedness is the existence of an isolated vertex: a.e. graph process $\widetilde{G}$ is such that $\tau_{Q_1} = \tau_{Q_2}$, i.e. the first edge incident with the last isolated vertex also makes the graph connected.

2.2 Properties of Almost All Graphs

If M is neither too small nor too close to N then for every fixed graph H a.e. G_M has the rather pleasant property that the graph H can be embedded in it vertex by vertex. To be more precise, given graphs $F \subset H$, in a large range of M a.e. G_M is such that if G_M has an induced subgraph isomorphic to F then G_M also has an induced subgraph H^* such that $H^* \supset F^*, H^* \simeq H$ and the isomorphism $H^* \simeq H$ is an extension of $F^* \simeq F$. This is an immediate consequence of the following result.

Let us say that a graph G has *property* P_k if whenever W_1, W_2 are disjoint sets of at most k vertices each then there is a vertex $z \in V(G) - W_1 \cup W_2$ joined to every vertex in W_1 and none in W_2. Clearly P_{k+1} implies P_k.

Theorem 2.5 *Suppose $M = M(n)$ and $p = p(n)$ are such that for every $\varepsilon > 0$ we have*

$$Mn^{-2+\varepsilon} \longrightarrow \infty \text{ and } (N - M)n^{-2+\varepsilon} \longrightarrow \infty, \tag{2.1}$$

$$pn^{\varepsilon} \longrightarrow \infty \text{ and } (1 - p)n^{\varepsilon} \to \infty. \tag{2.2}$$

Then for every fixed $k \in \mathbb{N}$ a.e. G_M has P_k and a.e. G_p has P_k.

Proof Although P_k is not a convex property, we can get away with considering only the model $\mathcal{G}(n, p)$. Indeed, $M(n)$ satisfies (2.1) if and only if $p = M/N$ satisfies (2.2). Therefore by Theorem 2.2(iii) it suffices to show that if p satisfies (2.2) then $P_p(\rceil P_k) = o(n^{-1})$. This is true with plenty to spare.

Note that if $|G| > 2k$, then G has P_k if and only if a vertex z can be found for all pairs W_1, W_2 with $|W_1| = |W_2| = k$.

Suppose p satisfies (2.2). Write $P_p(W_1, W_2; z)$ for the probability that a fixed vertex $z \notin W_1 \cup W_2$ will not do for a given pair $(W_1, W_2), |W_1| = |W_2| = k$, and let $P_p(W_1, W_2)$ be the probability that no vertex z will do for (W_1, W_2). Then

$$\begin{aligned} P(W_1, W_2; z) &= 1 - p^k q^k, \\ P(W_1, W_2) &= (1 - p^k q^k)^{n-2k} \leq \exp\{-(n-2k)p^k q^k\} \leq \exp(-n^{1/2}) \end{aligned}$$

and so

$$P_p(\rceil P_k) \leq n^{2k} \exp(-n^{1/2}) = o(n^{-1}). \qquad \square$$

The metatheory of graph theory could hardly be simpler. In the theory of graphs there is only one relation, adjacency, satisfying the condition $xRy \to yRx$ and $\rceil xRx$, where xRy means that the vertex x is adjacent to the vertex y. Consequently, first order sentences (sentences involving $=, \vee, \wedge, \exists, \forall, \rceil, \to$ and R) are particularly simple. As is shown by the next result, which is a slight extension of a theorem of Fagin (1976), for a large range of M and p first-order sentences are not too interesting when applied to graphs in $\mathcal{G}(n, M)$ and $\mathcal{G}(n, p)$.

Theorem 2.6 *Suppose M and p satisfy (2.1) and (2.2), and Q is a property of graphs given by a first-order sentence. Then either Q holds for a.e. graph in $\mathcal{G}(n, M)$ and $\mathcal{G}(n, p)$ or it fails for a.e. graph in $\mathcal{G}(n, M)$ and $\mathcal{G}(n, p)$.*

Proof We claim that there is a unique graph (up to isomorphism) with a countable vertex set which has P_k for every k. An example of such a graph is $G_0 = (\mathbb{N}, E)$ with $E = \{ij : i < j, p_i | j\}$, where $p_1, p_2, \ldots$ is an enumeration of the primes. The uniqueness follows from a standard 'back and forth' argument. Suppose G and H have P_k for every k, $V(G) = \{g_1, g_2, \ldots\}$ and $V(H) = \{h_1, h_2, \ldots\}$. Define 'partial isomorphisms' $\sigma_n : \{g_{i_1}, \ldots, g_{i_n}\} \to \{h_{i_1}, \ldots, h_{i_n}\}$ inductively as follows. Let $g_{i_1} = g_1$ and $h_{i_1} = h_1$. If $n \geq 2$ is even, pick i_{n+1} to be the least $i \geq 1$ not in $\{i_1, \ldots, i_n\}$. Since H has P_n there is a vertex $h_{j_{n+1}} \notin \{h_{j_1}, \ldots, h_{j_n}\}$ such that for all $s, 1 \leq s \leq n$, we have $h_{j_{n+1}} R h_{j_s}$ iff $g_{i_{n+1}} R g_{i_s}$. If $n \geq 2$ is odd, reverse the role of G and H above. The union of the partial isomorphisms is clearly an isomorphism between G and H.

Since the theory of graphs together with all P_k's has no finite models and all countable models are isomorphic, the theory is complete (see Vaught, 1954; Gaifman, 1964). Hence if Q is any first-order sentence then either Q or $\rceil Q$ is implied by some set of P_k's and so by some P_k, say by P_{k_0}. In particular, either $P(G \text{ has } Q) \geq P(G \text{ has } P_{k_0})$ or $P(G \text{ has } \rceil Q) \geq P(G \text{ has } P_{k_0})$. By Theorem 2.5, a.e. graph in our range has P_{k_0}, so the proof is complete. □

For monotone properties Theorem 2.6 can be restated in terms of hitting times as follows: if Q is a monotone property given by a first-order sentence then for almost no graph process Q does $M = \tau_Q(\widetilde{G})$ satisfy (2.1). The moral of Theorem 2.6 is that if we wish to study a property of random graphs given by a first-order sentence, then we have to do it in models that do not satisfy (2.1) and (2.2). In fact, many graph properties one studies are not given by first-order sentences: 'G is bipartite', 'G has chromatic number at least k', 'G is Hamiltonian', 'G contains $\lfloor n^{1/2} \rfloor$ vertices dominating all vertices', etc.

Theorems 2.5 and 2.6 are essentially best possible, as is shown by the following result.

Theorem 2.7 *Given $\varepsilon > 0$ choose $k \in \mathbb{N}$ such that $k\varepsilon > 1$ and define $p = p(n) > 0$ by*

$$2n^k e^{-p^k n} = k!$$

Let Q be the property that for every set of k vertices there is a vertex joined to all of them. Then $0 < p < \varepsilon$ if n is sufficiently large and

$$\frac{1}{2} \leq \underline{\lim} P(G_p \text{ has } Q) \leq \overline{\lim} P(G_p \text{ has } Q) \leq \frac{5}{8}.$$

Proof By definition

$$p \sim \left(\frac{k \log n}{n} \right)^{1/k},$$

so $p < \varepsilon$ if n is sufficiently large.

Denote by $X = X(G_p)$ the number of k-tuples of vertices of G_p for which no vertex can be found which is joined to all of them. Then

$$E(X) = \binom{n}{k} (1 - p^k)^{n-k} \sim n^k \mathrm{e}^{-p^k n}/k! \longrightarrow \frac{1}{2},$$

since the probability that a vertex x will not do for a k-tuple W is

$$P\{xy \in E(G_p) \text{ for some } y \in W\} = 1 - P\{xy \notin E(G_p) \text{ for all } y \in W\} = 1 - p^k.$$

Now let us calculate $E_2(X)$. There are $\binom{n}{k}\binom{k}{l}\binom{n-k}{k-l}$ ordered pairs of k-tuples sharing l vertices, $l = 0, 1, \ldots, k-1$. The probability that a vertex x is not good for either of these k-tuples is

$$1 - p^l + p^l(1 - p^{k-l})^2 = 1 - 2p^k + p^{2k-l}.$$

For $l = 0$ this is $(1 - p^k)^2$ and for $l \geq 1$ this probability is at most

$$(1 - p^k)^2(1 + p^{2k-l}).$$

Hence

$$\begin{aligned} E_2(X) &\leq \binom{n}{k}\binom{n}{k}(1 - p^k)^{2n-4k} \\ &\quad + \sum_{l=1}^{k-1}\binom{n}{k}\binom{k}{l}\binom{n-k}{k-l}(1 - p^k)^{2n-4k}(1 + p^{2k-l})^{n-2k} \\ &= E(X)^2 + \sum_{l=1}^{k} O(n^{2k-l}e^{-2p^k n}), \end{aligned}$$

since

$$(1 + p^{2k-l})^n \leq e^{p^{k+1}n} = 1 + \{(\log n)^{k+1}/n\}^{1/k}.$$

Consequently,

$$E_2(X) = E(X)^2\{1 + O(1/n)\} \longrightarrow \tfrac{1}{4}.$$

By Corollary 1.11 (or the first part of Theorem 1.16) and the trivial inequality $P(X = 0) \geq 1 - E(X)$, we have

$$\tfrac{1}{2} \sim 1 - E(X) \leq P(X = 0) \leq 1 - E(X) + \tfrac{1}{2}E_2(X) \sim \tfrac{5}{8}.$$

This proves our theorem, since G_p has Q iff $X(G_p) = 0$. □

The necessity of conditions (2.1) and (2.2) in Theorem 2.5 is also an easy consequence of some results in Chapter 4 (see Ex. 4 of Chapter 4).

2.3 Large Subsets of Vertices

The main reason why random graphs so often provide examples of graphs which are not easily constructed is that in a loose sense a random graph is an almost regular graph with surprisingly strong homogeneity properties. To be a little more precise, in large ranges of p and M most r.gs G_p and G_M are such that their vertices have about the same degrees and all not too small sets of vertices behave in a very similar way.

This similarity in the behaviour of sets of vertices will be discussed in this section, and the next entire chapter will be devoted to the degree sequence.

Consider a graph $G \in \mathscr{G}_p$. For brevity we write $e(U) = e(G[U])$ for the number of edges of G in the subgraph $G[U]$ spanned by a set $U \subset V$, that is for the number of edges joining vertices of U. Similarly we write $e(U, W)$ for the number of $U - W$ edges, where U and W are disjoint sets of vertices. Clearly the expected value of $e(U)$ is $p\binom{u}{2}$ and the expected value of $e(U, W)$ is puw, where u and w denote the number of vertices in U and W, respectively. An important aspect of the similarity of not too small sets of vertices is that almost every graph is such that $e(U)$ is close to $p\binom{u}{2}$ and $e(U, W)$ is close to puw whenever U and W are sufficiently large.

Theorem 2.8 *Let $0 < p = p(n) \le \frac{1}{2}$. Then a.e. $G \in \mathscr{G}_p$ is such that if U is any set of $u > (252/p)\log n$ vertices, then*

$$\left| e(U) - p\binom{u}{2} \right| < \left(\frac{7p\log n}{u}\right)^{1/2} \binom{u}{2}. \tag{2.3}$$

Proof Let U be a fixed set of $u > (252/p)\log n$ vertices. Then $e(U)$ has binomial distribution with parameters $\binom{u}{2}$ and p. Put $\varepsilon = \{(7\log n)/pu\}^{1/2}$. Clearly by assumption $\varepsilon < 1/6$ and

$$p\binom{u}{2} > \varepsilon^{-2} = \frac{pu}{7\log n}.$$

Consequently by Corollary 1.4 we have, for sufficiently large n,

$$P\left(\left| e(U) - p\binom{u}{2} \right| \ge \varepsilon p\binom{u}{2}\right)\binom{u}{2} < 2e^{-\varepsilon^2 p\binom{u}{2}/3q} < n^{-u-2}. \tag{2.4}$$

The second inequality in (4) holds because, if n is large enough,

$$\frac{7}{6q} > \frac{u+3}{u-1}.$$

Since there are $\binom{n}{u} \le n^u/u!$ sets of u vertices, the probability that some set U with $u > u_0 = \lfloor (252/p)\log n \rfloor$ elements violates the inequality of the theorem is at most

$$\sum_{u > u_0} \binom{n}{u} n^{-u-2} \le \frac{1}{n}. \qquad \square$$

As inequality (2.3) defines a convex property, by Theorem 2.2 the result above holds for $\mathcal{G}_M$ as well, where $M = p\binom{n}{2}$.

Note that Theorem 2.8 concerns only graphs of fairly many edges, for (2.3) holds vacuously unless $u \le n$ and so $p > (144/n)\log n, pn^2/2 > 72n\log n$. In fact, large sets of graphs of much smaller size also behave rather regularly. We state the result for $\mathcal{G}_M$.

Theorem 2.9 *Suppose $M = M(n) \le n^2/4$ and $u_0 = u_0(n) \le n/2$ satisfy*

$$Mu_0/\{n^2\log(n/u_0)\} \longrightarrow \infty.$$

Then for every $\varepsilon > 0$ a.e. G_M is such that every set U of $u > u_0$ vertices satisfies

$$|e(U) - M(u/n)^2| < \varepsilon M(u/n)^2. \tag{2.5}$$

Proof For a fixed set U of u vertices $e(U)$ has hypergeometric distribution with parameters $\binom{n}{2}, \binom{u}{2}$ and M. By inequality (2.12) of Chapter 1 we could approximate this distribution by $b\left\{k; M, \binom{u}{2}\binom{n}{2}\right\}$ and then could apply Theorem 1.7 to prove (2.5). However, it is easier to deal with the model $\mathcal{G}_p$ and then rely on Theorem 2.2 to translate the result back to $\mathcal{G}_M$. Inequality (2.5) defines a convex property, so by Theorem 2.2 it suffices to prove (2.5) for the model $\mathcal{G}_p$, where $p = M/\binom{n}{2}$.

By assumption, $pu_0^2 \to \infty$ and we may assume that $\varepsilon < 1/10$. Then by Theorem 1.7 for every fixed set $U, |U| = u > u_0$, we have

$$P\left(\left|e(U) - p\binom{u}{2}\right| > \frac{\varepsilon}{2}p\binom{u}{2}\right) < e^{-\varepsilon^2 pu^2/7}. \tag{2.6}$$

We have $\binom{n}{u} \le (en/u)^u$ choices for U, so the probability that (2.6) fails for some set $U, |U| > u_0$, is at most

$$\sum_{u>u_0} \exp[u\{-\varepsilon^2 pu/7 + 1 + \log(n/u)\}]$$
$$\le \sum_{u>u_0} \exp[u\{-\varepsilon^2 pu_0/7 + 1 + \log(n/u_0)\}] = o(1),$$

for

$$-\varepsilon^2 pu_0/7 + \log(n/u_0) \le -(\varepsilon^2/7)Mu_0/n^2 + \log(n/u_0) \longrightarrow -\infty.$$

This proves our theorem, since

$$\left|e(U) - p\binom{u}{2}\right| \le \frac{\varepsilon}{2}p\binom{u}{2}$$

implies (2.5). $\square$

Corollary 2.10 *If $M/n \to \infty$ and $\varepsilon > 0$ then a.e. G_M is such that*

$$|e(U) - Mu^2/n^2| < \varepsilon Mu^2/n^2$$

for every set U of at least εn vertices.

The corresponding results concerning $e(U, W)$ can be proved analogously to Theorems 2.8 and 2.9. The simple proofs are left to the reader.

Theorem 2.11 *Let $0 < p = p(n) \le 1/2$. Then a.e. G_p is such that*

$$|e(U, W) - puw| < \left(\frac{7p\log n}{u}\right)^{1/2} uw,$$

whenever U and W are disjoint sets of vertices satisfying $(252/p)\log n < u = |U| \le w = |W|$.

Theorem 2.12 *Suppose M and u_0 are as in Theorem 2.9. Then for every $\varepsilon > 0$ a.e. G_M is such that*

$$|e(U, W) - 2Muw/n^2| < \varepsilon Muw/n^2,$$

whenever U and W are disjoint sets of vertices satisfying $u_0 < u = |U| \le w = |W|$.

Corollary 2.13 *If $M/n \to \infty$ and $\varepsilon > 0$ then a.e. G_M is such that*

$$|e(U, W) - 2Muw/n^2| < \varepsilon Muw/n^2,$$

whenever U and W are disjoint sets of vertices satisfying $\varepsilon n \le u = |U| \le w = |W|$.

The next two results, essentially from Bollobás and Thomason (1982), are more technical. They also express the fact that in most graphs all large sets of vertices behave similarly.

Theorem 2.14 *Let $0 < \varepsilon < \frac{1}{6}$ be a positive constant, $p = p(n) \le \frac{1}{2}$ and suppose $w_0 = w_0(n) \ge \lceil 6\log n/(\varepsilon^2 p)\rceil$. Then a.e. G_p is such that if $W \subset V$ and $|W| = w \ge w_0$ then*

$$Z_W = \{z \in V - W : \| \Gamma(z) \cap W| - pw| \ge \varepsilon pw\}$$

satisfies

$$|Z_W| \le 12\log n/\{\varepsilon^2 p\}.$$

Proof We may assume that $w_0 \le n$ and so $pn \to \infty$. For fixed $w \ge w_0$, W and $x \in V - W$ Corollary 1.4 implies that

$$P(x \in Z_W) \le 2e^{-\eta p w},$$

where $\eta = \varepsilon^2/3$. Hence

$$P(|Z_W| \ge z) \le (2n)^z e^{-\eta p w z} \le e^{-\eta p w z/3}.$$

Therefore, if $z \ge 4(\log n)/\eta p$, the probability that some set W of order w exists which fails to satisfy the conclusions of the theorem is at most

$$n^w e^{-\eta p w z/3} \le n^{-w/3}.$$

Thus a graph fails the conclusions of the theorem with probability at most $\sum_{w \ge w_0} n^{-w/3} = o(1)$. □

Theorem 2.15 *Suppose $\delta = \delta(n)$ and $C = C(n)$ satisfy $\delta pn \ge 3 \log n. C \ge 3 \log(e/\delta)$ and $C\delta n \to \infty$. Then a.e. G_p is such that for every $U \subset V, |U| = u = \lceil C/p \rceil$ the set*

$$T_u = \{x \in V - U : \Gamma(x) \cap U = \emptyset\}$$

has at most δ n elements.

Proof For fixed U and $x \in V - U$ we have

$$P(x \in T_u) = (1-p)^u \le e^{-pu} \le e^{-C}.$$

Hence, for a fixed set U,

$$P(|T_u| \ge \delta n) \le \binom{n}{\delta n} e^{-C\delta n} \le (e/\delta)^{\delta n} e^{-C\delta n} \le e^{-2C\delta n/3}.$$

Finally, since there are at most $n^{\lceil C/p \rceil}$ choices for U,

$$P(|T_u| \ge \delta n \text{ for some } U) \le n^{\lceil C/p \rceil} e^{-2C\delta n/3}$$
$$\le \exp\left(\frac{4C}{3p} \log n - \frac{2}{3} C\delta n\right) \le \exp\left\{-\frac{1}{6} C\delta n\right\} = o(1). \qquad \square$$

2.4 Random Regular Graphs

Suppose the natural numbers n and $r = r(n)$ are such that $3 \le r < n$ and $rn = 2m$ is even. Denote by $\mathcal{G}(\eta, r\text{-reg}) = \mathcal{G}_{r\text{-reg}}$ the set of r-regular graphs. By our assumption on r, the set $\mathcal{G}_{r\text{-reg}}$ is not empty. We turn $\mathcal{G}_{r\text{-reg}}$ into a probability space by giving all elements the same probability, and call an element of this probability space, $\mathcal{G}_{r\text{-reg}}$, a *random r-regular graph.*

Then every graph invariant becomes a r.v. on $\mathscr{G}_{r\text{-reg}}$ and the expression 'a.e. r-regular graph has property Q' needs no explanation.

Before getting down to the study of r-regular graphs, a basic question has to be answered. About how many r-regular graphs of order n are there? In other words, what is the asymptotic magnitude of $L_r = L_r(n) = |\mathscr{G}_{r\text{-reg}}|$? The reason why the models $\mathscr{G}(n, M)$ and $\mathscr{G}(n, p)$ have rather long and distinguished histories while the model $\mathscr{G}_{\mathrm{r-reg}}$ is only a newcomer is exactly that such an asymptotic formula is not too easily come by.

Read (1959, 1960) obtained an exact formula for L_r, based on the enumeration theorem of Pólya (1937) [see Bollobás (1979*a*, chapter 8) for a more recent presentation of it]. Unfortunately, this formula is not easily penetrated. In particular, it seems that only for $r \leq 3$ can it be used to find the asymptotic value of L_r (see Harary and Palmer, 1973, p. 175). Bender and Canfield (1978) gave an asymptotic formula for L_r and, more generally, for the number of labelled graphs with given degree sequences. Earlier, Erdős and Kaplansky (1946), O'Neil (1969), Békéssy, Békéssy and Komlós (1972) and Bender (1974*b*) had studied similar questions concerning matrices and bipartite graphs.

Bollobás (1979*b*, 1980*b*) gave a simple model for the set of labelled regular graphs, which not only implies a proof of the asymptotic formula, but also makes the study of random regular graphs fairly accessible. The aim of this section is to prove the asymptotic formula via this model. The key result is the following.

Theorem 2.16 *Suppose Δ is a fixed natural number,*

$$\Delta \geq d_1 \geq d_2 \geq \ldots \geq d_n \geq 1, \sum_i^n d_i = 2m$$

is even, $2m - n \to \infty$ and G_0 is a graph of maximum degree at most Δ with vertex set $V = \{1, 2, \ldots, n\}$. Denote by $\mathscr{L}(\mathbf{d}; G_0)$ the set of graphs with vertex set V which do not share an edge with G_0 and whose degree sequence is exactly $(d_i)_1^n : d(i) = d_i, i = 1, \ldots, n$. Then

$$|\mathscr{L}(\mathbf{d}; G_0)| \sim e^{-\lambda/2-\lambda^2/4-\mu}(2m)_m \Big/ \left(2^m \prod_{i=1}^n d_i!\right),$$

where

$$\lambda = \frac{1}{m} \sum_{i=1}^n \binom{d_i}{2} \quad \text{and} \quad \mu = \frac{1}{2m} \sum_{ij \in E(G_0)} d_i d_j.$$

Proof We shall represent the graphs in $\mathscr{L}(\mathbf{d}; G_0)$ as images of so called configurations. Let $W = \bigcup_{j=1}^{n} W_j$ be a fixed set of $2m = \sum_{j=1}^{n} d_j$ labelled vertices, where $|W_j| = d_j$. A *configuration* F is a partition of W into m pairs of vertices, called *edges* of F. Let Φ be the *set of configurations.* Clearly

$$|\Phi| = N(m) = (2m)_m 2^{-m} = (2m-1)!!$$

Given a configuration $F \in \Phi$, let $\phi(F)$ be the graph with vertex set V in which ij is an edge iff F has a pair with one element in W_i and the other in W_j. Note that every $G \in \mathscr{L}(\mathbf{d}; G_0)$ is of the form $G = \phi(F)$ for exactly $\prod_{j=1}^{n} d_j!$ configurations. However, not every $\phi(F)$ belongs to $\mathscr{L}(\mathbf{d}; G_0)$ since $\phi(F)$ may share an edge with G_0 and the degree of vertex i in $\phi(F)$ may be smaller than d_i, either because F contains an edge entirely in W_i or because it contains two edges joining W_i to W_j.

In order to identify the set $\{\phi^{-1}(G) : G \in \mathscr{L}(\mathbf{d}; G_0)\}$, we consider the k-cycles of a configuration. For $k \in \mathbb{N}$ a *k-cycle* of a configuration F is a set of k edges, say $\{e_1, e_2, \ldots, e_k\}$ such that for some k distinct groups $W_{j_1}, W_{j_2}, \ldots, W_{j_k}$ the edge e_i joins W_{j_i} to $W_{j_{i+1}}$, where $W_{j_{k+1}} \equiv W_{j_1}$. A 1-cycle is said to be a *loop* and a 2-cycle is a *coupling.* With a slight abuse of terminology an edge of $F \in \Phi$ joining classes W_i, W_j with $ij \in E(G_0)$ is said to be a *0-cycle.* Then clearly $\phi(F) \in \mathscr{L}(\mathbf{d}; G_0)$ iff $X_0(F) = X_1(F) = X_2(F) = 0$. Hence, if we turn Φ into a probability space by giving all configurations the same probability, then

$$\mathscr{L}(\mathbf{d}; G_0) = P(X_0 + X_1 + X_2 = 0) N(m) \Big/ \prod_{i=1}^{n} d_i!$$

Therefore our theorem is equivalent to

$$P(X_0 + X_1 + X_2 = 0) \sim \mathrm{e}^{-\lambda/2 - \lambda^2/4 - \mu}. \tag{2.7}$$

We shall prove (2.7) by showing that for every fixed k the distribution of $(X_0, X_1, \ldots, X_k)$ is close to the distribution of $(Y_0, Y_1, \ldots, Y_k)$, where the Y_i's are independent Poisson r.vs with $E(Y_0) = \mu$ and $E(Y_i) = \lambda^i/2i, i = 1, \ldots, k$. Then $Y_0 + Y_1 + Y_2$ is a $P(\lambda/2 + \lambda^2/4 + \mu)$ r.v., so

$$P(X_0 + X_1 + X_2 = 0) \sim P(Y_0 + Y_1 + Y_2 = 0) = \mathrm{e}^{-\lambda/2 - \lambda^2/4 - \mu},$$

which is exactly (2.7).

In order to show that asymptotically the distribution is a Poisson distribution, we look at joint factorial moments. For $\sigma \subset V$ put

$$w(\sigma) = \prod_{i \in \sigma} d_i(d_i - 1).$$

Let n_2 denote the number of d_i's greater than 1, i.e. set $n_2 = \max\{l : l \leq n, d_l \geq 2\}$. Since $2m - n \to \infty$, we have $n_2 \to \infty$. Clearly

$$\sum_{|\sigma|=k} w(\sigma) \geq \binom{n_2}{k} 2^k$$

and a trite calculation gives

$$\sum_{|\sigma|=k} w(\sigma) \sim \left\{ \sum_{i=1}^{n} d_i(d_i - 1) \right\}^k / k! \tag{2.8}$$

for every $k \geq 1$.

For $k = 1, 2, \ldots$ set

$$C_k(\mathbf{d}) = \frac{1}{2}(k-1)! \sum_{|\sigma|=k} w(\sigma). \tag{2.9}$$

Then by (2.8)

$$\underline{\lim}_{n\to\infty} C_k(\mathbf{d})/n_2^k > 0.$$

Furthermore, put

$$C_0(\mathbf{d}) = \sum_{\substack{i>j \\ ij \in E(G_0)}} d_i d_j. \tag{2.10}$$

Clearly there are exactly $C_k(\mathbf{d})$ sets of pairs of vertices that can be k-cycles of configurations.

Let us show that if the sequence $\mathbf{d}$ is decreased a little then $C_k(\mathbf{d})$ does not decrease too much. More precisely, given a non-negative integer t, denote by $\mathbf{d} - t$ the sequence $d_{t+1}, d_{t+2}, \ldots, d_n$ and define $C_k(\mathbf{d} - t)$ by (2.9) and (2.10). Very crudely indeed, for all $k \geq 1$ and $1 \leq t \leq n$ we have

$$C_k(\mathbf{d}) - C_k(\mathbf{d} - t) \leq 2^t n_2^{k-1} \Delta^{2k} k!$$

since the edges of a k-cycle join groups of size at least 2. Consequently

$$C_k(\mathbf{d} - t) \geq \{1 + o(1)\} C_k(\mathbf{d}), \tag{2.11}$$

whenever k and t are fixed.

Similarly one can show that

$$C_0(\mathbf{d} - t) \geq \{1 + o(1)\} C_0(\mathbf{d}) \tag{2.12}$$

for every fixed t, provided $C_0(\mathbf{d}) \to \infty$, that is $e(G_0) \to \infty$.

The probability that a configuration contains a given fixed set of l vertex disjoint (independent) edges is

$$N(m-l)/N(m) = 1/\{(2m-1)(2m-3)\dots(2m-2l+1)\}.$$

If l is fixed, this probability is

$$\{1+o(1)\}(2m)^{-l}. \tag{2.13}$$

Now we can easily calculate the joint factorial moments of the X_i's. Note first that by (2.8), (2.9) and (2.13) we have for every $i \geq 1$

$$E_i = E(X_i) \sim C_i(\mathbf{d})(2m)^{-i} \sim \lambda^i/(2i) = \lambda_i \tag{2.14}$$

and by (2.10) and (2.13)

$$E_0 = E(X_0) = C_0(\mathbf{d})/(2m-1) \sim \mu = \lambda_0. \tag{2.15}$$

If $\lambda_0 = \mu = o(1)$ then $P(X_0 = 0) = 1 - o(1)$ and it suffices to consider the joint factorial moments of $X_1, X_2, \dots$. Hence we may assume that λ_0 is bounded away from 0.

Denote by $\mathscr{C}(r_0, r_1, \dots, r_k)$ the set of ordered r-tuples, $r = \sum_{i=0}^k r_i$, whose first r_0 elements are 0-cycles, the next r_1 elements are 1-cycles, etc. Let $\mathscr{C}'(r_0, r_1, \dots, r_k)$ be the subset of $\mathscr{C}(r_0, r_1, \dots, r_k)$ consisting of r-tuples for which no W_i contains endvertices of edges belonging to distinct cycles, and set $\mathscr{C}'' = \mathscr{C} \backslash \mathscr{C}'$. Finally, for a configuration $F \in \Phi$, denote by $Y(r_0, r_1, \dots, r_k)(F)$ the number of elements of $\mathscr{C}$ in F, and define the r.vs Y' and Y'' analogously. Then clearly

$$E\{(X_0)_{r_0}(X_1)_{r_1} \dots (X_k)_{r_k}\} = E\{Y(r_0, r_1, \dots, r_k)\} \tag{2.16}$$

and

$$E(Y) = E(Y') + E(Y''). \tag{2.17}$$

Furthermore,

$$\prod_{i=0}^k C_i(\mathbf{d}-t)^{r_i} \leq Y'(r_0, r_1, \dots, r_k) \leq \prod_{i=0}^k C_i(\mathbf{d})^{r_i},$$

where $t = 2r_0 + \sum_1^k ir_i$. Consequently by (2.11), (2.12), (2.13), (2.14) and (2.15) we have

$$E\{Y'(r_0, r_1, \dots, r_k)\} \sim \{C_0(\mathbf{d})^{r_0}/(2m)^{r_0}\} \prod_{i=1}^k \{C_i(\mathbf{d})^{r_i}/(2m)^{ir_i}\} \sim \prod_{i=0}^k \lambda_i^{r_i}. \tag{2.18}$$

On the other hand, the cycles of an r-tuple counted by $Y''(r_0, r_1, \dots, r_k)$

are such that for some $l \leq t = 2r_0 + \sum_{i=1}^{k} ir_i$ altogether they have at most l edges and these edges join at most $l-1$ groups W_i. Hence, very crudely indeed,

$$E\{Y''(r_0, r_1, \ldots, r_k)\} \leq \sum_{l=2}^{t} n^{l-1} 2^{\Delta t}(2m - 2t)^{-l} = O(n^{-1}).$$

Consequently, by (2.16), (2.17) and (2.18) we have

$$E\{(X_0)_{r_0}(X_1)_{r_1} \ldots (X_k)_{r_k}\} \sim \prod_{i=0}^{k} \lambda_i^{r_i}.$$

Therefore, by Theorem 1.20, $X_0, X_1, \ldots, X_k$ are asymptotically independent Poisson random variables with means $\lambda_0, \lambda_1, \ldots, \lambda_k$. In particular,

$$P(X_0 + X_1 + X_2 = 0) \sim \mathrm{e}^{-\lambda_0 - \lambda_1 - \lambda_2} = \mathrm{e}^{-\lambda/2 - \lambda^2/4 - \mu},$$

as required. □

Corollary 2.17 *Suppose $r \geq 2$ is fixed and rn is even. As before, denote by $L_r(n)$ the number of labelled r-regular graphs of order n. Then*

$$L_r(n) \sim e^{-(r^2-1)/4}(rn)!/\{(rn/2)!2^{rn/2}(r!)^n\} \sim \sqrt{2}e^{-(r^2-1)/4}\left(\frac{r^{r/2}}{e^{r/2}r!}\right)^n n^{rn/2}.$$

It is not hard to show that Δ in Theorem 2.16 need not be fixed. The same proof executed with slightly more care shows that the assertion holds for $\Delta \leq (\log n)^{1/2}/2$ (see Bollobás, 1980*b*; Bollobás and McKay, 1985).

The main significance of Theorem 2.16 and its proof is that when we study random regular graphs (whose degree does not grow too fast with n), instead of considering the set of regular graphs we are allowed to consider the set of configurations. In order to make this statement a little more precise, we restate some of the facts above for regular graphs.

Let $d_1 = d_2 = \ldots = d_n = r \geq 2$ and let Φ and ϕ be as in the proof of Theorem 2.16. Clearly,

$$\phi^{-1}(\mathscr{G}_{r\text{-reg}}) = \{F \in \Phi : X_1(F) = X_2(F) = 0\}$$

and $|\phi^{-1}(G)| = (r!)^n$ for every $G \in \mathscr{G}_{r\text{-reg}}$.

Given a set (property) $Q \subset \mathscr{G}_{r\text{-reg}}$, how can we estimate $P(Q)$? Find a set $Q^* \subset \Phi$ such that

$$Q^* \cap \phi^{-1}(\mathscr{G}_{r\text{-reg}}) = \phi^{-1}(Q).$$

Then, trivially,

$$\begin{aligned} P(Q) &= P(Q^*|X_1 = X_2 = 0) \\ &= 1 - \frac{P(\urcorner Q^* \text{ and } X_1 = X_2 = 0)}{P(X_1 = X_2 = 0)} \geq 1 - \frac{1 - P(Q^*)}{P(X_1 = X_2 = 0)}, \end{aligned}$$

giving the following simple consequence of the proof of Theorem 2.15.

Corollary 2.18 *If $r \geq 2$ is fixed and Q^* holds for a.e. configuration [i.e. $P(Q^*) \to 1$], then Q holds for a.e. r-regular graph.*

Although it does not really belong to this section, let us note another trivial consequence of the proof of Theorem 2.16 (see Bollobás, 1980*b*; Wormald, 1981*a*, *b*).

Corollary 2.19 *Let $r \geq 2$ and $m \geq 3$ be fixed natural numbers and denote by $Y_i = Y_i(G)$ the number of i-cycles in a graph $G \in \mathcal{G}_{r\text{-reg}}$. Then $Y_3, Y_4, \dots, Y_m$ are asymptotically independent Poisson random variables with means $\lambda_3, \lambda_4, \dots, \lambda_m$, where $\lambda_i = (r-1)^i/(2i)$.*

Proof The assertion is immediate from the fact that $X_1, X_2, \dots, X_m$ (random variables on Φ) are asymptotically independent Poisson random variables. □

It should be pointed out that $L_2(n)$, the number of 2-regular graphs of order n_1, is considerably easier to handle than $L_r(n), r \geq 3$. Here are some results from Comtet (1974, pp. 273–279). Clearly $L_2(1) = L_2(2) = 0$. A geometric interpretation of $L_2(n)$, due to Whitworth (1901, p. 269), leads to the recursive formula (Robinson, 1951, 1952; Carlitz, 1954, 1960)

$$L_2(n) = (n-1)L_2(n-1) + \binom{n-1}{2} L_2(n-3), n \geq 3,$$

where $L_2(0)$ is defined to be 1. From this one can deduce that the exponential generating function of $L_2(n)$ is

$$\sum_{n \geq 0} L_2(n)t^n/n! = \frac{1}{\sqrt{1-t}} \exp\left\{-\frac{t^2+2t}{4}\right\}.$$

In conclusion, let us say a few works about the considerably more difficult problem of estimating $L_r(n)$ when $r = r(n) \leq n/2$ grows with n fairly fast. McKay and Wormald (1990b, 1991) introduced powerful new methods and obtain several remarkable results. As in the case of small r, the problem of enumerating r-regular graphs does not really differ from that of graphs with given degree sequences. For $\mathbf{d} = (d_i)_1^n$, write $L(\mathbf{d})$, for the number of graphs on $[n]$ with $d(i) = d_i, i = 1, \ldots, n$. Thus, if G_0 is the empty graph then, with the notation of Theorem 2.16, $L(\mathbf{d}) = |\mathscr{L}(\mathbf{d}; G_0)|$.

McKay and Wormald (1990*b*) gave a complex integral formula for $L(\mathbf{D})$ under the assumption that for a sufficiently small $\varepsilon > 0$ and some $C > \frac{2}{3}$ we have $|d_i - d_j| < n^{1/2+\varepsilon}$ and $\min\{d_i, n - d_i\} \geq Cn/\log n$ for all i and j. However, the integral itself is rather difficult to estimate.

Using a different approach, McKay and Wormald (1991) gave an asymptotic formula for $L(\mathbf{d})$ under the assumption that $\Delta = \max d_i = o(m^{1/3})$, where $m = \frac{1}{2}\sum_1^n d_i$ is the number of edges. In particular, they proved the following substantial extension of Corollary 2.17: if $l \leq r = o(n^{1/2})$ and rn is even then

$$L_r(n) = \exp\left(-\frac{r^2-1}{4} - \frac{r^3}{12n} + O(r^2/n)\right) \frac{(rn)!}{(rn/2)!2^{rn/2}(r!)^n}.$$

McKay and Wormald (1990*a*) also gave an $O(r^3 n)$ algorithm to generate r-regular graphs uniformly when $r = o(n^{1/3})$.

Exercises

In Exercises 1–3 Q is a monotone increasing property.

2.1 Suppose $0 < M_1 < M_2 < N, P_{M_1}(Q) < 1$ and $P_{M_2}(Q) > 0$. Prove that $P_{M_1}(Q) < P_{M_2}(Q)$.

2.2 Suppose $0 < p_1 < p_2 < 1, p = (p_2 - p_1)/(1 - p_1)$ and

$$P_{p_2}(Q) = P_{p_1}(Q) + \{1 - P_{p_1}(Q)\}P_p(Q).$$

What is Q?

2.3 Let $M = \lceil pN \rceil$ and $pqN \to \infty$. Show that

$$P_p(Q) \geq P_M(Q)/2 + o(1)$$

and

$$P_M(Q) \geq 2P_p(Q) - 1 + o(1).$$

Prove that both inequalities are best possible.

2.4 Suppose Q is a convex property, $pqN \to \infty$ and almost no G_p has Q. Is it true that almost no graph in $\mathscr{G}(\lfloor pN \rfloor)$ has Q?

2.5 Let H_0 be a fixed graph and denote by $X(G)$ the number of subgraphs of G isomorphic to H_0. Show that if p_1, p_2 and M satisfy the conditions in Theorem 2.3, then the conclusion of the theorem holds.

[Let $\mathscr{H}$ be the collection of graphs isomorphic to H_0, with vertex set contained in V. For $H \in \mathscr{H}$ set

$$X_H(G) = \begin{cases} 1, & \text{if } H \subset G, \\ 0, & \text{otherwise.} \end{cases}$$

Note that $X = \sum_{H \in \mathscr{H}} X_H$ and $E_{p_i}(X_H) = E_{p_i}(X_{H'})$ and $E_M(X_H) = E_M(X_{H'})$ whenever $H, H' \in \mathscr{H}$. Apply Theorem 2.3 to $E_{p_i}(X_H)$ and $E_M(X_H)$.]

2.6 Imitate the proof of Theorem 2.8 to prove Theorem 2.11.

2.7 Let Ω_1 and Ω_2 be two models of r.gs. Suppose for all $\alpha_1, \alpha_2, \ldots, \alpha_s \in V^{(2)}$ we have

$$P_1(G \in \Omega_1 \text{ contains none of the edges } \alpha_1, \alpha_2, \ldots, \alpha_s)$$
$$\leq P_2(G \in \Omega_2 \text{ contains none of the edges } \alpha_1, \alpha_2, \ldots, \alpha_s).$$

(Intuitively, an element of Ω_1 is less likely to miss edges than an element of Ω_2, so an element of Ω_1 should have more edges than an element of Ω_2.) Let Q be a monotone (increasing) property. Does $P_1(Q) \geq P_2(Q)$ hold?

2.8 Let $k \geq 1$ and $\alpha_1, \alpha_2, \ldots, \alpha_s \in V^{(2)}, \alpha_i \neq \alpha_j$. Show that

$$P(G_{k\text{-out}} \text{ does not contain } \alpha_1) = \left(1 - \frac{k}{n-1}\right)^2 = q$$

and

$$P(G_{k\text{-out}} \text{ does not contain } \alpha_i, i = 1, \ldots, s) \leq q^s.$$

2.9 Consider the following Markov chain $(G_t)_1^\infty$ defined by Capobianco and Frank (1983). The states are finite graphs and the initial state G_1 is the trivial graph with one vertex. If G_{t-1} is complete then G_t is obtained from G_{t-1} by the addition of a vertex. If G_{t-1} is not complete then with probability p we add an edge to obtain G_t and with probability $q = 1 - p$ we add a vertex. Here $0 < p < 1$ is fixed, and all missing edges are equally likely to be added. [Note that $|G_t| + e(G_t) = t$ for every t.] Show that, with probability tending to 1, G_t has about pt vertices and qt edges.

2.10 Let $r \geq 3$ be fixed and let $u_0 = o(n)$. Prove that there is a function $\varepsilon = \varepsilon(n, u_0) \to 0$ such that if $G_0 = G_0(n)$ is a graph with vertex set $V = 1, \ldots, n\}$, size $u \leq u_0$ and maximum degree at most r, then

$$(1 - \varepsilon)\left(\frac{r}{en}\right)^u \leq P(G_{r\text{-reg}} \text{ contains } G_0) \leq (1 - \varepsilon)\left(\frac{r}{n}\right)^u.$$

2.11 For a fixed $k \in \mathbb{N}$ consider $\mathcal{G}_{k\text{-out}}$. Call an edge xy of a random graph a *double edge* if the original directed graph contains both $\vec{xy}$ and $\vec{yx}$. Use the technique of the proof of Theorem 2.16 to deduce that the number of double edges tends in distribution to $P(k^2/2)$. Show also that $E\{e(G_{k\text{-out}})\} = kn - k^2/2 + o(1)$.

2.12 Let r and s be fixed natural numbers. For $mr = ns = N$ denote by $B(m, n; r, s)$ the number of bipartite graphs with vertex sets $U = \{x_1, \dots, x_m\}$ and $W = \{y_1, \dots, y_n\}$ such that $d(x_i) = r$ and $d(y_i) = s$ for all i and j. Show that as $N \to \infty$

$$B(m, n; r, s) \sim \frac{N!}{(r!)^m (s!)^n} e^{-(r-1)(s-1)/2}.$$

(Békéssy, Békéssy and Komlós, 1972.)

[Imitate the proof of Theorem 2.16. Define a configuration as a 1-1 map F of $U' = \bigcup_{i=1}^m U_i$ into $W' = \bigcup_{j=1}^n W_j$, where $|U_i| = r$ and $|W_j| = s$. Note that there are $N!$ configurations. For a configuration F denote by $X(F)$ the number of 'double edges', i.e. pairs of elements (a, b) of U' for which $a, b \in U_i$ and $F(a), F(b) \in W_j$ for some i and j. Show that $X \xrightarrow{d} P\{(r-1)(s-1)/2\}$.]

2.13 For r, s, m, n and N as in Ex. 12, denote by $M(m, n; r, s)$ the number of $m \times n$ matrices with row-sums r and column-sums s. Show that as $N \to \infty$

$$M(m, n; r, s) \sim \frac{N!}{(r!)^m (s!)^n} e^{(r-1)(s-1)/2}.$$

(Békéssy, Békéssy and Komlós, 1972.)

[Consider the same configuration space as in Ex. 12 and treat the number of double edges, triple edges, etc., as random variables of the configuration space.]

2.14 Let $\varepsilon > 0$ be fixed. Show that (i) if $p = \{(2 + \varepsilon) \log n\}/n$, then a.e. G_p is connected and (ii) if $p = \{(1 + \varepsilon) \log n\}/n$, then a.e. G_p is connected. (The first assertion is quite trivial, the proof of the second needs a little work.)

2.15 Prove that for every fixed $\alpha > 1$ and $t = \lfloor \alpha n \log n \rfloor$ we have

$$P(G_t \text{ is connected}) = 1 - O(n^{1-2\alpha}).$$

3
The Degree Sequence

The degree of a vertex is one of the simplest graph invariants. If $x \in V$, then $d_G(x)$, as a function of $G \in \mathcal{G}(n,p)$, has binomial distribution with parameters $n-1$ and p. Furthermore, if $x, y \in V$ and $x \neq y$, then $d_G(x)$ and $d_G(y)$ are rather close to being independent random variables on $\mathcal{G}(n,p)$. Thus it is not surprising that one can get rather detailed information about the distribution of individual members of the degree sequence. Erdős and Rényi (1959) were the first to study the distribution of the maximum (minimum) degree, and various aspects of the degree sequence were investigated by Ivchenko (1973*a*), Erdős and Wilson (1977), Bollobás (1980*a*, 1981*a*, 1982*a*) and Cornuejols (1981).

In the first four sections, based on Bollobás (1981*a*, 1982*a*), we present the basic results concerning the degree sequence. The fifth section is devoted to a result of Babai, Erdős and Selkow (1980) concerning the graph isomorphism problem and to the sketch of a related result of Bollobás (1982*b*).

Throughout the section $\lim f(n)$ means the limit of $f(n)$ as $n \to \infty$ through a certain set of natural numbers.

3.1 The Distribution of an Element of the Degree Sequence

In this chapter we shall write $(d_i)_1^n$ for the degree sequence of a graph $G \in \mathcal{G}(n,p)$ arranged in descending order: $d_1 \geq d_2 \geq \ldots \geq d_n$. Thus $d_1(G) = \Delta(G)$ is the maximum degree and $d_n(G) = \delta(G)$ is the minimum degree. Our aim is to determine the distribution of this sequence. It will turn out that depending on the function $p = p(n)$, different members of this sequence are almost completely determined. In order to study the degree sequence we introduce some related random variables. We write $X_k = X_k(G)$ for the number of vertices of degree k, Y_k for the number of vertices of degree at least k and Z_k for the number of vertices of degree at most k. Thus

$$Y_k = \sum_{l \geq k} X_l \text{ and } Z_k = \sum_{l \leq k} X_l.$$

Clearly

$$d_r \geq k \text{ iff } Y_k \geq r$$

and

$$d_{n-r} \leq k \text{ iff } Z_k \geq r + 1.$$

If $p = o(n^{-3/2})$, then

$$E(Y_2) = \sum_{j=2}^{n-1} E(X_j) \leq n \sum_{j=2}^{n-1} \binom{n}{j} p^j \leq \sum_{j=2}^{\infty} (pn)^j / j! = o(1),$$

so a.e. $G_{n,p}$ consists of independent edges. Hence if also $pn^2 \to \infty$, then a.e. $G_{n,p}$ has degree sequence $d_1 = d_2 = \ldots = d_{2M} = 1, d_{2M+1} = \ldots = d_n = 0$, where $M = e(G_{n,p}) \sim pn^2/2$. Therefore in the discussion that follows we may assume that neither $p = o(n^{-3/2})$ nor $1 - p = o(n^{-3/2})$ holds.

Theorem 3.1 *Let $\varepsilon > 0$ be fixed, $\varepsilon n^{-3/2} \leq p = p(n) \leq 1 - \varepsilon n^{-3/2}$, let $k = k(n)$ be a natural number and set $\lambda_k = \lambda_k(n) = nb(k; n-1, p)$. Then the following assertions hold.*

(i) If $\lim \lambda_k(n) = 0$, then $\lim P(X_k = 0) = 1$.
(ii) If $\lim \lambda_k(n) = \infty$, then $\lim P(X_k \geq t) = 1$ for every fixed t.
(iii) If $0 < \underline{\lim}\, \lambda_k(n) \leq \overline{\lim}\, \lambda_k(n) < \infty$,

then X_k has asymptotically Poisson distribution with mean λ_k:

$$P(X_k = r) \sim e^{-\lambda_k} \lambda_k^r / r!$$

for every fixed r.

Proof We may assume without loss of generality that $p \leq 1/2$. Note that $\lambda_k = \lambda_k(n)$ is exactly the expectation of $X_k(G)$. Hence

$$P(X_k \geq 1) \leq E(X_k) = \lambda_k(n),$$

so the first assertion follows.

From now on we suppose that $\underline{\lim}\lambda_k(n) > 0$. The remaining assertions of the theorem will follow from the fact that for every fixed $r \geq 1$ the rth factorial moment $E_r(X_k)$ of X_k is asymptotic to $\lambda_k(n)^r$.

Recall that $E_r(X_k)$ is the expected number of ordered r-tuples of vertices $(x_1, x_2, \ldots, x_r)$ such that each vertex x_i has degree k. What is the probability that r given vertices $x_1, x_2, \ldots, x_r$ all have degree k? Suppose we have chosen the edges joining the x_i's. If there are l such edges and vertex x_i is joined to $\tilde{d}_i \leq k$ vertices $x_j, 1 \leq j \leq r$, then $\sum_{i=1}^r \tilde{d}_i = 2l$ and x_i has to be joined to $k - \tilde{d}_i$ vertices outside the set $\{x_1, x_2, \ldots, x_r\}$. The probability of this event is

$$\prod_{i=1}^{r} b(k - \tilde{d}_i; n-r, p). \tag{3.1}$$

Let us distinguish two cases according to the size of $p(n)$. Suppose first that $p(n) \leq \frac{1}{2}$ is bounded away from 0. Then $\underline{\lim}\, \lambda_k(n) > 0$ implies that $k(n)$ is about pn, say

$$\frac{1}{2}pn \leq k(n) \leq \frac{3}{2}pn.$$

[In fact, by Theorem 1.1, we have $k(n) = pn + O(n \log n)^{1/2}$.] From this it follows that for every $r \in \mathbb{N}$ there is a function $\phi_r(n)$ such that $\lim_{n\to\infty} \phi_r(n) = 0$ and

$$\left| \frac{b(k-d; n-r, p)}{b(k; n-1, p)} - 1 \right| \leq \phi_r(n).$$

Therefore, by (1),

$$E_r(X_k) \sim (n)_r b(k; n-1, p)^r \sim \lambda_k^r. \tag{3.2}$$

Now suppose that $p = o(1)$. Then (1) implies the following upper bound for $E_r(X_k)$:

$$E_r(X_k) \leq (n)_r \sum_{l=0}^{R} \binom{R}{l} p^l q^{R-l} \max_{\sum_1^r d_i^* = 2l} \prod_{i=1}^{r} b(k - d_i^*; n-r, p), \tag{3.3}$$

where $R = \binom{r}{2}$ and the maximum is over all sequences $d_1^*, d_2^*, \ldots, d_r^*$ with $\sum_1^r d_i^* = 2l$ and $0 \leq d_i^* \leq \min\{r-1, k\}$. Clearly $\underline{\lim}\, \lambda_k(n) > 0$ implies that $k(n) = o(n)$, so if $0 \leq d \leq \min\{r-1, k\}$ and n is sufficiently large,

$$\frac{b(k-d; n-r, p)}{b(k; n-r, p)} \leq \frac{(k)_d}{(n-r-k)_d} p^{-d} < 2\left(\frac{k}{pn}\right)^d.$$

Therefore (3) gives

$$E_r(X_k) \leq n^r b(k; n-r, p)^r \left\{ 1 + \sum_{l=1}^{R} \binom{R}{l} p^l 2^r \left(\frac{k}{pn}\right)^{2l} \right\}$$

$$\leq n^r b(k;n-r,p)^r \left\{1 + 2^{r^2} \sum_{l=1}^{R} \left(\frac{k^2}{pn^2}\right)^l\right\}. \tag{3.4}$$

Our assumption that $\underline{\lim}\, \lambda_k(n) > 0$ implies that $k^2 = o(pn^2)$. Indeed, if for some fixed $\eta > 0$ the inequality $k \geq \eta p^{1/2} n$ held for arbitrarily large n then we would have

$$\begin{aligned} \underline{\lim}\, \lambda_k(n) &\leq \underline{\lim}\, n \binom{n}{k} p^k \leq \underline{\lim}\, n \left(\frac{en}{k}\right)^k p^k \\ &= \underline{\lim}\, n \left(\frac{epn}{k}\right)^k \leq \underline{\lim}\, n \left(\frac{ep^{1/2}}{\eta}\right)^{\eta p^{1/2} n}, \\ &\leq \underline{\lim}\, n 2^{-n^{1/5}} = 0, \end{aligned}$$

contrary to our assumption. As $k^2 = o(pn^2)$, inequality (4) implies

$$E_r(X_k) \leq n^r b(k;n-r,p)^r \{1 + o(1)\} = \lambda_k^r \{1 + o(1)\}.$$

By considering only independent r-tuples of vertices of degree k we find that

$$E_r(X_k) \geq q^R (n)_r b(k;n-r,p)^r = \lambda_k^r \{1 + o(1)\},$$

since $q \to 1$, so

$$E_r(X_k) \sim \lambda_k^r. \tag{3.4$'$}$$

Thus the rth factorial moment of X_k is asymptotic to the rth factorial moment of $P(\lambda_k)$. Now if $\lim \lambda_k(n) = \infty$, then $E_2(X_k) \sim \lambda_k^2$ implies that $E(X_k^2) = \lambda_k^2\{1 + o(1)\}$ so the Chebyshev inequality gives

$$\lim_{n\to\infty} P(X_k \geq t) = 1$$

for every fixed t.

Finally, if $\overline{\lim}\, \lambda_k < \infty$, then by Theorem 1.20 relations (3.2) and (3.4′) imply that asymptotically X_k has Poisson distribution with mean λ_k. □

As an immediate consequence of Theorem 3.1 we see that if almost every $G_{n,p}$ has a vertex of degree k, then for every fixed t almost every $G_{n,p}$ has at least t vertices of degree k.

The proof of Theorem 3.1 can be modified to give analogous results about Y_k and Z_k.

Theorem 3.2 *Let $\varepsilon > 0$ be fixed, $\varepsilon n^{-3/2} \leq p = p(n) \leq 1 - \varepsilon n^{-3/2}$, let $k = k(n)$ be a natural number and set*

$$\mu_k = nB(k;n-1,p) \text{ and } \nu_k = n\{1 - B(k+1;n-1,p)\},$$

where

$$B(l;m,p) = \sum_{j \geq l} b(j;m,p).$$

Then the assertions of Theorem 3.1 hold if we replace X_k and λ_k by Y_k and μ_k or Z_k and ν_k. □

This last result enables us to determine the distribution of the first few and the last few values in the degree sequence. First we present some results concerning the case when p is neither too large nor too small.

Theorem 3.3 *Suppose $p = p(n)$ is such that $pqn/(\log n)^3 \to \infty$. Let c be a fixed positive constant, m a fixed natural number and let $x = x(n,c)$ be defined by*

$$\frac{1}{\sqrt{2\pi}} \frac{n}{x} \mathrm{e}^{-x^2/2} = c. \tag{3.5}$$

Then

$$\lim_{n\to\infty} P\{d_m < pn + x(pqn)^{1/2}\} = \mathrm{e}^{-c} \sum_{k=0}^{m-1} \frac{c^k}{k!}.$$

Proof Put $K = \lceil pn + x(pqn)^{1/2} \rceil$. Then $d_m < pn + x(pqn)^{1/2}$ means that at most $m-1$ vertices have degree at least K, that is

$$Y_K \leq m - 1.$$

By Theorem 3.2 the distribution of Y_K tends to $P(\mu_K)$, where

$$\mu_K = nB(K; n-1, p).$$

Now by the definition of x we have

$$x(pqn)^{1/2} = o\{(pqn)^{2/3}\},$$

so by Theorem 1.6

$$\mu_K \sim (c/n)n = c.$$

This implies the assertion of the theorem. □

For every fixed positive c the value of x calculated from (5) is about $(2\log n)^{1/2}$. Furthermore,

$$x(n,1) = (2\log n)^{1/2}\left\{1 - \frac{\log\log n}{4\log n} - \frac{\log(2\pi^{1/2})}{2\log n}\right\} + o\{(\log n)^{-1/2}\}.$$

Hence $x' = x(n,1) + \delta$ corresponds to $c' \sim \exp\{-(2\log n)^{1/2}\delta\}$, provided $\delta = o(1)$. Therefore Theorem 3.3 can be rewritten in the following form.

Theorem 3.3′ *Suppose $pqn/(\log n)^3 \to \infty$ and y is a fixed real number. Then for every fixed m we have*

$$\lim_{n\to\infty} P\left\{d_m < pn + (2pqn\log n)^{1/2}\left(1 - \frac{\log\log n}{4\log n} - \frac{\log(2\pi^{1/2})}{2\log n} + \frac{y}{2\log n}\right)\right\}$$
$$= \mathrm{e}^{-\mathrm{e}^{-y}} \sum_{k=0}^{m-1} \mathrm{e}^{-ky}/k!. \qquad \square$$

Corollary 3.4 *Suppose $pqn/(\log n)^3 \to \infty$ and y is a fixed real number. Then the maximal degree $\Delta = d_1$ of $G_{n,p}$ satisfies*

$$\lim_{n\to\infty} P\left\{\Delta < pn + (2pqn\log n)^{1/2}\left(1 - \frac{\log\log n}{4\log n} - \frac{\log(2\pi^{1/2})}{2\log n} + \frac{y}{2\log n}\right)\right\}$$
$$= \mathrm{e}^{-\mathrm{e}^{-y}}. \qquad \square$$

If p is close to 0 (or 1), then we rely on Theorem 3.2 for information on the maximum and minimum degrees. In the most interesting case both these degrees are bounded. The proof is left as an exercise (Exs. 1 and 2).

Theorem 3.5 *Let k, x and y be fixed, $k \geq 2, x > 0$ and $y \in \mathbb{R}$. If*

$$p \sim xn^{-(k+1)/k},$$

then

$$P\{\Delta(G_p) = k\} \to 1 - \mathrm{e}^{-x^k/k!} \text{ and } P\{\Delta(G_p) = k-1\} \to \mathrm{e}^{-x^k/k!}.$$

If

$$p = (\log n + k\log\log n + y)/n$$

then

$$P\{\delta(G_p) = k\} \to 1 - \mathrm{e}^{-\mathrm{e}^{-y}/k!} \text{ and } P\{\delta(G_p) = k+1\} \to \mathrm{e}^{-\mathrm{e}^{-y}/k!}. \qquad \square$$

3.2 Almost Determined Degrees

In what range of $p = p(n)$ is it true that almost all graphs $G \in \mathcal{G}(n,p)$ have the same maximum degree? What is the corresponding range of p if almost all G_p have the same minimum degree? In what range of p is it true that a.e. G_p has a unique vertex of maximum degree? The aim of this section is to answer these questions. The proofs of the results are based on Theorem 3.1.

We show first that if almost all graphs have the same maximum degree then $p = o(\log n/n)$ and then we show that this necessary condition is essentially sufficient.

Theorem 3.6 *Suppose that $p \le \frac{1}{2}$ and there is a function $D(n)$ such that in the space $\mathcal{G}(n,p)$ we have*

$$\lim_{n\to\infty} P\{\Delta(G) = D(n)\} = 1.$$

Then $p = o(\log n/n)$.

Proof By Theorem 3.1 we must have $\lim_{n\to\infty} nb(D; n-1, p) = \infty$ and $\lim_{n\to\infty} nb(D+1); n-1, p) = 0$. Therefore

$$\lim_{n\to\infty} b(D+1; n-1, p)/b(D; n-1, p) = \lim_{n\to\infty} \frac{p(n-D-1)}{q(D+1)} = 0,$$

so $pn/D \to 0$. Using again that $\lim nb(D; n-1, p) = \infty$, we find that for every $c > 1$

$$\lim_{n\to\infty} nb(\lceil cpn \rceil; n-1, p) = \infty$$

and so

$$\lim_{n\to\infty} n(epn/cpn)^{cpn} = \lim_{n\to\infty} n(e/c)^{cpn} = \infty.$$

As this holds for every $c > 1$, we have $p = o(\log n/n)$. □

Theorem 3.7 *Suppose $p = o(\log n/n)$. Let $k = k(n) \ge pn$ be such that* $\max\{\lambda_k(n), \lambda_k(n)^{-1}\}$ *is minimal. Then the following assertions hold.*

(i) If $0 < \underline{\lim}\, \lambda_k(n) \le \overline{\lim}\, \lambda_k(n) < \infty$, *then*

$$P\{\Delta(G) = k(n)\} \sim 1 - e^{-\lambda_k}(n)$$

and

$$P\{\Delta(G) = k(n) - 1\} \sim e^{-\lambda_k}(n).$$

(ii) If $\lim \lambda_k(n) = \infty$, *then a.e. G_p has maximum degree $k(n)$ and if* $\lim \lambda_k(n) = 0$, *then a.e. G_p has maximum degree $k(n) - 1$.*

Proof It is easily checked that $k/pn \to \infty$, $\lambda_{k+1}/\lambda_k \sim pn/(k+1) \to 0$ and $\lambda_k/\lambda_{k-1} \sim pn/k \to 0$. From these it follows that $\lambda_{k+1} \to 0$ and $\lambda_{k-1} \to \infty$.

By Theorem 3.1 the relation $\lambda_{k-1} \to \infty$ implies that a.e. G_p contains a vertex of degree $k(n)-1$ and so the maximum degree of a.e. G_p is at least $k(n)-1$. Furthermore

$$P\{\Delta(G) \geq k+1\} = P\left(\sum_{j=k+1}^{n-1} X_j \geq 1\right) \leq \sum_{j=k+1}^{n-1} E(X_j) = O(\lambda_{k+1}) = o(1).$$

Hence a.e. G_p is such that the maximum degree is $k(n)-1$ unless there is a vertex of degree $k(n)$, in which case it is exactly $k(n)$:

$$P\{\Delta(G) = k(n)\} \sim P(X_k \geq 1)$$

and

$$P\{\Delta(G) = k(n)-1\} \sim 1 - P\{\Delta(G) = k(n)\}.$$

Finally, by Theorem 3.1, we know the behaviour of $P(X_k \geq 1)$. □

If k_0 is the maximal integer with $\lambda_{k_0} \geq 1$ then k is k_0 or k_0+1, so the maximum degree of a.e. G_p is k_0-1, k_0 or k_0+1. It is easily seen that if $p = o(\log n/n)$ and $pn^{3/2} \to \infty$, then p can be altered slightly so that almost all graphs have the same maximum degree. To be precise, if $\phi(n) = o(\log n/n)$ and $\phi(n)n^{3/2} \to \infty$, then one can choose functions $p = p(n) \sim \phi(n)$ and $k(n)$ such that a.e. G_p has maximum degree $k(n)$.

In what range of p is the maximum degree of a.e. G_p a fixed natural number k? The results above show that this range is exactly $\{p : 0 < p < 1, pn^{(k+2)/(k+1)} \to 0 \text{ and } pn^{(k+1)/k} \to \infty\}$.

If $p \leq \frac{1}{2}$, then the minimum degree behaves somewhat differently from the maximum degree. We have the following analogue of Theorems 3.6 and 3.7.

Theorem 3.8 (*i*) *Suppose that* $p \leq \frac{1}{2}$ *and there is a function* $d(n)$ *such that in the space* $\mathcal{G}(n, p)$ *we have*

$$\lim_{n\to\infty} P\{\delta(n) = d(n)\} = 1.$$

Then

$$p \leq \{1 + o(1)\} \log n/n.$$

(*ii*) *If* $p \leq \{1 + o(1)\} \log n/n$, *then there is a function* $d(n)$ *such that the minimum degree of a.e.* G_p *is either* $d(n)$ *or* $d(n)-1$.

Proof (i) Write p in the form $p = \{\log n + \omega(n)\}/n$. Then, if $\omega(n) = O(\log n)$, say,

$$\lambda_0 = nb(0; n-1, p) = n(1-p)^{n-1} \sim nn^{-1}\, \mathrm{e}^{-\omega(n)} = \mathrm{e}^{-\omega(n)},$$

so, by Theorem 3.1, G_p almost surely has an isolated vertex iff $\omega(n) \to -\infty$. Therefore we may assume that $p \geq (\log n + C)/n$ for some constant C.

As in the proof of Theorem 3.6, we find that if $\lim_{n\to\infty} P\{\delta(n) = d(n)\} = 1$, then for every fixed ε, $0 < \varepsilon < \frac{1}{2}$, we have

$$n(\varepsilon pn)^{-1/2}(\mathrm{e}/\varepsilon p)^{\varepsilon pn} p^{\varepsilon pn}\, \mathrm{e}^{-pn+p^2\varepsilon n} \to \infty.$$

Hence

$$\log n - \frac{1}{2}\log(pn) + pn\{\varepsilon + \varepsilon\log(1/\varepsilon) + \varepsilon p - 1\} \to \infty.$$

As this holds for arbitrarily small positive values of ε, it follows that $p \leq \log n/n + o(\log n/n)$,

(ii) Proceed as in the proof of Theorem 3.7. □

Now let us turn to the question of uniqueness of a vertex of maximum (minimum) degree.

Theorem 3.9 *(i) If $p \leq \frac{1}{2}$ and $pn/\log n \to \infty$, then a.e. G_p has a unique vertex of maximum degree and a unique vertex of minimum degree.*

(ii) If $p \leq \frac{1}{2}$ and a.e. G_p has a unique vertex of maximum degree or a unique vertex of minimum degree, then $pn/\log n \to \infty$.

Proof (i) For simplicity write $b(l) = b(l; n-1, p)$ and $B(l) = B(l; n-1, p)$. Let k be the maximal natural number with

$$nB(k) \geq 1.$$

It is easily checked that $k > pn$, $k \sim pn$, $nb(k-1) \to 0$ and $b(k)/b(k-1) \to 1$. Consequently one can choose $l = l(n)$, $pn < l < k$, such that $nb(l) \to 0$ and $nB(l) \to \infty$. If we vary l in such a way that these relations remain valid then we can find an $m = m(n)$, $pn < m < k$, such that

$$nB(m) \to \infty \text{ and } nB(m)nb(m) \to 0.$$

We claim that a.e. G_p has a vertex of degree at least m, but almost no G_p has two vertices whose degrees are equal and at least m. Indeed, the expected number of vertices of degree at least m is $E(Y_m) = nB(m)$. Hence $E(Y_m) \to \infty$ and by Theorem 3.2 we have $\Delta(G_p) \geq m$ for a.e. G_p.

On the other hand, the probability that there are at least two vertices whose degrees are equal and at least m is at most

$$\begin{aligned}\sum_{j\geq m} P(X_j \geq 2) &\leq \sum_{j\geq m} E_2(X_j) \leq \sum_{j\geq m-1} n^2 b(j;n-2,p)^2 \\ &\leq nb(m-1;n-2,p)nB(m-1;n-2,p) \sim nb(m)nB(m).\end{aligned}$$

To see the second inequality above, note that the expected number of ordered pairs of vertices of degree $j \geq m$ is

$$n(n-1)\{pb(j-1;n-2,p)^2 + (1-p)b(j;n-2,p)^2\} \leq n^2 b(j;n-2,p)^2.$$

Hence $\sum_{j\geq m} P(X_j \geq 2) \to 0$, proving the assertion.

(ii) A sharper form of this assertion is left as an exercise for the reader [Ex. 3, see also Bollobás (1982*a*)]. □

Let us summarize the results of this section in a somewhat imprecise form. If $p = o(\log n/n)$, then both the minimum and maximum degrees are essentially determined and there are many vertices of minimum degree and many vertices of maximum degree. If $\varepsilon \log n/n \leq p \leq \{1+o(1)\}\log n/n$ for some $\varepsilon > 0$, then the minimum degree is essentially determined and there are many vertices of minimum degree, while the maximum degree is not confined to any finite set with probability tending to 1. If $(1+\varepsilon)\log n/n \leq p \leq C\log n/n$ for some $\varepsilon > 0$ and $C > 0$, then neither the minimum nor the maximum degree is essentially determined and the probability that there are several vertices of minimum and maximum degrees is bounded away from 0. Finally, if $pn/\log n \to \infty$ and $p \leq \frac{1}{2}$, then a.e. G_p has a unique vertex of maximum degree and a unique vertex of minimum degree.

3.3 The Shape of the Degree Sequence

Having investigated the smallest and largest members of the degree sequence, we turn to the study of a general member d_m of the degree sequence. Recall that $Y_k = \sum_{j\geq k} X_j$ is the number of vertices of degree at least k in G_p. The mean of Y_k is $\mu_k = nB(k;n-1,p)$. We shall use Chebyshev's inequality to show that in a certain range of p and k most graphs are such that Y_k is close to μ_k. Our main result is based on two lemmas. For simplicity we shall omit p from $b(l;N,p)$ and $B(l;N,p)$.

Lemma 3.10 *The variance of Y_k satisfies*

$$\sigma^2(Y_k) = E\{(Y_k - \mu_k)^2\} \leq \mu_k + n^2 pqb(k-1;n-2)^2.$$

Proof The second factorial moment of Y_k is easily calculated:

$$E_2(Y_k) = n(n-1)\{pB(k-1;n-2)^2 + qB(k;n-2)^2\}. \tag{3.6}$$

Indeed, the probability that both of two given vertices of G_p, say a and b, have degree at least k is

$$P\{ab \in E(G_p) \text{ and } d_{G_p-b}(a) \geq k-1, d_{G_p-a}(b) \geq k-1\}$$
$$+ P\{ab \notin E(G_p) \text{ and } d_{G_p-b}(a) \geq k, d_{G_p-a}(b) \geq k\}.$$

The events $\{ab \in E(G_p)\}$, $\{d_{G_p-b}(a) \geq k-1\}$ and $\{d_{G_p-a}(b) \geq k-1\}$ are independent, so the probability of their intersection is

$$P\{ab \in E(G_p)\}P\{d_{G_p-b}(a) \geq k-1\}P\{d_{G_p-a}(b) \geq k-1\} = pB(k-1;n-2)^2.$$

The second term in the expression (3.6) for $E_2(Y_k)$ is justified analogously. Hence

$$\begin{aligned}\sigma^2(Y_k) &= E(Y_k^2) - \mu_k^2 \\ &= \mu_k + n(n-1)\{pB(k-1;n-2)^2 + qB(k;n-2)^2\} - \mu_k^2 \\ &\leq \mu_k + n^2\{pB(k-1;n-2)^2 + qB(k;n-2)^2 - B(k;n-1)^2\}. \quad (3.7)\end{aligned}$$

Note now that

$$B(k;n-1) = pB(k-1;n-2) + qB(k;n-2)$$

and

$$B(k-1;n-2) - B(k;n-2) = \binom{n-2}{k-1} p^{k-1}q^{n-k-1} = b(k-1;n-2).$$

Substituting these into (3.7) we find that

$$\sigma^2(Y_k) \leq \mu_k + n^2pqb(k-1;n-2)^2. \qquad \square$$

Lemma 3.11

$$\sigma^2(Y_k) = O(\mu_k).$$

Proof This is immediate from Lemma 3.10, since one can check from Theorems 1.1–1.5 that

$$n^2pqb(k-1;n-2)^2 = O\{nB(k;n-1)\}. \qquad \square$$

Theorem 3.12 *Suppose $m = m(n) = o(n)$, $m(n) \to \infty$ and $\omega(n) \to \infty$ arbitrarily slowly. Define x by*

$$1 - \Phi(x) = m/n.$$

Then a.e. G_p satisfies

$$|d_m - pn - x(pqn)^{1/2}| \le \omega(n) \left(\frac{pqn}{m \log(n/m)} \right)^{1/2}.$$

Proof The assumptions imply that $x \to \infty$, so by (15′) of Chapter 3 we have

$$\frac{m}{n} \sim \frac{1}{\sqrt{2\pi}} \frac{1}{x} \, \mathrm{e}^{-x^2/2}$$

and

$$x \sim \{2 \log(n/m)\}^{1/2}.$$

We may assume without loss of generality that $\omega(n) \le m^{1/2}$ and $\omega(n) = o(x)$. Set

$$k = pn + x(pqn)^{1/2} + \omega(n)\{pqn/m \log(n/m)\}^{1/2}.$$

By Theorem 1.6

$$E(Y_k) \sim m \exp[-x\omega(n)/\{m \log(n/m)\}^{1/2} - \omega(n)^2/2m \log(n/m)] \to \infty$$

and

$$\begin{aligned} m - E(Y_k) &\sim m(1 - \exp[-x\omega(n)/\{m \log(n/m)\}^{1/2} - \omega(n)^2/2m \log(n/m)]) \\ &\sim mx\omega(n)/\{m \log(n/m)\}^{1/2} \ge \omega(n) m^{1/2}. \end{aligned}$$

Hence

$$m \ge E(Y_k) + \omega(n) E(Y_k)^{1/2}.$$

By Lemma 3.11 and Chebyshev's inequality we obtain that $Y_k < m$ in a.e. G_p, so a.e. graph G_p satisfies

$$d_m < k = pn + x(pqn)^{1/2} + \omega(n)\{pqn/m \log(n/m)\}^{1/2}.$$

A similar argument gives that for a.e. G_p we have

$$d_m > pn + x(pqn)^{1/2} - \omega(n)\{pqn/m \log(n/m)\}^{1/2}. \qquad \square$$

If m does not grow too fast, then the dependence of x above on m can be calculated precisely and one is led to the following corollary.

Corollary 3.13 *Let $\omega(n) \to \infty$ and $m = m(n) = O(\log n)/(\log\log n)^4$. Then a.e. G_p satisfies*

$$\left| d_m - pn - (2pqn\log n)^{1/2} + \log\log n \left(\frac{pqn}{8\log n}\right)^{1/2} + \log(2\pi^{1/2}m)\left(\frac{pqn}{2\log n}\right)^{1/2} \right| \le \omega(n)\left(\frac{pqn}{m\log n}\right)^{1/2}.$$

□

Another assertion implied by Theorem 3.12 is that if p is not too small, then almost all G_p's have about the same maximal degree.

Corollary 3.14 *If $pn/\log n \to \infty$, then a.e. G_p satisfies*

$$\Delta(G_p) = \{1 + o(1)\}pn.$$

Proof Taking $m = 1$ and $\omega(n) = (pn/\log n)^{1/2}$ in Theorem 3.12, we see that $x \le (2\log n)^{1/2}$ and so

$$\begin{aligned} |\Delta(G_p) - pn| &\le \{2(\log n)pqn\}^{1/2} + \omega(n)(pqn/\log n)^{1/2} \\ &\le O(pn) + \omega(n)(pn/\log n)^{1/2} \end{aligned}$$

almost surely.

The result above is best possible (Ex. 8). Furthermore, if $(pn - \log n)/\log\log n \to \infty$, then almost all G_p's have about the same minimal degree (Ex. 9).

McKay and Wormald (1997) proved several powerful general results about the joint distribution of the degrees of a random graph that imply the results above. They showed that the joint distribution can be closely approximated by models derived from a set of independent binomial distributions. For example, they proved that for a wide range of functions $M = M(n)$, the distribution of the degree sequence of a random graph $G_M \in \mathcal{G}(n, M)$ is well approximated by the conditional distribution $\{(X_1, \dots, X_n) : |\sum_1^n X_i = 2M\}$, where $X_1, \dots, X_n$ are independent r.vs, each with the same distribution as the degree of one vertex:

$$\mathbb{P}(X_i = k) = \binom{n-1}{k}\binom{N-n+1}{M-k} \Big/ \binom{N}{M}.$$

□

3.4 Jumps and Repeated Values

We have seen that if p is not too close to 0 or 1, then a.e. G_p has a unique vertex of maximum degree. In fact, unless p is close to 0 or 1, for a.e. G_p

the first several values of the degree sequence are strictly decreasing. The following result gives a good estimate of the likely jumps $d_i - d_{i+1}$.

Theorem 3.15 *Suppose $m = o(pqn/\log n)^{1/4}$, $m \to \infty$ and $\alpha(n) \to 0$. Then a.e. G_p is such that*

$$d_i - d_{i+1} \geq \frac{\alpha(n)}{m^2}\left(\frac{pqn}{\log n}\right)^{1/2} \quad \text{for every } i < m.$$

Proof As in the proof of Theorem 3.12, let x be defined by

$$1 - \Phi(x) = m/n.$$

Note that $x = O\{\log n)^{1/2}\}$. By Theorem 3.12, a.e. G_p satisfies

$$d_m \geq pn + (x - \varepsilon)(pqn)^{1/2},$$

where

$$\varepsilon = \{\log(n/m)\}^{1/2}.$$

Therefore the theorem will be proved if we show that almost no G_p contains an ordered pair of vertices (u, v) such that

$$K = \lceil pn + (x - \varepsilon)(pqn)^{1/2} \rceil \leq d(u) \leq d(v) \leq d(u) + J - 1,$$

where

$$J = \frac{\alpha(n)}{m^2}\left(\frac{pqn}{\log n}\right)^{1/2}.$$

The expected number of such ordered pairs is clearly

$$\begin{aligned} L &= n(n-1)\left\{p \sum_{k=K-1}^{n-2} b(k;n-2) \sum_{l=k}^{k+J-1} b(l;n-2)\right. \\ &\qquad \left. + q\sum_{k=K}^{n-2} b(k;n-2) \sum_{l=k}^{k+J-1} b(l;n-2)\right\} \\ &\leq n^2 \sum_{k=K-1}^{n-2} b(k;n-2)Jb(k;n-2) \\ &\leq n^2 JB(K-1;n-2)b(K-1;n-2). \end{aligned}$$

By Theorems 3.2 and 6 of Chapter 3 this gives that if n is sufficiently large, then

$$L \leq 2n^2 \frac{\alpha(n)}{m^2}\left(\frac{pqn}{\log n}\right)^{1/2} m \frac{x}{(pqn)^{1/2}} \frac{m}{n} = \frac{2\alpha(n)x}{(\log n)^{1/2}} = O\{\alpha(n)\}.$$

Since $\alpha(n) \to 0$, the expected number of pairs tends to 0. $\square$

Let us state without proof that Theorem 2.15 is essentially best possible.

Theorem 3.16 *Suppose $m \to \infty$ and $\omega(n) \to \infty$. Then a.e. G_p is such that*

$$d_i - d_{i+1} \leq \frac{\omega(n)}{m^2}\left(\frac{pqn}{\log n}\right)^{1/2} \quad \textit{for some } i < m.$$

3.5 Fast Algorithms for the Graph Isomorphism Problem

How fast an algorithm can one give in order to decide whether two given graphs are isomorphic? It is not known that there is such an algorithm whose running time is bounded by a polynomial of the number of vertices (or edges). However, Babai, Erdős and Selkow (1980) gave a very simple algorithm which, for almost every graph G of order n, tests for every graph H in time $O(n^2)$ whether G is isomorphic to H. This algorithm is based on the fact that the degree sequence of a.e. graph contains many gaps (cf. Theorem 3.15).

Let $\mathscr{H}$ be a set of graphs with vertex set $V = \{1, 2, \ldots, n\}$. A *canonical labelling algorithm* of $\mathscr{H}$ is an algorithm assigning to each $G \in \mathscr{H}$ a permutation π_G of V such that G and H in $\mathscr{H}$ are isomorphic if and only if $\pi_G(G)$ and $\pi_H(H)$ coincide. In other words, a canonical labelling algorithm relabels the vertices in such a way that two graphs are isomorphic if and only if the new labelled graphs coincide.

The next result is a slight extension of the result of Babai, Erdős and Selkow (1980); it is an easy consequence of Theorem 3.1.

Theorem 3.17 *Suppose $0 < p = p(n) \leq \frac{1}{2}$ is such that $p^5 n/(\log n)^5 \to \infty$. There is an algorithm which, for almost every graph G_p, tests in $O(pn^2)$ time for any graph H whether H is isomorphic to G_p or not.*

Proof First we give an algorithm which constructs a set $\mathscr{H} \subset \mathscr{G}(n,p)$ such that $P(\mathscr{H}) \to 1$. Then we construct a canonical labelling algorithm for $\mathscr{H}$. Both of these algorithms will work in $O(pn^2)$ time.

Set $m = \lceil 3 \log_{(1/q)} n \rceil$. Compute the degrees of the vertices of G_p and then order the vertices by degree: $x_1, x_2, \ldots, x_n$ are such that $d(x_1) = d_1 \geq d(x_2) = d_2 \geq \ldots \geq d(x_n) = d_n$. If $d_i \leq d_{i+1} + 2$ for some $i \leq m$, then put G_p into $\mathscr{G}(n,p) - \mathscr{H}$ and end the algorithm. Otherwise for $i = 1, 2, \ldots, n$ compute

$$f(x_i) = \sum_{j=1}^{m} a(i,j) 2^j,$$

where $a(i,j)$ is 1 if $x_i x_j \in E(G_p)$ or $i = j$ and 0 otherwise. If $f(x_i) = f(x_j)$ for some pair $i, j, 1 \le i < j \le n$, then put G_p into $\mathscr{G}(n,p) - \mathscr{K}$. Otherwise put G_p into $\mathscr{K}$.

It is clear that this algorithm runs in $O(pn^2)$ time. Furthermore, straight-forward calculations show that the conditions of Theorem 3.15 are satisfied with $\alpha(n) = 3m^2(\log n/pqn)^{1/2}$. Consequently, by Theorem 3.15 almost no graph is discarded because $d_i \le d_{i+1} + 2$ for some $i \le m$. What is the probability of discarding a graph G_p because of $f(x_i) = f(x_j)$? If $f(x_i) = f(x_j)$ then x_i and x_j are joined to exactly the same vertices in $V_{ij} = \{x_1, x_2, \ldots, x_m\} - \{x_i, x_j\}$. Let W_{ij} be the set of $m-2$ vertices of highest degree in $G_p - \{x_i, x_j\}$. Then $W_{ij} \subset V_{ij}$ since $d_1 \ge d_2 + 3 \ge d_2 \ge d_3 + 3 \ge \ldots \ge d_m \ge d_{m+1} + 3$. Since W_{ij} is independent of the edges incident with x_i and x_j,

$$\begin{aligned} P\{f(x_i) = f(x_j)\} \le\ & P(x_i \text{ and } x_j \text{ are joined to the same} \\ & \text{vertices in } W_{ij}) \le q^{m-2} = O(n^{-3}). \end{aligned}$$

Consequently, the probability of discarding a graph the second time round is not more than $\binom{n}{2} q^{m-2} = O(n^{-1})$. Hence $P(\mathscr{K}) \to 1$ as claimed.

The required fast canonical labelling algorithm is easily constructed. Let $x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}$ be the order of the vertices according to their f-values: $f(x_{\pi(1)}) > f(x_{\pi(2)}) > \ldots > f(x_{\pi(n)})$ and label $x_{\pi(i)}$ by $\pi(i)$. Clearly two graphs in $\mathscr{K}$ are isomorphic iff the new labelled graphs coincide. □

In the theorem above we did not care about $1 - P(\mathscr{K})$, the probability of rejection. All we wanted to ensure was that $1 - P(\mathscr{K}) = o(1)$. Inspired by the above theorem of Babai, Erdős and Selkow (1980) a number of fast algorithms were obtained by Lipton (1978), Karp (1979) and Babai and Kučera (1979) which have exponentially small probability of rejection. A canonical labelling given by Babai and Kučera (1979) runs in $O(n^2)$ time, with probability of rejection c^{-n} for some fixed $c > 1$. Furthermore, the rejected graphs are handled in such a way as to give a canonical labelling algorithm of all graphs with expected time $O(n^2)$.

Exercises

3.1 Let x be a positive constant, $k \ge 2$ a fixed integer and $p = p(n) \sim xn^{-1-1/k}$. Then a.e. G_p has no vertices of degree $k+1$ and the number of vertices of degree k tends to P_λ, where $\lambda = x^k/k!$. Deduce that if for fixed k we have $pn^{1+1/k} \to \infty$ and $pn^{(k+2)/(k+1)} \to 0$, then a.e. G_p has maximum degree k.

3.2 Suppose $y \in \mathbb{R}$, $k \geq 0$ and $p = \{\log n + k \log\log n + y + o(1)\}/n$. Then a.e. G_p has minimum degree at least k and the number of vertices of degree k tends to P_μ, where $\mu = e^{-y}/k!$ In particular, $P\{\delta(G_p) = k\} \to 1 - e^{-\mu}$ and $P\{\delta(G_p) = k+1\} \to e^{-\mu}$. Deduce that a.e. G_p has minimum degree at least $k+1$ iff

$$p = \{\log n + k \log\log n + \omega(n)\}/n \text{ where } \omega(n) \to \infty.$$

3.3 Let $0 < c < \infty$ be fixed and $p = \{c + o(1)\} \log n/n$. Let $k_0 = (1+\eta)pn$ be the maximal integer with $\lambda_0 = nb(k_0; n-1, p) \geq 1$. Set $k_j = k_0 + j$ and write $X_j = X_j(G_p)$ for the number of vertices of degree k_i. Then any fixed number of the X_j are asymptotically independent Poisson random variables with means $\lambda_j = \lambda_0(1+\eta)^j$, i.e. whenever $j_1 < j_2 < \ldots < j_t$ are fixed integers and r_1, r_2, ..., r_t are fixed non-negative integers,

$$P(X_{ji} = r_i, 1 \leq i \leq t) \to e^{-\lambda} \prod_{i=1}^{t} \lambda_{ji}^{r_i}/r_i!,$$

where $\lambda = \sum_{i=1}^{t} \lambda_{ji}$. (Bollobás, 1982*a*.)

3.4 Let c and p be as in the previous exercise. Let $\eta_\Delta = \eta_\Delta(c)$ be the unique positive root of

$$1 + c\eta = c(1+\eta)\log(1+\eta)$$

and, for $c > 1$, let $\eta_\delta = \eta_\delta(c)$ be the unique root satisfying $-1 < \eta_\delta < 0$ (see Figure 3.1). Show that a.e. G_p is such that

$$\Delta(G_p) \sim (1+\eta_\Delta)c \log n \text{ and } \delta(G_p) \sim (1+\eta_\delta)c \log n.$$

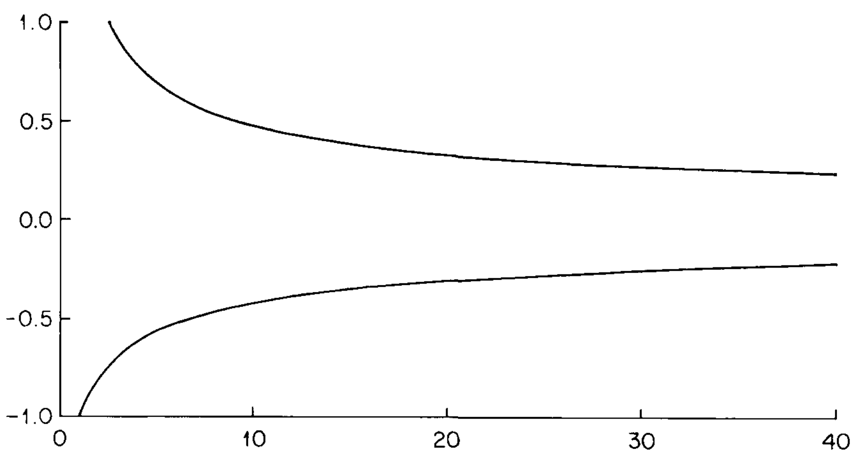


Fig. 3.1. The functions $\eta_\Delta(c)$ and $\eta_\delta(c)$.

3.5 Let $c > 0$ and $p = p(n) \sim c/n$. Prove that for a.e. G_p the maximum degree satisfies

$$\Delta(G_p) = \frac{\log n}{\log\log n}\left(1 + \frac{\log\log\log n}{\log\log n} + \frac{1 + \log c + o(1)}{\log\log n}\right).$$

3.6 Let $k \in \mathbb{N}$. Show that a.e. $G_{k-\mathrm{out}}$ has minimum degree k and maximum degree

$$\frac{\log n}{\log\log n}\left(1 + \frac{\log\log\log n}{\log\log n} + \frac{1 + \log k + o(1)}{\log\log n}\right).$$

3.7 Write B_p and B_M for random graphs from $\mathscr{G}\{K(n,n), p\}$ and $\mathscr{G}\{K(n,n), M\}$. Show that if $x \in \mathbb{R}, p(n) = \{\log n + k \log\log n + x + o(1)\}/n$ and $M(n) = (n/2)\{\log n + k \log\log n + x + o(1)\}$, then

$$\lim_{n\to\infty} P\{\delta(G_p) = k\} = \lim_{n\to\infty} P\{\delta(G_M) = k\} = 1 - \mathrm{e}^{-2\mathrm{e}^{-x}/k!}$$

and

$$\lim_{n\to\infty} P\{\delta(G_p) = k+1\} = \lim_{n\to\infty} P\{\delta(G_M) = k+1\} = \mathrm{e}^{-2\mathrm{e}^{-x}/k!}.$$

3.8 Prove that Corollary 3.14 is best possible: if almost all G_p's have about the same maximal degree, then $pn/\log n \to \infty$.

3.9 Show that if $(pn - \log n)/\log\log n \to \infty$, then there is a function $d(n) \to \infty$ such that $\delta(G_p) = \{1 + o(1)\}d(n)$ almost surely. [Note that $d(n)$ need not be pn.]

3.10 Let V_1, V_2, ..., V_t be disjoint copies of $V = \{1, 2, \ldots, n\}$. Select N elements of $\bigcup_{k=1}^{t} V_k^{(2)}$ at random and join i to j by as many edges as the number of copies of ij have been selected. Denote by $G_{t,n}$ the *random multigraph* obtained in this way and let $G_{s,t,N}$ be the graph in which i is joined to j iff in $G_{t,N}$ they are joined by at least s edges. Use the connection between G_N and G_p to prove that if $N = \frac{1}{2}n^{2-1/s}t\left[\{\log n + c + o(1)\}/\binom{t}{s}\right]^{1/s}$, then the distribution of the number of isolated vertices of $G_{s,t,N}$ tends to $P(\mathrm{e}^{-c})$. (Godehardt, 1980, 1981.)

4

Small Subgraphs

Given a fixed graph F, what is the probability that a r.g. G_p (or G_M) contains F? The present chapter is devoted to a thorough examination of this question.

The degree sequence of a graph $G \in \mathscr{G}^n$ depends only on the number of edges in the sets $V_i^{(2)} = \{ij : 1 \leq j \leq n, j \neq i\} \subset V^{(2)}$, $i = 1, \ldots, n$. Our job in the previous chapter was made fairly easy by the fact that these subsets $V_i^{(2)}$ are not very numerous and not very large (there are n of them, each of size $n - 1$) and that they are essentially disjoint (any two of them have one element in common). The property of containing a fixed graph F has similar advantages: it depends on the edge distribution in fairly few, fairly small and essentially independent subsets of $V^{(2)}$.

Erdős and Rényi (1959, 1960, 1961*a*) were the first to study the appearance of small subgraphs; further results were obtained by Schürger (1979*b*), Bollobás (1981*d*), Palka (1982) and Barbour (1982). In the first section we shall study a rather special class of subgraphs. As a corollary of the results, in the second section we shall determine the threshold function for the existence of an arbitrary subgraph F. It will turn out that the threshold function depends only on the maximum of the average degrees of the subgraphs of F. The third section is devoted to the case when a r.g. is likely to contain many copies of our graph F. The first two sections are based on Bollobás (1981*d*), the third section contains results from Barbour (1982).

The study of the number of subgraphs in a r.g. generated by some underlying geometric structure is related to the topic of this chapter but is outside our scope (see Hafner, 1972*a*,*b*; Schürger, 1976).

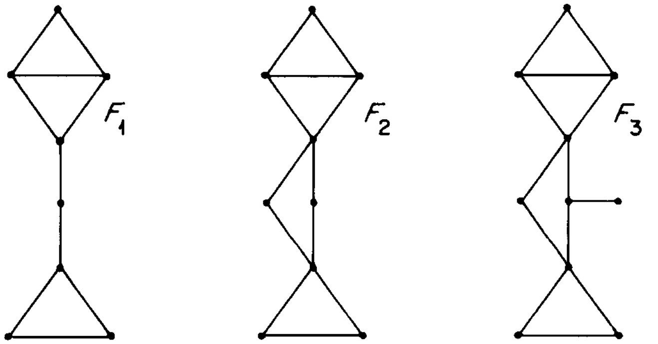


Fig. 4.1. F_1 is balanced, F_2 is strictly balanced and F_3 is not balanced.

4.1 Strictly Balanced Graphs

The *average degree* or simply *degree* of a graph F of order k and size l is $d(F) = 2l/k$. The *maximum average degree* of a graph H is defined as

$$m(H) = \max\{d(F) : F \subset H\}.$$

A graph H is *balanced* if $m(H) = d(H)$ and it is *strictly balanced* if $F \subset H$ and $d(F) = m(H)$ imply that $F = H$. Note that trees, cycles and complete graphs are strictly balanced.

It is fairly easy to determine the asymptotic distribution of the number of subgraphs isomorphic to a strictly balanced graph. The results below, from Bollobás (1981*d*), extend some theorems of Erdős and Rényi (1960). For simplicity we call a graph F an *H-graph* if $F \simeq H$. Similarly, F is an *H-subgraph* of G if $F \subset G$ and $F \simeq H$.

Theorem 4.1 *Suppose H is a fixed strictly balanced graph with k vertices and $l \geq 2$ edges, and its automorphism group has a elements. Let c be a positive constant and set $p = cn^{-k/l}$. For $G \in \mathcal{G}(p)$ denote by $X = X(G)$ the number of H-subgraphs of G. Then $X \xrightarrow{d} P(c^l/a)$, that is, for $r = 0, 1, \ldots$ we have*

$$\lim_{n\to\infty} P_p(X = r) = e^{-\lambda}\lambda^r/r!,$$

where $\lambda = c^l/a$.

Proof Note first that

$$E(X) = \binom{n}{k}\frac{k!}{a}p^l \sim \frac{n^k}{a}p^l = \frac{c^l}{a} = \lambda. \tag{4.1}$$

Indeed, there are $\binom{n}{k}$ ways of selecting the k vertices of an H-graph from $V = \{1, 2, \ldots, n\}$ and then there are $k!/a$ ways of choosing the edges of an H-graph with a given vertex set. The probability of selecting l given edges is p^l.

By Theorem 1.20 it suffices to show that for every fixed r, $r = 0, 1, \ldots,$ the rth factorial moment $E_r(X)$ of X tends to λ^r as $n \to \infty$.

Now let us estimate $E_r(X)$, the expected number of ordered r-tuples of H-graphs. Denote by $E_r'(X)$ the expected number of ordered r-tuples of H-graphs having disjoint vertex sets $V_1, V_2, \ldots, V_r$. Then, clearly,

$$E_r'(X) = \binom{n}{k}\binom{n-k}{k}\cdots\binom{n-(r-1)k}{k}\left(\frac{k!}{a}\right)^r p^{rl} = \frac{(n)_{rk}}{a^r}p^{rl} \sim \lambda^r. \quad (4.2)$$

Therefore all we need is that $E_r''(X) = E_r(X) - E_r'(X) = o(1)$. This will follow from the fact that H is strictly balanced.

Suppose the graphs A and B are such that B is an H-graph and it has exactly t vertices not belonging to A. If $0 < t < k$, then

$$e(A \cup B) \geq e(A) + tl/k + 1/k. \quad (4.3)$$

Indeed, since H is strictly balanced, fewer than $(k-t)l/k$ edges of B join its $k-t$ vertices in $V(A) \cap V(B)$.

Let $H_1, H_2, \ldots, H_r$ be H-graphs with $|\bigcup_{i=1}^r V(H_i)| = s < rk$. Suppose H_j has t_j vertices not belonging to $\bigcup_{i=1}^{j-1} H_i$, so that $\sum_{j=2}^r t_j = s - k$. We assume that $0 < t_2 < k$, so by (4.3)

$$e(H_1 \cup H_2) \geq l + \frac{t_2 l}{k} + \frac{1}{k}.$$

Since also

$$e\left(\bigcup_{i=1}^{j} H_i\right) \geq e\left(\bigcup_{i=1}^{j-1} H_i\right) + t_j l/k,$$

we have

$$e\left(\bigcup_{i=1}^{r} H_i\right) \geq \frac{sl}{k} + \frac{1}{k}.$$

Consequently, counting rather crudely, for $r \geq 2$ we have

$$\begin{aligned} E_r''(X) &\leq \sum_{s=k}^{kr-1} \binom{n}{s}\left\{\binom{s}{k}\frac{k!}{a}\right\}^r p^{sl/k+1/k} \\ &= \sum_{s=k}^{kr-1} O(n^s p^{sl/k+1/k}) = \sum_{s=k}^{kr-1} O(n^{-1/l}). \end{aligned} \quad (4.4)$$

In particular, $E_r''(X) = o(1)$, so the result follows. □

Because of Theorem 2.2, the result above implies the corresponding assertion about the model $\mathcal{G}\{n, M(n)\}$.

Corollary 4.2 *Let H, k, l, a, c and X be as in Theorem 4.1 and let $M(n) \sim (c/2)n^{2-k/l}$. Then*

$$\lim_{n\to\infty} P_M(X = r) = \mathrm{e}^{-\lambda}\lambda^r/r!$$

for every r, $r = 0, 1, \ldots$.

Proof Let $0 < c_1 < c < c_2$ and $p_i = c_i n^{-k/l}$, $i = 1, 2$. Since $X(G) \le X(G')$ whenever $G \subset G'$,

$$P_{p_1}(X \ge r) \le P_M(X \ge r) \le \{1 + o(1)\}P_{p_2}(X \ge r).$$

Hence the result follows from Theorem 4.1 if we recall that c_1 and c_2 are arbitrary numbers satisfying $0 < c_1 < c < c_2$. □

The conditions in Theorem 4.1 can be weakened to include the case when H depends on n but k and l grow rather slowly with n.

Theorem 4.3 *The conclusions of Theorem 4.1 hold if H, k, l, a and c depend on n, provided*

$$c^l/a \sim \lambda$$

for some positive constant λ and for every $r \in \mathbb{N}$ we have

$$k^{rkl} = o(n).$$

Proof All we have to check is that $E'_r \sim \lambda^r$ and $E''_r = o(1)$ continue to hold. The first is immediate:

$$E'_r = \binom{n}{k}\binom{n-k}{k}\cdots\binom{n-(r-1)k}{k}\left(\frac{k!}{a}\right)^r p^{rl}$$

so

$$(c^l/a)^r \ge E'_r \ge (c^l/a)^r\left(\frac{n-rk}{n}\right)^{rk} \ge (c^l/a)^r\left(1 - \frac{r^2k^2}{n}\right) = \{1+o(1)\}(c^l/a)^r.$$

To see the second, recall that

$$\begin{aligned} E''_r &\le \sum_{s=k+1}^{rk-1}\binom{n}{s}\left\{\binom{s}{k}\frac{k!}{a}\right\}^r p^{sl/k+1/k} \\ &\le \sum_{s=k+1}^{rk-1}(s!/a)^r cn^{-1/l} \le c(rk)^{r^3k}n^{-1/l}. \end{aligned}$$

By the conditions this is $o(1)$. □

It is worth noting that although $c = c(n)$ is no longer a constant, it is not far from being one, so the order of p is still about $n^{-k/l}$ and the order of M is about $n^{2-k/l}$. Indeed, if λ is a constant and

$$c(n) = (\lambda a)^{1/l},$$

then since $1 \le a \le k!$, for large k we have

$$\frac{1}{2} < c(n) < k^{k/l}.$$

The main condition in Theorem 3 is satisfied if k grows rather slowly with n.

Corollary 4.4 *The conclusions of Theorem 4.1 and Corollary 4.2 hold if H, k, l, a and c depend on n, provided $c^l/a \sim \lambda$ for some positive constant λ and*

$$k = O\{(\log n)^{1/4}\}.$$

Although the results above concern subgraphs which need be neither induced nor disjoint, in fact the subgraphs we get are almost surely disjoint induced subgraphs.

Corollary 4.5 *Let H, k, l, a, c and λ be as in Theorem 4.3 and denote by $X_d = X_d(G)$ the number of vertex disjoint induced H-graphs of G. Then for $p = cn^{-k/l}$ and $r = 0, 1, \ldots$ we have*

$$\lim_{n\to\infty} P_p(X_d = r) = \mathrm{e}^{-\lambda}\lambda^r/r!.$$

Proof Denote by $Y = Y(G)$ the number of subgraphs of G having at most $2k$ vertices and degree greater than $2l/k$. Since there are only finitely many such graphs,

$$E_p(Y) = o(1).$$

Consequently a.e. $G \in \mathscr{G}(p)$ that contains exactly rH-graphs is such that its H-graphs are induced and vertex disjoint. □

If H is a tree, then the subgraphs isomorphic to H turn out to be components of G_p.

Corollary 4.6 *(i) Let H be a tree of order $k \ge 3$, let a be the order of the automorphism group of H and let $c > 0$. Then for $p = cn^{-k/(k-1)}$ a.e. G_p is such that every subgraph of G_p isomorphic to H is component of G_p. In* *particular, the number of components of G_p isomorphic to H tends to P_λ, where $\lambda = c^{k-1}/a$.*

Proof Since there are $(k+1)^{k-1}$ labelled trees of order $k+1$, the probability that G_p contains a tree of order $k+1$ is at most

$$\binom{n}{k+1}(k+1)^{k-1}p^k = O(n^{-1/(k-1)}). \qquad \square$$

Corollary 4.7 *Let $k \geq 3$ be fixed, $c > 0$, $p = cn^{-k/(k-1)}$ and $\lambda = c^{k-1}k^{k-2}/k!$ Denote by X the number of trees of order k in G_p, by C the number of components of G_p with k vertices and by T the number of isolated spanned trees of order k. Then $X \xrightarrow{d} P_\lambda$, $C \xrightarrow{d} P_\lambda$, $C \xrightarrow{d} P_\lambda$ and $P(X = C = T) \to 1$.*

The proof of Theorem 4.1 and Theorem 1.21 imply easily that if $H_1, \ldots, H_m$ are non-isomorphic strictly balanced graphs having the same (average) degree then in an appropriate range of p the multiplicities of the H_i's are asymptotically independent Poisson r.vs. The easy proof is left as an exercise.

Theorem 4.8 *Let $H_1, \ldots, H_m$ be strictly balanced graphs. Suppose H_i has k_i vertices, $l_i \geq 2$ edges, and the automorphism group has a_i elements. Denote by $X_i = X_i(G)$ the number of subgraphs of G isomorphic to H_i. If the H_i's have the same average degree, say $2k_1/l_1 = \ldots = 2k_m/l_m = 2k/l$, c is a positive constant and $p \sim cn^{-k/l}$, then*

$$(X_1, \ldots, X_m) \xrightarrow{d} (P_{\lambda_1}, \ldots, P_{\lambda_m}),$$

where $\lambda_i = c^{l_i}/a_i$, that is

$$P(X_1 = s_1, \ldots, X_m = s_m) \to \prod_{i=1}^{m} \mathrm{e}^{-\lambda_i}\lambda_i^{s_i}/s_i!$$

for all $s_i \geq 0, \ldots, s_m \geq 0$.

Since cycles are strictly balanced and have average degree 2, we have the following corollary.

Corollary 4.9 *Denote by $X_i = X_i(G)$ the number of i-cycles of G. If $c > 0$ and $p \sim c/n$ then*

$$P(X_3, \ldots, X_m) \xrightarrow{d} (P_{\lambda_3}, \ldots, P_{\lambda_m}),$$

where $\lambda_i = c^i/2i$.

Proof The automorphism group of a cycle of length i has order $2i$. □

It is interesting to contrast this corollary with Corollary 2.19, giving the distribution of short cycles in regular graphs. In many ways a random r-regular graph is rather close to a random graph with $rn/2$ edges and to a random graph with probability r/n of an edge. However, in $\mathcal{G}_{r-\mathrm{reg}}$ the number of i-cycles has asymptotically Poisson distribution with mean $(r-1)^i/2i$, while in the latter two models the mean tends to $r^i/2i$. The condition of regularity makes the appearance of short cycles less likely.

The formulae in the proof of Theorem 4.1 tell us that $E(X)^r$ is a fairly good approximation of $E_r(X)$. Therefore, in a suitable range of p, Theorem 1.22 enables us to deduce normal convergence. The result below is an extension of a theorem of Schürger (1979*b*), who proved the result for complete subgraphs.

Theorem 4.10 *Let H and $X = X(G)$ be as in Theorem 4.1. Suppose $p = p(n)$ is such that*

$$pn^{k/l} \to \infty$$

and

$$pn^{k/l-\varepsilon} \to 0$$

for every $\varepsilon > 0$. Then

$$(X - \lambda_n)/\sqrt{\lambda_n} \xrightarrow{d} N(0,1),$$

where $\lambda_n = (n)_k p^l/a$.

Proof By (4.1) the expectation of X is exactly λ_n. The conditions on p imply that $\lambda_n \to \infty$ and $\lambda_n = o(n^\varepsilon)$ for every $\varepsilon > 0$. We wish to apply Theorem 1.22 to obtain normal convergence, so to prove our theorem it suffices to show that

$$E_r(X)/\lambda_n^r = 1 + o(\lambda_n^{-t}) \tag{4.5}$$

for all $r, t \in \mathbb{N}$.

Let r and t be fixed natural numbers and $\varepsilon > 0$. By (4.2) we have

$$E_r'(X) = \lambda_n^r (n)_{rk} \{(n)_k\}^{-r} = \lambda_n^r (1 - \varepsilon_n) \tag{4.6}$$

where

$$0 < \varepsilon_n < (rk)^2/n = o(\lambda_n^{-t}). \tag{4.7}$$

Furthermore, by (4.4),

$$\begin{aligned}
E_r''(X)/\lambda_n^r &\leq p^{1/k} \sum_{s=k}^{rk-1} n^s \left(\frac{(s)_k}{a}\right)^r p^{sl/k} \Big/ \left(\frac{(n)_k}{a} p^l\right)^r \\
&= p^{1/k} \sum_{s=k}^{rk-1} \frac{n^s}{(n-rk)^{rk}} s^{rk} p^{(s/k-r)l} \\
&\leq 2p^{1/k} \sum_{s=k}^{rk-1} n^{s-rk} s^{rk} p^{(s/k-r)l} \\
&\leq 4p^{1/k} \sum_{s=k}^{rk-1} \lambda_n^{s/k-r} a^{s/k-r} s^{rk} = O(p^{1/k}\lambda_n^r) \\
&= o(\lambda_n^{-t}). \qquad (4.8)
\end{aligned}$$

Since $E_r(X) = E_r'(X) + E_r''(X)$, relation (4.5) follows from (4.6), (4.7) and (4.8). □

In §3 we shall prove a considerably stronger result about Poisson approximation.

4.2 Arbitrary Subgraphs

If H is not strictly balanced, the distribution of the number of H-subgraphs is less straightforward. In order to gain some insight into the general case, we shall introduce a certain rather simple decomposition of a graph called a *grading*, whose definition is a little cumbersome.

Suppose H is a proper spanned subgraph of F with F having k more vertices and l more edges than H. Then we define the *additional degree of F over H* as $d(F|H) = 2l/k$. The *maximal additional degree of F over H* is

$$m(F|H) = \max\{\mathrm{d}(F'|H) : H \subset F' \subset F, V(H) \neq V(F')\}.$$

To define a grading of a graph F we proceed as follows. Let F_1 be a minimal subgraph of F with $d(F_1) = m(F)$. Suppose we have defined subgraphs $F_1 \subset F_2 \subset \ldots \subset F_k$. If $F_k = F$ we terminate the sequence. Otherwise let F_{k+1} be a subgraph of F with $V(F_k) \subset V(F_{k+1})$, $V(F_{k+1}) \neq V(F_k)$, such that $d(F_{k+1}|F_k) = m(F|F_k)$. This increasing sequence of subgraphs has to end after finitely many terms, say in $F_s = F$. Then we call $(F_1, F_2, \ldots F_s)$ a *grading* of F. For example, the graph F of Fig. 4.2 has grading (F_1, F_2, F_3), where F_1 is spanned by the vertices 1,2,3,4, F_2 is spanned by the vertices $1, 2, \ldots, 9$ and $F_3 = F$.

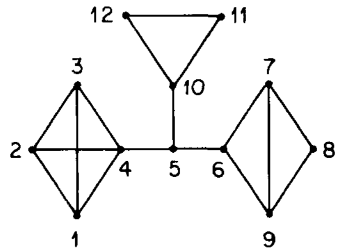


Fig. 4.2. A graph F with $m(F) = 3$ and $d(F) = 17/6$.

Note that we have

$$d(F_1) = m(F) \geq d(F_2|F_1) \geq d(F_3|F_2) \geq \ldots \geq d(F_s|F_{s-1}).$$

In order to find an F-subgraph of a random graph G, we shall consider a grading $(F_1, F_2, \ldots, F_s)$ of F. We shall find a copy of F_1 in G, then a copy of F_2 containing the copy of F_1, and so on. We shall need a technical lemma enabling us to find a copy of F_{i+1}, provided we have found a copy of F_i.

To simplify the notation let F_0 be a spanned subgraph of a graph F such that F has $k \geq 1$ more vertices and l more edges than F_0. Suppose F is the only subgraph of F with maximal additional degree over $F_0 : m(F|F_0) = d(F|F_0) = 2l/k$.

Lemma 4.11 *Let* $V = V_1 \cup V_2$, $V_1 \cap V_2 = \emptyset$, $|V_2| = m(n) \to \infty$ *and* $pm^{k/l} \to \infty$, *and let* $\widetilde{F}_0$ *be a fixed graph isomorphic to* F_0 *with* $V(\widetilde{F}_0) \subset V_1$. *Then*

$$\lim_{n\to\infty} P(G \supset H \supset \widetilde{F}_0 \textit{ for some } H \simeq F | G[V_1] \supset \widetilde{F}_0) = 1.$$

Proof Let us fix a graph $G_1 \supset \widetilde{F}_0$ with $V(G_1) = V_1$. It suffices to show that

$$\lim_{n\to\infty} P(G \supset H \supset \widetilde{F}_0 \text{ for some } H \simeq F | G[V_1] = G_1) = 1,$$

so in the proof we shall take everything conditional on $G[V_1] = G_1$. Denote by $Y = Y(G)$ the number of F-graphs H in G such that $H \supset \widetilde{F}_0$, $V(H) - V(\widetilde{F}_0) \subset V_2$ and there is an isomorphism between H and F carrying $\widetilde{F}_0$ into F_0. The (conditional) expectation of Y is clearly

$$E(Y) = c\binom{m}{k} p^l = \mu,$$

where $c \geq 1$ depends only on the pair (F, F_0). Since $pm^{k/l} \to \infty$, we have $\mu \to \infty$ as $m \to \infty$.

Let us give an upper bound for the second factorial moment $E_2(Y)$, that is for the expected number of ordered pairs (H_1, H_2) of appropriate H-graphs. Denote by $E_2'(Y)$ the expected number of pairs (H_1, H_2) with $V(H_1) \cap V(H_2) = V(\widetilde{F}_0)$ and set $E_2''(Y) = E_2(Y) - E_2'(Y)$. Clearly

$$E_2'(Y) = c^2 \binom{m}{k} \binom{m-k}{k} p^{2l} \leq \mu^2.$$

Furthermore, as in the proof of Theorem 4.1, if $H_1 \cup H_2$ has $s \leq 2k-1$ more vertices than $\widetilde{F}_0$, then $H_1 \cup H_2$ has at least $sl/k + 1/k$ more edges than $\widetilde{F}_0$. Consequently the following crude estimate holds:

$$\begin{aligned} E_2''(Y) &\leq c_1 \sum_{s=k}^{2k-1} m^s p^{sl/k+1/k} \\ &\leq c_2 \mu^2 \sum_{s=k}^{2k-1} m^{s-2k} p^{sl/k+1/k-2l} \\ &\leq c_3 \mu^2 m^{-1} p^{(2k-1)l/k+1/k-2l} \\ &= c_3 \mu^2 m^{-1} p^{-(l-1)k} = o(\mu^2). \end{aligned}$$

Here c_1, c_2 and c_3 depend only on F and F_0, and the inequalities hold if m is large enough. Thus

$$E_2(Y) = \{1 + o(1)\}\mu^2$$

and

$$E(Y^2) = \{1 + o(1)\}\mu^2.$$

By Chebyshev's inequality we have

$$P(Y = 0) = o(1),$$

completing the proof. □

This lemma enables us to prove the following extension of Theorem 4.1.

Theorem 4.12 *Suppose the graph F has a unique subgraph F_1 with $d(F_1) = m(F) = 2l/k$, where $k = |F_1|$ and $l = e(F_1) \geq 2$. Let $p \sim cn^{-k/l}$, where c is a positive constant and denote by $Y = Y(G)$ the number of F_1-graphs contained in F-graphs of $G \in \mathcal{G}(p)$. Then $Y \xrightarrow{d} P(\lambda)$, where $\lambda = c^l/a$ and a is the order of the automorphism of F_1.*

In particular, the probability that a r.g. G_p contains at least one F-graph tends to $1 - e^{-\lambda}$.

Proof Let $(F_1, F_2, \ldots, F_s)$ be a grading of F, say with F_i having k_i more vertices and l_i more edges than F_{i-1}. By assumption $l/k > l_2/k_2 \geq l_3/k_3 \geq \ldots \geq l_s/k_s$. Let $0 < \varepsilon < 1/s$ and set $c_\varepsilon = \{1-(s-1)\varepsilon\}^{k/l}$, $\lambda_\varepsilon = c_\varepsilon^l/a$. Partition V into disjoint sets $V_1, V_2, \ldots, V_s$ such that

$$n_1 = |V_1| \sim \{1-(s-1)\varepsilon\}n \text{ and } n_i = |V_i| \sim \varepsilon n, \quad i = 2, 3, \ldots, s.$$

Note that $p \sim c_\varepsilon n_1^{-k/l}$, so by Corollary 4.5

$$P(G[V_1] \text{ contains exactly } r \text{ disjoint } F_1\text{-graphs}) \sim e^{-\lambda_\varepsilon}\lambda_\varepsilon^r/r!.$$

Since $pn_i^{-k_i/l_i} \to \infty$ for $i = 2, 3, \ldots, s$, for every fixed F_1-graph $\widetilde{F}_1$ with vertex set in V_1 we have

$$P(G[V_1 \cup V_2] \supset H \supset \widetilde{F}_1 \text{ for some } H \simeq F_2 | G[V_1] \supset \widetilde{F}_1) \sim 1.$$

Similarly, if $\widetilde{F}_i$ is a fixed F_i-graph whose vertex set is contained in $\bigcup_{j=1}^i V_j$, then

$$P\left(G\left[\bigcup_{j=1}^{i+1} V_j\right] \supset H \supset \widetilde{F}_i \text{ for some } H \simeq F_{i+1} \,\middle|\, G\left[\bigcup_{j=1}^{i} V_j\right] \supset \widetilde{F}_i\right) \sim 1.$$

Hence almost every graph containing r disjoint F_1-graphs contains r F-graphs whose F_1-subgraphs are disjoint. Therefore

$$\varliminf_{n\to\infty} P(Y \geq r) \geq e^{-\lambda_\varepsilon} \sum_{j=r}^{\infty} \lambda_\varepsilon^j/j!.$$

Letting ε tend to 0 this gives

$$\varliminf_{n\to\infty} P(Y \geq r) \geq e^{-\lambda} \sum_{j=r}^{\infty} \lambda^j/j!, \tag{4.9}$$

since $\lambda_\varepsilon \to \lambda$ as $\varepsilon \to 0$.

On the other hand, if $X = X(G)$ is the number of F_1-subgraphs of G, then by Theorem 4.1

$$\lim_{n\to\infty} P(X \geq r) = e^{-\lambda} \sum_{j=r}^{\infty} \lambda^j/j!. \tag{4.10}$$

As $Y(G) \leq X(G)$ for every graph G, relations (4.9) and (4.10) imply

$$\lim_{n\to\infty} P(Y \geq r) = e^{-\lambda} \sum_{j=r}^{\infty} \lambda^j/j!,$$

so $Y \xrightarrow{d} P(\lambda)$, as claimed. □

In the result above we cannot discard the condition that F_1 is the unique subgraph of maximal average degree. For example, if $F = 2K^3$, that is F is a disjoint union of two triangles and $X(G)$ is the number of F-graphs in G, then with $p = c/n$ we have

$$\lim_{n\to\infty} P(X = s) = \begin{cases} e^{-\lambda}\lambda^r/r!, & \text{if } s = \binom{r}{2}, \\ 0, & \text{otherwise,} \end{cases}$$

where $\lambda = c^3/6$. However, given an arbitrary graph F, one can determine the rough order of p that guarantees that a.e. $G \in \mathcal{G}(p)$ contains F.

Theorem 4.13 *Let F be an arbitrary fixed graph with maximal average degree $2l/k > 0$. Then*

$$\lim_{n\to\infty} P_p(G \supset F) = \begin{cases} 0, & \text{if } pn^{k/l} \to 0, \\ 1, & \text{if } pn^{k/l} \to \infty. \end{cases}$$

Proof Suppose first that $pn^{k/l} \to \infty$. Let $F_1 \subset F_2 \subset \ldots \subset F_s$ be a grading of F. Partition V as $V = \bigcup_{i=1}^s V_i$ where $n_i = |V_i| \sim n/s$, $i = 1,\ldots,s$. Then $pn_1^{k/l} \to \infty$, so by Theorem 4.1

$$\lim_{n\to\infty} P(G[V_i] \supset F_1) = 1. \tag{4.11}$$

Furthermore, by Lemma 4.11,

$$\lim_{n\to\infty} P\left(G\left[\bigcup_{i=1}^{j+1} V_i\right] \supset F_{j+1} \,\middle|\, G\left[\bigcup_{i=1}^{j} V_i\right] \supset F_j \right) = 1. \tag{4.12}$$

Relations (4.11) and (4.12) imply

$$\lim_{n\to\infty} P(G \supset F_s) = 1.$$

On the other hand, if $pn^{k/l} \to 0$ then, again by Theorem 4.1,

$$\overline{\lim_{n\to\infty}}\, P(G \supset F) \le \overline{\lim_{n\to\infty}}\, P(G \supset F_1) = 0.$$

□

Recalling the close connection between $\mathcal{G}_p$ and $\mathcal{G}_{\lfloor pN \rfloor}$, Theorem 13 gives us the threshold function.

Corollary 4.14 *The threshold function of the property of containing a fixed non-empty graph F is $n^{2-2/m}$, where $m = m(F)$.* □

The approach taken above is somewhat of an overkill: the grading allows us to deduce much about the distribution of H-subgraphs of random graphs. However, if our aim is to prove Theorem 4.13 then, as shown by Ruciński and Vince (1985), one can proceed in a *much* simpler way. To present this elegant proof of Ruciński and Vince, write $X_H(G)$ for the number of H-subgraphs of a graph G, and for a non-empty graph F define

$$\Phi_F(n, p) = \min\{E_p(X_H(G_p)) : H \subset F, e(H) > 0\}.$$

A moment's thought tells us that

$$\Phi_F(n, p) \asymp \min\{n^{|H|}p^{e(H)} : H \subset F, e(H) > 0\},$$

and so $\Phi_F(n, p) \to \infty$ iff $np^{m(F)/2} \to \infty$.

More importantly, Ruciński and Vince (1985) showed that

$$\sigma^2(X_F) \asymp (1-p)\frac{(EX_F)^2}{\Phi_F},$$

where the constants implicit in $\asymp$ depend on F but not on n or p.

Now, to deduce the essential part of Theorem 4.13, note that if $np^{m(F)/2} \to \infty$ then

$$P_p(G_p \not\supset F) = P_p(X_F = 0) \leq \frac{\sigma^2(X_F)}{(E(X_F))^2} \asymp \frac{1}{\Phi_F} \to 0,$$

so a.e. G_p has an F-subgraph, as claimed. Karoński and Ruciński (1983) proposed yet another way of proving Theorem 4.13. They conjectured that every graph F can be extended to a *balanced* graph H with the some maximal average degree: there is a balanced graph H containing F with $m(H) = m(F)$. Combined with the result of Erdős and Rényi (1960) that Theorem 13 holds for balanced graphs, the conjecture implies Theorem 13. This conjecture of Karoński and Ruciński was proved by Győri, Rothschild and Ruciński (1985) and Payan (1986). In fact, it need not be very easy to find an appropriate balanced extension: Ruciński and Vince (1993) showed that the balanced extension may have to have many more vertices than the original graph.

The appearance of F-subgraphs in random graphs was studied in great detail by Janson, Łuczak and Ruciński (1990). Among other results, they proved the following beautiful inequality involving the probability $P_p(G_p \not\supset F)$ and the function $\Phi_F(n, p)$.

Theorem 4.15 *Let F be a fixed non-empty graph and, as before, set*

$\Phi_F(n,p) = \min\{E_p(X_H(G_p)) : H \subset F, e(H) > 0\}$. *Then*

$$e^{-\Phi_F/(1-p)} \le P_p(G_p \not\supset F) \le e^{-c\Phi_F}$$

for some positive constant $c = c_F$. □

The real content of this theorem is the upper bound; it can be proved by making use of the martingale inequality given in Theorem 1.20. For a sketch of this proof and many other beautiful results about small subgraphs of random graphs, see Chapter III of Janson, Łuczak and Ruciński (2000).

4.3 Poisson Approximation

Let us return to the study of strictly balanced subgraphs of random graphs. Our aim is to approximate the distribution of the number of subgraphs isomorphic to a fixed strictly balanced graph. In §1 we gave such approximations and found our task fairly easy provided the expectation is bounded or grows rather slowly with n. In this section we shall present a theorem of Barbour (1982) which is considerably stronger than the results of §1, and permits much faster growth of the expectation.

Theorem 4.16 *Suppose H is a fixed strictly balanced graph with k vertices, $l \ge 2$ edges and with a elements in its automorphism group. Denote by $Y = Y(G_p)$ the number of H-subgraphs of G_p.*

Suppose that

$$\lambda_n = \frac{(n)_k}{a} p^l \to \infty$$

and

$$p = o(n^{-k/\{l+1/(k-2)\}}).$$

Then the total variation distance between the distribution of Y and P_{λ_n} tends to 0, in fact

$$d\{\mathcal{L}(Y), P_{\lambda_n}\} = O(n^{k-2}p^{(k-2)l/k+1/k}) = o(1). \tag{4.13}$$

Proof Let $\mathcal{H}$ be the collection of all H-graphs whose vertex set is contained in V. Then

$$|\mathcal{H}| = \binom{n}{k}\frac{k!}{a} = \frac{(n)_k}{a}$$

and

$$E(Y) = |\mathcal{H}|p^l = \lambda_n.$$

With a slight abuse of notation the elements of $\mathscr{H}$ will be denoted by $\alpha, \beta, \ldots$.

For $\alpha \in \mathscr{H}$ and $G_p \in \mathscr{G}_p$ set

$$X_\alpha = X_\alpha(G_p) = \begin{cases} 1, & \text{if } \alpha \subset G_p, \\ 0, & \text{otherwise}. \end{cases}$$

so that $Y = \sum_\alpha X_\alpha$, where the summation is over $\mathscr{H}$. Furthermore, put

$$Y_\alpha = \sum_{\beta \cap \alpha = \emptyset} X_\beta,$$

where $\beta \cap \alpha$ denotes the set of common edges of the graphs β and α, and the summation is over all elements β of $\mathscr{H}$ satisfying $\beta \cap \alpha = \emptyset$. Finally, let us write p_α for $E(X_\alpha) = p^l$.

Our aim is to apply Theorem 1.28 of Chapter 1 to estimate the total variation distance between the distribution of Y and the Poisson distribution. The following identity, valid for all functions $x : \mathbb{Z}^+ \to \mathbb{R}$, will enable us to estimate the left-hand side of the equation appearing in Theorem 1.28(iii):

$$\begin{aligned} \lambda_n x(Y+1) - Yx(Y) \; = \; & \sum_\alpha p_\alpha \{x(Y+1) - x(Y_\alpha + 1)\} \\ & + \sum_\alpha (p_\alpha - X_\alpha) x(Y_\alpha + 1) \\ & + \sum_\alpha X_\alpha \{x(Y_\alpha + 1) - x(Y)\}. \qquad (4.14) \end{aligned}$$

Now let A be an arbitrary subset of $\mathbb{Z}^+$ and let $x = x_A = x_{\lambda,A}$ be the function defined in Theorem 1.28. Since $Y = Y_\alpha + \sum_{\beta \cap \alpha \neq \emptyset} X_\beta$,

$$|x(Y+1) - x(Y_\alpha + 1)| \leq (\Delta x) \sum_{\beta \cap \alpha \neq \emptyset} X_\beta. \qquad (4.15)$$

Furthermore, if $X_\alpha = 1$ then

$$0 \leq Y - Y_\alpha - 1 = \sum_{\substack{\beta \cap \alpha \neq \emptyset \\ \beta \neq \alpha}} X_\beta,$$

so

$$|X_\alpha \{x(Y_\alpha + 1) - x(Y)\}| \leq (\Delta x) X_\alpha \sum_{\substack{\beta \cap \alpha \neq \emptyset \\ \beta \neq \alpha}} X_\beta. \qquad (4.16)$$

Let us take the expectation of (4.14). Then (4.15), (4.16) and the independence of X_α and Y_α imply that

$$\begin{aligned}|E\{\lambda_n x(Y+1)-Yx(Y)\}| &\le \sum_\alpha p_\alpha(\Delta x)E\left\{\sum_{\beta\cap\alpha\neq\emptyset} X_\beta\right\}\\ &\quad+(\Delta x)\sum_\alpha E\left\{\sum_{\substack{\beta\cap\alpha\neq\emptyset\\ \beta\neq\alpha}} X_\alpha X_\beta\right\}\\ &\le (\Delta x)\left\{\sum_\alpha\sum_{\beta\cap\alpha\neq\emptyset} p_\alpha p_\beta+\sum_\alpha\sum_{\substack{\beta\cap\alpha\neq\emptyset\\ \beta\neq\alpha}} E(X_\alpha X_\beta)\right\}.\end{aligned} \tag{4.17}$$

If $\beta\cap\alpha\neq\emptyset$, then $|V(\beta)\cap V(\alpha)|\ge 2$ so the deduction of relation (4.4) implies

$$\sum_\alpha\sum_{\substack{\beta\cap\alpha\neq\emptyset\\ \beta\neq\alpha}} E(X_\alpha X_\beta)=0\left(\sum_{s=k+1}^{2k-2} n^s p^{sl/k+1/k}\right).$$

Since $n^k p^l\to\infty$, the sum above is

$$O(n^{2k-2}p^{(2k-2)l/k+1/k}). \tag{4.18}$$

Also,

$$\begin{aligned}\sum_\alpha\sum_{\beta\cap\alpha\neq\emptyset} p_\alpha p_\beta &= 0(|\mathscr{H}|p^l n^{k-2}p^l)=O(n^{2k-2}p^{2l})\\ &= O(n^{2k-2}p^{(2k-2)l/k+1/k}).\end{aligned} \tag{4.19}$$

Therefore Theorem 1.28(ii) and relations (4.17), (4.18) and (4.19) imply

$$\begin{aligned}|E\{\lambda_n x(Y+1)-Yx(Y)\}| &\le 2\lambda_n^{-1}O(n^{2k-2}p^{(2k-2)l/k+1/k})\\ &= O(n^{k-2}p^{(k-2)l/k+1/k}).\end{aligned} \tag{4.20}$$

Since the constants hidden in the O's above are independent of the set A, Theorem 1.28(iii) and (4.20) give

$$d\{\mathscr{L}(Y),P_{\lambda_n}\}=\sup_A|E\{\lambda_n x(Y+1)-Yx(Y)\}|=O(n^{k-2}p^{(k-2)l/k+1/k}),$$

as claimed by (4.13). □

Exercises

4.1 What is the threshold function of the property of containing a cycle? And a cycle and a diagonal?

4.2 Use Theorem 1.21 to prove Theorem 4.8.

4.3 Let F be a fixed graph with maximal average degree $m > 0$. Show that if $\lim_n P(G_M \supset F) = 1$, then $M/n^{2-2/n} \to \infty$ and if $\lim_n P(G_M \supset F) = 0$, then $M/n^{2-2/m} \to 0$.

4.4 Given $\varepsilon > 0$ and $0 < x < 1$, find a first-order sentence Q and a sequence $\{M(n)\}$ such that

$$n^{2-\varepsilon} \leq M(n) \leq N/2 \text{ and } \lim_{n\to\infty} P_M(Q) = x.$$

(cf. Theorem 2.6. Let Q be the property of containing a large complete subgraph.)

4.5 Let U and W be disjoint sets with $|U| = m$, $|W| = n$. Take a random bipartite graph $B_{1/2}$ with vertex classes U, W and with probability $\frac{1}{2}$ of an edge. Given $B_{1/2}$, let $T_{n,m} = T(B_{1/2})$ be the directed bipartite graph with vertex classes U and W, in which $\vec{uw}$ is an edge if $uw \in E(B_{1/2})$, and $\vec{wu}$ is an edge if $uw \notin E(B_{1/2})$, $u \in U$, $w \in W$.

We call $T_{n,m}$ a *random bipartite tournament*. Denote by $X_{n,m} = X(T_{n,m})$ the number of oriented 4-cycles in $T_{n,m}$. Use the method of Theorem 2.15 to show that

$$\frac{8X_{n,m} - \binom{m}{2}\binom{n}{2}}{\left\{\binom{m}{2}\binom{n}{2}(2m+2n-1)\right\}^{1/2}} \to N(0,1).$$

[Moon and Moser (1962); see also Frank (1979*b*). The probability $P_{m,n}$ that a tournament contains no 4-cycle (i.e. it is acyclic) was estimated by Bollobás, Frank and Karoński (1983), who also calculated the asymptotic value of $P_{n,\lfloor cn \rfloor}$. In particular, they proved that

$$P_{n,n} \sim 2^{-n^2}(n!)^2(\log 2)^{-2n+1}\{n\pi(1-\log 2)\}^{-1/2}.$$

The estimate above is connected to the enumeration of restricted permutations and to estimates of Stirling numbers; see, for example, Lovász and Vesztergombi (1976), Szekeres and Binet (1957) and Vesztergombi (1974).]

4.6 Let T be a tree with vertex set $V(T) = \{x_1, \ldots, x_k\}$. Furthermore, let $0 < c < \infty$ and $p \sim c/n$. Write $Y = Y(G_p)$ for the number of components C of G_p such that $V(C) = \{y_1, \ldots, y_k\}$ for some $1 \leq y_1 < y_2 < \ldots < y_k \leq n$ and $x_i \rightarrow y_i$ gives an isomorphism between T and C. Prove that $E(Y) \sim \gamma_0 n$ for some $\gamma_0 > 0$ and $\sigma^2(Y) = O(n)$. Deduce that $Y(G_p) = \gamma_0 n + o(n)$ for a.e. G_p.

5

The Evolution of Random Graphs—Sparse Components

In the next two chapters we shall study the global structure of a random graph of order n and size $M(n)$. We are interested mostly in the orders of the components, especially in the maximum of the orders of the components.

The chapters contain the classical results due to Erdős and Rényi (1960, 1961*a*) and the later refinements due to Bollobás (1984*b*). Before getting down to the details, it seems appropriate to give a brief, intuitive and somewhat imprecise description of the fundamental results. Denote by $L_j(G)$ the *order of the* jth *largest component* of a graph G. If G has fewer than j components, then we put $L_j(G) = 0$. Furthermore, often we write $L(G)$ for $L_1(G)$. Let us consider our random graph G_M as a living organism, which develops by acquiring more and more edges. More precisely, consider a random graph process $\widetilde{G} = (G_t)_0^N$. How does $L(G_M)$ depend on M? If $M/n^{(k-2)/(k-1)} \to \infty$ and $M/n^{(k-1)/k} \to 0$ then a.e. G_M is such that $L(G_M) = k$. If $M = \lfloor cn \rfloor$, where $0 < c < \frac{1}{2}$, then in a.e. G_M the order of a largest component is $\log n$ but if $M = \lfloor cn \rfloor$ and $c > \frac{1}{2}$ then a.e. G_M has a unique largest component with about εn vertices, where $\varepsilon > 0$ depends only on c. (The unique largest component is usually called the *giant component* of G_M.) Furthermore, in the neighbourhood of $t = n/2$ for a.e. $\widetilde{G} = (G_t)_0^N$ the function $L(G_t)$ grows rather regularly with the time: $L(G_t)$ increases about four times as fast as t.

The present chapter is devoted to the study of components which are trees or have only a few more edges than trees. The main aim of the subsequent chapter is to examine the giant component.

5.1 Trees of Given Sizes As Components

In Chapter 4 we determined the threshold function of a given tree. If T is a tree of order k whose automorphism group has order a,

$M = M(n) \sim \frac{1}{2}cn^{2-k/(k-1)}$ for some constant $c > 0$ and X_1 denotes the number of subgraphs of a random graph G_M isomorphic to T, then $X_1 \xrightarrow{d} P(\lambda)$, where $\lambda = c^{k-1}/a$. Also, if X_2 denotes the number of trees of order k contained in a graph G_M, then $X_2 \xrightarrow{d} P(\mu)$, where $\mu = c^{k-1}k^{k-2}/k!$ Furthermore, if X_3 is the number of components of G_M that are trees of order k, then $X_3 \xrightarrow{d} P(\mu)$ also holds.

As $M(n)$ grows to become of larger order than $n^{2-k/(k-1)}$, the number of tree components of order k of a typical G_M tends to infinity with n. However, in a large range of $M(n)$ the distribution of the number of tree components of order k is still asymptotically Poisson. The proof of this beautiful theorem of Barbour (1982) is rather similar to the proof of Theorem 4.15, in particular, it is also based on Theorem 1.28. To simplify the calculation we work with the model $\mathscr{G}(n,p)$.

Let $p = p(n)$, $k = k(n)$ and denote by $T_k = T_k(G_p)$ the number of isolated trees of order k in G_p. Write λ for the expectation of T_k. As by Cayley's formula there are k^{k-2} trees with k labelled vertices,

$$\lambda = E(T_k) = \binom{n}{k} k^{k-2}p^{k-1}q^{k(n-k)+\binom{k}{2}-k+1}. \tag{5.1}$$

Theorem 5.1

$$d\{\mathscr{L}(T_k), P_\lambda\} \le 2\{c_1(n,k,p) + c_2(n,k,p)\},$$

where

$$c_1(n,k,p) = k\binom{n-1}{k-1} k^{k-2}p^{k-1}q^{k(n-k)+\binom{k}{2}-k+1} = \frac{k^2}{n}\lambda$$

and

$$\begin{aligned} c_2(n,k,p) &= k^2p\binom{n-k}{k} k^{k-2}p^{k-1}q^{k(n-2k)+\binom{k}{2}-k+1} \\ &= \frac{(n-k)_k}{(n)_k}k^2pq^{-k^2}\lambda \le \mathrm{e}^{-k^2/n}k^2pq^{-k^2}\lambda. \end{aligned}$$

Proof Let $\mathscr{F}$ be the set of all trees of order k whose vertex set is contained in V. As in the proof of Theorem 4.15, we shall use α, β, γ, ... to denote elements of $\mathscr{F}$. Furthermore, we shall frequently suppress the suffix k in T_k. For $\alpha \in \mathscr{F}$ and $G_p \in \mathscr{G}_p$ set

$$X_\alpha(G_p) = \begin{cases} 1, & \text{if } \alpha \text{ is an isolated tree of } G_p, \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$|\mathscr{F}| = \binom{n}{k} k^{k-2}, E(X_\alpha) = P(X_\alpha = 1) = p^{k-1} q^{k(n-k)+\binom{k}{2}-k+1} = \mu,$$

and

$$E(T) \equiv E(T_k) = \sum_{\alpha \in \mathscr{F}} E(X_\alpha) = \binom{n}{k} k^{k-2} \mu = \lambda.$$

Let $T^* = T^*(G_p)$ be the number of isolated trees of order k in the graph $H_p = G_p[\{1, 2, \ldots, n-k\}]$, the subgraph of G_p spanned by the vertices $1, 2, \ldots, n-k$. Then for all $x : \mathbb{Z}^+ \to \mathbb{R}$ and $\alpha \in \mathscr{F}$ we have

$$E\{X_\alpha x(T)\} = P(X_\alpha = 1) E\{x(T^* + 1)\}.$$

Hence

$$\begin{aligned} E\{\lambda x(T+1) - T x(T)\} &= \lambda E\{x(T+1)\} - \sum_\alpha E\{X_\alpha x(T)\} \\ &= \lambda E\{x(T+1)\} - \sum_\alpha P(X_\alpha = 1) E\{x(T^*+1)\}, \\ &= \lambda E\{x(T+1) - x(T^*+1)\}. \end{aligned}$$

Furthermore, since

$$|E\{x(T+1) - x(T^*+1)\}| \le (\Delta x) E(|T - T^*|),$$

we have

$$|E\{\lambda x(T+1) - T x(T)\}| \le \lambda (\Delta x) E(|T - T^*|). \tag{5.2}$$

In order to be able to apply Theorem 1.28, we need an upper bound of the right-hand side of (5.2). Clearly

$$T - T^* \le \sum_{j=n-k+1}^{n} Z_j,$$

where

$$Z_j = \begin{cases} 1, & \text{if the vertex } j \text{ is in an isolated tree of order } k \text{ in } G_p, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore

$$E\{\max(T - T^*, 0)\} \le \sum_{j=n-k+1}^{n} E(Z_j) \le k \binom{n-1}{k-1} k^{k-2} \mu = c_1(n,k,p). \tag{5.3}$$

On the other hand, $T^* - T$ is certainly not larger than the number of isolated trees of order k in H_p which are joined to some vertices among $n-k+1,\ldots,n$. Consequently

$$
\begin{aligned}
E\{\max(T^* - T, 0)\} &\le (1-q^{k^2})E(T^*) \\
&\le k^2 p \binom{n-k}{k} k^{k-2} p^{k-1} q^{k(n-2k)+\binom{k}{2}-k+1} = c_2(n,k,p).
\end{aligned}
\tag{5.4}
$$

Now let $A \subset \mathbb{Z}^+$ and let $x = x_{\lambda,A}$ be the function defined in Theorem 1.28. Then by Theorem 1.28 and relations (5.2), (5.3), (5.4) we have

$$
\begin{aligned}
|P(T \in A) - P_\lambda(A)| &\le 2\lambda \min\{1, \lambda^{-1}\}\{c_1(n,k,p) + c_2(n,k,p)\} \\
&\le 2\{c_1(n,k,p) + c_2(n,k,p)\}
\end{aligned}
$$

and so

$$d(\mathscr{L}(T_k), P_\lambda) \le 2\{c_1(n,k,p) + c_2(n,k,p)\}. \qquad \square$$

Corollary 5.2 *If* $p(n)k(n) = O(1)$ *as* $n \to \infty$, *then*

$$d\{\mathscr{L}(T_k), P_\lambda\} \to 0$$

provided any of the following three conditions is satisfied:

(i) $k(n) \to \infty$, *(ii)* $np(n) \to \infty$, *(iii)* $k(n) \ge 2$ *and* $p(n) = o(n^{-1})$.

Proof Check that the conditions imply that

$$c_1(n,k,p) + c_2(n,k,p) = o(1) \quad \text{(Ex. 2)}. \qquad \square$$

In particular, if $k \ge 2$ is fixed and $p = o(n^{-1})$, then T_k has asymptotically Poisson distribution.

As $M(n)$ continues to grow and $M(n) = o(n)$ no longer holds, then T_k ceases to be asymptotically Poisson. However, as Corollary 5.2 shows, T_k again becomes asymptotically Poisson when $M(n)/n \to \infty$. Furthermore, $E(T_k)$ becomes bounded away from both 0 and ∞ if

$$M(n) = (n/2k)\{\log n + (k-1)\log\log n + \alpha(n)\},$$

where $\alpha(n)$ is a bounded function. This can be read out of Corollary 5.2, but it is also a simple consequence of Theorem 1.20.

Theorem 5.3 *Let* $p = \{\log n + (k-1)\log\log n + x + o(1)\}/kn$, *where* $x \in \mathbb{R}$ *is fixed and denote by* T_k *the number of components in a random graph* G_p *that are trees of order* $k \ge 1$. *Then* $T_k \xrightarrow{d} P(\lambda)$, *where* $\lambda = \mathrm{e}^{-x}/(k \cdot k!)$.

Proof As by Cayley's formula there are k^{k-2} trees with k labelled vertices,

$$E_r(T_k) = \binom{n}{k}\binom{n-k}{k}\cdots\binom{n-(r-1)k}{k} \times (k^{k-2})^r p^{r(k-1)}(1-p)^{rk(n-rk)+\binom{rk}{2}-r(k-1)}.$$

Indeed, in order to guarantee that r trees of order k with disjoint vertex sets are components of a graph G_p we have to make sure that $r(k-1)$ given pairs are edges and $rk(n-rk)+\binom{rk}{2}-r(k-1)$ other pairs are non-edges.

The assumption on p implies

$$\begin{aligned} E_r(T_k) &\sim \frac{n^{rk}}{(k!)^r}k^{(k-2)r}p^{r(k-1)}(1-p)^{rkn} \\ &\sim \left(\frac{n^k}{k!}k^{k-2}p^{k-1}e^{-\log n-(k-1)\log\log n-x}\right)^r \\ &\sim \left(\frac{n^k}{k!}k^{k-2}\left(\frac{\log n}{kn}\right)^{k-1}\frac{1}{n}\frac{1}{(\log n)^{k-1}}e^{-x}\right)^r \\ &= \lambda^r. \end{aligned}$$

The result follows by Theorem 1.21. □

We can now give a complete description of the asymptotic behaviour of the number of isolated trees of order k.

Theorem 5.4 *Denote by T_k the number of components in a random graph G_p that are trees of order $k \geq 2$.*

(i) If $p = o(n^{-k/(k-1)})$, then $T_k = 0$ for a.e. G_p.

(ii) If $p \sim cn^{-k/(k-1)}$ for some constant $c > 0$, then $T_k \xrightarrow{d} P(c^{k-1}k^{k-2}/k!)$.

(iii) If $pn^{k/(k-1)} \to \infty$ and $pkn - \log n - (k-1)\log\log n \to -\infty$, then for every $L \in \mathbb{R}$ we have

$$\lim_{n\to\infty} P(T_k \geq L) = 1.$$

(iv) If $pkn-\log n-(k-1)\log\log n \to x$ for some $x \in \mathbb{R}$, then $T_k \xrightarrow{d} P\{e^{-x}/(k \cdot k!)\}$.

(v) If $pkn - \log n - (k-1)\log\log n \to \infty$, then $T_k = 0$ for a.e. G_p.

Proof Parts (i) and (ii) were proved in Chapter 4, and (iv) is Theorem 5.3, above.

To see (iii) suppose $pkn \leq 2k \log n$. Then, as in the proof of Theorem 5.3,

$$\begin{aligned} E(T_k) &\sim \frac{n^k}{k!} k^{k-2} p^{k-1} (1-p)^{kn} \\ &\sim \frac{k^{k-2}}{k!} n^k p^{k-1} \mathrm{e}^{-pkn} = \frac{k^{k-2}}{k!} n (pn\mathrm{e}^{-kpn/(k-1)})^{k-1}. \end{aligned}$$

The last expression increases as pn increases from 0 to $(k-1)/k$, and from then on it decreases as pn increases. Hence if $pn^{k/(k-1)} \to \infty$ and $pkn - \log n - (k-1)\log\log n \to -\infty$, by parts (ii) and (iv) we find that $E(T_k) \to \infty$.

Furthermore,

$$E_2(T_k) \sim \frac{n^{2k}}{(k!)^2} n^{2k} p^{2(k-1)} (1-p)^{kn} \sim E(T_k)^2,$$

so the assertion follows by the Chebyshev inequality.

If p is rather large, say $p \geq 3(\log n)/n$, then a.e. G_p is connected (Ex. 14 of Chapter 2), so $T_k = 0$ for a.e. G_p. Finally, if $pn \leq 3 \log n$ and $pkn - \log n - (k-1)\log\log n \to \infty$ then, as before,

$$E(T_k) \sim \frac{k^{k-2}}{k!} n(pn\mathrm{e}^{-kpn/(k-1)})^{k-1} \to 0,$$

implying (v). □

The proof above shows that for a fixed k the expected number of isolated trees of order k in G_p increases as p increases up to $p \sim (k-1)/kn$, and from then on it decreases. Furthermore, the maximum is about

$$\frac{(k-1)^{k-1}}{k \cdot k!\, \mathrm{e}^{k-1}} n.$$

For large values of k this is about $(1/\sqrt{2\pi})k^{-5/2}n$.

To conclude this section, we state two beautiful theorems of Barbour (1982) about approximating T_k by the normal distribution. The first result concerns the space $\mathcal{G}(n, c/n)$, the space we shall study in this chapter and the next.

Theorem 5.5 *Let $k \geq 2$ and $c > 0$ be fixed and let $p = p(n) \sim c/n$. Then*

$$\sup_x |P[(T_k - \lambda_k)/\sigma_k \leq x] - \Phi(x)| = O(n^{-1/2}),$$

where

$$\lambda_k = E(T_k) \sim nk^{k-2}c^{k-1}\mathrm{e}^{-kc}/k!$$

and

$$\sigma_k^2 = \sigma^2(T_k) \sim \lambda_n\{1 + (c-1)(kc)^{k-1}e^{-kc}/k!\}. \qquad \square$$

It is clear that for $c \neq 1$ Poisson convergence does not hold, namely $d\{\mathscr{L}(T_k), P_{\lambda_k}\} \not\to 0$.

Theorem 5.6 *For every fixed $k \geq 2$ there exists a constant $C(k)$ such that the r.v. T_k on $\mathscr{G}\{n, p(n)\}$ satisfies*

$$\sup_x |P\{(T_k - \lambda_k)/\sigma_k \leq x\} - \Phi(x)| \leq C\sigma_k^{-1}$$

if n is sufficiently large, where $\lambda_k = E(T_k)$ and $\sigma_k = \sigma(T_k)$. $\square$

5.2 The Number of Vertices on Tree Components

In the previous section we studied the distribution of trees of a given order. Our main aim in this section is to obtain information about the total number of vertices on components that are trees. This information will be crucial in the study of the order of a largest component.

Denote by T the number of vertices of G_p belonging to isolated trees: $T = \sum_{k=1}^n kT_k$. The next result shows that if $p = o(1/n)$ or $p \sim c/n$ for some $c \leq 1$, then almost all vertices belong to isolated trees, but there is an abrupt change at $p \sim 1/n$.

Theorem 5.7 *(i) If $p = o(1/n)$, then $T = n$ for a.e. G_p.*

(ii) Suppose $p = c/n$, where c is a constant.
If $0 < c < 1$, then

$$E\{T(G_p)\} = n + O(1)$$

and if $1 < c < \infty$, then

$$E\{T(G_p)\} = t(c)n + O(1),$$

where

$$t(c) = \frac{1}{c}\sum_{k=1}^{\infty} \frac{k^{k-1}}{k!}(ce^{-c})^k. \qquad \square$$

Remark. By standard but tedious manipulations one can show that the function $s = s(c) = ct(c)$ is the only solution of

$$se^{-s} = ce^{-c} \tag{5.5}$$

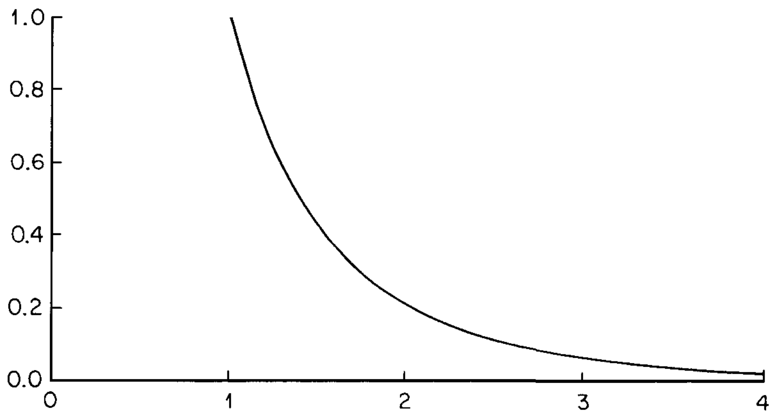


Fig. 5.1. The curve $y = t(c)$.

in the range $0 < s \leq 1$. In particular,

$$t(c) = s(c)/c = 1 \text{ for } 0 < c \leq 1 \tag{5.6}$$

and part (ii) of Theorem 5.7 states simply that

$$E(T) = t(c)n + O(1) \tag{5.7}$$

whenever $p = c/n$ and $c \neq 1$. In the proof below we shall show (5.7) instead of the assertion in part (ii).

Since $E\{T(G_p)\}$ is a continuous function of p, Theorem 5.7 implies that

$$E\{T(G_{1/n})\} = n + o(n). \tag{5.8}$$

It should be stressed that (5.8) cannot be strengthened to

$$E\{T(G_{1/n})\} = n + O(1).$$

Relation (5.6) can be shown without any analytic manipulations. It is easily seen (cf. Ex. 8) that if $p \sim c/n$ and $0 < c < 1$, then the expected number of vertices of G_p on components containing cycles is $O(1)$, so the expected number of vertices on tree components is $\{1 + o(1)\}n$. Hence if (5.7) holds as well, as we are about to show, then

$$\sum_{k=1}^{\infty} \frac{k^{k-1}}{k!}(ce^{-c})^k = c \quad \text{if} \quad 0 < c \leq 1.$$

This shows that $s = s(c) = ct(c)$ is a solution of $se^{-s} = ce^{-c}$ in $0 < s \leq 1$. It is easily seen that there is only one solution, so s is exactly this solution.

Proof of Theorem 5.7 (i) Write X_k for the number of k-cycles in G_p, where $p \le c/n$. Then

$$E(X_k) = \binom{n}{k}\frac{(k-1)!}{2}p^k \le \frac{c^k}{2k}$$

so

$$\sum_{k=3}^{\infty} E(X_k) \le \sum_{k=3}^{\infty} c^k.$$

Hence if $p = o(1/n)$, almost no G_p contains a cycle, that is a.e. G_p is a forest.

(ii) Suppose $p = c/n$ where $0 < c < \infty$ and $c \ne 1$. We shall give a particularly detailed proof of the assertion, because the proof of a slightly weaker assertion in Erdős and Rényi (1960) is based on some incorrect estimates. Clearly

$$E(T_k) = \binom{n}{k} k^{k-2}\left(\frac{c}{n}\right)^{k-1}\left(1-\frac{c}{n}\right)^{kn-k(k+3)/2+1} \tag{5.9}$$

Hence if $1 \le k \le n^{1/2}$, then

$$\begin{aligned} E(T_k) &\le n\frac{k^{k-2}}{k!}c^{k-1}e^{-ck}e^{ck^2/(2n)+3ck/(2n)} \\ &\le n\frac{k^{k-2}}{k!}c^{k-1}e^{-ck}(1+c_1k^2/n) \end{aligned} \tag{5.10}$$

and

$$\begin{aligned} E(T_k) &\ge n\frac{k^{k-2}}{k!}\left(1-\frac{k}{n}\right)^k c^{k-1}e^{-ck}e^{-c^2k/n} \\ &\ge n\frac{k^{k-2}}{k!}c^{k-1}e^{-ck}(1-c_2k^2/n), \end{aligned} \tag{5.11}$$

where c_1 and c_2 depend only on c. Consequently if $1 \le l \le m \le n^{1/2}$, then

$$\begin{aligned} &E\left(\sum_{k=l}^{m} kT_k\right) - n\sum_{k=l}^{m}\frac{k^{k-1}}{k!}c^{k-1}e^{-ck} \\ &\qquad \le \max\{c_1, c_2\}\sum_{k=l}^{m}\frac{k^{k+1}}{k!}c^{k-1}e^{-ck} = O(1). \end{aligned} \tag{5.12}$$

The assertion of our theorem will follow from inequality (5.12) if we show that the terms with $k \geq n^{1/2}$ contribute rather little to the sums. Note that by relation (5.9) that if $1 \leq k < n$, then

$$E\{(k+1)T_{k+1}\}/E(kT_k) = (n-k)\left(1+\frac{1}{k}\right)^{k-2}\frac{c}{n}\left(1-\frac{c}{n}\right)^{n-k-2}$$
$$\leq \left(1-\frac{k}{n}\right) \mathrm{e}c\,\mathrm{e}^{-c(1-k/n)}\left(1-\frac{c}{n}\right)^{-2} \leq \left(1-\frac{c}{n}\right)^{-2} = \lambda, \tag{5.13}$$

since $x\mathrm{e}^{1-x} \leq 1$ for $x > 0$.

Set $k_1 = \lfloor n^{1/3} \rfloor$. Then by Stirling's formula

$$E(k_1 T_{k_1}) = o(n^{-M})$$

for every $M > 0$, and so (5.13) implies

$$E\left(\sum_{k=k_1}^{n} kT_k\right) \leq E(k_1 T_{k_1})\sum_{j=0}^{n}\lambda^j = O(n^2)E(k_1 T_{k_1}) = o(n^{-3}). \tag{5.14}$$

The tail of the series defining $ct(c)$ is also rather small:

$$\sum_{k=k_1}^{\infty}\frac{k^{k-1}}{k!}(c\mathrm{e}^{-c})^k \sim \frac{1}{\sqrt{2\pi}}\sum_{k=k_1} k^{-3/2}(c\mathrm{e}^{1-c})^k = o(n^{-1}) \tag{5.15}$$

since $c\mathrm{e}^{1-c} < 1$.

Relations (5.12), (5.14) and (5.15) imply the desired estimate of $E(T)$:

$$\left|E\left(\sum_{k=1}^{n} kT_k\right) - n\sum_{k=1}^{\infty}\frac{k^{k-1}}{k!}c^{k-1}\mathrm{e}^{-ck}\right|$$
$$\leq \left|E\left(\sum_{k=1}^{k_1} kT_k\right) - n\sum_{k=1}^{k_1}\frac{k^{k-1}}{k!}c^{k-1}\mathrm{e}^{-ck}\right|$$
$$+E\left(\sum_{k=k_1}^{n} kT_k\right) + \frac{n}{c}\sum_{k=k_1}^{\infty}\frac{k^{k-1}}{k!}(c\mathrm{e}^{-c})^k = O(1).$$

Corollary 5.8 *Suppose $p = c/n$, $0 < c < 1$, and $\omega(n) \to \infty$. Then a.e. G_p is such that every component is a tree or a unicyclic graph, and there are at most $\omega(n)$ vertices on the unicyclic components.*

Proof We may assume that $\omega(n) \leq \log\log n$. Since $T(G_p) \leq n$ for every G_p and $E(T) = n + O(1)$,

$$\lim_{n\to\infty} P\{T \leq n - \omega(n)\} = 0.$$

To prove the second part it suffices to show that almost no G_p contains a component of order $k \le \omega(n)$ with at least $k+1$ edges. This can be done by the following crude estimation of the expected number of such components:

$$\sum_{k=4}^{\omega(n)} \binom{n}{k} 2^{k(k-1)/2} n^{-(k+1)} \le \sum_{k=4}^{\omega(n)} 2^{k^2}/n = o(1). \qquad \square$$

In §4 we shall examine the components containing cycles in considerably greater detail.

If $p = c/n$ and $c > 1$, then $T(G_p)$ is still concentrated close to its expectation, though it does not have such a strong peak.

Theorem 5.9 *Suppose $p = c/n, c > 1$ and $\omega(n) \to \infty$. Then a.e. G_p is such that*

$$|T(G_p) - t(c)n| < \omega(n)n^{1/2}.$$

Proof Let $k_1 = \lfloor n^{1/3} \rfloor$. Then by relation (5.14)

$$P\left(\sum_{k=k_1}^{n} kT_k \ge 1\right) \to 0.$$

Set $\widetilde{T} = \sum_{k=1}^{k_1} kT_k$. Then by Theorem 5.7

$$|E(\widetilde{T}) - t(c)n| = O(1),$$

so it suffices to prove that

$$P(|\widetilde{T} - E(\widetilde{T})| \ge \omega(n)n^{1/2} + O(1)) \to 0. \tag{5.16}$$

For $1 \le k \le l \le k_1$ the expected number of ordered pairs of components of G_p, the first of which is a tree of order k and the second is a tree of order l, is clearly

$$\binom{n}{k}\binom{n-k}{l} k^{k-2} l^{l-2} \left(\frac{c}{n}\right)^{k+l-2} \left(1 - \frac{c}{n}\right)^{(k+l)(n-k-l)+\binom{k+l}{2}-k-l+2}$$
$$\le E(T_k)E(T_l)\left(1 - \frac{c}{n}\right)^{-kl} \le E(T_k)E(T_l)\left(1 + \frac{2ckl}{n}\right).$$

Therefore if $1 \le k < l \le k_1$, then

$$E(T_k T_l) \le E(T_k)E(T_l)\left(1 + \frac{2ckl}{n}\right)$$

and if $1 \le k \le k_1$, then

$$\begin{aligned} E(T_k^2) &= E\{T_k(T_k-1)\} + E(T_k) \\ &\le E(T_k)^2\left(1 + \frac{2ck^2}{n}\right) + E(T_k). \end{aligned}$$

Hence

$$\begin{aligned} E(\widetilde{T}^2) &= E\left\{\left(\sum_{k=1}^{k_1} kT_k\right)^2\right\} \\ &\le \sum_{k=1}^{k_1} k^2\left\{E(T_k)^2\left(1+\frac{2ck^2}{n}\right) + E(T_k)\right\} \\ &+ 2\sum_{k<l} klE(T_k)E(T_l)\left(1+\frac{2ckl}{n}\right) \\ &\le \{E(\widetilde{T})\}^2 + O\left[\left\{\sum_{k=1}^{k_1} k^2E(T_k)\right\}^2\right]n^{-1} + O\left\{\sum_{k=1}^{k_1} k^2E(T_k)\right\} \\ &= E(\widetilde{T})^2 + O(n), \end{aligned} \tag{5.17}$$

since $ce^{1-c} < 1$ implies that $\sum_{k=1}^{k_1} k^2E(T_k) = O(n)$. Inequality (5.17) implies

$$\sigma^2(\widetilde{T}) = O(n)$$

so by the Chebyshev inequality

$$P\left\{|\widetilde{T} - E(\widetilde{T})| \ge \frac{1}{2}\omega(n)n^{1/2}\right\} \le \frac{4\sigma^2(\widetilde{T})}{\omega^2(n)n} = o(1),$$

implying relation (5.16). □

In the proofs of Theorems 5.7 and 5.9 we made use of the fact that $\sum_{k=k_1}^{n} k^2E_p(T_k) = o(1)$ if $p \sim c/n$ and $c > 1$. In fact, trees of considerably smaller order are also unlikely to appear in G_p.

Theorem 5.10 *Let* $0 < c < \infty, c \ne 1$ *and* $p = c/n$. *Set* $\alpha = c - 1 - \log c$ *and let*

$$k_0 = \frac{1}{\alpha}\left\{\log n - \frac{5}{2}\log\log n - l_0\right\} \epsilon \mathbb{N}, \qquad l_0 = O(1).$$

Denote by $X = X(G_p)$ *the number of components of* G_p *that are trees* *of order at least* k_0. *Then* X *has asymptotically Poisson distribution with mean*

$$\lambda_0 = \frac{1}{c\sqrt{2\pi}} \frac{\alpha^{5/2}}{1-e^{-\alpha}} e^{l_0}.$$

Proof It is easily seen that for $M > 0$ there is a constant $c_2 > 0$ such that

$$E\left(\sum_{k=k_2}^{n} T_k\right) = o(n^{-M}), \quad \text{where } k_2 = \lfloor c_2 \log n \rfloor.$$

Hence it suffices to show that

$$Y = \sum_{k=k_0}^{k_2} T_k$$

has asymptotically Poisson distribution with mean λ_0. Now

$$\begin{aligned} E(Y) &= \sum_{k=k_0}^{k_2} \binom{n}{k} k^{k-2} \left(\frac{c}{n}\right)^{k-1} \left(1-\frac{c}{n}\right)^{kn-k^2/2+3k/2-1} \\ &\sim \frac{n}{c\sqrt{2\pi}} \sum_{k=k_0}^{k_2} k^{-5/2} (c\, e^{1-c})^k \\ &\sim \frac{n}{c\sqrt{2\pi}} \sum_{l=0}^{\infty} \left(\frac{\log n}{\alpha}\right)^{-5/2} e^{-\alpha(k_0+l)} \\ &= \frac{\alpha^{5/2} e^{l_0}}{c\sqrt{2\pi}} \sum_{l=0}^{\infty} e^{-\alpha l} = \lambda_0. \end{aligned}$$

Furthermore, straightforward calculations show that for $r \geq 1$ the rth factorial moment of Y is

$$E_r(Y) = E(Y)^r \{1 + O(k_2^r/n)\} \sim E(Y)^r \sim \lambda_0^r.$$

Hence the assertion follows from Theorem 1.21. □

Corollary 5.11 *Let* $0 < c < \infty, c \neq 1, p = c/n, \alpha = c - 1 - \log c$ *and* $\omega(n) \to \infty$. *Denote by* $L^{(t)}(G_p)$ *the maximum order of a tree component of* G_p. *Then a.e.* G_p *is such that*

$$\left| L^{(t)}(G_p) - \frac{1}{\alpha}\left\{\log n - \frac{5}{2}\log\log n\right\}\right| \leq \omega(n). \qquad \square$$

The last result indicates that if p is very close to $1/n$, then the maximum order of a tree component of G_p is of larger order than $\log n$. We shall see in the next section that as p approaches $1/n$, this maximum order becomes $n^{2/3}$.

The study of the number of tree components is similar to the study of the number of vertices on tree components and the result is no surprise. The proof, which is very close to the proofs of Theorems 5.7 and 5.9, is left to the reader.

Theorem 5.12 *Let $0 < c < \infty, c \neq 1, p = c/n$ and denote by $U = U(G_p)$ the number of tree components of G_p. Then*

$$E(U) = u(c)n + O(1)$$

where

$$u(c) = \frac{1}{c}\sum_{k=1}^{\infty} \frac{k^{k-2}}{k!}(ce^{-c})^k$$

and

$$\sigma^2(U) = O(n).$$

If $\omega(n) \to \infty$, then a.e. G_p satisfies

$$|U(G_p) - u(c)n| \leq \omega(n)n^{1/2}. \qquad \square$$

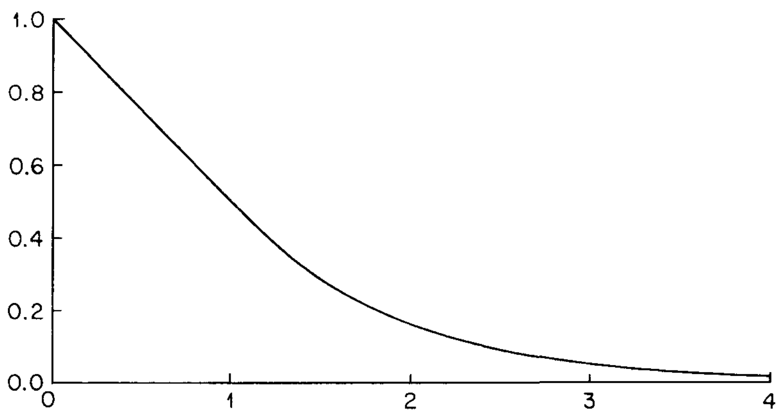


Fig. 5.2. The function $u(c)$.

Remark. Once again, by tedious manipulations one can show that

$$u(c) = 1 - c/2 \quad \text{for} \quad 0 \leq c \leq 1.$$

This is also a consequence of Corollary 5.8 and Theorem 5.12. Indeed, for $0 < c < 1$ a.e. $G_{c/n}$ is such that at least $n - \log n$ of its vertices belong to tree components. Since a.e. $G_{c/n}$ has $\{c/2 + o(1)\}n$ edges, a.e. $G_{c/n}$ must have $\{1 - c/2 + o(1)\}n$ tree components. Hence $u(c) = 1 - c/2$ for $0 < c < 1$.

5.3 The Largest Tree Components

For what function $k = k(n)$ is it true that for some $p = p(n)$ almost every G_p contains a component which is a tree of order k? For what $k_0 = k_0(n)$ is there some $p_0 = p_0(n)$ such that almost every G_{p_0} contains a component which is a tree and has at least k_0 vertices? The main aim of this section is to answer these questions.

It will be convenient to write $\theta = \theta(n)$ for $np = np(n)$, so that $p = \theta/n$. As we shall consider random graphs $G_{\theta/n}$ for various functions $\theta(n)$, occasionally it will be necessary to write $E_{\theta/n}$ instead of E, indicating that the expectation is taken in $\mathcal{G}(n, \theta/n)$. (Since $\theta/n < 1$, $E_{\theta/n}$ cannot be confused with E_r, the rth factorial moment.) Let us recall (5.1), the formula for $E_{\theta/n}(T_k)$, the expected number of trees of order k in $G_{\theta/n}$:

$$E_{\theta/n}(T_k) = \binom{n}{k} k^{k-2} \left(\frac{\theta}{n}\right)^{k-1} \left(1 - \frac{\theta}{n}\right)^{kn-k(k+3)/2+1} \tag{5.18}$$

Theorem 5.13 *Let $2 \le k(n) \le n$. Then $E_{\theta/n}(T_k)$ attains its supremum in $\theta \ge 0$ at $\theta_k = (k-1)n/[k\{n - (k+1)/2\}]$.*

If $k = n$ then $\theta_k = 2$ and

$$E_{2/n}(T_n) \sim (e^3/2n)(2/e)^n. \tag{5.19}$$

If $k \le n - 1$, then

$$\begin{aligned} E_{\theta_k/n}(T_k) &= O(1)\left(\frac{n}{k(n-k)}\right)^{1/2} nk^{-2}\left(1 + \frac{k}{n-k}\right)^{n-k} \\ &\quad \times \left(1 - \frac{k}{2n}\right)^{-k}\left(1 - \frac{1}{n-k/2}\right)^{k\{n-(k/2)\}} \\ &= O(nk^{-5/2}). \end{aligned} \tag{5.20}$$

If $k = o(n)$ and $k \to \infty$, then

$$E_{\theta_k/n}(T_k) \sim \left(\frac{n}{2\pi k(n-k)}\right)^{1/2} nk^{-2}\left(1 + \frac{k}{n-k}\right)^{n-k}$$

$$\times \left(1-\frac{k}{2n}\right)^{-k}\left(1-\frac{1}{n-k/2}\right)^{k(n-k/2)}$$
$$\leq \frac{1+o(1)}{\sqrt{2\pi}} nk^{-5/2}. \qquad (5.21)$$

Finally, if $k = o(n^{1/2})$ and $k \to \infty$, then

$$E_{\theta_k/n}(T_k) \sim \frac{1}{\sqrt{2\pi}} nk^{-5/2} \sim E_{1/n}(T_k). \qquad (5.22)$$

Proof The fact that $E_{\theta/n}(T_k)$ attains its supremum at $\theta_k = (k-1)n/[k\{n-(k+1)/2\}]$ follows from (5.18) upon differentiating with respect to θ. Hence

$$E_{\theta_k/n}(T_k) = \binom{n}{k} k^{k-2}\left(\frac{k-1}{k}\right)^{k-1}\left(\frac{1}{n-(k+1)/2}\right)^{k-1}$$
$$\times \left(1-\frac{k-1}{k\{n-(k+1)/2\}}\right)^{k\{n-(k+3)/2\}+1}. \qquad (5.23)$$

Clearly $\theta_n = 2$ and

$$E_{2/n}(T_n) = n^{n-2}\left(\frac{2}{n}\right)^{n-1}\left(1-\frac{2}{n}\right)^{n(n-3)/2+1}$$
$$\sim \frac{e^2}{2n}(2/e)^n,$$

since

$$\left(1-\frac{2}{n}\right)^{n^2/2} \sim e^{-n-1}.$$

The first part of relation (5.20) is a consequence of (5.23) and the inequalities

$$a^{1/2}(a/e)^a < a! < 4a^{1/2}(a/e)^a,$$

which hold for all $a \geq 1$.

The second part of relation (5.20) requires a little more work. We shall make use of the fact that if $x > 0$, then

$$(1+1/x)^x \Big/ \left\{ e\left(1-\frac{1}{2(x+1)}\right)\right\} < 1. \qquad (5.24)$$

Furthermore, since the left-hand side of (5.24) is a continuous function of x and tends to $2/e$ as $x \to 0$,

$$(1+1/x)^x \Big/ \left\{ e\left(1-\frac{1}{2(x+1)}\right)\right\} < 1-\varepsilon_0 < 1 \qquad (5.25)$$

for all $x, 0 < x < 1$, and some $\varepsilon_0 > 0$. Hence with $x = (n-k)/k$ we find that

$$\begin{aligned}
&\left(1+\frac{k}{n-k}\right)^{n-k}\left(1-\frac{k}{2n}\right)^{-k}\left(1-\frac{1}{n-k/2}\right)^{k(n-k/2)} \\
&\leq \left\{\left(1+\frac{k}{n-k}\right)^{(n-k)/k}\left(1-\frac{k}{2n}\right)^{-1}\mathrm{e}^{-1}\right\}^k \\
&= \left\{(1+1/x)^x\left(1-\frac{1}{2(x+1)}\right)^{-1}\mathrm{e}^{-1}\right\}^k \leq 1
\end{aligned} \tag{5.26}$$

and if $(n-k)/k < 1$, that is $k \geq n/2$, then

$$\left(1+\frac{k}{n-k}\right)^{n-k}\left(1-\frac{k}{2n}\right)^{-k}\left(1-\frac{1}{n-k/2}\right)^{k(n-k/2)} \leq (1-\varepsilon_0)^k \leq (1-\varepsilon_0)^{n/2}.$$

Therefore

$$E_{\theta_k/n}(T_k) = O\{n^{3/2}k^{-5/2}(1-\varepsilon_0)^{n/2}\}$$

if $k \geq n/2$, and otherwise

$$E_{\theta_k/n}(T_k) = O(nk^{-5/2}),$$

proving the second part of (5.20).

Relation (5.21) is an immediate consequence of (5.23), (5.26) and the Stirling approximation.

Finally, if $k = o(n^{1/2})$ and $k \to \infty$, then

$$\left(1+\frac{k}{n-k}\right)^{n-k} \sim \mathrm{e}^k,$$
$$\left(1-\frac{1}{2n}\right)^{-k} \sim 1$$

and

$$\left(1-\frac{1}{n-k/2}\right)^{k(n-k/2)} \sim \mathrm{e}^{-k},$$

implying our last assertion. □

Armed with Theorem 5.13 we can determine how small $k(n)$ has to be if we want to guarantee that for some p almost every G_p contains an isolated tree of order k.

Theorem 5.14 *(i) If $k/n^{2/5} \to \infty$, then almost no G_p contains an isolated tree of order k.*

(ii) If $c > 0$ is a constant and $k \sim cn^{2/5}$, then in $G_{1/n}$ we have $T_k \xrightarrow{d} P\{c^{-5/2}(2\pi)^{-1/2}\}$.

(iii) If $k/n^{2/5} \to 0$, then a.e. $G_{1/n}$ contains an isolated tree of order k.

(iv) If $k_0/n^{2/7} \to 0$, then a.e. $G_{1/n}$ contains an isolated tree of order k for every $k \le k_0$.

Proof (i) Suppose $k/n^{2/5} \to \infty$ and $0 < p < 1$. Then by (5.19) and (5.20)

$$P_p(T_k > 0) \le E_p(T_k) \le E_{\theta_k/n}(T_k) = O(nk^{-5/2}) = o(1).$$

(ii) Assume that $k \sim cn^{2/5}$. Then in $\mathcal{G}(n, 1/n)$ the rth factorial moment of T_k is easily estimated:

$$\begin{aligned} E_r(T_k) &= \frac{(n)_{rk}}{(k!)^r} k^{r(k-2)} n^{-r(k-1)} \left(1 - \frac{1}{n}\right)^{nrk+O(k^2)} \\ &\sim \left\{ \binom{n}{k} k^{k-2} n^{-k+1} \left(1 - \frac{1}{n}\right)^{nk} \right\}^r \sim \{E(T_k)\}^r. \end{aligned}$$

Since $E(T_k) \sim (1/\sqrt{2\pi})c^{-5/2}$, the result follows by Theorem 5.20 of Chapter 1.

(iii) Suppose $1 \le k_1 \le k_2 \le n - k_1$ and $0 < p \le 1/n$. Denote by $E_p(T_{k_1}, T_{k_2})$ the expected number of ordered pairs of components of G_p such that the first component is a tree of order k_1 and the second is a tree of order k_2. Then

$$\begin{aligned} E_p(T_{k_1}, T_{k_2}) &= \binom{n}{k_1} \binom{n-k_1}{k_2} k_1^{k_1-2} k_2^{k_2-2} p^{k_1-1+k_2-1} \\ &\quad \times (1-p)^{k_1\{n-(k_1+3)/2\}+1+k_2\{n-(k_2+3)/2\}+1-k_1k_2} \end{aligned}$$

so

$$\begin{aligned} E_p(T_{k_1}, T_{k_2})/E_p(T_{k_1})E_p(T_{k_2}) &\le \frac{(n-k_2)_{k_1}}{(n)_{k_1}} (1-p)^{-k_1k_2} \\ &\le \left(1 - \frac{k_2}{n}\right)^{k_1} \left(1 - \frac{1}{n}\right)^{-k_1k_2} \le 1, \end{aligned}$$

since for $0 < a \le 1 \le b$ we have

$$1 - ab \le (1-a)^b.$$

Consequently

$$E_p(T_{k_1}, T_{k_2}) \le E_p(T_{k_1})E_p(T_{k_2}). \tag{5.27}$$

Now if $k = o(n^{2/5})$ then in $\mathcal{G}(n, 1/n)$ we have $E(T_k) \to \infty$. Therefore, by (5.27),

$$E(T_k^2) = E(T_k, T_k) + E(T_k) \le E(T_k)^2 + E(T_k) \sim E(T_k)^2$$

and by the Chebyshev inequality

$$P(T_k = 0) \le E(T_k^2)/E(T_k)^2 - 1 = o(1).$$

(iv) Suppose $k < k_0 = o(n^{2/7})$. Then in $\mathcal{G}(n, 1/n)$

$$E(T_k) \sim (n/\sqrt{2\pi})k^{-5/2}.$$

Furthermore, as in (iii), by (5.27) we have

$$P(T_k = 0) \le 1/E(T_k).$$

Therefore

$$P(T_k = 0 \text{ for some } k \le k_0) = O\left\{n^{-1} \sum_{k=1}^{k_0} k^{5/2}\right\} = o(1). \qquad \square$$

Let us see now the maximal order of a tree component.

Theorem 5.15 *(i) If $k_0/n^{2/3} \to \infty$, then almost no G_p contains an isolated tree of order at least k_0.*

(ii) Let $\lambda > 0$ be a constant and let $c_1 = c_1(n) > 0$ be such that $c_1(n)n^{4/15} \to \infty$ and $c_1(n) \to 0$. Furthermore, let $c_2(n) > c_1(n)$ satisfy

$$c_2(n) - c_1(n) \sim \lambda\sqrt{2\pi}c_1(n)^{5/2}.$$

Then the number of isolated trees in $G_{1/n}$ whose orders are between $c_1(n)n^{2/3}$ and $c_2(n)n^{2/3}$ tends to the Poisson distribution $P(\lambda)$.

(iii) If $k_0/n^{2/3} \to 0$, then a.e. $G_{1/n}$ contains an isolated tree of order at least k_0.

Proof (i) Suppose $k_0/n^{2/3} \to \infty$. Then by Theorem 5.13

$$E_p\left(\sum_{k=k_0}^{n} T_k\right) \le \sum_{k=k_0}^{n} E_{\theta_k/n}(T_k) = O(n)\sum_{k=k_0}^{n} k^{-5/2} = o(1).$$

(ii) If $k = o(n^{3/4})$, then

$$\begin{aligned} E_{1/n}(T_k) &= \binom{n}{k} k^{k-2} n^{-k+1} \left(1 - \frac{1}{n}\right)^{k\{n-(k+3)/2\}+1} \\ &\sim \frac{nk^{-5/2}}{\sqrt{2\pi}} \left(1 - \frac{k}{n}\right)^{-(n-k)} \left(1 - \frac{1}{n}\right)^{k(n-k/2)} \end{aligned}$$

$$\sim \frac{nk^{-5/2}}{\sqrt{2\pi}} \exp\left\{(n-k)\left(\frac{k}{n}+\frac{k^2}{2n^2}+\frac{k^3}{3n^3}\right)\right.$$
$$\left. -k(n-k/2)\left(\frac{1}{n}+\frac{1}{2n^2}\right)+o(1)\right\}$$
$$\sim \frac{nk^{-5/2}}{\sqrt{2\pi}} \exp\{-k^3/(6n^2)\}. \tag{5.28}$$

In particular, if $k = o(n^{2/3})$, then $E_{1/n}(T_k) \sim nk^{-5/2}/\sqrt{2\pi}$.

Hence with $U = \Sigma\{T_k : c_1 n^{2/3} \le k \le c_2 n^{2/3}\}$ we have

$$\begin{aligned} E(U) &\sim \Sigma\left\{\frac{n}{\sqrt{2\pi}}k^{-5/2} : c_1 n^{2/3} \le k \le c_2 n^{2/3}\right\} \\ &\sim (c_2-c_1)n^{2/3}\frac{n}{\sqrt{2\pi}}(c_1 n^{2/3})^{-5/2} \\ &= (c_2-c_1)c_1^{-5/2}/\sqrt{2\pi} \sim \lambda. \end{aligned}$$

In the second relation above we made use of the fact that $\{c_2(n) - c_1(n)\}n^{2/3} \to \infty$.

Analogously to part (iii) of the proof of Theorem 5.14, denote by $E(T_{k_1}, T_{k_2}, \ldots, T_{k_r})$ the expected number of ordered r-tuples of components of $G_{1/n}$ such that the ith component is a tree of order k_i. If $K = \sum_1^r k_i = o(n^{2/3})$, then

$$\begin{aligned} &E(T_{k_1}, T_{k_2}, \ldots, T_{k_r})/E(T_{k_1})E(T_{k_2})\ldots E(T_{k_r}) \\ &= \binom{n}{k_1, k_2, \ldots, k_r} \Big/ \left\{\prod_{i=1}^r \binom{n}{k_i}\left(1-\frac{1}{n}\right)^{\Sigma_{i<j}k_i i_j}\right\} \\ &\sim \left(\frac{n}{n-K}\right)^{n-K}\prod_{i=1}^r\left(\frac{n-k_i}{n}\right)^{n-k_i}\left(1-\frac{1}{n}\right)^{-\Sigma_{i<j}k_ik_j} \\ &\sim \exp\left\{(n-K)\left(\frac{K}{n}+\frac{K^2}{2n^2}\right)-\sum_{i=1}^r(n-k_i)\left(\frac{k_i}{n}+\frac{k_i^2}{2n^2}\right)+\sum_{i<j}k_ik_j/n\right\} \\ &\sim \exp\left\{-\frac{K^2}{2n}+\sum_{i=1}^r\frac{k_i^2}{2n}+\sum_{i<j}k_ik_j/n\right\} \sim 1. \end{aligned} \tag{5.29}$$

Consequently

$$E_r(U) \sim \{E(U)\}^r \sim \lambda^r$$

for every $r \ge 1$, and so our assertion follows from Theorem 1.21.

(iii) This is an immediate consequence of (ii). □

From the proof above it is easy to calculate the expected number of isolated trees of order at least $cn^{2/3}$ in $G_{1/n}$, where $c > 0$ is a constant. Let $V = \sum' T_k$, where $\sum'$ denotes summation over $cn^{2/3} \le k \le n$. Then

$$E(V) = E\left(\sum{}' T_k\right) \sim \frac{n}{\sqrt{2\pi}} \sum{}' k^{-5/2} \exp\{-k^3/(6n^2)\},$$

where E denotes the expectation in $\mathcal{G}_{1/n}$. With the substitutions $u = k/n^{2/3}$ and $\upsilon = u^3/6$ we find that

$$E(V) \sim \frac{1}{\sqrt{2\pi}} \int_c^\infty u^{-5/2} e^{-u^3/6} du \sim \frac{1}{6\sqrt{3\pi}} \int_{c^3/6}^\infty \upsilon^{-3/2} e^{-\upsilon} d\upsilon = \mu = \mu(c).$$

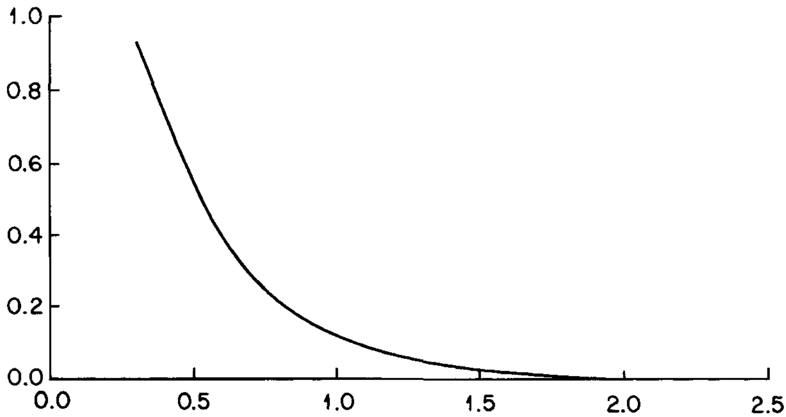


Fig. 5.3. The function $\mu(c) = (1/6\sqrt{3\pi}) \int_{c^3/6}^\infty \upsilon^{-3/2} e^{-\upsilon} d\upsilon$, the limit of the expected number of isolated trees of order at least $cn^{2/3}$ in $G_{1/n}$.

It is tempting to conjecture [and it was claimed by Erdős and Rényi (1960, Theorem 7b)] that V tends to $P(\mu)$. In fact, this is not so. If $cn^{2/3} \le k_1 \le k_2$, then similarly to (5.29) we find that

$$\begin{aligned} E(T_{k_1}, T_{k_2})/E(T_{k_1})E(T_{k_2}) &= \binom{n}{k_1, k_2} \Big/ \binom{n}{k_1}\binom{n}{k_2} \left(1 - \frac{1}{n}\right)^{k_1 k_2} \\ &\sim \exp\{-(k_1 k_2^2 + k_1^2 k_2)/2n^2\} \le e^{-c^3}. \end{aligned}$$

Hence

$$E_2(V) \le e^{-c^3}\{E(V)\}^2 = e^{-c^3}\mu^2,$$

so $V \xrightarrow{d} P(\lambda)$ does not hold.

5.4 Components Containing Cycles

We saw in §2 that if $p \sim c/n$ and $c > 1$, then a substantial proportion of the vertices of G_p lies on components containing cycles. Therefore it is not surprising that the study of the distribution of the components containing cycles is an important part of our investigation of the global structure of G_p for $p \sim c/n, c > 1$. The case of components which are cycles is rather simple.

Theorem 5.16 *Denote by C_k the number of those components in a r.g. G_p which are cycles of order $k = k(n) \geq 3$.*

(i) If $pn \to 0$ or $pn \to \infty$, then $C_k = 0$ for a.e. G_p.
(ii) If $p \sim c/n$ for some constant $c > 0$ and k is constant, then $C_k \xrightarrow{d} P\{(ce^{-c})^k/2k\}$.
(iii) If $k = k(n) \to \infty$, then $C_k = 0$ for a.e. G_p.

Proof If p is sufficiently large, say $p = \theta(n)/n \geq 3 \log n/n$, then a.e. G_p is connected (Ex. 14 of Chapter 2) so $C_k(G_p) = 0$ for a.e. G_p. Furthermore, if $p = o(1/n)$, then almost no G_p contains a cycle (Ex. 1 of Chapter 4). Therefore one may assume that $\varepsilon \leq \theta(n) \leq 3 \log n$ for some $\varepsilon > 0$. Clearly

$$E(C_k) = \binom{n}{k} \frac{(k-1)!}{2} p^k q^{k(n-k)+\binom{k}{2}-k} = \frac{(n)k}{2k} \left(\frac{\theta}{n}\right)^k \left(1 - \frac{\theta}{n}\right)^{kn-k(k+3)/2}$$
$$\leq \frac{1}{2k} \frac{(n)_k}{n^k} \theta^k \exp\{-k\theta + k^2\theta/2n + 3k\theta/2n\}.$$

With a little work one can show that if either $k(n) \to \infty$ or $\theta(n) \to \infty$ then $E(C_k) \to 0$. Finally, if k is constant and $p \sim c/n$ for some constant $c > 0$, then

$$E(C_k) \sim \frac{1}{2k} c^k e^{-kc} = \lambda$$

and for every $r \geq 1$

$$E_r(C_k) \sim \lambda^k,$$

so $C_k \to P_\lambda$ by Theorem 1.20. The details are left to the reader (Ex. 5). □

It is interesting to note that isolated cycles behave rather differently from isolated trees. By Theorem 5.16, the maximum of the expected number of components which are k-cycles increases up to $p \sim 1/n$ and from then on it decreases. Hence about the same value of p gives the maximum for every k. Furthermore, this maximum is less than 1 for every k. In fact, for $p = 1/n$ the expected number of components which are cycles is

$$E\left(\sum_{k=3}^{n} C_k\right) \sim \frac{1}{2}\sum_{k=3}^{\infty} \mathrm{e}^{-k}/k = \frac{1}{2} - \frac{1}{2}\log(\mathrm{e}-1) - \frac{1}{2\mathrm{e}} - \frac{1}{4\mathrm{e}^2}$$
$$= 0.011564\ldots.$$

The study of the components other than cycles needs some preparation. Denote by $\mathscr{C}(n,m)$ the set of *connected* graphs with vertex set $V = \{1,2,\ldots,n\}$ having m edges, and put $C(n,m) = |\mathscr{C}(n,m)|$. Clearly $\mathscr{C}(n,n+k) = \emptyset$ if $k \le -2, \mathscr{C}(n,n-1)$ is the set of trees so $C(n,n-1) = n^{n-2}$, and $\mathscr{C}(n,n)$ is the set of connected unicyclic graphs. The function $C(n,n)$ was determined by Katz (1955) and Rényi (1959*b*). The formula can also be read out of more general results of Ford and Uhlenbeck (1957), and another proof was given by Wright (1977*a*). Here we shall prove it from the following lemma, due to Rényi (1959*a*) but asserted already by Cayley (1889).

Lemma 5.17 *Let* $1 \le k < n$. *Denote by* $F(n,k)$ *the number of forests on* $V = \{1,2,\ldots,n\}$ *which have* k *components and in which the vertices* $1,2,\ldots,k$ *belong to distinct components. Then*

$$F(n,k) = kn^{n-1-k}. \tag{5.30}$$

Proof The lemma can be proved in many ways. Here we shall present two proofs. Both are different from those given by Katz (1955), Rényi (1959*a*) and Wright (1977*a*).

Our first proof is based on the following special case of Abel's generalization of the binomial formula:

$$\sum_{l=0}^{m} \binom{m}{l} (x+l)^{l-1}(y+m-l)^{m-l-1} = (x^{-1}+y^{-1})(x+y+m)^{m-1}. \tag{5.31}$$

For (5.31) see Riordan (1968, p. 23) or Gould (1972, p. 15).

Note that for $k = 1$ formula (5.30) is just Cayley's formula for the number of trees. Assume that (5.30) holds for $k-1$, where $k \ge 2$. Then the number of appropriate forests with $l+1$ vertices in the component containing vertex 1 is clearly

$$\binom{n-k}{l}(l+1)^{l-1}F(n-l-1,k-1) = \binom{n-k}{l}(l+1)^{l-1}(k-1)(n-l-1)^{n-k-l-1}.$$

On putting $x = 1, y = k-1$ and $m = n-k$ into (5.31) we find that

$$F(n,k) = \sum_{l=0}^{n-k} \binom{n-k}{l} (l+1)^{l-1}(k-1)(n-l-1)^{n-k-l-1} = kn^{n-k-1},$$

proving (5.30).

Our second proof is based on Prüfer codes for trees. The forests appearing in the lemma are in one-to-one correspondence with the trees on $V' = \{0, 1, 2, \ldots, n\}$ in which the neighbours of vertex 0 are $1, 2, \ldots, k$. If the code of a tree on V' is constructed by writing down the neighbour of the current end vertex with the maximal label then the code we obtain is such that the last $k-1$ elements are 0's, 0 does not occur anywhere else and the element preceding the 0's is one of $1, 2, \ldots, k$. Conversely, every such code belongs to a tree in which the neighbours of 0 are $1, 2, \ldots, k$. Since the number of such codes is $n^{n-1-k}k$, our lemma follows. □

The formula for $C(n,n)$ is an easy consequence of Lemma 5.17.

Theorem 5.18

$$C(n,n) = \frac{1}{2}n^{n-1} \sum_{r=3}^{n} \prod_{j=1}^{r-1} \left(1 - \frac{j}{n}\right) = \frac{1}{2}(n-1)! \sum_{j=0}^{n-3} \frac{n^j}{j!}.$$

Proof A connected graph of order n and size n is unicyclic. What is the number of such graphs in which the unique cycle contains r edges? There are

$$\binom{n}{r} \frac{r!}{2r} = (n)_r/(2r)$$

ways of choosing an r-cycle C^r. After the omission of the edges of C^r the graph becomes a forest with r components and the vertices of C^r belong to distinct components. Hence C^r is the unique cycle in $F(n,r)$ of our graphs. Therefore

$$\begin{aligned} C(n,n) &= \sum_{r=3}^{n} \frac{(n)_r}{2r} F(n,r) = \frac{1}{2} \sum_{r=3}^{n} (n)_r n^{n-r-1} \\ &= \frac{1}{2} n^{n-1} \sum_{r=3}^{n} \prod_{j=1}^{r-1} \left(1 - \frac{j}{n}\right). \end{aligned}$$

□

Corollary 5.19 $C(n,n) \sim (\pi/8)^{1/2} n^{n-1/2}$.

Proof Since

$$\prod_{j=1}^{r-1}\left(1-\frac{j}{n}\right) \le \exp\left\{-\binom{r}{2}\Big/n\right\}$$

and for $r = O(n^{2/3})$

$$\prod_{j=1}^{r-1}\left(1-\frac{j}{n}\right) = e^{-r^2/(2n)}\{1 + O(r/n) + O(r^3/n^2)\},$$

we have

$$\begin{aligned}\sum_{r=3}^{n}\prod_{j=1}^{r-1}\left(1-\frac{j}{n}\right) &= \sum_{r=3}^{\lfloor n^{5/9}\rfloor} e^{-r^2/(2n)} + O(1)\\ &= \sqrt{n}\int_0^\infty e^{-x^2/2}dx + O(1) = \left(\frac{\pi n}{2}\right)^{1/2} + O(1).\end{aligned}$$

Therefore

$$C(n,n) = (\pi/8)^{1/2}n^{n-1/2} + O(n^{n-1}). \qquad \square$$

The use of Lemma 5.17 enabled Rényi (1959*b*) to determine the asymptotic distribution of the length of the unique cycle contained in a connected graph of order n and size n (Ex. 7).

We shall present a number of consequences of Theorem 5.18 concerning the unicyclic components of random graphs, but first we continue the examination of the function $C(n, n+k)$.

Bagaev (1973) showed that $C(n, n+1) \sim \frac{5}{24}n^{n+1}$, and for $2 \le k = o(n^{1/3})$ Wright (1977*a*, 1978*b*, 1980, 1983) determined the asymptotic value of $C(n, n+k)$:

$$C(n, n+k) = \gamma_k n^{n+(3k-1)/2}\{1 + O(k^{3/2}n^{-1/2})\},$$

where

$$\gamma_k = \frac{\pi^{1/2}3^k(k-1)\delta_k}{2^{(5k-1)/2}\Gamma(k/2)}$$

and

$$\delta_1 = \delta_2 = \frac{5}{36},\ \delta_{k+1} = \delta_k + \sum_{h=1}^{k-1}\frac{\delta_h\delta_{k-h}}{k+1}\binom{k}{h}^{-1},\ k \ge 2.$$

In fact, if $k = o(n^{1/3})$ and $k \to \infty$ then

$$C(n, n+k) = \left(\frac{3}{4\pi}\right)^{1/2}\left(\frac{e}{12\,k}\right)^{k/2} n^{n+(3k-1)/2}\{1 + O(k^{3/2}n^{-1/2}) + O(k^{-1})\}.$$

Additional numerical data were given by Gray, Murray and Young (1977).

The results above were considerably extended by Łuczak (1990*a*) who showed that the last formula is a good approximation of $C(n, n+k)$ provided $k = o(n)$ and $k \to \infty$. Furthermore, Bender, Canfield and McKay (1990) proved a rather complicated asymptotic formula for $C(n, n+k)$ for every function $k = k(n)$ as $n \to \infty$.

In order to study the evolution of random graphs we shall not need an asymptotic formula for $C(n, n+k)$, but we do need the following upper bound, due to Bollobás (1984*a*).

Theorem 5.20 *There is an absolute constant c such that for $1 \le k \le n$*

$$C(n, n+k) \le (c/k)^{k/2} n^{n+(3k-1)/2}.$$

Proof Recall that $\mathscr{C}(n, n+k)$ is the set of connected graphs with vertex set $V = \{1, 2, \ldots, n\}$ having $n+k$ edges. Every graph $G \in \mathscr{C}(n, n+k)$ contains a unique maximal connected subgraph H in which every vertex has degree at least 2. Let W be the vertex set of H. Clearly $e(H) = w + k$, where $w = |W|$. Furthermore, G is obtained from H by adding to it a forest with vertex set W, in which each component contains exactly one vertex of W. Hence wn^{n-1-w} graphs $G \in \mathscr{C}(n, n+k)$ give the same graph H.

Denote by T the set of branch vertices of H and by $U = W - T$ the set of vertices of degree 2. Set $t = |T|$ and $u = |U| = w - t$. Clearly, H is obtained from a multigraph M (i.e. a 'graph' which may contain loops and multiple edges) with vertex set T by subdividing the edges with the vertices from U (see Fig. 5.4).

The multigraph M has $t + k$ edges and loops, so there are at most $u!B(u+t+k-1, t+k-1)$ ways of inserting the u vertices in order to obtain H from M. Since every vertex of M has degree at least 3 (a loop contributing 2 to the degree of the vertex incident with it),

$$3t \le 2(t+k), \text{ that is, } t \le 2k.$$

Consequently

$$C(n, n+k) \le \sum_{t=1}^{2k} \binom{n}{t} \psi(t, t+k)$$
$$\times \sum_{u=0}^{n-t} \binom{n-t}{u} u! \binom{u+t+k-1}{t+k-1} (t+u) n^{n-1-t-u}, \quad (5.32)$$

where $\psi(t, t+k)$ is the number of labelled multigraphs of order t in which

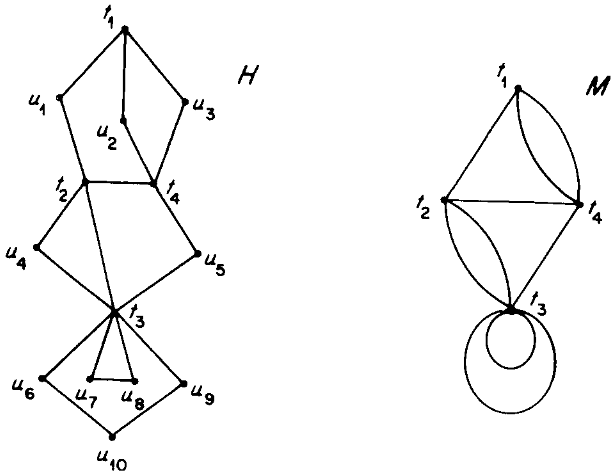


Fig. 5.4. A graph H and a multigraph M with $T = \{t_1, \ldots, t_4\}$ and $U = \{u_1, \ldots, u_{10}\}$.

every vertex has degree at least 3. Rather crudely

$$\psi(t, t+k) \leq B\left\{\binom{t}{2} + t + (t+k-1), t+k-1\right\}, \tag{5.33}$$

since a multigraph M is determined by the partition of its $t+k$ edges and loops into $\binom{t}{2} + t$ classes, $\binom{t}{2}$ classes for (multiple) edges and t classes for (multiple) loops.

To prove the theorem we shall simply estimate the bound for $C(n, n+k)$ implied by (5.32) and (5.33). We shall write $c_1, c_2, \ldots$ for positive absolute constants. Note first that if $t \leq 2k$, then

$$\binom{t^2/2 + 3t/2 + k - 1}{t+k-1} \leq (c_1 k)^{k+t-1}$$

and

$$\binom{n}{t}\binom{n-t}{u} u! = \frac{1}{t!}(n)_{t+u} \leq \frac{n^{t+u}}{t!}\exp(-u^2/2n).$$

Therefore

$$C(n, n+k) \leq n^{n-1} \sum_{t=1}^{2k} \sum_{u=0}^{n-t} A(t, u),$$

where

$$A(t,u) = \frac{1}{t!}(c_1k)^{k+t-1}\exp(-u^2/2n)\binom{u+t+k-1}{t+k-1}(t+u).$$

Let us split the double sum above into two parts, according to the size of u. Clearly

$$\begin{aligned}
\sum_{t=1}^{2k}\sum_{u=1}^{k} A(t,u) &\le \sum_{t=1}^{2k}\sum_{u=1}^{k}\frac{1}{t!}(c_1k)^{t+k-1}\exp(-u^2/2n)2^{t+k}(3k) \\
&\le n^{1/2}\sum_{t=1}^{2k}(c_2k)^{t+k-1}/t! \le n^{1/2}(c_3k)^{k-3/2} \\
&\le (c_3/k)^{k/2}n^{3k/2-1}. \qquad (5.34)
\end{aligned}$$

The case in which u is large is also easily dealt with:

$$\sum_{t=1}^{2k}\sum_{u=k+1}^{n-t} A(t,u) \le \sum_{t=1}^{2k}\sum_{u=k+1}^{n-t}\frac{1}{t!}(c_4k)^{t+k-1}\exp(-u^2/2n)\frac{u^{t+k}}{(t+k-1)!}.$$

Since by Ex. 8 of Chapter 1

$$\begin{aligned}
\int_0^\infty x^{t+k}e^{-x^2/2}dx &\le \{(t+k)!\}^{1/2}, \\
\sum_{t=1}^{2k}\sum_{u=k+1}^{n-t} A(t,u) &\le \sum_{t=1}^{2k}(c_5k)^{t+k-1}\frac{\{(t+k)!\}^{1/2}}{t!(t+k-1)!}n^{(t+k+1)/2} \\
&< n^{(k+1)/2}\sum_{t=1}^{2k}\frac{(c_6k)^{t+k}}{t!\{(t+k)!\}^{1/2}}n^{t/2} \\
&< n^{(k+1)/2}\sum_{t=1}^{2k}(c_7k)^{t/2+k/2}n^{t/2}/t! \\
&< n^{(k+1)/2}(c_8/k)^{k/2}n^k. \qquad (5.35)
\end{aligned}$$

The assertion of our theorem follows from inequalities (5.34) and (5.35):

$$\begin{aligned}
C(n,n+k) &\le n^{n-1}\{(c_3/k)^{k/2}n^{3k/2-1} + (c_8/k)^{k/2}n^{(3k+1)/2}\} \\
&\le (c/k)^{k/2}n^{n+(3k-1)/2}. \qquad \square
\end{aligned}$$

If k is close to n then the bound in the theorem above is worse than the bound, valid for all $k \ge -1$, given by the total number of graphs of order n and size $n+k$:

$$C(n,n+k) \le \binom{N}{n+k} \le \left(\frac{en^2}{2(n+k)}\right)^{n+k}. \tag{5.36}$$

Inequality (5.36) and Theorem 5.20 have the following immediate consequence.

Corollary 5.21 *There is an absolute constant c such that*

$$C(n,n+k) \le ck^{-k/2}n^{n+(3k-1)/2}$$

for all $n,k \in \mathbb{N}$ with $k \le N-n = \binom{n}{2} - n$.

Proof Theorem 5.20 implies that in proving this corollary we may assume that $n < k \le N-n$; in particular, $n \ge 6$. By inequality (5.36), in this range we have

$$\begin{aligned} C(n,n+k) &\le \sqrt{n}\left(\frac{e}{2}\right)^{n+k}\left(\frac{n}{n+k}\right)^{n+k/2}\left(\frac{k}{n+k}\right)^{k/2} k^{-k/2}n^{n+(3k-1)/2} \\ &< \sqrt{n}\left(\frac{e}{2}\right)^{n+k}\exp\left\{-\frac{k(n+k/2)}{n+k} - \frac{nk/2}{n+k}\right\} k^{-k/2}n^{n+(3k-1)/2} \\ &< \sqrt{n}\left(\frac{e}{2}\right)^{n+k} e^{-(n+k)/2}k^{-k/2}n^{n+(3k-1)/2} \\ &< k^{-k/2}n^{n+(3k-1)/2}, \end{aligned}$$

as claimed. □

With a little more work one can show that $c = 1$ will do in Theorem 5.20. Using this sharpening of Theorem 5.20, the proof above shows that $c = 1$ will do in Corollary 5.21 as well.

As mentioned earlier, Theorem 5.18 and Corollary 5.19 can be used to obtain fairly precise information about the unicyclic components of random graphs. Our first result concerns components of bounded order.

Theorem 5.22 *Let $p \sim c/n, 0 < c < \infty$ and denote by $X_k = X_k(G_p)$ the number of unicyclic components of order k in G_p. Let $3 \le k_1 < k_2 < \ldots < k_s$ be fixed. Then $X_{k_1}, X_{k_2}, \ldots, X_{k_s}$ are asymptotically independent Poisson random variables with means $\lambda_1, \lambda_2, \ldots, \lambda_s$, where*

$$\lambda_l = \frac{1}{2k_l}(ce^{-c})^{k_l}\sum_{j=0}^{k_l-3} k_l^j/j!.$$

Proof The joint factorial moments of $X_{k_1}, X_{k_2}, \ldots, X_{k_s}$ are easily estimated:

$$\begin{aligned} E\{(X_{k_1})_{r_1} \ldots (X_{k_s})_{r_s}\} &\sim \frac{(n)_r}{\left(\prod_{i=1}^{s} k_i!\right)^{r_i} \prod_{i=1}^{s} r_i!} \prod_{i=1}^{s} C(k_i,k_i)^{r_i} \left(\frac{c}{n}\right)^k \left(1-\frac{c}{n}\right)^{kn} \\ &\sim \prod_{i=1}^{s} [(ce^{-c})^{k_i r_i} \{C(k_i,k_i)/k_i!\}^{r_i}/r_i!], \end{aligned}$$

where $k = \sum_i^s =_1 r_i k_i$. By Theorem 5.18 this expression is exactly

$$\prod_{i=1}^{s} \lambda_i^{r_i}/r_i!.$$

Hence Theorem 1.21 implies the result. □

Theorem 5.23 *Denote by $X = X(G_p)$ the number of vertices of G_p belonging to unicyclic components. Then for $p \sim c/n, 0 < c < \infty, c \neq 1$, we have*

$$\begin{aligned} E(X) &\sim \frac{1}{2} \sum_{k=3}^{\infty} (ce^{-c})^k \sum_{j=0}^{k-3} k^j/j! = \mu(c), \\ \sigma^2(X) &\sim \frac{1}{2} \sum_{k=3}^{\infty} k(ce^{-c})^k \sum_{j=0}^{k-3} k^j/j! \end{aligned}$$

and for $p = 1/n$ we have

$$E(X) \sim \frac{6^{1/3}\Gamma(1/3)}{12} n^{2/3} \approx 0.406 n^{2/3}$$

and

$$\sigma^2(X) = O(n^{4/3}).$$

Proof (i) Suppose $p \sim c/n, 0 < c < \infty, c \neq 1$. Then by Theorem 5.18

$$\begin{aligned} E(X) &= \sum_{k=3}^{n} kE(X_k) = \sum_{k=3}^{n} k \binom{n}{k} C(k,k) p^k q^{k(n-k)+\binom{k}{2}-k} \\ &= \frac{1}{2} \sum_{k=3}^{n} \frac{(n)_k}{n^k} c^k \left(1-\frac{c}{n}\right)^{kn-k^2/2-3k/2} \left(\sum_{j=0}^{k-3} k^j/j!\right) \\ &\sim \frac{1}{2} \sum_{k=3}^{\infty} (ce^{-c})^k \sum_{j=0}^{k-3} k^j/j! \end{aligned}$$

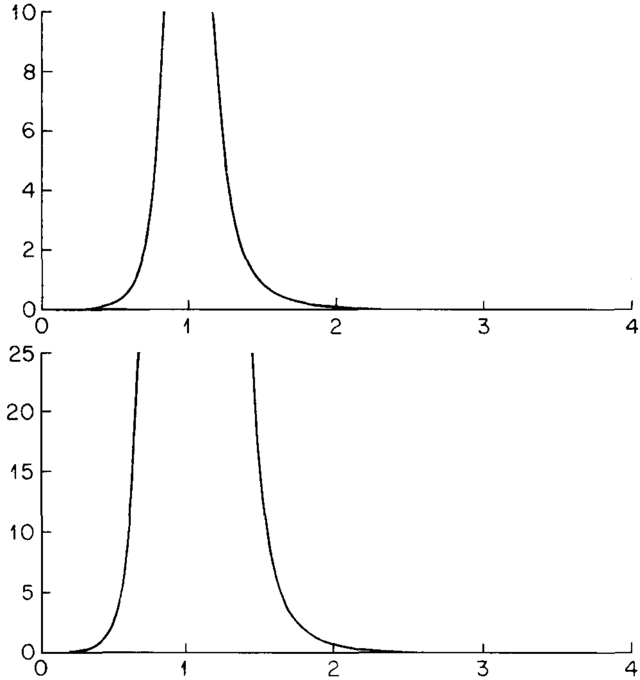


Fig. 5.5. The curves of $E_{c/n}(X)$ and $\sigma^2_{c/n}(X)$.

Furthermore, as in the proof of Theorem 5.22, for fixed k_1 and k_2 we have

$$E\{(X_{k_1})_2\} \sim E(X_{k_1})^2, E\{(X_{k_1})^2\} \sim E(X_{k_1})^2 + E(X_{k_1}),$$

and

$$E(X_{k_1}X_{k_2}) \sim E(X_{k_1})E(X_{k_2}).$$

Consequently, for every fixed $k_0 \geq 3$:

$$E\left(\sum_{k=3}^{k_0} kX_k\right)^2 \sim E\left(\sum_{k=3}^{k_0} kX_k\right)^2 + \sum_{k=3}^{k_0} k^2 E(X_k).$$

From this it follows that

$$\sigma^2(X) \sim \sum_{k=3}^{\infty} k^2 E(X_k) \sim \frac{1}{2}\sum_{k=3}^{\infty} k(ce^{-c})^k \sum_{j=0}^{k-3} k^j/j!$$

since the last double sum is convergent.

(ii) Suppose now that $p = 1/n$. Then by Corollary 5.19

$$\begin{aligned} E(X) &\sim \sum_{k=3}^{n} k \binom{n}{k} \left(\frac{\pi}{8}\right)^{1/2} k^{k-1/2} n^{-k} \left(1 - \frac{1}{n}\right)^{kn-k^2/2-3k/2} \\ &\sim \frac{1}{4} \sum_{k=3}^{n} e^k \frac{(n)_k}{n^k} \left(1 - \frac{1}{n}\right)^{kn-k^2/2-3k/2} \\ &\sim \frac{1}{4} \sum_{k=3}^{n} e^{k^2/2n+3k/2n} \prod_{j=1}^{k-1} \left(1 - \frac{j}{n}\right). \end{aligned}$$

Since

$$\prod_{j=1}^{k-1} \left(1 - \frac{j}{n}\right) \leq \exp\left\{-\frac{k(k-1)}{2n} - \frac{k(k-1)(2k-1)}{6n^2} - k^4/(4n^3)\right\},$$

in the sum above we may assume that $k = o(n^{3/4})$. Now if $k = o(n^{3/4})$, then

$$\prod_{j=1}^{k-1} \left(1 - \frac{j}{n}\right) = \exp\left\{-\frac{k^2}{2n} - \frac{k^3}{6n^2} + O\left(\frac{k}{n} + \frac{k^4}{n^3}\right)\right\}.$$

Consequently

$$\begin{aligned} E(X) &\sim \frac{1}{4} \sum_{k=1}^{\infty} \exp\left\{-\frac{k^3}{6n^2}\right\} \sim \frac{1}{4} \int_0^{\infty} e^{-k^3/6n^2} dk \\ &= \frac{6^{1/3}}{12} n^{2/3} \int_0^{\infty} x^{-2/3} e^{-x} dx = \frac{6^{1/3}\Gamma(1/3)}{12} n^{2/3}. \end{aligned}$$

The bound on the variance follows by straightforward manipulations. □

The theorem above implies a more precise estimate of the number of vertices on unicyclic components than the one provided by Corollary 5.8.

Corollary 5.24 (*i*) *Given* $0 < c < \infty, c \neq 1$, *there is a* $b = b(c)$ *such that*

$$P\{X(G_{c/n}) > t\} \leq b/t^2 \text{ for all } t > 0.$$

In particular, if $\omega(n) \to \infty$, *then a.e.* $G_{c/n}$ *has at most* $\omega(n)$ *vertices on its unicyclic components.*

(*ii*) *If* $\omega(n) \to \infty$ *then a.e.* $G_{1/n}$ *has at most* $\omega(n)n^{2/3}$ *vertices on its unicyclic components.*

Proof Both assertions follow from Theorem 5.23 and Chebyshev's inequality □

Exercises

5.1 Prove that if $k \geq 2$ is fixed and $p = p(n) = o(n^{-1})$, then $c_1(n,k,p) + c_2(n,k,p) = o(1)$, where c_1 and c_2 are as in Theorem 5.1. Deduce that

$$d\{\mathscr{L}(T_k), P_\lambda\} \to 0,$$

where $\lambda = E(T_k)$ is the expected number of tree components of G_p having order k.

5.2 Prove Corollary 5.2.

5.3 Use Chebyshev's inequality to prove the following assertion concerning the tree components of $G_{1/n}$: if $\varepsilon > 0$ is a constant and the functions $r = r(n), s = s(n)$ satisfy $1 \leq r \leq s \leq n$, then

$$\lim_{n\to\infty} P_{1/n}\left(\left|\sum_{k=r}^{s} kT_k - n\sum_{k=r}^{s}\frac{k^{k-1}}{k!}e^{-k}\right| > \varepsilon n\right) = 0$$

and

$$\lim_{n\to\infty} P_{1/n}\left(\left|\sum_{k=r}^{s} T_k - n\sum_{k=r}^{s}\frac{k^{k-2}}{k!}e^{-k}\right| > \varepsilon n\right) = 0.$$

5.4 By classifying the forests according to the number of neighbours joined to k specified vertices, deduce that

$$F(n,k) = \sum_{t=1}^{n-k}\binom{n-t}{t}k^t F(n-k,t).$$

Use this to prove Lemma 5.17 by induction on n. [Göbel (1963), see also Moon (1970*a*, p. 17).]

5.5 By considering rooted forests with n vertices and k components, show that for $1 \leq k \leq n-1$ we have

$$\binom{n}{k}kn^{n-1-k} = \sum\binom{n}{j, n_1, n_2, \ldots, n_m} j^{n_1} n_1^{n_2} \ldots n_{m-1}^{n_m},$$

where the summation is over all ordered partitions $(n_1, n_2, \ldots, n_m)$ of $n-j$. (Katz, 1955.)

5.6 Prove that there are

$$\binom{n-2}{k-1}(n-1)^{n-k-1}$$

trees on $\{1, 2, \ldots, n\}$ in which vertex 1 has degree k. [Clarke (1958), see also Rényi (1959*a*, p. 83) and Moon (1970*a*, p. 14).]

5.7 Denote by γ_n the length of the unique cycle in a connected graph of order n and size n. Let $x > 0$ be fixed and set $r_0 = [xn^{1/2}]$. Show that, analogously to Theorem 5.16,

$$P(\gamma_n \le r_0) = \left\{ \sum_{r=3}^{r_0} \prod_{j=1}^{r-1} (1 - j/n) \right\} \Bigg/ \left\{ \sum_{r=3}^{n} \prod_{j=1}^{r-1} (1 - j/n) \right\} \to 2\Phi(x) - 1.$$

Deduce that the distribution of $\gamma_n/n^{1/2}$ tends to the distribution of the absolute value of an $N(0,1)$ r.v., so, in particular, $E(\gamma_n) \sim (2n/\pi)^{1/2}$. (Rényi, 1959*b*.)

5.8 The following proof of the first (and easy) part of Theorem 5.7(ii) was suggested by B. Pittel.

Note that if the component of a vertex x_1 contains a cycle then the graph has a path $x_1 x_2 \ldots x_k$ and an edge $x_k x_j$ for some $j, 1 \le j \le k-2$. Deduce that if $0 < c < 1$ then the expected number of vertices of $G_{c/n}$ on components containing cycles is at most

$$\sum_{k=3}^{n} (n)_k (k-2) p^k \le \sum_{k=3}^{n} k c^k < \frac{1}{(1-c)^2}.$$

6

The Evolution of Random Graphs—the Giant Component

The results of the previous chapter imply that for $c < 1$ a.e. graph process $\tilde{G} = (G_t)_0^N$ is such that for $t \sim \frac{1}{2}cn$ it satisfies $L_1(G_t) = O(\log n)$, i.e. the maximum of the orders of the components of G_t is $O(\log n)$. As t passes $n/2, L_1(G_t)$ suddenly begins to grow. The main aim of this chapter is to investigate the speed of this growth.

Erdős and Rényi (1960, 1961*a*) proved that a.e. $\tilde{G}$ is such that $L_1(G_{\lfloor n/2 \rfloor})$ has order $n^{2/3}$ and if $c > 1$ then a.e. $\tilde{G}$ satisfies

$$L_1(G_{\lfloor cn/2 \rfloor}) \sim \{1 - t(c)\}n.$$

Furthermore, a.e. $\tilde{G}$ is such that $G_{\lfloor cn/2 \rfloor}$ has a 'giant' component, that is a component whose order is much larger than the order of any other component.

In this chapter we shall present the results of Bollobás (1984*b*), which shed considerably more light on the emergence of the giant component. If t is not much larger than $n/2$, then $L_1(G_t) \sim 4t - 2n$ for a.e. $\tilde{G}$, i.e. the largest component grows about four times as fast as the number of edges. As the process continues, the larger components are swallowed up by the giant component at such a rate that the order of the second largest component decreases. By time $cn/2, c > 1$, the second largest component has order $O(\log n)$ for a.e. $\tilde{G}$.

The final section is devoted to a result of Frieze (1985*a*) concerning economical spanning trees in graphs with random weights on the edges, and a result of Bollobás and Simon (1993) about the probabilistic analysis of the Weighted Quick-Find algorithm.

6.1 A Gap in the Sequence of Components

The key result in the proof of the sudden emergence of the giant component is that from shortly after time $n/2$ most graph processes never have a component whose order is between $\frac{1}{2}n^{2/3}$ and $n^{2/3}$. In fact, the gap becomes larger as the number of edges increases. The bound $t \le n$ in the theorem below is only for the sake of convenience, it can easily be removed.

Theorem 6.1 *Let* $s_0 = (2\log n)^{1/2}n^{2/3}$ *and for* $s \neq 0$ *set* $k_0(s) = \lfloor (3\log s - \log n - 2\log\log n)n^2/s^2) \rfloor$. *Then a.e. graph process* $\tilde{G} = (G_t)_0^N$ *is such that if* $t = n/2 + s, s_0 \le |s| < n/2$ *and* G_t *has a component of order* k, *then either* $k < k_0(s)$ *or* $k > n^{2/3}$.

In particular, a.e. graph process is such that, for $t_0 = \lceil (n/2)+s_0 \rceil \le t \le n$, *the graph* G_t *has no component whose order is between* $n^{2/3}/2$ *and* $n^{2/3}$.

Proof A component of a graph will be called a (k,d)*-component* if it has k vertices and $k+d$ edges. The number of (k,d)-components will be denoted by $X(k,d)$.

Since in our theorem the cases $s < 0$ and $s > 0$ have similar proofs, we shall assume that $s > 0$ and so $t = n/2 + s > n/2$. Furthermore, as the components we are interested in have order at most $n^{2/3}$, throughout the proof we shall suppose that $k_0(s) \le k \le n^{2/3}$. Denote by $E_t(k)$ the expected number of components of order k in G_t:

$$E_t(k) = \sum [E_t\{X(k,d)\} : -1 \le d \le k^*],$$

where $k^* = \binom{k}{2} - k$.

Set $k_1(s) = \min\{\lfloor n^{2/3} \rfloor, 3k_0(s)\}$. Then $k_0(s_0) < \frac{1}{2}n^{2/3}$, the functions $k_0(s), k_1(s)$ are monotone decreasing in $s_0 \le s < n/2$ and $k_0(s+1) < 2k_1(s)$. Therefore it suffices to show that a.e. graph process is such that for $s_0 \le s < n/2$ and $t = n/2 + s$, the graph G_t has no component whose order is at least $k_0(s)$ and at most $k_1(s)$. Indeed, suppose $\tilde{G}$ is such a graph process, $t < n-1$ and G_t has no component whose order is between $k_0(s)$ and $n^{2/3}$. Since $k_1(s+1) < 2k_0(s)$, the $(t+1)$st edge of the graph process cannot merge two components of G_t with fewer than $k_0(s)$ vertices to form a component of order at least $k_1(s+1)$ in G_{t+1}. Therefore, as G_{t+1} has no component whose order is between $k_0(s+1)$ and $k_1(s+1), G_{t+1}$ does not contain a component whose order is between $k_0(s+1)$ and $n^{2/3}$. Consequently our theorem follows if we show that

$$\sum_{t=t_0}^{n} \sum_{k=k_0(s)}^{k_1(s)} E_t(k) = o(1). \tag{6.1}$$

Set $s = s(t) = t - n/2, \varepsilon = \varepsilon(t) = (2t/n) - 1 = 2s/n$ and $p = p(t) =$

$2t/n^2 = (1+\varepsilon)/n$. A slight variant of Theorem 2.2(iii) implies that in our range

$$E_t(k) \le 4n^{1/2} E_p(k),$$

where

$$E_p(k) = \sum [E_p\{X(k,d)\} : -1 \le d \le k^*].$$

Hence instead of (6.1) it suffices to prove

$$\sum_{t=t_0}^{n} \sum_{k=k_0(s)}^{k_1(s)} E_p(k) = o(n^{-1/2}). \tag{6.2}$$

By Corollary 5.21 we have

$$C(k, k+d) \le c_0 6^{-d} k^{k+(3d-1)/2}$$

for some absolute constant c_0, so

$$\begin{aligned}
E_p(k) &= \sum_{d=-1}^{k^*} E_p\{X(k,d)\} \le \binom{n}{k} c_0 \sum_{d=-1}^{k^*} 6^{-d} k^{k+(3d-1)/2} p^{k+d} \\
&\quad \times (1-p)^{kn-k(k+3)/2-d} \\
&\le c_1 \binom{n}{k} k^{k-2} p^{k-1} \exp\left\{-p\left(kn - \frac{k^2}{2}\right)\right\} \\
&\le c_2 n k^{-5/2} \exp\left\{k - \frac{k^2}{2n} + \left(\varepsilon - \frac{\varepsilon^2}{2} + \frac{\varepsilon^3}{3}\right)k - \frac{1+\varepsilon}{n}\left(kn - \frac{k^2}{2}\right)\right\} \\
&\le c_2 n k^{-5/2} \exp\left\{-\frac{\varepsilon^2}{2}k + \frac{\varepsilon^3}{3}k + \frac{\varepsilon k^2}{2n}\right\}.
\end{aligned}$$

Thus

$$E_p(k) \le c_3 n k^{-5/2} \exp\{-0.499\varepsilon^2 k + \varepsilon^3 k/3\} = F_p(k),$$

since $k/n = o(s/n) = o(\varepsilon)$.

If $\varepsilon \ge 10^{-3}$, then

$$F_p(k+1)/F_p(k) < 1 - 10^{-7}.$$

Therefore (6.2) follows if we prove that

$$\sum_{t=t_1}^{n} F_p\{k_0(s)\} + \sum_{t=t_0}^{t_1} \sum_{k=k_0(s)}^{k_1(s)} F_p(k) = o(n^{-1/2}), \tag{6.3}$$

where $t_1 = \lfloor (1.001/2)n \rfloor$. Now for $t_1 \le t \le n$, $s = s(t)$ and $k = k_0(s)$ we have

$$F_p(k) \le c_4 n k^{-5/2} \exp\left\{-\left(3.9 - \frac{8s}{3n}\right)\log n\right\}.$$

This shows that

$$\sum_{t=t_1}^{n} F_p\{k_1(s)\} = O(n^{1-3.9+4/3+1}) = o(n^{-1/2}),$$

since $s \le n/2$ for $t \le n$.

Also, if $t_0 \le t \le t_1$ and $k_0(s) \le k \le 3k_0(s)$, then

$$F_p(k) \le c_3 n k^{-5/2} \exp\{-0.49\varepsilon^2 k\}.$$

Consequently

$$\begin{aligned}
\sum_{t=t_0}^{t_1} \sum_{k=k_0(s)}^{k_1(s)} F_p(k) &= c_3 n (\log n)^{-5/2} n^{-5} \sum_{t=t_0}^{t_1} s^5 \sum_{k=k_0(s)}^{k_1(s)} \exp\{-0.49\varepsilon^2 k\} \\
&\le c_5 n^{-4} (\log n)^{-5/2} \sum_{t=t_0}^{t_1} s^5 (\log n) \frac{n^2}{s^2} \exp\{-1.9(3\log s - \log n)\} \\
&= o(1) \sum_{t=t_0}^{t_1} s^{-2} = o(n^{-1/2}),
\end{aligned}$$

completing the proof of (6.3). □

Let us call a component *small* if it has fewer than $n^{2/3}/2$ vertices, and *large* if it has at least $n^{2/3}$ vertices. By Theorem 6.1 a.e. graph process is such that for $t_0 \le t \le n$ every component of G_t is either small or large. This will enable us to show that a.e. graph process is such that shortly after time $n/2$ it has a giant component and all other components are small. Hence, the order of the giant component is the difference between n and the number of vertices on the small components. The following theorem will be used to estimate the number of vertices on the small components.

Theorem 6.2 *Suppose* $\Lambda \subset \mathbb{N} \times \{\mathbb{N} \cup \{0, -1\}\}$, $-1 < \varepsilon = \varepsilon(n) \le n/4$ *and* $p = (1+\varepsilon)/n$. *Set*

$$\begin{aligned}
X_i &= \sum \{k^i X(k,d) : (k,d) \in \Lambda\}, \\
\mu_i &= E_p(X_i)
\end{aligned}$$

and

$$\tilde{k} = \max\{k : (k,d) \in \Lambda\}.$$

If $\varepsilon \geq -(1+\varepsilon)^2/n$ *and* $\tilde{k}^2\{\varepsilon + (1+\varepsilon)^2/n\} \leq n$, *then*

$$\sigma^2(X_i) \leq \mu_{2i} + \frac{2}{n}\left\{\varepsilon + \frac{(1+\varepsilon)^2}{n}\right\}\mu_{i+1}^2$$

and if $-1 < \varepsilon \leq -(1+\varepsilon)^2/n$, *then*

$$\sigma^2(X_i) \leq \mu_{2i}.$$

Proof Analogously to (6.2) we have

$$E_p(X_i) = \sum_{(k,d)\in\Lambda} k^i \binom{n}{k} C(k, k+d) p^{k+d}(1-p)^{k(n-k)+\binom{k}{2}-k-d}. \tag{6.4}$$

Also, if (k_1, d_1) and (k_2, d_2) are distinct elements of Λ, then

$$\begin{aligned} E_p\{X(k_1,d_1)X(k_2,d_2)\} &= \binom{n}{k_1}\binom{n-k_1}{k_2} C(k_1,k_1+d_1)C(k_2,k_2+d_2) \\ &\quad \times p^{k_1+k_2+d_1+d_2}(1-p)^{(k_1+k_2)(n-k_1-k_2)+\binom{k_1+k_2}{2}-k_1-k_2-d_1-d_2} \\ &= E_p\{X(k_1,d_1)\}E_p\{X(k_2,d_2)\}\frac{(n)_{k_1+k_2}}{(n)_{k_1}(n)_{k_2}}(1-p)^{-k_1k_2}. \end{aligned} \tag{6.5}$$

Similarly, for $(k,d) \in \Lambda$,

$$E_p\{X(k,d)^2\} = E_p\{X(k,d)\} + E_p\{X(k,d)\}^2 \frac{(n)_{2k}}{(n)_k(n)_k}(1-p)^{-k^2}. \tag{6.6}$$

Relations (6.5) and (6.6) give

$$\begin{aligned} E_p(X_i^2) &= E_p(X_{2i}) + \sum \Big\{ k_1^i k_2^i E_p\{X(k_1,d_1)\}E_p\{X(k_2,d_2)\} \\ &\quad \times \frac{(n)_{k_1+k_2}}{(n)_{k_1}(n)_{k_2}}(1-p)^{-k_1k_2} : (k_1,d_1),(k_2,d_2) \in \Lambda \Big\}. \end{aligned} \tag{6.7}$$

It is easily seen (Ex. 1) that if $0 \leq x \leq y \leq 1$, then

$$1 - y \leq (1-x)\,\mathrm{e}^{x-y}.$$

Consequently

$$\frac{(n)_{k_1+k_2}}{(n)_{k_1}(n)_{k_2}} = \prod_{i=0}^{k_1-1}\left\{\left(1-\frac{k_2+i}{n}\right)\Big/\left(1-\frac{i}{n}\right)\right\}$$

$$\leq \exp\left\{\sum_{i=0}^{k_1-1}\left(\frac{i}{n}-\frac{k_2+i}{n}\right)\right\} = \exp(-k_1k_2/n). \tag{6.8}$$

Furthermore, by inequality (1.10) of Chapter 1,

$$1-p = 1-\frac{1+\varepsilon}{n} \geq \exp\left\{-\frac{1+\varepsilon}{n}-\frac{(1+\varepsilon)^2}{n^2}\right\}. \tag{6.9}$$

Inequalities (6.8) and (6.9) give

$$\begin{aligned}\frac{(n)_{k_1+k_2}}{(n)_{k_1}(n)_{k_2}}(1-p)^{-k_1k_2} &\leq \exp\left\{-\frac{k_1k_2}{n}+\frac{(1+\varepsilon)k_1k_2}{n}+\frac{(1+\varepsilon)^2k_1k_2}{n^2}\right\}\\ &= \exp\left\{\frac{k_1k_2}{n}\left(\varepsilon+\frac{(1+\varepsilon)^2}{n}\right)\right\} = 1+\delta(k_1,k_2).\end{aligned}$$

Now if $\varepsilon+(1+\varepsilon)^2/n \leq 0$, then $\delta(k_1,k_2)\leq 0$ and so, by (6.7),

$$\sigma^2(X_i) \leq E_p(X_{2i}) = \mu_{2i}.$$

Finally, if $\varepsilon \geq -(1+\varepsilon)^2/n$ and $\tilde{k}^2\{\varepsilon+(1+\varepsilon)^2/n\} \leq n$, then

$$\delta(k_1,k_2) \leq \frac{2k_1k_2}{n}\left(\varepsilon+\frac{(1+\varepsilon)^2}{n}\right).$$

Therefore (6.7) gives

$$\begin{aligned}\sigma^2(X_i) &\leq E_p(X_{2i})+\left(\frac{2\varepsilon}{n}+\frac{2(1+\varepsilon)^2}{n^2}\right)\sum\{k_1^{i+1}k_2^{i+1}E_p\{X(k_1,d_1)\}\\ &\qquad \times E_p\{X(k_2,d_2)\} : (k_1,d_1),(k_2,d_2)\in\Lambda\}\\ &= \mu_{2i}+\left(\frac{2\varepsilon}{n}+\frac{2(1+\varepsilon)^2}{n^2}\right)\mu_{i+1}^2.\end{aligned}$$

□

Given a graph G of order n, denote by $S(G)$ the maximum of $\{k : k \leq n^{2/3}$ and G has a component of order $k\}\cup\{0\}$. If p is not too close to the critical value $1/n$, then it is fairly easy to estimate $S(G_p)$ for a random graph G_p.

Theorem 6.3 *Let $-1/4 < \varepsilon = \varepsilon(n) < 1/4$, $|\varepsilon| \geq 2n^{-1/3}$, $p=(1+\varepsilon)/n$ and define*

$$g_\varepsilon(k) = \log n - \frac{5}{2}\log k + k\{\log(1+\varepsilon)-\varepsilon\} + 2\log(1/\varepsilon) + k^2\varepsilon/2n.$$

Let $k_0 = k_0(n)$ and $k_2 = k_2(n) < n^{2/3}$ be such that

$$g_\varepsilon(k_0)\to\infty \quad \textit{and} \quad g_\varepsilon(k_2)\to-\infty.$$

Then a.e. G_p is such that

$$S(G_p) < k_2$$

and if $n|\varepsilon|^3(\log n)^{-2} \to \infty$, then a.e. G_p is such that

$$k_0 < S(G_p).$$

Proof (i) As in the proof of Theorem 6.1, for $k \le n^{2/3}$

$$\sum_{d=-1}^{k^*} E_p\{X(k,d)\} \le c_1 E_p\{X(k,-1)\}.$$

Hence the expected number of components of G_p with order between k_2 and $n^{2/3}$ is at most

$$\begin{aligned}
& c_1 \sum_{k=k_2}^{n^{2/3}} E_p\{X(k,-1)\} \\
& \le c_2 n \sum_{k=k_2}^{n^{2/3}} k^{-5/2} \exp(k - k^2/2n)(1+\varepsilon)^k \left(1 - \frac{1+\varepsilon}{n}\right)^{kn-k^2/2} \\
& \le c_2 n \sum_{k=k_2}^{n^{2/3}} k^{-5/2} \exp\left\{k - k^2/2n + k\log(1+\varepsilon) - k(1+\varepsilon) + \frac{k^2}{2n}(1+\varepsilon)\right\} \\
& \le c_3 n \sum_{k=k_2}^{n^{2/3}} k^{-5/2} \exp[k\{\log(1+\varepsilon) - \varepsilon\} + k^2\varepsilon/2n] \\
& \le c_4 n k_2^{-5/2} \exp[k_2\{\log(1+\varepsilon) - \varepsilon\} + k^2\varepsilon/2n]\varepsilon^{-2} \\
& = c_4 \exp\{g_\varepsilon(k_2)\}.
\end{aligned}$$

By our choice of k_2 we have $g_\varepsilon(k_2) \to -\infty$, so almost no G_p has a component whose order is between k_2 and $n^{2/3}$.

(ii) In the proof of the second inequality we may and shall assume that $n|\varepsilon|^3(\log n)^{-2} \to \infty$ and $k_0 \to \infty$. Set $k_\varepsilon = \lfloor 8(\log n)\varepsilon^{-2} \rfloor$, $\Lambda = \{(k,-1) : k_0 \le k \le k_\varepsilon\}$ and let X_0 be as in Theorem 6.2. Then $g_\varepsilon(k_\varepsilon) \to -\infty$ and

$$\mu_0 = E(X_0) = \sum_{k=k_0}^{k_\varepsilon} E(T_k) \ge c_5 n \sum_{k=k_0}^{k_\varepsilon} k^{-5/2} \exp[k\{\log(1+\varepsilon) - \varepsilon\}].$$

Clearly $k_\varepsilon > k_0 + \varepsilon^{-2}$, so by the choice of k_0 we have $\mu_0 \to \infty$. Furthermore, we may suppose that μ_0 does not grow too fast, say $\mu_0 = o\{n|\varepsilon|^3(\log n)^{-2}\}$. Then

$$\mu_0 \varepsilon k_\varepsilon^2/n = O\{\mu_0 \varepsilon (\log n)^2 \varepsilon^{-4} n^{-1}\} = o(1).$$

Theorem 6.2 implies that

$$\sigma^2(X_0) \le \mu_0 + 3\varepsilon\mu_1^2/n \le \mu_0 + 3\varepsilon\mu_0^2 k_\varepsilon^2/n = \mu_0\{1 + o(1)\},$$

so by Chebyshev's inequality $P(X > 0) \to 1$. □

Let us state some explicit bounds for $S(G_p)$ implied by Theorem 6.3.

Corollary 6.4 *Let* $p = (1+\varepsilon)/n$.

(i) If $0 < \varepsilon < 1/2$, *then a.e.* G_p *satisfies* $S(G_p) \le 3(\log n)\varepsilon^{-2}$.

(ii) If $n^{-\gamma_0} \le \varepsilon = o\{(\log n)^{-1}\}$, $0 < \gamma_0 < 1/3$, *and* $\omega(n) \to \infty$, *then* $|S(G_p) - (2\log n + 6\log\varepsilon - 5\log\log n)\varepsilon^{-2}| \le \omega(n)\varepsilon^{-2}$ *for a.e.* G_p.

Proof (i) As we may assume that $(\log n)\varepsilon^{-2} \le n^{2/3}$, all we have to check is that $g_\varepsilon(3(\log n)\varepsilon^{-2}) \to -\infty$.

(ii) Straightforward calculations show that

$$k_0 = \{2\log n + 6\log\varepsilon - 5\log\log n - \omega(n)\}\varepsilon^{-2}$$

and

$$k_2 = \{2\log n + 6\log\varepsilon - 5\log\log n + \omega(n)\}\varepsilon^{-2}$$

satisfy the conditions in Theorem 6.3. □

The corollary above enables us to prove an analogue of Theorem 6.1 for the time after n.

Theorem 6.5 *A.e. graph process* $\tilde{G} = (G_t)_0^N$ *is such that for* $t \ge 5n/8$ *the graph* G_t *has no small component of order at least 100 log n.*

Proof By Corollary 6.4, a.e. graph process is such that for some t satisfying $3n/5 < t < 5n/8$ the graph G_t has no small component whose order is at least 75 log n. Since the union of two components of order at most $a = \lceil 100\log n\rceil$ has order at most $2a < n^{2/3}$, the assertion of the theorem will follow if we show that a.e. graph process is such that for $t \ge 3n/5$ the graph G_t has no component whose order is at least a and at most $2a$. Furthermore, since for $t \ge 2n\log n$ a.e. G_t is connected (cf. Ex. 15 of Chapter 2), it suffices to prove this for $t \le 2n\log n$.

Let $\frac{3}{5}n \le t \le 2n\log n$ and set $c = 2t/n$. Then the expected number of components of G_t having order at least a and at most $2a$ is

$$E\left(\sum_{k=a}^{2a}\sum_{d=-1}^{k^*} X(k,d)\right) = \sum_{k=a}^{2a}\binom{n}{k}\sum_{d=-1}^{k^*} C(k,k+d)\binom{\binom{n-k}{2}}{t-k-d}\Big/\binom{N}{t}$$

$$
\begin{aligned}
&\le c_0 \sum_{k=a}^{2a} (en)^k k^{-5/2} \binom{\binom{n-k}{2}}{t-k+1} \Big/ \binom{N}{t} \\
&\le c_1 \sum_{k=a}^{2a} (en)^k k^{-5/2} \left(\frac{t}{N}\right)^{k-1} \left(\frac{N-kn}{N}\right)^{t-k} \\
&\le c_2 n \sum_{k=a}^{2a} e^k k^{-5/2} c^k \, e^{-ck} \\
&= c_2 n \sum_{k=a}^{2a} k^{-5/2} (c\, e^{1-c})^k,
\end{aligned}
$$

where c_0, c_1 and c_2 are absolute constants. Since for $c = 1.2$ we have $c - 1 - \log c > 0.0176$, the last expression is at most

$$
c_3 n (\log n)^{-3/2} n^{-1.7} = o(n^{-1/2}). \qquad \square
$$

6.2 The Emergence of the Giant Component

Given a graph process $\tilde{G} = (G_t)_0^N$, denote by w_t the number of components of G_t and write $\mathscr{P}_t$ for the partition of V into the vertex sets of the components of G_t. Note that for every t either $\mathscr{P}_t = \mathscr{P}_{t+1}$ or else $w_{t+1} = w_t - 1$ and $\mathscr{P}_t$ is a refinement of $\mathscr{P}_{t+1}$.

Recall that a component is *small* if it has fewer than $n^{2/3}/2$ vertices, and it is *large* if it has at least $n^{2/3}$ vertices. Let $\tilde{G}$ be a graph process which is such that for every $t \ge t_0$ every component of G_t is either small or large. Then for $t \ge t_0$ the graph G_{t+1} has at most as many large components as G_t, since no large component of G_{t+1} can be the union of two small components of G_t. Hence if $t \ge t_0$ and the graph G_t has a component which contains all large components of G_{t_0}, then G_t has a unique large component and so has every $G_{t'}$ for $t' \ge t$.

By Theorems 6.1 and 6.5 we know that a.e. graph process $\tilde{G}$ satisfies the conditions above with $t_0 = \lceil n/2 + (2\log n)^{1/2} n^{2/3} \rceil$. Hence in order to prove that a.e. $\tilde{G}$ is such that for $t \ge t_1 > t_0$ the graph G_t has a unique large component, it suffices to show that for a.e. $\tilde{G}$ all large components of G_{t_0} are contained in a single component of G_{t_1}. Furthermore, the order of the giant component is the number of vertices which do not belong to the small components. Thus we shall know the approximate order of the giant component if we manage to estimate fairly precisely the number of vertices belonging to the small components of a typical G_t. Since such an estimate will help us to prove that the large components of G_{t_0} are likely to merge soon after time t_0, we start with this estimate.

Theorem 6.6 *Let $(\log n)^{1/2} n^{-1/3} \le \varepsilon = o(1)$, $p = (1+\varepsilon)/n$ and $\omega(n) \to \infty$. Define $0 < \varepsilon' < 1$ by $(1-\varepsilon')\, e^{\varepsilon'} = (1+\varepsilon)\, e^{-\varepsilon}$. Denote by $Y_1(G_p)$ the number of vertices of G_p on the small (k, d)-components with $d \ge 1$, by $Y_0(G_p)$ the number of vertices on the small unicyclic components and by $Y_{-1}(G_p)$ the number of vertices on the small tree components. Then a.e. G_p is such that*

(i) $Y_1 = 0$,
(ii) $Y_0 \le \omega(n)\varepsilon^{-2}$,
(iii) $\left| Y_{-1} - \frac{1-\varepsilon'}{1+\varepsilon} n \right| \le \omega(n)\varepsilon^{-1/2} n^{1/2}$

and

$$|Y_{-1} - n + 2\varepsilon n| \le \omega(n)\varepsilon^{-1/2} n^{1/2} + O(\varepsilon^2 n).$$

Proof As in the proof of Theorem 6.3, set $k_\varepsilon = \lfloor 8(\log n)\varepsilon^{-2} \rfloor$. Since $g_\varepsilon(k_\varepsilon) \to -\infty$, by Theorem 6.3 almost no G_p has a small component of order at least k_ε. Hence we may replace the Y_i's by

$$\widetilde{Y}_1 = \sum_{k=4}^{k_\varepsilon} \sum_{d \ge 1} kX(k,d), \quad \widetilde{Y}_0 = \sum_{k=3}^{k_\varepsilon} kX(k,0)$$

and

$$\widetilde{Y}_{-1} = \sum_{k=1}^{k_\varepsilon} kX(k,-1).$$

(i) Corollary 5.21 and $k_\varepsilon = O(n^{2/3})$ imply that for $k \le k_\varepsilon$

$$E\left(\sum_{d \ge 1} X(k,d) \right) = O(1) E\{X(k,1)\} = O(1) \binom{n}{k} k^{k+1} p^{k+1} (1-p)^{kn-k^2/2}.$$

Hence, with $Y_1^* = \sum_{k=4}^{k_\varepsilon} \sum_{d \ge 1} X(k,d)$, we have

$$\begin{aligned}
E(Y_1^*) & \\
&= O(1) \sum_{k=4}^{k_\varepsilon} k^{k+1} \binom{n}{k} \left(\frac{1+\varepsilon}{n} \right)^{k+1} \left(1 - \frac{1+\varepsilon}{n} \right)^{kn-k^2/2} \\
&= O(n^{-1}) \sum_{k=4}^{k_\varepsilon} k^{1/2} \exp\left[k - \frac{k^2}{2n} + \left\{ \varepsilon - \frac{\varepsilon^2}{2} + O(\varepsilon^3) \right\} k - (1+\varepsilon)k + \frac{(1+\varepsilon)k^2}{2n} \right] \\
&= O(n^{-1}) \sum_{k=4}^{k_\varepsilon} k^{1/2} \exp\{-\varepsilon^2 k/6\},
\end{aligned}$$

since

$$\varepsilon^3 k + k^2\varepsilon/n = o(\varepsilon^2 k).$$

This gives us

$$E(Y_1^*) = O(n^{-1}\varepsilon^{-3}) = o(1).$$

Therefore $Y_1^* = 0$ almost surely, and so $Y_1 = \widetilde{Y}_1 = 0$ almost surely.

(ii) Recalling that $C(k,k) \sim (\pi/8)^{1/2}k^{k-1/2}$ (Corollary 5.19), the expectation of $\widetilde{Y}_0$ is easily estimated:

$$\begin{aligned}
E(\widetilde{Y}_0) &= \sum_{k\le k_\varepsilon} kE\{X(k,0)\} \\
&= \sum_{k\le k_\varepsilon} k\binom{n}{k}C(k,k)\left(\frac{1+\varepsilon}{n}\right)^k\left(1-\frac{1+\varepsilon}{n}\right)^{kn-k^2/2+3k/2} \\
&\sim \frac{1}{\sqrt{2\pi}}\sqrt{\pi/8}\sum_{k\le k_\varepsilon}\exp\{-k\varepsilon^2/2 + k^2\varepsilon/2n + O(k\varepsilon^3) + O(k/n)\} \\
&\sim \frac{1}{4}\int_0^\infty \exp\{-x\varepsilon^2/2\}\,\mathrm{d}x = \frac{1}{2}\varepsilon^{-2}.
\end{aligned}$$

Therefore, by Markov's inequality,

$$P\{\widetilde{Y}_0 \ge \omega(n)\varepsilon^{-2}\} \to 0.$$

(iii) It is easily checked that $\varepsilon' = \varepsilon - \frac{2}{3}\varepsilon^2 + O(\varepsilon^3)$, since $0 < \varepsilon' < 1$ is defined by $(1-\varepsilon')\,\mathrm{e}^{\varepsilon'} = (1+\varepsilon)\mathrm{e}^{-\varepsilon}$. Hence it suffices to prove the first inequality.

We shall estimate $E(\widetilde{Y}_{-1})$ rather precisely and then we shall make use of Theorem 6.2 to conclude that for a.e. G_p the variable Y_{-1} is rather close to its expectation.

Set $p' = (1-\varepsilon')/n$ and write E' for the expectation in $\mathcal{G}(n,p')$. We shall exploit the fact that E and E' are rather closely related.

First of all, calculations analogous to those in (i) and (ii) show that

$$E'(\widetilde{Y}_1) = E'(n - \widetilde{Y}_0 - \widetilde{Y}_{-1}) = o(\varepsilon^{-2})$$

and

$$E'(\widetilde{Y}_0) \sim \frac{1}{2}\varepsilon^{-2}.$$

Hence

$$E'(\widetilde{Y}_{-1}) = n - \frac{1}{2}\varepsilon^{-2} + o(\varepsilon^{-2}).$$

In order to pass from $E'(Y_{-1})$ to $E(Y_{-1})$, note that for $k \le k_\varepsilon$ we have

$$
\begin{aligned}
E\{X(k,-1)\}/E'\{X(k,-1)\} &= \left(\frac{1+\varepsilon}{1-\varepsilon'}\right)^{k-1} \left(\frac{n-1-\varepsilon}{n-1+\varepsilon'}\right)^{kn-k^2/2-3k/2+1} \\
&= \left(\frac{1+\varepsilon}{1-\varepsilon'}\right)^{k-1} \left(\frac{1-\varepsilon/(n-1)}{1+\varepsilon'/(n-1)}\right)^{k(n-1)-k(k+1)/2+1} \\
&= \frac{1-\varepsilon'}{1+\varepsilon} \exp\{O(\varepsilon k^2/n)\} = \frac{1-\varepsilon'}{1+\varepsilon} + O(\varepsilon k^2/n).
\end{aligned}
$$

Consequently

$$
\begin{aligned}
E(\widetilde{Y}_{-1}) &= \frac{1-\varepsilon'}{1+\varepsilon}\left\{n - \frac{1}{2}\varepsilon^{-2} + O(\varepsilon^{-2})\right\} + O(\varepsilon/n)\sum_{k=1}^{k_\varepsilon} k^3 E'\{X(k,-1)\} \\
&= \frac{1-\varepsilon'}{1+\varepsilon} n - \frac{1}{2}\varepsilon^{-2} + O(\varepsilon^{-2}).
\end{aligned}
$$

In fact, in order to apply Theorem 6.2, we need an even better estimate of an expectation similar to the one appearing above:

$$
\begin{aligned}
E\left(\sum_{k=1}^{k_\varepsilon} k^2 X(k,-1)\right) &= O(n)\sum_{k=1}^{k_\varepsilon} k^{-1/2}\exp(-k\varepsilon^2/2) \\
&= O(n)\int_1^\infty x^{-1/2}\, \mathrm{e}^{-x\varepsilon^2/2}\, \mathrm{d}x = O(n\varepsilon^{-1}).
\end{aligned}
$$

Therefore, by Theorem 6.2 we have

$$
\sigma^2(\widetilde{Y}_{-1}) = O\{n\varepsilon^{-1} + \varepsilon(n\varepsilon^{-1})^2/n\} = O(n\varepsilon^{-1}).
$$

Consequently, by Chebyshev's inequality a.e. G_p satisfies

$$
|\widetilde{Y}_{-1} - E(\widetilde{Y}_{-1})| = o\{\omega(n)n^{1/2}\varepsilon^{-1/2}\}.
$$

Since $\varepsilon^{-2} = o(n^{1/2}\varepsilon^{-1/2})$, this implies that

$$
\left|\widetilde{Y}_{-1} - \frac{1-\varepsilon'}{1+\varepsilon} n\right| \le \omega(n)n^{1/2}\varepsilon^{-1/2}
$$

for a.e. G_p, as claimed. □

The property of having at most x vertices on the small tree components is monotone and so are the properties of having at least y vertices on the large components and at most z vertices on the small components which are trees or unicyclic graphs. Therefore by Theorem 2.2 we have the following consequence of Theorem 6.6.

Corollary 6.7 *Suppose $t = (n/2) + s$ and $\frac{1}{2}(\log n)^{1/2}n^{2/3} \le s = o(n)$ and $\omega(n) \to \infty$. Then a.e. G_t has $4s + O(s^2/n) + O\{\omega(n)n/s^{1/2}\}$ vertices on its large components, at most $\omega(n)n^2/s^2$ vertices on its small unicyclic components and $n - 4s + O(s^2/n) + O\{\omega(n)n/s^{1/2}\}$ vertices on its small tree-components.*

Now we are ready to prove the emergence of the giant component shortly after time $n/2$.

Theorem 6.8 *A.e. graph process $G = (G_t)_0^N$ is such that for every $t \ge t_1 = \lfloor n/2 + 2(\log n)^{1/2}n^{2/3} \rfloor$ the graph G_t has a unique component of order at least $n^{2/3}$ and the other components have at most $n^{2/3}/2$ vertices each.*

Proof Let $s_0 = (3\log n)^{1/2}n^{2/3}$. By Theorems 6.1 and 6.5, a.e. graph process is such that for $t \ge t_0 = \lceil n/2 + s_0 \rceil$ every component of G_t is either small or large. Therefore our theorem will follow if we show that a.e. $\widetilde{G} = (G_t)_0^N$ is such that for some $t_0 \le t \le t_1$ all large components of G_{t_0} are contained in a single component of G_{t_1}.

By Corollary 6.7, a.e. G_{t_0} has at least 3_{s_0} vertices on its large components. For such a graph $H = G_{t_0}$ we can find disjoint subsets V_1, V_2, ..., V_m of $V(H) = V$ such that

$$m \ge 5(\log n)^{1/2}, \ |V_1| \ge n^{2/3}, \quad i = 1, \dots, m,$$

each V_i is contained in some $V(C_j)$ and

$$\bigcup_{i=1}^{m} V_i = \bigcup_{j=1}^{l} V(C_j),$$

where C_1, C_2, ..., C_l are the large components of $H = G_{t_0}$. Set $p = n^{-4/3}$ and denote by H_p the random graph obtained from H by adding to it edges independently and with probability p. Then a.e. H_p has at most $t_0 + n^{2/3} < t_1$ edges, so to prove our theorem it suffices to show that $\bigcup_{i=1}^m V_i$ is contained in a single component in a.e. H_p.

What is the probability that for a given pair (i,j), $1 \le i < j \le m$, some edge of H_p joins a vertex V_i to a vertex of V_j? It is clearly at least

$$1 - (1-p)^{n^{4/3}} \ge 1 - \mathrm{e}^{-1} \ge \frac{1}{2}.$$

Hence the probability that in H_p all V_i's are contained in the same component is at least the probability that a random graph in $\mathcal{G}(m, 1/2)$

is connected. Since $m \to \infty$, this probability tends to 1 (cf. Ex. 15 of Chapter 2 and Theorem 7.3).

This completes the proof of our theorem. □

In the proof above p can be chosen to be $n^{-4/3}(\log\log n)(\log n)^{-1/2}$. Then we obtain that the large components of G_{t_0} in a.e. $\widetilde{G}$ merge into a single component by time $t_0 + n^{2/3}(\log\log n)(\log n)^{-1/2}$. Thus, once we have the gap in the sequence of the orders of the components and there are fairly many vertices on the large components, the giant component is formed in a very short time.

Theorem 6.9 *Let $t = n/2 + s$ and $\omega(n) \to \infty$. If $2(\log n)^{1/2}n^{2/3} \le s = o(n)$, then a.e. G_t is such that*

$$L_1(G_t) = 4s + O(s^2/n) + O\{\omega(n)n/s^{1/2}\}$$

and

$$L_2(G_t) \le (\log n)n^2/s^2.$$

If $n^{1-\gamma_0} \le s = o(n/\log n)$ for some $\gamma_0 < \frac{1}{3}$ then a.e. G_t satisfies

$$|L_2(G_t) - 4(6\log s - 4\log n - \log\log n)n^2/s^2| \le \omega(n)n^2/s^2.$$

Proof The assertion concerning $L_1(G_t)$ follows from Theorem 6.8 and Corollary 6.7. The inequalities concerning $L_2(G_t)$ can be read out of Theorem 6.8 and Corollary 6.4, with $\varepsilon = 2s/n$. Unfortunately, Corollary 6.4 cannot be applied as it stands, since the property in question is not convex, but the proof of Theorem 6.3 can be adapted to give an analogous result for G_t instead of G_p (see Ex. 2). □

6.3 Small Components after Time $n/2$

As t grows substantially larger than $n/2$, the global structure of a typical r.g. G_t becomes surprisingly simple: it contains no small components with many edges and all its small components have order $O(\log n)$.

Theorem 6.10 *Let $1 < c_0 < c_1$ be fixed and $\omega(n) \to \infty$.*

(i) *Set $\tau_0 = \lfloor c_0 n/2 \rfloor$, $\tau_1 = \lfloor c_1 n/2 \rfloor$ and for $\tau_0 \le t$ define $c = c(t) = 2t/n$, $\alpha = \alpha(t) = c - 1 - \log c$ and $a = a(t) = \lfloor (1/\alpha)(\log n - \frac{3}{2}\log\log n + \omega(n)) \rfloor$. Then a.e. $\widetilde{G}$ is such that for $\tau_0 \le t \le \tau_1$ the graph G_t has no small component of order at least a.*

(ii) *A.e. $\tilde{G}$ is such that if $t \geq c_0 n/2$, then every small component of G_t is a unicyclic graph or a tree, and there are at most $\omega(n) \log n$ unicyclic components.*

(iii) *For $\omega(n) \to \infty$ a.e. $\tilde{G}$ is such that if $t \geq \omega(n)n$, then every component of G_t, with the exception of its giant component, is a tree.*

Proof As most of the proof is rather similar to that of Theorem 6.3, we shall not give all the details.

It is easily seen that if β is sufficiently large, then for $t \geq \tau_0$ the expected number of small components of G_t with at least $b = \lfloor \beta \log n \rfloor$ vertices is $o(n^{-2})$. Hence a.e. $\tilde{G}$ is such that if $t \geq \tau_0$, then G_t has no small component of order at least b.

By Corollary 5.21, for $\tau_0 \leq t = cn/2 \leq \tau_2 = \tau_1 + n$ and $k \leq b$ the expected number of components of order k in G_t is at most

$$\begin{aligned} 2E_t\{X(k,-1)\} &= 2\binom{n}{k} k^{k-2} \binom{\binom{n-k}{2}}{t-k+1} \Big/ \binom{N}{t} \\ &\leq 2\frac{n^k}{k!} k^{k-2} \left(\frac{N - kn + k^2}{N}\right)^{t-k+1} \left(\frac{t}{N-t+k-1}\right)^{k-1} \\ &\leq 2(en)^k k^{-5/2}\, \mathrm{e}^{-2kt/n} (2t/n^2)^{k-1} \\ &= 4nk^{-5/2} (c\, \mathrm{e}^{1-c})^k. \end{aligned} \tag{6.10}$$

Once a small component appears in a r.g. process, it stays a component for a fairly long time. To be precise, for $t \leq 2n \log n$ and $k = O(\log n)$ the life-time of a component of order k of G_t has approximately exponential distribution with mean $n/2k$ (see Ex. 8). In particular, conditional on a component of order k, $a(t) \leq k \leq b$, being present at time t, $\tau_0 \leq t \leq \tau_1$, it will remain a component of $G_{t+1}, G_{t+2}, \ldots, G_{t+l}$ with probability at least $\frac{1}{2}$, where $l = \lceil n/4k \rceil$. Consequently, by (6.10) for $k \leq b$,

$$\begin{aligned} &P(\text{for some } \tau_0 \leq t \leq \tau_1 \text{ the graph } G_t \text{ has a component of order } k) \\ &\leq \frac{4k}{n} \sum_{t=\tau_0}^{\tau_2} 4nk^{-5/2} (c\, \mathrm{e}^{1-c})^k = 16k^{-3/2} \sum_{t=\tau_0}^{\tau_2} (c\, \mathrm{e}^{1-c})^k, \end{aligned}$$

where $c = 2t/n$.

Therefore the probability that for some $\tau_0 \leq t \leq \tau_1$ the graph G_t contains a component whose order is at least $a = a(t)$ and at most b, is not more than

$$16\sum_{t=\tau_0}^{\tau_2}\sum_{k=a(t)}^{6} k^{-3/2}(c\,e^{1-c})^k \le \sum_{t=\tau_0}^{\tau_2} \frac{16}{1-c\,e^{1-c}} a^{-3/2}(c\,e^{1-c})^a$$

$$= O\{(\log n)^{-3/2}\}\sum_{t=\tau_0}^{\tau_2}(c\,e^{1-c})^a$$

$$= O\{(\log n)^{-3/2}\}\sum_{t=\tau_0}^{\tau_2}\exp\{-\log n + \tfrac{3}{2}\log\log n - \omega(n)\} = o(1).$$

In the second inequality we made use of $\log(c\,e^{1-c}) = -\alpha$. This completes the proof of (i).

The proofs of (ii) and (iii) are similar. □

The reason for the inequality $t \le \tau_1$ in part (i) of the theorem was to enable us to use a fairly small function for $a(t)$. With $a' = \lceil(2/\alpha)\log n\rceil$ no upper bound has to be put on t (see Ex. 9).

Let $c_0 > 1$, $c = 2t/n \ge c_0$ and let α and a be as in Theorem 6.10. By Corollary 5.19 the expected number of unicyclic components of G_t having order at most a is not more than

$$2\sum_{k=3}^{a}\binom{n}{k}k^{k-1/2}\left(\frac{2t}{n^2}\right)^k\left(1-\frac{2t}{n^2}\right)^{kn} \le \sum_{k=3}^{a}k^{-1}(c\,e^{1-c})^k = O(1),$$

and the expected number of vertices on unicyclic components of G_t is also $O(1)$. Recall that by Corollary 5.8 we have a similar assertion for $c < 1$.

Theorem 5.9 gives a rather precise estimate of the number of vertices on tree components of G_p. This estimate can be carried over to our graph G_t, since the number of vertices on tree components is a monotone decreasing function: if $G \subset H$ and $V(G) = V(H)$ then H has at most as many vertices on its tree components as G. Finally, an analogue of Theorem 5.10 gives an estimate of the maximum order of a tree component of G_t. Hence we arrive at the following result.

Theorem 6.11 *Let $c > 1$ be a constant, $t = \lfloor cn/2\rfloor$ and $\omega(n) \to \infty$. Then a.e. G_t is the union of the giant component, the small unicyclic components and the small tree components. There are at most $\omega(n)$ vertices on the unicyclic components. The order of the giant component satisfies*

$$|L_1(G_t) - \{1 - t(c)\}n| \le \omega(n)n^{1/2},$$

where

$$t(c) = \frac{1}{c}\sum_{k=1}^{\infty}\frac{k^{k-1}}{k!}(c\,e^{-c})^k,$$

and for every fixed $i \geq 2$

$$|L_i(G_t) - (1/\alpha)\left(\log n - \frac{5}{2}\log\log n\right)| \leq \omega(n),$$

where $\alpha = c - 1 - \log c$.

In the range of t covered by Theorem 6.9, the giant component increases about four times as fast as t. Another way of proving Theorem 6.9 would be to establish this fact first and then use it to deduce the assertion about the size of the giant component. What is the expectation of the increase of $L_1(G_t)$ as $t = (1+\varepsilon)n/2 = n/2 + s$ changes to $t+1$? The probability that the $(t+1)$st edge will join the giant component to a component of order L_j is about $L_1 L_j / \binom{n}{2}$. Hence the expectation increase of $L_1(G_t)$ is about

$$\begin{aligned}
(2L_1/n^2)\sum_{k=1}^{n^{2/3}} k^2 \binom{n}{k} k^{k-2}\left(\frac{1+\varepsilon}{n}\right)^{k-1}\left(1-\frac{1+\varepsilon}{n}\right)^{kn-k^2/2} \\
\sim (2L_1/n^2)\sum_{k=1}^{n^{2/3}}\frac{n}{\sqrt{2\pi}}k^{-1/2}\exp(-\varepsilon^2 k/2) \\
\sim \left(\frac{2}{\pi}\right)^{1/2}(L_1/n)\int_0^{\infty} x^{-1/2}\,\mathrm{e}^{-x\varepsilon^2/2}\,\mathrm{d}x \\
= \left(\frac{2}{\pi}\right)^{1/2}(L_1/n)\Gamma\left(\frac{1}{2}\right)(\varepsilon^2/2)^{-1/2} = 2L_1/(\varepsilon n) = L_1/s.
\end{aligned}$$

From this one can deduce that if t is $o(n)$ but not too small, then $L_1(t) = L_1(n/2+s) \sim c_1 s$. Since $t'(1) = -2$, by Theorem 6.11 we must have $c_1 = 4$.

In the rest of this section we shall investigate the number of components of G_t. For $t = \lfloor cn/2 \rfloor$, $c < 1$, Corollary 5.8 and Theorem 5.12 imply precise bounds on the number of components of almost every G_t. Theorem 6.11 shows that if $c > 1$ and $t = \lfloor cn/2 \rfloor$, then most components of a.e. G_t are trees. Since the number of tree components is a monotone decreasing function, Theorem 5.12 implies the following result.

Theorem 6.12 *Let $0 < c < \infty$, $c \neq 1$, $t = \lfloor cn/2 \rfloor$ and denote by $w = w(G_t)$ the number of components of G_t. Then for $\omega(n) \to \infty$ a.e. G_t satisfies*

$$|w(G_t) - u(c)n| \le \omega(n)n^{1/2},$$

where

$$u(c) = \frac{1}{c}\sum_{k=1}^{\infty}\frac{k^{k-2}}{k!}(c\,e^{-c})^k.$$

If we sacrifice the approximation in Theorem 6.12, we can get an approximation of $w(G_t)$ holding for all not too large values of t.

Theorem 6.13 *Let $\frac{2}{3} < \beta < 1$ be fixed and $t = cn/2$ where $c = c(n) \le 8\log n$. Then*

$$P\{|w(G_t) - u(c)n| \ge (\log n)n^\beta\} \le 100n^{1-2\beta}(\log n)^{-1}.$$

Proof Assume first that $t \neq \lfloor n/2 \rfloor + 1$, $\lfloor n/2 \rfloor + 2$, so that $c \le 1$ or $c \ge 1 + 4/n$. Let $p = c/n$, $\tilde{k} = \lfloor \frac{1}{4}n^{1/2}(\log n)^{-1/2} \rfloor$, and denote by $w^*(G)$ the number of components of order at most $\tilde{k}$ in a graph G. Put

$$\Lambda = \left\{(k,d) : 1 \le k \le \tilde{k}, -1 \le d \le \binom{k}{2} - k\right\},$$

and let X_0, X_1 and μ_0, μ_1 be as in Theorem 6.2. Note that our choice of the parameters ensures that the conditions of Theorem 6.2 are satisfied.

By definition $\mu_0 = E_p(X_0) = E(w^*(G_p))$. Furthermore, $X_1(G_p)$ is the number of vertices of G_p on components of order at most $\tilde{k}$ so $X_1 \le n$ and $\mu_1 \le n$.

Therefore, by Theorem 6.2,

$$\begin{aligned}\sigma^2(X_0) &\le \mu_0 + \left(\frac{16\log n}{n} + \frac{128(\log n)^2}{n^2}\right)n^2\\ &\le 17(\log n)n.\end{aligned}$$

Hence, by Chebyshev's inequality

$$P\left\{|X_0 - \mu_0| \ge \frac{1}{2}(\log n)n^\beta\right\} \le 68(\log n)^{-1}n^{1-2\beta}. \tag{6.11}$$

Straightforward calculations imply that

$$|\mu_0 - u(c)n| \le n^{2/3}. \tag{6.12}$$

Clearly

$$w^*(G_p) \le w(G_p) \le w^*(G_p) + n^{1/2}. \tag{6.13}$$

Inequalities (6.11), (6.12) and (6.13) imply

$$P\left\{|w(G_p) - u(c)n| \geq \tfrac{2}{3}(\log n)n^{\beta}\right\} \leq 68(\log n)^{-1}n^{1-2\beta}.$$

Finally, since $n \geq w(G_t) \geq w(G_{t+1}) \geq 1$ for every t, by the De Moivre-Laplace theorem (Theorem 1.6) we have for every t, $0 \leq t \leq 4n\log n$, that

$$P\{|w(G_t) - u(c)n| \geq (\log n)n^{\beta}\} \leq 100(\log n)^{-1}n^{1-2\beta},$$

as claimed. □

The function $u(c)$ is monotone decreasing, and so is $w(G_t)$ for every graph process $\tilde{G}$. Therefore Theorem 6.13 has the following immediate consequence.

Corollary 6.14 *The probability that for a fixed β a graph process $\tilde{G} = (G_t)_0^N$ satisfies*

$$|w(G_t) - u(2t/n)n| \leq 2(\log n)n^{\beta}$$

for every $t \leq 4n\log n$ is $1 - o(n^{2-3\beta})$. □

6.4 Further Results

The theorems in the previous sections are only the tip of the iceberg: Łuczak and Wierman (1989), Łuczak (1990*b*), Janson, Knuth, Łuczak and Pittel (1993), Łuczak, Pittel and Wierman (1994) and others proved numerous deep results about the behaviour of a random graph process (G_t) near its *phase transition*, i.e., near the time $t = n/2$. The deepest and most substantial study to date is that of Janson, Kauth, Łuczak and Pittel (1993), whose approach was not probabilistic: they used precise estimates of generating functions to obtain remarkably detailed results. In this section we shall sketch only some of the important results about the phase transition and the *supercritical range*, i.e., the range beyond the phase transition.

Let us define the *excess* $\mathrm{exc}(G)$ of a graph G as the maximal value of d for which G has a (k, d)-component, i.e., a component with k vertices and $k + d$ edges. Call a connected graph *complex* if it contains at least two cycles, i.e., if its excess is at least 1. Using this terminology, Theorem 6.6.(i) states that in that range almost no G_p is complex.

Theorem 6.9 tells us that the giant component of G_t arises when $t \geq n/2 + \omega(n)n^{2/3}$ and $\omega(n) \geq 2(\log n)^{1/2}$. It is clear from the proof that this bound $2(\log n)^{1/2}$ was only a slowly increasing function that enabled us to prove the required estimates. Łuczak (1990*b*) showed that it suffices to assume that $\omega(n) \to \infty$, so the 'window' of the phase transition of a random graph process is $O(n^{2/3})$. Here we shall state this result of Łuczak (1990*b*) for the entire supercritical range, but in a slightly weaker form.

In Theorem 6.6 for $\varepsilon > 0$ we defined $0 < \varepsilon' < 1$ by $(1-\varepsilon')e^{\varepsilon'} = (1+\varepsilon)e^{-\varepsilon}$. Similarly, for $s > 0$, define $0 < s' < n/2$ by

$$\left(1 - \frac{2s'}{n}\right) 2^{2s'/n} = \left(1 + \frac{2s}{n}\right) e^{-2s/n}.$$

Putting it slightly differently, with $\varepsilon = 2s/n$, we set $s' = \varepsilon' n/2$. Note that with $p = \frac{1+\varepsilon}{n}$ and $p' = \frac{1-\varepsilon'}{n}$, a random graph G_p has about $\frac{n}{2} + s$ edges and $G_{p'}$ about $\frac{n}{2} - s'$.

Theorem 6.15 *Let $t = \frac{n}{2} + s$, where $s/n^{2/3} \to \infty$. Then a.e. G_t is such that*

$$|L_1(G_t) - \frac{2(s+s')n}{n+2s}| = |L_1(G_t) - \frac{\varepsilon + \varepsilon'}{1+\varepsilon}n| \leq n^{2/3}/5.$$

Furthermore, the largest component is complex, and every other component is either a tree or unicyclic, and has at most $n^{2/3}$ vertices. □

Łuczak (1990*b*) gave the following precise estimate for the excess of G_t in the supercritical range.

Theorem 6.16 *Let $\omega(n) \to \infty$, and $t = n/2 + s$, where $\omega(n)n^{2/3} \leq s \leq n/\omega(n)$. Then a.e. G_t is such that*

$$\left| exc(G_t) - \frac{16s^3}{3n^2} \right| \leq \omega^{-0.1} s^3/n^2. \qquad \square$$

Janson, Knuth, Łuczak and Pittel (1993) extended this result: they showed that $\mathrm{exc}(G_t)$, suitably normalized, has asymptotically normal distribution.

Taking up a suggestion of Erdős, Janson (1987), Bollobás (1988*b*) and Flajolet, Knuth and Pittel (1989) studied the length $\xi_n = \xi(\widetilde{G})$ of the first cycle that appears in a random graph process $\widetilde{G} = (G_t)_0^N$ on n vertices. Rather interestingly, $E(\xi_n) \to \infty$ as $n \to \infty$, but ξ_n has a beautiful limit distribution.

Theorem 6.17 . *For every $k \geq 3$,*

$$\lim_{n\to\infty} P(\xi_n = k) = \frac{1}{2}\int_0^1 t^{k-1}e^{t/2+t^2/4}\sqrt{1-t}dt.$$

Furthermore,

$$E\xi_n \sim \frac{\pi^{1/2}\Gamma(1/3)}{2^{1/6}3^{2/3}}n^{1/6}.$$

In fact, Flajolet, Knuth and Pittel (1989) also accomplished the difficult task of giving precise estimates for all the moments of ξ_n, and Janson, Knuth, Łuczak and Pittel (1993) also proved a number of related detailed results. The first cycle in a certain random directed graph process, thought to be relevant to the explanation of the origin of life based on the idea of self-organization, as expounded by Eigen and Schuster (1979), was studied by Bollobás and Rasmussen (1989).

Let us turn to the k-core of a graph, introduced by Bollobás (1984*a*). For $k \geq 2$, the *k-core* $\text{core}_k(G)$ of a graph G is the maximal subgraph of minimal degree at least k. The 2-core is simply the *core* of the graph: $\text{core}(G) = \text{core}_2(G)$. As every graph of minimal degree at least 2, the core is made up of some vertex disjoint cycles and a set of branchvertices (vertices of degree at least 3) joined by vertex disjoint paths. There is a unique multigraph K of minimal degree at least 3 such that the 2-core of G is a subdivision of K. This multigraph K is the *kernel* $\ker(G)$ of G. Here the term 'multigraph' is used in a wide sense: in addition to loops and multiple edges, vertexless loops (called *free loops*) are allowed as well. Note that the multigraph M defined in the proof of Theorem 5.20 was precisely the kernel of $G \in \mathscr{C}(n, n+k)$.

Łuczak (1991*a*) conducted a detailed study of the core just beyond the critical probability $n/2$. Let us write $D_k(G)$. For the number of vertices of degree k in the core of G. Among other results, Łuczak (1991*a*) proved that if $t = n/2 + s$, where $s = o(n)$ and $s/n^{2/3} \to \infty$, then a.e. G_t is such that $D_2(G_t) \sim 8s^2/n$, $D_3(G_t) \sim 32s^3/3n^2$ and, for every fixed k, $D_k(G_t) = O(s^k/n^{k-1})$. Furthermore, a.e. G_t contains an induced topological random cubic graph on about $32s^3/3n^2$ vertices.

Since by the theorem of Robinson and Wormald (1992) a.e. cubic graph has a Hamilton cycle (see Theorem 8.22), a.e. G_t has a cycle that goes through about $32s^3/3n^2$ cubic vertices of the core. By tightening and continuing this argument, Łuczak (1991*a*) was able to give a good estimate of the *circumference*, the length of a longest cycle, of a random graph.

Theorem 6.18 *Let $t = n/2 + s$, where $s = o(n)$ and $s/n^{2/3} \to \infty$. Then a.e. G_t has circumference at least $(16 + o(1))s^2/3n$ and at most $15s^2/2n$.* □

Łuczak, Pittel and Wierman (1994) showed that the transition range from being planar to being non-planar is precisely the window of the phase-transition.

Theorem 6.19 *There is a function $f : \mathbb{R} \to (0,1)$ such that if $c \in \mathbb{R}$, $t = t(n) = n/2 + s$ and $s/n^{2/3} \to c$ as $n \to \infty$, then*

$$\lim_{n\to\infty} \mathbb{P}(G_t \text{ is non-planar}) = f(c).$$

Furthermore, $\lim_{c\to-\infty} f(c) = 0$ *and* $\lim_{c\to\infty} f(c) = 1$.

The smallest non-planar subgraph of the first non-planar graph G_t in a random graph process $\widetilde{G}$ is likely to have order $cn^{2/3}$, so in some sense the problem of non-planarity is still a rather local question. This is not the case with the k-core for $k \geq 3$: the very first non-empty k-core is a 'giant' subgraph, with order proportional to n. To state this precisely, let τ_k be the *hitting time of the k-core*, i.e., for $\widetilde{G} = (G_t)_0^N$ set

$$\tau_k(\widetilde{G}) = \min\{t : \quad \mathrm{core}_k(G_t) \neq \emptyset\}.$$

Furthermore, let $\gamma_k(\widetilde{G})$ be the order of the k-core at the time it emerges:

$$\gamma_k(\widetilde{G}) = |\mathrm{core}_k(G_{\tau_k})|.$$

The following beautiful and difficult result about the sudden emergence of the k-core was proved by Pittel, Spencer and Wormald (1996).

Theorem 6.20 *For every $k \geq 3$ there are constants $c_k > 1$ and $p_k > 0$ such that $\tau_k(\widetilde{G}) \sim c_k n/2$ and $\gamma_k(\widetilde{G}) \sim p_k n$ for a.e. graph process $\widetilde{G}$. Furthermore, c_k and p_k can be expressed in terms of Poisson branching processes. In particular, $c_k = \min_{\lambda>0} \lambda/\pi_k(\lambda) = k + \sqrt{k \log k} + O(\log k)$, where $\pi_k(\lambda) = P(\mathrm{Poisson}(\lambda) \geq k-1)$.* □

The above problem of finding a non-empty k-core looks rather similar to that of finding a subgraph that is not k-colourable. Nevertheless, the latter problem seems considerably harder and is rather far from being solved, as we shall see in §5 of Chapter 11.

Molloy and Reed (1995) studied the phase transition in a refinement of the models $\mathcal{G}(n,p)$ and $\mathcal{G}(n,M)$. Let $\lambda_0, \lambda_1, \ldots$ be a sequence of non-negative reals with $\sum \lambda_i = 1$. Consider the space of all graphs on n labelled vertices in which the number n_i of vertices of degree i satisfies

$|n_i - \lambda_i n| < 1$ for every i. Molloy and Reed (1995) proved that the existence of a giant component is governed by the quantity $Q = \sum i(i-z)\lambda_i$. If $Q > 0$ then a.e. random graph in this space has a giant component, and if $Q < 0$ then almost no random graph has a giant component.

In conclusion, let us say a few words about the various approaches to random graph problems, especially phase transitions. 'Statistical graph theory' had existed before Erdős and Rényi started their work on random graphs, but its aim was exact enumeration. Generating functions were found and then analytic methods were applied to obtain asymptotics. In this method there was nothing probabilistic, random variables and probability spaces were not mentioned.

Erdős and Rényi introduced an entirely novel approach—rather than strining for exact enumeration, they adopted a probabilistic point of view and treated every graph property as a random variable on a certain probability space. This is precisely the method we apply much of the time in this book; in particular, the results in this chapter were obtained by this 'static' probabilistic method.

It is fascinating to note that *percolation theory* (the theory of random subgraphs of lattices) was started by Broadbent and Hammersley (1957) at about the some time as Erdős and Rényi were laying the foundations of the theory of random graphs, but the two theories were developed with minimal interaction (see Grimmett (1999)). By now there is more and more interaction between the two disciplines; for example, the detailed study of the phase transition in the *mean-field random-cluster model* by Bollobás, Grimmett and Janson (1996) was based on the properties of the phase transition in the random graph process $(G_t)_0^N$

The original approach to random graphs based on generating functions is far from out of date; rather the opposite is true: it is more powerful than ever. This approach may require much work and technical expertise, but it can produce deep and difficult results. Perhaps the best examples of this can be found in the monumental paper of Janson, Knuth, Łuczak and Pittel (1993) about the structure of a random graph process next to its phase transition.

In addition to natural mixtures of these two basic approaches, there are several other lines of attack; perhaps the most exciting of these is the *dynamical approach* pioneered by Karp (1990). (The germs of this method can be found in the work of Erdős and Rényi.) In Karp's dynamical approach edges are 'uncovered' or 'tested' only when we need them: the random graph G_p unravels in front of our eyes, much as a birth process.

For example, to construct the vertex set of the component of a vertex u of $G_p \in \mathscr{G}(n,p)$, we may construct a sequence $(T_i, R_i)_0^l$ of subsets of $V(G_p)$ with $T_i \subset R_i$ as follows. Set $T_0 = \emptyset$ and $R_0 = \{u\}$. Having constructed the random sets (T_k, R_k), if $T_k = R_k$ then we set $l = k$ and stop the sequence. Otherwise, pick a vertex $t_{k+1} \in R_k/T_k$, set $T_{k+1} = T_k \cup \{t_{k+1}\}$, text the graph G_p for its potential edges joining t_{k+1} to vertices outside R_k, and add all the neighbours of t_{k+1} to R_k to obtain R_{k+1}. What is happening is this: at time k set T_k is the set of vertices we have tested and R_k is the set of vertices we have reached from u. Clearly, $T_l = R_l$ is precisely the vertex set of the component of u in G_p: at time l we have tested all the vertices that we have reached, so no other vertices can be reached from u.

As $|T_k| = k$ for every k, the component of u has $|T_l| = l$ vertices; furthermore, $|R_{k+1} \backslash R_k|$ has a binomial distribution with parameters $n - |R_k|$ and p. To find the other components, we start the same process on the remainder $V(G_p)\backslash|T_l|$, then on what remains after the removal of the next component, and so on.

Needless to say, this is only the beginning, and much work needs to be done to obtain worthwhile results. Karp (1990) used this approach to describe precisely the component structure of a random *directed* graph near its phase transition, but the some approach can be used to prove sharp results about the component structure of random graphs. For some results in this vein, see Bollobás, Borgs, Chayes, Kim and Wilson (2000).

6.5 Two Applications

There are several applications of the results concerning the global structure of random graph processes; here we shall describe two of them.

Let $\widetilde{X} = \{X_{ij} : 1 \le i < j \le n\}$ be a sample of size $N = \binom{n}{2}$ from the uniform distribution on [0, 1]. Assign weight X_{ij} to the edge ij of the complete graph with vertex set $V = \{1, 2, \ldots, n\}$ and denote by $H_n = H(\widetilde{X})$ the *random weighted graph* obtained in this way. Denote by $s(H_n)$ the *minimum weight of a spanning tree* of H_n. That is the expected value of $s(H_n)$, and what is the probability that $s(H_n)$ is close to its expectation? Our first aim in this section is to present a theorem of Frieze (1985*a*) answering these questions. At the first sight it is rather surprising that the answers are very elegant. Earlier a slightly weaker bound on the expectation was obtained by Fenner and Frieze (1982). Related problems were studied by Lueker (1981), Steele (1981) and Walkup (1979); see the discussion of the random assignment problem at the end of §30 Chapter 7.

Theorem 6.21 *(i)* $\lim_{n\to\infty} E\{s(H_n)\} = \zeta(3) = \sum_{k=1}^{\infty} k^{-3} = 1.202\ldots$.
(ii) For every $\varepsilon > 0$

$$\lim_{n\to\infty} P\{|s(H_n) - \zeta(3)| \geq \varepsilon\} = 0.$$

Proof Since H_n is a function of $\widetilde{X}$, we shall write $s(\widetilde{X})$ for $s(H_n)$. Let $X_{(1)} \leq X_{(2)} \leq \ldots \leq X_{(N)}$ denote the order statistics of the sample $\widetilde{X} = (X_{ij})$. With probability 1 no two X_{ij}'s take the same value, so with probability 1 we have $X_{(1)} < X_{(2)} < \ldots < X_{(N)}$. In this case $\widetilde{X} = (X_{ij})$ defines a graph process $\widetilde{G} = \widetilde{G}(\widetilde{X}) = (G_t)_0^N$ in a natural way: the edge set of G_t is

$$\{ij : X_{ij} = X_{(k)} \text{ for some } k \leq t\}.$$

Thus the edges of G_t are the t least expensive edges.

For this graph process $\widetilde{G}$ set

$$\psi(k) = \min\{t : w(G_t) = n - k\}, k = 1, 2, \ldots, n-1.$$

Then $\psi(1) = 1$ and $\psi(n-1)$ is the first time t when the graph G_t is connected. By the greedy algorithm of Kruskal (1954) (see also Bollobás, 1979*a*, Chapter I) an economical spanning tree of H_n is formed by the edges of $\widetilde{G}$ appearing at times $\psi(1)$, $\psi(2)$, …, $\psi(n-1)$, i.e.

$$s(\widetilde{X}) = \sum_{k=1}^{n-1} X_{\psi(k)}.$$

By Ex. 15 in Chapter 2

$$P(G_{\lfloor 2n\log n\rfloor} \text{ is disconnected}) = O(n^{-3}), \tag{6.14}$$

so with probability $1 - O(n^{-3})$ we have $\psi(n-1) \leq 2n\log n$. The r.v. $X_{(i)}$ is rather close to the constant $i/(N+1)$. To be precise, $E(X_{(i)}) = i/(N+1)$ and by a standard result in probability theory for every $\varepsilon > 0$ we have

$$\sup\left\{P\left\{\left|\sum_{i\in I} X_{(i)} - \sum_{i\in I} i/(N+1)\right| \geq \varepsilon\right\} :\right.$$
$$\left. I \subset \{1, 2, \ldots, \lfloor 2n\log n\rfloor\}, |I| = n-1\right\} = o(1).$$

Therefore in our proof we may replace $s(\widetilde{X})$ by

$$s'(\widetilde{X}) = \sum_{k=1}^{n-1} \psi(k)/(N+1).$$

Set $n_0 = n - \lfloor n^{7/8} \rfloor$. If $\psi(n-1) \leq 2n \log n$, then

$$\sum_{k=n_0}^{n-1} \psi(k)/(N+1) = O\left(\frac{n(\log n) n^{7/8}}{n^2}\right) = o(1),$$

so we may replace $s'(\widetilde{X})$ by

$$s''(\widetilde{X}) = \sum_{k=1}^{n_0} \psi(k)/(N+1).$$

About how large is $\psi(k)$? Since $\psi(k)$ is the first t for which G_t has $n-k$ components, and by Corollary 6.14 a graph G_t has about $u(2t/n)n$ components, $\psi(k)$ is about $\psi_0(k)$, where $\psi_0(k)$ is defined by

$$u\{2\psi_0(k)/n\}n = n - k.$$

To be precise, if $k \leq n_0$, then

$$u\{2\psi_0(k)/n\} \geq \lfloor n^{7/8} \rfloor / n$$

and so

$$\exp[-2\{\psi_0(k) + n^{8/9}\}/n] \geq \frac{1}{2} n^{-1/8}$$

since $u(c)\,\mathrm{e}^c \to 1$ as $c \to \infty$. Easy calculations show that $|u'(c)| \geq \frac{1}{2}\,\mathrm{e}^{-c}$ (Ex. 10). Hence, for $k \leq n_0$

$$\begin{aligned} u[2\{\psi_0(k) + n^{8/9}\}/n]n \;&\leq\; n - k - \frac{1}{4} n^{-1/8} 2n^{8/9} \\ &<\; n - k - 3(\log n) n^{3/4} \end{aligned} \tag{6.15}$$

and, similarly,

$$u[2\{\psi_0(k) - n^{8/9}\}/n]n > n - k + 3(\log n) n^{3/4}. \tag{6.16}$$

By applying Corollary 6.14 with $\beta = \frac{3}{4}$ we see that with probability $1 - o(n^{-1/4})$

$$|w(G_t) - u(2t/n)n| \leq 2(\log n) n^{3/4} \tag{6.17}$$

for every $t \leq 4n \log n$. Hence by (6.14), (6.15), (6.16) and (6.17) with probability $1 - o(n^{-1/4})$

$$\psi_0(k) - n^{8/9} \leq \psi(k) \leq \psi_0(k) + n^{8/9}. \tag{6.18}$$

This leads us to our final approximation of $s(\widetilde{X})$:

$$s_0(n) = \sum_{k=1}^{n_0} \psi_0(k)/(n+1)$$

Inequalities (6.14) and (6.18) show that

$$E\{s''(\widetilde{X})\} = s_0(n) + O(n^{-1/9})$$

and with probability $1 - o(n^{-1/4})$

$$s''(\widetilde{X}) = s_0(n) + O(n^{-1/9}).$$

All that remains to show is that $\lim_{n\to\infty} s_0(n) = \zeta(3)$. This can be done by straightforward calculations:

$$\lim_{n\to\infty} s_0(n) = \lim_{n\to\infty} \frac{2}{n^2} \sum_{k=1}^{n_0} \psi_0(k) = \lim_{n\to\infty} \frac{2}{n} \int_1^{t_0} t \, du(2t/n),$$

where $t_0 = \psi_0(n_0)$. Clearly $t_0 \sim \frac{1}{16} n \log n$ since $e^{-2t_0/n} n \sim u(2t_0/n)n = n - n_0 \sim n^{7/8}$. Hence

$$\begin{aligned}
\lim_{n\to\infty} s_0(n) &= \lim_{n\to\infty} \frac{2}{n} \int_1^{t_0} t u'(2t/n) \frac{2}{n} \, dt = \lim_{n\to\infty} \frac{4}{n^2} \int_0^{\infty} \frac{xn}{2} u'(x) \frac{n}{2} \, dx \\
&= \int_0^{\infty} x u'(x) \, dx = \int_0^{\infty} u(x) \, dx,
\end{aligned}$$

where the last equality followed by partial integration. Since

$$u(x) = \sum_{k=1}^{\infty} \frac{k^{k-2}}{k!} x^{k-1} e^{-kx},$$

we have

$$\lim_{n\to\infty} s_0(n) = \sum_{k=1}^{\infty} \frac{k^{k-2}}{k!} \int_0^{\infty} x^{k-1} e^{-kx} \, dx = \sum_{k=1}^{\infty} k^{-3} = \zeta(3),$$

completing the proof. □

Steele (1987) noted that the above theorem of Frieze holds for a under class of distribution: if the distribution function F of X_{ij} is differentiable from the right at 0 and $\alpha = F'(0) > 0$ then $s(H_n)$ converges to $\zeta(3)/\alpha$ in probability.

This result was sharpened by Frieze and McDiarmid (1989): by making use of martingale inequalities like Theorems 1.19 and 1.20, they proved that $s(H_n) \to \zeta(3)/\alpha$ with probability 1.

The second application of random graph processes we shall present concerns the probabilistic analysis of the Weighted Quick-Find (WQF) algorithm. First we have to set the scene. The Union-Find problem of Aho, Hopcroft and Ullman (1974) asks for maintaining a representation of a partition of an n-set S in such a way that the two self-explanatory operations called *Find*$[x]$ and *Union*$[x, y]$ can be carried out efficiently. One of the simplest algorithms proposed for this problem uses an array *Name*$[x]$ to store the name of the equivalence class that contains x, and for each name s and linked list $L[s]$ of all the elements in the equivalence class of u. The result of *Find*$[x]$ for $x \in S$ is the name *Name*$[x]$, and the result of *Union*$[x,y]$ for $x, y \in S$ is a new partition of S in which the equivalence classes C_x and C_y of x and y are merged into the single equivalence class $C_x \cup C_y$. To implement *Union*$[x,y]$, where *Name*$[x] \neq$ *Name*$[y]$, one must set *Name*$[u] \leftarrow$ *Name*$[y]$ for each u in $L[$*Name*$[x]]$ and append $L[$*Name*$[x]]$ to $L[$*Name*$[y]]$. Hence the cost is proportional to $|C_x|$, the cardinality of the equivalence class C_x of x. By maintaining a separate array $N[s]$ with the cardinality of the equivalence class s and changing the name of the elements in the *smaller* of the two classes, the cost *Union*$[x, y]$ can be reduced to $\min\{|C_x|, |C_y|\}$. This is the *Weighted Quick-Find* algorithm.

The average use behaviour was studied by Doyle and Rivert (1976), Yao (1976), Knuth and Schönhage (1978), and Bollobás and Simon (1993) under various models; here we consider the model closest to random graphs.

A random graph process $\widetilde{G} = (G_t)_0^N$ has a sequence of Unions in WQF naturally associated with it: the tth operation is *Union*$[x, y]$ if the tth edge in $\widetilde{G}$ or *weight* is xy, i.e. if $G_t = G_{t-1} + xy$. The *cost* or *weight of* this edge is $w(x, y) = \min\{|C_x|, |C_y|\}$ if xy joins two components of G_{t-1}, with vertex sets C_x and C_y. If xy joins two vertices of the some component of G_{t-1} then $w(x, y) = 0$. Finally, the cost $W(\widetilde{G})$ of the graph process $\widetilde{G}$ relative to WQF is the sum of the costs of its edges. Here is then the result of Bollobás and Simon (1993) concerning the expectation of $W(\widetilde{G})$.

Theorem 6.22 *The expected cost of a random graph process $\widetilde{G}$ relative to the Weighted Quick-Find algorithm is*

$$E(\widetilde{G}(W)) = c_0 n + O(n/\log n),$$

where

$$\begin{aligned} c_0 &= \log 2 - 1 + \sum_{k\geq 1} \left(\frac{1}{k} - \frac{k^k}{k!} \sum_{l=1}^{k-1} \frac{l^{l-1}}{l!} \frac{(k+l-2)!}{(k+l)^{k+l-1}} \right) \\ &= 2.0847\ldots. \end{aligned}$$

□

Strictly speaking, the value 2.0847 ... for the Bollobás–Simon constant is due to Knuth (2000, Chapter 21), who gave precise estimates for it and determined it up to 45 decimal places.

It is interesting to note, that the analogous expectation for the Quick—Find algorithm in which $w(xy) = (|C_x| + |C_y|)/2$ is considerably larger, namely $n^2/8 + O(n(\log n)^2)$.

Exercises

6.1 Prove that if $0 \le x \le y \le 1$, then

$$1 - y \le (1 - x)\, e^{x-y}.$$

6.2 Suppose $t = n/2 + o(n)$. Imitate the proof of Theorem 6.3 to show that a.e. G_t satisfies $S(G_t) \le (\log n)n^2/s^2$.

Show also that if

$$n/2 + n^{1-\gamma_0} \le t = n/2 + s \le n/2 + o\{(\log n)^{-1} n\}$$

for some $\gamma_0 < \frac{1}{3}$, and $\omega(n) \to \infty$, then

$$|S(G_t) - (6 \log s - 4 \log n - \log\log n)n^2/s^2| \le \omega(n)n^2/s^2$$

for a.e. G_t (cf. the proof of Theorem 9).

6.3 Let $\frac{1}{5} < \gamma < \frac{1}{3}$, $\varepsilon = n^{-\gamma}$, $p = (1+\varepsilon)/n$, and let $Y_1 = Y_1(G_p)$ be as in Theorem 6. Prove that there is a constant $c_\gamma > 0$ such that

$$E(Y_1) = \{c_\gamma + o(1)\}n^{5\gamma-1},$$

though $Y_1 = 0$ almost surely.

6.4 Suppose $\gamma_0 < \frac{1}{3}$, $n^{-\gamma_0} \le |\varepsilon| = o\{(\log n)^{-1}\}$, $p = (1+\varepsilon)/n$ and $\omega(n) \to \infty$. Prove that for every fixed $m \ge 2$ a.e. G_p is such that if $2 \le i \le m$, then

$$|L_i(G_p) - (2 \log n + 6 \log |\varepsilon| - 5 \log\log n)\varepsilon^{-2}| \le \omega(n)\varepsilon^{-2}.$$

(This follows rather easily from Corollary 6.4 and Theorem 6.8.)

6.5 Let $c > 1$. Prove that there is a constant c_1 such that

$$\max_{t \ge cn/2} P(G_t \text{ contains a small component of order at least } c_1 \log n) = o(n^{-2}).$$

6.6 (Ex. 5 ctd.) Show for $t \ge cn/2$ that the expected number of (k, d)-components of G_t with $k \le c_1 \log n$ and $d \ge 1$ is $O(n^{-1})$.

6.7 (Ex. 5 ctd.) Prove that there is a constant $c_2 = c_2(c, c_1)$ such that for $t \geq cn/2$ the expected number of vertices of G_t on unicyclic components of order at most $c_1 \log n$ is at most c_2.

6.8 Prove that for $t \leq 2n \log n$ and $k = O(\log n)$ the lifetime of a component of order k of G_t has approximately exponential distribution with mean $n/(2k)$.

6.9 For $t > n/2$ define $c(t) = 2t/n$, $\alpha(t) = c - 1 - \log c$ and $a'(t) = \lceil (2/\alpha) \log n \rceil$. Prove that for $c_0 > 1$, a.e. graph process $\widetilde{G}$ is such that for $t \geq c_0 n/2$ the graph G_t has no small component of order at least $a'(t)$ (cf. Theorem 6.10(i)).

6.10 Show that the function $u(c)$ of Theorem 6.12 satisfies $|u'(c)| \geq \frac{1}{2}\,\mathrm{e}^{-c}$ (cf. the proof of Theorem 6.15).

7
Connectivity and Matchings

Perhaps the most basic property of a graph is that of being connected. Thus it is not surprising that the study of connectedness of a r.g. has a vast literature. In fact, for fear of upsetting the balance of the book we cannot attempt to give an account of all the results in the area.

Appropriately, the very first random graph paper of Erdős and Rényi (1959) is devoted to the problem of connectedness, and so are two other of the earliest papers on r.gs: Gilbert (1959) and Austin *et al.* (1959). Erdős and Rényi proved that $(n/2)\log n$ is a sharp threshold function for connectedness. Gilbert gave recurrence formulae for the probability of connectedness of G_p (see Exx. 1 and 2). S. A. Stepanov (1969*a*, 1970*a*, *b*) and Kovalenko (1971) extended results of Erdős and Rényi to the model $\mathscr{G}\{n,(p_{ij})\}$, and Kelmans (1967*a*) extended the recurrence formulae of Gilbert. Other extensions are due to Ivchenko (1973*b*, 1975), Ivchenko and Medvedev (1973), Kordecki (1973) and Kovalenko (1975). In §1 we shall present some of these results in the context of the evolution of random graphs.

We know from Chapter 6 that a.e. graph process is such that a giant component appears shortly after time $n/2$, and the number of vertices not on the giant component decreases exponentially. Eventually the giant component swallows up all other components and the graph becomes connected. Our aim in §1 is to examine the transition from a disconnected graph to a connected one.

The edge-connectivity $\lambda(G_p)$ and the vertex-connectivity $\kappa(G_p)$ of a r.g. were examined by Erdős and Rényi (1961*b*), Ivchenko (1973*b*) and Bollobás (1981*a*). Some of these results will be proved in §2.

A *complete* (or *perfect*) *matching* in a graph of order n is a set of $n/2$ independent edges. It is trivial that if a graph is connected or if it has a complete matching then it has no isolated vertices. Erdős and Rényi

(1964, 1966) proved the following result, which is very surprising at first sight: if M is large enough to ensure that a.e. G_M has minimum degree at least 1, then a.e. G_M is connected and, if n is even, a.e. G_M has a perfect matching. A sharp version of this result is due to Bollobás and Thomason (1985): a.e. graph process is such that the moment the last isolated vertex vanishes, the graph becomes connected and, if n is even, the graph acquires a perfect matching. In §3 we consider matchings in bipartite graphs and in §4 we examine the general case.

The aim of §5 is to take a quick look at the rich body of results concerning reliable networks or, what it amounts to, the probability of connectedness of $G \in \mathscr{G}(H;p)$. Once again, we are faced with an impossible task. Rather than give an unsatisfactorily superficial account of good many results, we concentrate on a striking theorem of Margulis (1974*a*).

The connectivity properties and 1-factors of random regular graphs will be examined in §6.

7.1 The Connectedness of Random Graphs

Let us examine a graph process just before the giant component swallows up all the other components. We know from Theorem 6.10(iii) that if $\omega(n) \to \infty$, a.e. graph process is such that after time $\omega(n)n$ every component, other than the giant component, is a tree of order $o(\log n)$. When do these trees vanish? Given $k \in \mathbb{N}$ and a graph process $\widetilde{G} = (G_t)_0^N$, set

$$\tau(T_k) = \max\{0\} \cup \{t : G_t \text{ has a component which is a tree of order } k\}.$$

Thus $\tau(T_k)$ is the last time our graph contains an isolated tree of order k, provided it ever contains one.

As in Chapter 5, denote by T_k the number of components which are trees of order k. Clearly

$$E_p(T_k) = \binom{n}{k} k^{k-2} p^{k-1} (1-p)^{kn+O(k^2)},$$

so if $k = o(\log n)$, $k \to \infty$, $p = \theta/n$ and $\theta = o\{(n/k)^{1/2}\}$, then

$$E_p(T_k) \sim \frac{1}{\sqrt{2\pi}} k^{-5/2} \frac{n}{\theta} (\theta e^{1-\theta})^k.$$

For $k \in \mathbb{N}$ define $\theta_0 = \theta_0(k) > 1$ by

$$k^{-5/2} \frac{n}{\theta_0} (\theta_0 e^{1-\theta_0})^k = 1.$$

Theorem 7.1 *If $k = o(\log n)$ and $\omega(n) \to \infty$, then*

$$|\tau(T_k) - \theta_0(k)n/2| \le \omega(n)n/k$$

holds for a.e. graph process.

Proof (i) The lower bound on $\tau(T_k)$ is rather trivial. Let $t_1 = \lceil\{\theta_0 - \omega(n)/k\}n/2\rceil$ and $\theta_1 = 2t_1/n$. Then

$$E_{t_1}(T_k) \sim E_{\theta_1/n}(T_k) \sim \binom{n}{k} k^{k-2} \left(\frac{\theta_1}{n}\right)^{k-1} \mathrm{e}^{-k\theta_1}.$$

The definition of θ_0 implies that $E_{t_1}(T_k) \to \infty$. Furthermore, rather trivially, $\sigma^2_{t_1}(T_k) = o\{E_{t_1}(T_k)^2\}$ so $T_k(G_{t_1}) > 0$ for a.e. G_{t_1}. Hence $\tau(T_k) \ge t_1$ for a.e. graph process.

(ii) The proof of the upper bound is similar to the proof of Theorem 6.10. Since a.e. graph of size $b = \lfloor 2n \log n\rfloor$ is connected (cf. Ex. 15 of Chapter 2), we may restrict our attention to times up to b. Furthermore, we may and shall assume that $\omega(n) \le \log\log n$. Set

$$t_2 = \lfloor\{\theta_0 + \omega(n)/k\}n/2\rfloor \text{ and } \theta_2 = 2t_2/n.$$

Then

$$E_{t_2}(T_k) \sim E_{\theta_2/n}(T_k) \sim \binom{n}{k} k^{k-2} \left(\frac{\theta_2}{n}\right)^{k-1} \mathrm{e}^{-k\theta_2} = o(1).$$

Given a constant $c > 0$, set $s = \lfloor cn/(2k)\rfloor$ and $\theta = 2(t_2 + s)/n$. It is easily seen that

$$E_{t_2+s}(T_k) \sim E_{\theta/n}(T_k) \le 2^{-c} E_{\theta_2/n}(T_k).$$

Consequently

$$\sum_{t=t_2}^{2b} E_t(T_k) = o(n/k). \tag{7.1}$$

The survival time of a tree component of order k is asymptotically exponentially distributed with mean $n/(2k)$, so with probability $\frac{1}{2}$ a tree component of order k in G_t, for $t \le b$ will stay a component for at least $n/(4k)$ time. But, as in the proof of Theorem 6.10, by relation (7.1) this implies that a.e. $\tilde{G} = (G_t)_0^N$ is such that for $t_2 \le t \le b$ no G_t has a tree component of order k. $\square$

As a graph process runs, the tree components are swallowed up by the giant component at a regular rate, those of higher order vanishing first.

Theorem 7.2 *Suppose $t/n \to \infty$ and $k_0 = k_0(n) \in \mathbb{N}$ is such that $E_t(T_{k_0}) \to \infty$ and $E_t(T_{k_0+1}) \to 0$. Then a.e. G_t is such that all its components, with the exception of the giant component, are trees and*

$$\{k : G_t \text{ has a tree component of order } k\} = \{1, 2, \ldots, k_0\}.$$

Proof We know that a.e. G_t consists of a giant component and tree components of order $o(\log n)$. Hence in our proof it suffices to consider tree components of order at most $\log n$. Furthermore, it is easily seen that for $t \geq 2n \log n$ we have $\max E_t(T_{k_0}) \to 0$, so $t \leq 2n \log n$ must hold.

(i) Straightforward calculations show that for $1 \leq k \leq \log n$

$$E_t(T_{k+1})/E_t(T_k) \sim (2t/n)\mathrm{e}^{-2t/n}. \tag{7.2}$$

Since $t/n \to \infty$, this implies

$$\sum_{k=k_0+1}^{\lfloor \log n \rfloor} E_t(T_k) = o(1),$$

so almost no G_t has a tree component of order at least $k_0 + 1$.

(ii) By Chebyshev's inequality the probability that there is a k, $1 \leq k \leq k_0$, for which $T_k(G_t) = 0$ is at most

$$\sum_{k=1}^{k_0} \sigma_t^2(T_k) \Big/ E(T_k)^2. \tag{7.3}$$

Now, for $p = 2t/n^2$ the models $\mathscr{G}(n,t)$ and $\mathscr{G}(n,p)$ are practically interchangeable. If we apply Theorem 6.2 to the one element family $\wedge = \{(k, -1)\}$, then we see that

$$\sigma_p^2(T_k) \leq E_p(T_k) + 3tk^2 E(T_k)^2/n^2.$$

Imitating the relevant calculations in the proof of Theorem 6.2 we find that

$$\sigma_t^2(T_k) \leq E_t(T_k) + 4tk^2 E_t(T_k)^2/n^2.$$

This shows that the sum appearing in (7.3) is at most

$$\sum_{k=1}^{k_0} 1/E_t(T_k) + \sum_{k=1}^{k_0} 4tk^2/n^2 = \sum_{k=1}^{k_0} 1/E_t(T_k) + O(tk_0^2/n^2).$$

By relation (7.2) the sum on the right-hand side is $o(1)$. Furthermore, as $k_0 \leq \log n$ and $t \leq n \log n$, we have $O(tk_0^2/n^2) = O\{(\log n)^3/n\} = o(1)$. $\square$

Recalling Theorem 5.4, we see that for a fixed k the trees of order k vanish when $t \geq (n/2k)\{\log n + (k-1)\log\log n + \omega(n)\}$, where $\omega(n) \to \infty$. If $t = (n/2k)\{\log n + (k-1)\log\log n + x + o(1)\}$ for some fixed x, then tree components of order k exist with probability $1 - \mathrm{e}^{-\mathrm{e}^{-x}/(k \cdot k!)} + o(1)$.

From Theorem 7.2 it is easy to deduce the fundamental result proved by Erdős and Rényi (1959) that the probability of a r.g. G_p being connected is about the probability that it has no vertex of degree 0. In view of the importance of this result we also give a proof which does not rely on the structure of a typical G_p.

Theorem 7.3 *Let $c \in \mathbb{R}$ be fixed and let $M = (n/2)\{\log n + c + o(1)\} \in \mathbb{N}$ and $p = \{\log n + c + o(1)\}/n$. Then*

$$P(G_M \text{ is connected}) \longrightarrow \mathrm{e}^{-\mathrm{e}^{-c}} \tag{7.4}$$

and

$$P(G_p \text{ is connected}) \longrightarrow \mathrm{e}^{-\mathrm{e}^{-c}}. \tag{7.5}$$

Remark. By Theorem 2.2(ii), relations (7.4) and (7.5) are equivalent, so it suffices to prove one of them.

1st Proof By Theorem 7.2, a.e. G_M consists of a giant component and isolated vertices. Hence

$$P(G_M \text{ is connected}) = P\{\delta(G_M) \geq 1\} + o(1).$$

By Theorems 3.5 and 2.2(ii),

$$P\{\delta(G_M) \geq 1\} \to \mathrm{e}^{-\mathrm{e}^{-c}}.$$

In fact, recalling Theorem 5.4, we see also that the number of isolated vertices is asymptotically a Poisson r.v. with mean e^{-c}.

2nd Proof The probability that G_p has a component of order 2 (i.e. an isolated edge) is at most

$$\binom{n}{2} p(1-p)^{2(n-2)} \leq \frac{1}{2} n(\log n)\exp\{-2\log n + 5(\log n)/n\} \leq (\log n)/n.$$

What is the probability that for some r, $3 \leq r \leq n/2$, our random graph G_p contains a component of order r? Since a component of order r contains a tree of order r whose vertices are joined to no vertex outside the tree, this probability is at most

$$\sum_{r=3}^{\lfloor n/2\rfloor}\binom{n}{r} r^{r-2}p^{r-1}(1-p)^{r(n-r)} \le \sum_{r=3}^{\lfloor n/2\rfloor} nr^{-5/2}\exp\Big[r+r\log\log n+r\log 2$$
$$-r\{\log n+c+o(1)\}+\frac{r^2}{n}\{\log n+c+o(1)\}\Big]$$
$$\le n\sum_{r=3}^{\lfloor n/2\rfloor} r^{-5/2}\exp\{-2r(\log n)/5\}\le n^{-1/5}.$$

This shows that a.e. G_p consists of a giant component and isolated vertices, so by Theorem 3.5,

$$P(G_p \text{ is connected}) = P\{\delta(G_p)\ge 1\}+o(1) = \mathrm{e}^{-\mathrm{e}^{-c}}+o(1). \qquad \square$$

Theorem 7.3 shows that $M_0(n) = (n/2)\log n$ is a sharp threshold function for the connectedness of a graph: if $M(n) = \frac{n}{2}\{\log n + \omega(n)\}$, then a.e. G_M is connected if $\omega(n)\to\infty$ and almost no G_M is connected if $\omega(n)\to-\infty$.

Kovalenko (1975) generalized Theorem 7.3 to the model $\mathscr{G}\{n,(p_{ij})\}$. Set $q_{ij} = 1-p_{ij}$ (so that $q_{ii} = 1-p_{ii} = 0$ for every i),

$$Q_{ik} = \max_{i_1<\ldots<i_{n-k}} q_{ij_1}q_{ij_2}\ldots q_{ij_{n-k}} \text{ and } \lambda = \sum_{i=1}^{n} Q_{i0}.$$

Note that λ is the expected number of isolated vertices. Kovalenko proved that if

$$\max_{1\le i\le n} Q_{i0}\longrightarrow 0, \qquad \lambda\longrightarrow\lambda_0$$

and

$$\sum_{k=1}^{\lfloor n/2\rfloor}\frac{1}{k!}\left(\sum_{i=1}^{n} Q_{ik}\right)^k - (\mathrm{e}^{\lambda}-1)\longrightarrow 0 \tag{7.6}$$

then a.e. graph in $\mathscr{G}\{n,(p_{ij})\}$ consists of a giant component and isolated vertices, and the number of isolated vertices tends to P_{λ_0} in distribution.

Although in general relation (7.6) is not easily checked, it is satisfied if the probabilities p_{ij} are close to $(\log n)/n$ (see Ex. 3).

The analogue of Theorem 7.3 for random r-partite graphs (see Ex. 5) was proved by Palásti (1963, 1968). Considerably more-detailed investigations of the connectivity of random r-partite graphs were carried out by Kelmans (1967*b*) and Ruciński (1981).

Since connectedness is a monotone property, $P(G_M$ is connected$)\le P(G_{M+1}$ is connected$)$ for every $M = M(n)$. It is fairly surprising that, as proved by Wright (1972) (see also Wright, 1973*b*, 1974*c*, 1975*a*), the probability of connectedness of an unlabelled graph can be less for more edges. We shall return to this in Chapter 9.

7.2 The k-Connectedness of Random Graphs

The *vertex-connectivity* of a graph G is denoted by $k(G)$ and the edge-connectivity by $\lambda(G)$. Recall from Chapter 2 that, given a graph process $\widetilde{G} = (G_t)_0^N$, the *hitting time* $\tau(Q) = \tau(Q;\widetilde{G})$ of a monotone increasing property Q of graphs is defined as

$$\tau(Q) = \tau(Q;\widetilde{G}) = \min\{t : G_t \text{ has } Q\}.$$

Thus $\tau(Q;\widetilde{G})$ is the first time when the graph acquires property Q. In particular, $\tau\{\kappa(G) \geq k\}$ is the first time when the graph becomes k-connected and $\tau\{\delta(G) \geq k\}$ is the first time the minimum degree becomes k. Trivially $\tau\{\delta(G) \geq k;\widetilde{G}\} \leq \tau\{\kappa(G) \geq k;\widetilde{G}\}$ for every graph process $\widetilde{G}$. It is fascinating, and at the first sight rather surprising, that, in fact, equality holds for a.e. graph process. This was proved by Bollobás and Thomason (1985) for every function $k = k(n)$, $1 \leq k \leq n-1$, but here we prove it only in the case when k is constant.

Theorem 7.4 *Given $k \in \mathbb{N}$, a.e. $\widetilde{G}$ is such that*

$$\tau(\delta(G) \geq k) = \tau(k(G) \geq k).$$

The proof is based on a lemma concerning separators. Given a graph G, a set $S \subset V(G)$ is called a *separator* if $V(G)\backslash S$ is the disjoint union of two non-empty sets, say W_1 and W_2, such that G has no $W_1 - W_2$ edge. Our notation will always be chosen to satisfy $|W_1| \leq |W_2|$. If $|S| = s$, we call S an *s-separator*. A separator is *trivial* if $|W_1| = 1$. Note that every non-complete graph of minimal degree s has a trivial s-separator but it need not have a non-trivial s-separator.

Lemma 7.5 *Let $k \geq 2$, $\omega(n) \to \infty$, $\omega(n) \leq \log\log\log n$ and $p = \{\log n + (k-1)\log\log n - \omega(n)\}/n$. Then almost no G_p contains a non-trivial $(k-1)$-separator.*

Proof Denote by A_r the event that G_p contains a $(k-1)$-separator with $|W_1| = r$. Set $r_0 = \max\{k, 10\}$, $r_1 = \lfloor n^{5/9} \rfloor$ and $r_2 = \lfloor (n-k+1)/2 \rfloor$. The lemma claims that

$$P_p\left(\bigcup_{r=2}^{r_2} A_r\right) = o(1),$$

or, equivalently,

$$P\left(\bigcup_{r=2}^{r_0} A_r\right) + P\left(\bigcup_{r=r_0}^{r_1} A_r\right) + P\left(\bigcup_{r=r_1}^{r_2} A_r\right) = o(1) \tag{7.7}$$

In estimating the first probability above we shall make use of two facts.

(a) A.e. G_p has minimum degree $k-1$. This follows by Theorem 3.5.

(b) Given $l \in \mathbb{N}$, a.e. G_p is such that no two vertices of degree at most l are at distance at most l. Indeed, the expected number of paths of length $k \geq 1$ ending in vertices of degrees i and j is at most

$$n^{k+1}p^k(pn)^{i-1}(pn)^{j-1}(1-p)^{2n-i-j-2} = o(1).$$

Now (a) and (b), with $l = k + r_0$, imply that $P(\bigcup_{r=2}^{r_0} A_r) = o(1)$. To see this note that if $\delta(G_p) \geq k-1$ and G_p contains a $(k-1)$-separator with $|W_1| = r \geq 2$, then G_p contains two vertices of degree less than $k+r$ at a distance less than $k+r$.

Let us turn to the estimate of the second term in (7.7). If $\delta(G_p) \geq k-1$ and S is a $(k-1)$-separator with $r_0 \leq |W_1| = r \leq r_1$, then the graph spanned by $W_1 \cup S$ has at least $r(k-1)/2$ edges. Given S and W_1, the probability of such a graph is at most

$$\binom{\binom{r+k-1}{2}}{r(k-1)/2} p^{r(k-1)/2} \leq \left(\frac{4erp}{k-1}\right)^{r(k-1)/2} n^{-3r(k-1)/14}.$$

Consequently, by (a),

$$\begin{aligned} P\left(\bigcup_{r=r_0}^{r_1} A_r\right) &\leq o(1) + \sum_{r=r_0}^{r_1} \binom{n}{r}\binom{n-r}{k-1} n^{-3r(k-1)/14}(1-p)^{r(n-r-k+1)} \\ &\leq o(1) + \sum_{r=r_0}^{r_1} n^{r+k-3r(k-1)/14-r+2r^2/n} = o(1). \end{aligned}$$

Finally, a sufficiently good estimate of the third term in (7.7) follows from the fact that there are no $W_1 - W_2$ edges:

$$P\left(\bigcup_{r=r_1}^{r_2} A_r\right) \leq \sum_{r=r}^{r_2} \binom{n}{r}\binom{n-r}{k-1}(1-p)^{r(n-r-k+1)}$$

$$\leq \sum_{r=r_1}^{r_2} \left(\frac{en}{r}\right)^r n^k (1-p)^{r(n/2-k/2)}$$

$$\leq \sum_{r=r_1}^{r_2} n^{2k} \left(\frac{en}{r}(1-p)^{n/2}\right)^r$$

$$\leq \sum_{r=r_1}^{r_2} n^{2k} n^{-r/20} = o(1). \qquad \square$$

Equipped with Lemma 7.5, Theorem 7.4 is easily proved.

Proof of Theorem 7.4 (i) Suppose $k = 1$. In this case we do not even need Lemma 7.5. Set $\omega(n) = \log\log\log n$, $M_1 = \lfloor \frac{n}{2}\{\log n - \omega(n)\}\rfloor$ and $M_2 = \lfloor \frac{n}{2}\{\log n + \omega(n)\}\rfloor$. We know that a.e. $\widetilde{G}$ is such that $\tau\{\delta(G) \geq 1\} > M_1, G_{M_1}$ has at most $\log n$ isolated vertices and all other vertices of G_{M_1} belong to the giant component. Stop such a process at time M_1 and denote by $Z = \{z_1, \ldots, z_s\}$ the set of isolated vertices of G_{M_1}. Thus $1 \leq s \leq \log n$. Now run the process for $M_2 - M_1$ more steps. The probability that one of the next $M_2 - M_1$ edges joins two vertices of Z is at most

$$\frac{2s^2(M_2 - M_1)}{n^2} = o(1).$$

This shows that, with probability $1 - o(1)$, every edge incident with some z_i and drawn not later than time M_2, joins z_i to the giant component of G_{M_1}. On the other hand, a.e. G_{M_2} is connected. Hence $\tau\{\kappa(G) \geq 1\} = \tau\{\delta(G) \geq 1\}$ with probability tending to 1.

(ii) Suppose $k \geq 2$. In this case our theorem is an immediate consequence of Lemma 7.5. Indeed, by Lemma 7.5 and Theorem 2.2 there is a function $M(n)$ such that $M(n) < (n/2)\{\log n + (k-1)\log\log n - \log\log\log n\}$ and almost no G_M contains a non-trivial $(k-1)$-separator. Hence a.e. graph process $\widetilde{G} = (G_t)_0^N$ is such that for $t \geq M(n)$ the graph G_t does not contain a $(k-1)$-separator. To complete the proof all we have to note is that $\tau\{\delta(G) > k\} > M(n)$ for a.e. graph process and a graph with minimum degree k is k-connected unless it contains a non-trivial $(k-1)$-separator.

Let us note two more immediate consequences of Lemma 7.5 and Theorem 3.5. The first is due to Ivchenko (1973*b*) and the second to Erdős and Rényi (1961*b*).

Theorem 7.6 *If* $p(n) \leq (\log n + k \log\log n)/n$ *for some fixed* k, *then*

$$P\{\kappa(G_p) = \lambda(G_p) = \delta(G_p)\} \longrightarrow 1.$$

In fact, Theorem 7.6 holds without any restriction on p, as shown by Bollobás and Thomason (1985).

Theorem 7.7 *If $k \in \mathbb{N}$ and $x \in \mathbb{R}$ are fixed and $M(n) = (n/2)\{\log n + k \log\log n + x + o(1)\} \in \mathbb{N}$, then*

$$P\{\kappa(G_M) = k\} \longrightarrow 1 - e^{-e^{-x/k!}}$$

and

$$P\{\kappa(G_M) = k+1\} \longrightarrow e^{-e^{-x/k!}}. \qquad \square$$

The moral of these results is that the connectivity of a random graph is not higher than what it is only because single vertices can be separated by their neighbours from the rest of the graph. The next result, from Bollobás (1981*a*), shows that this is especially true for random graphs with constant probability of an edge.

Theorem 7.8 *Let p be fixed, $0 < p < 1$. Then a.e. G_p contains $t = \lfloor n^{1/7} \rfloor$ distinct vertices $x_1, x_2, \ldots, x_t$ such that if $G_0 = G$, and $G_i = G_{i-1} - \{x_i\}$, $i = 1, 2, \ldots, t$, then*

$$\kappa(G) < \kappa(G_1) - t < \kappa(G_2) - 2t < \ldots < \kappa(G_t) - t^2.$$

Furthermore, for each i, $0 \le i \le t$, we have $\kappa(G_i) = \delta(G_i)$ and G_i has larger minimum degree and larger vertex connectivity than any other subgraph of order $n - i$. $\square$

In 1995, Cooper and Frieze introduced the kth *nearest neighbour graph* and studied its connectivity properties. To define this random graph O_k, we start with the complete graph K_n with vertex set, and pick a random order $e_1, \ldots, e_N$ of the edges of K_n. For each vertex i, let E_i be the set of the first k edges incident with i, and define $O_k = ([n], \cup_1^n E_i)$.

The random graph O_k has a beautiful description in terms of random 'weights' on the edges. Assign i.i.d.r.vs from an atomless distribution to the edges of K_n. Then, with probability 1, no two edges have the same weight. To get the edge set of O_k, for each vertex take the k lightest edges.

There is a 'dynamic' description of O_k as well, based on a random graph process $(G_t)_0^N$ or, what is the some, a random permutation e_1, e_2, $\ldots$, e_N of the edges. Define a sequence of graphs $H_0 \subset H_1 \subset \ldots \subset H_N$ with vertex set $[n]$ as follows. Set $E(H_0) = \phi$. Having defined H_t, if at least one of the two endvertices of e_{t+1} has degree less than k then set

$E(H_{t+1}) = E(H_t) \cup \{e_{t+1}\}$, otherwise set $E_{t+1} = E_t$. The process stops when every degree of H_t is at least k.

The random graph O_k is rather close to $G_{k\text{-out}}$; for example, $kn/2 \leq e(O_k) \leq kn - \binom{k+1}{2}$. As pointed out by Cooper and Frieze (1995), a.e. O_k has about $3n/4$ edges, a.e. O_2 has about $11n/8$ edges and, in general, for $k = o(\log n)$, a.e. O_k has

$$kn - \frac{n(n-1)}{2n-3} \sum_{1 \leq i \leq j \leq k} \frac{\binom{n-2}{i-1}\binom{n-2}{j-1}}{2^{d(i,j)}\binom{2n-4}{i+j-2}} + O(k^2\sqrt{n}\log n)$$

edges, where $d(i,j)$ is the Kronecker delta. This is easy to deduce from the martingale inequalities Theorems 1.19 and 1.20, provided one can calculate the expectation

Concerning the connectivity of O_k, Cooper and Frieze (1995) proved that a.e. O_1 is disconnected and, for every fixed $k \geq 3$, a.e. O_k is k-connected. It is rather surprising that O_2 behaves in a somewhat peculiar way: for $\omega(n) \to \infty$, a.e. O_2 has a giant componant with at least $n - \omega(n)$ vertices. Furthermore,

$$\lim_{n\to\infty} P(O_2 \text{ is connected}) = r,$$

where r is a constant satisfying $0.99081 \leq r \leq 0.99586$. The proof of these assertions are ingenious and complicated.

A geometric random graph resembling O_k was introduced and studied by Penrose (1999). For a set X_n of n points in a metric space and a positive real $r > 0$, let $G_r(X_n)$ be the graph with vertex set X_n in which two vertices are joined by an edge if their distance is at most r. As r increases, $G_r(X_n)$ has larger and larger minimum degree and connectivity. Given X_n, let $\rho_{n,k} = \rho_k(X_n)$ be the minimal value of r at which $G_r(X_n)$ has minimal degree at least k, and define $\sigma_{n,k} = \sigma_k(X_n)$ similarly for k-connectedness. Formally, the *hitting radii* $S_{n,k}$ and $\sigma_{n,k}$ are given by

$$S_{n,k} = S_k(X_n) = \min\{r > 0 : \quad \delta(G_r(X_n)) \geq k\}$$

and

$$\sigma_{n,k} = \sigma_k(X_n) = \min\{r > 0 : \quad k(G_r(X_n)) \geq k\}.$$

Extending his result from 1997, Penrose (1999) proved that if X_n is a random n-subset of the d-dimensional unit cube I^d then, with probability tending to 1, for the geometric random graph $G_r(X_n)$ these two hitting radii coincide:

$$\lim_{n\to\infty} P\left(\sigma_{n,k} = S_{n,k}\right) = 1.$$

note that this result is the exact analogue of Theorem 7.6. However, we should not be misled by the easy proof of that result: the proof of this extension to geometric random graphs is much harder.

7.3 Matchings in Bipartite Graphs

In this section we shall consider the probability spaces $\mathcal{G}\{K(n,n);p\}$ and $\mathcal{G}\{K(n,n);M\}$ consisting of bipartite graphs with vertex sets V_1 and V_2 with $|V_1| = |V_2| = n$ (see §1 of Chapter 2). In the first model we select edges independently and with probability p, in the second we take all bipartite graphs with vertex classes V_1 and V_2 which have $M = M(n)$ edges. We write B_p and B_M for random elements of these models. Furthermore, we define a *random bipartite graph process* $\widetilde{B} = (B_t)_0^{n^2}$ in the natural way. Our aim is to find a threshold function for the existence of a complete matching. In other words, we are interested in the hitting time $\tau(\text{match}; \widetilde{B})$ of a matching in our bipartite graph.

Once again, it is trivial that $\tau(\text{match};\widetilde{B}) \geq \tau(\delta(B) \geq 1;\widetilde{B})$ for every bipartite graph process $\widetilde{B}$ since the minimum degree is at least 1 if the graph has a complete matching. Our main aim is to prove that we have equality for a.e. $\widetilde{G}$. This result, from Bollobás and Thomason (1985), is a slight extension of a theorem of Erdős and Rényi (1964, 1968). It is worth remarking that $\tau\{\kappa(B) \geq 1;\widetilde{B}\} = \tau\{\delta(B) \geq 1;\widetilde{B}\}$ also holds for a.e. $\widetilde{B}$ (see Ex. 4).

In proving that two hitting times agree a.e., it is useful to introduce some other models of random graphs. Although in the first application, which is the main result of this section, we shall work with bipartite random graphs, it is more natural to define the more commonly applicable models, namely $\mathcal{G}(n,p;\geq k)$ and $\mathcal{G}(n,M;\geq k)$, as in Bollobás (1984*a*).

Both models consist of graphs with vertex set V, whose edges are coloured blue and green. To define a random element of $\mathcal{G}(n,p;\geq k)$, first take an element H of $\mathcal{G}_p$, i.e. select edges independently and with probability p. Let $x_1, x_2, \ldots, x_s$ be the vertices of degree less than k in H. For each i, $1 \leq i \leq s$, add to H a random edge incident with x_i. Colour the edges of H *blue* and the edges added to H *green*. (So there are at most $s \leq n$ green edges.) This blue–green edge-coloured graph is a random element of $\mathcal{G}(n,p;\geq k)$. The model $\mathcal{G}(n,M;\geq k)$ is constructed analogously.

A little less formally: a random element of $\mathcal{G}(n, p; \geq k)$ is obtained from a random element of $\mathcal{G}(n, p)$, coloured blue, by adding one directed green edge $\overrightarrow{xy}$ for each vertex x of degree less than k and then forgetting the direction of the edges (and replacing multiple edges by simple edges).

Lemma 7.9 *Let $k \in \mathbb{N}$ be fixed and let Q be a monotone increasing property of graphs such that every graph having Q has minimum degree at least k. Let*

$$p = \{\log n + (k-1)\log\log n - \omega(n)\}/n$$

where $\omega(n) \to \infty$ and $\omega(n) \leq \log\log\log n$. If a.e. graph in $\mathcal{G}(n, p; \geq k)$ has Q, then

$$\tau(Q; \widetilde{G}) = \tau\{\delta(G) \geq k; \widetilde{G}\}$$

for a.e. graph process $\widetilde{G}$.

Proof Since a.e. graph in $\mathcal{G}(n, p; \geq k)$ has Q, by Theorem 2.2 there is a function $M_1(n) \in \mathbb{N}$ such that

$$\frac{n}{2}\left\{\log n + (k-1)\log\log n - \frac{3}{2}\omega(n)\right\} \leq M_1(n)$$
$$\leq \frac{n}{2}\left\{\log n + (k-1)\log\log n - \frac{1}{2}\omega(n)\right\}$$

and a.e. graph in $\mathcal{G}(n, M_1; \geq k)$ has Q.

Let $M_2(n) = \lfloor (n/2)\{\log n + (k-1)\log\log n + \omega(n)\}\rfloor$ and let $\widetilde{\mathcal{G}}_*$ be the set of graph processes $\widetilde{G} = (G_t)_0^N$ for which $\delta(G_{M_1}) = k-1$, $\delta(G_{M_2}) \geq k$ and no edge added at times M_1+1, M_1+2, ..., M_2 joins vertices which had degree less than k in G_{M_1}. It is easily checked (cf. §1 of Chapter 3) that a.e. G_{M_1} has minimum degree $k-1$ and at most $\log n$ vertices of degree $k-1$ which form an independent set. If an edge is added to such a graph, then the probability that the edge joins two vertices of degree $k-1$ is at most $4(\log n)^2/n^2$. Hence, with probability at least $1 - 10(\log n)^2\omega(n)/n$, no edge added at times M_1+1, M_1+2, ..., M_2 will join vertices of degree less than k in G_{M_1}. Furthermore, by Theorem 3.5, a.e. G_{M_2} satisfies $\delta(G_{M_2}) = k$. Consequently $P(\widetilde{\mathcal{G}}_*) = 1 - \delta_n$, where $\delta_n \to 0$.

Let $\mathcal{G}_*$ be the collection of graphs from $\mathcal{G}(n, M_1; \geq k)$ in which the blue graph has minimum degree $k-1$ and no (blue or green) edge joins two vertices of blue degree $k-1$. Once again, rather trivially, $P(\mathcal{G}_*) = 1 - \varepsilon_n$, where $\varepsilon_n \to 0$.

Let us define a map $\phi : \widetilde{\mathcal{G}}_* \to \mathcal{G}_*$ as follows. Given $\widetilde{G} = (G_t)_0^N \in \widetilde{\mathcal{G}}_*$, let $\phi(\widetilde{G})$ be the coloured graph whose blue subgraph is G_{M_1} and whose green edges are the *first edges* added after time M_1 and not later than M_2 which increased the degree of a vertex to k. Clearly $\phi(\widetilde{\mathscr{G}}_*) = \mathscr{G}_*$ and

$$(1-\varepsilon_n)P\{\phi^{-1}(A)\} = (1-\delta_n)P(A) \text{ for all } A \subset \mathscr{G}_*. \tag{7.8}$$

By assumption the set

$$\mathscr{G}_0 = \{G \in \mathscr{G}(n, M_1; \geq p) : G \text{ has } Q\}$$

is such that

$$P(\mathscr{G}_0) = 1 - \eta_n, \text{ where } \eta_n \to 0.$$

Hence

$$P(\mathscr{G}_0 \cap \mathscr{G}_*) \geq 1 - \varepsilon_n - \eta_n.$$

and by (7.8) the set $\widetilde{\mathscr{H}} = \phi^{-1}(\mathscr{G}_0 \cap \mathscr{G}_*)$ satisfies

$$P(\widetilde{\mathscr{H}}) \geq \frac{1-\delta n}{1-\varepsilon n}(1 - \varepsilon_n - \eta_n) \to 1.$$

This completes the proof since by our construction if $\widetilde{G} \in \widetilde{\mathscr{H}}$ [and so $\phi(\widetilde{G})$ has Q], then

$$\tau\{\delta(G) \geq k; \widetilde{G}\} = \tau(Q; \widetilde{G}). \qquad \square$$

It is very important (though rather trivial) that the probability measure in $\mathscr{G}(n, p; \geq k)$ is fairly close to the measure in $\mathscr{G}(n, p)$.

Lemma 7.10 *Let A and B be (disjoint) subsets of $V^{(2)}$. Then the probability that a graph G in $\mathscr{G}(n, p; \geq k)$ is such that*

$$A \subset E(G) \quad \text{and} \quad B \cap E(G) = \varnothing$$

is at most

$$\left(p + \frac{2}{n-k}\right)^{|A|}(1-p)^{|B|}.$$

Proof Note simply that the probability that a set $A_1 \subset V^{(2)}$ consists of green edges is at most $\{2/(n-k)\}^{|A_1|}$. $\square$

Now we are well prepared to prove the main result of the section.

Theorem 7.11 *A.e. random bipartite graph process $\widetilde{B}$ is such that*

$$\tau(match; \widetilde{B}) = \tau\{\delta(B) \geq 1\}.$$

Proof Set $p = (\log n - \log\log\log n)/n$ and give $\mathscr{G}\{K(n,n), p; \geq 1\}$ the obvious meaning. By the analogue of Lemma 7.9 for bipartite graphs, it suffices to prove that a.e. graph G in $\mathscr{G}\{K(n,n), p; \geq 1\}$ has a matching. In our estimate of the probability that a graph $G \epsilon \mathscr{G}\{K(n,n), p; \geq 1\}$ has no matching we shall make use of the following immediate consequence of Hall's theorem (see, for example, Bollobás, 1978*a*, pp. 9 and 52; 1979*a*, p. 54). □

Lemma 7.12 *Let G be a bipartite graph with vertex classes V_1 and $V_2, |V_1| = |V_2| = n$. Suppose G has no isolated vertices and it does not have a complete matching. Then there is a set $A \subset V_i$ $(i = 1, 2)$ such that:*

(*i*) *$\Gamma(A) = \{y : xy \in E(G)$ for some $x \in A\}$ has $|A| - 1$ elements,*
(*ii*) *the subgraph of G spanned by $A \cup \Gamma(A)$ is connected and*
(*iii*) $2 \leq |A| \leq (n+1)/2$.

Proof As G does not have a complete matching, Hall's condition is violated by some set $A \subset V_i$, i.e.

$$|\Gamma(A)| < |A|. \tag{7.9}$$

Choose a set A of smallest cardinality satisfying (7.9). Then (i) and (ii) hold, since otherwise A could be replaced by a proper subset of itself. If, say, $A \subset V_1$, then $B = V_2 - \Gamma(A)$ is such that $\Gamma(B) \subset V_1 - A$, and so B also satisfies inequality (7.9):

$$|\Gamma(B)| \leq |V_1| - |A| < |V_2| - |\Gamma(A)| = |B|.$$

Hence $|A| \leq |B| = |V_2| - |\Gamma(A)| = n - (|A| - 1)$, so $|A| \leq (n+1)/2$.

Let us continue the proof of Theorem 7.11. Denote by F_a the event that there is a set $A \subset V_i (i = 1$ or $2), |A| = a$, satisfying (i), (ii) and (iii) of Lemma 7.12. All we have to show is that in $\mathscr{G}\{K(n,n), p; \geq 1\}$ we have

$$P\left(\bigcup_{a=2}^{n_1} F_a\right) = o(1),$$

where $n_1 = \lfloor (n+1)/2 \rfloor$.

Let $A_1 \subset V_1, A_2 \subset V_2$ and $|A_1| = |A_2| + 1 = a$. What is the probability that the subgraph of G spanned by $A_1 \cup A_2$ has at least $2a - 2$ edges and no vertex of A_1 is joined to a vertex in $V_2 - A_2$? By the analogue of Lemma 7.10, very crudely this is at most

$$\binom{a(a-1)}{2a-2} \left(\frac{\log n}{n}\right)^{2a-2} (1-p)^{a(n-a+1)}.$$

Since we have $2\binom{n}{a}$ choices for A with $|A| = a$ and $\binom{n}{a-1}$ more choices for $\Gamma(A)$,

$$\sum_{a=2}^{n_1} P(F_a) \le 2\sum_{a=2}^{n_1} \binom{n}{a}\binom{n}{a-1}\binom{a(a-1)}{2a-2}\left(\frac{\log n}{n}\right)^{2a-2}(1-p)^{a(n-a+1)}$$
$$\le 2\sum_{a=2}^{n_1}\left(\frac{en}{a}\right)^a\left(\frac{en}{a-1}\right)^{a-1}\left(\frac{ea}{2}\right)^{2a-2}\left(\frac{\log n}{n}\right)^{2a-2}\left(\frac{n}{\log\log n}\right)^{-a+a^2/n}$$
$$\le \sum_{a=2}^{n_1}(e\log n)^{3a}n^{1+a+a^2/n} = o(1). \qquad \square$$

In view of Ex. 6 of Chapter 3, we have the following immediate consequence of Theorem 7.11.

Corollary 7.13 *Let* $x \in \mathbb{R}, M = (n/2)\{\log n + x + o(1)\} \in \mathbb{N}$ *and write* B_M *for a random element of* $\mathcal{G}\{K(n,n), M\}$. *Then*

$$P(B_M \text{ has a matching}) \longrightarrow e^{-2e^{-x}}. \qquad \square$$

We conclude this section with a brief account of a problem about matchings in randomly weighted complete bipartite graphs, the *random assignment problem.* The set-up is much like in the minimum weight spanning tree problem, discussed in §5 of Chapter 6. Let $X_n = (X_{ij})$ be an n by n matrix whose entries $X_{ij}, 1 \le i, j \le n$, are non-negative i.i.d. r. vs. Let $G(X_n)$ be the n by n bipartite graph with vertex classes $V = \{v_1, \dots, v_n\}$ and $W = \{w_1, \dots, w_n\}$, in which $v_i w_j$ has *weight* X_{ij}. What is the minimum weight $m(X_n)$ of a complete matching in $G(X_n)$? In other words, what is the minimum weight of a one-to-one assignment $V \to W$? If the X_{ij} are uniformly distributed in (0, 1), then we write $U_n = (U_{ij})$ instead of $X_n = (X_{ij})$ and call the problem the (*uniform*) *random assignment problem.*

Donath (1969) was the first to consider this problem and to notice experimentally that the expectation $E(m(U_n))$ seems to tend to some constant C^* between 1 and 2. Walkup (1979) proved that the expectation was indeed bounded, in fact, $\lim_{n\to\infty} E(m(U_n)) \le 3$. He deduced this from his result that a.e. n by n bipartite 2-out graph has a complete matching. Walkup's method was further developed by Walkup (1980), Frenk, van Houweninge and Rinnooy Kan (1987), Karp (1987), Dyer, Frieze and McDiarmid (1986) and Karp, Rinnooy Kan and Vohra (1994).

In particular, Karp (1987) lowered Walkup's upper bound to 2.

Concerning a lower bound, trivially,

$$E(m(X_n)) \geq \sum_{i=1}^{n} E(\min_j X_{ij}) = nE(\min_j X_{ij}).$$

In particular, for the uniform random assignment problem,

$$E(m(U_n)) \geq \frac{n}{n+1}.$$

The first non-trivial lower bound was given by Lazarus (1993), who proved that $\underline{\lim}_{n\to\infty} E(m(U_n)) \geq 1 + 1/e$. Goemans and Kodialam (1993) improved the lower bound to 1.44 by extending the methods of Lazarus, and Olin (1992) to 1.51.

It is clear that if we are interested in the limit of the expectation $E(m(X_n))$ then only the distribution of X_{ij} near 0 matters. In particular, we may replace U_{ij} by A_{ij}, where A_{ij} has exponential distribution with mean 1, i.e., $P(A_{ij} \leq x) = l - e^{-x}$ for $x \geq 0$. Aldous (1992) observed that considering the *exponential random assignment matrix* $A_n = (A_{ij})$ has many advantages over the uniform random assignment matrix $U_n = (U_{ij})$, and many of the proofs become much simpler. Among other results, Aldous (1992) proved that c^* does exist: the expected cost of a minimum assignment (with the exponential distribution, say) does tend to a constant c^* between 1.51 and 2.

Let us see how the lower bound $1+1/e$ given by Lazarus (1993) can be proved if we use exponential r. vs $A_{ij}, 1 \leq i, j \leq n$, each with mean 1. Set $\overline{A}_i = \min_j A_{ij}$ and $B_{ij} = A_{ij} - \overline{A}_i$. Then each $\overline{A}_i$ is exponentially distributed with mean $1/n$. Furthermore, the entries of the matrix $B_n = (B_{ij})$ are again i.i.d. exponential r. vs with mean 1 *except* that a random element $B_{ij(i)}$ of each row is replaced by 0. For $1 \leq j \leq n$, let $\bar{B}_j = \min_i B_{ij}$.

Trivially,

$$E(m(A_n)) \geq \sum_{i=1}^{n} E(\overline{A}_i) + \sum_{j=1}^{n} E(\bar{B}_j)$$

since a matching has an element in each row and column.

Hence

$$E(m(A_n)) \geq n\frac{1}{n} + E(2)/n = 1 + E(Z)/n,$$

where Z is the number of columns of B_n containing no 0. Indeed, if the jth column of B_n has a 0 then $E(\bar{B}_j) = 0$, otherwise $\bar{B}_j$. is the minimum of n independent exponential r. vs, each with mean l, so $E(\bar{B}_j) = l/n$.

Write S_r for the expected number of r-tuples of columns of B_n containing no 0, and set $p_k = P(Z = k)$. Then

$$S_r = \binom{n}{r}\left(\frac{n-r}{n}\right)^n,$$

and by the inclusion–exclusion formula (1.19),

$$\begin{aligned} E(Z) &= \sum_{k=1}^{n-1} k p_k = \sum_{k=1}^{n-1}\sum_{r=k}^{n-1} k(-1)^{r+k}\binom{r}{k}\binom{n}{r}\left(\frac{n-r}{n}\right)^n \\ &= \sum_{r=1}^{n-1}(-1)^r\binom{n}{r}\sum_{k=1}^{r}(-1)^k k\binom{r}{k} = n\left(\frac{n-1}{n}\right)^n. \end{aligned}$$

Therefore,

$$E(m(A_n)) \geq 1 + \left(\frac{n-1}{n}\right)^n,$$

and so $\lim\limits_{\overline{n\to\infty}} E(m(A_n)) \geq 1 + 1/\mathrm{e}$.

Mesard and Parisi (1985, 1987) used the 'replica method' of statistical physics to show that $c^* = \pi^2/6$. Although the replica method is not mathematically rigorous (at least, not yet), its predictions are frequently correct. Note that $\pi^2/6 = \sum_{k=1}^{\infty} k^{-2} = \zeta(2)$ is reminiscent of the value $\zeta(3) = \sum_{k=1}^{\infty} k^{-3}$ proved by Frieze (1985*a*) for the minimum spanning tree problem (see §5 of Chapter 6). After over a decade's stagnation, Coppersmith and Sorkin (1999) made progress with the upper bound: by analysing an appropriate assignment algorithm, they proved that $c^* < 1.94$. Shortly after that, in a remarkable paper, Aldous (2001) proved that c^* is indeed $\pi^2/6$.

However, this is not the end of the story. For from it. Parisi (1998) made the staggering conjecture that

$$E(m(A_n)) = \sum_{k=1}^{n} \frac{1}{k^2}$$

for every n. Here, as before, $A_n = (A_{ij})$ is the exponential random assignment matrix: $P(A_{ij} \leq x) = l - \mathrm{e}^{-x}$ for $x \geq 0$. Parisi's conjecture seems to be far from a proof, but Coppersmith and Sorkin (1999) gave an ingenious generalization of it. Let $A(n,m) = (A_{ij})$ be on n by m matrix whose entries are i.i.d. exponential r. vs, each with mean l. Let $m_k(A(m,n))$ be the minimal sum of k entries, no two of which are in the name row or column. Coppersmith and Sorkin (1999) conjectured that

$$E(m_k(A(m,n))) = \sum_{i,j\geq 0_{i+j<k}} \frac{1}{(m-i)(n-j)}$$

for every k, $l \leq k \leq \min\{m,n\}$. Note that for $m = n = k$ we have $m_k(A(m,n)) = m(A_n)$ and the Coppersmith–Sorkin conjecture implies the conjecture of Parisi.

Coppersmith and Sorkin (1999) proved some partial results that indicate that their conjecture is indeed true, and Alm and Sorkin (2001) proved the conjecture for $k \leq 4, k = m = 5$ and $k = m = n = 6$. For a wealth of information about the random assignment problem, see Coppersmith and Sorkin (1999) and Alm and Sorkin (2001).

7.4 Matchings in Random Graphs

At what stage t will a.e. random graph G_t of even order have a complete matching? Since the minimum degree of a graph with a complete matching is at least 1, this t has to be at least $(n/2)\{\log n + \omega(n)\}$, where $\omega(n) \to \infty$. The somewhat surprising fact that this trivial necessary condition is also sufficient was proved by Erdős and Rényi (1966). In this section we shall deduce this theorem from a sharper result: a.e. graph process on an even number of vertices is such that the edge raising the minimum degree to 1 also ensures that the graph has a complete matching. More importantly, as proved by Bollobás and Thomason (1985), when a r.g. has only slightly more than $(n/4)\log n$ edges, then with probability tending to 1 it has a matching covering all but at most one of the vertices of degree at least 1. A further strengthening of this result was proved by Bollobás and Frieze (1985).

We start with the last result mentioned above. As usual, we work with the model $\mathcal{G}(n,p)$. What can we say about p ($p \geq 1/n$, say), if a.e. G_p has a matching covering all but at most one of the vertices? If G_p is such a graph, then it does not contain six vertices: x_1, x_2, x_3, x_4, y_1 and y_2, such that each x_i has degree 1, x_1 and x_2 are joined to y_1, and x_3 and x_4 are joined to y_2. Indeed, if we have six such vertices, then every matching misses at least one of x_1 and x_2 and at least one of x_3 and x_4. Now the expected number of configurations formed by x_1, x_2 and y_1 is

$$\binom{n}{2}(n-2)p^2(1-p)^{2(n-3)}.$$

It is easily seen that if $1/n \leq p \leq (1/2n)(\log n + 2\log\log n + c)$ for some constant c, then the expectation is bounded away from 0 and, furthermore, with probability at least $\varepsilon(c) > 0$, the graph contains such a configuration of six vertices (Ex. 7). Hence p has to be at least $(1/2n)\{\log n + 2\log\log n + \omega(n)\}$, where $\omega(n) \to \infty$. The main result of the section shows that this trivial necessary condition is sufficient.

Theorem 7.14 *Let* $p = \{\log n + 2\log\log n + \omega(n)\}/2n$, *where* $\omega(n) \to \infty$. *Then a.e.* G_p *has a matching covering every vertex of degree at least* 1, *with the exception of at most one vertex.*

Proof Let $p_0 = (\log n + \log\log n)/n$. Since a.e. G_{p_0} is connected, we may and shall assume that $p \le p_0$. The proof consists of a series of lemmas. The first three have no obvious connection with matchings.

Let A_1 be the event that (i) G_p consists of a giant component and at most $n^{1/2}/\log n$ isolated vertices, (ii) it has at most $n^{1/2}$ vertices of degree 1, and (iii) no two vertices of degree 1 have a common neighbour. □

Lemma 7.15 $P(A_1) = 1 + o(1)$.

Proof By the remark after Theorem 7.2, the trees of order 2 vanish after time $(n/4)\{\log n + \log\log n + \omega(n)\}$. Furthermore, it is immediate (cf. the proof of Theorem 7.3. 1) that the expected number of vertices of degree 0 is $o(n^{1/2}/\log n)$ and the expected number of vertices of degree 1 is $o(n^{1/2})$.

Finally, p was chosen exactly to ensure that the expected number of pairs of vertices of degree 1 having a common neighbour tends to 0:

$$\binom{n}{2}(n-2)p^2(1-p)^{2(n-3)}$$
$$\sim \frac{n^3}{2}\left(\frac{\log n + \omega(n)}{2n}\right)^2 \exp\{-\log n - 2\log\log n - \omega(n)\} = o(1) \quad \square$$

Let A_2 be the event that G_p does not have $r_0 = (4\log\log n/\log n)n$ independent vertices.

Lemma 7.16 $P(A_2) = 1 + o(1)$.

Proof The expected number of r_0-tuples of independent vertices is

$$\binom{n}{r_0}(1-p)^{r_0(r_0-1)/2} \le \left(\frac{en}{r_0}\right)^{r_0} e^{-pr_0(r_0-1)/2}. \tag{7.10}$$

Since

$$e^{pr_0/2} \geq \frac{1}{2}\log n > \frac{e \log n}{\log\log n} > 2\frac{en}{r_0},$$

the right-hand side of (9) is $o(1)$. □

Let A_3 be the event that the complement of G_p does not contain a $K(r_0, r_0)$, i.e. a complete bipartite graph with r_0 vertices in each class.

Lemma 7.17 $P(A_3) = 1 + o(1)$.

Proof The two vertex classes of a $K(r_0, r_0)$ can be selected in $\frac{1}{2}\binom{n}{r_0}\binom{n-r_0}{r_0} < \binom{n}{r_0}$ different ways. Hence, as in the proof of Lemma 7.16, the expected number of $K(r_0, r_0)$ graphs in the complement of G_p is at most

$$\binom{n}{r_0}^2 (1-p)^{r_0^2} < \left\{\left(\frac{en}{r_0}\right)^2 e^{-pr_0}\right\}^{r_0} < 2^{-r_0} = o(1). \qquad \square$$

The combinatorial basis of the proof is the extension of Tutte's factor theorem (1947) due to Berge (1958) (see Bollobás, 1978*a*, pp. 55–57). Call a component of a graph *odd* if it has an odd number of vertices, and denote by $q(H)$ the number of odd components of a graph H. Then no matching covers all but at most one vertex of a graph H if there is a set $R \subset V(H)$ such that

$$q(\dot{H} - R) \geq |R| + 2. \tag{7.11}$$

For $r = 0, 1, \ldots$ denote by B_r the event that there is a minimal set $R \subset V$ such that $|R| = r$, and $G_p - R$ has at least $r + 2$ components which are joined to R and each of which is either an isolated vertex or has at least three vertices. Furthermore, let $B(r, s)$ be the event that B_r holds and the union of the $r + 1$ smallest components in the definition above, which we shall denote by S, has s elements. Note that if $s \leq r$ then $B_r = \emptyset$.

We see from (7.11) that if A_1 holds for G_p and G_p does not satisfy the conclusions of Theorem 7.14, then B_r holds for some $r, 0 \leq r \leq n/2$. Hence, by Lemma 7.15, Theorem 7.14 is proved if we show that

$$P\left(\bigcup_{r=1}^{\lfloor n/2 \rfloor} B_r\right) = o(1). \tag{7.12}$$

If B_r holds, then G_p contains a set of $r + 2$ independent vertices:

selecting one vertex each from $r+2$ components of $G_p - R$ we obtain such a set. Hence

$$\bigcup_{r=r_0}^{\lfloor n/2 \rfloor} B_r \subset A_2,$$

so by Lemma 7.16 relation (7.12) follows if we show

$$P\left(\bigcup_{r=1}^{r_0} B_r\right) = o(1). \tag{7.13}$$

Let A_4 be the event that one cannot find a set $R \subset V$ such that $1 \le |R| \le r_0$, $G_p - R$ has at least two components and the union of all but a largest of the components of $G_p - R$ has at least r_0 vertices.

Lemma 7.18 $P(A_4) = 1 + o(1)$.

Proof We claim that $A_3 \subset A_4$, so the assertion follows from Lemma 7.17. To see $A_3 \subset A_4$, suppose $G_p - R$ has components of orders $a_1 \le a_2 \le \ldots \le a_l$ and $\sum_{i=1}^{l-1} a_i > r_0$. Let j be the smallest index with $\sum_{i=1}^{j} a_i \ge r_0$. Then

$$\sum_{i=1}^{j} a_i \le r_0 + a_j \le r_0 + (n - r_0)/2 = (n + r_0)/2$$

so

$$\sum_{i=j+1}^{l} a_i \ge n - r_0 - (n + r_0)/2 \ge r_0$$

Since no edge joins one of the first j components to the others, the complement of G_p contains a

$$K\left(\sum_{i=1}^{j} a_i, \sum_{i=j+1}^{l} a_i\right) \supset K(r_0, r_0). \qquad \square$$

Clearly

$$\bigcup_{r=1}^{r_0} B_r \subset \bigcup_{r=1}^{r_0} \bigcup_{s=r+1}^{n} B(r,s)$$

and

$$\left\{\bigcup_{r=1}^{r_0} \bigcup_{s=r_0}^{n} B(r,s)\right\} \cap A_4 = \varnothing$$

so by Lemma 7.18 relation (7.13) and our theorem follow if we show that

$$P\left(\bigcup_{r=1}^{r_0}\bigcup_{s=r+1}^{r_0} B(r,s)\right) = o(1). \tag{7.14}$$

Our next aim is to replace $\bigcup_{s=r+1}^{r_0} B(r,s)$ by a considerably smaller union. Set $s_0 = (\log n)^3 n^{1/2}$.

Lemma 7.19 *Relation (7.14) holds if*

$$P\left(\bigcup_{r=1}^{s_0}\bigcup_{s=r+1}^{s_0} B(r,s)\right) = o(1). \tag{7.15}$$

Proof We have $\binom{n}{r}\binom{n-r}{s}$ choices for R and S. The minimality of R implies that the $R-S$ edges and the edges joining vertices of S form a connected subgraph of G_p. Hence there are at least $2r$ edges from R to S. Finally, no vertex in S is joined to a vertex not in $R \cup S$. Therefore if $1 \le r < s \le r_0$, then

$$\begin{aligned} P\{B(r,s)\} &\le \binom{n}{r}\binom{n-r}{s}\binom{rs}{2r} p^{2r}(1-p)^{s(n-r-s)} \\ &\le \left(\frac{en}{r}\right)^r \left(\frac{en}{s}\right)^s \left(\frac{eps}{2}\right)^{2r} e^{-psn_0} = \bar{B}(r,s), \end{aligned}$$

where $n_0 = n - 2r_0$.

By the definition of p and n_0

$$e^{-pn_0} \le \varepsilon(n)(\log n)^3 n^{-1/2},$$

where $\varepsilon(n) \to 0$. Hence if $s_0 \le s \le r_0$ and $r \le s$, then

$$\bar{B}(r,s+1)/\bar{B}(r,s) \le (en/s)e^2 e^{-pn_0} < \frac{1}{2}.$$

This implies that with $s_0(r) = \max(r, s_0)$ we have

$$\sum_{s=s_0(r)}^{r_0} \bar{B}(r,s) \le 2B\{r, s_0(r)\}.$$

Therefore if (7.15) holds, then so does (7.14), provided

$$\sum_{r=s_0}^{r_0} \bar{B}(r,r) = o(1).$$

The last relation is immediate since

$$\sum_{r=s_0}^{r_0} \bar{B}(r,r) \le \sum_{r=s_0}^{r_0} \mathrm{e}^{4r} \left(\frac{pn}{2}\right)^{2r} \mathrm{e}^{-prn_0} \le \sum_{r=s_0}^{r_0} \{\mathrm{e}^4 (\log n)^5 n^{-1/2}\}^r. \qquad \square$$

For $h \ge 1$ let C_h be the event that V contains pairwise disjoint sets T, H and S such that $0 \le |T| = t \le s_0 - h, |H| = h, 3 \le |S| = s \le s_0$, S spans a component of $G_p - T \cup H$, each vertex of $T \cup H$ is joined by an edge to some vertex in S and for each $x \in T$ there is a vertex y which is isolated in $G_p - T \cup H$ and is adjacent to x.

Lemma 7.20 $P(C_h) = o(1)$ *for every* $h \in \mathbb{N}$.

Proof The probability that a set S of s vertices spans a connected subgraph is at most

$$\binom{\binom{s}{2}}{s-1} p^{s-1} \le \left(\frac{\mathrm{e}sp}{2}\right)^{s-1}.$$

Hence the expected number of triples (T, H, S) with the parameters above is at most

$$\begin{aligned}
\binom{n}{t}^2 \binom{n}{h} \binom{n}{s} t!p^t(1-p)^{tn_0} \left(\frac{\mathrm{e}sp}{2}\right)^{s-1} (sp)^{t+h}(1-p)^{sn_0} \\
\le \frac{c_1^{s+t}}{t!} \{n^{-1/2}(\log n)^3\}^{t+s} (\log n)^{2t+s+h} s^{t+h} n \\
\le \frac{c_1^{s+t}}{t!} s^{t+h} n^{1-t/2-s/2} (\log n)^{5t+4s+h} = \bar{C}(s,t),
\end{aligned}$$

where c_1 is an absolute constant.

Now if $s \le t$, then

$$\bar{C}(s,t+1)/\bar{C}(s,t) \le c_1 n^{-1/2} (\log n)^5$$

and if $t \le s$, then

$$\bar{C}(s+1,t)/\bar{C}(s,t) \le c_1 \mathrm{e} 2^h n^{-1/2} (\log n)^4.$$

Consequently

$$\begin{aligned}
\sum_{s=3}^{s_0} \sum_{t=0}^{s_0-h} \bar{C}(s,t) &\le 2\left\{\sum_{s=3}^{s_0} \bar{C}(s,s) + \sum_{t=0}^{2} \bar{C}(3,t)\right\} \\
&\le \sum_{s=3}^{s_0} (\mathrm{e}c_1)^{2s} s^h n^{1-s} (\log n)^{9s+h} + O\{n^{-1/2}(\log n)^{h+12}\} = o(1),
\end{aligned}$$

which completes the proof of the lemma. $\square$

We have arrived at the last step in the proof Theorem 7.14. Let $h_0 \geq 6$ be fixed. Given $t \geq 0, u \geq h_0$ and $w \geq 3u$, denote by $C(t,u,w)$ the event that with $r = t + u$ and $s = t + w$ the event B_r holds, $R = T \cup U, S = T' \cup W, |T| = |T'| = t, |U| = u$ and $|W| = w$, the set T' consists of vertices isolated in $G_p - T \cup U, G_p$ contains a complete matching from T to T', each vertex in T is adjacent to at least one vertex in W, W consists of $u + 1$ components of $G_p - T \cup U$ and each of those components sends at least h_0 edges to U. Recalling that if A_1 holds then no vertex has two neighbours of degree 1,

$$\bigcup_{r=1}^{s_0} \bigcup_{s=r+1}^{s_0} \{B(r,s) \cap A_1\} \subset \bigcup_{h=0}^{h_0} C_h \cup \bigcup_{t=0}^{s_0} \bigcup_{u=h_0}^{s_0} \bigcup_{w=3u+3}^{s_0} C(t,u,w).$$

Consequently, by Lemmas 7.15 and 7.19 our theorem is proved if we show that

$$\sum_{t=0}^{s_0} \sum_{u=h_0}^{s_0} \sum_{w=3u+3}^{s_0} P\{C(t,u,w)\} = o(1). \tag{7.16}$$

To prove (7.16) we make use of the fact that $G_p[W]$ has at least $w - u - 1$ edges and U and W are joined by at least uh_0 edges. We obtain the following crude upper bound on $P\{C(t,u,w)\}$:

$$\begin{aligned} &\binom{n}{t}^2 t!p^t(1-p)^{tn_0}\binom{wt}{t}p^t\binom{n}{u}\binom{n}{w}\binom{w(w-1)/2}{w-u-1}p^{w-u-1}\binom{uw}{uh_0}p^{uh_0}(1-p)^{wn_0} \\ &\quad \leq \frac{1}{t!}c_1^{t+u+w}(pn)^{2t}w^t\{n^{-1/2}(\log n)^3\}^{t+w_n u+w_u-u_w-u-1}p^{w-u-1}(pw/h_0)^{uh_0} \\ &\quad = \bar{C}(t,u,w), \end{aligned}$$

where c_1 is a positive absolute constant.

Clearly

$$\bar{C}(t,u+1,w)/\bar{C}(t,u,w) \leq \frac{c_1 n}{pw}(pw)^{h_0} \leq n^{-1},$$

so for $w \leq s_0 \leq n^{1/2}(\log n)^3$

$$\begin{aligned} \sum_{u=h_0}^{s_0} \bar{C}(t,u,w) &\leq 2\bar{C}(t,h_0,w) \\ &\leq \frac{1}{t!}c_2^{t+w}(\log n)^{5t+4w+4h_0^2}n^{-t/2-w/2+2h_0+1-h_0^2/2}w^t \\ &\leq \frac{1}{t!}(\log n)^{6t+5w}w^t n^{-t/2-w/2-2}, \end{aligned}$$

where c_2 depends only on h_0.

Therefore

$$\sum_{t=0}^{s_0}\sum_{u=h_0}^{s_0}\sum_{w=h_0}^{t}\bar{C}(t,h_0,w) \le \sum_{t=0}^{s_0}\sum_{w=h_0}^{t}(\log n)^{12t}n^{-t/2-w/2-2} = o(1)$$

and

$$\sum_{t=0}^{s_0}\sum_{u=h_0}^{s_0}\sum_{w=t}^{s_0}\bar{C}(t,h_0,w) \le \sum_{t=0}^{s_0}\sum_{w=t}^{s_0}w^t n^{-t/2-t/4-2} = o(1).$$

Relation (7.14) is a consequence of these inequalities so the proof of Theorem 7.14 is complete. □

The proof of Theorem 7.14 was rather cumbersome because we had to consider graphs with only about $(n/4)\log n$ edges. As we know, about twice as many edges are needed to make it likely that a r.g. has no isolated vertices. In that range the proof would have been considerably simpler, as would a direct proof of the following immediate consequence of Theorem 7.14, which is an analogue of Theorem 7.3.

Corollary 7.21 *(i) Let $x \in \mathbb{R}, n = 2m$ and $M = (n/2)\{\log n + x + o(1)\}$. Then*

$$\lim_{m\to\infty} P(G_M \text{ has a 1-factor}) = \lim_{m\to\infty} P\{\delta(G_M) \ge 1\} = 1 - \mathrm{e}^{-\mathrm{e}^{-x}}.$$

(ii) If n is even, $\omega(n) \to \infty$ and $M = (n/2)\{\log n + \omega(n)\}$ then a.e. G_M has a 1-factor. □

Not much effort is needed to prove the hitting time version of Corollary 7.21: one checks that the estimates in the proof of Theorem 7.14 sail through for $\mathcal{G}(n,p;\ge 1)$ with $p = (\log n - \log\log\log n)/n$ and then applies Lemma 7.9.

Theorem 7.22 *A.e. graph process $\widetilde{G}$ on an even number of vertices is such that*

$$\tau(G \text{ has a 1-factor}; \widetilde{G}) = \tau\{\delta(G) \ge 1; \widetilde{G}\} = \tau\{\kappa(G) \ge 1; \widetilde{G}\}.$$

If we do not insist on a complete matching and are satisfied with a set of $(n/2) + o(n)$ independent edges, then many fewer than $(n/2)\log n$ edges will do.

Theorem 7.23 *Let $M = n\omega(n)$, where $\omega(n) \to \infty$. Then a.e. G_M contains $(n/2) + o(n)$ independent edges.*

Proof This is an immediate consequence of Berge's extension of Tutte's factor theorem and the fact that for any fixed $\varepsilon > 0$ almost no G_M contains $\lfloor \varepsilon n \rfloor$ independent vertices (Ex. 8). □

Theorem 22 tells us that the obstruction to a 1-factor is the existence of vertices of degree 0. What happens if we take only those elements of $\mathcal{G}(n, M)$ which do have minimal degree at least 1? Bollobás and Frieze (1985) proved that, perhaps not too surprisingly, the critical value of M is about $\frac{1}{4}n\log n + \frac{1}{2}n\log\log n$.

Theorem 7.24 *Let* $M = (n/4)(\log n + 2n\log\log n + c_n), n = 2m, m \in \mathcal{N}$. *Then*

$$\lim_{n\to\infty} P\{G_M \textit{ has a 1-factor } |\delta(G_M) \geq 1\} = \begin{cases} 0, & \textit{if } c_n \to -\infty \\ & \textit{sufficiently slowly,} \\ e^{-e^{-c}/8}, & \textit{if } c_n \to c, \\ 1, & \textit{if } c_n \to \infty. \end{cases}$$

□

The condition that $c_n \to -\infty$ sufficiently slowly seems curiously out of place but, in fact, some condition is clearly needed for if, rather crudely, $M = m = n/2$, then

$P\{G_M$ has a 1-factor $|\delta(G_M) \geq 1\} = 1$ since $\delta(G_M) = 1$ implies that G_M consists of m independent edges.

In spite of the strong resemblance between Theorems 7.14 and 7.24, the results are very different since Theorem 7.24 claims that a.e. element of a set of very small probability has a matching, while Theorem 7.14 is about a.e. element of the entire space.

There is a function $m(c)$ such that if $c > 0$ is a constant and $M \sim cn/2$, then a.e. G_M is such that the maximal number of independent edges in G_M is $\{m(c) + o(1)\}n$. Unfortunately, at present there is no closed form expression for $m(c)$. Karp and Sipser (1981) gave simple algorithms which with probability tending to 1 find $\{m(c) + o(1)\}n$ independent edges in a r.g. G_M. Earlier, Angluin and Valiant (1979) gave a fast algorithm which for a sufficiently large constant c finds complete matchings in $\mathcal{G}(2m, c\log n/n)$ with probability at least $1 - O(n^{-2})$.

For large values of c we have rather tight bounds on $m(c)$. Since a.e. $G_{c/n}$ has about $e^{-c}n$ isolated vertices, $m(c) \leq (1 - e^{-c})/2$. Frieze (1985*d*) proved that this upper bound gives the correct order of $m(c)$:

$$e^{-c} \leq 1 - 2m(c) \leq \{1 + \varepsilon(c)\}e^{-c},$$

where $\lim_{c\to\infty} \varepsilon(c) = 0$.

A k-factor is a natural generalization of a complete matching: a *k-factor* of a graph G is a k-regular subgraph H of G whose vertex set is the entire vertex set of G. Most of the results concerning complete matchings can be extended to k-factors. The next result, due to Shamir and Upfal (1981*a*), generalizes Corollary 21(ii).

Theorem 7.25 *If $k \geq 1$, kn is even, $\omega(n) \to \infty$ and $M = (n/2)\{\log n + (k-1)\log\log n + \omega(n)\}$, then a.e. G_M has a k-factor.* □

The hitting time version of Theorem 7.24 is an immediate consequence of a theorem of Bollobás and Frieze (1985): a.e. graph process is such that for even n the very edge increasing the minimum degree to k ensures that the graph contains k independent 1-factors.

It is interesting to note that Shamir and Upfal proved Theorem 7.25 by the method of alternating chains rather than by making use of Tutte's f-factor theorem. Shamir and Upfal (1981*b*) also proved a variant of Theorem 7.24 for graphs with at least $n(\log n)\omega(n)$ edges, where $\omega(n) \to \infty$.

Aronson, Frieze and Pittel (1998) greatly sharpened the Karp–Sipser results on matching algorithms we mentioned above. For example, they proved that if $c > \mathrm{e}$ then in $G_{c/n}$ the Karp–Sipser algorithm almost merely finds a matching whose site is within $n^{1/5+o(1)}$ of the optimum.

Frieze, Radcliffe and Suen (1995) ran the following very simple matching algorithm on random cubic graphs. At each stage, choose a vertex u of minimal degree from the current graph, pick a neighbour v of u at random, add uv to the matching under construction, and delete u and v from the current graph. Frieze, Radcliffe and Suen proved the rather surprising result that if we write λ_n for the number of vertices not matched when this algorithm is run on a random cubic graph $G_{3\text{-reg}}$, then the expectation of λ_n satisfies

$$c_1 n^{1/5} \leq E(\lambda_n) \leq C_2 n^{1/5} \log n$$

for some positive constants c_1 and c_2.

Dyer and Frieze (1991), Dyer, Frieze and Pittel (1993), Aronson, Dyer, Frieze and Suen (1994, 1995) and others analysed the performance of randomized matching algorithms ran on fixed graphs. For example, Dyer and Frieze (1991) studied the *randomized greedy matching algorithm* in which the next edge is always chosen at random from those remaining. They showed that there are graphs G for which this algorithm usually constructs a matching with hardly more than $\alpha_1(G)/2$ edges, where

$\alpha_1(G)$ is the maximal number of edges in a matching in G. (Trivially, every matching that cannot be enlarged has at least $\alpha_1(G)/2$ edges.) On the other hand, Aronson, Dyer, Frieze and Suen (1995) proved the rather surprising result that if we change the algorithm slightly by picking first a non-isolated vertex of the current graph and then its neighbour, then the expected site is at least $(\frac{1}{2}+\varepsilon)\alpha_1(G)$ for some fixed $\varepsilon > 0$.

Rather different aspects of random matchings were studied by Kahn and Kim (1998) and Alon, Rödl and Ruciński (1998). Thus, Kahn and Kim proved that if in a fixed r-regular graph G we consider a matching M selected at random from the set of *all* matchings (not only maximal matchings) then for large r the probability that a given vertex v is not on an edge of M is about $r^{-1/2}$.

Following Alon, Rödl and Ruciński, call a graph of order $2n$ *super* (α, ε)*-regular* if it is bipartite with classes V_1 and V_2, where $|V_1| = |V_2| = n$, such that the degree of every vertex is at least $(\alpha-\varepsilon)n$ and at most $(\alpha+\varepsilon)n$, and if $U \subset V_1$ and $W \subset V_2$ with $|U| \geq \varepsilon n$ and $|W| \geq \varepsilon n$ then

$$\left| \frac{e(u,w)}{|u||w|} - \frac{e(V_1,V_2)}{|V_1||V_2|} \right| < \varepsilon.$$

Alon, Rödl and Ruciński (1998) proved that if $0 < 2\varepsilon < \alpha < 1$ and $n > n(\varepsilon)$ then every super (α, ε)-regular graph of order $2n$ has at least $(\alpha - 2\varepsilon)^n n!$ and at most $(\alpha + 2\varepsilon)^n n!$ complete matchings. Note that for $r = r(n) > 2\varepsilon n$ almost every r-regular biportite graph satisfies these conditions.

The rest of this section is somewhat of a digression from the main line of this book; we shall give a brief account of some results about 1-factors and large matchings (sets of vertex disjoint hyperedges) in uniform hypergraphs.

Using Chebyshev's inequality, de la Vega (1982) proved the analogue of Theorem 7.23 for hypergraphs: if $r \geq 2$ is fixed and $M = n\omega(n)$, where $\omega(n) \to \infty$, then a.e. r-uniform hypergraph with n labelled vertices and M edges has $n/r + o(n)$ vertex disjoint hyperedges (see Ex. 9).

It is considerably more difficult to investigate 1-factors of hypergraphs. Schmidt and Shamir (1983) proved that if $r \geq 3$ is fixed, n is a multiple of r, $\omega(n) \to \infty$ and $M = n^{3/2}\omega(n)$, then a.e. r-uniform hypergraph with n labelled vertices and M edges has a 1-factor, i.e., has n/r vertex disjoint edges.

By applying the analysis of variance technique first used by Robinson and Wormald (1992) in their study of Hamilton cycles (see Chapter 8), Frieze and Janson (1995) greatly improved this result: for every $\varepsilon > 0$, a.e. 3-uniform hypergraph on $[n]$ with $M(n) = \lfloor n^{4/3+\varepsilon} \rfloor$ edges (3-tuples) has a 1-factor. It seems that this difficult result is still far from best possible: it is likely that the threshold for a 1-factor is again the same as the threshold for minimal degree at least 1. Thus the following extension of Corollary 7.21 is likely to be true. Let $X \in \mathbb{R}$ and $M = M(n) = \frac{n}{r}(\log r + x + o(1))$. Then if $n \to \infty$ through multiples of r, the probability that a random r-uniform hypergraph on $[n]$ with M edges has a 1-factor tends to $1 - e^{-e^{-x}}$. In fact, with probability tending to 1, the hitting time of a 1-factor may well be exactly the hitting time of minimal degree at least 1.

Cooper, Frieze, Molloy and Reed (1996) used a similar technique to prove surprisingly precise results about 1-factors in random regular hypergraphs. Fix $r \geq 2$ and $d \geq 2$, and set $\rho_d = 1 + (\log d)/\left((d-1)\log \frac{d}{d-1}\right)$.

Let $G^{(r)}_{d\text{-reg}}$ be a random d-regular r-uniform hypergraph with vertex set $[n]$, where r divides dn. If $r < \rho_d$ then a.e. $G^{(r)}_d$ has a 1-factor, and if $r > \rho_d$ then almost no $G^{(r)}_d$ has a 1-factor. The proof requires rather difficult moment calculations.

Finally, we turn to a beautiful and deep theorem of Alon, Kim and Spencer (1997) about near-perfect matchings in fixed graphs. There are constants $c_3, c_4, \ldots$ such that the following holds. Let H be an r-uniform d-regular hypergraph on n vertices such that no two edges have more than one vertex in common. Then, for $r = 3$, H contains a matching covering all but $c_3 n d^{-1/2}(\log d)^{1/2}$ vertices and, for $r > 3$, there is a matching missing fewer than $c_k n d^{-1/(r-1)}$ vertices. In a Steiner triple system on n points, every point is in $d = \frac{(n-1)}{2}$ triples, so this theorem implies that every Steiner triple system on n points contains at least $n/3 - c_3 n^{1/2}(\log n)^{3/2}$ pairwise disjoint triples.

7.5 Reliable Networks

Graphs are unsophisticated models of communication networks. Adopting a rather simplistic view, one can say that a communication network should carry messages between pairs of centres as reliably as possible. Each communication line has a certain probability of failing, and one is interested in the probability that in spite of the failure of some lines it is still possible to send a message from any centre to any other centre. In the simplest case it is assumed that each communication line transmits information both ways and that the lines fail independently and with a common probability. Thus one is led to the model $\mathscr{G}(H;p)$ and the question: what is the probability that a random element of $\mathscr{G}(H;p)$ is connected?

Recall that a random element of $\mathscr{G}(H;p)$ is obtained by selecting edges of H independently and with probability p. In other words, we have a communication network H in which the lines fail independently and with probability $q = 1 - p$. Let us write $f_H(p)$ for the probability that a random element of $\mathscr{G}(H;p)$ is connected.

If H is a graph with m edges then, trivially,

$$f_H(p) = \sum_{j=n-1}^{m} f_j p^j (1-p)^{m-j},$$

where $f_j = f_j(H)$ is the number of sets of edges of cardinality j which contain a spanning tree of H. This form of $f_H(p)$ was first investigated by Moore and Shannon (1956). By now there is a formidable literature on the problem of finding exact or asymptotic information about this polynomial: Birnbaum, Esary and Saunders (1961), Kelmans (1967*a*, 1970, 1971, 1976*a*), Lomonosov and Polesskii (1971, 1972*a*, *b*), Polesskii (1971*a*, *b*), Boesch and Felzer (1972), Frank, Kahn and Kleinrock (1972), Van Slyke and Frank (1972), Lomonosov (1974), Margulis (1974), Bixby (1975), Even and Tarjan (1975), Rosenthal (1975), Valiant (1979), Ball (1980), Buzacott (1980), Ball and Provan (1981*a*, *b*), Bauer *et al.* (1981), Boesch, Harary and Kabell (1981) and Provan and Ball (1981).

The papers in the list above, which is far from complete, tackle a variety of aspects of the reliability problem: they study the computational difficulty of finding some or all the coefficients of the polynomial $f_H(p)$, analyse the cut sets and spanning trees of H, choose a graph with as many spanning trees as possible (provided the order and size are fixed) and discuss how suitable subcollections of spanning trees and cut sets can give reasonable bounds on $f_H(p)$.

Instead of saying a few superficial words about each of the papers above, we shall concentrate on a beautiful theorem of Margulis (1974), which belongs to the pure theory of random graphs. This result concerns a threshold phenomenon in the model $\mathscr{G}(H;p)$.

Let H_n be a connected graph of order $n > 1$. What can we say about the function $f_{H_n}(p)$ as $n \to \infty$? Since connectedness is a monotone increasing property, by the remark after Theorem 2.1 the function $f_{H_n}(p)$ is strictly increasing, $f_{H_n}(0) = 0$ and $f_{H_n}(1) = 1$. Will $f_{H_n}(p)$ increase from being almost 0 to being almost 1 in a short interval? In other words, given

$0 < \varepsilon < \frac{1}{2}$, does $f_{H_n}^{-1}(1-\varepsilon) - f_{H_n}^{-1}(\varepsilon)$ tend to 0 as $n \to \infty$? If it does, then the sequence (H_n) behaves like (K^n), the sequence of complete graphs, namely there is a threshold function $p_0(n) \in (0,1)$ such that if p is slightly smaller than p_0, then $f_{H_n}(p)$ is close to 0 and if p is slightly larger than p_0, then $f_{H_n}(p)$ is close to 1.

Not every sequence has a threshold function for connectedness. As a simple example, let H_n consist of two complete graphs K^{n_1} and $K^{n_2} = K^{n-n_1}$ joined by an edge, where $n_1 = \lfloor n/2 \rfloor$. Then $f_{H_n}(p) \to p$ uniformly on [0,1], since the probability of H_n being connected depends mostly on the probability of the edge joining K^{n_1} to K^{n_2}.

Clearly, if we join K^{n_1} and K^{n_2} by a fixed number of edges, then the obtained sequence (H_n) still fails to have a threshold function for connectedness. On the other hand, if we join K^{n_1} and K^{n_2} by $l(n)$ edges and $l(n) \to \infty$, then (H_n) does have a threshold function. Note that in the latter case the edge-connectivity $\lambda(H_n)$ of H_n tends to ∞ as $n \to \infty$. What Margulis proved is exactly that $\lambda(H_n) \to \infty$ ensures that the sequence (H_n) has a threshold function for connectedness.

Theorem 7.26 *There is a function $k : (0,1) \times (0,1) \to \mathbb{R}$ such that if $\lambda(H) \geq k(\delta, \varepsilon)$, then*

$$f_H^{-1}(1-\varepsilon) - f_H^{-1}(\varepsilon) < \delta.$$

Theorem 7.26 is a consequence of a more general theorem of Margulis (1974), which concerns set systems. Let X be a finite set of cardinality m and let $\mathscr{A}$ be a collection of subsets of $X : \mathscr{A} \subset \mathscr{P}(X)$. Endow $\mathscr{P}(X)$ with the Hamming distance: $d(A,B) = |A \Delta B|$ and define the *boundary* $\partial\mathscr{A}$ of $\mathscr{A}$ as

$$\partial\mathscr{A} = \{A \in \mathscr{A} : \exists B \notin \mathscr{A}, d(A,B) = 1\}.$$

Define a function $h_{\mathscr{A}} : \mathscr{P}(X) \to \mathbb{Z}^+$ by

$$h_{\mathscr{A}}(A) = \begin{cases} |\{B \notin \mathscr{A} : d(A,B) = 1\}|, & \text{if } A \in \mathscr{A}, \\ 0, & \text{if } A \notin \mathscr{A}, \end{cases}$$

and for $\emptyset \neq \mathscr{A} \neq \mathscr{P}(X)$ set

$$k(\mathscr{A}) = \min\{h_{\mathscr{A}}(A) : A \in \partial\mathscr{A}\}.$$

Call $\mathscr{A}$ a *monotone set system over* X if $A \subset B \subset X$ and $A \in \mathscr{A}$ imply $B \in \mathscr{A}$.

Given $0 \leq p \leq 1$ and a set X, select the elements of X independently and with probability p. Denote by $f_{\mathscr{A}}(p)$ the probability that the set formed by the selected elements belongs to $\mathscr{A}$. If $\mathscr{A}$ is monotone and

$\emptyset \neq \mathscr{A} \neq \mathscr{P}(X)$, then (cf. the remark after Theorem 2.1) $f_{\mathscr{A}}(p)$ is a strictly increasing function, $f_{\mathscr{A}}(0) = 0$ and $f_{\mathscr{A}}(1) = 1$.

Theorem 7.27 *There is a function $k : (0,1) \times (0,1) \to \mathbb{R}$ such that if $\mathscr{A}$ is a monotone system and $k(\mathscr{A}) \geq k(\delta, \varepsilon)$, then*

$$f_{\mathscr{A}}^{-1}(1-\varepsilon) - f_{\mathscr{A}}^{-1}(\varepsilon) < \delta.$$

Let us see first that Theorem 7.27 implies Theorem 7.26. Let $k(\delta, \varepsilon)$ be the function given in Theorem 7.26 and let $H = (V, E)$ be a graph with $\lambda(H) \geq k(\delta, \varepsilon)$. Set $X = E$ and

$$\mathscr{A} = \{A : A \subset E \text{ and } H - A \text{ is disconnected}\}.$$

Then $\mathscr{A}$ is a monotone system and

$$1 - f_H(p) = f_{\mathscr{A}}(1-p).$$

Hence all we have to show is that

$$k(\mathscr{A}) \geq \lambda(H). \tag{7.17}$$

Let $A \epsilon \partial\mathscr{A}$. Then $H - A$ is disconnected and there is an edge $\alpha \epsilon E - A$ such that $(H - A) + \alpha$ is connected. Consequently, $H - A$ consists of two components, say with vertex sets V_1 and $V_2 = V - V_1$, and $h_{\mathscr{A}}(A)$ is the number of $V_1 - V_2$ edges of H. Thus $h_{\mathscr{A}}(A) \geq \lambda(H)$, proving (7.17).

We shall not present the entire proof of Theorem 7.27, but we shall show how the specific conditions on $\mathscr{A}$ are used.

Denote by μ_p the measure on $\mathscr{P}(X)$ defined by our independent selection of the elements: for $B \epsilon \mathscr{P}(X)$ put

$$\mu_p(B) = p^{|B|}(1-p)^{m-|B|}, \text{ where } m = |X|,$$

and for $\mathscr{B} \subset \mathscr{P}(X)$ put

$$\mu_p(\mathscr{B}) = \sum_{B \epsilon \mathscr{B}} \mu_p(B).$$

Note that $f_{\mathscr{A}}(p) = \mu_p(\mathscr{A})$. Furthermore, set

$$\psi_p(\mathscr{A}) = \int_{\mathscr{A}} h_{\mathscr{A}}(A) \mathrm{d}\mu_p.$$

By the definition of $h_{\mathscr{A}}$, we have

$$\psi_p(\mathscr{A}) \geq \int_{\partial\mathscr{A}} h_{\mathscr{A}}(A) \mathrm{d}u_p \geq h(\mathscr{A})\mu_p(\partial\mathscr{A}). \tag{7.18}$$

Lemma 7.28 *Let $\mathscr{A}$ be a monotone family. Then for $0 < p < 1$*

$$\frac{df_{\mathscr{A}}(p)}{dp} = \frac{\psi_p(\mathscr{A})}{p}.$$

Proof For $0 \le k \le m = |X|$ let

$$\mathscr{B}_k = X^{(k)} = \{B \in \mathscr{P}(X) : |B| = k\} \text{ and } \mathscr{A}_k = \mathscr{A} \cap \mathscr{B}_k.$$

Furthermore, given $\mathscr{C}, \mathscr{D} \subset \mathscr{P}(X)$, write $[\mathscr{C}, \mathscr{D}]$ for the *number* of pairs (C, D) such that $C \supset D, C \in \mathscr{C}$ and $D \in \mathscr{D}$. Clearly

$$\begin{aligned}\sum_{A\in\mathscr{A}_k} h_{\mathscr{A}}(A) &= [\mathscr{A}_k, \mathscr{B}_{k-1} - \mathscr{A}_{k-1}] = [\mathscr{A}_k, \mathscr{B}_{k-1}] - [\mathscr{A}_k, \mathscr{A}_{k-1}] \\ &= k|\mathscr{A}_k| - (m-k+1)|\mathscr{A}_{k-1}|.\end{aligned}$$

Therefore with the convention $\mathscr{A}_{-1} = \varnothing$ we have

$$\begin{aligned}\psi_p(\mathscr{A}) &= \int_{\mathscr{A}} h_{\mathscr{A}}(A)\mathrm{d}\mu_p = \sum_{k=0}^{m} \int_{\mathscr{A}_k} h_{\mathscr{A}}(A)\mathrm{d}\mu_p = \sum_{k=0}^{m}\left\{p^k(1-p)^{m-k}\sum_{A\in\mathscr{A}_k} h_{\mathscr{A}}(A)\right\} \\ &= \sum_{k=0}^{m} p^k(1-p)^{m-k}\{k|\mathscr{A}_k| - (m-k+1)|\mathscr{A}_{k-1}|\} \\ &= \sum_{k=0}^{m} k|\mathscr{A}_k|p^k(1-p)^{m-k} - \sum_{k=0}^{m}(m-k)|\mathscr{A}_k|p^{k+1}(1-p)^{m-k-1} \\ &= \sum_{k=0}^{m} |\mathscr{A}_k|p^k(1-p)^{m-k}\left(k - \frac{p(m-k)}{1-p}\right) \\ &= p\sum_{k=0}^{m} |\mathscr{A}_k|p^k(1-p)^{m-k}\left(\frac{k}{p} - \frac{m-k}{1-p}\right) = p\frac{\mathrm{d}f_{\mathscr{A}}(p)}{\mathrm{d}p}.\end{aligned}$$

□

In addition to inequality (7.18) and Lemma 7.28, the proof of Theorem 7.27 hinges on the following theorem about general set systems. (In fact, one only needs the result for monotone set systems.) For a proof, which is far from easy, the reader is referred to the original paper of Margulis (1974).

Theorem 7.29 *There is a continuous strictly positive function $g : (0,1) \times (0,1) \to (0,1)$ such that if $\mathscr{A} \subset \mathscr{P}(X), 0 < p < 1$ and $0 < \alpha = \mu_p(\mathscr{A}) < 1$, then*

$$\mu_p(\partial\mathscr{A})\psi_p(\mathscr{A}) > g(p, \alpha).$$

Proof of Theorem 7.27 It suffices to prove the existence of a suitable $k(\delta, \varepsilon)$ for small δ and ε. Let $0 < \delta < \frac{1}{3}, 0 < \varepsilon < \frac{1}{3}$ and set

$$\gamma = \min\{g(p, \alpha) : \delta/2 \leq p \leq 1 - \delta/2, \varepsilon \leq \alpha \leq 1 - \varepsilon\}$$

Then $\gamma > 0$ and we claim that $k(\delta, \varepsilon) = \gamma^{-1}(2/\delta)^2$ has the required properties.

Suppose this is not so and the non-trivial monotone family $\mathscr{A}$ is such that $k(\mathscr{A}) = \gamma^{-1}(2/\delta)^2$ and

$$f_{\mathscr{A}}^{-1}(1 - \varepsilon) - f_{\mathscr{A}}^{-1}(\varepsilon) \geq \delta.$$

Then there exist p_1 and p_2 such that

$$\delta/2 \leq p_1 < p_1 + \delta/2 \leq p_2 \leq 1 - \delta/2$$

and

$$\varepsilon \leq f_{\mathscr{A}}(p_1) \leq f_{\mathscr{A}}(p_2) \leq 1 - \varepsilon$$

Since $f_{\mathscr{A}}(p)$ is a polynomial in p, by the mean value theorem there is a $p \in (p_1, p_2)$ such that

$$\frac{\mathrm{d}f_{\mathscr{A}}(p)}{\mathrm{d}p} \leq \frac{1 - 2\varepsilon}{\delta/2} < \frac{2}{\delta}.$$

Consequently, by Lemma 7.28, inequality (7.18) and Theorem 7.29 we have

$$\begin{aligned} \left(\frac{2}{\delta}\right)^2 &> \left(\frac{\mathrm{d}f_{\mathscr{A}}(p)}{\mathrm{d}p}\right)^2 = \left(\frac{\psi_p(\mathscr{A})}{p}\right)^2 > \psi_p(\mathscr{A})^2 \geq k(\mathscr{A})\mu_p(\partial\mathscr{A})\psi_p(\mathscr{A}) \\ &\geq k(\mathscr{A})g(p, \alpha) \geq \gamma^{-1}\left(\frac{2}{\delta}\right)^2 g(p, \alpha), \end{aligned}$$

contradicting the definition of γ.

The minimal cardinality of a dependent set in a matroid is sometimes said to be the *girth* of the matroid. [For the theory of matroids see Welsh (1976).] The condition $k(\mathscr{A}) \geq k$ appearing in Theorem 7.27 is perhaps easiest to check when $\mathscr{A}$ is the collection of dependent sets of a matroid with girth k. Indeed, if C_1 and C_2 are circuits of a matroid (i.e. they are minimal dependent sets) then by the circuit axiom of matroids (see Welsh, 1976, p. 9) the set $C_1 \cup C_2 - \{x\}$ is a dependent set for every x. Hence if $A \supset C_1 \cup C_2$, then $A \notin \partial\mathscr{A}$. In other words if $A \in \partial\mathscr{A}$, then A contains a unique circuit C of the matroid. Then $A - \{c\}$ is independent for every $c \in C$ so $k(\mathscr{A}) \geq |C|$. From this it follows that $k(\mathscr{A})$ is exactly the girth of the matroid. Thus one obtains the following corollary of Theorem 7.27.

Corollary 7.30 *There is a function $k : (0,1) \times (0,1) \to \mathbb{R}$ such that if $\mathscr{A}$ is the collection of dependent sets of a matroid with girth at least $k(\delta,\varepsilon)$, then*

$$f_{\mathscr{A}}^{-1}(1-\varepsilon) - f_{\mathscr{A}}^{-1}(\varepsilon) < \delta.$$

Theorem 7.26 is a special case of Corollary 7.30: the matroid in question is the cocycle matroid $M^*(H)$ of the graph H. By applying Corollary 7.30 to the cycle matroid $M(H)$ we get the following result.

Corollary 7.31 *Let $g_H(p)$ be the probability that a graph in $\mathscr{G}(H,p)$ contains a cycle. There is a function $k : (0,1) \times (0,1) \to \mathbb{R}$ such that if H has girth at least $k(\delta,\varepsilon)$, then*

$$g_H^{-1}(1-\varepsilon) - g_H^{-1}(\varepsilon) < \delta.$$

7.6 Random Regular Graphs

In terms of connectivity, the most we can hope is that an r-regular graph is almost surely r-connected. It turns out that this is true with plenty to spare: a.e. r-regular graph is such that if a small set separates it, then at least one of the components is rather small. Note that if $U \subset V(G_{r\text{-reg}})$ spans a connected subgraph and $|U| < n/r$, then $\Gamma(U)\backslash U$ does separate $G_{r\text{-reg}}$ and $|\Gamma(U)\backslash U| \le (r-2)|U| + 2$. Furthermore, if the connected subgraph spanned by U contains a cycle then $|\Gamma(U)\backslash U| \le (r-2)|U|$. Therefore, since the probability that $G_{r\text{-reg}}$ contains a triangle is bounded away from 0 as $n \to \infty$, the following result is best possible, that is a.e. $G_{r\text{-reg}}$ spreads as much as it can be hoped.

Theorem 7.32 *For $r \ge 3$ and $a_0 \ge 3$, a.e. $G_{r\text{-reg}}$ is such that if $V = A \cup S \cup B, a = |A| \le |B|, s = |S|$ and there is no $A-B$ edge, then*

$$\begin{aligned} s &\ge r, \quad if\, a = 1,\\ s &\ge 2r-3, \quad if\, a = 2,\\ s &\ge (r-2)a, \quad if\, 3 \le a \le a_0 \end{aligned}$$

and

$$s \ge (r-2)a_0, \quad if\, a \ge a_0.$$

Proof The assertions follow easily from the model in §4 of Chapter 2. First of all, there is a constant $c = c(r)$ such that almost no $G_{r-\text{reg}}$ has a subgraph with $k < c\log n$ vertices and at least $k+1$ edges. This is true since there are $N(m-k+1) = (rn-2k-2)!!$ configurations containing $k+1$ given edges and, by Theorem 5.20, the number of connected graphs on k labelled vertices, having $k+1$ edges, is $O(k^{k+1})$. In fact, it is easily checked that any $c < 1/\{\log(r-1)+1\}$ will suffice (Ex. 13, cf. also inequality (7.17) of Chapter 8).

Set $s_1 = (r-2)a_0, a_1 = 4s_1$ and $a_2 = \lfloor (n-a_1)/2 \rfloor$. Take a graph $G = G_{r\text{-reg}}$ in which every set of $k \le ra_1 < c \log n$ vertices span at most k edges; we have just seen that a.e. $G_{r\text{-reg}}$ is such. Now if $V = A \cup S \cup B, a = |A|, s = |S|$ and G has no $A-B$ edges, then for $a = 2$ we have

$$2r + s + 1 \le 2(s+2),$$

so $s \ge 2r-3$ and for $3 \le a \le a_1$ and $s \le (r-2)a_1$ we have

$$ra + s \le 2e(G[A \cup S]) \le 2(a+s)$$

so $s \ge (r-2)a$.

To complete the proof it suffices to show that a.e. $G_{r\text{-reg}}$ is such that if $V = A \cup S \cup B, a = |A| \ge a_1$ and $|S| = s_1$, then there is at least one $A-B$ edge. By Corollary 2.18 it suffices to prove that a.e. configuration has the corresponding property, and this is what we proceed to do, using the notation of Theorem 2.16. What is the probability, $S(a)$, that for a given value of a there is a partition with no $A-B$ edge? We have $\binom{n}{s_1}$ choices for S and $\binom{n-s_1}{a}$ choices for A. With probability at least $(n-s_1-a)/n$, a configuration edge incident with an element of $A^* = \bigcup_{i\in A} W_i$ joins this element to $B^* = \cup_{i\in B} W_i$ and so, pairing off the elements of A^* one by one, we see, very crudely, that

$$S(a) \le \binom{n}{s_1}\binom{n-s_1}{a}\left(\frac{a+s_1}{n}\right)^{ar/2} \le n^{s_1}\binom{n-s_1}{a}\left(\frac{a+s_1}{n}\right)^{3a/2} = S'(a).$$

Now $S'(a_1) = O(n^{s_1+a_1-3a_1/2}) = O(n^{-s_1}) = o(1)$ and for $a_1 \le a < a+1 \le a_2$ we have $S'(a+1)/S'(a) = O(n^{-1/2})$, so

$$\sum_{a=a_1}^{a_2} S(a) \le \sum_{a=a_1}^{a_2} S'(a) = o(1),$$

as required. □

The proof above shows that Theorem 7.32 holds for $a_0 = \lfloor c_0 \log n \rfloor$ as well, where $c_0 > 0$ depends only on r.

Theorem 7.32 implies immediately that for $r \ge 3$ a.e. r-regular graph of even order has a 1-factor.

Corollary 7.33 *For $r \geq 3$, a.e. element of $G(n,r\text{-reg})$ has $\lfloor n/2 \rfloor$ independent edges.*

Proof It is well known that every r-connected r-regular graph has $\lfloor n/2 \rfloor$ independent edges (see, for example, Bollobás, 1978*a*, p. 88).

Bollobás and McKay (1986) calculated the expectation and variance of the number of 1-factors of $G_{r\text{-reg}}$. It is interesting to note that although the expectation is large, so is the variance and therefore Chebyshev's inequality does not even imply Corollary 7.33, which itself is very weak. □

Theorem 7.34 *Let $r \geq 3$ be fixed, n even, and denote by $X = X(G)$ the number of 1-factors of $G \in \mathcal{G}(n, r\text{-reg})$. Then*

$$E(X) \sim e^{1/4}\{(r-1)^{(r-1)}/r^{r-2}\}^{n/2}$$

and

$$E(X^2) \sim E(X)^2 e^{-(2r-1)/4(r-1)^2}.$$

Every r-regular bipartite graph of order $2n$ has a 1-factor, even more, the number of 1-factors is the permanent of the matrix $(a_{ij})_1^n$ in which a_{ij} is the number of edges joining the ith vertex of the first class to the jth vertex of the second. Hence, by van der Waerden's conjecture, proved by Egorychev (1980*a*, *b*) and Falikman (1979), every r-regular bipartite graph of order $2n$ has at least $r^n n!/n^n$ 1-factors. Although for a fixed value of r this lower bound is very crude indeed, it does not seem easy to construct an r-regular bipartite graph with few 1-factors. Extending results of Erdős and Kaplansky (1946), O'Neil found that the expected number of matchings in a random r-regular bipartite graph of order $2n$ is asymptotic to $e^{-1/2}r^{2n}/\binom{rn}{n}$, so there is an r-regular bipartite graph of order $2n$ with at most $\{1+o(1)\}e^{-1/2}r^{2n}/\binom{rn}{n}$ 1-factors. A slightly weaker result was proved by Schrijver and Valiant (1979) (see also Schrijver, 1980). The variance was calculated by Bollobás and McKay (1985).

The final model we consider briefly is $\mathcal{G}_{k\text{-out}}$. A simpler version of the proof of Theorem 7.32 implies the exact analogue of that result; here we state only the assertion about connectivity, due to Fenner and Frieze (1982), the stronger result is left as an exercise (Ex. 15).

Theorem 7.35 *For $k \geq 2$, a.e. $G_{k\text{-out}}$ is k-connected.*

Unlike in the case of regular graphs, Theorem 7.35 does not imply that a.e. $G_{k\text{-out}}$ has $\lfloor n/2 \rfloor$ independent edges. Nevertheless, this is true, only one has to work to prove it. Shamir and Upfal (1982) proved that a.e. $G_{6\text{-out}}$ has $\lfloor n/2 \rfloor$ independent edges, and Frieze (1985*c*) extended this to the following best possible result.

Theorem 7.36 *For $k \geq 2$, a.e. $G_{k\text{-out}}$ has $\lfloor n/2 \rfloor$ independent edges. In Chapter 8 we shall see considerably stronger results about $\mathcal{G}_{k\text{-out}}$.*

Exercises

7.1 Let $0 < p < 1$ be fixed and set $P_n = P(G_p$ is connected). By considering the probability that the component containing vertex 1 has k vertices, prove that

$$1 - P_n = \sum_{k=1}^{n-1} \binom{n-1}{k-1} P_k q^{k(n-k)}. \tag{E7.1}$$

(Gilbert, 1959.)

7.2 Let $0 < p < 1$ be fixed and set $R_n = P$ (vertices 1 and 2 belong to the same component of G_p). As in Ex. 1, prove that

$$R_n = 1 - \sum_{k=1}^{n-1} \binom{n-2}{k-1} P_k q^{k(n-k)} = \sum_{k=2}^{n} \binom{n-2}{k-2} P_k q^{k(n-k)}.$$

(Gilbert, 1959.)

7.3 Prove that if $p_{ij} = (\log n + c_{ij})/n$ and $\max |c_{ij}| = O(1)$, then Kovalenko's condition (7.6) is satisfied.

7.4 Use Lemma 8 to prove that

$$\tau\{\kappa(B) \geq 1; \widetilde{B}\} = \tau\{\delta(B) \geq 1; \widetilde{B}\}$$

for a.e. random bipartite graph process $\widetilde{B}$.

7.5 Deduce from Ex. 4 that if $c \in \mathbb{R}$ and $M = (n/2)\{\log n + c + o(1)\} \in \mathbb{N}$, then the probability that an element of $\mathcal{G}\{K(n,n), M\}$ is connected tends to $e^{-2e^{-c}}$. (Palásti (1963, 1968.)

7.6 Prove the following analogue of Theorem 7.3 and the result in Ex. 5. Let $c \in \mathbb{R}$ and $M = n\{\log n + c + o(1)\}$. Deduce from Ex. 5 that the probability that a random *directed* graph with n labelled vertices and M arcs (directed edges) is strongly connected (i.e. for any pair of vertices there is a directed path from the first to the second) tends to $e^{-2e^{-c}}$. (Palásti (1966.)

7.7 Let $c \in \mathbb{R}$ and $1 \leq np \leq \log n + 2 \log\log n + c$. Show that there is an $\varepsilon(c) > 0$ such that for $n \geq 6$ the probability that G_p contains two distinct vertices, each of which has two neighbours of degree 1, is at least $\varepsilon(c)$.

7.8 Show that if $\varepsilon > 0$ is fixed and $M/n \to \infty$, then almost no G_M contains $\lfloor \varepsilon n \rfloor$ independent vertices.

(*Hint*: simply write down the expected number of $\lfloor \varepsilon n \rfloor$-sets of independent vertices.)

7.9 Prove the theorem of de la Vega (1982) about independent edges in an r-graph by showing that the greedy algorithm is likely to produce $\{1 + o(1)\}(n/r)$ independent edges. Let $\mathscr{G}^{(r)}(n, p)$ be the space of r-graphs with probability p of a hyperedge. Suppose $p = \omega(n)n^{-r+1}$, where $\omega(n) \to \infty$. Construct sets $V_0 = V \supset V_1 \supset \ldots \supset V_{\lfloor n/r \rfloor}$ as follows. Having constructed $V_i, 0 \le i < \lfloor n/r \rfloor$, set $x_i = \min V_i$ and try to find a hyperedge containing x_i and contained in V_i. If there is one, say $\alpha \in V_i^{(r)}$, set $V_{i+1} = V_i - \alpha$, otherwise set $V_{i+1} = V_i - \{x_i\}$. Note that if $m \ge r$ then

$$P(|V_{i+1}| = |V_i| - 1 \| V_i| = m) \le (1-p)^{\binom{m-1}{r-1}} \le \exp\{-\omega_1(n)(m/n)^{r-1}\},$$

where $\omega_1(n) \to \infty$. Deduce that the expected number of times $|V_{i+1}| = |V_i| - 1$ for $0 \le i < \lfloor n/r \rfloor$ is at most

$$\sum_{k=1}^{\lfloor n/r \rfloor} \exp\{-\omega_1(n)(k/n)^{r-1}\} = o(n),$$

so a.e. $G_p^{(r)} \in \mathscr{G}^{(r)}(n, p)$ is such that the greedy algorithm constructs $\{1 + o(1)\}(n/r)$ independent edges.

7.10 Fill in the details in the proof of Theorem 7.23.

7.11 Construct a sequence of connected graphs $H_3, H_4, \ldots$ with $|H_i| = i$, such that

$$f_{H_n}^{-1}\left(\frac{7}{8}\right) - f_{H_n}^{-1}\left(\frac{1}{8}\right) \ge (7^{1/3} - 1)/2$$

for every $n \ge 3$. (cf. Corollary 7.31.)

7.12 Prove that for every $\varepsilon > 0$ there is a constant $c > 0$ for which a.e. $G_{c/n}$ is such that any two sets of at least εn vertices are joined by an edge.

7.13 Let $r \ge 3$ and $c < 1/\{\log(r-1) + 1\}$. Prove that a.e. $G_{r-\text{reg}}$ is such that any $k \le c \log n$ vertices span at most k edges. Deduce that Theorem 7.32 holds with a_0 replaced by $\lfloor (c/4r) \log n \rfloor$. (In fact, it holds with $a_0 = \lfloor \{c/(r-1)\} \log n \rfloor$, but that needs a little more work.)

7.14 Prove that for $r \geq 3$ and $a_0 \geq 3$ there is an $\varepsilon = \varepsilon(r, a_0) > 0$ such that if n is sufficiently large, then with probability at least ε, a graph $G_{r-\mathrm{reg}}$ is such that with a and s as in Theorem 7.32, $s \geq (r-2)a + 2$ if $1 \leq a \leq a_0$ and $s \geq (r-2)a_0$ if $a > a_0$.

7.15 Prove that for $t \geq 3$ a.e. $G_{k-\mathrm{out}}$ is such that any t vertices span at most t edges. Deduce that for $a_0 \geq 2$ a.e. $G_{k-\mathrm{out}}$ is such that if $V = A \cup S \cup B, a = |A| \leq |B|, s = |S|$ and there is no $A - B$ edge then $s \geq (k-1)a$ for $2 \leq a \leq a_0$ and $s \geq (k-1)a_0$ for $a > a_0$. Show also that this holds for $a_0 = \lfloor c \log n \rfloor$ as well, where $c > 0$ is some constant.

7.16 Let $c \in \mathbb{R}$ and $M = M(n) = \lfloor (n/2)(\log n + c) \rfloor$ and set

$$a_n(s) = \binom{n}{s}\binom{N - s(n-s)}{M} \Big/ \binom{N}{M}.$$

Prove that there are $n_0(c)$ and $0 < b < 1$ such that if $n \geq n_0(c)$, then

$$a_n(s) \leq \mathrm{e}^{(3-c)s}/s!, \qquad \text{if } s \leq n/\log n,$$

and

$$a_n(s) \leq b^s, \qquad \text{if } n/\log n \leq s \leq n/2.$$

[Godehardt and Steinbach (1981), correcting an inequality claimed by Erdős and Rényi (1959), who applied it to prove that for $M = \lfloor (n/2)(\log n + c) \rfloor$ a.e. G_M consists of a giant component and isolated vertices (see Theorem 7.3).]

7.17 Let $x \in \mathbb{R}$ be fixed and $p = \frac{3}{2}\{\log n + \frac{1}{2}\log\log n + \frac{1}{2}\log\frac{3}{8} + x + o(1)\}^{1/2}/n^{1/2}$. Write X for the number of edges of G_p which are contained in no triangle. Prove that $X \xrightarrow{d} P(\mathrm{e}^{-x})$.

7.18 Call a graph G *locally connected* if for every vertex u the subgraph $G[\Gamma(u)]$ of G induced by the set of neighbours of u is connected. Show that for p as in Ex. 17, the probability that G_p is locally connected tends to $\mathrm{e}^{-\mathrm{e}^{-x}}$. (Erdős, Palmer and Robinson, 1983.)

8

Long Paths and Cycles

In what models of random graphs is it true that almost every graph is Hamiltonian? In particular, how large does $M(n)$ have to be to ensure that a.e. G_M is Hamiltonian? This is one of the important questions Erdős and Rényi (1961*a*) raised in their fundamental paper on the evolution of random graphs. After several preliminary results due to Palásti (1969*a*, *b*, 1971*a*, *b*), Perereplica (1970), Moon (1972*d*), Wright (1973*a*, 1974*b*, 1975*b*, 1977*b*), Komlós and Szemerédi (1975), a breakthrough was achieved by Pósa (1976) and Korshunov (1976). They proved that for some constant c almost every labelled graph with n vertices and at least $cn \log n$ edges is Hamiltonian. This result is essentially best possible since even almost sure connectedness needs more than $\frac{1}{2}n \log n$ edges. A great many extensions and improvements of the Korshunov–Pósa result above have been proved by D. Angluin and Valiant (1979), Korshunov (1977), Komlós and Szemerédi (1983), Shamir (1983, 1985), Bollobás (1983*a*, 1984*a*), Bollobás, Fenner and Frieze (1987), Bollobás and Frieze (1987) and Frieze (1985*b*).

Another basic problem concerns the maximal length of a path in $G_{c/n}$, where c is a constant. We know that for $c > 1$ a.e. $G_{c/n}$ contains a giant component—in fact a component of order $\{1 - t(c) + o(1)\}n$—but the results of Chapter 6 tell us nothing about the existence of long cycles. Erdős conjectured that if $f(c) = \sup\{\alpha : \text{a.e. } G_{c/n} \text{ contains a path of length at least } \alpha n\}$, then $f(c) > 0$ for $c > 1$ and $\lim_{c\to\infty} f(c) = 1$. This conjecture was proved by Ajtai, Komlós and Szemerédi (1981*a*) and, in a slightly weaker form, by de la Vega (1979). These results were improved greatly by Bollobás (1982*d*) and Bollobás, Fenner and Frieze (1984); finally Frieze (1986*d*) determined the correct speed of convergence $f(c) \to 1$.

The main reason why a random graph $G_{c/n}$ is unlikely to be Hamiltonian even if c is a very large constant is that most $G_{c/n}$ contain (many) vertices of degree 0 and 1. What happens if our model is such that every vertex has a reasonably large degree? Is a.e. $G_{k\text{-}out}$ Hamiltonian if k is sufficiently large? And $G_{r\text{-}reg}$? In this area the breakthrough is due to Fenner and Frieze (1983), who answered the first question in the affirmative. Subsequently the method of the proof was extended by Bollobás (1983a) and Fenner and Frieze (1984) to prove the analogous result about $G_{r\text{-}reg}$.

8.1 Long Paths in $G_{c/n}$—First Approach

Ajtai, Komlós and Szemerédi (1981a) proved that there is a function $\alpha : (1, \infty) \to (0, 1)$ such that $\lim_{c\to\infty} \alpha(c) = 1$ and a.e. $G_{c/n}$ contains a path of length at least $\alpha(c)n$. A little later, but independently, de la Vega (1979) (the dates of Hungarian publications can be peculiar!) proved the existence of such an α with domain $(4\log 2, \infty)$. Although de la Vega's theorem is slightly weaker than the result of Ajtai, Komlós and Szemerédi, we shall present it here in a slightly stronger form, for de la Vega's proof is particularly simple and elegant.

In the theorem below, the upper bound on θ is only for the sake of convenience so that a small error term can be hidden in our main term. We write θ instead of c to emphasize the fact that θ may be a slowly increasing function of n.

Theorem 8.1 *Let $0 < \theta = \theta(n) < \log n - 3\log\log n$ and $p = \theta/n$. Then a.e. G_p contains a path of length at least*

$$\left(1 - \frac{4\log 2}{\theta}\right) n.$$

Proof Set $r = p/2$ and consider the space $\mathcal{G}(n; r, r)$ of red–blue coloured multigraphs (see §1 of Chapter 2), in which the red edges are selected with probability r and the blue edges are selected with probability r. By forgetting the colours of the edges and replacing multiple edges by simple edges we obtain a random graph G_{p_0}, where $p_0 = 1 - (1 - r)^2 = p - p^2/4 < p$. Hence it suffices to show that a.e. $G \in \mathcal{G}(n; r, r)$ contains a long path. Before going into details, let us give an intuitive description of the proof.

The advantage of the model $\mathcal{G}(n; r, r)$ is that we have two chances of using independence: first when considering the red edges and then when considering the blue edges. We shall try to construct a long path in a beautifully straightforward fashion. We start with an arbitrary vertex and try to construct a long path by extending our path edge by edge, using only red edges. When we grind to a halt, we give the blue edges a try to help us out. If there is a blue edge which can be used to continue our path, we use it, and continue testing the graph for red edges. If at some stage we find that no blue edge goes to a new vertex either, we retrace our steps to the first vertex from which the blue edges have not yet been tried. If during this process our current path shrinks to a vertex which we can no longer leave, we start a new sequence of paths by picking a new initial vertex. As we shall see, with probability tending to 1 this algorithm does produce a long path.

Now let us give a formal definition of the algorithm. Given a random coloured graph $G \in \mathscr{G}(n;r,r)$ the algorithm constructs a sequence of triples (P_k, U_k, B_k), where P_k is a directed path (the *current path* after k steps), U_k is a set of vertices (the set of *untried* vertices) and B_k is the set of *blue* vertices (the set of vertices which have been tried for red edges). To start the algorithm, pick a vertex $x_0 \in V(G)$ and set $P_0 = x_0, U_0 = V - \{x_0\}$ and $B_0 = \emptyset$. Suppose we have constructed (P_k, U_k, B_k), where the directed path P_k has initial vertex x_k, terminal vertex y_k and the set U_k has u_k vertices. If $U_k = \emptyset$, we stop the algorithm; otherwise we distinguish three cases.

Case 1 $y_k \notin B_k$. *If there is a red $y_k - U_k$ edge, say $y_k y_{k+1}$, continue P_k to $y_{k+1} : P_{k+1} = x_k P_k y_k y_{k+1}$ and set $U_{k+1} = U_k - \{y_{k+1}\}, B_{k+1} = B_k$. If there is no red $y_k - U_k$ edge, colour y_k blue, that is set $P_{k+1} = P_k, U_{k+1} = U_k$ and $B_{k+1} = B_k \cup \{y_k\}$.*

Case 2 $y_k \in B_k$ *and* $V(P_k)/B_k \neq \emptyset$. *If there is a blue $y_k - U_k$ edge, say $y_k y_{k+1}$, continue P_k with this edge: $P_{k+1} = x_k P_k y_k y_{k+1}$ and set $U_{k+1} = U_k - \{y_{k+1}\}, B_{k+1} = B_k$. If there is no blue $y_k - U_k$ edge, y_{k+1} be the last vertex of P_k not in B_k, set $P_{k+1} = x_k P_k y_{k+1}$, recolour y_{k+1} blue: $B_{k+1} = B_k \cup \{y_{k+1}\}$ and set $U_{k+1} = U_k$.*

Case 3 $V(P_k) \subset B_k$. *With probability $(1-r)^{u_k}$ set $(P_{k+1}, U_{k+1}, B_{k+1}) = (P_k, U_k, B_k)$ and with probability $1-(1-r)^{u_k}$ look for a blue $y_k - U_k$ edge. If there is such an edge, continue P_k to y_{k+1} as in Case 2, otherwise restart the current path at an arbitrary vertex x_{k+1} of $U_k : P_{k+1} = x_{k+1}, U_{k+1}, = U_k - \{x_{k+1}\}, B_{k+1} = B_k$.*

Let $l(k)$ be the length of P_k and let $b_k = |B_k|$. By definition $n - u_0 + b_0 = 1$ and clearly

$$(n - u_{k+1}) + b_{k+1} \leq (n - u_k) + b_k + 1,$$

since in each case we increase at most one of $n - u_k$ and b_k, and by at most 1. (In fact, but for the 'idle' step in Case 3 we would have equality.) Hence

$$(n - u_k) + b_k \leq k + 1$$

for every k. Furthermore,

$$V - U_k - V(P_k) \subset B_k$$

so

$$\begin{aligned} l(k) &= |P_k| - 1 \geq n - u_k - b_k - 1 \geq n - u_k - \{k + 1 - (n - u_k)\} - 1 \\ &= 2(n - u_k) - k - 2. \end{aligned} \tag{8.1}$$

Thus it suffices to show that with probability tending to 1 the right-hand side of (8.1) is large for some k.

Let us show that the triples $P_k(G), U_k(G), B_k(G)$ form a Markov chain as G ranges over $\mathcal{G}(n; r, r)$. In fact, all we shall need is that $\{u_k(G)\}_{k=0}^{\infty}$ is a Markov chain.

Write $\mathcal{H}_k(G) = \{P_i(G), U_i(G), B_i(G), E_i(G)\}_{i=0}^{k}$, where $E_i(G)$ is the set of $y_i - U_i$ edges of the colour we have already tried to find in the graph G. [Briefly, $\mathcal{H}_k(G)$ is the entire history of the process up to time k.] At each step the algorithm tests some $y_k - U_k$ edges (red or blue) which have not been tested before, so the probability of failing to find such an edge at step k is precisely $(1 - r)^{u_k}$. Therefore

$$P\{u_{k+1}(G) = j | u_k(G) = j, \mathcal{H}_k(G) = \mathcal{H}\} = (1 - r)^{u_k} \tag{8.2}$$

for all k, j, and $\mathcal{H}$. Since $u_{k+1}(G)$ is $u_k(G)$ or $u_k(G) - 1$, the sequence $\{u_k(G)\}_{k=0}^{\infty}$ is a Markov chain, as claimed.

For $1 \leq i \leq n - 1$ set

$$X_i = \max\{k - l : u_k = u_l = i\}$$

so that $X_i + 1$ is the length of the sojourn of u_k in state i and

$$Y_j = \sum_{i=j+1}^{n-1} (X_i + 1)$$

is the hitting time of state j of u_k:

$$P(u_k \leq j) = P(Y_j \leq k). \tag{8.3}$$

This shows that with probability tending to 1 our algorithm does construct a long path provided for some pair (j, k) we have $P(Y_j \leq k) \to 1$ and $2j + k$ is fairly small.

By relation (8.2), $X_{n-1}, X_{n-2}, \ldots, X_1$ are independent geometric random variables with

$$E(X_i) = \frac{(1-r)^i}{1-(1-r)^i}$$

and

$$\sigma^2(X_i) = \frac{(1-r)^i}{\{1-(1-r)^i\}^2}$$

(see §1 and Ex. 3 of Chapter 1).

Set $j = \lceil (\log 2)/r \rceil$. Then $(1-r)^j \le e^{-rj} \le \frac{1}{2}$, so

$$\sigma^2(Y_j) = \sum_{i=j+1}^{n-1} \sigma^2(X_i) \le 2(n-j-1) < 2n.$$

Furthermore,

$$\begin{aligned} E(Y_j) &= \sum_{i=j+1}^{n-1} E(X_i+1) \le \sum_{i=j+1}^{n-1} 1/(1-e^{-ri}) \\ &\le \int_j^{n-1} (1-e^{-rx})^{-1} dx \le \frac{1}{r}\int_{\log 2}^{rn} (1-e^{-y})^{-1} dy \\ &= \frac{1}{r}\left[y - \sum_{m=1}^{\infty} \frac{1}{m} e^{-my} \right]_{\log 2}^{rn} = \frac{1}{r}\left\{ rn - \sum_{m=1}^{\infty} \frac{1}{m} e^{-mrn} \right\} < n - \frac{1}{r}e^{-rn}, \end{aligned}$$

since $\Sigma_{m=1}^{\infty}(1/m)2^{-m} = \log 2$.

Therefore by Chebyshev's inequality for $\omega(n) = \log\log\log n$, we have

$$P(Y_j < n - (1/r)e^{-rn} + \omega(n)n^{1/2}) \to 1.$$

Consequently, by (8.1) and (8.3) with probability tending to 1 our algorithm does find a path of length at least

$$\begin{aligned} &2\left(n - \left\lceil \frac{\log 2}{r} \right\rceil\right) - n + \frac{1}{r}e^{-rn} - \omega(n)n^{1/2} - 2 \\ &= n - 2\left\lceil \frac{\log 2}{r} \right\rceil + \frac{1}{r}e^{-rn} - \omega(n)n^{1/2} - 2 \\ &\ge n\left(1 - \frac{4\log 2}{\theta}\right). \end{aligned}$$ □

A rather attractive feature of the algorithm above is that the algorithm it is based on never reverses the direction of an edge with respect to the direction of the current path. Consequently de la Vega's proof implies the following result as well.

Theorem 8.2 *Let $\vec{G}_p$ be a random directed graph of order n with probability p of the edges. If $p = \theta(n)/n$ and $\theta(n) \leq \log n - 3\log\log n$, then a.e. $\vec{G}_p$ has a directed path of length at least $n\{1-(4\log 2)/\theta\}$.*

As the property of containing long paths is monotone, by theorem 2.2 Theorems 8.1 and 8.2 have the following immediate consequence. □

Theorem 8.3 *Let $M_1(n) \leq (n/2)(\log n - 3\log\log n)$ and $M_2(n) \leq n(\log n - 3\log\log n)$. Then a.e. G_{M_1} has a path of length at least $n-2(\log 2)n^2/M_1(n)$ and a.e. directed graph with $M_2(n)$ edges has a direct path of length at least $n-2(\log 2)n^2/M^2(n)$.* □

8.2 Hamilton Cycles—First Approach

The aim of this section is to determine the threshold function of a Hamilton cycle; the next result will be devoted to a considerably sharper result about the appearance of Hamilton cycles. Before stating the main result we prove a number of crucial lemmas.

The breakthrough by Pósa concerning Hamilton cycles was based on a very useful lemma. Let $P = x_0x_1\ldots x_h$ be a longest x_0-path (i.e. a longest path beginning in x_0). A *simple transform* P' of P is a path of the form $P' = x_0x_1\ldots x_ix_hx_{h-1}\ldots x_{i+1}$. Thus P' is obtained from P by adding an edge x_hx_i $(0 \leq i < h)$ and erasing x_ix_{i+1}. An x_0-path is a *transform of* P if it is obtained from P by a sequence of simple transformations. Let U be the set of endvertices of transforms of P and set

$$N = \{x_i : 0 \leq i \leq h-1, \{x_{i-1}, x_{i+1}\} \cup U \neq \emptyset\},$$

and

$$R = V(P) - U \cup N.$$

Thus U is the set of ultimate vertices, N is the set of neighbours and R is the rest of the vertex set of P.

We are now ready to state and prove Pósa's lemma.

Lemma 8.4 *The graph contains no $U-R$ edges.*

Proof Suppose $x \in U$ and $xy \in E(G)$. Let P_x be a transform of P ending in x. Since $xy \in E(G), P_x$ has a simple transform P_z ending in a vertex z which is a neighbour of y on P_x.

If $yz \in E(P)$, then $y \in N$. Otherwise an edge $yw \in E(P)$ had to be erased in one step of the sequence $P \to P' \to \ldots \to P_x$. When yw was erased for the first time, then one of y and w became an endvertex, so we have $\{y, w\} \subset U \cup N$. Hence $y \in U \cup N$. □

We shall need the following immediate consequence of Lemma 8.4.

Lemma 8.5 *Suppose h, $u \in \mathbb{N}, h \geq 2$, and a graph is such that its longest path has length h but it contains no cycle of length $h+1$. Suppose, furthermore, that for every set U with $|U| < u$ we have*

$$|U \cup \Gamma(U)| \geq 3|U|. \tag{8.4}$$

Then there are u distinct vertices $y_1, y_2, \ldots, y_u$ and u not necessarily distinct sets $Y_1, Y_2, \ldots, Y_u$ such that for $i = 1, 2, \ldots, u$ we have $y_i \notin Y_i, |Y_i| \geq u$ and the graph has no $y_i - Y_i$ edge. Furthermore, the addition of any of the $y_i - Y_i$ edges creates a cycle of length $h + 1$. In particular, there are at least $u(u + 1)/2$ non-edges such that if any one of them is turned into an edge, the new graph contains an $(h + 1)$-cycle.

Proof Let $P = x_0, x_1, \ldots, x_h$ be a longest path and let U, N and R be as in Lemma 8.4. Then every $x_0 - U$ edge creates a cycle of length $h + 1$ and

$$U \cup \Gamma(U) \subset U \cup N = U \cup \{x_{h-1}\} \bigcup_{\substack{x_j \in U \\ j<l}} \{x_{j-1}, x_{j+1}\}$$

so

$$|U \cup \Gamma(U)| \leq 3|U| - 1.$$

Consequently, by relation (8.4) we have $|U| \geq u$, say

$$\{y_1, y_2, \ldots, y_u\} \subset U.$$

For each y_i there is a y_i-path P_i of maximal length h, which is a transform of P. Viewing P_i as a y_i-path, let Y_i be the set of endvertices of transforms of P_i. As before, $|Y_i| \geq u$ for every $i, 1 \leq i \leq h$, no edge joins y_i to Y_i and if we join y_i to any of the vertices in Y_i, then we create a cycle of length $h + 1$. Since for $i \neq j$ we have

$$|\{y_i y : y \in Y_i\} \cap \{y_j y : y \in Y_j\}| \leq 1,$$

the last assertion of the lemma follows. □

Another immediate consequence of Lemma 8.4 concerns long paths in graphs; although this result is not needed in this chapter, we present it for future reference.

Lemma 8.6 *Suppose $u \in \mathbb{N}$ is such that for every set $U \subset V(G), |U| \leq u$, we have*

$$|U \cup \Gamma(U)| \geq 3|U|.$$

Then G contains a path of length at least $3u-1$.

Proof Let $P = x_0 x_1 \ldots x_l$ be a longest path in G and let U, N and R be as in Lemma 8.4. By Lemma 8.4, G contains no $U - R$ edges, so $\Gamma(U) \subset U \cup N$, implying

$$|U \cup \Gamma(U)| \leq 3|U| - 1.$$

This shows that $|U| > u$. Let $U_0 \subset U, |U_0| = u$. Then by assumption

$$l \geq |U_0 \cup \Gamma(U_0)| \geq 3u,$$

as claimed. □

Let us continue our preparations for the result concerning Hamilton cycles in random graphs. Our next aim is to show that condition (8.4) of Lemma 5 is likely to be satisfied by certain random graphs.

Lemma 8.7 *(i) Let $p = \log n/n, 0 < \delta < 1/\gamma < \frac{1}{2}, u_0 = \lfloor (\log n)^\gamma \rfloor$ and $u_1 = \lceil \delta n \rceil$. Then a.e. G_p is such that if $U \subset V(G_p)$ and $u_0 \leq |U| \leq u_1$, then*

$$|U \cup \Gamma(U)| \geq \gamma |U|.$$

(ii) Let $p = O(\log n/n), c > 1$ and $l_0 = o(n(\log n)^{c/(1-c)})$. Then a.e. G_p is such that for every $l \leq l_0$ a set of l vertices spans at most cl edges.

Proof (*i*) Let $E(u, w)$ be the expected number of pairs (U, W) such that $U, W \subset V(G_p), U \cap W = \emptyset, |U| = u \geq 1, |W| = w \geq 1$ and

$$\Gamma(U) \backslash U = W.$$

Then clearly

$$\begin{aligned} E(u,w) &= \binom{n}{u}\binom{n-u}{w}(1-p)^{u(n-u-w)}\{1-(1-p)^u\}^w \\ &\leq n^{u+w}\left(\frac{e}{u}\right)^u\left(\frac{e}{w}\right)^w n^{-u\{1-(u+w)/n\}}(pu)^w \\ &= (\log n)^w\left(\frac{e}{u}\right)^u\left(\frac{eu}{w}\right)^w n^{u(u+w)/n} \end{aligned}$$

since

$$1-(1-p)^u \leq pu.$$

Consequently, the probability that a G_p does not have the required properties is at most

$$\sum_{u=u_0-1}^{u_1} \sum_{w=1}^{\lfloor(\gamma-1)u\rfloor} (\log n)^w \left(\frac{e}{u}\right)^u \left(\frac{eu}{w}\right)^w n^{\gamma u^2/n}$$

$$\leq \sum_{u=u_0-1}^{u_1} \gamma u(\log n)^(\gamma - 1)u \left(\frac{e}{u}\right)^u e^{(\gamma-1)u} n^{\gamma u^2/n}$$

$$= \gamma \sum_{u=u_0-1}^{u_1} (e^\gamma (\log n)^{\gamma-1} n^{\gamma u/n})^u u^{-u+1} = o(1).$$

(*ii*) For $l \leq l_0$ and $m \geq cl$ there are

$$\binom{\binom{l}{2}}{m} \leq \left(\frac{el}{2c}\right)^m$$

labelled graphs of order l and size m. Since

$$\sum_{m=\lceil cl\rceil}^{\infty} \left(\frac{el}{2c}\right)^m p^m < 2(elp)^{cl},$$

the probability that G_p does not have the required property is at most

$$2\sum_{l=4}^{l_0} \binom{n}{l} (elp)^{cl} < \sum_{l=4}^{l_0} (e^{c+1} l^{c-1} np^c)^l = o(1). \qquad \square$$

Lemma 8.8 *Let $\omega(n) \to \infty$ and $p = (1/n)\{\log n + \log\log n + \omega(n)\}$. Then a.e. G_p is such that if $U \subset V(G_p)$ and $|U| \leq \frac{1}{4}n$, then*

$$|U \cup \Gamma(U)| \geq 3|U|. \tag{8.5}$$

Proof By applying Lemma 8.7 with $\delta = \frac{1}{4}$ and $\gamma = 3$, we see that it suffices to show that a.e. G_p satisfies the condition provided $|U| \leq u_0 = \lfloor(\log n)^3\rfloor$. Furthermore, $\delta(G_p) \geq 2$ for a.e. G_p, so the condition is satisfied if $|U| = 1$. It is also easy to see that almost no G_p has two adjacent vertices of degree 2 [cf. Lemma 8.10(iv)].

Suppose now that $\delta(G_p) \geq 2$, no two vertices of degree 2 are adjacent and (8.5) fails for some set U where $|U| \leq u_0$. Let U be a minimal set for which (8.5) fails. Set $T = U \cup \Gamma(U)$ and $t = |T|$. Then $4 \leq t \leq 3u_0, G_p[T]$ is connected and some $\lceil t/3\rceil$ of its vertices are joined to vertices only in T. By Corollary 5.19 there are at most $ct^{t+(3k-1)/2}$ connected graphs with t given vertices and $t+k$ edges, so the probability that there is an appropriate set T is at most

$$c\binom{n}{t}\sum_{k=-1}^{t^*} t^{t+(3k-1)/2}p^{t+k}\binom{t}{\lceil t/3\rceil}(1-p)^{(n-t)\lceil t/3\rceil},$$

where $t^* = \binom{t}{2} - t$. Clearly this probability is at most

$$cn^t e^t\left(\frac{2\log n}{n}\right)^{t-1} 2^t n^{-\lceil t/3\rceil} \leq cn^{1-\lceil t/3\rceil}(12\log n)^t.$$

Since

$$\sum_{t=4}^{3u_0} n^{1-\lceil t/3\rceil}(12\log n)^t = o(1),$$

the lemma follows. $\square$

We are now ready to determine the threshold function of a Hamilton cycle. If G is Hamiltonian, then $\delta(G) \geq 2$ so

$$P(G_M \text{ is Hamiltonian}) \leq P\{\delta(G_M) \geq 2\}.$$

Since $P\{\delta(G_M) \geq 2\} \to 1$ iff $\omega(n) = 2M/n - \log n - \log\log n \to \infty$ (see Theorem 3.5), if a.e. G_M is Hamiltonian we must have $\omega(n) \to \infty$. Komlós and Szemerédi (1983) and Korshunov (1977) were the first to show that this rather trivial necessary condition is also sufficient to ensure that a.e. G_M is Hamiltonian. The proof we present is from Bollobás (1983*a*).

Theorem 8.9 *Let* $\omega(n) \to \infty, p = (1/n)\{\log n + \log\log n + \omega(n)\}$ *and* $M(n) = \lfloor (n/2)\{\log n + \log\log n + \omega(n)\}\rfloor$. *Then a.e.* G_p *is Hamiltonian and a.e.* G_M *is Hamiltonian.*

Proof Since the property of being Hamiltonian is monotone, it suffices to prove the assertion concerning G_p.

Set $k = \lfloor 4n/\log n\rfloor, p_i = 64\log n/n^2, 1 \leq i \leq k$, and $p_0 = p - kp_1 = p - (64\log n/n^2)k$. Consider the spaces $\mathcal{G}_j = \mathcal{G}_c(n; p_0, p_1, \ldots, p_j)$ of coloured multigraphs whose edges are chosen independently, with those of colour i having probability p_i. If we replace multiple edges by simple edges and forget the colours, then $\mathcal{G}_j$ is naturally identified with $\mathcal{G}(n; p'_j)$, where $p'_j \leq p_0 + jp_1$. Clearly, $\mathcal{G}_0$ is just the space $\mathcal{G}(n; p_0)$. Since $p'_k \leq p_0 + kp_1 = p$, it suffices to show that a.e. graph in $\mathcal{G}_k$ is Hamiltonian. This will be done by first showing that for $0 \le j < k$ an element of $\mathscr{G}_j$ contains a long path with probability $1 - o(1)$.

For $G_k \in \mathscr{G}_k$ and $0 \le j \le k$ let G_j be the subgraph of G_k formed by the edges of colours $0, 1, \dots, j$. Then $G_k \to G_j$ defines a measure-preserving map of $\mathscr{G}_k$ into $\mathscr{G}_j$. Conversely, a random element of $\mathscr{G}_j$ is obtained from a random element of $\mathscr{G}_{j-1}$ by adding edges of colour j with probability $p_j = p_1$.

Given a non-Hamiltonian graph G of order n, let $l(G)$ be the maximal length of a path in G; if G is Hamiltonian, set $l(G) = n$. Furthermore, let Q be the property that G is connected and if $U \subset V(G)$ and $|U| \le n/4$,

$$|U \cup \Gamma(U)| \ge 3|U|.$$

Our earlier remarks about $\mathscr{G}_j$ imply that our theorem follows if we show that

$$P_0 = P\{l(G_0) \ge n - k \text{ and } G_0 \text{ has } Q\} = 1 - o(1) \tag{8.6}$$

and

$$P_j = P\{l(G_j) = n-k+j-1 | l(G_{j-1}) = n-k+j-1 \text{ and } G_{j-1} \text{ has } Q\} \le n^{-2} \tag{8.7}$$

for $j = 1, 2, \dots, k$. Indeed, if (8.6) and (8.7) hold, then

$$P\{l(G_k) < n\} \le 1 - P_0 - \sum_{j=1}^{k} P_j = o(1).$$

Since $p_0 \ge (1/n)\{\log n + \log\log n + \frac{1}{2}\omega(n)\}$, by Theorem 7.1 a.e. G_0 is connected, so by Lemma 8.8 a.e. G_0 has Q. By Theorem 8.1 a.e. G_0 is such that $l(G_0) \ge n\{1 - (4\log 2)/(\log n - 3\log\log n)\} > n - k$ so (8.6) does hold. Suppose now that $n > h = l(G_{j-1}) \ge n - k + j - 1$ and G_{j-1} has Q. By Lemma 8.5 the graph G_{j-1} has at least $n^2/32$ pairs of vertices such that if any of them is added to G_{j-1}, the resulting graph G'_{j-1} has a cycle of length $h + 1$. Since G_{j-1} is connected, this implies that $l(G'_{j-1}) \ge h + 1$. Consequently

$$\begin{aligned} P\{l(G_j) &= n - k + j - 1 | l(G_{j-1}) = n - k + j - 1 \text{ and } G_{j-1} \text{ has } Q\} \\ &\le (1 - p_1)^{n^2/32} \le n^{-2}, \end{aligned}$$

as required. □

The reader is justified in wondering why we chose such a tortuous road to the theorem above. Could we not have proved the result by using Chebyshev's inequality? The answer is an emphatic no: the number of

Hamilton cycles in G_M tends to have very large variance and so from Chebyshev's inequality we cannot even conclude that $\underline{\lim}_{n\to\infty} P\{G_{n,\lfloor \log n\rfloor}$ is Hamiltonian$\} > 0$. Note also that for $c > \mathrm{e}$ the expected number of Hamilton cycles is $G_{c/n}$ tends to infinity but a.e. graph contains many isolated vertices and so a.e. $G_{c/n}$ is non-Hamiltonian (see Exx. 1 and 2).

8.3 Hamilton Cycles—Second Approach

Since the minimum degree of a Hamiltonian graph is at least 2, the hitting time of being Hamiltonian is at least as large as the hitting time of having minimum degree at least 2. The main aim of this section is to show that, in fact, equality holds for a.e. graph process: with probability tending to 1, the very edge which increases the minimum degree to 2 also makes the graph Hamiltonian. This assertion was conjectured by Erdős and Spencer and was also stated, without any indication of a proof, by Komlós and Szemerédi (1983). The result was first proved by Bollobás (1984*a*); this is the proof we shall reproduce here.

Similarly to the proof of Theorem 7.11, we shall rely on Lemma 7.9 concerning the model $\mathscr{G}(n, M; \geq 2)$. The relevant properties of a random element of $\mathscr{G}(n, M; \geq 2)$ are collected in the lemma below. We denote by $\mathscr{G}_c(n, M; \geq 2)$ the space of blue–green coloured graphs used in the construction of $\mathscr{G}(n, M; \geq 2)$ and by G_c a random element of this space.

Lemma 8.10 *Let* $M(n) = (n/2)\{\log n + \log\log n - \alpha(n)\} \in \mathbb{N}, \alpha(n) \to \infty, \alpha(n) = o(\log\log\log n)$ *and let* $k \geq 1$ *be fixed. Then a.e. graph* $G_c \in \mathscr{G}_c(n; M, \geq 2)$ *is such that*

(*i*) $\delta(G_c) = 2, \Delta(G_c) \leq 3\log n$ *and* G_c *is connected,*

(*ii*) *the graph* G_c *has at most* $g_0 = \lfloor \log\log n\rfloor$ *green edges and the green edges are independent,*

(*iii*) *there are* $o\{n/(\log n)\}$ *vertices of degree at most* $\frac{1}{2}\log n$*, and there are at most* n *edges incident with these vertices,*

(*iv*) *no two vertices of degree at most* $\frac{1}{10}\log n$ *are within distance* k *of each other,*

(*v*) *no cycle of length at most* k *contains a vertex of degree at most* $\frac{1}{10}\log n$*,*

(*vi*) *for* $(\log n)^4 \leq s \leq n/4$*, every set* S *of* s *vertices has at least* $3s$ *neighbours which do not belong to* S*,*

(*vii*) *for* $l \leq n(\log n)^{-3}$*, every set of* l *vertices spans at most* $2l$ *edges.*

Proof a.e. G_M is connected and has at most $\log\log n$ vertices of degree 1 implying assertions (i) and (ii). To prove (iii) it suffices to show that in $G_p, p = M/N$, the expected number of vertices of degree at most $d_0 = \lfloor \frac{1}{2}\log n \rfloor$ is $o(n/\log n)$:

$$n\sum_{d=0}^{d_0}\binom{n-1}{d}p^d(1-p)^{n-1-d} \le \sum_{d=1}^{d_0}\left(\frac{\mathrm{e}np}{d}\right)^d n^{-1}+1 = o(n^{0.9}).$$

What is the expected number of pairs of vertices of degree at most $d_1 = \lfloor \frac{1}{10}\log n \rfloor$ within distance k of each other in a graph G_M? It is at most

$$\begin{aligned}
&\sum_{l=1}^{k} n^{l+1}\sum_{d=0}^{2d_1}\binom{2n}{d}\binom{N-2n+3}{M-l-d}\Big/\binom{N}{M}\\
&\le 2\sum_{l=1}^{k} n^{l+1}\binom{2n}{2d_1}\binom{N-2n}{M-l-2d_1}\Big/\binom{N}{M}\\
&\le 3n^{k+1}\binom{2n}{2d_1}\binom{N-2n}{M-k-2d_1}\Big/\binom{N}{M}\\
&= 3n^{k+1}\binom{2n}{2d_1}\frac{(N-M)_{2n-2d_1-k}(M)_{2d_1+k}}{(N)_{2n}}\\
&\le 4n^{k+1}\left(\frac{\mathrm{e}n}{d_1}\right)^{2d_1}\mathrm{e}^{-2nM/N}\left(\frac{M}{N}\right)^{2d_1+k}\\
&\le n^{k+1}28^{(\log n)/5}n^{-2}\left(\frac{\log n}{n}\right)^k = o(n^{2/3}).
\end{aligned}$$

Hence a.e. G_M is such that the balls of radius k about its vertices of degree at most $\frac{1}{10}\log n$ are disjoint and contain $o(n^{3/4})$ vertices. Therefore the probability that the other endvertex of a green edge belongs to such a ball is $o(n^{-1/4})$. Since a.e. G_c has at most g_0 green edges, (iv) follows.

A slight variant of the argument above shows (v).

Assertion (vi) is immediate from Lemma 8.7(i).

Finally, Lemma 8.7(ii) implies that a.e. G_M is such that any set of $l \le n(\log n)^{-3}$ vertices spans at most $2l$ edges. Since the green edges are independent in almost every G_c, assertion (vii) follows. □

Theorem 8.11 *A.e. graph process $\widetilde{G}$ is such that*

$$\tau(\widetilde{G}; \underline{\mathrm{Ham}}) = \tau(\widetilde{G}; \delta \ge 2).$$

Proof Let $M = M(n) = (n/2)\{\log n + \log\log n - \alpha(c)\} \in \mathbb{N}$, where

$\alpha(n) \to \infty$ and $\alpha(n) = o(\log \log n)$. By Lemma 7.9 it suffices to show that a.e. $G_c \in \mathscr{G}_c(n, M; \geq 2)$ is Hamiltonian. Suppose this is not so, say

$$\overline{\lim_{n\to\infty}}\, P_c(G_c \text{ is not Hamiltonian}) = 2\alpha > 0. \tag{8.8}$$

Set $\mathscr{F}_c = \mathscr{F}_c(n) = \{G_c \in \mathscr{G}(n, M; \geq 2) : G_c$ is not Hamiltonian and satisfies the conclusions of Lemma 8.10 with $k = 4\}$. Then by (8.8) there is an infinite set $\Lambda \subset \mathscr{N}$ such that

$$P_c\{\mathscr{F}_c(n)\} \geq \alpha \text{ if } n \in \Lambda. \tag{8.9}$$

In addition to Lemma 7.9, the proof is based on the colouring method due to Fenner and Frieze (1983). Given $G \in \mathscr{F}_c(n)$, write $L(G)$ for a longest path in G. Recolour $R = \lfloor (\log n)^2 \rfloor$ of the blue edges of G red in such a way that

(a) no edge of $L(G)$ is red,
(b) each endvertex of a red edge has degree at least $\frac{1}{10}\log n$ and
(c) the R red edges are independent.

Call the blue–green–red coloured graph arising in this way a *coloured pattern*, or simply *pattern*, and write $F(n)$ for the total number of patterns arising from graphs in $\mathscr{F}_c(n)$. Our aim is to arrive at a contradiction by proving contradictory bounds for $F(n)$.

Let us give a lower bound for $F(n)$. At least how many patterns do we obtain from a graph $G \in \mathscr{F}_c(n)$? Denote by M_0 the number of edges of G which must not be coloured red because of (a) and (b). As $L(G)$ has at most $n-1$ edges and by Lemma 8.10(iii) there are at most n blue edges incident with vertices of degree at most $\frac{1}{2}\log n$, we have $M_0 < 2n$. What is the probability that one of the $\binom{M-M_0}{R}$ colourings satisfying (a) and (b) violates (c)? It is at most the expected number of pairs of adjacent red edges so at most

$$n\binom{3\log n}{2}\binom{M-M_0-2}{R-2}\binom{M-M_0}{R}^{-2} = O\{n(\log n)^2 R^2 M^{-2}\} = o(1),$$

since $\Delta(G) \leq 3\log n$. Hence if $n \in \Gamma$ is sufficiently large, each $G \in \mathscr{F}_c(n)$ gives rise to at least $\frac{1}{2}\binom{M-2n}{R}$ coloured patterns. Consequently, if $n \in \Gamma$ is sufficiently large, then

$$F(n) \geq \frac{\alpha}{4}\binom{N}{M}\binom{M-2n}{R}. \tag{8.10}$$

Our next aim is to give an upper bound for $F(n)$. Let B be the blue-green subgraph of G obtained after the omission of the red edges of a pattern constructed from G. We claim that B satisfies the conditions of Lemma 8.5 with $u = \lfloor n/4 \rfloor$, i.e. if $|S| < u = \lfloor n/4 \rfloor$, then

$$|S \cup \Gamma_B(S)| \geq 3|S|. \tag{8.11}$$

This is immediate if $|S| \geq (\log n)^4$, for then, by Lemma 8.10(vi) and condition (c) on the choice of the red edges,

$$|S \cup \Gamma_B(S)| \geq |S \cup \Gamma_G(S)| - |S| \geq 3|S|.$$

Suppose now that $|S| < (\log n)^4$ and

$$|S \cup \Gamma_B(S)| < 3|S|. \tag{8.12}$$

Set

$$S_1 = \{x \in S : d_G(x) \leq \tfrac{1}{10} \log n\}, S_2 = S - S_1.$$

Since for $x \in S_1$ we have $\Gamma_B(x) = \Gamma_G(x)$ and in G no two vertices of S_1 are within distance 4 of each other,

$$|S_1 \cup \Gamma_B(S_1)| = |S_1 \cup \Gamma_G(S_1)| = \sum_{x \in S_1} \{d_G(x) + 1\} \geq 3|S_1|. \tag{8.13}$$

Furthermore, by Lemma 8.10 (iv) and (v) every vertex is joined to at most one vertex in $S_1 \cup \Gamma_G(S_1)$, so (8.12) and (8.13) give

$$\begin{aligned} |S_2 \cup \Gamma_G(S_2)| &\leq |S_2 \cup \Gamma_B(S_2)| + |S_2| \\ &\leq |S_2 \cup \{\Gamma_B(S_2) \backslash (S_1 \cup \Gamma_B(S_1))\}| + 2|S_2| < 5|S_2|. \end{aligned}$$

This shows that the set $T = S_2 \cup \Gamma_G(S_2)$ of at most $5(\log n)^4$ vertices spans at least $\frac{1}{2}|T|\frac{1}{10}\log n > 10|T|$ edges, contradicting Lemma 8.7(vii). This completes the proof of (8.11).

At most how many graphs $G \in \mathscr{F}_c(n)$ give rise to the same blue–green graph B? Since every graph $G \in \mathscr{F}_c(n)$ is connected and non-Hamiltonian, (8.11) and Lemma 8.5 with $u = \lceil n/4 \rceil$ imply that for every B there are $\lfloor n^2/32 \rfloor$ pairs of vertices which cannot be joined by red edges. Hence each blue–green graph belongs to at most

$$\binom{N - \lfloor n^2/32 \rfloor}{R}$$

graphs $G \in \mathscr{F}_c(n)$. How many choices do we have for B? Rather crudely, at most

$$\binom{N}{M - R} n^{2g_0}.$$

Consequently, if $n \in \Lambda$ is sufficiently large, then

$$F(n) \le \binom{N - \lfloor n^2/32 \rfloor}{R} \binom{N}{M - R} n^{2g_0}. \tag{8.14}$$

The proof of our theorem is complete since inequalities (8.10) and (8.14) lead to the following contradiction:

$$\begin{aligned} 1 &\le \frac{4}{\alpha} \binom{N - \lceil n^2/32 \rceil}{R} \binom{N}{M-R} n^{2g_0} \binom{N}{M}^{-1} \binom{M-2n}{R}^{-1} \\ &\le \frac{4}{\alpha} n^{2g_0} \left(\frac{16}{17}\right)^R \binom{M}{R} \binom{M-2n}{R} \\ &\le \frac{4}{\alpha} n^{2g_0} \left(\frac{16}{17}\right)^R \left(1 - \frac{3n}{M}\right)^{-R} = o(1). \end{aligned}$$

□

Theorem 8.11 implies the following extension of Theorem 8.9.

Corollary 8.12 *Set $\omega(n) = 2M(n)/n - \log n -$ log log$n$. Then a.e. G_M is Hamiltonian iff $\omega(n) \to \infty$, and a.e. G_M is non-Hamiltonian iff $\omega(n) \to -\infty$.* □

All the proofs above are non-algorithmic, so it is natural to ask for a polynomial time algorithm which, with probability tending to 1, finds a Hamilton cycle in $G_{n,M(n)}$ if $M(n)$ is not too small. Needless to say, one would like an algorithm which works for $M(n) \ge (n/2)\{\log n + \log \log n + \omega(n)\}, \omega(n) \to \infty$. The first polynomial algorithm was given by d. Angluin and Valiant (1979), for $M(n) \ge cn \log n$; this result was improved by Shamir (1983) whose algorithm worked for $M(n) \ge (n/2)\{\log n + (4 + \varepsilon)\log \log n\}, \varepsilon > 0$. Finally, Bollobás, Fenner and Frieze (1986) constructed an algorithm, say HAM, which is essentially best possible.

Theorem 8.13 *(i) For $M(n) = (n/2)(\log n +$ log log$n + c_n)$*

$$\lim_{n\to\infty} P(\textit{HAM finds a Hamilton cycle in } G_{n,M}) = \begin{cases} 0, & \textit{if } c_n \to -\infty, \\ e^{-e^{-c}}, & \textit{if } c_n \to c, \\ 1, & \textit{if } c_n \to \infty. \end{cases}$$

(ii) For $\varepsilon > 0$, HAM runs in $o(n^{4+\varepsilon})$ time. □

Algorithm *HAM* runs simply by extending a current path at each end and when no extension exists, taking a simple transform, whenever possible. It turns out that the probability of failure is so small that one can apply dynamic programming (see Held and Karp, 1962) to obtain an algorithm which solves the Hamilton cycle problem in polynomial expected running time in the space $\mathscr{G}(n, \frac{1}{2})$.

In fact, for spaces of dense graphs like $\mathscr{G}(n, \frac{1}{2})$, there are several Hamilton cycle algorithms with very fast expected running times. Improving an algorithm proposed by gurovich and Shelah (1987), Thomason (1989*a*) constructed on algorithm for finding a Hamilton path between two specified vertices if one exists or proving its non-existence. This algorithm is made up of two fast greedy algorithms; for some constant $c > 0$, it needs cn storage and its expected running time over $\mathscr{G}(n,p)$ is at most cn/p, provided $p \geq 12n^{-1/3}$. Frieze (1987) parallelized the algorithms of Thomason (1989*a*) and Gurevich and Shelah (1987).

Counting the exact number of Hamilton cycles in dense graphs and digraphs is #P-complete; however, Frieze and Suen (1992) gave a fully polynomial randomized approximation scheme for estimating the number of Hamilton cycles in a random digraph D_M provided $M^2/n^3 \to \infty$. Also, Dyer, Frieze and Jerrum (1998) gave a similar algorithm for graphs of order n and minimal degree at least $\left(\frac{1}{2} + \alpha\right) n$, where $\alpha > 0$ is any positive constant.

It is not unreasonable to expect that the problem of finding Hamilton cycles in random bipartite graphs is easier than the problem in $\mathscr{G}(n,p)$. Surprisingly, this does not seem to be true, although Frieze (1985*b*) did manage to determine the exact probability distribution: for $p = (\log n + \log\log n + c_n)/n$ the probability that a random bipartite graph $G \in \mathscr{G}(n,n;p)$ is Hamiltonian, tends to $e^{-2e^{-c}}$ as $c_n \to c$, the obstruction being, once again, the existence of a vertex of degree 1.

Although we are mainly concerned with random graphs, it would be strange not to mention a beautiful result about random digraphs. What is the threshold function for a Hamilton cycle in a random directed graph (digraph)? This problem seems harder than the corresponding problem for graphs, since we cannot use transforms of cycles and so we do not have an analogue of Pósa's lemma. Nevertheless, by an ingenious and elegant conditioning argument McDiarmid (1981, 1983b) proved that the probability that a random digraph $D_{n,p}$ is Hamiltonian is not smaller than the probability that $G_{n,p}$ is Hamiltonian and so deduced that if $P = (1+\varepsilon)(\log n)/n$, then

$$P(D_{n,p} \text{ is Hamiltonian}) \to \begin{cases} 1, & \text{if } \varepsilon > 0, \\ 0, & \text{if } \varepsilon < 0. \end{cases}$$

The second relation follows from the fact that for $\varepsilon < 0$ almost no $D_{n,p}$ is connected (see Ex. 6).

Theorem 8.11 tells us that the primary obstruction to a Hamilton cycle is the existence of a vertex of degree at most 1. Similarly, the primary obstruction to l edge-disjoint Hamilton cycles is the existence of a vertex of degree at most $2l-1$. Bollobás, Fenner and Frieze (1990) studied the secondary obstruction to these properties. More precisely, for $k \geq 1$ we say that a graph G has property $\mathscr{A}_k$, in notation, $G \in \mathscr{A}_k$, if G contains $\lfloor k/2 \rfloor$ edge-disjoint Hamilton cycles and, if k is odd, a matching with $\lfloor n/2 \rfloor$ edges. Thus, if n is even, $G \in \mathscr{A}_k$ iff G has a k-factor F which contains $\lfloor k/2 \rfloor$ edge-disjoint Hamilton cycles. To rule out the primary obstruction, we simply condition on the minimal degree being at least k, that is we consider the space $\mathscr{G}(n, M; \delta \geq k)$ of all graphs on $[n]$ with M edges and minimal degree at least k. (If $M < kn/2$ then this set is clearly empty). We write $G_{n,m;k}$ for a random element of $\mathscr{G}(n, M; \delta \geq k)$.

For $k \geq 2$, what is the main obstruction to $\mathscr{A}_k$ in $\mathscr{G}(n, M; \delta \geq k)$? As noted by Luczak (1987), *k-legged spiders* or simply *k-spiders* provide such an obstruction: $k+1$ vertices of degree k having a common neighbour.

Bollobo's, Fenner and Frieze (1990) proved that this is indeed the case and so, somewhat surprisingly, the threshold function for $\mathscr{A}_k$ in $\mathscr{G}(n, M; \delta \geq k)$ is *decreasing* with k. The proof of this result is rather involved, partly due to the fact that the random graphs $G_{n,M;k}$ are not too easy to generate in a form that is pleasant to study.

Theorem 8.14 *Let* $k \geq 2, d \in \mathbb{R}$ *and* $M = \frac{n}{2}\left(\frac{\log n}{k+1} + k \log\log n + d_n\right)$. *Then*

$$\lim_{n\to\infty} P\left(G_{n,M;k} \in \mathscr{A}_k\right) = \begin{cases} 0 & \textit{if } d_n \to -\infty, \textit{ sufficiently slowly}, \\ \mathrm{e}^{-\vartheta_k(d)} & \textit{if } d_n \to d, \\ 1 & \textit{if } d_n \to +\infty, \end{cases}$$

where

$$\vartheta_k(d) = \frac{\mathrm{e}^{-(k+1)d}}{(k+1)!\{(k-1)!\}^{k+1}(k+1)^{k(k+1)}}. \qquad \square$$

Note that if k is even or k is odd and n is even and v is a vertex of degree k in $\mathscr{G}(n, M; \delta \geq k)$ than all k edges incident with v appear in the $k/2$ Hamilton cycles: the configuration we look for 'fills' the edges at v. Bollobás, Cooper, Fenner and Frieze (2000) proved the somewhat surprising theorem that in $\mathscr{G}(n, M; \geq k)$ the threshold for $\mathscr{A}_{k-1}$ is considerably lower than for $\mathscr{A}_k$, in fact, the threshold is linear. Thus the little elbow room that at no vertex do we have to use all the edges guaranteed by our conditioning $\delta \geq k$ greatly lowers the threshold.

Theorem 8.15 *Let $k \geq 3$. Then there exists a constant $c_k \leq (k+1)^3$ such that if $\underline{\lim}_{n\to\infty} \inf M/n \geq c_k$ then a.e. $G_{n,M;k}$ has $\mathscr{A}_{k-1}$.*

The proof of this result is again rather complicated. The linearity of the threshold for $\mathscr{A}_{k-1}$ in $\mathscr{G}(n, M; \delta \geq k)$ contrasts sharply with the fact that in $\mathscr{G}(n, M)$ the threshold for $\mathscr{A}_{k-1}$ is about $\frac{1}{2}\log n$. □

8.4 Long Paths in $G_{c/n}$—Second Approach

How long a path can we find in a.e. $G_{c/n}$ for a large constant c? We saw in §1 that for $c > 1$ a.e. $G_{c/n}$ contains a path of length at least $c'n$, where $c' > 0$; furthermore, $c' \to 1$ as $c \to \infty$. Our aim in this section is to study the speed of the convergence $c' \to 1$. To this end, for $c > 0$ set

$$1 - \alpha(c) = \sup\{\alpha \geq 0 : \text{ a.e. } G_{c/n} \text{ contains a path of length } \geq \alpha n\}$$

and

$$1 - \beta(c) = \sup\{\beta \geq 0 : \text{ a.e. } G_{c/n} \text{ contains a cycle of length } \geq \beta n\}.$$

Clearly $\alpha(c) \geq \beta(c)$ and it is, in fact, likely that $\alpha(c) = \beta(c)$ for all $c > 0$. We shall not prove this but we shall give the same bounds for $\alpha(c)$ and $\beta(c)$.

At least how large does $\alpha(c)$ have to be? Since a.e. $G_{c/n}$ contains

$$\{1 + o(1)\}n\left(1 - \frac{c}{n}\right)^{n-1} = \{1 + o(1)\}e^{-c}n$$

isolated vertices and

$$\{1 + o(1)\}n^2\frac{c}{n}\left(1 - \frac{c}{n}\right)^{n-2} = \{1 + o(1)\}c\, e^{-c}n$$

vertices of degree 1, we have

$$\beta(c) \geq \alpha(c) \geq (c+1)e^{-c}. \tag{8.15}$$

This bound can be improved by taking into account that after the deletion of the vertices of degree 1, many more vertices of degree 1 will be created in a typical $G_{c/n}$, whose deletion results in a further batch of vertices of degree 1, etc., but we shall be content with (8.15).

Now let us turn to the upper bound on $\beta(c)$. We know from Theorem 1 that $\alpha(c) = O(1/c)$. Bollobás (1982*d*) was the first to show that $\beta(c)$ decays exponentially: $\beta(c) \leq c^{24}e^{-c/2}$ if c is sufficiently large. This bound was improved to an essentially best possible bound by Bollobás, Fenner and Frieze (1987).

Theorem 8.16 *There is a polynomial P of degree at most 6 such that a.e. $G_{c/n}$ contains a cycle of length at least $\{1 - P(c)e^{-c}\}n$: In particular,*

$$\beta(c) \leq P(c)e^{-c}.$$

We shall only give a brief sketch that $P(c) = c^6$ will suffice if c is sufficiently large. The first step is to find a large subgraph of a typical $G_{c/n}$ in which the degrees of the vertices are neither too large, nor too small. Given a r.g. $G_{c/n}$, define

$$U_0 = \{x \in V : d(x) \leq 6 \text{ or } d(x) \geq 4c\}$$

where $V = V(G_{c/n})$. Suppose we have constructed a nested sequence of subsets of $V : U_0 \subset U_1 \subset \ldots \subset U_j$. Set

$$U'_{j+1} = \{x \in V - U_j : |\Gamma(x) \cap U_j| \geq 2\}.$$

If $U'_{j+1} = \emptyset$, stop the sequence, otherwise put

$$U_{j+1} = U_j \cup U'_{j+1}.$$

Suppose the sequence stops with $U_s \neq V$. Let $H = H(G_{c/n})$ be the subgraph of $G_{c/n}$ spanned by $V - U_s$ and set $h = |H|$. Then every vertex of H has degree at least 6 and at most $4c$, since every vertex. $x \in V - U_s$ has degree at least 7 in G and is joined to at most one vertex of U_s.

The following lemma summarizes the salient properties of a typical $G_{c/n}$ and its subgraph H. The proof is left to the reader (Ex. 3).

Lemma 8.17 *Let $\varepsilon > 0$. If c is sufficiently large, then a.e. $G_{c/n}$ is such that*

(i) any $t \leq n/6c^3$ vertices of $G_{c/n}$ span at most $3t/2$ edges,
(ii) any $t \leq n/3$ vertices of $G_{c/n}$ span at most $ct/5$ edges,
(iii) $n - h < c^6e^{-c}n$,
(iv) the set $W = \{x : (1-\varepsilon)c < d_H(x) < (1+\varepsilon)c\}$ has at least $(1-c^{-4})h$ elements, and spans at least $(1-\varepsilon)ch/2$ edges and
(v) H has at most $(1+\varepsilon)ch/2$ edges.

Let us assume that the graph $H = H(G_{c/n})$ has vertex set $\{1, 2, \ldots, h\}$ and degree sequence $6 \leq d_1 \leq d_2 \leq \ldots \leq d_n \leq 4c$. Let $\mathscr{H} = \mathscr{H}(G_{c/n})$ be the set of all graphs with vertex set $\{1, 2, \ldots, h\}$ and degree sequence $(d_i)_1^n$. Turn $\mathscr{H}$ into a probability space by giving all members of $\mathscr{H}$ the same probability. Note that all members of $\mathscr{H}$ occur as $H = H(G_{c/n})$ with precisely the same probability since if $H_1, H_2 \in \mathscr{H}$ and F is such that $V(F) = \{1, 2, \ldots, n\}$, no edge of F joins two vertices of H_1 and

$H_1 = H(H_2 \cup F)$. Hence a.e. $G_{c/n}$ is such that a.e. element H of $\mathscr{H}(G_{c/n})$ satisfies the conclusions of Lemma 8.17.

In view of this, it suffices to show that for some $\varepsilon > 0$ and large enough c a.e. graph in $\mathscr{H}$ is Hamiltonian. The proof of this is based on the colouring argument due to Fenner and Frieze (1983), encountered in the previous section, and the model of random graphs with a fixed degree sequence, introduced by Bollobás (1980*b*) and discussed in §4 of Chapter 2.

The space $\mathscr{H}$ is rather close to the space of regular graphs (say c-regular graphs) so this assertion is rather close to Theorem 8.21, below, stating that for large enough r, a.e. r-regular graph is Hamiltonian. In fact, our task here is considerably easier since we may use the properties in Lemma 8.17. Nevertheless, we shall not give the proof for we shall encounter the colouring argument once again in the next section (Theorem 8.19), in a somewhat simpler form.

Frieze (1986*d*) further improved the upper bound on $\beta(c)$ and showed that, asymptotically, $\alpha(c)$ and $\beta(c)$ are equal to the right-hand side of (8.15), which gives the correct order of $\alpha(c)$ and $\beta(c)$.

Theorem 8.18 *There is a function* $\varepsilon(c)$ *satisfying* $\lim_{c\to\infty} \varepsilon(c) = 0$ *such that*

$$(c+1)e^{-c} \le \alpha(c) \le \beta(c) \le \{1 + \varepsilon(c)\}ce^{-c}. \qquad \square$$

In fact, Frieze proved that the analogue of Theorem 8.18 holds for $c = c(n) \to \infty$ as well; in particular, Theorem 8.9 is a special case of this extension.

8.5 Hamilton Cycles in Regular Graphs—First Approach

We saw in §3 that in a typical r. g. G_M the obstruction to a Hamilton cycle is the existence of vertices of degree at most 1, so unless M is greater than $(n/2)\log n$ the probability that G_M is Hamiltonian is very small. Are Hamiltonian cycles more likely to occur in a considerably sparser r.g. if we make sure that the minimal degree is not too small? In particular, if r is not too small, is a.e. r-regular graph Hamiltonian?

Before turning to this question, we shall study a substantially simpler model, $\mathscr{G}_{k\text{-out}}$, whose properties are, nevertheless, fairly close to those of $\mathscr{G}_{r\text{-reg}}$. Note that, for a fixed k, the graphs in $\mathscr{G}_{k\text{-out}}$ have only $O(n)$ edges, so we are looking for a Hamilton cycle in a very sparse graph indeed. Is it true then that if k is sufficiently large, then a.e. $G_{k\text{-out}}$ is Hamiltonian? In answering this question in the affirmative, Fenner and Frieze (1983) achieved a considerable breakthrough. The ingenious proof was the first example of the colouring argument.

Theorem 8.19 *There is a $k_0 \in \mathbb{N}$ such that if $k \geq k_0$, then a.e. $G_{k\text{-out}}$ is Hamiltonian.*

Proof We shall start by showing that a.e. $G_{k\text{-out}}$ spreads, i.e. satisfies an assertion similar to Lemma 8.7. To be precise, consider $\vec{\mathscr{G}}_{k\text{-out}}$ and for $U \subset V$ and $\vec{G} \in \vec{\mathscr{G}}_{k\text{-out}}$ write

$$\vec{\Gamma}(U) = \vec{\Gamma}_{\vec{G}}(U) = \{x \in V : \vec{ux} \in \vec{E}(\vec{G}) \text{ for some } u \in U\}. \qquad \square$$

Lemma 8.20 *If $0 < \alpha < \frac{1}{4}$ and $k \in \mathbb{N}$ satisfy*

$$4^k \alpha^{k-4}(1-4\alpha)^{4-1/\alpha} < 27, \tag{8.16}$$

then a.e. $\vec{G} \in \vec{\mathscr{G}}_{k\text{-out}}$ is such that

$$|U \cup \vec{\Gamma}(U)| \geq 4|U| + 1 \tag{8.17}$$

whenever $U \subset V$ and $|U| \leq \alpha n$.

Proof Note that the conditions imply that $k \geq 5$. If (8.17) fails, then $|U| \geq u_0 = \lceil k/4 \rceil \geq 2$. For $u_0 \leq u \leq u_1 = \lfloor \alpha n \rfloor$, the probability that (8.17) fails is clearly at most

$$\begin{aligned}
&\binom{n}{u}\binom{n-u}{3u}\left\{\binom{4u}{k}\Big/\binom{n}{k}\right\}^u \\
&\qquad < \left(\frac{n}{u}\right)^u \left(\frac{n}{n-u}\right)^{n-u} \left(\frac{n-u}{3u}\right)^{3u} \left(\frac{n-u}{n-4u}\right)^{n-4u} \left(\frac{4u}{n}\right)^{ku} \\
&\qquad < \{3^{-3}4^k(u/n)^{k-4}(1-4u/n)^{4-n/u}\}^u \\
&\qquad = S_u \leq c_k n^{-2}
\end{aligned}$$

for some constant c_k, provided n is sufficiently large. Hence

$$\sum_{u=u_0}^{u_1} S_u = o(1),$$

implying our lemma. $\square$

We shall show that Theorem 8.19 holds with $k_0 = 23$. Set $\alpha = 0.202$ and note that for $k \geq k_0$ inequality (8.16) holds and

$$(1-\alpha)^{2\alpha} < 1 - 2/k_0 \leq (k-2)/k. \tag{8.18}$$

Call a graph $G_{k\text{-out}}$ *exceptional* if it is connected, satisfies (8.17) and is non-Hamiltonian; let $\mathscr{G}_0$ be the set of exceptional graphs and set $\gamma_0 = \gamma_0(k, n) = P(\mathscr{G}_0)$. By Lemma 8.20 and Theorem 7.35, claiming that for $k \geq 2$ a.e. $G_{k\text{-out}}$ is connected, our theorem follows if we show that $\gamma_0 = o(1)$.

As in §1 of Chapter 2, let $G = \phi(\vec{G})$ be the graph $G_{k\text{-out}}$ obtained from $\vec{G} \in \vec{\mathscr{G}}_{k\text{-out}}$ and set

$$\vec{\mathscr{G}}_0 = \{\vec{G} \in \vec{\mathscr{G}}_{k\text{-out}} : \phi(\vec{G}) \in \mathscr{G}_0\}$$

Then, by the definition of the measure on $\mathscr{G}_{k\text{-out}}$,

$$|\vec{\mathscr{G}}_0| = \gamma_0 |\vec{\mathscr{G}}_{k\text{-out}}| = \gamma_0 \binom{n-1}{k}^n .$$

Given $\vec{G} \in \vec{\mathscr{G}}_0$, for each vertex x colour $k-1$ of the arcs leaving x *blue* and the remaining arc *red*: let $\vec{G} = \vec{B} \cup \vec{R}$ be the resulting colouring. Let $\vec{\mathscr{H}}_0$ be the collection of coloured graphs obtained from elements of $\vec{\mathscr{G}}_0$ for which $B = \phi(\vec{G})$ has as long a path as $\phi(\vec{G})$. By construction,

$$|\vec{\mathscr{H}}_0| \geq |\vec{\mathscr{G}}_0| \{k(k-2)\}^{n/2} = \gamma_0 \binom{n-1}{k}^n \{k(k-2)\}^{n/2}. \tag{8.19}$$

Let $\vec{G} = \vec{B} \cup \vec{R} \in \vec{\mathscr{H}}_0$. Then, by (8.17), $B = \phi(\vec{B})$ satisfies (8.4) for $u = \lceil \alpha n \rceil$ since $\vec{\Gamma}_{\vec{B}}(U)$ is at most $|U|$ smaller than $\vec{\Gamma}_{\vec{G}}(U)$. Furthermore, as $G = \phi(\vec{G})$ is connected and non-Hamiltonian, its longest path is longer than its longest cycle hence, by the choice of $\vec{B}$, the same holds for B. Consequently, by Lemma 8.5, there are $u = \lceil \alpha n \rceil$ vertices and for each of these vertices u arcs leaving it (depending only on B) so that none of these u^2 arcs can appear in either $\vec{B}$ or $\vec{R}$. Therefore $\vec{B}$ is the blue subgraph of at most

$$(n-1)^{n-u}(n-1-u)^u \leq (1-\alpha)^{\alpha n} n^n$$

elements of $\vec{\mathscr{H}}_0$. Since, rather crudely, we have at most $\binom{n-1}{k-1}^n$ choices for $\vec{B}$,

$$|\vec{\mathscr{H}}_0| \leq \binom{n-1}{k-1}^n (1-\alpha)^{\alpha n} n^n. \tag{8.20}$$

Inequalities (8.19) and (8.20) imply

$$\gamma_0 \leq e^{k+1}(1-\alpha)^{\alpha n} \left(\frac{k}{k-2}\right)^{n/2} = o(1),$$

with the second relation following from (8.18).

With more effort one could prove that Theorem 19 holds for a smaller k_0, say for $k_0 = 19$. Nevertheless, this would not be worth the additional effort, however slight, since Cooper and Frieze (2000) used a different method to prove it for $k_0 = 4$. We shall return to this in the next section. Furthermore, it is very likely that the theorem holds even for $k_0 = 3$: a.e. $G_{3-\text{out}}$ is Hamiltonian. If true, this result would be best possible since $\underline{\lim}_{n\to\infty} P(G^n_{2-\text{out}}$ is not Hamiltonian$) > 0$ (see Exx. 4 and 5).

In view of Theorem 8.19, it is not too surprising that if r is sufficiently large, then a.e. $G_{r\text{-reg}}$ is Hamiltonian. This was proved independently by Bollobás (1983*a*) and Fenner and Frieze (1984), by adapting the proof above to the model of random regular graphs. Since the proof is fairly intricate and not too short, we do not give it here.

Theorem 8.21 *There is an $r_0 \in \mathbb{N}$ such that if $r \geq r_0$, then a.e. $G_{r\text{-reg}}$ is Hamiltonian.* □

As we shall see in the next section, much better results have been proved by different methods.

Fenner and Frieze (1984) gave a fairly small bound for r_0, namely $r_0 \leq 796$, and with more work even that bound could be reduced. However, the remarks after Theorem 8.19 are valid in this case as well: it would not be worthwhile to prove $r_0 \leq 10$, say, at the expense of more involved calculations, for it is very likely that a.e. cubic graph is Hamiltonian, so one can take $r_0 = 3$. In fact, by estimating the variance of the number of Hamilton cycles, Robinson and Wormald (1984) proved that the probability that a cubic graph is Hamiltonian is at least 0.974. Furthermore, they also proved that a.e. bipartite cubic graph is Hamiltonian. On the other hand, a result of Richmond, Robinson and Wormald (1985) shows that, occasionally, Hamilton cycles are rare: a.e. cubic planar graph is non-Hamiltonian.

8.6 Hamilton Cycles in Regular Graphs—Second Approach

With Theorem 8.21 of Bollobás (1983a) and Fenner and Frieze (1984), the race was on to prove the best possible result that one may take $r_0 = 3$. Fenner and Frieze (1984) gave a fairly small bound for r_0, namely $r_0 \leq 796$, and by taking more care with the proof above, that bound could be reduced. In 1988, Frieze used a slightly different, algorithmic approach to prove that $r_0 = 85$ will do in Theorem 8.21.

The usual way of proving that a.e. random graph contains a certain subgraph is to study the number X of those subgraphs and to prove that

$P(X > 0) \to 1$ as $n \to \infty$. This was the approach used in Chapters 3 and 4 when we studied degrees and small subgraph, but the methods in the proofs of Theorems 8.19 and 8.21 were entirely different. The obvious explanation for this is that in Theorems 8.19 and 8.21 we were looking for very large and fairly complicated subgraphs; after all, it is NP—complete find a Hamilton cycle in a graph. In view of this it is rather surprising that a streamlined and more sophisticated version of the second moment method enabled Robinson and Wormald (1994) to prove Theorem 8.21 with $r_0 = 3$.

Theorem 8.22 *For* $r \geq 3$, *a.e.* $G_{r\text{-ref}}$ *is Hamiltonian.*

Before we say a few words about the proof of Theorem 8.22, let us note that occasionally Hamilton cycles are more elusive than they seen. For example, Tait conjectured in 1880 that every 3-connected, 3-regular, planar graph is Hamiltonian, and it was only in 1996 that Tutte found a counterexample. In 1985 Richmond, Robinson and Wormald proved that counterexamples to Tait's conjecture are anything but rare: almost no 3-connected, 3-regular, planar graph has a Hamilton cycle.

At the first right it is surprising that Robinson and Wormald first proved Theorem 8.21 for cubic graphs (i.e., $r = 3$) and they needed more ideas to extend the result to all r-regular graphs with $r \geq 3$. The reason for this is the method they used: it is exiting to compute moments of the number of Hamilton cycles in the space of cubic graphs thin in the space of r-regular graphs for $r \geq 4$.

Here we give only an all-too-brief sketch of the work of Robinson and Wormald. Let us write $H = H(G_{r\text{-ref}})$ for the number of Hamilton cycles in $G_{r\text{-ref}}$. First, Robinson and Wormald (1984) proved that in the space $\mathcal{G}_{3\text{-ref}}$ of cubic graphs of order n, with n even,

$$E(H(G_{3\text{-reg}})) \sim \frac{e\sqrt{\pi}}{\sqrt{2n}} \left(\frac{4}{3}\right)^{n/2}$$

and

$$\sigma^2(H(G_{3\text{-reg}})) \sim \left(\frac{3}{e} - 1\right)(E(H))^2.$$

Although this variance is for two large to enable one to deduce that a.e. cubic graph is Hamiltonian, these relations imply that asymptotically at last 2–3/e of all cubic graphs are Hamiltonian. Robinson and Wormald had the striking idea that the second moment method (i.e., Chebyshev's inequality) may still give the required result if the space $\mathscr{G}_{3\text{-reg}}$ is partitioned into suitable subsets. To start this programme, by considering triangle-free cubic graphs, Robinson and Wormald (1984) proved that for large n the probability that a cubic graph is Hamiltonian is at last 0.974.

To prove Theorem 8.22 for $r = 3$, Robinson and Wormald (1992) went considerably further: they partitioned $\mathscr{G}_{3-\text{reg}}$ according to the distribution of short *old* cycles. (Even cycles do not seem to matter.) Recall from Corollary 2.19 of Bollobás (1980*a*) and Wormald (1981*a*,*b*) that if we denote by $Y_k = Y_k(G_{r\text{-reg}})$ the number of cycles of length k in $G_{r\text{-reg}}$ then $Y_3, Y_4, \ldots, Y_l$ are asymptotically independent Poisson r.v. with means $\lambda_3, \lambda_4, \ldots, \lambda_l$, where $\lambda_k = (r-1)^k/2k$. In particular,

$$E(Y_{2k+1}(G_{3\text{-reg}})) \sim \frac{4^k}{2k+1}.$$

Robinson and Wormald (1992) partitioned $\mathscr{G}_{3-\text{reg}}$ into sets

$$\Omega(c_1, \ldots, c_l) = \{G_{3\text{-reg}} : Y_{2k+1}(G_{3\text{-reg}}) = c_k, k = 1, \ldots, l\}.$$

They estimated the mean and variance of H on such a set, and applied Chebyshev's inequality to show that, as $l \to \infty$, the conditional probability $P(H > 0|\Omega(c_1, \ldots, c_l))$ tends to 1 for every response $c_1, c_2, \ldots$. Needless to say, much work and ingenuity are needed to carry out this task.

The case $r \geq 4$ of Theorem 8.22 is proved in a rather different way. It is easily seen that

$$E(H(G_{r\text{-reg}})) \sim \left(\frac{(r-2)^{(r-2)/2}(r-1)}{r^{(r-2)/2}}\right)^n e\sqrt{\frac{\pi}{2n}},$$

but much work is needed to shown that

$$\sigma^2(H(G_{r\text{-reg}})) \sim \left(\frac{re^{-2/(r-1)}}{r-2} - 1\right)(E(H))^2.$$

In order to prove that $P(H > 0) \to 1$, one could proceed as in the cubic case sketched above but it turns out that the work would be technically extremely difficult. This is simply because it is much hunter to compute the variance of the number of Hamilton cycles on a set $\Omega(c_1, c_2, \ldots, c_l)$ due to the fact that in $\mathscr{G}_{3\text{-reg}}$ the union of two Hamilton cycles has only vertices of degrees 2 and 3, while in $\mathscr{G}_{r\text{-reg}}$, with $r \geq 4$, these may be vertices of degree 4 as well.

Rather than taking this route, Robinson and Wormald conditioned on the distribution of 1-factors, assuming that n is even. They showed that the removal of a random 1-factor (complete matching) from $G_{r\text{-reg}}$

produces a reasonably random $(r-1)$-regular graph. Hence Theorem 8.22 is proved by induction on r. In fact, this line of attack proves much more, namely that for n even a.e. $G_{r\text{-ref}}$ is the union of a Hamilton cycle and $r-2$ complete matchings. A minor variation of the approach takes care of odd values of n.

These ideas were carried considerably further by Janson (1995) and Molloy, Robalewska, Robinson and Wormald (1997). Call two sequences of (finite) probability spaces (Ω_n, P_n) and (Ω'_n, P'_n) *contiguous* if they have the some almost sure events, i.e., $P_n(\Omega_n \backslash \Omega'_n) \to 0$, $P'_n(\Omega'_n \backslash \Omega_n) \to 0$ and if $A_n \subset \Omega_n \cap \Omega'_n$ than $\lim_{n\to\infty} P_n(A_n) = 0$ iff $\lim_{n\to\infty} P'_n(A_n) = 0$.

There are many ways of constructing random r-regular graphs in addition to the basic method of taking all of them. For example, for n even we may take the union of r random edge-disjoint complete matchings or we may take the union of a random $(r-1)$-regular graph and a random edge-disjoint complete matching. For $r = 3$, we may take the union of a random Hamilton cycle and a random edge-disjoint matching. As proved by Janson (1995) and Molloy, Robalewska, Robinson and Wormald (1997), all these models of random regular graphs are contiguous. In particular, for $r \geq 2J \geq 4$, a.e. $G_{r\text{-reg}}$ is the edge-disjoint union of J Hamilton cycles.

Cooper, Frieze and Molloy (1994) proved the analogue of Theorem 8.22 for digraphs: a.e. 3-regular digraph is Hamiltonian. Theorem 8.22 has an algorithmic version as well, proved by Frieze, Jerrum, Molloy, Robinson and Wormald (1996): there are polynomial time algorithms that find Hamilton cycles in $G_{r\text{-reg}}$ with high probability, and approximately count their number.

Let us mention that occasionally one searches for Hamilton cycles in rather strange spaces of random graphs; for example, Frieze, Karoúski and Thoma (1999) proved that the probability that the union of five random trees on $[n]$ contains a Hamilton cycle tends to 1 as $n \to \infty$.

The regularity of graphs is an extremely useful condition in proving the existence of Hamilton cycles: although in many ways $\mathcal{G}_{k\text{-out}}$ is much more pleasant than $\mathcal{G}_{r\text{-reg}}$ (for example, it is much easier to generate a $G_{k\text{-out}}$ than a $G_{r\text{-reg}}$), it seems to be harder to prove best possible results about $G_{k\text{-out}}$ than about $G_{r\text{-reg}}$. Nevertheless, Cooper and Frieze (2000) have come very close to doing precisely that. They defined a *random digraph* $D_{\alpha\text{-in},\beta\text{-out}}$ as follows: the vertex set is $[n]$, and for each $v \in [n]$ we choose α random edges directed *into* v, and β random edges directed *out of* v. The choices are made without replacement, although this makes rather little difference. Thus $D_{\alpha\text{-in},\beta\text{-out}}$ has $(\alpha+\beta)n$ edges. The strong connectivity of

$D_{\alpha-\text{in},\beta-\text{out}}$ was studied by Fenner and Frieze (1982), Cooper and Frieze (1990) and Reed and McDiarmid (1992).

Concerning Hamilton cycles, Frieze and Łuczak (1990) greatly improved on the bound in Theorem 8.19: they proved that a.e. $G_{5\text{-out}}$ is Hamiltonian. Cooper and Frieze (1994) proved the difficult result that a.e. $D_{3\text{-in},3\text{-out}}$ digraph is Hamiltonian and in 2000, in a long and complicated paper, they further improved this result.

Theorem 8.23 *A.e. $D_{2\text{-in},2\text{-out}}$ is a Hamiltonian digraph.* □

This result of Cooper and Frieze is best possible since almost no $D_{1\text{-in},2\text{-out}}$ is Hamiltonian. Indeed, a.e. $D_{1\text{-in},2\text{-out}}$ contains two vertices of indegree 1 with the some in-neighbour.

Note that by ignoring the orientation in $D_{2\text{-in},2\text{-out}}$, we find that a.e. $G_{4\text{-out}}$ is Hamiltonian. It is widely believed that one more improvement is possible, namely that a.e. $G_{3\text{-out}}$ is Hamiltonian. In view of the rapid development of the topic, it is unlikely that this conjecture will remain open for long.

Exercises

8.1 Denote by μ_p and σ_p^2 the expectation and variance of the number of Hamilton cycles in a graph in $\mathcal{G}(n,p)$. Note that $\mu_p = \frac{1}{2}(n-1)!p^n$ and conclude that if $c > 0$ is a constant, then

$$\lim_{n\to\infty} \mu_p = \begin{cases} 0, & \text{if} c \le \mathrm{e}, \\ \infty, & \text{if} c > \mathrm{e}. \end{cases}$$

8.2 (Ex. 1 ctd.) Prove that for $p = c(\log n)/n, 0 < c < \infty$, one has $\mu_p = o(\sigma_p)$.

8.3 Give a detailed proof of Lemma 8.17.

8.4 Consider the directed graphs $\vec{G}_{2\text{-out}}$. Call a set $\{a_1, a_2, \dots, a_k, b\} \subset V$ a *k-legged spider* if each a_i sends an arc to b and no arc ends in any of the a_i. Prove that for every $k \in \mathbb{N}$, the expected number of k-legged spiders in $\vec{G}_{2\text{-out}}$ tends to ∞. Prove also that a.e. $\vec{G}_{2\text{-out}}$ contains a k-legged spider.

8.5 Deduce from Ex. 4 that $G_{2\text{-out}}$ is almost surely non-Hamiltonian.

8.6 Let $p = (\log n + \log\log n + c_n)/n$. Prove that the probability that a random digraph is connected tends to $\mathrm{e}^{-2\mathrm{e}^{-c}}$ as $c_n \to c$.

8.7 Prove that for $r \ge 3$ the expected number of Hamilton cycles in $G_{r\text{-}reg}$ is about

$$\left(\frac{(r-2)^{(r-2)/2}(r-1)}{r^{(r-2)/2}}\right)^n \mathrm{e}\sqrt{\frac{\pi}{2n}}.$$

9

The Automorphism Group

The theory of random graphs is almost exclusively concerned with random graphs on distinguishable vertices. This would be a rather unsatisfactory state of affairs but for the fact that unless a result concerns labelled graphs which are rather close to the empty graph or the complete graph, it can be carried over to unlabelled graphs. This deduction is made possible (and very simple) by an important theorem of Wright (1971). The heart of this chapter is §1, in which we prove this theorem. The second section is devoted to an analogous result about regular graphs, and the final three sections contain a variety of other results.

9.1 The Number of Unlabelled Graphs

Denote by $U_M = U_{n,M}$ the number of unlabelled graphs of order n and size M and write $L_M = L_{n,M}$ for the number of labelled graphs: $L_M = \binom{N}{M}$. Our main aim in this section is to show that under suitable conditions on M we have

$$U_M \sim L_M/n! = \binom{N}{M} \Big/ n! \tag{9.1}$$

Since every unlabelled graph is isomorphic to a set of at most $n!$ labelled graphs,

$$U_M \geq L_M/n!$$

Furthermore, if the automorphism group of an unlabelled graph is nontrivial then the graph is isomorphic to at most $n!/2$ labelled graphs. Hence (9.1) implies that almost every unlabelled graph has a trivial automorphism group so, *a fortiori*, almost every graph in $\mathcal{G}_M$ has a trivial automorphism group. However, (9.1) is considerably stronger than the fact that the automorphism group of a.e. G_M is trivial.

Before even starting on a reformulation of (9.1), let us see a rather simple condition M has to satisfy if (9.1) is true. If the automorphism group of a graph of order n is trivial, then the graph contains at most one isolated vertex and at most one vertex of degree $n-1$. Hence, by Theorem 3.5, if (9.1) holds then

$$\frac{2M}{n} - \log n \to \infty \text{ and } \frac{2(N-M)}{n} - \log n \to \infty. \tag{9.2}$$

It is perhaps a little surprising that this simple necessary condition on M is in fact sufficient to imply (9.1). This important result is due to Wright (1971); earlier Pólya (see Ford and Uhlenbeck, 1957), Erdős and Rényi (1963) and Oberschelp (1967) had proved (9.1) under much stronger conditions than (9.2). In order to give an entirely combinatorial proof of this result, rather different from the original one, we shall proceed very slowly and cautiously.

What do we have to do to prove (9.1)? Consider the symmetric group S_n acting on $V = \{1, 2, \ldots, n\}$. For $\rho \in S_n$ let $\mathscr{G}(\rho)$ be the set of graphs in $\mathscr{G}_M$ invariant under ρ and put $I(\rho) = |\mathscr{G}(\rho)|$. Then

$$\sum_{\rho \in S_n} I(\rho) = \sum_{G \in \mathscr{G}_M} a(G),$$

where $a(G)$ is the order of the automorphism group of $G \in \mathscr{G}_M : a(G) = |\mathrm{Aut}\, G|$. Since $\mathscr{G}_M$ has exactly $n!/a(G)$ graphs isomorphic to a given graph $G \in \mathscr{G}_M$,

$$U_M = \sum_{G \in \mathscr{G}_M} \{n!/a(G)\}^{-1} = \frac{1}{n!} \sum_{G \in \mathscr{G}_M} a(G) = \frac{1}{n!} \sum_{\rho \in S_n} I(\rho).$$

For the identity permutation $1 \in S_n$ we have $I(1) = L_M$, so (9.1) holds iff

$$\sum_{\substack{\rho \in S_n \\ \rho \neq 1}} I(\rho) = o(L_M). \tag{9.3}$$

It is clear that $I(\rho)$ depends only on the size of the orbits of ρ acting on $V^{(2)}$, the set of N pairs of vertices, because a graph G_M belongs to $\mathscr{G}(\rho)$ if and only if the edge set of G_M is the union of some entire orbits of ρ acting on $V^{(2)}$. Let us pause for a moment to consider in how many ways a set of given size can be made up of entire orbits.

Let A be a fixed set with a elements. We shall consider set systems $\mathscr{A} = \{A_1, A_2, \ldots, A_s\}$ partitioning $A : A = \bigcup_{i=1}^{s} A_i$. Denote by $\mathscr{F}(b; \mathscr{A}) = \mathscr{F}(b; A_1, \ldots, A_s)$ the collection of those b-element subsets of A which are the unions of some of the sets A_i. Thus $B \in \mathscr{F}(b; \mathscr{A})$ iff $|B| = b$ and for every i we have $A_i \subset B$ or $B \cap A_i = \emptyset$. Suppose there are m_1 sets A_i of size 1, m_2 sets of size $2, \ldots, m_t$ sets of size t and no set with more than t elements. Note that these parameters satisfy

$$a = \sum_{j=1}^{t} jm_j.$$

The definition of $\mathscr{F}(b;\mathscr{A})$ implies that if $f(b;\mathscr{A}) = |\mathscr{F}(b;\mathscr{A})|$, then

$$f(b;\mathscr{A}) = f(b;m_1,m_2,\ldots,m_t) = \sum_{(i_j)} \binom{m_1}{b-k} \prod_{j=2}^{t} \binom{m_j}{i_j}, \tag{9.4}$$

where the summation is over all $(i_j)_2^t$ satisfying $0 \le i_j \le m_j$ and $k = k((i_j)_2^t) = \sum_{j=2}^t ji_j \le b, b-k \le m_1$.

If $\mathscr{A}'$ is obtained from $\mathscr{A}$ by decomposing an A_i into some sets (that is if the partition $\mathscr{A}'$ is a *refinement* of $\mathscr{A}$), then clearly $\mathscr{F}(b;\mathscr{A}) \subset \mathscr{F}(b;\mathscr{A}')$, so

$$f(b;\mathscr{A}) \le f(b;\mathscr{A}'). \tag{9.5}$$

In particular, if $m_1 + 2m_2 = a$ and $0 \le k \le m_2$, then

$$f(b;m_1,m_2) \le f(b;m_1+2k, m_2-k). \tag{9.6}$$

Furthermore, if $\mathscr{A}$ is the union of two disjoint systems, say $\mathscr{A}'$ and $\mathscr{A}''$, then

$$f(b;\mathscr{A}) = \sum_{i=0}^{b} f(b-i;\mathscr{A}')f(i;\mathscr{A}'').$$

Consequently, if $m_j = m_j' + m_j''$ with $m_j' \ge 0$ and $m_j'' \ge 0$, then

$$f(b;m_1,\ldots,m_t) = \sum_{i=0}^{b} f(b-i;m_1',\ldots,m_t')f(i;m_1'',\ldots,m_t''). \tag{9.7}$$

The last property of the function $f(b;m_1,\ldots,m_t)$ we need is not quite immediate so we state it as a lemma.

Lemma 9.1 *Suppose $m_1 \le a-2$. If $a-m_1$ is odd,*

$$f(b;m_1,\ldots,m_t) \le f\left(b;m_1+1,\tfrac{1}{2}(a-m_1-1)\right)$$

and if $a-m_1$ is even, then

$$f(b;m_1,m_2,\ldots,m_t) \le f\left(b;m_1+2,\tfrac{1}{2}(a-m_1-2)\right).$$

Proof Since a set A_i with more than three elements can be partitioned into sets of size 2 and 3, by (9.5) we may suppose that $\mathscr{A}$ contains no sets of size greater than 3, that is $m_4 = m_5 = \ldots = m_t = 0$. Furthermore, if $m_3 = 0$ the lemma is proved, since then $a - m_1 = 2m_2$ and by (9.6)

$$f(b; m_1, m_2, \ldots, m_t) = f(b; m_1, m_2) \le f(b; m_1 + 2, m_2 - 1).$$

Now suppose that $m_3 > 0$. We distinguish two cases according to the parity of m_3, which is also the parity of $a - m_1$. First suppose that m_3 is odd, say $m_3 = 2k + 1 \ge 1$. We know from (9.7) that

$$f(b; m_1, m_2, 2k+1) = \sum_{i=0}^{b} f(b-i; m_1, m_2) f(i; 0, 0, 2k+1)$$

and

$$f(b; m_1 + 1, m_2 + 3k + 1) = \sum_{i=0}^{b} f(b-i; m_1, m_2) f(i; 1, 3k+1).$$

Hence it suffices to show that

$$f(i; 0, 0, 2k+1) \le f(i; 1, 3k+1). \tag{9.8}$$

In order to show (9.8) we use (9.4) to write out the two sides explicitly. If the left-hand side of (9.8) is not zero, then i is a multiple of 3. Furthermore, if $i = 6j$, then (9.8) becomes

$$\binom{2k+1}{2j} \le \binom{3k+1}{3j}$$

and if $i = 6j + 3$, then (9.8) is

$$\binom{2k+1}{2j+1} \le \binom{3k+1}{3j+1}.$$

Both inequalities are obvious.

Finally, if m_3 is even, say $m_3 = 2k + 2$, then

$$f(b; m_1, m_2, 2k+2) \le f(b; m_1+1, m_2+1, 2k+1) \le f(b; m_1+2, m_2+3k+2),$$

completing the proof. $\square$

Let us return to our central theme, relation (9.3). We shall prove it by estimating $I(\rho)$ in terms of the number of vertices fixed by ρ. Denote by $S_n^{(m)}$ the set of permutations moving m vertices, that is fixing $n - m$ vertices. Then $S_n^{(0)} = \{1\}$ and $S_n^{(1)} = \varnothing$. Furthermore, if $\rho \in S_n^{(m)}$, then the m vertices moved by ρ can be selected in $\binom{n}{m}$ ways and there are at most $m!$ permutations moving the same set of m vertices. Hence

$$|S_n^{(m)}| \leq \binom{n}{m} m! = (n)_m. \tag{9.9}$$

Lemma 9.2 *Let $2 \leq m \leq n, n \geq 3$, and denote by $N_1 = N_1(m)$ the integer satisfying*

$$\binom{n-m}{2} + \frac{m+1}{2} \leq N_1 \leq \binom{n-m}{2} + \frac{m+4}{2}$$

for which $N_2 = (N - N_1)/2$ is also an integer. Then for $\rho \in S_n^{(m)}$ we have

$$I(\rho) \leq f(M; N_1, N_2).$$

Proof Suppose $\rho \in S_n^{(m)}$ as a permutation acting on $V^{(2)}$ has M_i orbits of size $i, i = 1, 2, \ldots, N$. Since a graph G_M belongs to $\mathcal{G}(\rho)$ iff its edge set is the union of some entire orbits,

$$I(\rho) = |\mathcal{G}(\rho)| = f(M; M_1, M_2, \ldots, M_N).$$

Hence if M_1' is chosen to be $M_1 + 1$ or $M_1 + 2$ so that $M_2' = (N - M_1')/2$ is an integer, then by Lemma 9.1 we have

$$I(\rho) \leq f(M; M_1', M_2').$$

At most how large is M_r? If a permutation fixes two pairs of vertices, say $\{x, y\}$ and $\{y, z\}$, then it also fixes y, the common vertex, and so x and z as well. Consequently a pair fixed by $\rho \in S_n^{(m)}$ either consists of two vertices fixed by ρ or it is disjoint from all other pairs fixed by ρ. Hence

$$M_1 \leq \binom{n-m}{2} + m/2$$

and so

$$M_1' \leq N_1.$$

Therefore by inequality (9.6) we have

$$I(\rho) \leq f(M; M_1', M_2') \leq f(M; N_1, N_2). \qquad \square$$

Before embarking on the proof of the main theorem, we prove (9.3) under a stronger assumption. There are two reasons for this. First, having obtained the preliminary result, in the proof of the main theorem we may assume that $M = O(n \log n)$, which will turn out to be rather useful.

Second, the proof of the preliminary result is considerably simpler than that of the main theorem. In fact, the proof is so straightforward that we do not even rely on our lemmas, since a very weak form of Lemma 9.2 will suffice.

Theorem 9.3 *If $c > 1$ is a constant and*

$$cn \log n \le M \le N - cn \log n,$$

then

$$U_M \sim L_M/n!$$

Proof Suppose $\rho \in S_n$, as a permutation acting on $V^{(2)}$, has M_j orbits of size $j, j = 1, \dots, N$. Then $\sum_{j=1}^N jM_j = N$ and

$$I(\rho) = \left[\prod_{j=1}^{N} (1 + X^j)^{M_j}\right]_M$$

where $[F(X)]_k$ is the coefficient of X^k in the polynomial $F(X)$.

It is trivial that if a polynomial $F(X)$ has non-negative coefficients and $x > 0$, then

$$[F(X)]_k \le x^{-k} F(x).$$

Applying this inequality with $x = p/q$, where $p = M/N$ and $q = 1 - p$, we obtain

$$\begin{aligned} I(\rho) &\le (p/q)^{-M} \prod_{j=1}^{N} \{1 + (p/q)^j\}^{M_j} \\ &= p^{-M} q^{M-M_1} \prod_{j=2}^{N} \{1 + (p/q)^j\}^{M_j} \\ &\le p^{-M} q^{M-M_1} \prod_{j=2}^{N} \{1 + (p/q)^2\}^{jM_j/2} \\ &= p^{-M} q^{-(N-M)} (p^2 + q^2)^{(N-M_1)/2}. \end{aligned}$$

The second inequality holds since $1 + x^j \le (1 + x^2)^{j/2}$ for every $x \in \mathbb{R}$ and $j \ge 2$, and the second equality is true since $\sum_{j=1}^N jM_j = N$.

Now if $\rho \in S_n^{(m)}, m \ge 2$, then

$$M_1 \le \binom{n-m}{2} + m/2,$$

so

$$N - M_1 \geq m\left(n - 1 - \frac{m}{2}\right) = N(m).$$

By inequality (9.5) of Chapter 1 we have

$$L_M \geq 8^{-1/2} p^{-M} q^{-(N-M)} (pqN)^{-1/2}.$$

Hence, recalling (9.9), we find that

$$\begin{aligned} \sum_{\rho \in S_n^{(m)}} I(\rho)/L_M &\leq |S_n^{(m)}|(p^2+q^2)^{N(m)/2} 8^{1/2}(pqN)^{1/2} \\ &\leq (n)_m (p^2+q^2)^{N(m)/2} n \leq n^{m+1}(p^2+q^2)^{(m/2)\{n-1-(m/2)\}}. \end{aligned}$$

Here we have made use of the inequality

$$pqN \leq \tfrac{1}{4}N \leq n^2/8.$$

The time has come to make use of the restriction on M. By assumption

$$2c\frac{\log n}{n-1} \leq p \leq 1 - 2c\frac{\log n}{n-1}$$

so

$$p^2 + q^2 \leq 1 - 4c\frac{\log n}{n-1}\left(1 - 2c\frac{\log n}{n-1}\right)$$

and

$$\log(p^2+q^2) \leq -4c\frac{\log n}{n-1} + 32c^3\left(\frac{\log n}{n-1}\right)^3 \leq -4c\frac{\log n}{n}.$$

Therefore

$$\sum_{\rho \in S_n^{(m)}} I(\rho)/L_M \leq n^{m+1}\exp\left\{-2cm(\log n)\left(1 - \frac{1}{n} - \frac{m}{2n}\right)\right\}.$$

It is easily checked that if n is sufficiently large, then

$$2cm\left(1 - \frac{1}{n} - \frac{m}{2n}\right) \geq m + 1 + c$$

for every $m, 2 \leq m \leq n$. Hence if n is large enough, then

$$\sum_{\rho \in S_n^{(m)}} I(\rho)/L_M \leq n^{-c}$$

and so

$$\sum_{\rho \neq 1} I(\rho)/L_M = \sum_{m=2}^{n} \sum_{\rho \in S_n^{(m)}} I(\rho)/L_M \leq n^{1-c} = o(1),$$

showing that (9.3) does hold. □

We have to be considerably more careful with our estimates to prove the main result.

Theorem 9.4 *Suppose* $\omega(n) \to \infty$ *and*

$$\tfrac{1}{2}n\log n + \omega(n)n \le M \le N - \tfrac{1}{2}n\log n - \omega(n)n.$$

Then

$$U_M \sim L_M/n!$$

Proof The map sending a graph into its complement preserves the automorphism group and sets up a one-to-one correspondence between $\mathcal{G}_M$ and $\mathcal{G}_{N-M}$. Hence in proving this result we may assume that $M \le N/2$. Furthermore, because of Theorem 3 we may and shall assume that

$$\tfrac{1}{2}n\log n + \omega(n)n \le M \le 2n\log n.$$

We shall also assume that $n \ge n_0$ where n_0 depends on the function $\omega(n)$ and is chosen so that all our inequalities hold. It will be easy to check that there is such an n_0. As usual, we shall assume that $\omega(n)$ does not grow fast, say $\omega(n) = o(\log\log n)$.

Let $N_1 = N_1(m)$ and $N_2 = N_2(m) = \frac{1}{2}(N - N_1)$ be as in Lemma 9.2 and set

$$\begin{aligned} L(m,i) &= \binom{N_1}{M-2i}\binom{N_2}{i}, \\ L(m) &= \sum L(m,i), \end{aligned}$$

where the summation is over all i satisfying $0 \le i \le N_2$ and $M - N_1 \le 2i \le M$. If $\rho \in S_n^{(m)}$, then by Lemma 9.2 we have

$$I(\rho) \le L(m).$$

Hence, by (9.3) and (9.9) the theorem follows if we show that

$$\sum_{m=2}^{n}(n)_m L(m)/L_m = o(1) \tag{9.10}$$

For the sake of convenience let us recall the inequality N_1 satisfies:

$$m\{n-(m/2)-2\} - 2 \le N - N_1 \le m\{n-(m/2)-2\} - \tfrac{1}{2}. \tag{9.11}$$

Note that by inequality (9.6) of Chapter 1 we have

$$L(m,0)/L_M = \binom{N_1}{M} \Big/ \binom{N}{M} \le (N_1/N)^M$$

$$\leq \exp\left\{-2M\frac{m}{n}\left(1-\frac{m+5}{2n}\right)\right\}. \tag{9.12}$$

Set

$$l(m,i) = \frac{L(m,i)}{L(m,i-1)} = \frac{N-N_1-2i+2}{2i}\frac{(M-2i+2)(M-2i+1)}{(N_1-M+2i-1)(N_1-M+2i)}$$

and note that for a fixed value of m the ratio $l(m,i)$ is a decreasing function of i. In fact, if $1 \leq i < j$, then

$$l(m,j) \leq \frac{i}{j} l(m,i)$$

and so

$$L(m,j) \leq \frac{\{l(m,1)\}^j}{j} L(m,0). \tag{9.13}$$

In order to prove (9.10) we shall decompose the range of m into three intervals and show that the sum over each of these intervals is $o(1)$.

(a) Suppose that $2 \leq m \leq 10n/(\log n)^2$. Then

$$\begin{aligned} l(m,1) &= \frac{N-N_1}{2}\frac{M(M-1)}{(N_1-M+1)(N_1-M+2)} \\ &\leq \frac{mn}{2}\frac{(2n\log n)^2}{(N-mn-M)^2} \leq 100. \end{aligned}$$

Since

$$l(m,i) \leq (1/i)l(m,1),$$

this shows that

$$L(m) \leq c_0 L(m,0)$$

for some absolute constant c_0, say 100^{100}. Therefore by (9.12)

$$\begin{aligned} L(m)/L_M &\leq c_1 \exp\left\{-2M\frac{m}{n}\left(1-\frac{m}{2n}\right)\right\} \\ &\leq c_1 \exp\left[-m\{\log n + \omega(n)\}\left(1-\frac{m}{2n}\right)\right] \\ &\leq c_1 \exp\{-m\log n - \omega(n)m + (m^2/n)\log n\} \\ &\leq \exp\left\{-m\log n - \frac{1}{2}\omega(n)m\right\}. \end{aligned}$$

Summing over the m in our range, we find that

$$\sum_m (n)_m L(m)/L_M \leq \sum_m \exp\left\{-\frac{1}{2}\omega(n)m\right\} = o(1).$$

(b) Now let us turn to the largest interval we shall consider:

$$10n/(\log n)^2 \le m \le n - n^{3/4}(\log n)^2.$$

It is easily checked that in this range $l(m,1) \ge 4$.

Put

$$j = \lfloor 2l(m,1) \rfloor.$$

Then

$$l(m, j+1) \le \frac{l(m,1)}{j+1} \le \frac{l(m,1)}{2l(m,1)} = \frac{1}{2}$$

so, estimating rather crudely,

$$L(m) \le 2\sum_{i=1}^{j} \frac{\{l(m,1)\}^i}{i} L(m,0) \le 3\{l(m,1)\}^{2l(m,1)} L(m,0). \tag{9.14}$$

Since

$$N_1/N \le \left\{ \binom{n-m}{2} + m/2 + 2 \right\} \Big/ N \le \left(\frac{n-m}{n}\right)^2 (1 + n^{-1/2}),$$

by (9.12) we have

$$\log\{L(m,0)/L_M\} \le 2M \log\{(n-m)/n\} + Mn^{-1/2}. \tag{9.15}$$

Furthermore,

$$N_1 - M > \frac{2}{5}(n-m)^2$$

so

$$l(m,1) \le \frac{n^2}{4} \frac{(2n\log n)^2}{\left\{\frac{2}{5}n^{3/2}(\log n)^4\right\}^2} < 7n/(\log n)^6.$$

Hence by (9.14) and (9.15) we have

$$\sum (n)_m L(m)/L_M = o(1)$$

for the sum over the range at hand, if, say,

$$(m+2)\log n + 14\frac{n}{(\log n)^6}\log n + 2M \log\frac{n-m}{n} + Mn^{-1/2} < 0. \tag{9.16}$$

The derivative of the left-hand side with respect to m is

$$\log n - 2M/(n-m) < 0$$

so it suffices to check (9.16) for the minimal value of m, namely $m = \lceil 10n/(\log n)^2 \rceil$. Since

$$2M \ge n\{\log n + \omega(n)\} \text{ and } \log\{(n-m)/n\} \le -m/n,$$

the left-hand side of (9.16) is at most

$$2\log n + 14n/(\log n)^5 - \omega(n)m + 2n^{1/2}\log n < 15n/(\log n)^5 - m < 0,$$

as required.

(c) Finally, suppose that

$$m \geq n - n^{3/4}(\log n)^2.$$

In this range the crudest estimates will suffice. Since $N_2 \leq N/2$,

$$\begin{aligned} L(m,i)/L_M &= \binom{N_2}{i}\binom{N_1}{M-2i}\Big/\binom{N}{M} \\ &\leq \frac{(N/2)^i}{i!}\frac{N_1^{M-2i}}{(M-2i)!}\frac{M!}{(N-M)^M} = h(m,i). \end{aligned}$$

If $2(i+1) \leq M$, we have

$$\frac{h(m,i+1)}{h(m,i)} = \frac{N}{2(i+1)}\frac{N_1^2}{(M-2i)(M-2i-1)} \geq \frac{n^4}{8M^3} > 2,$$

as $N_1 \geq n/2$ holds for every m. Furthermore, at the maximal value of i, $\lfloor M/2 \rfloor$, we have

$$h(m, \lfloor M/2 \rfloor) \leq n^4 M^{M/2}/(N-M)^{M/2} \leq n^{-3n}.$$

Consequently, in our range we have

$$\sum (n)_m L(m)/L_M \leq \sum_m (n)_m 2h(m, \lfloor M/2 \rfloor) \leq n^{-n}.$$

completing the proof of our theorem. □

Let us see now how Theorem 9.4 allows us to translate results concerning random labelled graphs into results about random unlabelled graphs, as claimed in Chapter 2 and in the introduction of the present chapter. Although it is intuitively obvious, let us define what we mean by a random unlabelled graph. Consider the set of all $U_M = U_{n,M}$ unlabelled graphs of order n and size M, and turn it into a probability space by taking all elements equiprobable. Denote by $\mathcal{G}^u(n,M)$ this probability space; denoted by $G_M^u = G_{n,M}^u$, are *random unlabelled graphs of order* n *and size* M. Write $P_M^u(\cdot)$ for the probability in the space $\mathcal{G}(n,M)$.

Theorem 9.5 *Let Q be a property of graphs of order n and let $M = M(n)$ satisfy (9.2), i.e. $2M/n - \log n \to \infty$ and $2(N-M)/n - \log n \to \infty$. Then*

$$P_M(Q) \leq \{1 + o(1)\}P_M^u(Q).$$

In particular, a.e. $G_M \in \mathcal{G}(n,M)$ has Q iff a.e. $G_M^u \in \mathcal{G}^u(n,M)$ has Q.

Proof Let

$$\begin{aligned} U(Q) &= \{G \in \mathcal{G}^u(n, M) : G \text{ has } Q\}, \\ L(Q) &= \{G \in \mathcal{G}(n, M) : G \text{ has } Q\}, \end{aligned}$$

and set $u(Q) = |U(Q)|$ and $l(Q) = |L(Q)|$.

A graph of order n is isomorphic to at most $n!$ elements of $\mathcal{G}(n, M)$, so

$$l(Q) \le n!u(Q).$$

Hence, by Theorem 9.4,

$$\begin{aligned} P_M(Q) &= l(Q)/L_M \le n!u(Q)/L_M \\ &\le \{1 + o(1)\}n!u(Q)/n!U_M \\ &= \{1 + o(1)\}u(Q)/U_M = \{1 + o(1)\}P^u_M(Q). \end{aligned}$$

To see the second assertion, note that if $P_M(Q) = 1 + o(1)$, then $P^u_M(Q) = 1 + o(1)$, and if $P^u_M(Q) = 1 + o(1)$, then $P^u_M(\neg Q) = o(1)$ so $P_M(\neg Q) = o(1)$ and $P_M(Q) = 1 + o(1)$. □

It can be shown that condition (9.2) is not only sufficient but it is also necessary (see Ex. 3).

Corollary 9.6 *If Q is a property of graphs of order n, $0 < c < 1$, and M satisfies (9.2), then*

$$\lim_{n\to\infty} P_M(Q) = c \text{ iff } \lim_{n\to\infty} P^u_M(Q) = c. \qquad \square$$

Despite Theorem 9.5 and Corollary 9.6, the model $\mathcal{G}^u(n, M)$ has to be treated with caution. For example, $P_M(Q) \sim P^u_M(Q)$ need not hold if $P_M(Q)$ is not bounded away from 0 or $P^u_M(Q)$ is not bounded away from 1 (see Ex. 4). More importantly, Theorem 2.1, concerning monotone properties, does not hold for unlabelled graphs. We do not even have to look far to find a property showing this, for one of the simplest properties, connectedness, will do. Denote by $p_u(n, M)$ the probability that $G^u_M \in \mathcal{G}^u(n, M)$ is connected. Wright (1972) proved that for every $k \in \mathbb{N}$ there is an $n = n_0(k)$ such that

$$p_u(n, N - n - l) > p_u(n, N - n - l + 1)$$

for all $l, 0 \le l \le k$.

Wright (1972, 1973*b*, 1974*a*, *c*, 1975*a*, 1976), Walsh (1979) and Walsh and Wright (1978) carried out a detailed study of various spaces of unlabelled graphs [relying on exact enumeration, in the vein of Gilbert

(1956), rather than on the probabilistic approach] including the space of all unlabelled graphs of order n and the space of all unlabelled graphs of size M. For example, it is easily seen that for every $k \geq 1$, almost all unlabelled graphs on n vertices are k-connected (see Ex. 5). On the other hand, somewhat paradoxically, though almost all unlabelled graphs without an isolated vertex on M edges are connected, almost none of them are 2-connected.

The automorphisms of trees were studied by Schwenk (1977) and Harary and Palmer (1979). Among others, Harary and Palmer showed that the probability of a fixed point in a random tree of order n tends to $0.6995\ldots$ as $n \to \infty$.

Although this book is on random finite graphs, it is appropriate to say a few words about random infinite graphs. In §1 of Chapter 11 we shall study the cliques of the initial sections of elements of $\mathcal{G}(\mathbb{N}, p)$, the space of random graphs introduced in §1 of Chapter 2. What happens if we ignore the order of the vertex set, i.e. if we construct random graphs by joining elements of a countable set at random, with a fixed probability p, independently of each other? It is trivial to see that a.e. $G_{\infty,p} \in \mathcal{G}(\mathbb{N}, p)$ has property P_k for every $k \in \mathbb{N}$ and hence, by the back-and-forth argument, $G_{\infty,p}$ is, up to isomorphism, unique (see the proof of Theorem 2.6 for a concrete example of such a graph) and independent of p. Thus, picking a countable graph at random, almost surely we shall pick a graph isomorphic to *the* random graph G_0. This was observed by Erdős and Rényi (1963) and the graph G_0 was explicitly constructed by Rado (1964).

In the proof of Theorem 2.6 we gave a slick construction of G_0: here is a more down-to-earth one. Let $(A_1, B_1), (A_2, B_2), \ldots$ be an enumeration of all pairs of disjoint finite subsets of $\mathbb{N}$ such that $A_1 = B_1 = \emptyset$ and $\max A_j \cup B_j \leq j-1$ for $j \geq 2$. To define G_0, for $1 \leq i < j$ join i to j iff $i \in A_j$. In fact, a rather sparse pregraph of G_0 determines G_0 up to isomorphism (Ex. 6).

What can we say about the automorphisms of G_0? Since if we pick an element of $\mathcal{G}(\mathbb{N}, p)$ at random, we almost surely pick a graph isomorphic to G_0, Aut G_0 is far from being trivial, in sharp contrast with the automorphism group of a random finite graph. Indeed, it is immediate that Aut G_0 acts vertex transitively and even transitively on all finite subgraphs. Cameron (1984) studied Aut G_0 in detail; Truss (1985) proved that it is simple.

9.2 The Asymptotic Number of Unlabelled Regular Graphs

Are we justified in concentrating on random labelled regular graphs? Can we translate results about random labelled regular graphs into results about random unlabelled regular graphs? The following theorem of Bollobás (1982*c*) answers these questions in the affirmative.

Theorem 9.7 *Let $r \geq 3$ be fixed and denote by $L_r(n)$ the number of labelled r-regular graphs of order n and by $U_r(n)$ the number of unlabelled r-regular graphs of order n. Then, provided rn is even,*

$$U_r(n) \sim L_r(n)/n \sim \mathrm{e}^{-(r^2-1)/4}(rn)!/\{(rn/2)!2^{rn/2}(r!)^n n!\}. \qquad \square$$

The second relation is just Corollary 2.17, but the proof of the first relation is more complicated than that of Theorem 9.4. This is only to be expected since the graphs in Theorem 9.7 have many fewer edges than those in Theorem 9.4 and, furthermore, when proving Theorem 9.7, we have to work with a fairly complicated model of random graphs. Of course, the basic aim is the same: we have to prove the analogue of relation (9.3). Instead of presenting the fairly involved proof, we shall just pinpoint some of the crucial steps.

To start with, recall the machinery set up in the proof of Theorem 2.16. In particular, $m = rn/2$ and $N(m)$ is the number of configurations associated with labelled r-regular graphs of order n. We know from the proof of Theorem II.16 that if $0 < c_0 < \mathrm{e}^{-(r^2-1)/4}$ and n is sufficiently large, then

$$L_r(n) \geq c_0 N(m)/(r!)^n.$$

Let us estimate the probability that a random graph $G \in \mathcal{G}(n, r\text{-reg})$ contains a fixed set of $l = l(n)$ edges. In Chapter 2 we considered the case when l is fixed: here we need a crude bound valid for all functions $l(n)$. Clearly there are at most r^{2l} sets of l pairs that are mapped into our l edges. There are $N(m-l)$ configurations that contain l given pairs so, if n is sufficiently large, the probability above is at most

$$\begin{aligned} r^{2l}N(m-l)/\{c_0 N(m)\} &= \frac{1}{c_0} r^{2l} N(m-l)/N(m) \\ &= \frac{1}{c_0} r^{2l}\{(2m-1)(2m-3)\ldots(2m-2l+1)\}^{-1} \\ &\leq \frac{1}{c_0} r^{2l}\{(2m-2)!\}^{-l/(2m-1)} \leq \left(\frac{c_1}{n}\right)^l. \qquad (9.17) \end{aligned}$$

In the proof of Theorem 9.4 it was sufficient to find an upper bound on $I(\rho)$, the number of labelled graphs invariant under a permutation $\rho \in S_n$, in terms of the number of fixed points of ρ, acting on V. Here we need a finer partition of S_n; let $M(s; s_2, s_3)$ be the set of permutations in S_n that move s vertices and have s_2 2-cycles and s_3 3-cycles. Thus if $M(s; s_2, s_3) \neq \emptyset$, then $2s_2 + 3s_2 \leq s$; furthermore, $M(0;0,0) = \{1\}, M(1; s_2, s_3) = \emptyset$ and, rather crudely,

$$|M(s; s_2, s_3)| \leq n^s / \{s_2! s_3!\}. \tag{9.18}$$

Then the heart of the proof is a careful analysis of the orbits of $\rho \in M(s; s_2, s_3)$ acting on $V^{(2)}$ and hence, using (9.17), a fairly careful estimate of $I(\rho)/L_r(n)$ for $\rho \in M(s; s_2, s_3)$, good enough to give the result when combined with (9.18).

McKay and Wormald (1984) proved that the first relation in Theorem 9.7 holds even if $r = r(n)$ is a rather fast growing function of n, namely if $r = o(n^{1/2-\varepsilon})$ for some $\varepsilon > 0$. It is interesting to note that the extension to the case $r \sim n/2$ which, intuitively, seems to be obvious, is not covered by this extension and is unlikely to be easy.

As an immediate consequence of Theorem 9.7, we obtain analogues of Theorem 9.5 and Corollary 9.6 for regular graphs. Define $P_{r\text{-reg}}(\cdot)$, $P^u_{r\text{-reg}}(\cdot)$, $G_{r\text{-reg}}$ and $G^u_{r\text{-reg}}$ in the natural way.

Theorem 9.8 *Let $r \geq 3$ be fixed and let $n \to \infty$ such that rn is even. Let Q be a property of graphs of order n. Then*

$$P_{r\text{-reg}}(Q) = \{1 + o(1)\} P^u_{r\text{-reg}}(Q),$$

Q holds for a.e. $G_{r\text{-reg}}$ iff it holds for a.e. $G^u_{r\text{-reg}}$ and $\lim_{n\to\infty} P_{r\text{-reg}}(Q) = c, 0 < c < 1$, iff $\lim_{n\to\infty} P^u_{r\text{-reg}}(Q) = c$. □

We close this brief section with a result resembling Theorem 9.7 but outside the scope of this book: Babai (1980*c*) proved that a.e. Steiner triple system is asymmetric, i.e., has a trivial automorphism group. Note however, that a Steiner triple system on n points has fairly many triples: every point is contained in $(n-1)/2$ triples, so the lack of symmetry is not too surprising.

9.3 Distinguishing Vertices by Their Distance Sequences

If M is neither too small nor too large [to be precise, if it satisfies (9.2)] then a.e. G_M has trivial automorphism group. Similarly, for $r \geq 3$, a.e. $G_{r\text{-reg}}$ has trivial automorphism group. However, for an arbitrary graph it is rather difficult to decide whether its automorphism group is trivial or not. This is especially so if the graph is regular. Is there then a fast algorithm which, for a.e. G_M and a.e. $G_{r\text{-reg}}$ decides whether the automorphism group is trivial or not?

The canonical labelling algorithm, discussed in §5 of Chapter 3, was precisely such an algorithm. However, that algorithm was based on large gaps in the degree sequence which we do not have for G_M if M is fairly small, say $M \le n^{6/5}$, and certainly do not have for $G_{r\text{-reg}}$. In spite of this, a sequence closely related to the degree sequence, the so-called distance sequence, enables us to distinguish the vertices of a.e. G_M and a.e. $G_{r\text{-reg}}$.

The *distance sequence* of a vertex x of a graph is $\{d_i(x)\}_1^n$, where $d_i(x)$ is the number of vertices at distance i from x. Thus the first term of the distance sequence, $d_1(x)$, is precisely the degree of x.

The following two theorems are due to Bollobás (1982*b*); for the proofs the reader is referred to the original paper.

Theorem 9.9 *Suppose $\omega(n) \to \infty$ and*

$$(n/2)\{\log n + \omega(n)\} \le M \le n^{13/12}.$$

Then a.e. G_M is such that for every pair of vertices (x, y) there is an $l, 1 \le l \le l_0 = 3\lceil\{(\log n)/\log(M/n)\}^{1/2}\rceil$, with $d_l(x) \ne d_l(y)$. □

The second theorem concerns regular graphs. We do know from Corollary 2.19 that for all $r \ge 3$ and $g \ge 3$ there is an $\varepsilon(r, g) > 0$ such that if n is sufficiently large, then with probability at least $\varepsilon(r, g)$ the girth of $G_{r\text{-reg}}$ is greater than g. Consequently, if n is large enough, with probability at least $\varepsilon(r, 2k) > 0$, for every vertex x the first k terms of the distance sequence $\{d_i(x)\}_1^n$ are precisely $r, r(r-1), r(r-1)^2, \dots, r(r-1)^{k-1}$. Nevertheless, later members of the distance sequence do distinguish vertices of regular graphs.

Theorem 9.10 *Let $r \ge 3$ and $\varepsilon > 0$ be fixed and set $l_0 = \lfloor(\frac{1}{2} + \varepsilon)\log n/\log(r-1)\rfloor$. Then a.e. r-regular labelled graph of order n is such that every vertex x is uniquely determined by $\{d_i(x)\}_1^{l_0}$.* □

In fact, the proof of Theorem 9.10 shows that it suffices to consider only the terms $d_i(x)$ with i close to l_0: putting $l_1 = l_0 + \lceil 3/\varepsilon\rceil + 3$, a.e. r-regular labelled graph of order n is such that if x and y are distinct vertices then $d_i(x) \ne d_i(y)$ for some $i, l_0 \le i \le l_1$.

The theorems above can be used to parallel Theorem 3.17 for spaces ($\mathcal{G}_M$ and $\mathcal{G}_{r\text{-reg}}$) whose members are hardly distinguished by their degree sequences. We state only a crude consequence of Theorem 10.

Theorem 9.11 *For every fixed $r \geq 3$ there is an algorithm which, for a.e. $G \in \mathscr{G}(n, r\text{-reg})$, tests in $O(n^2)$ time, for any graph H, whether H is isomorphic to G or not.*

Proof Imitate the proof of Theorem 3.17, putting a graph $G \in \mathscr{G}(n, r\text{-reg})$ into $\mathscr{K}$ iff the vertices of G are distinguished by the distance sequences. Order these distance sequences lexicographically. □

We would not like to give the impression that research on the graph isomorphism problem is closely related to the theory of random graphs: this is certainly not the case, although random algorithms are often faster than deterministic ones. The main and very substantial body of research on the graph isomorphism problem is outside the scope of this book; for earlier results the reader is referred to Read and Corneil (1977) and for more recent results, many of which are based on the theory of permutation groups, the reader could consult, among others, Babai (1980*a*, *b*, 1981), Babai, Grigoryev and Mount (1982), Filotti, Miller and Reif (1979), Furst, Hopcroft and Luks (1980), Hoffmann (1980), Hopcroft and Tarjan (1972, 1974), Hopcroft and Wong (1974), Lichtenstein (1980), Luks (1980), Mathon (1979), Miller (1978, 1979, 1980) and Zemlyachenko (1975). For example, Luks (1980) proved that isomorphism of graphs of bounded degree can be tested in polynomial time (cf. Theorem 9.11).

9.4 Asymmetric Graphs

A graph whose automorphism group is trivial is said to be *asymmetric*, otherwise it is *symmetric*. We know from §1 that almost every graph of order n is asymmetric: almost no $G_{1/2}$ has a non-trivial automorphism. (In fact, as we remarked earlier, this assertion is considerably weaker than Wright's theorem; see Ex. 1.) But how far are most graphs from being symmetric? How many edges do we have to change (add and delete) to turn most graphs into symmetric graphs? And what is the maximum of the number of changes that may be needed for a graph of order n? These questions were posed by Erdős and Rényi (1963), who also gave almost complete answers to them.

The *degree of asymmetry* of a graph G with vertex set V is

$$A(G) = \min\{|E(G)\Delta E(H)| : H \text{ is a symmetric graph on } V\},$$

i.e. $A(G)$ is the minimal number of total changes (additions and deletions of edges) symmetrizing G. The *degree of local asymmetry* of G is

$$A^*(G) = \min\{|E(G)\Delta E(H)| : \text{Aut } H \text{ contains a transposition}\}.$$

Erdős and Rényi (1963) proved the following upper bounds on $A(n)$, the maximal degree of asymmetry of a graph of order n, and on $A^*(n)$, the maximal degree of local asymmetry of a graph of order n.

Theorem 9.12 $A(n) \le A^*(n) \le (n-1)/2$.

Proof Let G be a graph of order n. Clearly

$$A(G) \le A^*(G) = \min_{\substack{x,y\in G\\ x\neq y}} |A(x,y)|,$$

where

$$\begin{aligned} A(x,y) &= \Gamma(x)\Delta\Gamma(y) - \{x,y\} \\ &= \{z \in V(G) - \{x,y\} : z \text{ is joined to precisely one of } x \text{ and } y\}. \end{aligned}$$

For every vertex $z \in V(G)$ there are $2d(z)\{n-1-d(z)\}$ ordered pairs (x,y) with $z \in A(x,y)$. Hence

$$\sum_x \sum_{y\neq x} |A(x,y)| = 2\sum_z d(z)\{n-1-d(z)\} \le 2n\{(n-1)/2\}^2.$$

Therefore

$$A(G) \le A^*(G) \le \frac{1}{n(n-1)} \sum_x \sum_{y\neq x} |A(x,y)| \le (n-1)/2,$$

as claimed. □

The proof above shows that $A^*(G) = (n-1)/2$ if and only if G is $(n-1)$-regular and $|A(x,y)| = (n-1)/2$ for any two distinct vertices x and y, i.e. if for any two distinct vertices there are precisely $(n-1)/2$ vertices in different relation to x than to y. Graphs with this property are the so-called *conference graphs* (see §3 of Chapter 13), the prime examples of which are the Paley graphs (see §2 of Chapter 13).

Erdős and Rényi (1963) showed that the bound above is essentially best possible and, even more, a.e. $G_{1/2}$ shows that the bound is essentially the best possible.

Theorem 9.13 *A.e.* $G \in \mathscr{G}(n, \frac{1}{2})$ *satisfies*

$$A(G) = \{1 + o(1)\}n/2.$$ □

A natural way of proving this theorem is to proceed as in the proof of Theorem 9.3. The difference is that instead of estimating $I(\rho)$, we have to give an upper bound for $I(\rho, \varepsilon)$, the number of graphs which can be turned into ρ-invariant graphs by changing at most $(1-\varepsilon)(n/2)$ edges, where $\varepsilon > 0$ is fixed. If $\rho \in S_n$, and after changing h edges of a graph G the new graph belongs to $\mathcal{G}(\rho)$, then those orbits of ρ, acting on $V^{(2)}$, which consist only of edges of G or only of non-edges of G, make up $V^{(2)}$ pairs. What this means in practice is that the bound $M_1 \leq \binom{u-m}{2} + m/2$ appearing in the proof of Theorem 9.3 has to be replaced by $M_1 \leq \binom{u-m}{2} + m/2 + 2h$.

It is easily seen that a graph of order n with degree of asymmetry about $n/2$ must have about $n^2/4$ edges. As shown by Erdős and Rényi (1963), if we specify that our graph has precisely M edges, then the bound in Theorem 9.12 can be improved (see Ex. 8); furthermore, once again the degree of asymmetry of a.e. G_M is close to being maximal, provided M is neither too large nor too small.

Theorem 9.14 *(i) Every graph of order n and average degree d has degree of asymmetry at most* $2d\{1 - d/(n-1)\}$.

(ii) Suppose $M = M(n) = (n/2)d(n) \in \mathbb{N}$ *satisfies*

$$M/(n \log n) \to \infty \text{ and } (N - M)/(n \log n) \to \infty.$$

Then

$$A(G_M) = \{2 + o(1)\}d\left(1 - \frac{d}{n-1}\right)$$

almost surely.

Theorems 9.12 and 9.13 show that

$$A(n) = \max_{|G|=n} A(G) = \left\{\tfrac{1}{2} + o(1)\right\} n. \tag{9.19}$$

Spencer (1976) found an ingenious way of improving (9.19) considerably, by taking care of local and global symmetries separately. Given a graph G and a permutation ρ of $V = V(G)$, put $B_\rho(G) = |E(G) \Delta E\{\rho(G)\}|$. Furthermore, let

$$B(G) = \min_{\rho \neq 1} B_\rho(G) \text{ and } B(n) = \max_{|G|=n} B(G).$$

Thus each of $A(G), A^*(G)$ and $B(G)$ measures the asymmetry of G, with each invariant being 0 if G is symmetric. As $A^*(G)$ measures the asymmetry of G with respect to transpositions, $B(G) \leq 2A^*(G)$ so $B(n) \leq$

$2A^*(n)$. Furthermore, it is easily seen that $B(G) \le 2A(G) \le 2A^*(G)$ so, in fact, $B(n) \le 2A(n) \le 2A^*(n)$ (Ex. 9).

Spencer (1976) proved that these inequalities are rather close to being equalities.

Theorem 9.15 *If n is sufficiently large, then*

$$A^*(n) - 200 \le \tfrac{1}{2}B(n) \le A(n) \le A^*(n). \qquad (9.20)$$

Furthermore,

$$n/2 - \{1 + o(1)\}(n \log n)^{1/2} \le \tfrac{1}{2}B(n) \le A(n) \le A^*(n) \le (n-1)/2. \quad (9.21)$$

□

Just a few words about the proof. It is easily shown that a.e. $G \in \mathscr{G}(n, \frac{1}{2})$ is such that $A^*(G) = (n/2) - \{1 + o(1)\}(n \log n)^{1/2}$; in fact, this is an immediate consequence of the fact that each $|A(x, y)|$ has binomial distribution with parameters $n-2$ and $\frac{1}{2}$. In the main part of the proof one shows that if $A^*(n) \ge 0.49n$, and n is sufficiently large, then (9.20) holds. This is done by picking a graph G with $A^*(G) = A^*(n)$ and replacing G by $G \Delta H$, where H is the union of 100 random sets of $\lfloor n/2 \rfloor$ independent edges (not necessarily in G). Almost equivalently, H is a random 200-regular graph. It turns out that a.e. H destroys all global symmetries, i.e. symmetries which are not transpositions.

For some values of n one can do much better than (9.21): if there is a conference graph of order n, then $A^*(n) = (n-1)/2$ so $(n-1)/2 - 200 \le A(n) \le (n-1)/2$. In particular, as pointed out by Erdős and Rényi (1963), for every prime power q satisfying $q \equiv 1 \pmod 4$ there is a Paley graph P_q of order q, we have $(q-1)/2 - 200 \le A(q) \le (q-1)/2$. Spencer (1976) conjectured that $A^*(n) = n/2 + O(1)$ and so $A(n) = n/2 + O(1)$. In fact, it seems likely that $A(n) = (n-1)/2$ for infinitely many values of n.

9.5 Graphs with a Given Automorphism Group

In §1 we proved considerable extensions of the assertion that a.e. labelled graph of order n has no non-trivial automorphisms (see Ex. 1). This rather easy assertion prompted Cameron (1980) to ask for which groups H it is true that a.e. graph G on n labelled vertices satisfying $H \le \operatorname{Aut} G$ satisfies $H = \operatorname{Aut} G$ as well. To be precise, for a finite group H, let $a_n(H)$ be the proportion of those graphs G on n labelled vertices with $H \le \operatorname{Aut} G$ which satisfy $H = \operatorname{Aut} G$. For which groups H is it then true that $\lim_{n\to\infty} a_n(H) = 1$? Cameron (1980) proved some results implying a complete answer to this question: here we state only one theorem, made up of several attractive consequences of the main result. Earlier related results had been proved by Sheehan (1968), making use of his extension (Sheehan, 1967) of Pólya's enumeration theorem.

Theorem 9.16 (*i*) $\lim_{n\to\infty} a_n(H) = a(H)$ *exists for every finite group H and it is a rational number.*

(*ii*) $a(H) = 1$ *if and only if H is a direct product of symmetric groups.*

(*iii*) *If H is Abelian but not an elementary Abelian 2-group then* $a(H) = 0$.

(*iv*) *The values of* $a(H)$ *for metabelian groups H are dense in* $[0, 1]$. □

The result above is in striking contrast with the case of Cayley graphs. Babai and Godsil (1982) conjectured that, unless a group H belongs to a known class of exceptions, almost all Cayley graphs of H have H for their full automorphism group. Though this assertion is somewhat cryptic, we do not expand on it; Cayley graphs will make another appearance in §1 of Chapter 13.

Exercises

9.1 Without relying on any of the results in this chapter, give a simple proof of the fact that a.e. $G \in \mathscr{G}(n, \frac{1}{2})$ has trivial automorphism group.

9.2 Define an appropriate model $\mathscr{G}^u(n,p)$ and state and prove an analogue of Theorem 9.5 for the models $\mathscr{G}(n,p)$ and $\mathscr{G}^u(n,p)$.

9.3 (cf. Theorem 9.5.) Let $M = (n/2)(\log n + x)$ where $x \to c, c \in \mathbb{R}$, and let Q be the property of having at least two isolated vertices. Sketch a proof of the fact that

$$\underline{\lim} P_M(Q)/P^u_M(Q) > 1.$$

9.4 Let M satisfy (9.2), G_0 be a graph of order n and size M with a non-trivial automorphism and let Q be the property of being isomorphic to G_0. Show that

$$P_M(Q) \le \left\{\tfrac{1}{2} + o(1)\right\} P^u_M(Q).$$

9.5 Deduce from the proof of Theorem 9.12 that if G is a graph of order n with degree of asymmetry $(n-1)/2$, then $n \equiv 1 \pmod 4$.

9.6 A *pregraph* with vertex set V is a triple $P = (V, E', E'')$ such that $E', E'' \subset V^{(2)}$ and $E' \cap E'' = \emptyset$. The set E' is the set of *edges* and E'' is the set of *non-edges* (and $V^{(2)} \backslash E' \cup E''$ is the set of undecided pairs, which may be turned into either edges or non-edges). A graph $G = (V, E)$ is said to contain P if $E' \subset E \subset V^{(2)} \backslash E''$.

Now let $P = (\mathbb{N}, E', E'')$ be defined by $E' = \{ij : 1 \leq i < j, i \in A_j\}$ and $E'' = \{ij : 1 \leq i < j, i \in B_j\}$, where $(A_1, B_1), (A_2, B_2), \ldots$ are as after Corollary 9.6. Show that every graph containing P is isomorphic to the infinite random graph G_0. Deduce that for some sequence $\varepsilon_k \to 0$ there is a pregraph $P = (\mathbb{N}, E', E'')$ for which

$$|\{i : i < k, ik \in E'\} \cup \{j : j < k, jk \in E''\}| \leq \varepsilon_k k$$

and every graph containing P is isomorphic to G_0.

9.7 Let $k \geq 1$. Deduce from Theorem 9.5 that almost all unlabelled graphs on n vertices are k-connected (Walsh and Wright, 1978).

9.8 Prove Theorem 9.14(i) by imitating the proof of Theorem 9.12. [Note that $\sum_z d(z)\{n - 1 - d(z)\} = n(n-1)d - \sum_z d^2(z) \leq n(n-1)d - nd^2$.]

9.9 Check that $B(G) \leq 2A(G)$ for every graph G.

10
The Diameter

The *diameter* of a graph G, denoted by diam G, is the maximal distance between pairs of vertices of G. A graph is disconnected iff its diameter is ∞, so one always studies the diameter of a connected graph.

The diameter, one of the simplest graph invariants, is often encountered in various applications of graph theory, especially in the theory of communication networks and in the study of computational complexity based on breadth-first search, so it is certainly worthwhile to investigate the diameter of a random graph. As an unexpected bonus, we find that several results about random graphs happen to give the best bounds known at present on some important functions involving the diameter.

In the first section we present a brief review of the results concerning large graphs of given maximal degree and small diameter. The next two sections are devoted to the models $\mathcal{G}(n, p)$, $\mathcal{G}(n, M)$ and $\mathcal{G}(n, r\text{-reg})$. In §4 we examine the diameter of the sparsest connected random graphs G_M, namely the diameter at the hitting time of connectedness in a graph process. The final section contains several related results, including theorems of Burtin concerning graph invariants which are finer than the mere diameter.

10.1 Large Graphs of Small Diameter

Graphs of small diameter are of interest as examples of efficient communication networks. It is natural to impose the condition that no degree is large so one arrives at the problem of determining or at least estimating the function

$$n(D, \Delta) = \max\{|G| : \text{diam } G \le D, \Delta(G) \le \Delta\}.$$

Here D and Δ are natural numbers and $\Delta \ge 2$. This innocent-looking problem is perhaps the simplest case of several more general problems posed by Erdős and Rényi (1962), and Murty and Vijayan (1964); in this form it seems to be due to Elspas (1964). In spite of its innocent appearance, the problem is very resilient; we are still far from a satisfactory solution. For reviews of this problem and other related questions see Bollobás (1978*a*, chapter IV) and Bermond and Bollobás (1982).

A cycle of length $2D+1$ shows that $n(D,2) = 2D+1$ for all $D \in \mathbb{N}$. Furthermore, as in a graph of maximal degree Δ there are at most $\Delta(\Delta-1)^{k-1}$ vertices at distance k from a vertex, we have the following obvious upper bound on $n(D,\Delta)$.

Theorem 10.1 $n(D,2) = 2D+1$ *for all* $D \in \mathbb{N}$*; if* $\Delta \geq 3$*, then*

$$\begin{aligned} n(D,\Delta) &\leq 1 + \Delta\{1 + (\Delta-1) + \ldots + (\Delta-1)^{D-1}\} \\ &= \{\Delta(\Delta-1)^D - 2\}/(\Delta-2) = n_0(D,\Delta) \end{aligned}$$

The bound in Theorem 10.1 is usually called the *Moore bound*, and the graphs showing equality are the *Moore graphs of diameter D and degree* Δ. It is clear from the definition of $n_0(D,\Delta)$ that a Moore graph of diameter D and degree Δ is a Δ-regular graph of girth $2D+1$ and order $n_0(D,\Delta)$. This description may also be taken as the definition of a Moore graph. It is unfortunate that there are very few Moore graphs: Hoffman and Singleton (1960) proved that if there is a Moore graph of diameter 2 and degree $\Delta \geq 3$, then $\Delta \in \{3,7,57\}$, and Damerell (1973) and Bannai and Ito (1972) proved that there is no Moore graph for $D \geq 3$ and $\Delta \geq 3$. In fact, Moore graphs do exist for $D = 2$ and $\Delta = 3$ and 7, but it is not known whether there is a Moore graph of diameter 2 and degree 57.

Though there are only few Moore graphs, it is difficult to improve substantially the upper bound $n_0(D,\Delta)$. For $D = 2$ Erdős, Fajtlowicz and Hoffman (1980) proved that if Δ is even and at least 4, then $n(2,\Delta) \leq \Delta^2 - 1 = n_0(2,\Delta) - 2$. However, we do not know whether $\sup_\Delta\{n_0(2,\Delta) - n(2,\Delta)\} = \infty$; or even more, it is not even known whether $\sup_{D,\Delta}\{n_0(D,\Delta) - n(D,\Delta)\} = \infty$.

Of course, the relation $\sup_{D,\Delta}\{n_0(D,\Delta) - n(D,\Delta)\} < \infty$ would show that the trivial upper bound $n_0(D,\Delta)$ is, in fact, almost the correct value of $n(D,\Delta)$. Sadly, the lower bounds for $n(D,\Delta)$ we do know at the moment are rather far from $n_0(D,\Delta)$. It is precisely here that random graphs come in: several of the best bounds follow from results on random graphs. However, this is for later: in the present section we present bounds obtained by constructions. Although this book is on random graphs, it would be unreasonable to deny that constructions, especially simple constructions, are more informative than bounds based on random graphs.

After various constructions given by Elspas (1964), Akers (1965), Friedman (1966, 1971), Korn (1967), Storwick (1970), Memmi and Raillard (1982) and others, substantially better constructions were found by Bermond, Delorme and Farhi (1982, 1984), Delorme (1985), Delorme and Farhi (1984), Leland and Solomon (1982), Leland (1981), Leland *et al.* (1981) and Jerrum and Skyum (1982); for a survey, see Bermond *et al.* (1983).

Several of these constructions are based on the de Bruijn graph. Let $h, k \geq 2$ be natural numbers and set $W = \{1, 2, \ldots, h\}^k$. The *de Bruijn graph* $B(h,k)$ has vertex set W and every vertex $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ is joined to every vertex $(*, a_1, a_2, \ldots, a_{k-1})$ (forward shift) and to every vertex $(a_2, a_3, \ldots, a_k, *)$ (backward shift), where $*$ denotes an arbitrary element of $\{1, 2, \ldots, h\}$. The following result is immediate from the definition.

Theorem 10.2 *The de Bruijn graph $B(h,k)$ has order h^k, maximal degree $2h$ and diameter at most k. In particular, if $\Delta \geq 2$ is even, then*

$$n(D, \Delta) \geq (\Delta/2)^D. \tag{10.1}$$

□

Bermond, Delorme and Farhi (1982, 1984) used a new product of graphs to construct graphs of small diameter and obtained particularly good results for small values of D and Δ. Products of graphs based on finite geometries give the following considerable improvement on $n(3, \Delta)$.

Theorem 10.3 *If q is an odd prime and $\Delta = 3(q+1)/2$ is an integer, then there is a graph of order $(8\Delta^3 - 12\Delta^2 + 18\Delta)/27$, maximal degree Δ and diameter 3.* □

Set $c(D) = \underline{\lim}_{\Delta \to \infty} n(D, \Delta)/n_0(D, \delta) = \underline{\lim}_{\Delta \to \infty} n(D, \Delta)\Delta^{-D}$. Although it seems likely that $c(D) = 1$ for all $D \geq 1$, it is not known that the infinum of $c(D)$ is positive. By Theorem 10.3 one has $c(3) \geq 8/27$, and Bermond, Delorme and Farhi (1982) obtained the following lower bounds on $c(D)$ for small values of D.

Theorem 10.4 $c(3) \geq 8/27, c(4) \geq 3/16, c(5) \geq 1/32, c(6) \geq 2/81, c(7) \geq 2^{-7}, c(8) \geq 3 \cdot 2^{-8}, c(9) \geq 3 \cdot 2^{-10}$ *and* $c(10) \geq 3 \cdot 2^{-19}$. □

What can we say about $n(D, \Delta)$ for a fixed value of Δ and large values of D? Leland and Solomon (1982) constructed cubic graphs of small diameter and large order. For $k \in \mathbb{N}, k \geq 2$, the Leland–Solomon graph

G_k on the vertex set $V = \{0,1\}^k$ of the k-dimensional cube by joining a vertex $(a_1, a_2, \ldots, a_k)$ to the vertices $(a_2, a_3, \ldots, a_k, \bar{a}_1), (\bar{a}_k, a_1, a_2, \ldots, a_{k-1})$ and $(a_1, a_2, \ldots, a_{k-2}, \bar{a}_{k-1}, \bar{a}_k)$, where $\bar{a} = 0$ if $a = 1$ and $\bar{a} = 1$ if $a = 0$.

Theorem 10.5 *The Leland–Solomon graph G_k is a cubic graph of order 2^k and diameter at most $3k/2$.* □

Let $H_1, H_2, \ldots$ be explicitly constructed graphs of maximal degree Δ with $|H_k| \to \infty$. As a measure of the efficiency of this construction let us take

$$\lambda_\Delta = \inf \{\lambda : \text{ diam } H_k \le \{\lambda + o(1)\} \log_2 |H_k|, k = 1, 2, \ldots\}.$$

The smaller the λ_Δ value of a sequence is, the better the construction is. From the Moore bound we know that $\lambda_\Delta \ge \log_{\Delta-1} 2$ for any $\Delta \ge 3$ and any sequence of graphs; for any even $\Delta \ge 4$ the constant belonging to the sequence of de Bruijn graphs is $\lambda_\Delta = \log_{\Delta/2} 2$. The Leland–Solomon graphs achieve $\lambda_3 = 1.5$. This was improved by Leland (1981) and Jerrum and Skyum (1982) to $\lambda_3 = 1.472169$.

In fact, Jerrum and Skyum constructed infinite sequences of low diameter graphs of maximal degree Δ for every Δ between 3 and 30, and managed to obtain surprisingly small λ_Δ's. For example, their sequences of graphs give $\lambda_5 = 0.676820$, $\lambda_9 = 0.417864$ and $\lambda_{17} = 0.296702$; the Moore bound tells us that we cannot do better than 0.5, 0.33… and 0.25.

The ingenious construction of Jerrum and Skyum is based on the de Bruijn graphs: a fixed graph H is inserted into each vertex of a de Bruijn graph. If in H the average distance between pairs of vertices is small and the edges joining the copies of H are chosen cleverly, then the new graph turns out to have small diameter. For all but the case $\Delta = 3$, Jerrum and Skyum took H to be one of the 12-cages constructed by Benson (1966).

10.2 The Diameter of G_p

The diameter of a r.g. in $\mathcal{G}(n,p)$ has been studied by a great many authors, including Moon and Moser (1966), Korshunov (1971*b*), Burtin (1973*a, b*, 1974, 1975), Trahtenbrot and Barzdin (1973), Thanh (1977, 1979), Bollobás (1981*b*, 1984*a*) and Klee and Larman (1981). Burtin examined several graph invariants related to the diameter and containing considerably more information about the graph than the mere numerical value of the diameter.

The main aim of this section is to prove, loosely speaking, that for most values of p, almost all graphs G_p have precisely the same diameter.

As we mentioned in §1, this result gives a surprisingly good bound on $n(D, \Delta)$. Our presentation is based on Bollobás (1981*b*).

In order to study the diameter, we shall examine the sets of vertices within a given distance from a certain vertex. Denote by $\Gamma_k(x)$ the set of vertices at distance k from a vertex x in a graph $G \in \mathscr{G}(n, p)$:

$$\Gamma_k(x) = \{y \in G : d(x, y) = k\}$$

and write $N_k(x)$ for the set of vertices within distance k from x:

$$N_k(x) = \bigcup_{i=0}^{k} \Gamma_i(x).$$

Thus diam $G \leq d$ iff $N_d(x) = V(G)$ for every vertex x, and diam $G \geq d$ iff there is a vertex y for which $N_{d-1}(y) \neq V$.

Why does a.e. G_p have small diameter, provided p is not too small? Because a random graph is likely to be 'spreading': given a not too large subset W of V, with large probability G_p has almost $pn|W|$ vertices adjacent to vertices in W. Thus, with large probability, the number of neighbours of a vertex $x, d(x) = |\Gamma_1(x)|$, is not much smaller than pn; the number of vertices at distance 2, $|\Gamma_2(x)|$, is not much smaller than $(pn)^2$; and so on, the number of vertices at distance k, $|\Gamma_k(x)|$, is not much smaller than $(pn)^k$, where, say, $d = d(n) = 2k$. Now if $|\Gamma_k(x)|$ and $|\Gamma_k(y)|$ are sufficiently large, then, with large probability, either $\Gamma_k(x) \cap \Gamma_k(y) \neq \emptyset$ or else G_p contains a $\Gamma_k(x) - \Gamma_k(y)$ edge. Hence, with large probability, diam $G_p \leq 2k + 1 = d + 1$.

When we try to justify the steps above, we encounter two problems. First, the exceptional probability we work with must be kept rather small since the estimates have to be carried out about $d(n)$ times for each vertex. To make sure that the sum of the exceptional probability is still small, we shall work with concrete constants rather than constants $c_1, c_2, \ldots$, and we shall avoid terms of the form $O(n^{-k})$, $O(1)$, etc. As concrete constants are rather unpleasant to work with, we shall keep our estimates very crude indeed. Secondly, we have to try to make sure that in each subproblem we tackle we can work with independent events. This is why we shall keep estimating conditional probabilities.

In preparation for our main result, we need four lemmas. In these lemmas we shall suppose that $0 < p = p(n) < 1$, $d = d(n)$ is a natural number, $d \geq 2, p^d n^{d-1} = \log(n^2/c)$ for some positive constant c and $pn/\log n \to \infty$ as $n \to \infty$. As our final conclusion will be that in a range of p and d, slightly smaller than the range given just now, almost every G_p

has diameter d or $d+1$, the restriction on p is not too severe. Indeed, we know that if $\underline{\lim}_{n\to\infty} P(G_p$ is connected$) = \underline{\lim}_{n\to\infty} P(\text{diam } G_p < \infty) > 0$, then $p \geq (\log n + c_0)/n$ for some constant c_0. We also know that if p is bounded away from 0, or even if just $pn^{1/2-\varepsilon}$ is bounded away from 0, then diam $G_p \leq 2$ for a.e. G_p (see Theorem 2.6), so we may assume that $p = o(n^{-1/2+\varepsilon})$ for every $\varepsilon > 0$.

Note that

$$p = n^{1/d-1}\{\log(n^2/c)\}^{1/d}$$

and

$$d = \{\log n + \log\log n + \log 2 + O(1/\log n)\}/\log(pn),$$

so the maximum of d is $\{1+o(1)\}\log n/\log\log n$. Clearly

$$(pn)^{d-1} = \log(n^2/c)/p = o(n),$$

and so $p(pn)^{d-2} = o(1)$. As we are interested in large values of n, we may and shall assume that $n \geq 100$, $pn > 100\log n$, $(pn)^{d-2} < n/10$ and so $p(pn)^{d-2} < 1/10$.

Lemma 10.6 *Let x be a fixed vertex, let $1 \leq k = k(n) \leq d-1$, and let $K = K(n)$ satisfy*

$$6 \leq K < (pn/\log n)^{1/2}/12.$$

Denote by $\Omega_k \subset \mathcal{G}(n,p)$ the set of graphs for which $a = |\Gamma_{k-1}(x)|$ and $b = |N_{k-1}(x)|$ satisfy

$$\tfrac{1}{2}(pn)^{k-1} \leq a \leq \tfrac{3}{2}(pn)^{k-1}$$

and

$$b \leq 2(pn)^{k-1}.$$

Set

$$\alpha_k = K\{\log n/(pn)^k\}^{1/2},\ \beta_k = p(pn)^{k-1} \text{ and } \gamma_k = 2(pn)^{k-1}/n = 2\beta_k/pn.$$

Then

$$P\left\{\left||\Gamma_k(x)| - apn\right| \geq (\alpha_k+\beta_k+\gamma_k)apn \,\middle|\, \Omega_k\right\} \leq n^{-K^2/9}.$$

Proof How do we find the sets $\Gamma_{k-1}(x)$ and $N_{k-1}(x)$? First we test which vertices are adjacent to x, then which vertices are adjacent to $\Gamma_1(x)$, and so on, up to $\Gamma_{k-2}(x)$. At each stage we have to test pairs of vertices, at least one of which belongs to $N_{k-2}(x)$. Hence the probability that a vertex $y \notin N_{k-1}(x)$ is joined to some vertices in $\Gamma_{k-1}(x)$, conditional on Ω_k, is precisely $p_a = 1-(1-p)^a$. Clearly, p_a satisfies the inequality

$$pa(1-pa/2) \le p_a \le pa.$$

Our remarks imply that, conditional on Ω_k, the random variable $|\Gamma_k(x)|$ has binomial distribution with parameters $n_k = n-b$ and p_a. Since $(pn)^{k-1} \le (pn)^{d-2} < n/10$, we have $b \le 2(pn)^{k-1} < n/5$, and so $4n/5 < n_k \le n, ap(n-n_k) \le \gamma_k\, apn$ and $(ap-p_a) \le \beta_k ap$. Therefore, by Theorem 1.7(i) we have

$$\begin{aligned}
&P\left(\big||\Gamma_k(x)|-apn\big| \ge (\alpha_k+\beta_k+\gamma_k)apn \,\Big|\, \Omega_k\right)\\
&\le P\left(\big||\Gamma_k(x)|-apn_k\big| \ge (\alpha_k+\beta_k)apn_k \,\Big|\, \Omega_k\right)\\
&\le P\left(\big||\Gamma_k(x)|-p_a n_k\big| \ge \alpha_k apn_k \,\Big|\, \Omega_k\right)\\
&\le (\alpha_k^2 p_a n_k)^{-1/2}\exp\{-\alpha_k^2 p_a n_k/3\} \le \exp\{-\alpha_k^2 p_a n_k/3\}\\
&\le \exp\{-\alpha_k^2 (pn)^k/9\} = n^{-K^2/9}.
\end{aligned}$$

Theorem 1.7(i) could be applied since

$$\begin{aligned}
0 < p_a &\le pa \le \tfrac{3}{2}p(pn)^{k-1} \le \tfrac{3}{2}p(pn)^{d-2} < \tfrac{1}{2},\\
0 < \alpha_k &= K\{\log n/(pn)^k\}^{1/2} \le K\{\log n/(pn)\}^{1/2} < 1/12,
\end{aligned}$$

and

$$\alpha_k p_a(1-p_a)n_k \ge (K/2)\{\log n/(pn)^k\}^{1/2}\tfrac{3}{10}(pn)^k \ge 2K > 12. \qquad \square$$

Lemma 10.7 *Let $K > 12$ be a constant and define $\alpha_k, \beta_k, \gamma_k, k = 1, 2, \ldots, d-1$, as in Lemma 10.6. Set*

$$\delta_k = \exp\left\{2\sum_{l=1}^{k}(\alpha_l+\beta_l+\gamma_l)\right\} - 1.$$

If n is sufficiently large, then with probability at least $1-n^{-K-2}$ for every vertex x and every natural number k, $1 \le k \le d-1$, we have

$$\big||\Gamma_k(x)| - (pn)^k\big| \le \delta_k (pn)^k.$$

Proof The conditions imply that $\delta_{d-1} \to 0$ as $n \to \infty$, so we may assume that $\delta'_{d-1} < \frac{1}{4}$.

Let x be a fixed vertex and denote by Ω_k^* the set of graphs for which

$$\big||\Gamma_l(x)| - (pn)^l\big| \le \delta_l (pn)^l, \quad 0 \le l \le k.$$

Clearly, $\Omega_k^* \subset \Omega_{k-1}^* \subset \Omega_k$.

We shall prove by induction that

$$1 - P(\Omega_k^*) \le 2kn^{-K^2/9} \tag{10.2}$$

for every $k, 0 \le k \le d-1$. For $k = 0$ there is nothing to prove. Assume that $1 \le k < d-1$ and (10.2) holds for smaller values of k. Clearly

$$1 - P(\Omega_k^*) = 1 - P(\Omega_{k-1}^*) + P(\Omega_{k-1}^*)P\{||\Gamma_k(x)| - (pn)^k| \ge \delta_k(pn)^k \,|\, \Omega_{k-1}^*\}.$$

Now if $G \in \Omega_{k-1}^*$, then $a = |\Gamma_{k-1}(x)|$ satisfies $|(pn)^k - apn| \le \delta_{k-1}(pn)^k$. Therefore

$$\begin{aligned}
&P\left\{||\Gamma_k(x)| - (pn)^k| \ge \delta_k(pn)^k \,\middle|\, \Omega_{k-1}^*\right\}\\
&\quad \le P(\Omega_{k-1}^*)^{-1}P\left\{||\Gamma_k(x)| - apn| \ge (\delta_k - \delta_{k-1})(pn)^k \,\middle|\, \Omega_k\right\}\\
&\quad \le \left\{1 - 2(k-1)n^{-K^2/9}\right\}^{-2}P\left\{||\Gamma_k(x)| - apn| \ge 2(\alpha_k + \beta_k + \gamma_k)(pn)^k \,\middle|\, \Omega_k\right\}\\
&\quad \le 2P\left\{||\Gamma_k(x)| - apn| \ge (\alpha_k + \beta_k + \gamma_k)apn \,\middle|\, \Omega_k\right\}\\
&\quad \le 2n^{-K^2/9}.
\end{aligned}$$

The last inequality holds because of Lemma 10.6, and the second inequality holds since $dn^{-K^2/9} < 1$. Consequently

$$1 - P(\Omega_k^*) \le 2(k-1)n^{-K^2/9} + 2n^{-K^2/9} = 2kn^{-K^2/9},$$

proving (10.2). Lemma 10.7 is an immediate consequence of inequality (10.2). □

Lemmas 10.6 and 10.7 tell us that, with probability close to 1, the sets $\Gamma_1(x), \Gamma_2(x), \ldots, \Gamma_{d-1}(x)$ do grow at the required rate. The next two lemmas, which we shall state only, show that, with probability close to 1, two given vertices are far from each other. These lemmas enable one to prove that the diameter of G_p is unlikely to be small.

Given distinct vertices x and y, and a natural number k, define

$$\begin{aligned}
\Gamma_k^*(x,y) = \{&z \in \Gamma_k(x) \cap \Gamma_k(y) :\\
&\Gamma(z) \cap \{\Gamma_{k-1}(x) - \Gamma_{k-1}(y)\} \ne \emptyset \text{ and } \Gamma(z) \cap \{\Gamma_{k-1}(y) - \Gamma_{k-1}(x)\} \ne \emptyset\}.
\end{aligned}$$

Denote by $\Pi_k \subset \mathscr{G}(n,p)$ the set of graphs satisfying $|\Gamma_{k-1}(x)| \le 2(pn)^{k-1}$ and $|\Gamma_{k-1}(y)| \le 2(pn)^{k-1}$. Pick a constant $K > e^7$ and for $1 \le k \le d/2$ define $c_k = c_k(n,p,K)$ by

$$c_k 4p^{2k}n^{2k-1} = (K+4)\log n,$$

and put

$$m_k = m_k(n,p,K) = 2(K+4)\log n/\log c_k.$$

Finally, for $d/2 < k \le d$, set $m_k = m_k(n,p) = 2p^{2k}n^{2k-1}$.

Lemma 10.8 *If n is sufficiently large, then for every $k, 1 \le k \le d-1$, we have*

$$P\left\{|\Gamma_k^*(x,y)| \ge m_k \,\middle|\, \Pi_k\right\} \le n^{-K-4}. \qquad \square$$

Lemma 10.9 *If n is sufficiently large, then, with probability at least $1-n^{-K}$, the following assertions hold.*
(i) *For every vertex x,*

$$|N_{d-2}(x)| < 2(pn)^{d-2} \text{ and } |\Gamma_{d-1}(x) - (pn)^{d-1}| \le \delta_{d-1}(pn)^{d-1},$$

where δ_{d-1} is the number defined in Lemma 10.7.
(ii) *For distinct vertices x and y,*

$$|N_{d-1}(x) \cap N_{d-1}(y)| \le 8p^{2d-2}n^{2d-3}$$

and

$$|\Gamma\{N_{d-1}(x) \cap N_{d-1}(y)\}| \le 16p^{2d-1}n^{2d-2}.$$

We are ready to present the main result of the section, from Bollobás (1981*b*).

Theorem 10.10 *Let c be a positive constant, $d = d(n) \ge 2$ a natural number, and define $p = p(n,c,d)$, $0 < p < 1$, by*

$$p^d n^{d-1} = \log(n^2/c).$$

Suppose that $pn/(\log n)^3 \to \infty$. Then in $\mathcal{G}(n,p)$ we have

$$\lim_{n\to\infty} P(\text{diam } G = d) = e^{-c/2} \text{ and } \lim_{n\to\infty} P(\text{diam } G = d+1) = 1 - e^{-c/2}.$$

Proof Though, strictly speaking, we do not know yet that a.e. G_p has diameter at least d and at most $d+1$, it is clear from the statement of our theorem that diam $G_p \le d+1$ and diam $G_p \ge d$ almost surely. This will be proved by considering the number of pairs of vertices 'far' from each other.

If for some vertices $x, y \in G$ we have $y \notin N_d(x)$ [equivalently, $x \notin N_d(y)$], then we say that x is *remote from* y and we call (x, y) a *remote pair*. Let $X = X(G)$ be the number of remote pairs of vertices in G. We shall show that the distribution of X tends to the Poisson distribution with parameter $c/2$. Assuming $P(\text{diam } G_p \le d-1) + P(\text{diam } G_p \ge d+2) = o(1)$, this is more than enough to imply the assertion of the theorem.

Our first aim is to prove that almost no G_p contains two remote pairs sharing a vertex. Let x, y and z be fixed distinct vertices. By Lemma 10.7 we have

$$P\{|N_{d-1}(x)| < \tfrac{5}{6}(pn)^{d-1}\} < n^{-4}$$

provided n is sufficiently large: $n \geq n(p,d)$. The probability that y is joined to no vertex in a set $W \subset V(G) - \{y\}, |W| \geq \frac{5}{6}(pn)^{d-1}$, is

$$(1-p)^{|W|} \leq \exp\{-\tfrac{5}{6}p(pn)^{d-1}\} = \exp\{-\tfrac{5}{6}\log(n^2/c)\} = c^{5/6}n^{-5/3}.$$

Consequently,
$P(x$ is remote from both y and $z)$

$$\begin{aligned}
&\leq P\{|N_{d-1}(x)| < \tfrac{5}{6}(pn)^{d-1}\} \\
&\quad + P\left\{\{y,z\} \cap N_d(x) = \varnothing \middle| \mid N_{d-1}(x) \mid \geq \tfrac{5}{6}(pn)^{d-1}\right\} \\
&\leq n^{-4} + c^{5/3}n^{-10/3} < n^{-3-1/4}.
\end{aligned}$$

Therefore the probability that G_p contains two remote pairs sharing a vertex is at most

$$n\binom{n}{2}n^{-3-1/4} < n^{-1/4}.$$

A similar argument shows that, for every fixed r, the rth factional moment of X is within $o(1)$ of the expected number of ordered r-tuples of disjoint remote pairs. In turn, this implies that

$$E_r(X) = (n)_r 2^{-r} F_r\{1 + o(1)\} + o(1), \tag{10.3}$$

where F_r is the probability that a fixed r-tuple $\tau = (x_1, \ldots, x_r)$ of vertices consists of vertices remote from other vertices. The factor 2^{-r} is due to the fact that r disjoint pairs of vertices contain $2^r r$-sets of vertices remote from some other vertices. For $1 \leq i \leq r$ write

$$\begin{aligned}
A_i &= \Gamma_{d-1}(x_i) - \bigcup_{j \neq i} N_{d-1}(x_j), \\
T &= \bigcap_{i \neq j}\{N_{d-1}(x_i) \cap N_{d-1}(x_j)\}, \\
S &= V(G) - \bigcup_{j=1}^{r} N_{d-1}(x_j), \\
S' &= S - \Gamma(T), \\
a_i &= |A_i|,\ s = |S|,\ s' = |S'| \ \text{ and } \ t = |T|.
\end{aligned}$$

Let $K = \max\{r+2, e^7\}$. Then, by Lemma 10.9, if n is sufficiently large, with probability at least $1 - n^{-K}$ we have

$$\begin{aligned} |a_i - (pn)^{d-1}| &\le \delta_{d-1}(pn)^{d-1} + 8rp^{2d-2}n^{2d-3} \\ &= (pn)^{d-1}[\delta_{d-1} + 8r\{\log(n^2/c)\}/(pn)] = \delta(pn)^{d-1}, \quad (10.4) \\ n &\ge s \ge s' \ge n - 8r^2p^{2d-1}n^{2d-2} = (1-\varepsilon)n. \quad (10.5) \end{aligned}$$

We claim that the functions δ and ε defined here satisfy

$$\delta \log n \longrightarrow 0 \text{ and } \varepsilon \longrightarrow 0.$$

Indeed, the first relation holds since $pn/(\log n)^3 \to \infty$, and, if n is large,

$$\begin{aligned} \delta_{d-1} &\le 3\sum_{l=1}^{d-1}(\alpha_l + \beta_l + \gamma_l) \le 4(\alpha_1 + \beta_{d-1} + \gamma_{d-1}) \\ &= 4\left\{K\left(\frac{\log n}{pn}\right)^{1/2} + p^{d-1}n^{d-2} + 2p^{d-2}n^{d-3}\right\} \\ &\le 4\left\{K\left(\frac{\log n}{pn}\right)^{1/2} + \frac{3\log n}{pn} + \frac{6\log n}{(pn)^2}\right\}. \end{aligned}$$

Furthermore, $\varepsilon \to 0$ since

$$p^{2d-1}n^{2d-3} = (p^d n^{d-1})^2/(pn) < (3\log n)^2/pn \longrightarrow 0.$$

Denote by $P'(\cdot)$ the probability conditional on a particular choice of the sets A_i, S and S', satisfying (10.4) and (10.5). In order to estimate F_r, we shall estimate the conditional probability $Q_r = P'$ (τ consists of remote vertices). Put

$$R_r = P'(\forall i,\ 1 \le i \le r,\ \exists y_i \in S \text{ not joined to } A_i)$$

and

$$R_r' = P'(\forall i,\ 1 \le i \le r,\ \exists y_i \in S' \text{ not joined to } A_i, i = 1, \ldots, r).$$

Clearly, $R_r' \le Q_r \le R_r$. Furthermore,

$$R_r = \prod_{i=1}^{r}\{1 - (1 - (1-p)^{a_i})^s\},$$

and R_r' is given by an analogous expression.

In order to estimate R_r from above, note that

$$(1-p)^{a_i} \le e^{-pa_i} \le e^{-p^d n^{d-1}(1-\delta)} = (c/n^2)\{1 + o(1)\},$$

so $R_r \leq (c/n)^r\{1 + o(1)\}$. Similarly, R_r' can be estimated from below as follows:

$$\begin{aligned}(1-p)^{a_i} \geq \mathrm{e}^{-pa_i(1+p)} \geq \mathrm{e}^{-p^d n^{d-1}(1+p)(1+\delta)} &= (c/n^2)\{1+o(1)\},\\ \{1-(1-p)^{a_i}\}^{s'} \leq 1-(s'c/n^2)\{1+o(1)\} &= 1-(c/n)+o(1/n).\end{aligned}$$

Consequently $Q_r = (c/n)^r\{1 + o(1)\}$.

Since (10.4) and (10.5) hold with probability at least $1 - n^{-K}$,

$$(1-n^{-K})Q_r \leq F_r \leq (1-n^{-K})Q_r + n^{-K},$$

so $F_r = (c/n)^r\{1 + o(1)\}$. Therefore (10.3) implies

$$E_r(X) = n^r 2^{-r}(c/n)^r\{1+o(1)\} + o(1) = (c/2)^r + o(1). \tag{10.6}$$

As so often before, we invoke Theorem 1.20 and conclude from (10.6) that $X \xrightarrow{d} P_{c/2}$, as claimed. In particular,

$$P(\text{diam } G_p \leq d) = P(X = 0) \longrightarrow \mathrm{e}^{-c/2}. \tag{10.7}$$

Now the proof of our theorem is completed easily. If $d = 2$, then clearly

$$P(\text{diam } G_p \leq 1) = P(G_p = K^n) = p\binom{n}{2} \longrightarrow 0.$$

Since the property of having diameter at most k is monotone, by Theorem 2.1 if $0 < p_1 < p_2 < 1$, then $P(\text{diam } G_{p_1} \leq k) \leq P(\text{diam } G_{p_2} \leq k)$. Define $c_1 = c_1(n)$ and $c_2 = c_2(n)$ by

$$p^{d-1}n^{d-2} = \log(n^2/c_1) \text{ and } p^{d+1}n^d = \log(n^2/c_2).$$

For $d \geq 3$ we find that $c_1 \to \infty$ so (10.7) implies that

$$P(\text{diam } G_p \leq d-1) \longrightarrow 0. \tag{10.8}$$

Also, for $d \geq 2$ we have $c_2 \to 0$, so (10.7) gives

$$P(\text{diam } G_p \leq d+1) \to 1. \tag{10.9}$$

The assertion of the theorem is precisely the union of the three relations (7), (10.8) and (10.9). □

As an immediate consequence of Theorem 10.10, we find that in a large range of p almost every graph G_p has the same diameter. A similar assertion holds for the model $\mathscr{G}(n, M)$.

Corollary 10.11 *(i) Suppose $p^2n - 2\log n \to \infty$ and $n^2(1-p) \to \infty$. Then a.e. G_p has diameter 2.*

(ii) Suppose the function $M = M(n) < \binom{n}{2}$ satisfies

$$2M^2/n^3 - \log n \longrightarrow \infty.$$

Then a.e. G_M has diameter 2.

Both assertions are best possible.

Proof The first condition in (i) ensures that $P(\text{diam } G_p \le 2) \to 1$. As $P(\text{diam } G_p = 1) = P(G_p = K^n) = p^{\binom{n}{2}}$, $P(\text{diam } G_p \ge 2) \to 1$ iff $n^2 \log p \to -\infty$.

Assertion (ii) follows from (i) and Theorem 2.2. □

Corollary 10.12 *(i) Suppose that functions $d = d(n) \ge 3$ and $0 < p = p(n) < 1$ satisfy*

$$(\log n)/d - 3\log\log n \longrightarrow \infty,$$
$$p^d n^{d-1} - 2\log n \longrightarrow \infty \quad \text{and} \quad p^{d-1}n^{d-2} - 2\log n \to -\infty.$$

Then a.e. G_p has diameter d.

(ii) Suppose the functions $d = d(n) \ge 3$ and $M = M(n)$ satisfy

$$(\log n)/d - 3\log\log n \to \infty,$$
$$2^{d-1}M^d n^{-d-1} - \log n \to \infty \quad \text{and} \quad 2^{d-2}M^{d-1}n^{-d} - \log n \to -\infty.$$

Then a.e. G_M has diameter d.

Both assertions are best possible.

Proof Part (i) is an immediate consequence of Theorem 10.10; in fact, we could say that this was proved in the final section of the proof of Theorem 10.10. This is how we can deduce it from the theorem itself. Let K_1 and K_2 be positive constants and define $0 < p_1 < p_2 < 1$ by

$$p_1^{d+1}n^d = \log(n^2/K_1) \text{ and } p_2^d n^{d-1} = \log(n^2/K_2).$$

Then $p_1 < p < p_2$ if n is sufficiently large and so

$$\overline{\lim}_{n\to\infty} P(\text{diam } G_p \ge d+1) \le \overline{\lim}_{n\to\infty} P(\text{diam } G_{p_1} \ge d+1) = 1 - e^{-K_1/2}$$

and

$$\overline{\lim}_{n\to\infty} P(\text{diam } G_p \le d-1) \le \overline{\lim}_{n\to\infty} P(\text{diam } G_{p_2} \le d-1) = e^{-K_2/2}.$$

As K_1 may be chosen arbitrarily small and K_2 arbitrarily large, the assertion follows.

The property of having diameter d is convex, so (ii) follows from Theorem 2.2. □

These results imply that if Δ is considerably larger than D, then $n(D,\Delta)$ is not too far from $n_0(D,\Delta)$. Unfortunately the lower bound we get still does not imply that $\overline{\lim}_{D\to\infty,\Delta\to\infty} n(D,\Delta)/n_0(D,\Delta) > 0$.

Corollary 10.13 *Suppose* $0 < \varepsilon < 1$ *and the sequences* $(D_k), (\Delta_k)$ *are such that*

$$D_k^4 \le \Delta_k \textit{ and } D_k \longrightarrow \infty.$$

Then if k *is sufficiently large,*

$$n(D_k, \Delta_k) \ge \frac{\{(1-\varepsilon)\Delta_k\}^{D_k}}{2D_k \log \Delta_k}.$$

Proof Set $n_k = \lceil \{(1-\varepsilon)\Delta_k\}^{D_k}/(2D_k \log \Delta_k)\rceil$ and define

$$p_k = n_k^{1/D_k - 1}(2\log n_k + \log\log n_k)^{1/D_k}.$$

Then, by Corollary 10.12, a.e. graph in $\mathscr{G}(n_k, p_k)$ has diameter at most D_k. We know also that a.e. graph has maximal degree about $p_k n_k$ (see Corollary 3.14), say a.e. graph has maximal degree at most

$$p_k n_k (1-\varepsilon)^{-1/3} \le n_k^{1/D_k}(1-\varepsilon)^{-1/3}(2\log n_k)^{1/D_k}(1-\varepsilon)^{-1/3} < \Delta_k,$$

provided k is sufficiently large. □

10.3 The Diameter of Random Regular Graphs

The proof Corollary 10.13 shows that if Δ is considerably larger than D, then random graphs G_p are likely to imply good lower bounds on $n(D,\Delta)$. How can we use random graphs to obtain lower bounds on $n(D,\Delta)$ if Δ is small, say constant, and D is large? Clearly the model $\mathscr{G}(n,p)$ is of no use for this, since if G_p is likely to be connected then its maximal degree is likely to be at least $\log n$. The model to consider is clearly $\mathscr{G}(n, r\text{-reg})$, the space of r-regular graphs; as we shall see, this model does give a good lower bound for $n(D,r)$.

If $r \ge 3$ is fixed or is a not too fast growing function of n, then almost all r-regular graphs have almost the same diameter. The aim of this section is to present this result of Bollobás and de la Vega (1982). Let us start with an upper bound on the diameter of a.e. graph.

Theorem 10.14 *Let $r \geq 3$ and $\varepsilon > 0$ be fixed and let $d = d(n)$ be the least integer satisfying*

$$(r-1)^{d-1} \geq (2+\varepsilon)rn\log n.$$

Then a.e. r-regular graph of order n has diameter at most d.

Proof We shall omit most of the details but will give some of the underlying ideas.

Recall from Chapter 2 that elements of $\mathcal{G}(n, r\text{-reg})$ are obtained as images of configurations, i.e. images of partitions of $\bigcup_{i=1}^n W_i$ into pairs (edges), where $W_1, W_2, \ldots, W_n$ are disjoint r-sets. Let F be a configuration and let W_i, W_j be classes. Define the *distance* $d(W_i, W_j) = d_F(W_i, W_j)$ between W_i and W_j in F as the minimal k for which one can find classes $W_{i_0} = W_i, W_{i_1}, \ldots, W_{i_k} = W_j$ such that for every $h, 0 \leq h \leq k-1$, some edge of F joins W_{i_h} to $W_{i_{h+1}}$. If there is no such k, then the distance between W_i and W_j is said to be infinite. The diameter of F is diam $F = \max_{1 \leq i < j \leq n} d(W_i, W_j)$. By Corollary 2.17 the theorem follows if we show that diam $F \leq d$ for a.e. configuration F.

The proof of this resembles the proof of Theorem 10.10. Let $t_1 = \lfloor d/2 \rfloor$ and $t_2 = \lceil d/2 \rceil - 1$. We wish to show that for a fixed class, say W_1, and any integer $k \leq t_1$, with probability close to 1, the set $\Gamma_k(W_1)$ of classes at distance k from W_1 is rather large; furthermore, there are many edges joining the classes in $\Gamma_k(W_1)$ to the classes in $\Gamma_{k+1}(W_1)$. The final step is then to show that, with probability tending to 1, and two classes, say W_1 and W_2, are such that, either they are within distance $d-1$ or else some class in $\Gamma_{t_1}(W_1)$ is joined to some class in $\Gamma_{t_2}(W_2)$.

As in the proof of Theorem 10.10, the key is to keep our choices independent as far as possible. In fact, in the proof it is convenient to use a recursive definition of a configuration, rather than the, admittedly very simple, original definition.

We shall construct a random configuration by picking edges one by one, taking those nearest to a fixed class, say W_1, first. To be precise, we shall construct sets E_i, S_i and M_i in such a way that S_i will be the set of indices j with $d(W_1, W_j) = i$ in the final configuration, E_i will turn out to be the set of edges incident with the classes at distance less than i from W_1 and M_i will be the set of vertices (members of the classes W_j) not incident with any edge in E_i. Thus to get E_{i+1} from E_i, we add to E_i all the edges incident with the vertices in $L_i = M_i \cap (\bigcup_{j \in S_i} W_j)$.

By the remarks above, it is clear that we shall set $E_0 = \emptyset, S_0 = \{1\}$ and $M_0 = W = \bigcup_{j=1}^n W_j$. Suppose we have defined E_i, S_i and M_i. In order to define E_{i+1}, S_{i+1} and M_{i+1}, we pass through a number of intermediate stages, corresponding to random selections of single edges.

Set $E_i^{(0)} = E_i, S_i^{(0)} = \emptyset, M_i^{(0)} = M_i$ and $L_i^{(0)} = L_i = M_i \cap (\bigcup_{l \in S_i} W_l)$. The set L_i is the set of elements of classes at distance i from W_1 which are not (and will not be) joined to classes nearer to W_1. Suppose we have defined $E_i^{(j)}, S_i^{(j)}, M_i^{(j)}$ and $L_i^{(j)}$. If $L_i^{(j)} = \emptyset$ (so we can no longer add edges incident with classes at distance i from W_1, for we have run out of free elements) then put $E_{i+1} = E_i^{(j)}, S_{i+1} = S_i^{(j)}, M_{i+1} = M_i^{(j)}$ and $L_{i+1} = M_{i+1} \cap (\bigcup_{j \in S_{i+1}} W_j)$. Otherwise pick a vertex $x \in L_i^{(j)}$ (say take the first vertex in $L_i^{(j)}$ in some predefined order or just take a random vertex in $L_i^{(j)}$), give all vertices in $M_i^{(j)} - \{x\}$ the same probability, and choose one of them, say y, at random. Add the edge xy to our configuration to be constructed: set $E_i^{(j+1)} = E_i^{(j)} \cup \{(x, y)\}, L_i^{(j+1)} = L_i^{(j)} - \{x, y\}$ and $M_i^{(j+1)} = M_i^{(j)} - \{x, y\}$. Finally, if $y \in W_l$ and $l \notin S_i$, then set $S_i^{(j+1)} = S_i^{(j)} \cup \{l\}$, otherwise put $S_i^{(j+1)} = S_i^{(j)}$.

Since $|M_i^{(j+1)}| = |M_i^{(j)}| - 2$ and $L_i^{(j+1)} \subset M_i^{(j+1)}$, the process does terminate so it does define E_{i+1}, S_{i+1} and M_{i+1}.

What is the significance of the sets E_i, S_i, M_i for a random configuration? After a certain number of steps we must arrive at $E_{k+1} = E_k$ and so $S_{k+1} = \emptyset$. If $M_k = \emptyset$, then we have constructed a random configuration. If $M_k \neq \emptyset$, then M_k is a union of some entire classes W_j. Pick one of these classes, say W_2, and repeat the process for M_k and W_2 instead of W and W_1. Having ground to a halt, once again check whether we have got an entire configuration. If not, then what we have is a partition of some entire classes W_j, so pick a new class, say W_3, and continue the process. When, finally, the process does grind to a halt, we have selected a random configuration.

Fortunately, there is no need to construct an entire random configuration: we may stop with E_k, S_k and M_k, where k is the minimal natural number with $E_{k+1} = E_k$. Then E_k is precisely the edge set of the component of a random configuration containing W_1 in the following sense: for every $i \leq k$ the probability that $E_i = \tilde{E}$ is the same as the probability that $\tilde{E}$ is the set of edges incident with the classes at distance less than i from W_1.

The description above, of course, does nothing to justify the claims at the beginning of the proof, but it does make our task fairly pleasant. Nevertheless, for the details we refer the reader to Bollobás and de la Vega (1982). □

It is, perhaps, a little surprising that it is more troublesome to give a good lower bound for the diameter of a.e. regular graph. The following result, whose proof we omit, is also from Bollobás and de la Vega (1982).

Theorem 10.15 *For a fixed natural number $r \geq 3$, the diameter of a.e. r-regular graph of order n is at least*

$$\lfloor \log_{r-1} n \rfloor + \lfloor \log_{r-1} \log n - \log_{r-1}\{6r/(r-2)\} \rfloor + 1. \qquad \square$$

By Theorems 10.14 and 10.15, for every fixed $r \geq 3$, the diameters of almost all graphs take only boundedly many values; in fact, the results show that if r is large, then for many values of n the diameter tends to take only one of three possible values. With considerably more work one could show that for some sequences $n_k \to \infty$ and $d_j \to \infty$ a.e. r-regular graph of order n_k has diameter d_k or $d_k + 1$. Thus the diameter of a random r-regular graph is also almost constant.

If we restrict our attention to r-regular graphs of large girth, then one can show that there are r-regular graphs of slightly smaller diameter than guaranteed by Theorem 10.14. Namely, if $r \geq 3$ and $\varepsilon > 0$ are fixed and

$$d = d(n) = \left\lceil \log_{r-1} \left(\frac{2+\varepsilon}{r} n \log n \right) \right\rceil + 1,$$

then for every large enough n there is an r-regular graph of order n and diameter at most d. This gives us the following bound on $n(D, \Delta)$.

Corollary 10.16 *If $\Delta \geq 3$ and $\varepsilon > 0$ are fixed and D is sufficiently large, then*

$$n(D, \Delta) > \frac{(\Delta-1)^D}{(2+\varepsilon)D \log(\Delta - 1)}. \qquad \square$$

This shows that $\lim_{D\to\infty}\{\log_2 n(D,\Delta)\}/D = \log_2(\Delta - 1)$, guaranteeing that there is plenty of room for improvement on the constructions mentioned after Theorem 10.5: one should aim for $\lambda_\Delta = \{\log_2(\Delta-1)\}^{-1}$, which would be best possible.

10.4 Graph Processes

In §2 we studied the diameter of a r.g. G_p for not too small values of p. In this section we shall examine the diameter of a r.g. G_p where p is just about large enough to guarantee that a.e. G_p is connected. To be precise, our main aim is to present a theorem, due to Bollobás (1984*a*), concerning the diameter of a graph process at the hitting time of connectedness.

Let $\tau_0 = \tau_0(\widetilde{G})$ be the hitting time of connectedness: $\tau_0(\widetilde{G}) = \tau\{\widetilde{G}; \kappa(G) \geq 1\} = \min\{t : G_t$ is connected, where $\widetilde{G} = (G_t)_0^N\}$. We know from Chapter 7 that for $\omega(n) \to \infty$ we have $|\tau_0(\widetilde{G}) - (n/2)\log n| \geq \omega(n)$ almost surely. How large is the diameter of G_{τ_0}?

Theorem 10.17 *Almost every graph process $\widetilde{G}$ is such that*

$$\left\lfloor \frac{\log n - \log 2}{\log\log n} \right\rfloor + 1 \leq \text{diam } (G_{\tau_0}) \leq \left\lceil \frac{\log n + 6}{\log\log n} \right\rceil + 3.$$

Proof We shall give a detailed proof of the second inequality, which is the main assertion of the theorem.

Set $D = \lceil (\log n + 6)/\log\log n \rceil + 3$. The second inequality states that

$$\tau(\widetilde{G} : \text{diam } G \leq D) \leq \tau_0. \tag{10.10}$$

Since, trivially, $\tau_0 = \tau(\widetilde{G}; \text{diam } G < \infty) \leq \tau(\widetilde{G}; \text{diam } G \leq D)$, we have to show that the hitting time of diameter at most D is almost surely the hitting time of connectedness. Since by Theorem 7.4 the hitting time of connectedness is almost surely the hitting time of minimal degree at least 1, inequality (10.10) is equivalent to

$$\tau(\widetilde{G}; \text{diam } G \leq D) \leq \tau\{\widetilde{G}; \delta(G) \geq 1\}. \tag{10.11}$$

To prove (10.11), we proceed as in several proofs in Chapters 7 and 8, i.e. we make use of the model $\mathcal{G}(n, M; \geq 1)$ and Lemma 7.9, where $M = (n/2)\{\log n - \alpha(n)\}, \alpha(n) \to \infty$ and $\alpha(n) = o(\log\log\log n)$. Set $p = \{\log n - \alpha(n)\}/n$. We know from Chapter 2 that $\mathcal{G}_M$ and $\mathcal{G}_p$ are closely related; say, by Theorem 2.2,

$$P(G_M \text{ has } Q) \leq 3P(G_p \text{ has } Q) \tag{10.12}$$

for every monotone property Q. We shall often use (10.12) to estimate probabilities in the blue subgraph of a graph in $\mathcal{G}(n, M; \geq 1)$.

Let us show that a.e. graph in $\mathcal{G}(n, M; \geq 1)$ is such that for $k \leq d/2$ every vertex has many vertices at distance k from it. As earlier in this chapter, for a graph G and vertex $x \in V = V(G)$ set $\Gamma_k(x) = \{y \in V : d_G(x, y) = k\}$, and put $d_k(x) = |\Gamma_k(x)|$. We claim that a.e. $G \in \mathcal{G}(n, M; \geq 1)$ is such that for every vertex x we have

$$\tfrac{1}{9}(\log n)^2 \leq d_3(x) \leq 9(\log n)^3 \tag{10.13}$$

and if $3 \leq k \leq D/2$, then

$$\frac{1}{9}(\log n)^{k-1}\left(1 - \frac{\alpha(n)}{\log n}\right)^k \leq d_k(x) \leq 9(\log n)^k\left(1 + \frac{\alpha(n)}{\log n}\right)^k. \tag{10.14}$$

To see (10.13), note that in a.e. $G \in \mathcal{G}(n, M; \geq 1)$ there are few green edges and few vertices of degree at most $\frac{1}{2}\log n$. Hence a.e. graph is such that no green edge has an endvertex of degree at most $\frac{1}{2}\log n$, so

$$|\Gamma_1(x) \cup \Gamma_1(y)| \geq \left\lceil \tfrac{1}{3}\log n \right\rceil + 1 = m_0, \tag{10.15}$$

whenever xy is a green edge. Furthermore, the probability that some blue edge xy fails to satisfy (10.15) is by (10.12), at most

$$\begin{aligned} &3\binom{n}{2} p \sum_{m=0}^{m_0} \binom{n-2}{m} \{1-(1-p)^2\}^m (1-p)^{2(n-m-2)} \\ &\leq 3n(\log n)\frac{n^{m_0}}{m_0!}(2p)^{m_0} n^{-2} e^{2\alpha(n)} \\ &\leq n^{-1}(\log n)(6e)^{(\log n)/3} = o(1). \end{aligned}$$

A similar argument shows that, with probability $1 - o(n^{-1}), m$ given vertices have at least $m(\log n)/2$ and at most $3m(\log n)/2$ neighbours in the blue graph, provided $m_0/10 \leq m \leq (\log n)^3$. This implies the first inequality in (10.13). The second follows from the fact that a.e. $G \in \mathcal{G}(n, M; \geq 1)$ has maximal degree at most 3 log n. Furthermore, this shows also that

$$\max\left\{\left(\frac{1}{3}\log n\right)^2, \frac{\log n}{2} d_2(x)\right\} \leq d_3(x)$$

holds almost surely for every vertex x.

We prove (10.14) by induction on k. The case $k = 3$ is precisely relation (10.13), and the induction step is a consequence of the following simple assertion.

Let $A \subset B \subset V, b = |B| \leq 2a = 2|A|$ and $\frac{1}{9}(\log n)^2 \leq a \leq (\log n)^3 n^{1/2}$. Set $\delta = (\log\log n)/\log n$ and

$$\tilde{\Gamma}(A) = \{y \in V \backslash B : \exists x \in A, xy \in E(G)\} = \Gamma(A) \backslash B.$$

Then

$$P_p(||\tilde{\Gamma}(A)| - a\log n| \geq \delta a \log n) = o(n^{-2}) \tag{10.16}$$

To prove (10.16) note that for any given vertex $y \in V \backslash B$ we have $P_p\{y \notin \tilde{\Gamma}(A)\} = (1-p)^a = \bar{q}$, say, so, in $\mathcal{G}(n,p), |\tilde{\Gamma}(A)|$ has binomial distribution with parameters $n - b$ and $\bar{p} = 1 - \bar{q}$. Since

$$ap(1-ap) \leq 1 - e^{-ap} \leq \bar{p} = 1 - (1-p)^a \leq pa,$$

we have

$$|(n-b)\bar{p} - a\log n| \leq (\delta/10)a\log n.$$

Furthermore, $ap \le (\log n)^4 n^{-1/2}$ and

$$\frac{9\delta}{10}(n-b)\bar{p}\bar{q} \ge \frac{\log\log n}{2\log n}\frac{n}{2}\frac{ap}{2}\frac{1}{2} \ge (\log n)^2 \ge 12,$$

so, by Theorem 1.7(i), we find that

$$\begin{aligned}
&P_p\{||\tilde{\Gamma}(A)| - a\log n| \ge \delta a \log n\}\\
&\le P_p\left\{||\tilde{\Gamma}(A)| - (n-b)\bar{p}| \ge \frac{8\delta}{9}(n-b)\bar{p}\right\}\\
&\le \exp\left\{-\frac{64}{81}\delta^2(n-b)\bar{p}/3\right\} \le \exp\{-(\delta^2/4)(a\log n)\}\\
&= o(n^{-\log\log n}) = o(n^{-2}).
\end{aligned}$$

This proves (10.16) and so the proof of (10.14) is complete.

We are ready to show that a.e. graph in $\mathcal{G}(n, M; \ge 1)$ has diameter at most D. Set $D_1 = \lfloor D/2 \rfloor$ and $D_2 = \lceil D/2 \rceil - 1 = D - D_1 - 1$. Then a.e. graph is such that for any two vertices x and y

$$|\Gamma_{D_1}(x)| \ge a_1 = \lceil (\log n)^{D_1-1}/10 \rceil \text{ and } |\Gamma_{D_2}(y)| \ge a_2 = \lceil (\log n)^{D_2-1}/10 \rceil. \tag{10.17}$$

Now if $N_{D_1}(x) \cap N_{D_2}(y) \ne \emptyset$, then $d(x,y) \le D_1 + D_2 = D - 1$. On the other hand, if $N_{D_1}(x) \cap N_{D_2}(y) = \emptyset$ and (10.17) holds then, conditional on the subgraphs $G[N_{D_1}(x)]$ and $G[N_{D_2}(y)]$, the probability that no blue edge joins $\Gamma_{D_1}(x)$ to $\Gamma_{D_2}(y)$ is, by (10.12) at most

$$3(1-p)^{a_1 a_2} \le \exp\left\{-\frac{1}{101n}(\log n)^{D-2}\right\} \le \exp\left(-\frac{5}{2}\log n\right) = o(n^{-2}).$$

This shows that a.e. graph is such that any two of its vertices are within distance $D_1 + D_2 + 1 = D$ of each other, completing the proof of (10.11).

The first inequality in Theorem 10.10 is considerably easier to prove. For example, take $p = (\log n + \log\log\log n)/n$. Then a.e. G_p is connected, so the first inequality holds if a.e. G_p has diameter at least $\lfloor (\log n - \log 2)/\log\log n \rfloor + 1$. This can be shown by proving appropriate analogues of inequalities (10.13) and (10.14). □

With some more work, one could increase the lower bound in Theorem 10.17 by about 1 and so obtain that for most values of n the diameter of G_{τ_0} is, almost surely, one of two values. Furthermore, by imitating the proof of Theorem 10.17, one can show that for any $t \ge \tau_0$ the diameter of G_t is almost determined.

Theorem 10.18 *Suppose $M = M(n) = (n/2)d(n) \in \mathbb{N}, d(n) - \log n \to \infty$ and $d(n) \le n-1$. Then a.e. G_M is such that*

$$\left\lfloor \frac{\log n - \log 2}{\log d(n)} \right\rfloor + 1 \le \operatorname{diam} G_M \le \left\lceil \frac{\log n + 6}{\log\log n} \right\rceil + 3. \qquad \square$$

Recalling Theorem 10.10, we see that the assertion of Theorem 10.18 is new only in the range $d(n) - \log n \to \infty$ and $d(n) = O\{(\log n)^3\}$. Moreover, if $d(n)$, the average degree, is considerably greater than $\log n$, then the gap in Theorem 10.18 can be narrow (cf. Ex. 2).

A variant of the proof of Theorem 10.17 shows that if $c > 1$ and $M = \lfloor cn/2 \rfloor$, then, almost surely, the diameter of the giant component of G_M is $O(\log n)$. Furthermore, if c is large enough, then the asymptotic order of the giant component is almost determined.

Theorem 10.19 *Let $\varepsilon > 0$. If c is sufficiently large, then with $M = \lfloor cn/2 \rfloor m$, a.e. G_M is such that the giant component H of G_M satisfies*

$$(1-\varepsilon)\frac{\log n}{\log c} \le \operatorname{diam} H \le (1+\varepsilon)\frac{\log n}{\log c}. \qquad \square$$

10.5 Related Results

What can we say about the diameter of a random bipartite graph? By a *random bipartite graph* $G_{m,n;p}$ we mean an element of the space $\mathcal{G}(m,n;p) = \mathcal{G}\{K(m,n);p\}$ of r.gs obtained from a complete bipartite graph $K(m,n)$ by deleting edges independently, with probability $q = 1-p$, as defined in §1 of Chapter 2. In what follows we shall assume that $m = m(n) \le n, 0 < p = p(n) < 1$ and $K(m,n)$ has bipartition (V, W). Thus $|V| = m, |W| = n$, and for each $v \in V$ and $w \in W$ the edge vw is present with probability p, independently of the presence of other edges.

The first results concerning diameters of bipartite r.gs are due to Klee, Larman and Wright (1980, 1981); related results had been proved earlier by Harary and Robinson (1979) and Bollobás (1981*e*).

Note that a bipartite graph of order at least 3 has diameter at least 2, and the diameter is 2 iff the bipartite graph is complete. Thus 3 is the lowest diameter which is of interest. The case of $p = \frac{1}{2}$ and diameter 3 was examined by Klee, Larman and Wright (1980).

Theorem 10.20 *A necessary and sufficient condition that a.e. element of $\mathcal{G}(m,n;\frac{1}{2})$ has diameter 3 is that*

$$m(n)\log\left(\tfrac{4}{3}\right) - 2\log n \to \infty.$$

For higher diameters and varying probabilities, Bollobás and Klee (1984) obtained essentially best possible results. The first of the following two results covers the case when $m = m(n)$ is much smaller than n, the second concerns the case m is not much less than n.

Theorem 10.21 *If*

$$n(1-p)^m \longrightarrow 0 \text{ and } n(\log n)^2/m^2 - 2\log m > c$$

for some constant c, then a.e. $G_{m,n;p}$ is such that any two vertices of V have a common neighbour in W. A fortiori, a.e. $G_{m,n;p}$ has diameter at most 4. □

Theorem 10.22 *Suppose that for all n,*

$$pn \geq pm \geq (\log n)^4$$

and that k is a fixed positive integer.

If k is odd and

$$p^k m^{(k-1)/2} n^{(k-1)/2} - \log(mn) \longrightarrow \infty$$

or if k is even and

$$p^k m^{k/2} m^{k/2-1} - 2\log n \longrightarrow \infty,$$

then almost every $G_{m,n;p}$ is of diameter at most $k+1$.

If k is odd and

$$p^k m^{(k-1)/2} n^{(k-1)/2} - \log(mn) \longrightarrow -\infty$$

or if k is even and

$$p^k m^{k/2} n^{k/2-1} - 2\log n \longrightarrow -\infty,$$

then almost every $G_{m,n;p}$ is of diameter at least $k+2$. □

The first condition in Theorem 10.21 is necessary to ensure that almost no $G_{m,n;p}$ have an isolated vertex (Ex. 2), the second condition is, essentially, that m is at most $(n\log n)^{1/2}$ (see Ex. 3). Thus Theorem 10.21 gives another example of a property having the same threshold function as a considerably more restrictive property, a phenomenon encountered on many occasions in Chapters 7 and 8: if $m = m(n) < (1-\varepsilon)n(\log n)^{1/2}$ for some fixed $\varepsilon > 0$ and all sufficiently large n, then a.e. $G_{m,n;p}$ is connected iff a.e. $G_{m,n;p}$ has diameter at most 4.

Burtin (1973*a*,*b*, 1974, 1975) investigated in great detail several graph invariants closely connected to the diameter: the radius, the r-dominating number and the r-independence number. Of these invariants, the radius is well known: rad $G = \min_{x \in V(G)} \max\{d(x, y) : y \in V(G)\}$. For $r \in \mathbb{N}$, a set $W \subset V(G)$ is said to be *r-dominating* if every vertex of G is within distance r of some vertex of W; the *r-dominating number* $\gamma_r(G)$ is the minimal cardinality of an r-dominating set. Similarly, a set $U \subset V(G)$ is said to be *r-independent* if no two vertices of U have distance at most r; the *r-independence number* $\beta_r(G)$ is the maximal cardinality of an r-independent set. Thus the radius is the smallest value of r for which the r-dominating number is 1 and the diameter is the smallest value of r for which the r-independence number is 1; the 1-dominating number is usually called the *dominating number* and the 1-independence number is the (vertex) *independence number*. [It is somewhat unfortunate that the latter is usually denoted by $\beta_0(G)$ and $\beta_1(G)$ denotes the maximal number of independent edges. Nevertheless, this will not lead to confusion.]

Denote by $X_{r,s}(G)$ the number of r-independent sets of cardinality s in $V(G)$ and by $Y_{r,s}(G)$ the number of r-dominating sets of cardinality s. Burtin (1973*a*, 1975) determined the asymptotic distributions of $X_{r,s}(G_p)$ and $Y_{r,s}(G_p)$ for a large set of the parameters r, s and p. The following theorems are special cases of some of the results proved by Burtin; we do not state them in full generality since we shall not prove them.

Theorem 10.23 *Let $d \geq 2$, $s \geq 2, c > 0$ and define $p = p(n, c, d, s)$ by*

$$p^d n^{d-1} = \log(n^{2/(s-1)}/c).$$

Then $X_{d,s} \xrightarrow{d} P(c^{\binom{s}{2}}/s!)$. □

Corollary 10.24 *With the conditions in Theorem 10.23,*

$$\lim_{n\to\infty} P\{\beta_d(G_p) = s - 1\} = \exp(-c^{\binom{s}{2}}/s!)$$ □

and

$$\lim_{n\to\infty} P\{\beta_d(G_p) = s\} = 1 - \exp(-c^{\binom{s}{2}}/s!).$$

Theorem 10.25 *Let $d \geq 2, s \geq 1, c > 0$ and define $p = p(n, c, d, s)$ by*

$$p^d n^{d-1} = (1/s) \log\{cn/(\log n)^s\}.$$

Then $Y_{d,s} \xrightarrow{d} P(c/s!)$. □

Corollary 10.26 *With the conditions in Theorem 10.25,*

$$\lim_{n\to\infty} P\{\gamma_d(G_p) = s + 1\} = e^{-c/s!}$$

and

$$\lim_{n\to\infty} P\{\gamma_d(G_p) = s\} = 1 - e^{-c/s!}. \qquad \square$$

The diameter of a connected graph G is the minimal integer d such that from any vertex x we can get to any other vertex y by a path of length at most d. Needless to say, the path we choose depends on x and y. Can we find a short universal route: say a walk coded by a sequence independent of the graph G and the starting vertex x, guaranteed to pass through y?

To formulate this question precisely, suppose that G is an r-regular graph and for each vertex x of G the r edges incident with x are labelled $1, 2, \dots, r$. The labelling need not be consistent in any sense: an edge xy may be labelled i from x and $j \neq i$ from y. Given a labelling, every sequence $a_1 a_2 \dots a_t \in \{1, 2, \dots, r\}^t$ gives a walk from every vertex: simply follow the edge labels given by the sequence. Call a sequence (n, r)-*universal* if, for every r-regular graph of order n, the walk given by the sequence reaches all vertices, no matter where we start.

How short (n, r)-universal sequences are there? This question, posed by Cook, was answered by Aleliunas *et al.* (1979). The answer is both surprising and beautiful; the elegant proof is based on a pleasing theorem about random walks on graphs, the proof of which is left as an exercise (Exx. 6–8).

Theorem 10.27 *Let G be a connected graph of order n and size m. Consider a random walk that starts at a vertex x, and whenever it reaches a vertex y, as its next edge, it chooses an edge at random from the edges incident with y. Then the expected number of edges traversed before all vertices of G have been visited is at most $2m(n-1)$.* $\square$

Theorem 10.28 *(i) Let $r \geq 2, n \geq 3$ and $t \in \mathbb{N}$ satisfy*

$$2^t > 2n \left(\frac{rn}{e}\right)^{rn/2}.$$

Then there are (n, r)-universal sequences of length $2rn(n-1)t$.

(ii) If $r \geq 2$ and $\varepsilon > 0$, then, for n sufficiently large, there are (n, r)-universal sequences of length at most $(1+\varepsilon)r^2 n^3 \log_2 n$.

Proof The second assertion is an immediate consequence of the first, so that is all we have to prove. Set $s = 2rn(n-1)t$ and $\Omega = \{1, 2, \dots, r\}^s$. Turn into a probability space by taking all sequences $\omega \in \Omega$ equiprobable. Let

$\mathcal{G}_*$ be the set of all connected r-regular graphs on $\{1, 2, \ldots, n\}$, together with a distinguished vertex and an edge-labelling. (Thus for $r = 2$ and $n = 3$ the set $\mathcal{G}_*$ has $3 \cdot 2^3 = 24$ elements.) Note that, ignoring the distinguished vertex, the elements of $\mathcal{G}_*$ are in one-to-one correspondence with the configurations projecting into regular graphs (cf. the proof of Theorem 2.16). Thus, somewhat crudely,

$$|\mathcal{G}_*| \leq nN(rn) = n\frac{(rn)!}{(rn/2)!2^{rn/2}} < 2n\left(\frac{rn}{\mathrm{e}}\right)^{rn/2}.$$

For $G \in \mathcal{G}_*$ let X_G be the 0–1 r.v. on Ω which is 0 at a point $\omega \in \Omega$ iff the walk on G, given by the sequence ω and starting at the distinguished vertex of G, visits all vertices. Define

$$Y(\omega) = \sum_{G \in \mathcal{G}_*} X_G(\omega).$$

Then $Y(\omega) = 0$ iff ω is an (n, r)-universal sequence: $Y(\omega)$ is precisely the number of 'failures', the number of edge-labelled graphs with distinguished vertices for which ω will not do.

Since Y is a non-negative integer valued r.v., our theorem follows if we show that $\mathrm{E(Y)} < 1$, for then $Y(\omega) = 0$ for some $\omega \in \Omega$.

To show that $E(Y) < 1$, write $\omega \in \Omega$ as $\omega = \omega_1\omega_2 \ldots \omega_t$, a concatenation of sequences of length $l = 2rn(n-1)$. By Theorem 10.27, for any $G \in \mathcal{G}_*$, at least half of all sequences of length l give walks visiting all vertices. Therefore, the probability that ω_i does not visit all vertices of a fixed member G of $\mathcal{G}_*$ is at most $\frac{1}{2}$. Since the sequences $\omega_1, \omega_2, \ldots, \omega_t$ are independent of each other,

$$E(X_G) \leq 2^{-t} \text{ for every } G \in \mathcal{G}_*,$$

and so

$$E(Y) = \sum_{G \in \mathcal{G}_*} E(X_G) \leq 2^{-t}|\mathcal{G}_*| < 2^{-t+1}n\left(\frac{rn}{\mathrm{e}}\right)^{rn/2} < 1,$$

completing the proof. □

It is interesting to note that universal sequences for directed graphs have a different order of magnitude: a universal sequence for directed graphs of order n in which every vertex has outdegree r, has length at least $r^n + r - 1$.

10.6 Small Worlds

In the previous sections we presented several results asserting that a random graph has about as small a diameter as allowed by its order and degree. These results seem to justify the 'small world phenomenon', the principle that, with very few exceptions, we are all linked by short chains of acquaintances. This work goes back to experimental studies in the social sciences in the 1960s, especially the work of Fararo and Sunshine (1964) and Wilgram (1967). As a results of this work, people would talk of 'six degrees of separation' in the United States. (See Kleinberg (2000) for related algorithmic results.)

In the late 1980s this work intensified and has since become considerably more mathematical: numerous 'real life' networks have been scrutinized with special emphasis on the diameter and the distribution of the degrees. The networks under investigation include the power grid, networks of telephone calls, neural networks, polymers, collaboration networks, metabolic pathways and, perhaps above all, the world-wide web. In addition to examining many of these models, Watts and Strogatz (1998) and Watts (1999) raised the possibility of approximating them by random graphs, and quickly come to the conclusion that one needs random graph models that are rather different from the standard graph models $\mathcal{G}(n,p)$, $\mathcal{G}(n,M)$, $\mathcal{G}_{r\text{-reg}}$ and $\mathcal{G}_{k\text{-out}}$.

In order to model the world-wide web and other large networks, Barabási and Albert (1999) introduced a random graph process in which new vertices are added to a random graph one at a time and joined by k edges to earlier vertices in such a way that the probability of joining one to an earlier vertex x is proportional to the degree of x. After a number of empirical studies, Barabási and Albert (1999), Albert, Jeong and Barabási (1999) and Huberman and Adamic (1999) suggested that, resembling the world-wide web, the degree distribution of such a random graph is rather lopsided and obeys a power law with exponent close to -3. Furthermore, computer experiments carried out by Albert, Jeong and Barabási (1999), Barabási, Albert and Jeong (2000), and heuristic arguments given by Newman, Strogatz and Watts (2000) suggested that after n steps the resulting random graph should have diameter approximately $\log n$.

There are several difficulties with the empirical approach above. As it happens, even the start is uncertain: the above description of a random graph process fails to define a unique process. Bollobás and Riordan (2002) were the first to define a model that has the required properties and give precise bounds for the diameter. In what follows, we shall give a brief sketch of these results.

Our first aim is to define a random graph process $(G_k^t)_{t=1}^{\infty}$ for each $k \geq 1$ such that G_k^t has vertex set $[t]$ and kt edges, and the probability of an edge tj is proportional to the degree of j in G_k^t. Since the distribution of a random k-element subset of $[t]$ is not specified by the marginal probabilities with which the various elements are contained in this set when we add a vertex to G_k^t, we shall add k new edges one at a time. If we want to start with really small graphs like the 'vertexless and edgeless graph' or a graph with one vertex and some edges (loops) than we are forced to allow multiple edges and loops. Following Bollobás and Riordan (2002), this is the route we shall take.

First we define a random process $(G_k^t)_{t=1}^{\infty}$ for $k = 1$; the general case will follow easily. The graphs are nested: $G_1^1 \subset G_1^2 \subset \ldots$, with G_1^t having vertex set $[t]$ and t edges (and loops), with precisely one of these edges incident with t. Thus for $s < t$ the graph G_1^s is the subgraph of G_1^t induced by $[s]$. Clearly, G_1^1 is the graph on $[1]$ with a single loop. All that remains is to specify how to choose the random edge st incident with t in G_1^t, given G_1^{t-1}. The random variable s is distributed as follows:

$$P(s = i) = \begin{cases} d_{G_1^{t-1}(i)}/(2t-1) & \text{if } 1 \leq i \leq t-1, \\ 1/(2t-1) & \text{if } i = t. \end{cases}$$

Thus, given G_1^{t-1}, to get to G_1^t we send an edge c from t to a random vertex s, where the probability that we choose vertex i as s is proportional to the degree of i at the time, counting c as already contributing 1 to the degree of t. This is a perfectly natural choice if we count half-edges or we orient e out of t, but count the total degrees everywhere. The graph G_1^{t-1} has precisely $t-1$ edges, so the sum of the degrees at the time when we have already sent e out of t but have not yet decided where to send it is exactly $2t-1$.

Let $\mathcal{G}_1^n$ be the space formed by the random graphs G_1^n; this is the space we are interested in.

There is a crisp description of $\mathcal{G}_1^n$ in terms of pourings that constructs G_1^n at once, without going through the process. An *n-pairing* is a partition of $[2n]$ into pairs, so that there are $(2n)!/(n!2^n)$ n-pairings. Pairings are also thought of as *linearized chord diagrams* or LCD, (see Stoimenow (1998) and Bollobás and Riordan (2000)), where an LCD with n chords consists of $2n$ distinct points on the x-axis paired off by semi-circular chords in the upper half-plane. Two LCDs are considered to be the same if one can be changed into the other by moving the points on the x-axis without changing their order. Given an LCD L, construct a graph $\phi(L)$ as follows. Starting from the left, merge all endpoints up to and including the first right endpoint to form the vertex 1. Then, continuing to the right, merge all subsequent endpoints up to and including the next (i.e., second) endpoint to form the vertex 2, and so on, up to the nth and last endpoint. If L is chosen uniformly at random from all $(2n)!/(n!2^n)$ LCDs with n chords then $\phi(L)$ has the some distribution as a random graph $G_1^n \in \mathcal{G}_1^n$.

To get G_k^n and so $\mathcal{G}_k^n$ for $k > 1$, we simply take G_1^{kn} and identify blocks of k vertices: $1, \ldots, k$ are identified to form vertex 1, then $k+1, \ldots, 2k$ are identified to form vertex 2, and so on.

Clearly, $\mathcal{G}_k^n$ is reminiscent of both $\mathcal{G}_{k\text{-out}}$ and $\mathcal{G}_{r\text{-reg}}$; perhaps it is best viewed as a weighted and sequential version of $\mathcal{G}_{k\text{-out}}$.

For example, for $n = 3$ and $k = 2$, we start with a 12-pairing, say $L = \{(1,7),(2,4),(3,6),(5,9),(8,11),(10,12)\}$, then $G_1^6 = \phi(L)$ has vertices $1, \ldots, 6$ and edges 11, 12, 13, 24, 45, 56, and G_1^3 has vertices 1, 2, 3 and edges 11, 11, 12, 12, 23 and 33.

Having defined the Barabrási–Albert small world model in great detail, we are ready to state the result of Bollobás and Riondan (2002) on the diameter.

Theorem 10.29 *For $k \geq 2$ and $\varepsilon > 0$, a.e. $G_k^n \in \mathcal{G}_k^n$ is connected and has diameter diam G_k^n satisfying*

$$(1-\varepsilon)\frac{\log n}{\log\log n} \leq \text{diam } G_k^n \leq (1+\varepsilon)\frac{\log n}{\log\log n}. \tag{10.18}$$

□

For the rather long proof of this theorem we refer the reader to the original article; here we shall give only a brief sketch, paying more attention to the lower bound, which is considerably easier than the upper bound.

The lower bound can be proved by comparing G_1^{kn} with a random graph on $[N] = [kn]$, in which the edges are chosen independently of each other, and the probability of an edge ij is $c/\sqrt{ij}$ for some constant $c > 0$. To be precise, the following lemma turns out to be very useful.

Lemma 10.30 *Let H be a loopless graph on $[N]$ in which every vertex i has at most one neighbour j with $1 \leq j < i$. Then*

$$P(H \subset G_1^N) \leq 2^{e(H)(\Delta(H)+2)} \prod_{ij \in E(H)} \frac{1}{\sqrt{ij}}.$$

□

This lemma can be proved by examining what happens in the process (G_1^t) as we pass from G_1^{t-1} to G_1^t.

With the aid of Lemma 10.30, one can prove the following slightly stronger form of the lower bound in (10.18): a.e. G_k^n is such that the distance $\rho(n, n-1)$ between n and $n-1$ is at least $L = \log n/(20k^2 \log n)$. In fact, this stronger assertion can be proved by estimating the expectation $E(X_l)$ of the number X_l of paths of length l between n and $n-1$.

Consider a particular path $Q = v_0 v_1 \dots v_l$ on $[n]$ with $v_0 = n, v_l = n-1$ and $l \le L$. A graph H on $[kn]$ is a *realization* of Q if H has edges $x_j y_{j+1}, j = 0, 1, \dots, l-1$, with $\lceil x_j/k \rceil = \lceil y_j/k \rceil = v_j$. Since H has maximal degree at most 2, Lemma 10.30 implies that

$$P(H \subset G_1^{kn}) \le 2^{4l} \prod_{j=0}^{l-1} \frac{1}{\sqrt{x_j y_{j+1}}} \le 16^l \prod_{j=0}^{l-1} \frac{1}{\sqrt{v_j v_{j+1}}} = \frac{16^l}{\sqrt{v_0 v_l}} \prod_{j=1}^{l-1} \frac{1}{v_j}.$$

As Q has k^{2l} realizations, and $Q \subset G_k^n$ if and only if at least one of these realizations is present in G_1^{kn}, we have

$$P(Q \subset G_k^n) \le \frac{(16k^2)^l}{\sqrt{v_0 v_l}} \prod_{j=1}^{l-1} \frac{1}{v_j}.$$

Therefore, if n is large enough, for $1 \le l \le L$ we have

$$\begin{aligned} E(X_l) &\le \frac{(16k^2)^l}{\sqrt{n(n-1)}} \sum_{1 \le v_1, \dots, v_{l-1} \le n-2} \prod_{j=1}^{l-1} \frac{1}{v_j} \\ &= \frac{(16k^2)^l}{\sqrt{n(n-1)}} \left(\sum_{v=1}^{n-2} \frac{1}{v} \right)^{l-1} \\ &\le \frac{(18k^2)^l}{n} (\log n)^{l-1} \le \left(\frac{9}{10} \right)^l (\log n)^{-1}, \end{aligned}$$

since $l \le L$ implies that $(20k^2 \log n) \le n$. Hence

$$\sum_{l=1}^{\lfloor L \rfloor} E(X_l) \le 9/\log n = o(1),$$

so $\rho(n, n-1) > L$ in a.e. G_k^n, as claimed.

The proof of the upper bound in Theorem 10.28 is more complicated. Very roughly, considering a random N-pairing as an LCD pairing of random points in [0,1], we choose the right endpoints of the chords first. Given these right endpoints, the left endpoints are independent of each other, and the only constraint is that each comes before its corresponding right endpoint. We fix a 'typical' distribution of the right endpoints, and use the randomness provided by the left endpoints.

To show that diam G_k^n is likely to be small, we proceed as in the case of random graph models: starting with a given vertex v, we consider the set $N_l(v)$ of vertices within distance l of v, and show that $N_l(v)$ increases at an appropriate rate. However, the sine of $N_l(v)$ is not the usual cordinality $|N_l(v)|$ but the weight

$$w(N_l(v)) = \sum_{j \in N_l(v)} \frac{1}{\sqrt{j}}.$$

Essentially, given $w(N_l(v))$, the expected value of $w(N_{l+1}(v))$ is about $(\log n)w(N_l(v))$ as long as this is not too large. This indicates that in about $\log n/\log\log n$ steps we can reach every vertex from v. Needless to ray, there are numerous complications on the way.

Theorem 10.29 states that for $k \geq 2$ the diameter of G_k^n is even smaller than predicted by computer experiments and heuristic arguments. With hindright, it is perhaps more surprising that the diameter of G_k^n is not smaller than it is rather than that it is not larger.

As mentioned earlier, Barabási and Albert (1999) and Barabási, Albert and Jeong (1999) also predicted the degree distribution of a typical G_k^n. Their prediction was proved by Bollobás, Riordan, Spencer and Tusnády (2001). To be precise, they proved that for $k \geq 1$ and $1 \leq d = d(n) \leq n^{1/15}$ the expected proportion of vertices of degree d in G_k^n is about

$$\frac{2k(k+1)}{(d+k+1)(d+k+2)(d+k+3)},$$

i.e., the fraction of vertices of G_k^n with degree d falls off as d^{-3} as $d \to \infty$. This result can also be used to prove Theorem 10.29: we fix a typical degree sequence $(d_i)_1^n$ and show that most graphs on $[n]$ with this degree sequence in which each vertex i is incident with k edges joining it to vertices j with $j \leq i$ have diameter about $\log n/\log\log n$. Once again, much work is needed to term this vague idea into a proper proof.

Exercises

10.1 Give a detailed proof of Theorem 10.18.

10.2 Let $M = M(n) = (n/2)d(n) \in \mathbb{N}$ be such that $d(n)/\log n \to \infty$ and $d(n) \leq (\log n)^4$. Prove that almost every G_M satisfies

$$\left\lfloor \frac{\log n + \log\log n}{\log d(n)} \right\rfloor \leq \text{diam } G_M \leq \left\lceil \frac{\log n + \log\log n + 1}{\log d(n)} \right\rceil.$$

10.3 (cf. Theorem 10.21 and the assertion after Theorem 10.22.) Prove that almost no $G_{m,n;p}$ has an isolated vertex iff

$$n(1-p)^m \longrightarrow 0.$$

10.4 (cf. Theorem 10.21.) Show that if

$$m < (n \log n)^{1/2} \left\{ 1 - \left(\frac{1}{2} + \delta \right) \frac{\log \log n}{\log n} \right\}$$

for some fixed $\delta > 0$, then

$$\frac{n(\log n)^2}{m^2} - 2 \log m \geq c$$

for some constant c, and that this latter condition implies

$$m < (n \log n)^{1/2}$$

provided n is sufficiently large.

10.5 Deduce Corollaries 10.24 and 10.26 from Theorems 10.23 and 10.25.

10.6 With the assumptions of Theorem 10.27, show that the stationary probability of vertex x is $d(x)/2m$, and deduce that the mean recurrence time of vertex x is $2m/d(x)$.

10.7 Denote by $T(x, y)$ the expected number of edges traversed until y is reached from x. Prove that $T(x, y) + T(y, x) \leq 2m$.

10.8 Deduce Theorem 10.27 from Ex. 7. (Aleliunas *et al.*, 1979.)

11

Cliques, Independent Sets and Colouring

The main aim of this chapter is the study of the complete subgraphs of $G_{n,p}$ for a fixed p. We know from §1 of Chapter 2 that one of the advantages of keeping p fixed is that the spaces $\mathcal{G}\{n, P(\text{edge}) = p\}$ need not be considered one at a time, for they are images of the single probability space $\mathcal{G}(\mathbb{N}, p)$ consisting of graphs on $\mathbb{N}$ whose edges are chosen independently and with probability p. A pleasing property of $\mathcal{G}(\mathbb{N}, p)$ is that the term 'almost every' has its usual measure theoretic meaning.

A clique of $G_{n,p}$ depends on many of the edges incident with few of the vertices. A consequence of this turns out to be that the clique number of $G_{n,p}$ is remarkably close to a constant. There are a set $M \subset \mathbb{N}$ of density 1 and a function $\text{cl}: M \to \mathbb{N}$ such that for a.e. $G \in \mathcal{G}(\mathbb{N}, p)$ there is a number $m_0 = m_0(G)$ such that if $n \geq m_0, n \in M$, then $\text{cl}(G_n) = \text{cl}(n)$. A proof of this theorem of Bollobás and Erdős (1976*a*) is the main aim of §1. In §2 we discuss the possibility of approximating the distribution of the number of complete subgraphs of a given order by a Poisson distribution.

As an application of the results of §1, in §3 we obtain estimates of the greedy chromatic number of $G_{n,p}$, while the second section is about an approximation of the number of complete r-graphs by a Poisson r.v. The highlight of the chapter is §4, in which we use martingale inequalities to determine the asymptotic value of $\chi(G_{n,p})$ for p constant. The last section is about sparse graphs: we shall sketch a large number of results.

11.1 Cliques in G_p

A maximal complete subgraph of a graph is called a *clique* of the graph. The *clique number* $\text{cl}(G)$ of a graph is the maximal order of a clique of G; equivalently, $\text{cl}(G)$ is simply the maximal order of a complete subgraph. The *independence number* $\beta_0(G)$ of G is the maximal cardinality of an independent set of vertices in G. Thus $\beta_0(G) = \text{cl}(\overline{G})$.

Matula (1970, 1972, 1976) was the first to notice that for fixed values of p the distribution of the clique number of a r.g. G_p is highly concentrated: almost all G_p's have about the same clique number. Results asserting this phenomenon were proved by Grimmett and McDiarmid (1975); these results were further strengthened by Bollobás and Erdős (1976*a*).

As we mentioned earlier, for the greater part of this section we fix $0 < p < 1$ and consider the space $\mathcal{G}(\mathbb{N}, p)$. Given a graph $G \in \mathcal{G}(\mathbb{N}, p)$, we write G_n for $G[1,2,\dots,n]$, the subgraph of G spanned by the set $\{1,2,\dots,n\}$. It turns out that for a.e. $G \in \mathcal{G}(\mathbb{N}, p)$ the sequence $\mathrm{cl}(G_n)$ is almost entirely determined.

For $r \in \mathbb{N}$ let Y_r be the r.v. on $\mathcal{G}(n, p)$ defined by

$$Y_r = Y(n,r) = Y_r(G_p) = k_r(G_p),$$

where, as usual, $k_r(G)$ denotes the number of complete r-graphs in a graph G. [See Chapter 6 of Bollobás (1978*a*) about extremal properties of the function $k_r(G)$.] Writing $X_n = X_n(G_p) = \mathrm{cl}(G_p)$ for the clique number of a r.g. $G_p \in \mathcal{G}(n, p)$, clearly

$$X_n = \max\{r : k_r(G_p) > 0\} = \max\{r : Y_r > 0\}.$$

For small values of r the expectation of Y_r is large and the variance is fairly small. As we increase r, for most values of n the expectation of Y_r drops below 1 rather suddenly: for some r_0 we have $E(Y_{r_0})$ large (much larger than 1) and $E(Y_{r_0+1})$ very small (much smaller than 1). We are interested in this value r_0 for then we have $X_n = r_0$ with great probability.

All we have to do is calculate the expectation and variance of Y_r for certain values of r. This is precisely what we did in §1 of Chapter 4 for more complicated subgraphs. Clearly we have

$$E_r = E(n,r) = E(Y_r) = \binom{n}{r} p^{\binom{r}{2}}. \tag{11.1}$$

Let $r_0 = r_0(n, p)$ be the positive real number satisfying

$$f(r_0) = (2\pi)^{-1/2} n^{n+1/2} (n - r_0)^{-n+r_0-1/2} r_0^{-r_0-1/2} p^{r_0(r_0-1)/2} = 1.$$

[Note that $f(r)$ is simply the expression for E_r in which $\binom{n}{r}$ has been replaced by its Stirling approximation.] It is easily checked that

$$\begin{aligned} r_0 &= 2\log_b n - 2\log_b \log_b n + 2\log_b(e/2) + 1 + o(1) \\ &= 2\log_b n + O(\log\log n) = \frac{2\log n}{\log b} + O(\log\log n), \end{aligned}$$

where, to simplify the notation, we wrote b for $1/p$.

Let $0 < \varepsilon < \frac{1}{2}$. Given a natural number $r \geq 2$ let n_r be the maximal natural number for which

$$E(n_r, r) \leq r^{-(1+\varepsilon)}$$

and let n'_r be the minimal natural number for which

$$E(n'_r, r) \geq r^{1+\varepsilon}.$$

A brief examination of the function $E(n, r)$ shows that $n_r < n'_r$,

$$n_r = \frac{r}{e} b^{(r-1)/2} + o(rb^{r/2}), \quad n'_r = \frac{r}{e} b^{(r-1)/2} + o(rb^{r/2})$$

and

$$n'_r - n_r < \{(5 \log r)/(2r)\} n_r.$$

Therefore, with at most finitely many exceptions, one has

$$n_r < n'_r < n_{r+1},$$
$$(n'_r - n_r)/(n_{r+1} - n'_r) < 3(b^{1/2} - 1)^{-1} r^{-1} \log r$$

and

$$\lim_{r \to \infty} (n_{r+2} - n_{r+1})/(n_{r+1} - n_r) = b^{1/2}.$$

In particular, the set of natural numbers $M = \{n : n'_r \leq n \leq n_{r+1}$ for some $r \geq 2\}$ has density 1. This is the set of graph orders for which the clique number is almost determined.

Theorem 11.1 *For a.e. $G \in \mathcal{G}(\mathbb{N}, p)$ there is a constant $m_0 = m_0(G)$ such that if $n \geq m_0$ and $n'_r \leq n \leq n_{r+1}$, then* $\mathrm{cl}(G_n) = r$.

Proof As indicated, we shall estimate the expectation and variance of $Y_r = Y(n, r)$, on the space $\mathcal{G}(n, p)$ for r not too far from $r_0(n)$. Let $0 < \eta < 1$ be a constant. We shall consider the r.vs $Y_r = Y(n, r)$ for

$$(1 + \eta) \log_b n < r < 3 \log_b n$$

and large values of n.

Arguing as in §1 of Chapter 4, we find that

$$E(Y_r^2) = \sum_{l=0}^{r} \binom{n}{r} \binom{r}{l} \binom{n-r}{r-l} p^{2\binom{r}{2} - \binom{l}{2}} \tag{11.2}$$

since the probability that G_p contains a given pair of K^r subgraphs with l vertices in common is precisely $p^{2\binom{r}{2}-\binom{l}{2}}$. By (11.1) we have

$$E_r^2 = \sum_{l=0}^{r} \binom{n}{r}\binom{r}{l}\binom{n-r}{r-l} p^{2\binom{r}{2}}$$

so the variance of Y_r is

$$\sigma_r^2 = \sigma^2(Y_r) = \sum_{l=2}^{r} \binom{n}{r}\binom{r}{l}\binom{n-r}{r-l} p^{2\binom{r}{2}}(b^{\binom{l}{2}} - 1)$$

and thus

$$\sigma_r^2/E_r^2 = \sum_{l=2}^{r} \frac{\binom{r}{l}\binom{n-r}{r-l}}{\binom{n}{r}}(b^{\binom{l}{2}} - 1) = \sum_{l=2}^{r} F_l. \tag{11.3}$$

Routine and crude calculations show that, if n is sufficiently large and $3 \le l \le r-1$, then

$$F_l < F_3 + F_{r-1}.$$

Consequently (11.3) implies that

$$\begin{aligned} \sigma_r^2/E_r^2 &< F_2 + F_r + (r-3)(F_3 + F_{r-1}) \\ &< \frac{r^4}{2n^2}(b-1) + \frac{1}{E_r} + r\left(\frac{r^6}{6n^3}(b^3-1) + \frac{rnp^{r-1}}{E_r}\right). \end{aligned}$$

By our assumption,

$$b^r > n^{1+\eta} \text{ and } r < 3\log_b n$$

and so, if n is sufficiently large,

$$\sigma_r^2/E_r^2 < br^4n^{-2} + 2E_r^{-1}. \tag{11.4}$$

Let us draw the threads together. By (11.4) we have

$$P(Y_r = 0) < \sigma_r^2/E_r^2 < br^4n^{-2} + 2E_r^{-1}.$$

Therefore, by the choice of n_r',

$$P\{Y(n_r', r) = 0\} < br^4 n_r^{-2} + 2E(n_r', r)^{-1} < 3r^{-(1+\varepsilon)}.$$

On the other hand, the choice of n_{r+1} implies

$$P\{Y(n_{r+1}, r+1) > 0\} \le E\{Y(n_{r+1}, r+1)\} < r^{-(1+\varepsilon)}.$$

Turning now to the space $\mathcal{G}(\mathbb{N}, p)$, these inequalities imply that, for a fixed r

$$P\{G : X_n(G) \neq r \text{ for some } n,\ n'_r \leq n \leq n_{r+1}\} < 4r^{-(1+\varepsilon)}.$$

As $\sum_{r=2}^{\infty} r^{-(1+\varepsilon)} < \infty$, the Borel-Cantelli lemma implies that for a.e. graph $G \in \mathcal{G}(\mathbb{N}, p)$, with the exception of finitely many r's we have

$$X_n(G) = r \text{ for all } n, n'_r \leq n \leq n_{r+1}. \qquad \square$$

Since $\mathrm{cl}(G_n) \leq \mathrm{cl}(G_{n'})$, whenever $n \leq n'$, roughly speaking, Theorem 11.1 tells us that there is a function cl: $\mathbb{N} \to \mathbb{N}$ such that for a.e. $G \in \mathcal{G}(\mathbb{N}, p)$ there is an integer $m_0(G)$ such that if $n \geq m_0(G)$, then $\mathrm{cl}(G_n) = \mathrm{cl}(n)$ or $\mathrm{cl}(n) + 1$; furthermore, for a.e. n we have $\mathrm{cl}(G_n) = \mathrm{cl}(n)$. What is this function $\mathrm{cl}(n)$? Note that for $\delta = o(1)$ we have

$$f(r_0 + \delta) \sim (n/r_0)^{\delta} p^{\delta r_0}, \tag{11.5}$$

where $r_0 = r_0(n)$, since $f(r_0) = 1$, so if $\delta = 2(\log\log n)/\log n$, then

$$f(r_0 - \delta) > r_0^{3/2} \text{ and } f(r_0 + \delta) < r_0^{-3/2}.$$

This gives us the following consequence of Theorem 11.1.

Corollary 11.2 *For a.e. $G \in \mathcal{G}(\mathbb{N}, p)$ there is a constant $m_0(G)$ such that if $n \geq m_0(G)$, then*

$$\lfloor r_0(n) - 2(\log\log n)/\log n \rfloor \leq \mathrm{cl}\ (G_n) \leq \lfloor r_0(n) + 2(\log\log n)/\log n \rfloor.$$

Furthermore,

$$|\mathrm{cl}\ (G_n) - 2\log_b n + 2\log_b \log_b n - 2\log_b(e/2) - 1| < \tfrac{3}{2}. \qquad \square$$

Let us estimate the probability that $\mathrm{cl}(G_n)$ differs from $r_0(n)$ substantially. First, for the probability that $\mathrm{cl}(G_n)$ is substantially larger than $r_0(n)$ we have the following trivial but fairly good upper bound:

$$P\{\mathrm{cl}(G_n) \geq r\} \leq E(Y_{\lceil r \rceil}) \leq 2f(r) < n^{r_0(n) - r}$$

provided n is sufficiently large.

We shall be slightly more subtle in our estimate of the probability that $\mathrm{cl}(G_n)$ is smaller than $r_0(n)$. If $0 < \delta < 2$ and $r = r_0 - \delta \in \mathbb{N}$, then

$$E(n, r) > n^{\delta}(\log_b n)^{-\delta},$$

so, by (11.4),

$$P\{\mathrm{cl}(G_n) \leq r_0 - \delta\} < 2(\log_b n)^{\delta} n^{-\delta}.$$

For larger deviations we can do considerably better.

Theorem 11.3 *(i) Let* $0 < \varepsilon, r : \mathbb{N} \to \mathbb{N}, 0 < r(n) < r_0(n), r(n) \to \infty$ *and put*

$$t = t(n) = \lfloor r_0(n) - r(n) - \varepsilon \rfloor - 1.$$

Then

$$P\{\mathrm{cl}\ (G_n) \le r(n)\} \le n^{-\lfloor b^{t/2} \rfloor}.$$

(ii) Let $0 < \alpha < \beta < 1$. *Then*

$$P\{\mathrm{cl}\ (G_n) \le (1-\beta) r_0(n)\} < n^{-n^{2\alpha}}.$$

Proof (i) Put $s = \lfloor b^{t/2} \rfloor$ and choose subsets $V_1, V_2, \ldots, V_s$ of $V(G_n) = \{1, 2, \ldots, n\}$ such that $|V_i \cap V_j| \le 1$ and $|V_i| \ge n/s, 1 \le i, j \le s, i \ne j$. Then

$$r_0(|V_i|) > r_0(n) - \varepsilon/2 - 2\log_b s \le r_0(n) - \varepsilon/2 - t \le r(n) + 1 + \varepsilon/2.$$

Thus, if n is large, the probability that $G_n[V_i]$ contains no K^l with $l > r(n)$ is at most n^{-1}. Since the graphs $G_n[V_i], i = 1, 2, \ldots, s$, are independent of each other,

$$P\{\mathrm{cl}(G_n) \le r(n)\} \le n^{-s}.$$

(ii) Once again, we shall partition G_n into edge-disjoint subgraphs, each of which has a large clique number with probability close to 1. Set $r = \lfloor (1-\beta) r_0(n) \rfloor + 1$ and pick a prime P between n^α and $2n^\alpha$. Put

$$Q = P^2 + P + 1 \text{ and } m = \lfloor n/Q \rfloor.$$

Partition $V(G_n) = \{1, 2, \ldots, n\}$ into Q classes, say $C_1, C_2, \ldots, C_Q$, each having m or $m+1$ vertices. Consider the sets $C_1, C_2, \ldots, C_Q$ as points of a finite projective geometry. For each line e of this geometry, let G_e be the subgraph of G_n with vertex set $W_e = \cup_{C_i \in e} C_i$ whose edges are the edges of G_n joining distinct C_i's. Note that G_e is just a random element of $\mathscr{G}(K_e, p)$, where K_e is the complete $(P+1)$-partite graph with vertex classes $C_i \in e$. [See §1 of Chapter 2 for the model $\mathscr{G}(H, p)$.]

Since

$$\binom{P+1}{r} m^r \sim \binom{|W_e|}{r},$$

almost every r-tuple in W_e meets each C_i in at most one vertex. This implies that

$$P\{\mathrm{cl}(G_e) < r\} \sim P\{\mathrm{cl}(G_{|W_e|}) < r\}$$

(see Ex. 2). Now $|W_e| \sim n/P \geq n^{1-\alpha}/2$, so $r < r_0(|W_e|) - 4$, say, if n is sufficiently large. Hence

$$P\{\mathrm{cl}(G_e) < r\} < n^{-3/2}$$

so

$$P\{\mathrm{cl}(G_n) < r\} < n^{-3Q/2} < n^{-n^{2\alpha}}. \qquad \square$$

What natural numbers are likely to appear as orders of cliques of G_n? It turns out that the orders which do occur in a.e. G_n are almost precisely the numbers between $r_0(n)/2$ and $r_0(n)$. The probability that r given vertices span a clique is clearly

$$(1-p^r)^{n-r}p^{\binom{r}{2}},$$

so if we write Z_r for the number of r-cliques, then

$$E(Z_r) = \binom{n}{r}(1-p^r)^{n-r}p^{\binom{r}{2}}. \tag{11.6}$$

It is easily checked that if $\varepsilon > 0$ and n is sufficiently large, then $E(Z_r)$ is large for all r's between $(\frac{1}{2}+\varepsilon)r_0(n)$ and $(1-\varepsilon)r_0(n)$ and small for all r's outside the range $\{(\frac{1}{2}-\varepsilon)r_0(n), (1+\varepsilon)r_0(n)\}$. This leads to the following result (Ex. 3).

Theorem 11.4 *Given constants $0 < p < 1$ and $0 < \varepsilon < \frac{1}{2}$, a.e. random graph in $\mathscr{G}(n,p)$ is such that it has a clique of order r for all r satisfying*

$$(1+\varepsilon)\log_b n < r < (2-\varepsilon)\log_b n$$

but has no clique of order r if

$$r < (1-\varepsilon)\log_b n \text{ or } r > (2+\varepsilon)\log_b n. \qquad \square$$

So far we have found large complete subgraphs in the initial segments of a r.g. $G \in \mathscr{G}(\mathbb{N}, p)$. What about infinite complete graphs meeting each initial segment in a fairly large set? Denote by $K(x_1, x_2, \ldots)$ the complete graph with vertex set $\{x_1, x_2, \ldots\} \subset \mathbb{N}$, where $x_1 < x_2 < \ldots$. For how dense a sequence $(x_n)_1^\infty$ may we hope to find $K(x_1, x_2, \ldots)$. in a r.g. $G \in \mathscr{G}(\mathbb{N}, p)$? To be precise, what is the infimum c_0 of those positive constants c for which a.e. $G \in \mathscr{G}(\mathbb{N}, p)$ contains a $K(x_1, x_2, \ldots)$ such that $x_r \leq c^r$ if r is sufficiently large?

Theorem 11.1 and Corollary 11.2 show that $c_0 \geq b^{1/2}$, and at the first sight it seems possible that $c_0 = b^{1/2}$. However, it turns out that a sequence cannot be continued with such a density and, in fact, $c_0 = b$.

To see that $c_0 \le b$ note that not only is an element of $\mathcal{G}(n,p)$ unlikely to contain cliques of order less than $(1-\varepsilon)\log_b n$, but it is also unlikely to contain any set of $r < (1-\varepsilon)\log_b n$ vertices not dominated by another vertex. Even more, if $r < (1-\varepsilon)\log_b n$, then the probability that some r-set of vertices is not dominated by any vertex in a fixed subset of εn vertices is at most

$$\binom{n}{r}(1-p^r)^{\varepsilon n-r} < n^r \exp(-p^r \varepsilon n/2) < e^{-n^{\varepsilon/2}} < e^{-r},$$

provided n is sufficiently large. Since $\sum_1^\infty e^{-r} = 1/(e-1) < \infty$, the first part of the next theorem follows. The second part is left an exercise (Ex. 4).

Theorem 11.5 *Let $0 < p < 1$ and $\varepsilon > 0$ be fixed. Set $b = 1/p$.*
(i) A.e. $G \in \mathcal{G}(\mathbb{N},p)$ contains a $K(x_1,x_2,\ldots)$ such that

$$x_r < b^{r(1+\varepsilon)}$$

for every sufficiently large r.
(ii) A.e. $G \in \mathcal{G}(\mathbb{N},p)$ is such that for every $K(x_1,x_2,\ldots) \subset G$

$$x_r > b^{r(1-\varepsilon)}$$

holds for infinitely many values of r. □

Let us consider briefly, for what functions $r = r(n)$ we can find a probability $p = p(n)$ such that a.e. G_p has clique number r. It is not unexpected that large clique numbers tend to have a smoother distribution; equivalently, the smaller $p(n)$ is, the more likely it is that the clique number of G_p is almost determined, that is a.e. G_p has the same clique number. We saw this phenomenon in §§1 and 3 of Chapter 4 for a fixed clique size $k \ge 2$ and $p(n)$ about $n^{-k/(k-1)}$; the peak was even greater than for fixed values of p (Theorem 11.1).

The next result covers the case when $r = r(n)$ is rather large, and so $q = 1-p$ is small. Note that, by relation (11.1), for $r = o(n)$ if $E(n,r+1) < 1$, then

$$E(n,r+1)/E(n,r) = \frac{n-r}{r+1}p^r \le p^{r/2} \le \frac{r}{n} = o(1).$$

This shows that in the following theorem the function $p(n)$ can be chosen to satisfy the stated conditions.

Theorem 11.6 *Let $r = r(n) = O(n^{1/3})$ and let $p = p(n)$, $0 < p < 1$, be such that*

$$\binom{n}{r} p^{\binom{r}{2}} \to \infty \text{ and } \binom{n}{r+1} p^{\binom{r+1}{2}} \to 0.$$

Then a.e. G_p has clique number r.

Proof The second condition on p implies that almost no G_p contains a K^{r+1}, so $\mathrm{cl}(G_p) \le r$ for a.e. G_p. Furthermore, the first condition on p is simply that $E(Y_r) \to \infty$, so the theorem follows if one shows that $\sigma^2(Y_r)/E(Y_r)^2 \to 0$. This can be deduced from (11.3). As in the proof of Theorem 11.1, relation (11.3) implies that

$$\sigma^2(Y_r)/E(Y_r)^2 = F_2 + F_{r-1} + F_r + o(1).$$

Now $F_r \le E(Y_r)^{-1}$,

$$F_2 \le \frac{r^4}{n^2}(p^{-1} - 1) = o(1)$$

and

$$\begin{aligned} F_{r-1} &= \frac{rn}{\binom{n}{r}}(p^{-\binom{r-1}{2}} - 1) \le \frac{rn}{\binom{n}{r}} \left\{ E(Y_r) \Big/ \binom{n}{r} \right\}^{-1} p^{r-1} \\ &= \frac{rn}{E(Y_r)} p^{r-1} = O[r^3/\{nE(Y_r)\}] = o(1). \end{aligned}$$ □

It is easily seen that $p(n)$ in Theorem 11.6 can be about as large as $1 - \frac{4}{3}(\log n)n^{-1/3}$. Theorem 11.6 is essentially best possible; if $k/n^{1/3} \to \infty$, then no r satisfies all of $E(Y_{r+1}) \to 0, E(Y_r) \to \infty$ and $\sigma^2(Y_r) = o\{E(Y_r)^2\}$. In fact, outside the range of r given in Theorem 11.6 there is no p such that a.e. G_p has clique number r.

When $q = 1 - p = O\{(\log n)n^{-1/3}\}$, it is more natural and more customary to consider the independence number of G_q instead of the clique number of G_p. This will be done in §5.

11.2 Poisson Approximation

We saw in the previous section that the distribution of the clique number of G_p for fixed values of p has a strong peak about some integer $r = r(n)$ satisfying $r \sim 2\log_b n = 2(\log n)/\log(1/p)$, namely a.e. G_p has clique number $r(n) - 1$ or $r(n)$. What happens when both $r(n) - 1$ and $r(n)$ occur as clique numbers, with probabilities bounded away from 0? A fairly cumbersome application of Theorem 1.20 shows that in that case $Y_r = Y_r(G_p) = k_r(G_p)$ has asymptotically Poisson distribution which allows us to approximate $P\{\mathrm{cl}(G_p) = r-1\}$ and $P\{\mathrm{cl}(G_p) = r\}$. As we shall prove a stronger result, the proof of this assertion is omitted.

Theorem 11.7 *Suppose $0 < p < 1$ is fixed and $r = r(n) \in \mathbb{N}$ is such that $E(Y_r) = E\{k_r(G_p)\} \to \lambda$ for some $\lambda > 0$. Then $Y_r \xrightarrow{d} P_\lambda$,*

$$\lim_{n\to\infty} P\{\mathrm{cl}(G_p) = r-1\} = \mathrm{e}^{-\lambda} \text{ and } \lim_{n\to\infty} P\{\mathrm{cl}(G_p) = r\} = 1 - \mathrm{e}^{-\lambda}.$$

Corollary 11.8 *Let $0 < p < 1$ be fixed and let*

$$r = r(n) = \max\{s : E(Y_s) \geq 1\} = \max\left\{s : \binom{n}{s} p^{\binom{s}{2}} \geq 1\right\}.$$

Set

$$\lambda_n = E(Y_r) = \binom{n}{r} p^{\binom{r}{2}} \quad \text{and} \quad \mu_n = E(Y_{r+1}) = \binom{n}{r+1} p^{\binom{r+1}{2}}.$$

Then

$$P\{\mathrm{cl}(G_p) = r-1\} = \mathrm{e}^{-\lambda_n} + o(1),$$
$$P\{\mathrm{cl}(G_p) = r\} = \mathrm{e}^{-\mu_n} - \mathrm{e}^{-\lambda_n} + o(1)$$

and

$$P\{\mathrm{cl}(G_p) = r+1\} = 1 - \mathrm{e}^{-\mu_n} + o(1).$$

The form of Corollary 11.8 is slightly misleading: it gives the impression as if in a certain range of n three clique numbers could appear with probabilities bounded away from 0 although, by Corollary 11.2, we know that this is not the case. The explanation is, of course, very simple: given $0 < c < C < \infty$, if n is sufficiently large, then at most one of λ_n and μ_n is in the interval (c, C). Note also that instead of the definition of r in Corollary 11.8, we could have taken $r = \lfloor r_0 \rfloor$ or $r = \lceil r_0 \rceil$, where r_0 is the real number used in the proof of Theorem 11.1 and appearing in Corollary 11.2: an approximation of $r \in \mathbb{R}$ satisfying $E(Y_r) = 1$, with a suitable interpretation of this expectation.

Theorem 11.7 is easily extended to the case when $E(Y_r)$ tends to ∞ rather slowly. However, by the method of Barbour we can do much better. All we have to do is imitate the proof of Theorem 4.15.

Theorem 11.9 *Let $0 < p < 1$ be fixed and let $r = r(n)$ be such that with*

$$\lambda = E(Y_r) = \binom{n}{r} p^{\binom{r}{2}} \text{ we have}$$

$$\underline{\lim}\, \lambda > 0 \text{ and } \lambda = o\{n^2/(\log n)^4\}.$$

Then Y_r has asymptotically Poisson distribution with mean λ:

$$d\{\mathcal{L}(Y_r), P_\lambda\} = O\{\lambda(\log n)^4/n^2 + (\log n)^3/n\}.$$

Proof As in the proof of Theorem 4.15, write $\mathcal{H}$ for the set of all complete r-graphs with vertex set contained in $\{1, 2, \ldots, n\}$, write $\alpha, \beta, \ldots$ for the elements of $\mathcal{H}$ and for $\alpha \in \mathcal{H}$ define a r.v. X_α on $\mathcal{G}(n, p)$ by

$$X_\alpha(G_p) = \begin{cases} 1, & \text{if } \alpha \subset G_p, \\ 0, & \text{otherwise.} \end{cases}$$

Then $Y(G_p) = \sum_{\alpha \in \mathcal{H}} X_\alpha(G_p)$ and, as in Theorem 4.15, we set

$$Y_\alpha = \sum_{\substack{\beta \cap \alpha \neq \emptyset \\ \beta \neq \alpha}} X_\beta \text{ and } p_\alpha = E(X_\alpha) = p^{\binom{r}{2}},$$

where, once again, $\beta \cap \alpha$ is the set of edges shared by β and α.

Furthermore, let A be an arbitrary subset of $\mathbb{Z}^+$ and let $x = x_{\lambda, A}$ be the function defined in Theorem 1.28. As in the proof of Theorem 4.15, our theorem follows if we show that the right-hand side of (17) in Chapter 4 is $O\{\lambda(\log n)^4/n^2\}$. Since, by Theorem 1.28 we have $\Delta x \leq 2\lambda^{-1}$, what we need is that

$$R = \sum_\alpha \sum_{\beta \cap \alpha \neq \emptyset} P_\alpha P_\beta + \sum_\alpha \sum_{\substack{\beta \cap \alpha \neq \emptyset \\ \beta \neq \alpha}} E(X_\alpha X_\beta) = O\{\lambda^2 (\log n)^4/n^2 + \lambda(\log n)^3/n\}.$$

Note that our assumption on λ implies that

$$np^{r/2} = O(r), r = O(np^{r/2}) \text{ and } r \sim 2\log_b n.$$

Therefore

$$\begin{aligned} \sum_\alpha \sum_{\beta \cap \alpha \neq \emptyset} p_\alpha p_\beta &= \binom{n}{r} p^{2\binom{r}{2}} \sum_{l=2}^{r} \binom{n-r}{r-l}\binom{r}{l} \\ &= \lambda^2 \sum_{l=2}^{r} \binom{n-r}{r-l}\binom{r}{l} \Big/ \binom{n}{r} \\ &\leq 2\lambda^2 \binom{n-r}{r-2}\binom{r}{2} \Big/ \binom{n}{r} \leq \lambda^2 r^4/n^2. \end{aligned}$$

Let us turn to the second summand making up R:

$$\sum_\alpha \sum_{\substack{\beta \cap \alpha \neq \emptyset \\ \beta \neq \alpha}} E(X_\alpha X_\beta) = \binom{n}{r} \sum_{l=2}^{r-1} \binom{n-r}{r-l}\binom{r}{l} p^{2\binom{r}{2} - \binom{l}{2}}$$

$$= \binom{n}{r} p^{\binom{r}{2}} \sum_{l=2}^{r-1} \binom{n-r}{r-l} \binom{r}{l} p^{\binom{r}{2}-\binom{l}{2}} = \lambda \sum_{l=2}^{r-1} R_l.$$

Now

$$R_{l+1}/R_l = \frac{(r-l)^2}{(l+1)(n-2r+l+1)} p^{-l},$$

so if l is small, say bounded, then this ratio is $O\{(\log n)^2/n\}$, and if l is large, say $r - l = O(1)$, then rather crudely, the ratio is at least $n^{1/2}$. Hence

$$\begin{aligned} \lambda \sum_{l=2}^{r-1} R_l &\le 2\lambda(R_2 + R_{r-1}) \\ &\le 2\lambda\{\lambda(r^4/n^2)p^{-1} + rnp^{r-1}\} \\ &= O\{\lambda^2(\log n)^4/n^2 + \lambda(\log n)^3/n\}. \end{aligned}$$

Thus

$$R = O\{\lambda(\log n)^4/n^2 + (\log n)^3/n\},$$

as required. □

If $r - r_0 = O(1)$, then $E(Y_r)/E(Y_{r+1}) = \{(r+1)/(n-r)\}p^{-r}$ has order $n/\log n$. This implies that there is a function $r = r(n)$ such that

$$1 \le E(Y_r) \le n^2/(\log n)^5$$

whenever n is sufficiently large; in particular, one can find a function $r = r(n)$ satisfying the conditions of Theorem 11.9. Furthermore, this function is close to being unique: if $0 < c < C < \infty$ and n is sufficiently large, then at most two integers r satisfy

$$c < E(Y_r) < Cn^2/(\log n)^4.$$

The merit of Theorem 11.9 is that it allows us to approximate Y by a Poisson distribution even when $E(Y)$ is rather large. However, if we want to use Theorem 11.9 to provide us with a positive lower bound for $P(Y_r = 0)$, then, unfortunately, the Theorem 11.9 estimate of the total variation distance does not allow us to let $E(Y_r)$ large. Nevertheless, we have the following consequence of Theorem 11.9: if $\lambda = E(Y_r) < \log n - 3\log\log n - \omega(n)$, where $\omega(n) \to \infty$, then

$$P(Y_r = 0) = e^{-\lambda}\{1 + o(1)\}.$$

11.3 Greedy Colouring of Random Graphs

The greedy algorithm is probably the simplest algorithm for colouring the vertices of a graph; in spite of its simplicity, it is often surprisingly efficient [see, for example, Bollobás (1979*a*), Chapter 5, §1]. As we shall see in this section, it also happens to be an algorithm whose performance on a random graph G_p, p constant, can be analysed rather precisely. Given a graph G, order the vertex set, say let $V(G) = \{1, 2, \ldots, n\}$, as when G is a r.g. of order n. Then the *greedy algorithm* colours the vertices with colours $1, 2, \ldots$ by colouring the vertices one by one, starting with vertex 1, and colouring each vertex with the first permissible colour. Thus vertex 1 is coloured 1, vertex 2 is coloured 1 if it is not a neighbour of vertex 1, otherwise it is coloured 2, etc. Denote by $\chi_g(G)$ the number of colours used by the greedy algorithm.

The first results concerning $\chi_g(G_p)$ were proved by Grimmett and McDiarmid (1975); these results were sharpened considerably by Bollobás and Erdős (1976*a*).

Theorem 11.10 *Let* $0 < p < 1$ *be fixed*, $q = 1 - p$ *and* $d = 1/q$.

(i) Let $0 < \gamma < \frac{1}{2}$ *be fixed and let* $u = u(n) \geq \gamma^{-1/2}$. *If* n *is sufficiently large, then*

$$P\left[\chi_g(G_p) < \frac{n}{\log_d n}\{1 + u(\log_d n)^{-1/2}\}^{-1}\right] < n^{-\gamma u^2 + 1}.$$

(ii) Let $0 < \tau_0 = \tau_0(n) < 1$ *and* $k_0(n) = \lceil n/[\{1 - \tau_0(n)\} \log_d n]\rceil$. *Then*

$$P\{\chi_g(G_p) > k_0(n)\} < \exp(\log n - n^{\tau_0}/\log_d n).$$

Proof (i) We shall prove considerably more than we have to: we shall show that for each $l, 1 \leq 1 \leq n$, with probability greater than $1 - n^{-\gamma u^2}$ the lth colour class C_l has fewer than

$$k = k(n) = \lceil \log_d n \rceil + \lfloor u(n)(\log_d n)^{1/2} \rfloor = k_1(n) + k_2(n) = k_1 + k_2$$

vertices.

Indeed, what is the probability $P(l; j_1, j_2, \ldots, j_{k_2})$ that for each $i, 1 \leq i \leq k_2$ vertex j_i is precisely the $(k_1 + i)$th vertex of C_l? Clearly

$$P(l; j_1, j_2, \ldots, j_{k_2}) \leq \prod_{i=1}^{k_2} q^{k_1 + i - 1} = q^{k_1 k_2 + k_2(k_2 - 1)/2},$$

since the probability that vertex j_i is not joined to any vertex in a given set of $k_1 + i - 1$ vertices is precisely q^{k_1+i-1}. Hence

$$\begin{aligned} P(|C_l| \geq k_1 + k_2) &\leq \binom{n}{k_2} q^{k_1k_2+k_2(k_2-1)/2} \\ &< n^{k_2} q^{k_1k_2+k_2(k_2-1)/2} \leq q^{k_2(k_2-1)/2} < n^{-\gamma u^2}, \end{aligned}$$

if n is sufficiently large.

Therefore with probability greater than $1 - n^{1-\gamma u^2}$ every colour class produced by the greedy algorithm has at most $k-1$ vertices so $P\{\chi_g(G_p) < n/(k-1)\} < n^{1-\gamma u^2}$.

(ii) Let A_j^k be the event that at least k colours are used to colour the first j vertices, let $A^k = A_n^k$ be the event $\chi_g(G_p) \geq k$ and let B_j^k be the event that vertex j gets colour k. Note that for $1 \leq j < n$ we have

$$B_{j+1}^{k+1} \subset A_j^k \subset A_{j+1}^k \subset A^k \text{ and } A^{k+1} = \bigcup_{j=k+1}^{n} B_j^{k+1}.$$

At most how large is the conditional probability $P(B_{j+1}^{k+1}|A_j^k)$? Suppose when we are about to colour vertex $j+1$, we have j_i vertices of colour i, $1 \leq i \leq k$. Then the probability that vertex $j+1$ gets colour $k+1$ is precisely

$$\prod_{i=1}^{k}(1 - q^{j_i}) \leq (1 - q^{j/k})^k \leq \exp\{-q^{j/k}k\} = P_{j,k}$$

since $\log(1 - q^x)$ is convex for $x > 0$ and $\sum_{i=1}^{k} j_i \leq j$. Hence

$$P(B_{j+1}^{k+1}|A_j^k) \leq P_{j,k}$$

and so

$$P(B_{j+1}^{k+1}|A^k) \leq P_{j,k}$$

and

$$P(A^{k+1}) \leq P(A^{k+1}|A^k) \leq \sum_{j=k+1}^{n} P_{j,k} \leq nP_{n,k}.$$

Therefore

$$\begin{aligned} P(A^{k_0(n)+1}) \leq nP_{n,k_0(n)} &= n\exp(-q^{n/k_0(n)}k_0(n)) \\ &< n\exp(-q^{(1-\tau_0)\log_d n} n/\log_d n) \\ &= \exp(\log n - n^{\tau_0}/\log_d n), \end{aligned}$$

as claimed. □

With $\gamma = \frac{1}{3}, u(n) = 2(\log\log n)^{1/2}$ and $\tau_0(n) = 4(\log\log n)/\log n$ we find, rather crudely, that

$$P\left[\chi_g(G_p) < \frac{n}{\log_d n}\{1 - 3(\log\log n)^{1/2}/(\log n)^{1/2}\}\right] < n^{-\log\log n}$$

and

$$P\left[\chi_g(G_p) > \frac{n}{\log_d n}\{1 + 5(\log\log n)/\log n\}\right] < n^{-\log n}.$$

These inequalities imply the following assertion.

Corollary 11.11 *For p and d as in Theorem 11.10, $\chi_g(G_p)(\log_d n)/n \to 1$ in any mean and almost surely.* □

Unfortunately, the results concerning the *chromatic number* $\chi(G_{n,p})$ are rather weak. A graph G of order n and independence number $\beta_0(G)$ has chromatic number at least $\lceil n/\beta_0(G)\rceil$ and the number of colours used by the greedy algorithm in some order is at most the chromatic number. Furthermore, $\beta_0(G) = \mathrm{cl}(\overline{G})$, where $\overline{G}$ is the complement of G, and the complement of a G_p is a G_p, so Corollary 11.2 and Theorem 11.10 have the following consequence.

Theorem 11.12 *Let $0 < p < 1$ and $\varepsilon > 0$ be fixed and set $d = 1/(1-p)$. Then a.e. G_p satisfies*

$$\frac{n}{2\log_d n}(1+\log_d \log n/\log n) \le \chi(G_p) \le \frac{n}{\log_d n}\{1+(2+\varepsilon)\log\log n/\log n\}.$$

□

As we shall see in §4, the upper bound in Theorem 11.12, proved by the greedy algorithm, can almost be halved and $\chi(G_p) = \{\frac{1}{2} + o(1)\}n/\log_d n$ for a.e. G_p. The difficulty is in finding a colouring algorithm which gets much closer than the greedy algorithm to the real chromatic number and still does not test too many edges, so that a semblance of independence remains and allows us to analyse the algorithm. This difficulty will be overcome by making use of martingale inequalities.

As usual, let $p_G(x)$ be the chromatic polynomial of a graph G so that $p_G(k)$ is the number of k-colourings of G. As shown by Grimmett and McDiarmid (1975), the expectation of $p_{G_p}(k)$ has a sharp increase around $k = [\frac{1}{2}n/\log_d n]$. The proof is left as an exercise (Ex. 5).

Theorem 11.13 *Let $0 < p < 1$ and $c > 0$ be constants and set $d = 1/(1-p)$ and $k = \lfloor cn/\log_d n \rfloor$. Then*

$$\lim_{n\to\infty} E\{p_{G_{n,p}}(k)\} = \begin{cases} 0, & \text{if } c < \frac{1}{2}, \\ \infty, & \text{if } c > \frac{1}{2} \end{cases}. \qquad \square$$

The result above seems to indicate that $\chi(G_p)$ is indeed about $\frac{1}{2}n/\log_d n$ for a.e. G_p; the trouble is that for $k \sim (\frac{1}{2}+\varepsilon)n/\log_d n$ the variance of $p_{G_p}(k)$ is rather large so Chebyshev's inequality does not imply that $p_{G_p}(k) > 0$ for a.e. G_p.

Let us take another look at the greedy algorithm. By Theorem 11.10(ii) we know that the probability of the greedy algorithm using substantially more than $n/\log_d n$ colours is very small. In fact, as pointed out by McDiarmid (1979*a*), if we wish, we can very easily obtain a much better bound on the probability of this unlikely event. Indeed, in the proof we were very generous: all we used was that the (k_0+1)st colour is unlikely to occur, even if k_0 colours do occur. But for any $k \in \mathbb{N}$ the (k_0+k)th colour is even less likely to arise provided the first k_0+k-1 colours do occur. Hence the least we can conclude from the proof is that

$$P\{\chi_g(G_p) \geq k_0 + k\} < \exp(k \log n - kn^{\tau_0}/\log_d n).$$

For example, if $3(\log\log n)/\log n \leq \tau_1(n) < 1$,

$$\tau_0(n) = \tau_1(n) - 1/\log n \text{ and } k_i(n) = \lceil n/(1-\tau_i)\log_d n \rceil, i = 0, 1,$$

then, for sufficiently large n, we have

$$\begin{aligned} P\{\chi_g(G_p) \geq k_1\} &\leq \prod_{k=k_0}^{k_1-1} P(A^{k+1}|A^k) \\ &\leq \exp\{(k_1 - k_0)\log n - (1/e)(k_1 - k_0)n^{\tau_1}/\log_d n\} \\ &\leq \exp\{n/(\log_d n) - \frac{1}{3}n^{1+\tau_1}(\log_d n)^{-2}(\log n)^{-1}\} \\ &\leq \exp\{-\frac{1}{4}n^{1+\tau_1}(\log_d n)^{-2}(\log n)^{-1}\} \\ &= \exp\{-c_0 n^{1+\tau_1}/(\log n)^3\}, \end{aligned}$$

where $c_0 = (\log d)^2/4$. In the estimate above, we made use of the facts that $k_1 - k_0 \sim n(\log_d n)^{-1}(\log n)^{-1}$ and $n^{\tau_1}/(\log n)^2 \to \infty$. This proves the following theorem of McDiarmid (1979*a*).

Theorem 11.14 *Let $3(\log\log n)/\log n \leq \tau_1 = \tau_1(n) < 1$. Then*

$$P\{\chi_g(G_p) \geq n/(1-\tau_1)\log_d n\} < \exp\{-c_0 n^{1+\tau_1}/(\log n)^3\}. \qquad \square$$

The bound in Theorem 11.14 is rather small, even if $\tau_1(n) \to 0$ rather fast. For example, with $\tau_1 = \frac{9}{2}(\log\log n)/\log n$ the bound is $o(1/n!)$. Since there are $n!$ ways of ordering the vertices of G_p, we arrive at the following result of McDiarmid (1979*a*).

Corollary 11.15 *A.e. G_p is such that, no matter what order of the vertices we take, the greedy algorithm uses fewer than $\{1+5(\log\log n)/\log n\}n/\log_d n$ colours.* □

This corollary is fairly surprising, since for every $k \geq 2$ there is a bipartite graph on $\{1, 2, \ldots, 2k-2\}$ for which the greedy algorithm uses no fewer than k colours.

As another application of Theorem 11.14, McDiarmid (1983) proved that a.e. G_p is such that every subgraph of it with chromatic number $\chi(G_p)$ has almost $n/2$ vertices. However, as we shall see in §4, much more is true: $n/2 + o(n)$ can be replaced by $n + o(n)$.

11.4 The Chromatic Number of Random Graphs

Martingale inequalities can be used in two rather different ways. First, they may enable us to prove that α r.v. is concentrated in a *very short* interval with probability tending to 1 and, second, they may imply that α r.v. is concentrated in a not too short interval with probability *extremely close* to 1. In combinations, both uses of martingale inequalities first occurred in connection with the chromatic number of random graphs. Earlier these inequalities had been used in the geometry of Banach spaces but, rather surprisingly, were hardly ever used in probability theory.

There are two natural filtrations on the space $\mathcal{G}(n,p)$ that give rise to martingales that are frequently used in proving concentration results: the vertex-revealing filtration and the edge-revealing filtration.

The *vertex-revealing filtration* $\mathscr{F}_0 \subset \mathscr{F}_1 \subset \ldots \subset \mathscr{F}_n$ is defined by taking for $\mathscr{F}_k$ the σ-field in which an atom is the set of graphs on $[n]$ inducing the some subgraph on $[k]$. More precisely, set $G \equiv_k^v H$ if $G[k] = H[k]$, and let the equivalence classes of the equivalence relation $\equiv_k^v$ be the atoms of $\mathscr{F}_k$. (Here v stands for *vertex* and k shows that we have the kth equivalence relation.)

For a r.v. X on $\mathcal{G}(n,p)$, the *vertex-revealing martingale of* X is the sequence $(X_k)_0^n$ with $X_k = E(X|\mathscr{F}_k)$. Clearly, if X is such that $|X(G) - X(H)| \leq c$ whenever G and H differ only in some edges incident with a single vertex, then $|X_k - X_{k-1}| \leq c$ for every k.

The edge-revealing filtration and edge-revealing martingale are defined similarly. Let $e_1, \ldots, e_N$ be an enumeration of the N pairs $[n]^{(2)}$, i.e., the N possible edges of a graph on $[n]$. For $0 \leq k \leq N$ and $G, H \in \mathscr{G}^n$, set $G \equiv_k^e H$ if for $i \leq k$ we have $e_2 \in E(G)$ iff $e_i \in E(H)$. (Needless to say, here e stands for *edge*.) Let $\mathscr{F}_k$ be the σ-field whose atoms are the classes of the equivalence relation $\equiv_k^e$. The nested sequence $\mathscr{F}_0 \subset \mathscr{F}_1 \subset \ldots \subset \mathscr{F}_N$ is the *edge-revealing filtration* associated with the order $e_1, e_2, \ldots, e_N$, and, for a r.v. X, the sequence $(X_k)_0^n$, defined by $X_k = E(X|\mathscr{F}_k)$, is the *edge-revealing martingale* of X associated with the order. Finally, if X is such that $|X(G) - X(H)| \leq c$ whenever G is obtained from H by adding a single edge then $|X_k - X_{k-1}| \leq c$ for every k.

Clearly, the choice of the martingale depends on the random variable we wish to study. For example, suppose that $X = X(G_{n,p})$ is a graph invariant such that

$$|X(G) - X(H)| \leq c \tag{11.7}$$

whenever $E(G)\Delta E(H)$ consists only of edges incident with the some vertex. Then, taking the vertex-revealing martingale of X, we find that either Theorem 1.19 or Theorem 1.20 implies that, for $t > 0$,

$$P(X \leq EX - t) \leq \mathrm{e}^{-t^2/2nc^2} \tag{11.8}$$

and

$$P(|X - EX| \geq t) \leq 2\mathrm{e}^{-t^2/2nc^2}. \tag{11.9}$$

There are many graph invariants that satisfy (7) for a small value of c. For example, if X is the clique number then (7) holds with $c = l$, so

$$P(|l(G_{n,p}) - E(l(G_{n,p}))| \geq t) \leq 2\mathrm{e}^{-t^2/2n}.$$

Similarly, the chromatic number of a graph changes by at most 1 if we change some of the edges incident with a vertex, so

$$P(|\chi(G_{n,p}) - E(\chi(G_{n,p}))| \geq t) \leq 2\mathrm{e}^{-t^2/2n}.$$

In particular, if $\omega(n) \to \infty$ then a.e. $G_{n,p} \in \mathscr{G}(n,p)$ is such that its clique number is within $\omega(n)n^{1/2}$ of $f(n) = E(l(G_{n,p}))$ and its chromatic number is within $\omega(n)n^{1/2}$ of $g(n) = E(\chi(G_{n,p}))$. This theorem of Shamir and Spencer (1987) was the first result about random graphs that used a martingale inequality to prove that, with probability tending to 1, a r.v. is concentrated in a short interval. In fact, Shamir and Spencer also proved that for small values of p the chrometic number of a.e. $G_{n,p}$ is in a considerably shorter interval.

Theorem 11.16 *Let* $0 < p = p(n) = cn^{-\alpha} < 1$, *where* $c > 0$ *and* $0 \le \alpha < 1$. *Then there is a function* $u(p, n)$ *such that*

(*i*) *if* $0 \le \alpha < 1/2$ *and* $\omega(n) \to \infty$ *then*

$$P(u \le \chi(G_{n,p}) \le u + \omega(n)(\log n)n^{1/2-\alpha}) \to 1$$

as $n \to \infty$,

(*ii*) *if* $1/2 < \alpha < 1$ *then*

$$P\left(u \le \chi(G_{n,p}) \le u + \left\lceil \frac{2\alpha + 1}{2\alpha - 1} \right\rceil\right) \to 1. \qquad \square$$

Note that, in particular, if $\alpha > \frac{5}{6}$ than, for a.e. $G_{n,p}$, the chromatic number $\chi(G_{n,p})$ takes one of five values.

What is fascinating about the result above is that although it tells us that for $p = \frac{1}{2}$, say, $\chi(G_{n,1/2})$ is concentrated in an interval of length $\omega(n)(\log n)n^{1/2}$, it gives no information about the location of this interval. All we know, from Theorem 11.12, is that this interval is contained in the interval $\left[(1 + o(1))\frac{n}{2\log_2 n}, (1 + o(1))\frac{n}{\log_2 n}\right]$.

To locate the position of this interval or, equivalently, to determine the asymptotic value of $E(X(G_{n,p}))$, Bollobás (1988*c*) used the other strength of our martingale inequalities, namely that they can guarantee exponentially small probabilities of 'bowl events'. It turns out that, for p fixed, say, a.e. $G_{n,p}$ is such that $X(G_{n,p})$ is about as small as permitted by Theorem 11.12.

We shall use a simple-minded way of colouring a graph. This method gives an inefficient algorithm, much worse than the greedy algorithm, but it is easy to describe, and it is also easy to analyse it for $G_{n,p}$. To colour a graph G, first select an independent set V_1 of G of maximal size, and set $G_1 = G \backslash V_1$. Next, select an independent set V_2 of G_1 of maximal size and set $G_2 = G_1 \backslash V_2 = G \backslash V_1 \cup V_2$. Proceeding in this way, we get a partition $V(G) = V_1 \cup V_2 \cup \ldots \cup V_k$ of the vertex set into independent sets and so a colouring of G. If our aim is to show that a graph G of order n satisfies $\chi(G) \le (1 + o(1))n/2\log_2 n$, as when $G = G_{n,1/2}$, than it suffices to show that we have $|V_i| \ge (1 + o(1))\log_2 n$ for $1 \le i \le h$, where h is such that $G_h = G \backslash V_1 \cup \ldots \cup V_h$ has $o(n/\log_2 n)$ vertices. To achieve this, it suffices to prove that for some $r = (1 + o(1))\log_2 n$ the probability that $G_{n,1/2}$ does *not* have r independent vertices is extremely small, say, at most $e^{-n^{1+\varepsilon}}$ for some $\varepsilon > 0$. A straightforward way of proving this would be to show that the number Y_r of independent r-sets is highly concentrated. Although this is true, it is not easily proved.

Following the idea in Bollobás (1988*c*), what we *can* prove very easily is that a variant of Y_r is highly concentrated. As customary, we formulate the result in terms of complete graphs rather than independent sets. As before, write $Y_r = Y_r(G_{n,p})$ for the number of complete r-graphs in $G_{n,p}$, and $E_r = E(n,r)$ for the expectation $E(Y_r(G_{n,p}))$.

Theorem 11.17 *Let $0 < p < 1$ be fixed, and let $r_1 = r_1(n) \geq 3$ and $\alpha = \alpha(n) \geq 1/2$ be such that $E_p(n, r_1) = n^\alpha = o(n^2/(\log n)^2)$. Then for $0 < c \leq 1$ we have*

$$P(Y_{r_1} \leq (1-c)n^\alpha) \leq \exp\{-(c^2 + o(1))n^{2\alpha-2}\}.$$

Proof Let $r_0 = r_0(n,p)$ be as defined after relation (11.1). Thus, if r_0 is an integer then $E_p(n, r_0) = 1$, otherwise $E_p(n, \lceil r_0 \rceil) < 1 < E_p(n, \lfloor r_0 \rfloor)$. Also, $r_0 = 2\log_b n - 2\log_b \log_b n + O(1)$, where $b = 1/p$, and $\mathrm{e}n/r_0 \sim p^{-r_0/2}$. Since for $r - r_0 = O(1)$ we have $E_p(n, r+1)/E_p(n,r) = \frac{n-r}{r+1}p^r \sim \frac{h}{r}p^{r-r_0}\left(\frac{r_0}{\mathrm{e}n}\right)^2 \sim \frac{r_0}{\mathrm{e}^2 n}p^{r-r_0} = \Theta\left(\frac{\log n}{n}\right)$, for n large enough r_1 and α can be chosen as prescribed. Furthermore, for $r' \geq r_0 + 1$ we have $E_p(n, r') = o(1)$, and if $3 \leq r'' \leq r_0 - 3$ than $E_p(n, r'')/n^2 \to \infty$. Hence $r_0 - 3 < r_1 < r_0 + 1$ and so, in particular,

$$p^{-r_1} = \Theta\left(\frac{n^2}{(\log n)^2}\right).$$

Let $U = U(G_{n,p})$ be the maximal number of edge-disjoint complete r_1-graphs K^{r_1} in $G_{n,p}$. By definition, $U \leq Y_{r_1}$, so it suffices to bound the probability that

$$U \leq (1-c)n^\alpha.$$

Let $(U_k)_0^N$ be on edge-revealing martingale obtained from U, i.e., with $U_N = U$. Then $|U_k - U_{k-1}| \leq 1$ for every k so, by Theorem 1.19,

$$\begin{aligned} P(U \leq (1-c)n^\alpha) &\leq \exp\{-(E(U) - (1-c)n^\alpha)^2/2N\} \\ &\leq \exp\{-(E(U) - (1-c)n^\alpha)^2/n^2\}, \end{aligned}$$

provided $E(U) > (1-c)n^\alpha$. Hence, the theorem follows if we show that $E(U) = (1+o(1))n^\alpha$.

In fact, more is true: let $U'(G_{n,p})$ be the number of complete r_1-graphs in $G_{n,p}$ that share no edge with another K^{r_1}. Then $U' \leq U$, and

$$E(U') \geq \binom{n}{r_1} p^{\binom{r_1}{2}} - \sum_{l=2}^{r_1-1} \binom{n}{r_1}\binom{n-r_1}{r_1-l} p^{2\binom{r_1}{2}-\binom{l}{2}}$$

Proceeding as in the proof of Theorem 11.1, we find that

$$E(U') \geq (1+o(1)) \binom{n}{r_1} p^{\binom{r_1}{2}},$$

and so $E(U) \geq E(U') = (1+o(1))n^{\alpha}$, completing the proof. □

After this preparation, it is easy to determine the chromatic number of a.e. random graph $G_{n,p}$.

Theorem 11.18 *Let $0 < p < 1$ be fixed, and set $q = 1 - p$ and $d = 1/q$. Then a.e. $G_{n,p}$ is such that*

$$\frac{n}{2\log_d n}\left(1 + \frac{\log\log n}{\log n}\right) \leq \chi(G_{n,p}) \leq \frac{n}{2\log_d n}\left(1 + \frac{3\log\log n}{\log n}\right).$$

In particular, $\chi(G_{n,p}) = (1+o(1))n/2\log_d n$ for a.e. $G_{n,p}$.

Proof The lower bound is in Theorem 11.12, so our task is to prove the upper bound.

Set $s_1 = \lceil 2\log_d n - 5\log_d \log n \rceil$, and let n_1 be the smallest natural number such that

$$E_q(n_1, s_1) \geq 2n^{5/3}.$$

It is easily seen that if n is large enough,

$$n/(\log n)^3 \leq n_1 \leq n/(\log n)(\log\log n)$$

and

$$2n^{5/3} \leq E_q(n_1, s_1) \leq 3n^{5/3}.$$

Hence, by Theorem 11.17,

$$P(\mathrm{cl}(G_{n_1,q}) < s_1) \leq e^{-n^{4/3}}$$

This implies that a.e. $G_{n,p}$ is such that every set of n_1 vertices contains s_1 independent vertices, and so

$$\chi(G_{n,p}) \leq \frac{n}{s_1} + n_1 \leq \frac{n}{2\log_d n}(1 + 3\log_d \log n),$$

as claimed. □

Matula (1987) used a rather different approach to the study of the chromatic number of a random graph; with this '*expose-and-merge*' algorithm, Matula and Kučera (1990) gave an alternative proof of Theorem 11.18.

As an immediate consequence of Theorem 11.18, we see that a.e. $G_{n,p}$

is such that every subgraph of chromatic number $\chi(G_{n,p})$ has $(1+o(1))n$ vertices.

By refining the above proof of Theorem 11.18, McDiarmid (1990) proved that $\chi(G_{n,p})$ is concentrated in an even smaller interval than claimed there.

Theorem 11.19 *Let $0 < p < 1$ be fixed, and set $q = 1 - p, d = 1/q$ and $s = s(n) = 2\log_d n - 2\log_d \log_d n + 2\log_d(\mathrm{e}/2)$. Then for a.e. $G_{n,p}$ we have*

$$\frac{n}{r + o(1)} \le \chi(G_{n,p}) \le \frac{n}{r - \frac{1}{2} - \frac{1}{1-\sqrt{q}} + o(1)}. \qquad \square$$

Although for close to thirty years the aim had been to prove that $\chi(G_{n,p})$ is highly concentrated, after the results above the obvious task is to show that $\chi(G_{n,p})$ is *not* concentrated in a very short interval. It would not be too surprising if, for a fixed p, the shortest interval containing the chromatic number of a.e. $G_{n,p}$ were of order about $n^{1/2}$, but at the moment we cannot even exclude the unlikely possibility that for some $l = l(p)$ and $c = c(n,p)$, the chromatic number of a.e. $G_{n,p}$ is in the interval $[c, c+l]$.

11.5 Sparse Graphs

As we remarked at the end of §1, if p is large (more precisely, if $q \to 0$ rather fast) then instead of studying the clique number of $G_{n,p}$ it is more natural to study the independence number of $\overline{G}_{n,p}$. However, rather than deal with $\overline{G}_{n,p}$, we take p small and study the independence number of G_p. Let us start with some results of Bollobás and Thomason (1985).

Let $p = \alpha/n$, where $0 < \alpha = \alpha(n) < n$. To start with, let α be constant and set

$$f(\alpha) = \sup\{c : \lim_{n\to\infty} P\{\beta_0(G_{n,p}) > cn\} = 1\},$$

where, as before, $\beta_0(G)$ denotes the (vertex) independence number of G, i.e. the maximal cardinality of an independent set of vertices.

In the range $0 < \alpha \le 1$, we have an explicit formula for $f(\alpha)$. Although the formula is far from being pretty, it does enable us to compute particular values of $f(\alpha)$.

Theorem 11.20 *For $0 < \alpha \le 1$ we have $f(\alpha) = f_1(\alpha) + f_2(\alpha)$, where*

$$f_1(\alpha) = \mathrm{e}^{-\alpha} + \frac{1}{\alpha}\sum_{k=2}^{\infty}\sum_{l=1}^{k-1}\frac{k^l l^{k-1}}{k!\,l!}(\alpha\mathrm{e}^{-\alpha})^{k+l} + \frac{1}{2\alpha}\sum_{k=1}^{\infty}\frac{k^{2k-1}}{(k!)^2}(\alpha\mathrm{e}^{-\alpha})^{2k}$$

and

$$f_2(\alpha) = \frac{1}{\alpha} \sum_{k=1}^{\infty} \sum_{l=0}^{k} \sum_{m=k}^{2k-1} \frac{m-k}{(k+l)!} (\alpha e^{-\alpha})^{k+l} t_{k,l,m},$$

where $t_{k,l,m}$ is the number of trees on $\{1, 2, \ldots, k+l\}$ with bipartition (k, l) and independence number m.

Proof The result is an easy consequence of some results of Chapter 5. By Theorem 11.7(ii) and Ex. 3 of Chapter 5 we know that for $p = \alpha/n \leq 1/n$ a.e. $G_{n,p}$ is such that all but $o(n)$ of the vertices belong to trees. Furthermore, for every fixed tree T a.e. $G_{n,p}$ has

$$\{1 + o(1)\} \frac{n}{\alpha} \frac{1}{a(T)} (\alpha e^{-\alpha})^{|T|} \tag{11.10}$$

components isomorphic to T, where $a(T)$ is the order of the automorphism group of T and $|T|$ is the order of T.

Denote by $\mathscr{F}_s$ the set of trees with vertex set $\{1, 2, \ldots, s\}$ and by $\mathscr{F}_{k,l}$ the set of trees with vertex set $\{1, 2, \ldots, k+l\}$ in which every edge is of the form ij with $i \leq k$ and $j > k$. Thus

$$|\mathscr{F}_s| = s^{s-2} \text{ and } |\mathscr{F}_{k,l}| = k^{l-1} l^{k-1}.$$

Then, by (10),

$$f(\alpha) = \frac{1}{\alpha} \sum_{s=1}^{\infty} \sum_{T \in \mathscr{F}_s} \frac{\beta_0(T)}{s!} (\alpha e^{-\alpha})^s. \tag{11.11}$$

Given a tree T, denote by $\beta_0'(T)$ the cardinality of a largest colour class of T, considered as a 2-chromatic graph. Thus, if $l \leq k$ and $T \in \mathscr{F}_{k,l}$, then $\beta_0'(T) = k = \beta_0(T)$. Hence, by (11),

$$f(\alpha) \geq \frac{1}{\alpha} \sum_{s=1}^{\infty} \sum_{T \in \mathscr{F}_s} \frac{\beta_0'(T)}{s!} (\alpha e^{-\alpha})^s. \tag{11.12}$$

Since for $s = k+l, k > l$, the set $\mathscr{F}_s$ contains $\binom{s}{k} k^{l-1} l^{k-1}$ trees isomorphic to some tree in $\mathscr{F}_{k,l}$, and for $s = 2k$ the set $\mathscr{F}_s$ contains $\frac{1}{2} \binom{s}{k} k^{2k-2}$ trees isomorphic to some tree in $\mathscr{F}_{k,k}$, the right-hand side of (12) is $f_1(\alpha)$ and the difference of the two sides is precisely $f_2(\alpha)$. □

Although the series giving $f_1(\alpha)$ does not converge fast, it is fairly easy to calculate concrete values of $f_1(\alpha)$. The series of $f_2(\alpha)$ is not too pleasant, but it does converge fast.

For $\alpha > 1$ the lower bounds on $f(\alpha)$ are rather weak. In fact, for some values of α we can hardly do better than apply the following theorem of Shearer (1983) concerning the independence number of (non-random) triangle-free graphs. The theorem will be proved, in a slightly different form, in the next chapter (Theorem 12.13; as we shall see there, the proof is based on the greedy algorithm for constructing independent sets.

Theorem 11.21 *The independence number of a triangle-free graph of order n and average degree at most $\alpha > 1$ is at least $\{(\alpha \log \alpha - \alpha + 1)/(\alpha - 1)^2\}n$.* □

Corollary 11.22 $f(\alpha) \geq (\alpha \log \alpha - \alpha + 1)/(\alpha - 1)^2$ *for all* $\alpha > 1$.

Proof Let $1 < \alpha < \alpha_1$. Since

$$E\{Y_3(G_{n,\alpha/n})\} = E\{k_3(G_{n,\alpha/n})\} = \binom{n}{3}(\alpha/n)^3 \sim \alpha^3/6,$$

a.e. $G_{n,\alpha/n}$ has at most $\log n$ triangles. Hence a.e. $G_{n,\alpha/n}$ contains a triangle-free subgraph G_0 spanned by at least $n - \log n$ vertices. Furthermore, a.e. $G_{n,\alpha/n}$ is such that G_0 has average degree at most α_1. Consequently

$$\beta_0(G_{n,\alpha/n}) \geq \beta_0(G_0) \geq \frac{\alpha_1 \log \alpha_1 - \alpha_1 + 1}{(\alpha_1 - 1)^2}(n - \log n)$$

for a.e. $G_{n,\alpha/n}$, proving the corollary. □

There are slightly better lower bounds on $f(\alpha)$, but we shall not go into them. However, in estimating the chromatic number of a sparse r.g., we shall need the following bound on $\beta_g(G_{n,p})$, the order of the independent set of $G_{n,p}$ constructed by the greedy algorithm. For a proof the reader is referred to Bollobás and Thomason (1985).

Theorem 11.23 *Let* $p = \alpha(n)/n, 0 < \alpha \leq n/2$.
(*i*) *If* $\alpha > 0$ *is constant, then with probability* $1 - 0(n^{-1})$

$$f(\alpha)n \geq \beta_g(G_{n,p}) \geq \frac{\log(\alpha+1)}{\alpha}n.$$

(*ii*) *If* $\alpha(n) = o(n/\log n)$, *then for every fixed positive* ε

$$\beta_g(G_{n,p}) \geq \frac{\log \alpha - \varepsilon}{\alpha}n$$

holds with probability $1 - O\{\alpha(n)/n\}$.

(*iii*) *If* $\alpha(n) \geq n^{1/2}$, *then for every fixed positive* ε

$$\beta_g(G_{n,p}) \geq (1-\varepsilon)\frac{\log \alpha}{n\log\{1/(1-\alpha/n)\}}$$

holds with probability $1 - O(n^{-1/2})$.

Now let us turn to upper bounds on the independence number of r.gs. The basic bound is based on an estimate of the expected number of independent sets of a certain size.

Lemma 11.24 *Suppose* $1 < \alpha = \alpha(n) < n$ *and* $b = b(n) > 1$ *are such that*

$$\frac{n}{b}\left\{\frac{\alpha}{2b} - b\log b + (b-1)\log(b-1) - \frac{\alpha}{2n}\right\} \to \infty. \tag{11.13}$$

Then a.e. $G_{n,\alpha/n}$ *satisfies*

$$\beta_0(G_{n,\alpha/n}) \leq n/b.$$

Proof We may suppose that $k = n/b$ is an integer. Set $p = \alpha/n$ and write E_k for the expected number of independent k-sets in G_p. It suffices to show that $\lim_{n\to\infty} E_k = 0$. Clearly, by inequality (1.5),

$$\begin{aligned} E_k &= \binom{n}{k}(1-p)^{\binom{k}{2}} \leq b^n(b-1)^{-(b-1)n/b}\exp\left(-\frac{pk^2}{2}+\frac{pk}{2}\right) \\ &= \exp\left\{n\left(\log b - \frac{b-1}{b}\log(b-1) + \frac{\alpha}{2bn} - \frac{\alpha}{2b^2}\right)\right\} \to 0. \end{aligned}$$ □

For large values of α the upper bound on $f(\alpha)$, implied by Lemma 11.24, is about $2\log\alpha/\alpha$, as shown by Bollobás and Thomason (1985), Gazmuri (1984), McDiarmid (1984) and de la Vega (1984).

Theorem 11.25 (*i*) *Suppose* $\alpha > 1$ *and* $b > 1$ *are constants and*

$$2b^2\log b - 2b(b-1)\log(b-1) < \alpha. \tag{11.14}$$

Then

$$f(\alpha) \leq 1/b.$$

(*ii*) *If* $2.27 < \alpha = \alpha(n) \leq n/2$, *then a.e.* $G_{n,\alpha/n}$ *satisfies*

$$\beta_0(G_{n,\alpha/n}) \leq \frac{2\log\alpha}{\alpha}n.$$

In particular,

$$f(\alpha) \leq 2\log\alpha/\alpha$$

for all $\alpha > 2.27$.

(iii) If $\alpha(n) \to \infty$ *and* $\alpha(n) \le 3n/4$, *then*

$$\beta_0(G_{n,\alpha/n}) \le 2\log_d \alpha \le \frac{2\log\alpha}{\alpha}n,$$

almost surely, where $d = 1/q = 1/(1-\alpha/n)$.

(iv) If $0 < \alpha(n) \le (1 - 1/\log n)n$, *then*

$$\beta_0(G_{n,\alpha/n}) \le 2\log_d n$$

almost surely, where $d = 1/(1-\alpha/n)$.

Proof (i) Inequality (11.14) implies (11.13) if n is sufficiently large.

(ii) For $\alpha > \mathrm{e}^{\mathrm{e}/2} + 0.1$ and $b = \alpha/2\log\alpha$ the expression in (11.13) is

$$\begin{aligned}&(n/b)[\log\alpha - (b-1)\{\log b - \log(b-1)\} - \log b - \alpha/2n]\\ &\ge (n/b)(\log\alpha - 1 - \log b - \alpha/2n)\\ &= (n/b)(\log\log\alpha + \log 2 - 1 - \alpha/2n) \to \infty.\end{aligned}$$

For $2.27 < \alpha \le \mathrm{e}^{\mathrm{e}/2} + 0.1$ the assertion follows from Lemma 11.24 by a computer check.

(iii) With $k = \lceil 2\log_d \alpha\rceil$ and E_k as in Lemma 11.24, we have

$$\begin{aligned}E_k = \binom{n}{k} q^{\binom{k}{2}} &\le \left(\frac{\mathrm{e}n}{k}\right)^k q^{\binom{k}{2}} \le \left(6\frac{n}{k}\alpha^{-1}\right)^k \le \left(3n\frac{-\log(1-\alpha/n)}{(\log\alpha)\alpha}\right)^k\\ &\le \left(6n\frac{\alpha/n}{(\log\alpha)\alpha}\right)^k = \left(\frac{6}{\log\alpha}\right)^k < 1\end{aligned}$$

if n is sufficiently large

(iv) Proceed as in the proof of (iii). □

The number of colours used by the greedy algorithm defined in §3, $\chi_g(G_{n,p})$, gives a rather poor upper bound for $\chi(G_{n,p})$ if p is small, say $p = c/n$. Indeed, a.e. $G_{n,c/n}$ satisfies

$$\chi_g(G_{c/n}) \ge k \tag{11.15}$$

for all constants $k \in \mathbb{N}$ and $c > 0$. This can be seen as follows. It is easily proved (Ex. 6) that for every $k \in \mathbb{N}$ there is a tree T with vertex set $W = \{1, 2, \dots, 2^{k-1}\}$ such that $\chi_g(T) \ge k$, where χ_g is taken with respect to the natural order on W. By Ex. 6 of Chapter 4, a.e. $G_{n,c/n}$ has a component isomorphic to T, with the unique order-preserving map giving an isomorphism, so (11.15) holds.

In view of (11.15), for small values of p we shall apply a variant of the greedy algorithm to colour a r.g. $G_{n,p}$. Use the greedy algorithm to construct the colour classes one by one. If at any stage the graph H spanned by the remaining vertices is such that all its components are trees and unicyclic graphs then colour H with $\chi(H)$ colours. [Clearly $\chi(H) = 3$ if H contains an odd cycle, otherwise $\chi(H) \leq 2$.] Denote by $\chi_{g_0}(G)$ the number of colours used by this algorithm. By definition, $\chi_{g_0}(G) \geq \chi(G)$ for every graph on V.

Theorem 11.26 *Let $p = \alpha(n)/n$ and suppose $\alpha(n) < k(n) \log k(n) \leq n^{1/2}$. Then a.e. $G_{n,p}$ is such that*

$$\chi_{g_0}(G_{n,p}) \leq k + 3.$$

Proof If $\alpha < 1$ is a constant and $p = \alpha/n$, then by Corollary 5.8 a.e. $G_{n,p}$ is a union of components each of which is a tree or a unicyclic graph. Therefore in this case $\chi_{g_0}(G_{n,p}) \leq 3$.

Suppose next that $\alpha > 1$ is a constant and $k = k(n) \leq 15$. Then by the second part of Theorem 11.23 a.e. $G_{n,p}$ is such that the first colour class found by the greedy algorithm has at least $n_1 = \lceil [\{\log(\alpha + 1) - \varepsilon\}/\alpha] n \rceil$ vertices. In the subgraph spanned by the remaining at most $n_2 = n - n_1$ vertices the probability of an edge is

$$\frac{\alpha}{n} = \frac{\alpha}{n_2} \frac{n_2}{n} \leq \frac{\alpha - \log(\alpha + 1) + \varepsilon}{n_2} = \frac{\alpha'}{n_2}.$$

Hence if a.e. $G_{n,\alpha'/n}$ satisfies

$$\chi_g(G_{n,\alpha'/n}) \leq s$$

then

$$\chi_g(G_{n,\alpha/n}) \leq s + 1$$

for a.e. $G_{n,\alpha/n}$. Therefore if

$$\chi_g(G_{n,\alpha/n}) \leq s$$

for all $\alpha < \alpha_0 - \log(\alpha_0 + 1)$, then

$$\chi(G_{n,\alpha/n}) \leq s + 1$$

for all $\alpha < \alpha_0$. Easy calculations show that this implies

$$\chi_{g_0}(G_{n,\alpha/n}) \leq k + 3$$

whenever $\alpha \leq k \log k, k \leq 15$.

Suppose finally that $k \geq 16$. By Theorem 11.23(ii) we have that if $\varepsilon > 0$ is fixed and $\alpha_k > \alpha_{k-1} > \ldots > \alpha_{15}$ are such that

$$\begin{aligned} \alpha_{15} &\leq 15 \log 15, \\ \alpha_l - \log \alpha_l + \varepsilon &< \alpha_{l-1} \text{ for } 16 \leq l \leq k \end{aligned}$$

and

$$\sum_{l=16}^{k} \alpha_k = o(n),$$

then

$$\chi_{g_0}(G_{\alpha_k/n}) \leq k + 3$$

for a.e. $G_{n,\alpha_k/n}$. If $\alpha_l = l \log l \leq n^{1/2}$ for $15 \leq l \leq k \leq n^{1/2}/\log\log n$ then these conditions are satisfied since

$$\begin{aligned} \inf_{16 \leq l \leq k} [\alpha_{l-1} - \alpha_l + \log \alpha_l] &= \inf_{16 \leq l \leq k} \{(l-1)\log(l-1) - l \log l \\ &\qquad + \log l + \log\log l\} \\ &= 15 \log(15/16) + \log\log 16 > 0. \end{aligned}$$

This completes the proof of our theorem. □

If α is not too small, then the greedy algorithm works rather well, even without a good colouring of the sparse subgraph at the end.

Theorem 11.27 *Suppose $\alpha(n) < n, \alpha(n)/\log n \to \infty$ and $p = \alpha(n)/n$. Set $\varepsilon = (3 \log\log n)/\log \alpha$. Then a.e. $G_{n,p}$ is such that*

$$\chi_g(G_{n,p}) \leq \left\lceil (1+\varepsilon) \frac{\log(1/q)}{\log \alpha} n \right\rceil = k,$$

where $q = 1 - p$.

Proof What is the probability that the simple greedy algorithm uses the $(k+1)$st colour to colour vertex $j+1$? It is at most

$$\max \left\{ \prod_{i=1}^{k} (1 - q^{n_i}) : n_i \geq 0, \sum_{i=1}^{k} n_i = j \right\} \leq (1 - q^{j/k})^k.$$

Hence

$$\begin{aligned} P\{\chi_g(G_{n,p}) > k\} &\leq \sum_{j=0}^{n-1} (1 - q^{j/k})^k \\ &< n(1 - q^{n/k})^k \leq n(1 - \alpha^{-1/(1+\varepsilon)})^k \end{aligned}$$

$$\begin{aligned}&\le n\exp(-\alpha^{-1/(1+\varepsilon)}k)\\&\le \exp\left\{\log n + (1+\varepsilon)\alpha^{-1/(1+\varepsilon)}\frac{\log(1-\alpha/n)}{\log\alpha}n\right\}\\&\le \exp\{\log n - (1+\varepsilon)\alpha^{1-1/(1+\varepsilon)}/\log\alpha\}\\&\le \exp(\log n - \alpha^{3\varepsilon/4}/\log\alpha) \to 0,\end{aligned}$$

proving the theorem. □

Once again, it is easily seen that the upper bound is essentially best possible: for $p = \alpha/n$ a.e. $G_{n,p}$ satisfies $\chi_g(G_{n,p}) \sim \{\log(1/q)/\log\alpha\}n$.

Theorems 11.26 and 11.27 contain most of the early results about colouring spaces random graphs, including several results of Kalnins (1970), Erdős and Spencer (1974, pp. 94–96), McDiarmid (1979*a*), de la Vega (1985) and Bollobás and Thomson (1985).

These results are reminiscent of Theorem 11.12: although they give good bounds on greedy colourings, they do not come close to determining the asymptotic chromatic number of almost every $G_{n,\alpha/n}$. After the appearance of Theorem 11.18, martingale methods were brought in to tackle colouring problems, and all this changed rapidly.

Frieze (1990) proved the following sharp result about the independence number.

Theorem 11.28 *For every $\varepsilon > 0$ there is an $\alpha_\varepsilon > 0$ such that if $\alpha_\varepsilon \le \alpha = \alpha(n) = o(n)$ then a.e. $G_{n,\alpha/n}$ is such that*

$$\left|\beta_0(G_{n,\alpha/n}) - \frac{2(\log\alpha - \log\log\alpha - \log 2 + 1)}{\alpha}n\right| \le \frac{\varepsilon n}{\alpha}. \qquad \square$$

Just as in the proof of Theorem 11.17 we estimated a restricted version of the number of complete subgraphs, Frieze applied the Hoeffding–Azuma inequality (Theorem 1.19) to the restricted version $\beta_0'(G_{n,\alpha/n})$ of the independence number. To define β_0', set $m = \lfloor\alpha/(\log\alpha)^2\rfloor$, $l = \lfloor n/m\rfloor$, and let $V_1, \ldots, V_l$ be disjoint subsets of $[n] = V(G_{n,\alpha/n})$ with $|V_1| = \ldots = |V_l| = m$. For a graph G with vertex set $[n]$, we define $\beta_0'(G)$ to be the maximal rise of an independent set of vertices meeting each V_i in at most one vertex.

As a by-product of the proof of Theorem 11.18, Bollobás (1988*c*) gave good bounds for $\chi(G_{n,p})$ in the case when $p > n^{-1/3}$. Luczak (1991*b*) went considerably further: combining the martingale method of Bollobás (1988*c*), and the expose-and-merge algorithm of Matula (1987), he gave precise bounds for $\chi(G_{n,p})$ in the entire range $p = o(1)$, provided pn is sufficiently large.

Theorem 11.29 *There is a constant α_0 such that if $\alpha_0 \le \alpha = \alpha(n) = o(n)$ then a.e. $G_{n,\alpha/n}$ is such that*

$$\frac{\alpha}{2\log\alpha}\left(1+\frac{\log\log\alpha-1}{\log\alpha}\right) < \chi(G_{n,\alpha/n}) < \frac{\alpha}{2\log\alpha}\left(1+\frac{30\log\log\alpha}{\log\alpha}\right).$$

□

We know from Theorem 11.16 of Shamir and Spencer (1987) that if $p = p(n) < n^{-112-\varepsilon}$ for some fixed $\varepsilon > 0$ then the chromatic number of a.e. $G_{n,p}$ takes one of $s(\varepsilon)$ consecutive values; in particular, if $p < n^{-5/6-\varepsilon}$ then for a.e. $G_{n,p}$ the chromatic number $\chi(G_{n,p})$ takes one of five values. Łuczak (1991*b*) refined the argument to show that in the latter case we have concentration on *two* values. By bringing many new ideas to bear on the problem, Alon and Krivelevich (1997) proved that this best possible concentration holds in a much wider range of the probability p.

Theorem 11.30 *For all positive ε, σ, there is an integer $n_0 = n_0(\varepsilon, \sigma)$ such that if $0 < p = p(n) \le n^{-1/2-\sigma}$ then there is an integer $k = k(n,p)$ such that*

$$P(k \le \chi(G_{n,p}) \le k+1) > 1-\varepsilon.$$

□

Furthermore, Alon and Krivelevich (1997) used the method of proof of Theorem 11.30 to show that for a wide range of pairs (n,p) almost all $G_{n,p}$ have the same chromatic number.

Theorem 11.31 *Given a constant $0 < \gamma < 1/2$ and an integer-valued function $k(n)$ satisfying $1 \le k(n) \le n^{\gamma}$, there is a function $p = p(n)$, $0 < p(n) < 1$, such that*

$$\lim_{n\to\infty} P(\chi(G_{n,p}) = k(n)) = 1.$$

For α constant, rather than study the random variable $\chi(G_{n,\alpha/n})$, it is convenient to study the sequences $(d'_k)_2^{\infty}$, $(d''_k)_2^{\infty}$ defined as follows:

$$d'_k = \sup\{\alpha : P(\chi(G_{n,\alpha/n}) \le k) \to 1\}$$

and

$$d''_k = \inf\{\alpha : P(\chi(G_{n,\alpha/n}) \le k) \to 0\}.$$

By definition, $d'_k \le d''_k$. Since a graph is 2-colourable iff it contains no odd cycles, it is easy to show that $d'_2 = 0$ and $d''_2 = 1$.

For $k \ge 3$ the situation is very different: it is very likely that $d'_k = d''_k =$

d_k for every $k \geq 3$, i.e., there is a constant $d_k > 0$ such that for every ε, $0 < \varepsilon < d_k$, we have

$$P(\chi(G_{n,(d_k-\varepsilon)/n}) \leq k) \to 1$$

and

$$P(\chi(G_{n,(d_k+\varepsilon)/n}) \leq k) \to 0.$$

Building on the deep results of Friedgut (1999) on necessary and sufficient conditions for sharp threshold functions, Achlioptas and Friedgut (1999) proved that there is a sharp transition from being k-colourable to having no k-colourings. To state this result, for $n > k \geq 3$ and $0 < \varepsilon < 1$, define $d_k(n, \varepsilon)$ by

$$P(\chi(G_{n,d_k(n,\varepsilon)/n}) = k) = \varepsilon.$$

Then, for fixed k and ε, $d_k(n, \varepsilon) - d_k(n, -\varepsilon) \to 0$ as $n \to \infty$. This result of Achlioptas and Friedgut corresponds to Theorem 11.16, guaranteeing concentration in some interval, but what is missing is the analogue of Theorem 11.18, telling us that the short threshold interval does not move around much as $n \to \infty$. It is likely that a major new idea is needed to prove that $d'_k = d''_k$.

The sequences (d'_k) and (d''_k) are related to the sequence (c_k) associated with the appearance of a k-core discussed in Section 6.4. Recall that the *k-core* of a graph is the maximal subgraph of minimal degree at least k, and we may define c_k as follows:

$$c_k = \sup\{\alpha : P(G_{n,\alpha/n} \text{ has a } k\text{-core}) \to 0\}.$$

In fact, (c_k) does have the property we demand of the conjectured sequence (d_k): for every $\varepsilon > 0$,

$$P(G_{n,(c_k+\varepsilon)/n} \text{ has a } k\text{-core}) \to 1.$$

Since a graph without a k-core is k-colourable, $c_k \leq d'_k$ for every k, and a priori it does not seem impossible that $c_k = d'_k$ for $k \geq 3$. In fact, this is not the case, as proved by Molloy (1996) (and, independently, by Łuczak) for $k \geq 4$ and by Achlioptas and Molloy (1997) for $k = 3$.

To prove that $d'_k > c_k$ for $k \geq 4$, Molloy (1996) made use of the following inequality due to Bollobás and Thomason (1985), valid for $k \geq 2$:

$$d'_{k+1} \geq d'_k + \log d'_{k+1}. \tag{11.16}$$

Also, as stated in Theorem 6.20, Pittel, Spencer and Wormald (1996) gave an exact expression for c_k in terms of Poisson branching processes, and deduced that $c_k = k + \sqrt{k \log k} + O(\log k)$. In particular, $c_3 = 3.35 \ldots \le d_3$. Hence, by (11.16), we have $d_4 \ge 5.16 > c_4 = 5.14 \ldots$, and repeated application of (11.16) gives that $d'_k > c_k$ for $4 \le k \le 40$. As noted by Molloy (1996), Theorem 6.20 of Pittel, Spencer and Wormald implies that $c_k \le 2.3k$. On the other hand, (11.16) implies that $d'_k > k \log k > 3k$ for $k \ge 40$, and so $d'_k > c_k$ for $k \ge 4$, as claimed.

Let us say a few words about d'_k and d''_k for small values of k. The first lower bounds on d'_3, namely $d'_3 \ge 2.88$, due to Chvátal (1991), and $d'_3 \ge 3.34$, due to Molloy and Reed (1995), were really lower bounds on c_3. Achlioptas and Molloy (1997) were the first to go considerably beyond the bound given by the 3-core: they proved that $d'_3 \ge 3.846$. Achlioptas and Molloy (1999) made use of a technique of Kirousis, Kranakis, Krizanc and Stamation (1998) to give upper bounds for d''_k. Among other results, they showed that $d''_3 \le 5.044$, $d''_4 \le 9.174$, $d''_5 \le 13.896$, $d''_6 \le 19.078$ and $d''_7 \le 24.632$.

Although in a random graph process a k-core appears well before a $(k+1)$-chromatic subgraph, as shown by Molloy and Reed (1999), shortly after the emergence of a k-core a.e. random graph contains a subgraph of the type Gallai showed to appear in $(k+1)$-critical graphs. Thus to get closer to proving the existence of d_k and determining its value, we shall have to go beyond Gallai's condition.

To conclude this section, we shall consider the independence chromatic number of random r-regular graphs. We start with a brief review of some results on the independence number of (non-random) graphs. The *independence ratio* $i(G)$ of a graph G of order n is $\beta_0(G)/n$. Let $i(\Delta, g)$ be the infimum of the independence ratio of graphs with maximum degree Δ and girth at least g. For $g = 3$ we have no restriction on the girth so put $i(\Delta) = i(\Delta, 3)$. Clearly $i(\Delta) = i(\Delta, 3) \le i(\Delta, 4) \le \ldots$; furthermore set $i^*(\Delta) = \lim_{g \to \infty} i(\Delta, g)$.

Turán's classical theorem [see Bollobás (1978*a*, Chapter 6) for numerous extensions] implies that $i(G) \ge 1/(d+1)$, where $d = d(G)$ is the average degree of G. The inequality was improved by Wei (1980, 1981) to the following: if G has degree sequence $d_1, \ldots, d_n$, then

$$\beta_0(G) \ge \sum_{i=1}^{n} \frac{1}{d_i + 1}. \tag{11.17}$$

As remarked by Griggs (1983*a*), inequality (11.17) is a consequence of the following extension of Turán's theorem, due to Erdős (1970) (see also Bollobás, 1978*a*, Theorem 6.1.4: the degree sequence of a graph without a K^{s+1} is dominated by the degree sequence of an s-partite graph. Griggs (1983*a*) strengthened (11.17):

$$\beta_0(G) \geq \frac{n}{\Delta(\Delta+1)} + \sum_{i=1}^{n} \frac{1}{d_i+1}$$

provided G is connected and $\Delta = \Delta(G) \geq 3$.

If G is connected and $G \neq K^{\Delta+1}$, then Brooks' (1941) theorem [see also Berge (1973, Theorem 11.15.1.6) or Bollobás (1978*a*, Theorem 5.1.6)] implies that

$$i(G) \geq 1/\Delta(G). \tag{11.18}$$

Albertson, Bollobás and Tucker (1976) proved that if $\mathrm{cl}(G) \leq \Delta - 1$ and G is not one of two exceptional graphs then we have strict inequality in (11.18).

Fajtlowicz (1977, 1978) and Staton (1979) proved bounds on the independence ratio of triangle-free graphs. Staton (1979) showed that

$$i(\delta, 4) \geq 5/(5\Delta - 1), \tag{11.19}$$

which, as shown by an example of Fajtlowicz (1977), is best possible for $\Delta = 3$. Thus $i(3,4) = 5/14$. For $\Delta \geq 4$, Fajtlowicz (1978) improved (11.19) to

$$i(\Delta, 4) \geq 2/(2\Delta + 3). \tag{11.20}$$

Concerning larger values of g, Hopkins and Staton (1982) proved that

$$i(\Delta, 6) \geq \frac{(2\Delta - 1)^2}{\Delta^2 + 2\Delta - 1} \tag{11.21}$$

and

$$i^*(3) = \lim_{g \to \infty} i(3, g) \geq 7/18. \tag{11.22}$$

It turns out that inequalities (11.18)–(11.21) are useful only for small values of Δ since Ajtai, Komlós and Szemerédi (1980, 1981*b*) achieved a breakthrough for large values of Δ:

$$i(\Delta, 4) > c \log \Delta / \Delta \tag{11.23}$$

for some constant $c > 0$. This result was sharpened by Griggs (1983*b*) and Shearer (1982), the latter improving (11.23) to

$$i(\Delta, 4) \geq (\Delta \log \Delta - \Delta + 1)/(\Delta - 1)^2, \tag{11.24}$$

which is a consequence of Theorem 11.18, to be proved in the next chapter (Theorem 12.14).

Let us turn, at last, to the independence ratio of random regular graphs. We know from Corollary 2.19 that for every $r \geq 3$, a.e. $G_{r-\text{reg}}$ is essentially triangle-free: it has, say, fewer than $\omega(n)$ triangles, provided $\omega(n) \to \infty$. Hence deleting an edge from each triangle will hardly increase the independence number, so $\beta_0(G_{r\text{-reg}}) \geq \{n - \omega(n)\}i(r, 4)$. Even more, in this inequality $i(r, 4)$ can be replaced by $i(r, g)$ for any fixed g since, again by Corollary 2.18, a.e. $G_{r\text{-reg}}$ contains at most $\omega(n)$ cycles of length less than g. Hence inequalities (11.22) and (11.24) imply lower bounds for the independence ratio of a.e. $G_{r\text{-reg}}$.

By making use of these ideas and properties of the model $\mathcal{G}(n, r\text{—reg})$ described in Chapter 2, Bollobás (1981c) proved that

$$\frac{r \log r - r + 1}{(r-1)^2} \leq i(G_{\text{r}-\text{reg}}) < \frac{2 \log r}{r} \tag{11.25}$$

if $r \geq 4$ and

$$\frac{7 + o(1)}{18} \leq i(G_{3-\text{reg}}) < \frac{6}{13}. \tag{11.26}$$

For r large enough, inequality (11.25) was improved to an essentially best possible result by Frieze and Łuczak (1992); the proof is based on a detailed and ingenious analysis of an algorithm that constructs an independent set.

Theorem 11.32 *For $\varepsilon > 0$ and $0 < \theta < 1/3$, there is an r_0 such that if $r_0 \leq r = r(n) \leq n^\theta$ then the independence ratio $i(G_{r-reg})$ of a.e. r-regular graph satisfies*

$$|i(G_{r-\text{reg}}) - \frac{2}{r}(\log r - \log\log r + 1 - \log 2)| \leq \varepsilon|r. \qquad \square$$

Frieze and Łuczak (1992) also determined the chromatic number of a.e. r-regular graph; not responsibility, $\chi(G_{r-\text{reg}})$ is about $1/i(G_{r-reg})$ for a.e. $G_{r-\text{reg}}$ if r is in an appropriate range.

Theorem 11.33 *If $r = r(n)$ is sufficiently large and not more than n^θ for some fixed $\theta < 1/3$ than the chromatic number $\chi(G_{r-\text{reg}})$ of a.e. r-regular graph satisfies*

$$\left|\chi(G_{r-reg}) - \frac{r}{2 \log r} - \frac{8r \log\log r}{(\log r)^2}\right| \leq \frac{8r \log\log r}{(\log r)^2}. \qquad \square$$

For fixed $r \geq 3$ and $g \geq 4$, the probability that a random r-regular graph has girth at least g is bounded away from 0. Hence, Theorem 11.33 implies that if $r \geq 3$, $g \geq 4$, n is large enough and r_n is even then there is an

r-regular graph of order n, girth at least g, and chromatic number about $r/2 \log r$. Kim (1995*a*) and Anders Johansson proved the major result that this order is guaranteed by *much* weaker conditions; if G is a graph of maximal degree Δ and girth at least 5 then $\chi(G) \leq (1+\varepsilon_\Delta)\Delta/\log\Delta$, where $\varepsilon_\Delta \to 0$ as $\Delta \to \infty$. Although this deep result is *not* about random graphs, the proof is entirely probabilistic: it is based on a superb application of the so-called 'semi-random method' or 'Rödl's nibble method'.

In spite of the beautiful results above concerning the independence ratio and chromatic number of regular graphs, for small values of r we are rather for from knowing the independence ratio of a.e. r-regular graph. The case $r = 3$ was studied by Frieze and Suen (1994): in a substantial paper they improved the upper bound on 0.4615 $i(G_{r-\text{reg}})$ in (11.26) to 0.432..., so that we have $0.388 < i(G_{r-\text{reg}}) < 0.433$ for a.e. cubic graph. Closing this gap seems to be a difficult problem.

Exercises

11.1 Show that for every $\varepsilon > 0$ there are $0 < q(n) < \left(\frac{4}{3}+\varepsilon\right)(\log n)n^{-1/2}$, $p(n) = 1 - q(n)$ and $r(n) \in \mathbb{N}$ such that p and r satisfy the conditions of Theorem 11.1 and so a.e. G_p has clique number r.

11.2 Prove that if H is any graph of order n, then

$$k_r(H)\Big/\binom{n}{r}$$
$$\leq P\{G \in \mathscr{G}(H,p) : \mathrm{cl}(G) \geq r\}/P\{G \in \mathscr{G}(n,p) : \mathrm{cl}(G) \geq r\} \leq 1.$$

11.3 Use (11.6) and an estimate of the variance to deduce Theorem 11.4.

11.4 Prove Theorem 11.5(ii) by showing that $\lim_{N\to\infty} P_{n,N} = 0$, where $P_{n,N}$ is the probability that $G \in \mathscr{G}(\mathrm{N},p)$ contains a complete graph with vertex set $\{x_1, x_2, \ldots, x_N\}$ such that $x_k \leq b^{k(1-\varepsilon)}$ for all k, $n \leq k \leq N$.

11.5 Prove Theorem 11.13. (Grimmett and McDiarmid, 1975.) [Suppose $c > \frac{1}{2}$, $k = \lfloor cn/\log_d n \rfloor$ and $n = km$. Denote by E_u the expected number of k-colourings of G_p with each class containing precisely m vertices (*uniform* k-colourings). Then

$$E_u = \frac{n!}{(m!)^k} q^{\binom{m}{2}k} = \frac{n!}{(m!)^k} q^{n(m-1)/2},$$

so

$$(1/E_u)^{1/n} \sim \frac{m}{n} d^{(m-1)/2} = O\left(\frac{1}{k} n^{1/(2c)}\right) = o(1).]$$

11.6 Show that for every $k \in \mathbb{N}$ there is a tree T with vertex set $W = \{1, 2, \ldots, 2^{k-1}\}$ such that $\chi_g(T) \geq k$, where χ_g is taken with respect to the natural order on W.

11.7 Deduce from (11.20) and Theorem 11.27 that

$$0.2828 \leq i(4,4) \leq i^*(4) \leq 0.4212,$$
$$0.2529 \leq i(5,4) \leq i^*(5) \leq 0.3887.$$

11.8 Denote by $T(n, l, k)$ the minimal number of edges in a k-graph (i.e. k-uniform hypergraph) of order n such that every l-set of vertices contains an edge. By counting the number of edges spanned by sets of s vertices each, prove that

$$T(n, l, k) \geq T(s, l, k) \binom{n}{j} \binom{n-k}{s-k}^{-1}$$

for all $2 \leq k \leq l \leq s \leq n$.

[This was proved by Katona, Nemetz and Simonovits (1964). Recently de Caen (1983) improved this bound by giving a lower bound for the variance of the number of edges spanned by s vertices.]

11.9 A *topological H-graph*, TH, is a graph obtained from H by subdividing some edges of H by new vertices; the *topological clique number* of a graph G is defined as $\mathrm{tcl}(G) = \max\{s : \mathrm{TK}^s \subset G\}$. Prove that for $0 < p < 1$ fixed, there are constants $0 < c_1 < c_2$ such that

$$c_1 n^{1/2} < \mathrm{tcl}(G_p) < c_2 n^{1/2} \qquad \text{(E11.1)}$$

for a.e. G_p.

[Extending results of Erdős and Fajtlowicz (1977), Bollobás and Catlin (1981) proved that $\mathrm{tcl}(G_p) = \{1 + o(1)\}\{2n/(1-p)\}^{1/2}$ for a.e. G_p. Subsequently, Ajtai, Komlós and Szemerédi (1979) (those curious Hungarian dates!) extended (11.21) by showing that if $p = cn^{-1/2}$ for some $c > 0$, then a.e. G_p satisfies $\mathrm{tcl}(G_p) > c_3 n^{1/2}$ for some $c_3 > 0$; furthermore, they used the existence of long paths (§1 of Chapter 8) to prove that if $c > 1$, then a.e. $G_{c/n}$ satisfies $\mathrm{tcl}(G_{c/n}) = \{1 + o(1)\} \log n / \log\log n$. In particular, for every $s \geq 4$ the threshold function of TK^s is $M_o(n) = n/2$: if $\varepsilon > 0$ and $M \geq (1+\varepsilon)n/2$, then a.e. G_M contains a TK^s and if $M \leq (1+\varepsilon)n/2$, then $\mathrm{TK}^s \notin G_M$ almost surely.

The main aim of Erdős and Fajtlowicz was to disprove the conjecture of Hajós that $\chi(G) = k$ implies $G \supset TK^k$; since $\chi(G_{1/2}) > (\frac{1}{2} - \varepsilon)n/\log_2 n$, the upper bound in (11.21) shows that for a.e. $G_{1/2}$ the topological clique number is much smaller than the chromatic number.]

11.10 The *contraction clique number* $\mathrm{ccl}(G)$ of a graph G is the maximal integer s for which G has a *subcontraction* to K^s (or K_s is a *minor* of G, in notation $G > K^s$): G has vertex disjoint connected subgraphs $G_1, G_2, \ldots, G_s$ such that for all $1 \le i < j \le s$ the graph G contains a $G_i - G_j$ edge. Prove that $\mathrm{ccl}(G_{1/2}) = \{1 + o(1)\}n/(\log_2 n)^{1/2}$ for a.e. $G_{1/2}$.

[This was proved, in a sharper form, by Bollobás, Catlin and Erdős (1980). One of the most famous conjectures in graph theory, Hadwiger's conjecture (1943), states that if $\chi(G) = s$, then $G > K^s$. The result in the exercise shows that Hadwiger's conjecture is true for a.e. graph. In fact, for every fixed p, $0 < p < 1$, we have $\mathrm{ccl}(G_p) = \{1 + o(1)\}n/(\log_d n)^{1/2}$, where $d = 1/q$.

It is rather surprising that the assertion that a.e. G_p has 'large' contraction clique number can be strengthened considerably: *every* graph of order n and size about $pn^2/2$ has contraction clique number of the order $n/(\log_d n)^{1/2}$. This was proved by Kostochka (1982) and Thomason (1984), extending earlier results of Mader (1967). To be precise, Thomason proved that if s is sufficiently large, $|G| = n$ and $e(G) \ge 2.68s(\log_2 s)^{1/2}n$, then $G > K^s$.]

11.11 Let $0 < p < 1$ and $\varepsilon > 0$ be fixed and set $d = 1/q$. Prove the following assertions.

(i) a.e. G_p is such that for every set S of $s < (1 - \varepsilon)\log_d n$ vertices there is a vertex $x \notin S$ joined to precisely one vertex in S, and so, in particular, every induced tree of order s is contained in an induced tree of order $s + 1$.

(ii) Almost no G_p contains an induced tree of order $\lfloor (2 + \varepsilon)\log_d n \rfloor$.

(iii) a.e. G_p contains a maximal induced tree of order r for every r satisfying $(1 + \varepsilon)\log_d n < r < (2 - \varepsilon)\log_d n$. (Erdős and Palka, 1983.)

12

Ramsey Theory

Many beautiful and elegant results assert that if we partition a sufficiently large structure into k parts, then at least one of the parts contains a substructure of a given size. For example, Schur (1916) proved that if the natural numbers are partitioned into finitely many classes, then $x+y=z$ is solvable in one class, and van der Waerden (1927) proved that one class of such a partition contains arbitrarily long arithmetic progressions. The quintessential partition theorem is the classical theorem of Ramsey (1930) which concerns very simple structures indeed: if for some $r \in \mathbb{N}$ the set $\mathbb{N}^{(r)}$ of all r-subsets of $\mathbb{N}$ is divided into finitely many classes then $\mathbb{N}$ has an infinite subset all of whose r-subsets belong to the same class. All these statements have analogues for finite sets; these analogues tend to be more informative and are of great interest in finite combinatorics. The theory dealing with theorems in this vein has become known as *Ramsey theory.*

By now there is an immense literature on Ramsey theory; the popularity of the field owes a great deal to Paul Erdős, who proved many of the major results and who was the first to recognize the importance of partition theorems.

In this brief chapter we restrict our attention to Ramsey theorems concerning graphs whose proofs are based on the use of random graphs, so our treatment of the subject is far from encyclopaedic. One reason why an entire chapter is devoted to the random graph aspects of Ramsey theory is that the early development of the theory of random graphs was greatly influenced by some results of Erdős (1947, 1961) on Ramsey theory. For a comprehensive treatment of the many facets of Ramsey theory the reader is referred to the excellent book by Graham, Rothschild and Spencer (1980).

Ramsey theorems are usually formulated in terms of colourings: any

k-colouring of a sufficiently large system contains a monochromatic subsystem of a given size; furthermore, for $k = 2$ one almost invariably considers red–blue colourings. However, as our main aim in this chapter is to study 2-colourings of complete graphs and a red–blue colouring of K^n is naturally identified with the subgraph G formed by the red edges, say, so that the blue subgraph is the complement of G in K^n, more often than not we shall study graphs and their complements rather than red–blue colourings of complete graphs.

12.1 Bounds on $R(s)$

Given natural numbers s and t, the *Ramsey number* $R(s,t)$ is the minimal $n \geq 1$ for which every red–blue colouring of the edges of K^n yields a red K^s or a blue K^t. Equivalently, $R(s,t)$ is the smallest n for which every graph of order n has clique number at least s or independence number at least t. One usually writes $R(s) = R(s,s)$. The numbers $R(1), R(2), \ldots$ are the *diagonal Ramsey numbers*; $R(s,t)$ is an *off-diagonal Ramsey number* if $s \neq t$. *A priori* it is not clear that the function $R(s,t)$ is well defined but, trivially, $R(s,1) = R(1,s) = 1$ and $R(s,2) = R(2,s) = s$ for all $s \geq 2$. However, the following classical result (Skolem, 1933; Erdős and Szekeres, 1935; Erdős, 1957; see also Bollobás, 1979*a*, p. 104; Graham, Rothschild and Spencer, 1980, p. 77) not only proves that $R(s,t)$ is well defined but it also gives an upper bound on the function which is considerably better than the original bound proved by Ramsey (1930). Although the proof has nothing to do with random graphs, we reproduce it here since it is both elegant and simple.

Theorem 12.1 *If $s > 2$ and $t > 2$, then*

$$R(s,t) \leq R(s-1,t) + R(s,t-1) \tag{12.1}$$

and

$$R(s,t) \leq \binom{s+t-2}{s-1}. \tag{12.2}$$

Proof (i) In the proof of (12.1) we may assume that $R(s-1,t)$ and $R(s,t-1)$ are finite. Let G be a graph of order $R(s-1,t) + R(s,t-1)$ and let H be its complement. Pick a vertex x. Since

$$d_G(x) + d_H(x) = R(s-1,t) + R(s,t-1) - 1,$$

by symmetry we may assume that $d_G(x) \geq R(s-1,t)$. Let $W = \Gamma_G(x)$, $G_1 = G[W]$ and $H_1 = H[W]$. As $|W| \geq R(s-1,t)$, either G_1 contains a complete graph K_1 of order $s-1$ or else H_1 contains a K^t. In the first case K_1 and x form a K^s in G and in the second case H contains a K^t. Thus (12.1) holds.

(ii) If $s = 2$ and $t \geq 2$, then $R(s,t) = t$, so equality holds in (12.2); similarly we have equality in (12.2) for $s \geq 2$ and $t = 2$. Assume now that $s \geq 3$, $t \geq 3$ and (12.2) holds for all (s', t') with $2 \leq s' \leq s$, $2 \leq t' \leq t$ and $s' + t' < s + t$. Then by (12.1) we have

$$\begin{aligned} R(s,t) &\leq R(s-1,t) + R(s,t-1) \\ &\leq \binom{s+t-3}{s-2} + \binom{s+t-3}{s-1} = \binom{s+t-2}{s-1}. \qquad \square \end{aligned}$$

Much effort has been spent on determining exact values of the function $R(s,t)$ for $3 \leq s \leq t$, with distressingly little success: $R(3,3) = 6$, $R(3,4) = 9$, $R(3,5) = 14$, $R(4,4) = 18$, $R(3,6) = 18$ and $R(3,7) = 23$. The first four values were determined by Greenwood and Gleason (1995), the last two are due to Kalbfleisch (1967) and Graver and Yackel (1968): for a survey of Ramsey numbers see Chung and Grinstead (1983).

It would be even more interesting to determine the correct order of $R(s)$. By Theorem 12.1,

$$R(s) \leq \binom{2s-2}{s-1} < \frac{1}{6} 4^s s^{-1/2}$$

for $s \geq 4$. This upper bound was improved by Yackel (1972).

Theorem 12.2 *There is a constant c such that for all $s \geq 3$*

$$R(s) < \frac{c \log\log s}{\log s} \binom{2s-2}{s-1} < \frac{c \log\log s}{\log s} 4^s s^{-1/2}$$

Erdős (1947) was the first to give an exponential lower bound for $R(s)$. Although, by now, the result looks very simple indeed, the proof was the first exciting application of random graphs. We know from Corollary 11.2 that a.e. $G_{n,1/2}$ has clique number about $2\log_2 n$. Hence for s slightly larger than $2\log_2 n$ a.e. $G_{n,1/2}$ is such that neither $G_{n,1/2}$ nor its complement contains a K^s. In other words, a.e. $G_{n,1/2}$ shows that $R(s) \geq n+1$, giving a lower bound only slightly greater than $2^{s/2}$. In fact, there is no need to require $\mathrm{cl}(G_{n,1/2}) \leq s-1$ for a.e. $G_{n,1/2}$: clearly $P\{\mathrm{cl}(G_{n,1/2}) \leq s-1\} > \frac{1}{2}$ will suffice.

Theorem 12.3 *Suppose* $s \geq 2$ *and*

$$\binom{n}{s} < 2^{\binom{s}{2}-1}.$$

Then $R(s) \geq n+1$.

Proof Consider the space $\mathcal{G}(n, \frac{1}{2})$. Denote by $Y_s = Y_s(G_{1/2})$ the number of K^s subgraphs of $G_{1/2}$ and by $\bar{Y}_s$ the number of K^s subgraphs in the complement. Then by (12.1) of Chapter 11 we have

$$P(Y_s + \bar{Y}_s \geq 1) \leq E(Y_s + \bar{Y}_s) = 2\binom{n}{s} 2^{-\binom{s}{2}} < 1.$$

Hence some element G of $\mathcal{G}(n, \frac{1}{2})$ is such that neither G nor $\bar{G}$ contains a complete graph of order s, showing $R(s) \geq n+1$. □

Corollary 12.4 $R(s) \geq (s/\mathrm{e})2^{(s-1)/2}$.

Proof If $n < (s/\mathrm{e})2^{(s-1)/2}$, then

$$2\binom{n}{s} 2^{\binom{s}{2}} < \frac{1}{s^{1/2}} \left(\frac{\mathrm{e}n}{s}\right)^s 2^{\binom{s}{2}} < \frac{1}{s^{1/2}} < 1.$$ □

The essential part of the proof of Theorem 12.3 is practically forced on us. Indeed, trivially,

$$R(s) = \max\{n : P\{Y_s(G_{n,1/2}) + \bar{Y}_s(G_{n,1/2}) = 0\} = 0\}$$

so our task is to find a small n for which $P\{Y_s(G_{n,1/2}) + \bar{Y}_s(G_{n,1/2}) \geq 1\}$ is not 1. Now in the proof of Theorem 12.3 we used the inequalities

$$P(Y_s + \bar{Y}_s \geq 1) \leq P(Y_s \geq 1) + P(\bar{Y}_s \geq 1) \tag{12.3}$$

and

$$P(Y_s \geq 1) + P(\bar{Y}_s \geq 1) \leq E(Y_s) + E(\bar{Y}_s) = 2E(Y_s). \tag{12.4}$$

Both inequalities are crude, but which is cruder in the context above? We know from Theorem 11.7 that if $E(Y_s)$ tends to a constant μ, then $P(Y_s \geq 1)$ is not only bounded by $\mu + o(1)$, as asserted by (12.4), but it tends to $1 - \mathrm{e}^{-\mu}$. All this means that it suffices to make sure that $E(Y_s)$ is slightly smaller than $\log 2$, rather than $\frac{1}{2}$. Unfortunately, this only allows us to increase the bound $n+1$ in Theorem 12.3 to about $n + cn/\log n$, a gain hardly worth bothering about.

What can we gain by improving inequality (12.3)? As discovered by Spencer (1975), we can gain a factor 2 by applying the Lovász Local Lemma (Theorem 1.18) on a family of almost independent events.

Theorem 12.5 *Suppose $s \geq 2$ and*

$$\sum_{k=2}^{s-1} \binom{s}{k} \binom{n-s}{s-k} \leq \frac{1}{\mathrm{e}} 2^{\binom{s}{2}-1}.$$

Then $R(s) \geq n+1$.

Proof Consider the probability space $\mathscr{G}(n, \frac{1}{2})$. For $\sigma \in V^{(s)}$, i.e. for an s-subset σ of the vertex set V, let A_σ be the event that the graph spanned by σ is either complete or empty. Furthermore, let F be a graph on $V^{(s)}$ in which two vertices $\sigma_1, \sigma_2 \in V^{(s)}$ are joined by an edge iff $|\sigma_1 \cap \sigma_2| \geq 2$. Then F is a dependence graph of the system of events $\{A_\sigma : \sigma \in V^{(s)}\}$,

$$\Delta = \Delta(F) = \sum_{k=2}^{s-1} \binom{s}{k} \binom{n-s}{s-k}$$

and

$$P(A_\sigma) = 2^{-\binom{s}{2}+1} < \frac{1}{\mathrm{e}\Delta} < (\Delta - 1)^{\Delta-1}/\Delta^{\Delta}.$$

Consequently, by Theorem 1.18 we have

$$P\left(\bigcap_{\sigma \in V^{(s)}} \overline{A}_\sigma\right) > 0.$$

Now a graph on V belongs to $\bigcap_{\sigma \in V^{(s)}} \overline{A}_\sigma$ iff $\mathrm{cl}(G) \leq s-1$ and $\mathrm{cl}(\overline{G}) = \beta_0(G) \leq s-1$, so every graph in $\bigcap_{\sigma \in V^{(s)}} \overline{A}_\sigma$ shows that $R(s) \geq n+1$. □

The condition in Theorem 12.5 implies that $s = O(\log n)$ and $\Delta(F) \sim \binom{s}{2}\binom{n-s}{s-2} \sim \binom{n}{s} s^2(s-1)^2/2n^2$. Hence, analogously to Corollary 12.4 we have the following immediate consequence of Theorem 12.5.

Corollary 12.6 $R(s) \geq \{(1/\mathrm{e}) + o(1)\}s\, 2^{(s+1)/2}$.

It is a little sad that the use of the ingenious Lovász Local Lemma has gained us only a factor 2 over the bound resulting from the most straight-forward method.

12.2 Off-Diagonal Ramsey Numbers

Let $3 \le s \le t < n$, $0 < p < 1$, and consider the space $\mathscr{G}(n,p)$. As before, write $Y_s = Y_s(G_p)$ for the number of K^s-subgraphs in G_p and $\bar{Y}_t = \bar{Y}_t(G_p)$ for the number of K^t-subgraphs in the complement of G_p. Then $R(s,t) \ge n+1$ iff $Y_s(G_p) = \bar{Y}_t(G_p) = 0$ for some $G_p \in \mathscr{G}(n,p)$, i.e.

$$R(s,t) \ge n+1 \quad \text{iff} \quad P\{(Y_s + \bar{Y}_t)(G_{n,p}) = 0\} > 0. \tag{12.5}$$

Clearly the truth of the assertion on the right is independent of our choice of p; however, our proof of $P(Y_s + \bar{Y}_t = 0) > 0$ tends to hinge on a suitable choice of p.

As in the proof of Theorem 6, the event $Y_s + \bar{Y}_t = 0$ can be written as the intersection of many events, each of which, one hopes, has a large probability. Let $V = V(G_p) = \{1,2,\dots,n\}$ be, as usual, the vertex set of the graphs in $\mathscr{G}(n,p)$, set $U = V^{(s)}$, $W = V^{(t)}$; for $\sigma \in U$ let A_σ be the event that σ, a set of s vertices, spans a complete subgraph of G_p, and for $\tau \in W$ let B_τ be the event that τ, a set of t vertices, is an independent set in G_p. Then the event $Y_s + Y_t = 0$ is precisely $\bigcap_{\sigma\in U} \bar{A}_\sigma \cap \bigcap_{\tau\in W} \bar{B}_\tau$ so

$$R(s,t) > 0 \quad \text{iff} \quad P\left\{\bigcap_{\sigma\in U} \bar{A}_\sigma \cap \bigcap_{\tau\in W} \bar{B}_\tau\right\} > 0. \tag{12.6}$$

Before turning to lower bounds, we remark that Graver and Yackel (1968) and Yackel (1972) improved Theorem 12.1 for off-diagonal (and rather lop-sided) Ramsey numbers. For every $s \ge 3$ there is a constant c_s such that

$$R(s,t) \le c_s \frac{\log\log t}{\log t}\binom{s+t-2}{s-1} < c_s \frac{\log\log t}{\log t} t^{s-1} \tag{12.7}$$

for all $t \ge s$. In §3 we shall return to upper bounds and we shall improve on (12.7).

As shown by Spencer (1975), the straightforward method used by Erdős (1947) in Theorem 12.3 gives a reasonably good lower bound for every $R(s,t)$: all we have to do is apply (12.5) for suitable values of n and p.

Theorem 12.7 *Suppose* $3 \le s \le t$, $0 < p < 1$ *and*

$$\binom{n}{s} p^{\binom{s}{2}} + \binom{n}{t}(1-p)^{\binom{t}{2}} < 1. \tag{12.8}$$

Then

$$R(s,t) \ge n+1.$$

Proof Consider $\mathscr{G}(n,p)$. The left-hand side of (12.8) is $E(Y_s + \bar{Y}_t)$, so

$$P(Y_s + \bar{Y}_t = 0) \geq 1 - E(Y_s + \bar{Y}_t) > 0.$$

Hence the result follows from (12.5). □

Corollary 12.8 *Let $3 \leq s \leq t$ and*

$$\left(\frac{s}{en}\right)^{2/(s-1)} + \left(\frac{t}{en}\right)^{2/(t-1)} > 1. \qquad (12.9)$$

Then $R(s,t) \geq n+1$.

Proof Let $p = (s/en)^{2/(s-1)}$ and $q_1 = 1 - p_1 = (t/en)^{2/(t-1)}$. Then $q = 1 - p < q_1$ by our assumption, so

$$E_p(Y_s) = \binom{n}{s} p^{\binom{s}{2}} < \frac{1}{2}\left(\frac{en}{s}\right)^s p^{\binom{s}{2}} = \frac{1}{2}$$

and

$$E_p(\bar{Y}_t) = E_q(Y_t) < E_{q_1}(Y_t) = \binom{n}{t} q_1^{\binom{t}{2}} < \frac{1}{2}\left(\frac{en}{t}\right)^t q_1^{\binom{t}{2}} = \frac{1}{2}.$$

Hence (12.8) holds for our choice of n and p. □

Corollary 12.9 *For $3 \leq s \leq t$ we have*

$$R(s,t) \geq \frac{1}{e} t^{(s-1)/2} s^{-(s-3)/2} (\log t)^{-(s-1)/2}.$$

Proof Set $n = \lfloor (1/e) t^{(s-1)/2} s^{-(s-3)/2} (\log t)^{-(s-1)/2} \rfloor$. By Corollary 12.8 it suffices to check that (12.9) holds. Note that, by inequality (12.8) of Chapter 1,

$$\begin{aligned} \left(\frac{t}{en}\right)^{2/(t-1)} &\geq \left(t^{-(s-3)/2} s^{(s-3)/2} (\log t)^{(s-1)/2}\right)^{2/(t-1)} \\ &\geq t^{-\{(t-1)s/2t\}2/(t-1)} \\ &= \exp\{-(\log t)s/t\} > 1 - (\log t)s/t \geq 1 - \left(\frac{s}{en}\right)^{2/(s-1)}. \end{aligned}$$ □

The following is a less precise but more concise formulation of Corollary 12.9: there is a function $\alpha(s,t)$ such that $\lim_{t\to\infty} \alpha(s,t) = 0$ for every $s \geq 3$ and

$$R(s,t) \geq t^{\{s-1-\alpha(s,t)\}/2}. \qquad (12.10)$$

Our next aim is to present a result of Spencer (1977) implying that the exponent $s-1$ can be replaced by $s+1$ in inequality (12.10). This is the analogue of Corollary 12.6 and, as that result, it is based on Theorem 1.18. As our aim is to apply (12.6), we start with a consequence of Theorem 1.18 concerning two kinds of events and not quite regular dependence graphs. The notation we choose is suggested by the form of the formula in (12.6).

Let U and W be disjoint sets and let $\{A_i : i \in U\} \cup \{B_j : j \in W\}$ be a set of events with dependence graph F. Suppose for all $i \in U$ and $j \in W$ we have

$$\begin{array}{ll} P(A_i) = p_A, & P(B_j) = p_B, \\ |\Gamma(i) \cap U| = d_A, & |\Gamma(i) \cap W| = d_{AB} \\ |\Gamma(j) \cap U| = d_{BA}, & |\Gamma(j) \cap W| = d_B. \end{array}$$

Then, by Theorem 1.18,

$$P\left\{\bigcap_{i\in U} \bar{A}_i \cap \bigcap_{j\in W} \bar{B}_j\right\} > 0 \tag{12.11}$$

provided one can find $0 < \gamma_A < 1$ and $0 < \gamma_B < 1$ such that

$$p_A \le \gamma_A(1-\gamma_A)^{d_A}(1-\gamma_B)^{d_{AB}} \tag{12.12}$$

and

$$p_B \le \gamma_B(1-\gamma_A)^{d_{BA}}(1-\gamma_B)^{d_B}. \tag{12.13}$$

Now if, say, $p_A > 2^{-d_A}$ and $p_B > 2^{-d_B}$, then (12.12) and (12.13) imply that $0 < \gamma_A < \frac{1}{2}$ and $0 < \gamma_B < \frac{1}{2}$. In that case, by inequality (12.10) of Chapter 1, inequality (12.11) follows if instead of (12.12) and (12.13) we require that

$$p_A \le \gamma_A \exp\{-(1+\gamma_A)\gamma_A d_A - (1+\gamma_B)\gamma_B d_{AB}\} \tag{12.12$'$}$$

and

$$p_B \le \gamma_B \exp\{-(1+\gamma_A)\gamma_A d_{BA} - (1+\gamma_B)\gamma_B d_B\}. \tag{12.13$'$}$$

Substituting $\delta_A = \gamma_A/p_A$ and $\delta_B = \gamma_B/p_B$, as in Ex. 19 of Chapter 1, we find the following consequence of Theorem 1.18.

Theorem 12.10 *If there are δ_A, δ_B such that $1 < \delta_A < 1/(2p_A)$, $1 < \delta_B < 1/(2p_B)$,*

$$\log \delta_A \ge (1+\delta_A p_A)(d_A p_A)\delta_A + (1+\delta_B p_B)(d_{AB} p_B)\delta_B \tag{12.14}$$

and

$$\log \delta_B \geq (1+\delta_A p_A)(d_{BA} p_A)\delta_A + (1+\delta_B p_B)(d_B p_B)\delta_B, \tag{12.15}$$

then

$$P\left\{\bigcap_{i\in U} \bar{A}_i \cap \bigcap_{j\in W} \bar{B}_j\right\} > 0.$$

The following theorem is a slight sharpening of some results of Spencer (1977), giving the promised improvement on (12.10).

Theorem 12.11 *Let $s \geq 3$ be fixed. Then as $t \to \infty$,*

$$R(s,t) \geq \{c_s + o(1)\}(t/\log t)^{(s+1)/2},$$

where

$$c_s = \left(\frac{(s-2)(s+1)}{s(s-1)^2}\right)^{(s+1)/2} \left(\frac{2(s-2)!}{s(s-1)}\right)^{1/(s-2)}.$$

Proof Fix a positive c, $c < c_s$. We have to show that

$$R(s,t) \geq c(t/\log t)^{(s+1)/2} \tag{12.16}$$

if t is sufficiently large. Find positive numbers a, b and ε such that $0 < \varepsilon < \frac{1}{4}$,

$$\{2(s-2)!\}b > (1+\varepsilon)^2 a^{\binom{s}{2}} c^{s-2} \tag{12.17}$$

and

$$a > 2b + s - 1. \tag{12.18}$$

Such a choice is possible since if we take $\varepsilon = 0$, $c = c_s$ and replace the inequalities in (12.17) and (12.18) by equalities, then, as one can check, the solutions in a and b are positive.

Set $n = \lfloor c(t/\log t)^{(s+1)/2} \rfloor$, $p = a(\log t)/t$ and consider the probability space $\mathcal{G}(n,p)$. Let $U = V^{(s)}$, $W = V^{(t)}$ and let A_σ, B_τ ($\sigma \in U$, $\tau \in W$) be the events as in (12.6). Let F be the graph on $U \cup W$ in which two vertices are joined by an edge iff the corresponding subsets of V have at least two vertices in common. Then F is precisely a dependence graph of $\{A_\sigma : \sigma \in U\} \cup \{B_\tau : \tau \in W\}$ and, with the notation used in Theorem 12.10,

$$p_A = p^{\binom{s}{2}} = \{a(\log t)/t\}^{\binom{s}{2}},$$

$$
\begin{aligned}
p_B &= (1-p)^{\binom{t}{2}} \le \exp\left\{-p\binom{t}{2}\right\} = t^{-a(t-1)/2},\\
d_A &\le \binom{s}{2}\binom{n}{s-2} \le 3n^{s-2} \le 3c^{s-2}(t/\log t)^{(s-2)(s+1)/2},\\
d_{BA} &\le \binom{t}{2}\binom{n}{s-2} < \frac{t^2}{2(s-2)!}n^{s-2} = \frac{c^{s-2}t^2}{2(s-2)!}(t/\log t)^{(s-2)(s+1)/2},\\
d_B &\le \binom{n}{t} < \left(\frac{en}{t}\right)^t, d_{AB} \le \binom{n}{t} < \left(\frac{en}{t}\right)^t.
\end{aligned}
$$

By (12.6) and Theorem 12.10, inequality (12.16) follows if we can find δ_A, δ_B satisfying the conditions of Theorem 12.10. We claim that $\delta_A = 1+\varepsilon$ and $\delta_B = t^{bt}$ will suffice, provided t is sufficiently large. Indeed,

$$
d_A p_A \le 3n^{s-2}\{a(\log t)/t\}^{\binom{s}{2}} = O\{(t/\log t)^{(s+1)(s-2)/2-s(s-1)/2}\} = o(1)
$$

and

$$
\begin{aligned}
d_{AB}p_B\delta_B &\le \left(\frac{en}{t}\right)^t t^{-a(t-1)/2}t^{bt}\\
&\le (ec)^t t^{(s-1)t/2-a(t-1)/2+bt}(\log t)^{-t(s+1)/2} = o(1)
\end{aligned}
$$

since, by (12.18), the exponent of t is negative if t is sufficiently large. Hence (12.14) does hold.

To complete the proof we have to check (12.15). Now, by the last inequality, $d_B p_B \delta_B = o(1)$. Furthermore,

$$
\begin{aligned}
\delta_A p_A d_{BA} &= (1+\varepsilon)\{a(\log t)/t\}^{\binom{s}{2}}\frac{c^{s-2}t^2}{2(s-2)!}\{t/(\log t)\}^{(s-2)(s+1)/2}\\
&= \frac{(1+\varepsilon)a^{\binom{s}{2}}c^{s-2}}{2(s-2)!}(t\log t) < (1+\varepsilon)^{-1}\log\delta_B,
\end{aligned}
$$

which, since $\delta_A p_A = o(1)$, implies (12.15) if t is sufficiently large. □

Once again, one is tempted to exclaim: all this ingenuity and effort just to increase the exponent $(s-1)/2$ to $(s+1)/2$. However, this time the complaint would not be justified, partly because we gain a factor $(t/\log t)$ rather than only 2, and t can be large, and more importantly because it is of great interest to estimate $R(s,t)$ for a fixed small value of s and if s is small, say 3 or 4, then the improvement replaces a trivial result by a substantial one.

Of course, Theorem 12.11 is sharpest for $s = 3$: the lower bound on $R(3, t)$ given by Theorem 12.11 is rather close to the upper bound given by (12.7), which will be improved slightly in §3. This lower bound is essentially due to Erdős (1961), and the proof was one of the first real, and fairly complicated, applications of random graphs. Spencer (1977) improved the lower bound a little (to the one given in Theorem 12.11) and gave a considerably simpler proof, namely the proof presented above.

To close this section we present a streamlined version of the proof due to Erdős (1961) that

$$R(3,t) \geq c(t/\log t)^2 \tag{12.19}$$

for some constant $c > 0$. We do this partly in recognition of the importance of this proof in the history of random graphs, and also because it is an ingenious proof, using the widely applicable method of suitably altering a r.g. In fact, our proof shows that (12.19) is true for every $c < 1/27$, provided t is sufficiently large, i.e. we are going to prove the improvement due to Spencer (1977), namely the case $s = 3$ of Theorem 12.11.

Suppose then that $0 < c < 1/27$ and choose $0 < \varepsilon < 1/12$ and $3 < a < 10/3$ so that

$$a - (1+\varepsilon)^4 ca^3 > 2 + 2\varepsilon. \tag{12.20}$$

[Note that (12.20) is almost precisely the condition on a and c implied by inequalities (12.17) and (12.18).] Set $n = c(t/\log t)^2$ and $p = a(\log t)/t$. [We write $c(t/\log t)^2$ instead of $\lfloor c(t/\log t)^2 \rfloor$ to make the calculations look less cumbersome; this clearly does not affect the validity of the arguments. Equivalently, instead of c we could take a function $c(t)$ with $\lim_{t\to\infty} c(t) = c$.]

Consider the space $\mathscr{G}(n,p)$. For $G_p \in \mathscr{G}(n,p)$ let $E = E(G_p)$ be a minimal set of edges of G_p such that $H_p = G_p - E$ contains no triangles. (The graph H_p is not a uniquely defined function of G_p; usually we have many choices for H_p: we pick one of them.) The following theorem clearly implies that (12.19) holds if t is sufficiently large.

Theorem 12.12 *A.e. G_p is such that H_p has no set of t independent vertices.*

Proof We know from Corollary 3.4 that a.e. G_p has maximal degree at most $\Delta_0 = \lfloor 2pn \rfloor = \lfloor 2act/\log t \rfloor$. From now onwards in this proof most probabilities are taken conditional on $\Delta(G_p) \leq \Delta_0$; for simplicity, we shall just speak of *c-probability* and write P^c instead of P. As we shall estimate c-probabilities only from above, our task is rather easy: crudely we bound the c-probability of an event by twice its probability. Let us pick a set $W \subset V$ of vertices and denote by C_W the event that $G_p[W]$ has an edge xy such that G_p contains no triangle xyz with $z \in V - W$.

Our interest in C_W stems from the fact that if $G_p \in C_W$, then W is not an independent set in H_p. Indeed, if $G_p \in C_W$ and a minimal set $E \subset E(G_p)$ contains xy, then $H_p + xy \subset G_p$ contains a triangle xyw. Now $G_p \in C_W$ implies $w \in W$, and so H_p contains the edges xw and yw.

Hence, our theorem follows if we prove that a.e. G_p belongs to $\cap C_W$, where the intersection is taken over all $W \in V^{(t)}$. Since we have $\binom{n}{t} < \left(\frac{en}{t}\right)^t < t^t/(\log t)$ choices for W (if t is sufficiently large) this, in turn, follows if we show that

$$P^c(\bar{C}_W) \le t^{-t}. \tag{12.21}$$

Why is (12.21) true? Because (i) the c-probability that 'many' pairs of vertices of W have common neighbours (outside W) is very small and (ii) the c-probability that in a given large set of pairs of vertices of W no pair is an edge is also small.

Let us turn to a real proof of (12.21). Set $\eta = \varepsilon^2/2$, $d_0 = \lceil pt(1+\varepsilon)\rceil$, $n_0 = \lceil t^{2-\eta}\rceil$, $d_i = \lceil e^{2i}(pt)/i\rceil$ and $n_i = \lceil t/e^{2i}\rceil$, $i = 1, 2, \ldots, i_0 = \lfloor(\log t - \log\log t)/2\rfloor$. Write P_i for the c-probability that at least n_i vertices in $V - W$ are joined to at least d_i vertices in W. Denoting by $d_W(z)$ the number of neighbours of a vertex $z \in V - W$ in W, we see that the r.vs $d_W(z)$, $z \in V - W$, are independent binomial r.vs, each having parameters p and t, and so mean $pt = a(\log t)$. Hence, by Theorem 1.7(i),

$$P_0 \le 2\binom{n}{n_0} e^{-\{\varepsilon^2 a(\log t)/3\}n_0} < t^{\eta n_0} t^{-\varepsilon^2 n_0} < t^{-2t-1},$$

and, by Theorem 1.7(ii), we find that, for $1 \le i \le i_0$,

$$P_i \le 2\binom{n}{n_i} e^{-e^{2i}a(\log t)n_i} < t^{2te^{-2i}-at} < t^{-2t-1}.$$

These inequalities show that, with c-probability at least $1-t^{-2t}$, $d_W(z) \ge d_0$ for at most $n_0 - 1$ vertices $z \in V - W$, $d_W(z) \ge d_1$ for at most $n_1 - 1$ vertices, and so on, finally $d_W(z) \ge d_{i_0}$ for no vertex $z \in V - W$, since $d_{i_0} > \Delta_0$. Therefore, with c-probability at least $1 - t^{-2t}$, the number of pairs of vertices in W sharing a neighbour in $V - W$ is at most

$$n\binom{d_0}{2} + \sum_{i=1}^{i_0-1}(n_{i-1} - 1)\binom{d_i}{2}$$
$$\le \frac{ca^2(1+\varepsilon)^3}{2}t^2 + 2e^2 t(a\log t)^2 \sum_{i=1}^{i_0-1} e^{2i}/i^2$$

$$\leq \frac{ca^2(1+\varepsilon)^3}{2}t^2 + 40t(a\log t)^2\left(\frac{t}{\log t}\right)5(\log t)^{-2}$$

$$< \frac{ca^2(1+\varepsilon)^4}{2}t^2. \tag{12.22}$$

The proof is almost complete. By (12.20), if t is sufficiently large, then

$$\binom{t}{2} - \frac{ca^2(1+\varepsilon)^4}{2}t^2 > r \tag{12.22'}$$

where $r = \lceil (1+\varepsilon)t^2/a \rceil$. What is the c-probability that none of r given pairs of vertices in W is an edge of G_p? It is at most

$$2(1-p)^r \leq 2\exp\{-(1+\varepsilon)t\log t\} = 2t^{-(1+\varepsilon)t}. \tag{12.23}$$

The edges joining vertices in W are independent of the edges joining W to $V - W$. Hence (12.22), (12.22') and (12.23) imply

$$P^c(\bar{C}_W) \leq 2\{1 - (1 - t^{-2t})(1 - 2t^{-(1+\varepsilon)t})\} < t^{-t},$$

proving (12.21), and so our theorem. □

It is fascinating to compare the proof of Theorem 12.12 with the proof of the case $s = 3$ of Theorem 12.11. The arguments concern precisely the same model, namely $\mathscr{G}(n, p)$, where $n = c(t/\log t)^2$ and $p = a(\log t)/t$, and both are aimed at proving $R(s,t) \geq n+1$, i.e. $P(\Omega) > 0$ where $\Omega = \Omega_1 \cap \Omega_2$, Ω_1 is the event $\mathrm{cl}(G_p) \leq 2$ and Ω_2 is the event $\mathrm{cl}(\bar{G}_p) \leq t-1$.

The expected number of triangles in G_p is $\binom{n}{3}p^3 \sim (a^3c^3/6)(t/\log t)^3 = (a^3c^{3/2}/6)n^{3/2}$, a rather large number, so $P(\Omega_1)$ is rather small. In spite of this, in Theorem 12.11 we managed to show that although $P(\Omega) < P(\Omega_1)$ is small, it is not zero. Thus the proof of Theorem 12.11 represents the head-on approach, for $R(s,t) \geq n+1$ iff $P(\Omega) > 0$; of course, it is rather satisfying that we could actually prove that an event of very small probability does have positive probability.

Theorem 12.12 is completely different, although its aim is also the proof of $R(s,t) \geq n+1$. Nevertheless, rather than showing that an event of small probability does have positive probability, we show that a.e. G_p is rather close to showing $R(s,t) \geq n+1$, namely a.e. G_p is such that every maximal triangle-free subgraph of it has at most $t-1$ independent vertices. In this sense Theorem 12.12 is a little stronger than Theorem 12.11, for it does imply $P(\Omega) > 0$, but $P(\Omega) > 0$ is far from implying that a.e. G_p can be altered a little, in the most natural way, to result in a graph belonging to Ω. Thus, for fairly large values of t, Theorem 12.12 gives a method of trying to construct a concrete graph giving a good lower bound for $R(s,t)$.

12.3 Triangle-Free Graphs

We know from the previous section, from Theorem 12.11 (or 12.12) and inequality (12.7), that there are positive constants c' and c'' such that

$$c'(t/\log t)^2 < R(3,t) < c''\frac{\log\log t}{\log t}t^2 \tag{12.24}$$

for all $t \geq 3$. Considering the notoriety of Ramsey numbers, the bounds in (12.24) are fairly tight. Nevertheless, as we shall see in this section, one can do much better.

We start with improving the upper bound on $R(3,t)$ in (12.24). Ajtai, Komlós and Szemerédi (1980, 1981*b*) were the first to remove the factor $\log\log t$ from (12.24). The trick is to go for a little more than an upper bound on $R(3,t)$. A lower bound on the independence number $\beta_0(G)$ of a graph G of order n and average degree d easily implies an upper bound on $R(3,t)$, and Ajtai, Komlós and Szemerédi managed to prove a surprisingly good lower bound on the independence number. A little later, Shearer (1982) gave a simple and elegant proof of a slightly stronger result. Although the result has nothing to do with random graphs, the proof can be rewritten in a way which emphasizes its probabilistic nature. Even more, one can formulate a slightly stronger theorem which concerns random algorithms; as we shall see, in that case the proof takes care of itself. This pleasing phenomenon is not too uncommon in mathematics, but one is always happy to encounter it.

Given a graph G, define $\tilde{\beta}_0(G)$ as the expected cardinality of the independent set constructed by a greedy algorithm, the expectation taken with respect to the order of the vertices, each order with the same probability. As one can show (Ex. 2), $\tilde{\beta}_0(G)$ is also the expected cardinality of an independent set constructed by the following *random greedy algorithm*: pick a vertex x_1 at random, if $V(G) \neq \{x_1\} \cup \Gamma(x_1)$ set $G_1 = G - \{x_1\} \cup \Gamma(x_1)$; then pick a vertex x_2 of G_1 at random, if $V(G_1) \neq \{x_2\} \cup \Gamma(x_2)$ set $G_2 = G_1 - \{x_2\} \cup \Gamma(x_2)$; and so on. When the process stops, take the independent set $\{x_1, x_2, \ldots\}$. Clearly $\beta_0(G) \geq \tilde{\beta}_0(G)$ for every graph G.

Recall that $d(G)$ denotes the average degree of a graph G. It will be convenient to talk of the average of the empty set of numbers: we take it to be 0, say. Thus the average degree of the null graph is also 0.

Define a function $f : \mathbb{R}^+ \to \mathbb{R}^+$ by $f(0) = 1$, $f(1) = \frac{1}{2}$ and

$$f(d) = (d\log d - d + 1)/(d-1)^2, \quad d \neq 0, 1.$$

Clearly f is continuous, and routine checking shows that $f(d)$ is strictly decreasing from 1 to 0 and is convex. Furthermore, we have

$$\begin{aligned} f'(d) &= \frac{(\log d)(d-1) - 2(d\log d - d + 1)}{(d-1)^3} \\ &= \frac{-(d+1)\log d + (d^2-1)/d + (d-1)^2/d}{(d-1)^3} \end{aligned}$$

and, in fact, for all $0 < d < \infty$,

$$1 - (d+1)f(d) + (d-d^2)f'(d) = 0. \qquad (12.25)$$

Theorem 12.13 *Let G be a triangle-free graph of order n and average degree d. Then*

$$\tilde{\beta}_0(G) \geq f(d)n.$$

In particular, $\beta_0(G) \geq f(d)n$.

Proof Let us apply induction on n. For $n = 0$ there is nothing to prove, so suppose $n > 0$ and the assertion holds for smaller values of n. We may also assume that $d > 0$.

For $x \in V = V(G)$ let $d(x)$ be the degree of $x, \tilde{d}(x)$ the average degree of the neighbours of x and set $G_x = G - \{x\} \cup \Gamma(x)$ and $d_x = d(G_x)$. Our graph G is triangle-free, so no two neighbours are joined by an edge. Therefore

$$|G_x| = n - d(x) - 1$$

and

$$d_x\{n - d(x) - 1\} = 2e(G_x) = 2e(G) - 2\sum_{g\in\Gamma(x)} d(y) = nd - 2d(x)\tilde{d}(x). \quad (12.26)$$

Furthermore, by the convexity of f,

$$f(d_x) \geq f(d) + (d_x - d)f'(d)$$

and so, by our induction hypothesis,

$$\begin{aligned} \tilde{\beta}_0(G) &= 1 + \frac{1}{n}\sum_{x\in V}\tilde{\beta}_0(G_x) \geq 1 + \frac{1}{n}\sum_{x\in V} f(d_x)\{n - d(x) - 1\} \\ &\geq 1 + \frac{1}{n}\sum_{x\in V}\{f(d) + (d_x - d)f'(d)\}(n - d(x) - 1). \end{aligned}$$

By making use of (12.26) and $\sum_{x\in V} d(x) = nd$, we find that

$$\begin{aligned}\tilde{\beta}_0(G) &\geq 1 + f(d)n - f(d)(d+1) + \frac{f'(d)}{n}\sum_{x\in V}\{-2d(x)\tilde{d}(x) + dd(x) + d\}\\ &= f(d)n + 1 - f(d)(d+1) + f'(d)(d^2+d) - 2\frac{f'(d)}{n}\sum_{x\in V} d(x)\tilde{d}(x).\end{aligned}$$

Now $f'(d) < 0$ and

$$\sum_{x\in V} d(x)\tilde{d}(x) = \sum_{x\in V}\sum_{y\in\Gamma(x)} d(y) = \sum_{y\in V} d^2(y) \geq nd^2,$$

so

$$\tilde{\beta}_0(G) \geq f(d)n + 1 - f(d)(d+1) + f'(d)(d^2+d) - 2f'(d)d^2 = f(d)n,$$

where in the last step we made use of (12.25). □

It is reasonable to wonder how the function f was found and whether we could do better by choosing another function. Assume then that a function $g : \mathbb{R}^+ \to \mathbb{R}^+$ is such that $\tilde{\beta}_0(G) \geq g(d)n$ for every triangle-free graph G of order n and average degree d. We hope to prove this by setting $G_x = G - \{x\} \cup \Gamma(x)$ and $d_x = d(G_x)$ for a vertex $x \in G$ and then using

$$\tilde{\beta}_0(G) = 1 + \frac{1}{n}\sum_{x\in G} g(d_x)\{n - d(x) - 1\}.$$

Hence we would like to have

$$1 + \frac{1}{n}\sum_{x\in G} g(d_x)\{n - d(x) - 1\} \geq g(d)n.$$

Suppose now that $d > 1$ is fixed, n is large and G is d-regular. Then with $h = d - d_x$ we have

$$h = d - \frac{nd - 2d^2}{n-d-1} = \frac{d^2-d}{n-d-1}$$

and we would like to have

$$1 + g(d-h)(n-d-1) \geq g(d)n,$$

that is

$$(d^2-d)\frac{g(d)-g(d-h)}{h} = (n-d-1)\{g(d)-g(d-h)\} \leq 1 - (d+1)g(d).$$

Letting $n \to \infty$, we have $h \to 0$ and therefore, assuming that the derivative exists,

$$(d^2 - d)g'(d) \leq 1 - (d+1)g(d). \tag{12.27}$$

Assuming, though we should not, that (12.27) holds for all $d \geq 1$, we cannot do better than choosing for $g(d)$, $d \geq 1$, the solution of

$$(d^2 - d)g'(d) = 1 - (d+1)g(d), g(1) = \tfrac{1}{2},$$

which is precisely $(d \log d - d + 1)/(d-1)^2 = f(d)$, the function appearing in Theorem 12.13. The initial condition $g(1) = \frac{1}{2}$ follows from the fact that if G consists of $n/2$ independent edges, then $d(G) = 1$ and $\tilde{\beta}_0(G) = \beta_0(G) = n/2$, so $g(1) \leq \frac{1}{2}$.

The only weakness in the argument above is that (12.27) was assumed to hold for all $d > 1$; nevertheless, it is clear that even a refinement of the proof of Theorem 12.13 cannot give more than $\beta_0(G) \geq \{1+o(1)\} \log d/d$. On the other hand, for $d < 1$ one can do considerably better (Ex. 4).

Instead of the function $f(d)$, it is often more convenient to use the following consequence of Theorem 12.13: if G is a triangle-free graph of order n and average degree $d > 0$, then

$$\beta_0(G) \geq \tilde{\beta}_0(G) \geq \frac{\log d - 1}{d} n. \tag{12.28}$$

The promised upper bound on $R(3, t)$ is an immediate corollary of Theorem 12.13.

Theorem 12.14 *For $t \geq 3$ we have*

$$R(3, t) \leq \frac{(t-1)(t-2)^2}{(t-1)\log(t-1) - t + 2} + 1.$$

Proof Suppose that, contrary to the assertion of the theorem, there is a graph G of order

$$n = \left\lfloor \frac{(t-1)(t-2)^2}{(t-1)\log(t-1) - t + 2} \right\rfloor + 1,$$

which is triangle-free and whose independence number is at most $t-1$. Then, since the neighbours of every vertex of G are independent, $\Delta(G) \leq t-1$, and so $d(G) \leq t-1$. Hence, by Theorem 12.13,

$$t - 1 \geq \beta_0(G) \geq \frac{(t-1)\log(t-1) - t + 2}{(t-2)^2} n,$$

contradicting the choice of n. □

There is no doubt that Theorem 12.14 is a beautiful and substantial result, and its proof is elegant and ingenious. Nevertheless, improving the lower bound on $R(3,t)$ in (12.24) is a quite different matter, so it was a major achievement that Kim (1995*b*) improved the lower bound to an essentially best possible result.

Theorem 12.15 *There is a constant* $c > 0$ *such that*

$$R(3,t) \geq c\ t^2/\log t$$

for every $t \geq 2$. □

In fact, Kim proved that $R(3,t) \geq (\frac{1}{162} + o(1))t^2/\log t$ as $t \to \infty$, although he did not make an effort to maximize the constant $1/162$. With this result Kim completed the determination of $K(3,t)$ up to a constant:

$$\left(\frac{1}{162} + o(1)\right)\frac{t^2}{\log t} \leq R(3,t) \leq (1 + o(1))\frac{t^2}{\log t}.$$

Kim's proof (1995*b*) of Theorem 12.15 is full of ideas; to carry out his line of attack, Kim had to overcome major technical obstacles. The proof is based on Hoeffding–Azuma type martingale inequalities and, more importantly, makes an elaborate use of the *'semi-random method'* or *'Rödl's nibble method'*, whose origins go back to the paper of Ajtai, Komlós and Szemerédi (1980) in which they removed the log log t factor from the upper bound in (12.24). Very crudely, in the semi-random method we select our objects in many small 'nibbles' rather than in one big 'bite', and take great care to analyse in what way the nibbles change the structure of the remainder. As we remarked in §5 of Chapter 11, this method was used by Kim (1995*a*) and Johansson to prove a considerable strengthening of Brooks' theorem for sparse graphs, namely that every graph of maximal degree $\Delta \geq 2$ and girth at least 5 has chromatic number at most $(1 + o(1))\Delta/\log\Delta$.

Erdős proposed the study of the maximal chromatic number of a triangle-free graph of order n. Writing $f(n)$ for this maximum, as remarked by Nilli (2000), Theorems 12.14 and 12.15 imply that

$$c_1(n/\log n)^{1/2} \leq f(n) \leq c_2(n/\log n)^{1/2}$$

for some positive constants c_1 and c_2. Furthermore, Nilli (2000) used a theorem of Johansson (2000) to determine the asymptotic order of another function defined by Erdős, the maximal chromatic number $g(m)$ of a triangle-free graph with m edges.

Johansson (2000) used the semi-random method to prove that the maximal chromatic number of a triangle-free graph of maximal degree $\Delta \geq 2$ is at most $c_3\Delta/\log\Delta$ for some constant c_3. In proving Theorem 12.15, Kim showed that if n is large enough then there is a triangle-free graph of order n, size at most $c_4 n^{3/2}(\log n)^{1/2}$ and independence number at most $c_5(n\log n)^{1/2}$, where c_4 and c_5 are constants. Nilli combined these deep results to deduce that

$$c_6 m^{1/3}/(\log m)^{2/3} \leq g(m) \leq c_7\, m^{1/3}/(\log m)^{2/3}$$

for some positive constants c_6 and c_7.

In order to bound $R(s,t)$ for $s \geq 4$, we need an upper bound on the independence number of a graph containing few triangles. For $n \in \mathbb{N}$, $d \geq 0$ and $h \geq 0$ define

$$\beta_0(n,d,h) = \min\{\beta_0(G) : |G| = n, d(G) \leq d \text{ and } k_3(G) \leq h\}.$$

By definition, $\beta_0(n,d,h)$ is a monotone increasing function of each of its variables. Theorem 12.13 and inequality (12.28) have the following easy consequence.

Lemma 12.16 (*i*) *If* $d > 0$, *then*

$$\beta_0(n,d,n) > \frac{1}{e^2}\frac{\log d}{d}n.$$

(*ii*) *With* $c_0 = 2^7 5^{-2} 7^{-2} > 1/10$ *we have*

$$\beta_0(n,d,h) \geq c_0(n/d)\left\{\log d - \frac{1}{2}\log(h/n)\right\}.$$

Proof (i) A graph G of order n with at most n triangles contains a triangle-free subgraph G_1 of order $n_1 \geq (16/35)n$ (see Ex. 5). Clearly $d(G_1) \leq d(G)n/n_1 \leq (35/16)d$, so the assertion follows from Theorem 12.13.

(ii) Suppose $|G| = n, d(G) \leq d$ and G has at most h triangles. Because of (i), we may assume that $h > n$. Furthermore, we may assume also that $d \geq 1000$ and $\log d - \frac{1}{2}\log(h/n) \geq 9$, for otherwise, since $\beta_0(G) \geq n/(d+1)$, there is nothing to prove. Consequently $h \leq n^3/e^{18}$. Set $n_0 = \lfloor (n^3/2h)^{1/2} \rfloor > e^8$ and note that $n_0^2 > n^3/(2.01h)$ and

$$(n_0-1)(n_0-2) < \frac{n(n-1)(n-2)}{2h}.$$

Consider all subgraphs of G induced by n_0 vertices. The expected number of edges in these subgraphs is

$$e(G)\binom{n_0}{2}\Big/\binom{n}{2} < \frac{d}{2}n_0^2/n$$

and the expected number of triangles is

$$k_3(G)\binom{n_0}{3}\Big/\binom{n}{3} \leq \frac{hn_0(n_0-1)(n_0-2)}{n(n-1)(n-2)} < n_0/2.$$

Hence, simply by Chebyshev's inequality, there is a subgraph G_0 spanned by n_0 vertices which satisfies

$$e(G_0) < dn_0^2/n \text{ and } k_3(G_0) < n_0.$$

Then, again by Ex. 4, G_0 has a subgraph G_1 spanned by $n_1 = \lceil (16/35)n_0 \rceil$ vertices, which is triangle-free. As

$$d_1 = d(G_1) = 2e(G_1)/n_1 \leq 2e(G_0)/n_1 < 2dn_0^2/(nn_1) = d_2,$$

by inequality (12.28) we have

$$\begin{aligned} \beta_0(G) &\geq \beta_0(G_1) \geq f(d_1)n_1 \geq \{\log(d_2-1)/d_2\}n_1 \\ &\geq \frac{1}{2}\left(\frac{16}{35}\right)^2 \frac{n}{d}\left\{\log\left(2d\frac{35}{16}\frac{n^{1/2}}{(2.01h)^{1/2}}\right)-1\right\} \\ &> c_0(n/d)\left\{\log d - \tfrac{1}{2}\log(h/n)\right\} \end{aligned}$$

□

Lemma 12.16 gives the following upper bound on $R(s,t)$.

Theorem 12.17 *There are constants $c_3, c_4, \ldots$ such that for every $s \geq 3$ we have $c_s < 2(20)^{s-3}$ and, if t is sufficiently large,*

$$R(s,t) < c_s t^{s-1}/(\log t)^{s-2}.$$

Proof The existence of c_3 is guaranteed by Theorem 12.13. Suppose now that we have shown the existence of $c_4, \ldots, c_{s-1}$. Pick a constant c_s satisfying

$$20c_{s-1} < c_s < 2(20)^{s-3}.$$

Let G be a graph of order $n = \lfloor c_s t^{s-1}/(\log t)^{s-2} \rfloor$ with $\mathrm{cl}(G) \leq s-1$ and $\beta_0(G) \leq t-1$. Our aim is to arrive at a contradiction.

Set $n_1 = \lfloor c_{s-1}t^{s-2}/(\log t)^{s-3} \rfloor, n_2 = R(s-2,t) = R(2,t) = t$ if $s = 4$ and $n_2 = \lfloor c_{s-2}t^{s-3}/(\log t)^{s-4} \rfloor$ if $s \geq 5$. Note that if t is sufficiently large, then, by the induction hypothesis, $R(s-1,t) \leq n_1$ and $R(s-2,t) \leq n_2$. Therefore $\Delta(G) < R(s-1,t) \leq n_1$ and so $d(G) < n_1$. Write h for the number of triangles in G. We distinguish two cases according to the size of h.

(a) Suppose $h \geq nn_1n_2/6$. Then some vertex x is in at least

$$\frac{3}{n}\frac{nn_1n_2}{6} = \frac{n_1n_2}{2}$$

triangles, i.e. the subgraph H_1 spanned by $\Gamma(x)$ has at least $n_1n_2/2$ edges. Since $|H_1| < n_1$, some vertex y of H_1 has degree at least n_2 in H_1. Equivalently, the set $W = \Gamma(x) \cap \Gamma(y)$ has at least n_2 vertices. Set $H_2 = G[W]$. Then $\beta_0(H_2) \leq \beta_0(G) \leq t-1$ and $|H_2| \geq n_2 \geq R(s-2,t)$ imply that $\mathrm{cl}(H_2) \geq s-2$. However, this is impossible since a complete $(s-2)$-subgraph of H_2 can be extended to a complete s-subgraph of G by adding x and y.

(b) Suppose now that $h < nn_1n_2/6$. Then, by Lemma 12.16, if n is sufficiently large,

$$\beta_0(G) \geq c_0(n/n_1)\left\{\log n_1 - \tfrac{1}{2}\log(h/n)\right\},$$

since $d(G) < n_1$. We have

$$n_1(n/h)^{1/2} > (6n_1/n_2)^{1/2}$$

so, for sufficiently large t,

$$\begin{aligned}\beta_0(G) &\geq c_0\left\{\tfrac{1}{2}+o(1)\right\}(c_s/c_{s-1})(t/\log t)\log(6n_1/n_2)\\ &= c_0\left\{\tfrac{1}{2}+o(1)\right\}(c_s/c_{s-1})t > (c_s/20c_{s-1})t > t,\end{aligned}$$

contradicting our assumption on G. □

12.4 Dense Subgraphs

Theorem 12.1, Ramsey's classical theorem, has numerous variants and extensions. Here we shall note only very few of them, related to random graphs; for a more substantial look at generalized Ramsey theory the reader is referred to Graham, Rothschild and Spencer (1980, 1990).

In Ramsey's theorem we consider a 2-colouring of K^n and look for a monochromatic complete subgraph of order r. Now let us look for monochromatic subgraphs which need not be complete but only fairly dense. We shall use two different ways of measuring how close a colouring is to being monochromatic.

Define the *discrepancy*, disc H, of a graph H as disc $H = |e(H)-e(\bar{H})|$, where $\bar{H}$ is the complement of H. Note that disc H = disc$\bar{H}$, so we may define the discrepancy of a 2-colouring of a complete graph K^r

as the discrepancy of the subgraph formed by the edges of one of the colours. Erdős and Spencer (1972) determined the order of the maximal discrepancy every 2-colouring has.

Theorem 12.18 *There is a constant $c > 0$ such that every 2-colouring of K^n contains a complete graph whose colouring has discrepancy at least $cn^{3/2}$.*

Numerous extensions of Theorem 12.18 were proved by Bollobás and Scott (2001).

Another measure of near-completeness of a graph is the ratio of the minimal degree and maximal possible degree. For $0 \le \alpha \le 1$ and $r \in \mathbb{N}$ denote by $R_\alpha(r)$ the smallest integer n such that if G is any graph of order n, then either G or $\overline{G}$ contains a subgraph H of order at least r satisfying

$$\delta(H) \ge \alpha(|H| - 1).$$

Clearly $R_0(r) = r$ and $R_1(r) = R(r)$. For $0 < \alpha < 1$ the function $R_\alpha(r)$ was studied by Erdős and Pach (1983). There is a striking difference between the cases $\alpha < \frac{1}{2}$ and $\alpha > \frac{1}{2}$.

Theorem 12.19 *(i) For $0 < \alpha < \frac{1}{2}$ there is a constant $c_1(\alpha)$ such that $R_\alpha(r) \le c_1(\alpha)r$.*

(ii) For $\frac{1}{2} < \alpha < 1$ there is a constant $c_2(\alpha) > 1$ such that $R_\alpha(r) \ge \{c_2(\alpha)\}^r$. □

The first part of this result can be proved by successive deletion of appropriate vertices (Ex. 8); the second part is proved by considering $\mathcal{G}(n, \frac{1}{2})$ for $n = \lfloor e^{r(\alpha-1/2)^2/2} \rfloor$ (see Ex. 9).

What can we say about $R_\alpha(r)$ in the most interesting case, namely when $\alpha = \frac{1}{2}$? Erdős and Pach came rather close to determining the exact growth of $R_{1/2}(r)$.

Theorem 12.20 *There are positive constants c_1 and c_2 such that*

$$c_1 \frac{r \log r}{\log \log r} \le R_{1/2}(r) \le c_2 r \log r.$$ □

In fact, Erdős and Pach proved only the following slightly weaker form of the lower bound in Theorem 12.19.

Theorem 12.20′ *For every $c \in \mathbb{N}$ there exist $\varepsilon(c) > 0$ and $r_0(c) \in \mathbb{N}$ such that for every $r \ge r_0(c)$ there is a graph G such that $|G| \ge cr$ and if H is any subgraph of G or $\overline{G}$ with at least r vertices, then $\delta(H) \le \{\frac{1}{2} - \varepsilon(c)\}|H|$.*

The proof of Theorem 12.20′ makes use of the model $\mathscr{G}\{n,(p_{ij})\}$, defined in §1 of Chapter 2. Let $c \in \mathbb{N}, c \geq 2$, and let $r \in \mathbb{N}$ be sufficiently large. Set $k = c+2, l = \lfloor\{1-(1/3k)\}r\rfloor, n = kl \geq cr$, and $V = \{1,2,\ldots,n\}$. Partition V into k equal classes: $V = \cup_{i=1}^{k} V_i$. For $1 \leq s < t \leq n$ set

$$P_{st} = \begin{cases} \frac{1}{2} - (3k)^{-3i-3j-1}, & \text{if } s \in V_i, t \in V_j \text{ and } i \neq j, \\ \frac{1}{2} + (3k)^{-6i}, & \text{if } s,t \in V_i. \end{cases}$$

Then, as shown by Erdős and Pach, a.e. $G \in \mathscr{G}\{n;(p_{ij})\}$ will suffice for the graph G in Theorem 12.20′.

Given graphs G_1, G_2 and H, we write $H \to (G_1, G_2)$ for the assertion that every red–blue colouring of the edges of H contains either a red G_1 or a blue G_2.

Define the *Ramsey number of* G_1 *versus* G_2 as $r(G_1,G_2) = \min\{n : K^n \to (G_1,G_2)\}$; for simplicity, write $r(G) = r(G,G)$ and call it the *Ramsey number of* G. A central problem in generalized Ramsey theory is the determination or at least good estimation of $r(G_1,G_2)$ for various pairs of graphs G_1, G_2. We shall not go into this problem here, but in §3 of Chapter 13, we shall estimate the Ramsey number of C^4, a four-cycle versus K^s.

12.5 The Size-Ramsey Number of a Path

Analogously to the Ramsey number of a pair of graphs, define the *size-Ramsey number of* G_1 *versus* G_2 as

$$\hat{r}(G_1,G_2) = \min\{E(H) : H \to (G_1,G_2)\}.$$

Also, call $\hat{r}(G) = \hat{r}(G,G)$ the *size-Ramsey number of* G. Clearly,

$$\hat{r}(G_1,G_2) \leq \binom{n}{2} \tag{12.29}$$

when $n = r(G_1,G_2)$, since $K^n \to (G_1,G_2)$; furthermore, even more trivially, $r(G_1,G_2) \leq 2\hat{r}(G_1,G_2)$.

For dense graphs G_1 and G_2 inequality (12.29) is not too crude, but for sparse graphs (12.29) is very bad indeed. The aim of this section is to present a striking example of the latter, namely a beautiful theorem of Beck (1983*a*) showing that the size-Ramsey number $\hat{r}(P^s)$ of a path of length s is surprisingly small: $\hat{r}(P^s) = O(s)$. [Note that inequality (12.29) is slightly worse than $\hat{r}(P^s) \leq s^2/2$.] The proof below is essentially from Beck (1983*a*); for a slight variant of the proof, relying on different lemmas, see Bollobás (1985*a*).

Given sets $X, Y \subset V = V(G)$, write $e(X,Y) = e_G(X,Y)$ for the number of $X - Y$ edges in G and set

$$d(X) = d_G(X) = (1/|X|)e_G(X, V).$$

Thus if $X = \{x\}$, then $d(X)$ is precisely the degree of x; however, note that $d(V) = e(G)/|V|$ is only half of the average degree $d(G)$. In particular, a connected k-regular graph G contains no subgraph H with $d_H\{V(H)\} > \frac{1}{2}d(G)$. This shows that the lemma below is best possible.

Lemma 12.21 *Every graph G contains a subgraph H such that*

$$d_H(X) \geq \tfrac{1}{2}d(G)$$

for every non-empty subset X of $V(H)$.

Proof Let $W \subset V$ be a minimal non-empty subset satisfying

$$e(G[W]) \geq \tfrac{1}{2}d(G)|W|$$

and set $H = G[W]$. Then for $\varnothing \neq X \subset W, Y = W - X \neq \varnothing$ we have

$$\begin{aligned} d_H(X) &= \frac{1}{|X|}\{e(H) - e(H[Y])\} > \frac{1}{|X|}\left\{e(H) - \frac{1}{2}d(G)|Y|\right\} \\ &\geq \frac{1}{|X|}\left\{\frac{1}{2}d(G)|W| - \frac{1}{2}d(G)|Y|\right\} = \frac{1}{2}d(G). \end{aligned}$$ □

Lemma 12.22 *Suppose a graph G is such that if $X \subset Y \subset V(G)$ and $|Y| \leq 3|X| - 1 \leq 3u - 1$, then*

$$e(X,Y) < \tfrac{1}{4}d(G)|X|.$$

Let G' be a subgraph of G satisfying

$$e(G') \geq \tfrac{1}{2}e(G).$$

Then G' contains a path of length $3u - 1$.

Proof Let H be a subgraph of G' whose existence is guaranteed by Lemma 20 so that

$$d_H(X) \geq \tfrac{1}{2}d(G') \geq \tfrac{1}{4}d(G)$$

for every $X \subset V(H), X \neq \varnothing$. Let $U \subset V(H)$ and $|U| \leq u$. Then

$$|U \cup \Gamma_H(U)| \geq 3|U|, \tag{12.30}$$

for otherwise with $X = U$ and $Y = U \cup \Gamma_H(U)$ we would find that

$$d_H(X)|X| = e(X, Y) < \tfrac{1}{4}d(G)|X|.$$

By Lemma 8.6, relation (12.30) implies that H contains a path of length $3u - 1$. □

Theorem 12.23 *For every sufficiently large natural number s there is a graph G of size at most 720s such that if in a red–blue colouring of the edges of G there are at least as many red edges as blue, then G contains a red path of length s. In particular,*

$$\hat{r}(P_s) \leq 720s.$$

Proof Let $d \in \mathbb{N}, 16 \leq 4d < c < c' < (4.001)d, 0 < \alpha < 0.03, \rho > c'/6\alpha, p = c/n, u = \lfloor \alpha n \rfloor$ and $s = 3u - 1$. Let us consider the space $\mathcal{G}(n, p)$. We know that a.e. G_p satisfies

$$d(G_p) \geq d \text{ and } e(G_p) \leq c'n/2. \tag{12.31}$$

Our aim is to show that if c, c', d, α and ρ are chosen suitably, then a.e. G_p is such that if $X \subset Y \subset V, |Y| = 3|X| = 3t \leq 3u$, then

$$e(X, Y) < dt. \tag{12.32}$$

Because of Lemma 12.21, relations (12.31) and (12.32) will imply that a.e. G_p is such that if $G' \subset G_p$ and $e(G') \geq \frac{1}{2}e(G_p)$, then G' contains a path of length s and so $\hat{r}(P_s) < \rho s$ if s is sufficiently large.

Denote by $Z_t = Z_t(G_p)$ the number of pairs (X, Y) violating condition (12.32). Then our aim is to prove that

$$P\left(\sum_{t=1}^{u} Z_t \geq 1\right) = o(1). \tag{12.33}$$

For a fixed pair $(X, Y), X \subset Y, |Y| = 3|X| = 3t \leq 3u$ the number of $X - Y$ edges has binomial distribution with parameters $t^* = \binom{t}{2} + 2t^2 < \frac{5}{2}t^2$ and p. Since

$$dt > 3\left(\tfrac{5}{2}t^2 p\right),$$

by Theorem 1.1 we have

$$\begin{aligned} E(Z_t) &\leq \binom{n}{t, 2t}\binom{5t^2/2}{dt} p^{dt}(1-p)^{5t^2/2-dt} \\ &\leq c_0 t^{-3/2}\left(\frac{n}{t}\right)^t \left(\frac{n}{2t}\right)^{2t} \left(\frac{n}{n-3t}\right)^{n-3t} \left(\frac{5etc}{2dn}\right)^{dt} e^{-5t^2c/2n} \\ &\leq c_0 t^{-3/2}(t/n)^{(d-3)t}2^{-2t}e^{(d+3)t}(10.01)^{dt}e^{-5t^2c/2n}, \end{aligned} \tag{12.34}$$

where $c_0 = c_0(\alpha, c, d)$, since $(1-x)^{x-1} < \mathrm{e}^x$ for $0 < x < 1$. Hence

$$E(Z_t) \le c_0\{tn^{-1}(10.01)^{d/(d-3)}\mathrm{e}^{(d+3)/(d-3)}2^{-2/(d-3)}\}^{(d-3)t}, \tag{12.35}$$

since $c < (4.0001)d$. With $c = 72.001, c' = 72.002, d = 18, \alpha = 1/59$ and $\rho = 720$ we find that our conditions are satisfied and the base on the right-hand side of (12.35) is bounded away from 1, so

$$\sum_{t=1}^{u} E(Z_t) = o(1),$$

which implies (12.33). □

The constant 720 in Theorem 12.23 can be reduced slightly if one is a little more careful with the estimates. Inequality (12.34) implies that

$$\sum_{t=1}^{u_0} E(Z_t) = o(1)$$

where $u_0 = \lfloor \alpha_0 n \rfloor, \alpha_0 = \alpha_0(d) > 0$. Also, if $u_0 \le t = \beta n \le u$, then (12.34) gives that

$$\begin{aligned} \log E(Z_t) \;\le\; & t\{(d-3)\log\beta - 2\log 2 + \{3-(1/\beta)\}\log(1-3\beta) \\ & +d\log(10.01\mathrm{e}) - 10d\beta\} = tf(d,\beta). \end{aligned}$$

Setting $d = 20$ and $\alpha = 1/40$, we find that for $0 < \beta \le \alpha$

$$\frac{\mathrm{d}f(20,\beta)}{\mathrm{d}\beta} = \frac{17}{\beta} - \frac{9}{1-3\beta} + \frac{1}{\beta^2}\log(1-3\beta) + \frac{3}{\beta(1-3\beta)} \ge \frac{17}{\beta} - 10 > 0.$$

Since $\phi = f(20, 0.025) > 0$, we find that

$$\sum_{t=u_0}^{u} E(Z_t) \le \sum_{t=u_0}^{u} \mathrm{e}^{-\phi t} = o(1).$$

Consequently if $c = 80.001, c' = 80.002, d = 20, \alpha = 0.025$ and $\rho = 540$, then our conditions are satisfied and (12.33) also holds. Hence $\hat{r}(P_s) \le 540s$ if s is sufficiently large.

It is easily seen that Theorem 12.23 has the following extension: for every $\varepsilon > 0$ there is a constant $c(\varepsilon)$ such that for every $s \in \mathbb{N}$ there is a graph of size $c(\varepsilon)s$, whose every subgraph of size at least $\varepsilon c(\varepsilon)s$ contains a path of length s. A consequence of this is that $\hat{r}_k(P^s) \le c(1/k)s$, where $\hat{r}_k$ denotes the size-Ramsey number for k-colourings. As expected, this extension has numerous other consequences concerning size-Ramsey numbers of various graphs.

At least how large does $\hat{r}(s)$ have to be? Trivially, $\hat{r}(s) \ge 2s - 1$ since every graph with at most $2s-2$ edges has a red–blue colouring with at most $s-1$ red edges and at most $s-1$ blue edges, and so without a monochromatic P^s. However, it is not immediate to see that for some $c>2$ we have $\hat{r}(P^s) \geq cs$ for all sufficiently large s. This was proved by Beck (1985), who showed that $\hat{r}(P^s) \geq (9/4)s$; a slightly better bound can be found in Bollobás (1985*a*): $\hat{r}(P^s) \geq (1+\sqrt{2})s - 2$ for every s.

There is a recent result concerning generalized Ramsey numbers which resembles Beck's theorem in form but not in essence. Settling a conjecture of Burr and Erdős (1975), Chvátal *et al.* (1983) proved that for every $\Delta \in \mathbb{N}$ there is a constant $c(\Delta)$ such that if G is a graph of order n and maximal degree at most Δ, then $r(G) \leq c(\Delta)n$. (The proof of this result does not make use of random graphs.) However, as an extension of Theorem 12.23, one would like to have $\hat{r}(G) \leq c'(\Delta)n$ which would be much stronger than $r(G) \leq c(\Delta)n$.

Exercises

12.1 Prove that if G has n vertices, then $\beta_0(G) \geq n/(d+1)$. [This is more or less Turán's classical theorem, see Bollobás (1978*a*, chapter 6) for numerous related results.]

12.2 Consider the following two random greedy algorithms for constructing independent sets in a graph G.

(a) Take a random linear order on $V(G)$ and run the greedy algorithm.

(b) Pick a vertex at random, put it in your independent set and delete the vertex and all its neighbours; pick another vertex at random, put it in your independent set and delete the vertex and all its neighbours; and so on.

Show that (a) and (b) define the same probability measure on the set of independent sets of G; in particular, they give the same expected order $\tilde{\beta}_0(G)$ of an independent set.

12.3 Do all independent k-sets occur with the same probability in an independent set constructed by a random greedy algorithm? Do they occur with the same probability as the first k elements of an independent set?

12.4 Prove that if G is a graph of order n and average degree $d<1$, then

$$\beta_0(G) \geq \tilde{\beta}_0(G) \geq (1-d/2)n.$$

12.5 Let G be a graph of order n, containing h triangles. Run the following greedy algorithm to eliminate the triangles in G. Set $G_0 = G$. Having constructed G_j, if $k_3(G_j) > 0$, pick a vertex x_j of G_j in as many triangles as possible and set $G_{j+1} = G_j - \{x_j\}$, if $k_3(G_j) = 0$, terminate the sequence in G_j. Let G_s be the final member of the sequence. Show that

$$|G_s| \geq \alpha_l(ln - h) \text{ for } \{(l-1)/3\}n \leq h \leq (1/3)n,$$

where

$$\alpha_l = \prod_{j=2}^{l} \frac{2j-2}{2j+1}, \text{ so } \alpha_1 = 1, \alpha_2 = \frac{2}{5}, \alpha_3 = \frac{8}{35}, \text{ etc.}$$

12.6 Show that for fixed values of l the bounds in Ex. 5 are essentially best possible. Note that as $h/n \to \infty$ the bound is about $cn^{5/2}h^{-3/2}$.

12.7 Deduce from the proof of Theorem 12.17 that for all $\varepsilon > 0$ and $s \geq 3$ there exists a constant $c(\varepsilon, s) > 0$ such that if t is sufficiently large, then either

$$R(s,t) < c(\varepsilon, s)R(s-1,t)(t/\log t)$$

or

$$R(s-1,t) < R(s-2,t)t^{\varepsilon}.$$

(Ajtai, Komlós and Szemerédi, 1980.)

12.8 Let $0 < \alpha < \frac{1}{2}$ and $(\frac{1}{2}-\alpha)n^2+(2\alpha-1)n+3c > (1-\alpha)r^2+(4\alpha-1)r$. By successively deleting each vertex of too small degree, show that if G is a graph of order n and size at least $\frac{1}{2}(n/2)$, then G has a subgraph H of order at least r such that $\delta(H) \geq \alpha(|H|-1)$.

Deduce Theorem 12.18(i).

12.9 Let $\frac{1}{2} < \alpha < 1$ be fixed and $r \in \mathbb{N}$. Set $n = \lfloor e^{r(\alpha-1/2)^2/2} \rfloor$ and denote by P_r the probability that $G \in \mathscr{G}(n, \frac{1}{2})$ has a subgraph H such that $|H| \geq r$ and $\delta(H) \geq \alpha(|H|-1)$. Prove that $\lim_{r\to\infty} P_r = 0$ and deduce Theorem 12.19(ii).

12.10 Let $c_1 < \frac{1}{2}$. Prove that for every sufficiently large n, there is a graph of order n satisfying

$$\chi(G)/\text{cl}(G) > c_1 n/(\log_2 n)^2.$$

Show also that if $c_2 > 4$ and n is sufficiently large, then every graph G of order n satisfies

$$\chi(G)/\text{cl}(G) < c_2 n/(\log_2 n)^2.$$

[The first inequality follows from Corollary 11.2 and Theorem 11.12. To see the second, note that, by Theorem 12.1, if $|G| = n, \mathrm{cl}(G) = r$ and $n^{1-\varepsilon} \geq \binom{r+s-2}{r-1} \geq R(r,s)$, then $\beta_0(H) \geq s$ for all $H \subset G, |H| \geq n^{1-\varepsilon}$, and so $\chi(G) \leq (n/s) + n^{1-\varepsilon}$.] (Erdős, 1967.)

13
Explicit Constructions

Random graphs have numerous applications to standard problems in graph theory, mainly because they enable us to show the existence of graphs with peculiar properties, without the need for constructing them. Nevertheless, one must realize that, more often than not, constructions are more illuminating than existence proofs, so it is useful to give explicit constructions of graphs having some properties of typical random graphs. These explicit constructions resembling typical r.gs will be called *concrete random graphs* or *pseudo-random graphs*. At first sight it may be surprising that such constructions are not easily come by and even now there are rather few of them, although their usefulness has been known for about two decades.

The quintessential example of a concrete r.g. is the *Paley graph* or *quadratic residue graph* P_q, whose vertex set is $\mathbb{F}_q$, the finite field of order q, where q is a prime power congruent to 1 modulo 4, in which xy is an edge iff $x - y$ is a quadratic residue. As we shall see, P_q is rather similar to a typical element of $\mathcal{G}(q, P(\text{edge}) = \frac{1}{2})$. The salient properties of P_q will be presented in §2, while §1 will be devoted to the prerequisites of the proofs of these properties, such as various results about Gaussian sums and the Riemann hypothesis for curves over finite fields.

In §3 we shall present some algebraic constructions based on quadratic residues and finite geometries. The graphs constructed in this way tend to be rather dense. Concrete random graphs of bounded degree will be discussed in the final section.

13.1 Character Sums

In order to show that the Paley graph Q_q strongly resembles a typical element of $\mathcal{G}(q, P(edge) = \frac{1}{2})$, one has to rely on André Weil's famous

(1940, 1948) theorem, the *Riemann hypothesis for the zeta-function of an algebraic function field over a finite field.* The original proof of Weil, making essential use of algebraic geometry, has been simplified greatly over the years. In a series of papers Stepanov (1969, 1970, 1971, 1972*a*, *b*, 1974) gave an entirely new proof of special cases of Weil's theorem. This proof was extended by Bombieri (1973) and Schmidt (1973) to yield the full result of Weil. Stepanov's proof is combinatorial in nature and is related to methods in diophantine approximation and transcendence theory (see Baker, 1975). For an elegant and detailed presentation of a collection of results related to Weil's theorem on curves over finite fields, based on the combinatorial approach, the reader is referred to Schmidt (1976).

For lack of space the main result of the section, Theorem 13.3, will not be proved: we shall confine ourselves to proving a considerably simpler result, Theorem 13.2. Nevertheless, the proof of Theorem 13.2 will give the flavour of Stepanov's method. We start with an elementary lemma.

Let $F = \mathbb{F}_q$ be the finite field of order q, and let $F[X]$ be the ring of polynomials over F. Given $p(X) \in F[X]$ and $0 \leq l$, denote by $D^l p(X)$ the lth derivative of $p(X)$ with respect to X.

Lemma 13.1 *Suppose q is a prime, $x_0 \in F$ and $(D^l p)(x_0) = 0$ for $0 \leq l < L \leq q$. Then x_0 is a zero of p with multiplicity at least L.*

Proof We apply induction on L, starting with the empty assertion for $L = 0$. Suppose $L > 0$ and the lemma holds for smaller values of L. Then $p(X) = (X - x_0)^{L-1} r(X) = (X - x_0)^{L-1}\{(X - x_0)s(X) + c\} = (X - x_0)^L s(X) + c(X - x_0)^{L-1}$, where $r(X), s(X) \in F[X]$ and $c \in F$. Since

$$0 = (D^{L-1}p)(x_0) = [D^{L-1}\{c(X - x_0)^{L-1}\}](x_0) = c(L-1)!$$

we have

$$p(X) = (X - x_0)^L s(X). \qquad \square$$

Theorem 13.2 *Suppose $d \geq 3$ is an odd integer, $q > 4d^2$ is a prime, $F = \mathbb{F}_q$ and $f(X) \in F[X]$ is a polynomial of degree d. Then the number s of solutions of the equation*

$$y^2 = f(x)$$

satisfies

$$|s - q| \leq 4dq^{1/2}.$$

Proof We start by listing the elementary relations that will be needed in the proof proper. Put $L = \lfloor q^{1/2} \rfloor$ and $J = \frac{1}{2}(L+u)$, where $u = 2d$ or $2d+1$, so that J is an integer. It is easily checked that

$$E = L\left\{\tfrac{1}{2}(q-d-2) + (L-1)(d-1) + J\right\} < V = J(q-d) \qquad (13.1)$$

and

$$\tfrac{1}{2}(q-d-2) + (J-1)q + d(q-1)/2 \le L\{(q/2) + 2dq^{1/2} - d\}. \quad (13.2)$$

For $0 \le j < J$ and $k = 0, 1$ put $A(j,k) = qj + kd(q-1)/2$ and $B(j,k) = \frac{1}{2}(q-d-2)+qj+kd(q-1)/2$. We claim that the intervals $[A(j,k), B(j,k)]$ are disjoint. Indeed, suppose that $[A(j,k), B(j,k)] \cap [A(j',k'), B(j',k')] \neq \emptyset$, where $(j,k) \neq (j',k')$. Then clearly $k \neq k'$, say $k = 0$ and $k' = 1$, and so either

$$A(j,0) \le A(j',1) \le B(j,0)$$

or

$$A(j',1) \le A(j,0) \le B(j',1).$$

Now the first relation implies that

$$0 \le q(j'-j) + dq/2 - d/2 \le \tfrac{1}{2}q - \tfrac{1}{2}(d+2),$$

giving the contradiction

$$\tfrac{1}{2}q - d/2 \le \tfrac{1}{2}q - \tfrac{1}{2}(d+2),$$

and the second relation implies

$$0 \le d/2 + q(j-j'-d/2) \le \tfrac{1}{2}q - \tfrac{1}{2}(d+2),$$

which is also impossible since $d/2$ is not an integer.

Set $g(X) = f(X)^{(q-1)/2}$. Given $0 \le l < L$ and a polynomial $p(X) \in F[X]$,

$$D^l\{p(X)g(X)\} = \frac{r(X)}{f(X)^l} g(X)$$

for some polynomial $r(X)$ with

$$\deg r(X) \le \deg p(X) + l(d-1).$$

We shall write $D_1^l\{p(X)\} = r(X)$ and $D_0^l\{p(X)\} = f(X)^l D^l\{p(X)\}$. Clearly D_0^l and D_1^l are linear maps $F[X] \to F[X]$ depending on $f(X)$.

Now let us turn to the actual proof of the theorem. Denote by S and S' the number of solutions of $g(x) = 1$ and $g(x) = -1$, respectively. Since for every $x \in F$ either $f(x) = 0$ or $g(x)^2 = \{f(x)\}^{q-1} = 1$, we have

$S+S' \geq q-d$. For a given $x \in F$ there is a $y \in F$ satisfying $y^2 = f(x) \neq 0$ if and only if $f(x)^{(q-1)/2} = g(x) = 1$, and then there are exactly two such values of y. Consequently

$$2S \leq s \leq 2S + d.$$

We shall show that both S and S' are at most $\frac{1}{2}q + 2dq^{1/2} - d$. Then $S \geq q - d - S' \geq \frac{1}{2}q - 2dq^{1/2}$ so

$$q - 4dq^{1/2} \leq s \leq q + 4dq^{1/2} - d,$$

implying the assertion of the theorem. In fact we shall prove the above estimate only for S since the proof for S' is almost identical.

The proof depends on the existence of $2J$ polynomials $p_{jk}(X), 0 \leq j < J, k = 0, 1$, which are not all zero, have degree at most $\frac{1}{2}(q - d - 2)$ and for which each of the L polynomials

$$\Psi_l(X) = \sum_{j=0}^{J-1} [D_0^1\{p_{j0}(X)\} + D_1^l\{p_{j1}(X)\}]X^j, \quad 0 \leq l < L,$$

is zero. Since $\deg \Psi_l(X) \leq \frac{1}{2}(q-d-2) + (L-1)(d-1) + J - 1$, in order to satisfy $\Psi_l(X) = 0$ for each l we have to solve E homogeneous linear equations in the coefficients of the polynomials $p_{jk}(X)$. This is possible since we have $V = \frac{1}{2}(q-d)2J = J(q-d)$ variables [coefficients of the $p_{jk}(X)$] and (13.1) states that $V > E$.

Let us put together the polynomials $p_{jk}(X)$ into a single auxiliary polynomial:

$$\Phi(X) = \sum_{j=0}^{J-1} \sum_{k=0}^{1} p_{jk}(X)X^{qj}g(X)^k.$$

This polynomial $\Phi(X)$ is not zero since all non-zero summands have different degrees. Indeed, if $p_{jk}(X)$ is not the zero polynomial, then

$$A(j,k) \leq \deg\{p_{jk}(X)X^{qj}g(X)^k\} \leq B(j,k),$$

and we know that the intervals $[A(j,k), B(j,k)]$ are disjoint. The most important property of Φ is that $D^l\Phi(x) = 0 (0 \leq l < L)$ for all $x \in F$ satisfying $g(x) = 1$. Indeed, as $D^l\{p(X)X^{qj}\} = X^{qj}D^l\{p(X)\}$, and $x^q = x$ for every $x \in F$, if $g(x) = 1$ we have

$$(D^l\Phi)(x) \;=\; \{f(x)\}^{-l}\sum_{j=0}^{J-1}\{(D_0^l p_{j0})(x) + (D_1^l p_{j1})(x)g(x)\}x^{qj}$$

$$= \{f(x)\}^{-l} \sum_{j=0}^{J-1} \{(D_0^l p_{j0})(x) + (D_1^l p_{j1})(x)\} x^j$$
$$= \{f(x)\}^{-l} \Psi_l(x) = 0.$$

By Lemma 13.1 the polynomial $\Phi(X)$ has a zero of order at least L at each x satisfying $g(x) = 1$, so $SL \leq \deg \Phi \leq \frac{1}{2}(q-d-2)+(J-1)q+d(q-1)/2$. Hence (13.2) implies

$$S \leq q/2 + 2dq^{1/2} - d,$$

as required. □

From now on $F = \mathbb{F}_q$ is taken to be a field of prime power order. Recall that a (multiplicative) *character* of F is a homomorphism from F^*, the multiplicative group of the non-zero elements of F, to the multiplicative group of complex numbers with modulus 1. The identically 1 function is the *principal character* of F and is denoted by χ_0. Since $x^{q-1} = 1$ for every $x \in F^*$ we have $\chi^{q-1} = \chi_0$ for every character χ. A character χ *is of order* d if $\chi^d = \chi_0$ and d is the smallest positive integer with this property. It is customary to extend a character χ to the whole of F by putting $\chi(0) = 0$.

The *quadratic (residue) character* is defined by $\chi(x) = x^{(q-1)/2}$. Equivalently, χ is 1 on squares 0 at 0 and -1 otherwise. Given a polynomial $f(X) \in F[X]$, clearly

$$\sum_{x \in F} \chi(f(x)) = S - S',$$

where S and S' are as in the proof of Theorem 13.2. Therefore, if $f(X)$ has odd degree $m \geq 3$ and $q > 4m^2$ is a prime, then the proof of Theorem 13.2 implies that

$$\left| \sum_{x \in F} \chi(f(x)) \right| = |S - S'| < 4mq^{1/2}. \tag{13.3}$$

In fact, a similar inequality holds for arbitrary characters. Although this result is still considerably less general than the inequality proved by Weil in order to deduce the Riemann hypothesis for curves over finite fields, its proof needs substantially more care, so we shall not give it here. The interested reader may care to consult Schmidt (1976, p. 43).

Theorem 13.3 *Let χ be a character of order $d > 1$. Suppose $f(X) \in F[X]$ has precisely m distinct zeros and it is not a dth power, that is $f(x)$ is not* *the form* $c\{g(X)\}^d$, *where* $c \in F$ *and* $g(X) \in F[X]$. *Then*

$$\left|\sum_{x\in F} \chi(f(x))\right| \le (m-1)q^{1/2}. \qquad \square$$

Another consequence of Weil's theorem concerns the number of roots of polynomials in two variables. For a proof by the Stepanov method see Schmidt (1976, p. 92).

Theorem 13.4 *Suppose* $f(X,Y) \in F[X,Y]$ *is absolutely irreducible (i.e. irreducible over every algebraic extension of* $F = \mathbb{F}_q$*) and has total degree* $d > 0$. *Then the number* s *of solutions* $(x,y) \in F^q$ *of the equation*

$$f(x,y) = 0$$

satisfies

$$|s-q| < \sqrt{2d}^{5/2} q^{1/2} \qquad \square$$

provided $q > 250d^2$.

How can we tell whether a polynomial is absolutely irreducible? Schmidt (1976, p. 92) has the following simple criterion. Let

$$f(X,Y) = g_0Y^d + g_1(X)Y^{d-1} + \ldots + g_d(X),$$

where $g_0 \neq 0$ is constant. If

$$\max_{1\le i\le d}(\deg g_i)/i = m/d \quad \text{and} \quad (m,d) = 1, \tag{13.4}$$

then $f(X,Y)$ is absolutely irreducible.

In addition to the results above, we shall need some basic properties of sums involving a multiplicative and an additive character, especially Gaussian sums. [For an introduction to these sums, see Shapiro (1983).] An *additive character* of the field $F = \mathbb{F}_q$ is a homomorphism of $(F,+)$ into the circle group. The identically 1 function is the *principal additive character*; it is denoted by ψ_0. [Thus $\psi_0(x) = \chi_0(x)$ if $x \neq 0$ but $\psi_0(0) = 1$ and $\chi_0(0) = 0$.] If q is a prime, then the additive characters of $\mathbb{F}_q$ are precisely

$$\psi_a(x) = \mathrm{e}(ax/q), \quad a = 0, 1, \ldots, q-1,$$

where

$$\mathrm{e}(x) = \exp(2\pi i x).$$

We are interested in sums of the form

$$\sum_{x\in F} \chi(f(x))\psi(g(x)), \tag{13.5}$$

where f and g are polynomials, χ is a multiplicative character and ψ is an additive character. For $f(x) = g(x) = x$ the sum above is the *Gaussian sum*

$$G(\chi, \psi) = \sum_{x\in F} \chi(x)\psi(x).$$

In what follows, χ will always stand for a multiplicative character and ψ for an additive character. Note first (Ex. 1) that if $\chi \neq \chi_0$ and $\psi \neq \psi_0$, then

$$\sum_{x\in F} \chi(x) = 0 \quad \text{and} \quad \sum_{x\in F} \psi(x) = 0. \tag{13.6}$$

Also,

$$G(\chi_0, \psi) = 0 \quad \text{if} \quad \psi \neq \psi_0$$

and

$$G(\chi, \psi_0) = 0 \quad \text{if} \quad \chi \neq \chi_0.$$

Furthermore, trivially,

$$G(\chi_0, \psi_0) = q - 1.$$

Lemma 13.5 *If $\chi \neq \chi_0$ and $\psi \neq \psi_0$, then*

$$|G(\chi, \psi)| = q^{1/2}.$$

Proof Since for $y \neq 0$ we have $\overline{\chi(y)} = \{\chi(y)\}^{-1} = \chi(1/y)$ and $\overline{\psi(y)} = \{\psi(y)\}^{-1} = \psi(-y)$,

$$\begin{aligned}
|G(\chi, \psi)|^2 &= \sum_{x}\sum_{y\neq 0} \chi(x)\psi(x)\overline{\chi(y)\psi(y)} \\
&= \sum_{x}\sum_{y\neq 0} \chi(x)\psi(x)\chi(1/y)\psi(-y) \\
&= \sum_{y\neq 0}\sum_{z} \chi(zy)\psi(zy)\chi(1/y)\psi(-y) \\
&= \sum_{z} \chi(z)\sum_{y\neq 0} \psi((z-1)y) = \sum_{z} \chi(z)\sum_{y} \psi((z-1)y) - \sum_{z} \chi(z) \\
&= \sum_{z} \chi(z)\sum_{y} \psi((z-1)y) = q + \sum_{z\neq 1} \chi(z)\sum_{y} \psi((z-1)y) \\
&= q + \sum_{z\neq 1} \chi(z)\sum_{u} \psi(u) = q,
\end{aligned}$$

where in two of the last three steps we used (13.6). □

Our next lemma concerns another special case of the sum in (13.5).

Lemma 13.6 *Suppose q is odd, $\psi \neq \psi_0$ is an additive character and $a, b, c, \in \mathbb{F}_q, a \neq 0$. Then*

$$\left|\sum_{x \in F} \psi(ax^2 + bx + c)\right| = q^{1/2}.$$

Proof Let χ be the quadratic residue character so that for $y \neq 0$ we have $\chi_0(y)+\chi(y) = 2$ if y is a quadratic residue and $\chi_0(y)+\chi(y) = 0$ otherwise. Then

$$\begin{aligned}\sum_x \psi(ax^2) &= \sum_y \psi(ay)\{\chi_0(y) + \chi(y)\} \\ &= \chi(a^{-1})\{G(\chi_0, \psi) + G(\chi, \psi)\} = \chi(a)G(\chi, \psi).\end{aligned}$$

Therefore, by Lemma 13.5,

$$\left|\sum_x \psi(ax^2)\right| = q^{1/2}. \tag{13.7}$$

Finally, (13.7) implies our lemma:

$$\begin{aligned}\left|\sum_x \psi(ax^2 + bx + c)\right| &= \left|\sum_x \psi\left(a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a^2}\right)\right| \\ &= \left|\sum_x \psi\left(a\left(x + \frac{b}{2a}\right)^2\right)\right| = \left|\sum_y \psi(ay^2)\right| = q^{1/2}.\end{aligned}$$

Our last lemma is a slight extension of a lemma in Bollobás (1984*c*). □

Lemma 13.7 *Let $\chi \neq \chi_0$ be a multiplicative character of $\mathbb{F}_q$ and let $U, W \in \mathbb{F}_q$. Then*

$$\left|\sum_{u \in U} \sum_{w \in W} \chi(u - w)\right| \leq \{q|UW|\}^{1/2}.$$

Proof Let ψ be a non-principal additive character. Note first that for $c \in \mathbb{F}_q$ we have

$$\chi(c)G(\bar{\chi}, \psi) = \sum_y \bar{\chi}(y)\psi(cy). \tag{13.8}$$

Indeed, this is immediate for $c = 0$, and if $c \neq 0$, then

$$\sum_x \chi(c)\bar{\chi}(x)\psi(x) = \sum_x \bar{\chi}(x/c)\psi(x) = \sum_y \bar{\chi}(y)\psi(cy).$$

Also, if $T \subset \mathbb{F}_q$, then

$$\begin{aligned}
\sum_x \left|\sum_{t\in T} \psi(tx)\right|^2 &= \sum_x \sum_{t\in T} \psi(tx) \sum_{t'\in T} \bar{\psi}(t'x) \\
&= \sum_x \sum_{t,t'\in T} \psi((t-t')x) = \sum_{t,t'\in T} \sum_x \psi((t-t')x) \\
&= \sum_{t\in T} \sum_x \psi(0) + \sum_{t,t'\in T_{t\neq t'}} \sum_x \psi((t-t')x) = q|T|, \quad (13.9)
\end{aligned}$$

with the last step following from (13.6).

After these preparations, our lemma is easily proved. Indeed, by Lemma 13.5 and (13.8),

$$\begin{aligned}
q^{1/2}\left|\sum_{u\in U}\sum_{w\in W}\chi(u-w)\right| &= \left|G(\bar{\chi},\psi)\sum_{u\in U}\sum_{w\in W}\chi(u-w)\right| \\
&= \left|\sum_{u\in U}\sum_{w\in W}\sum_y \bar{\chi}(y)\psi((u-w)y)\right| \\
&= \left|\sum_y \bar{\chi}(y)\sum_{u\in U}\sum_{w\in W}\psi((u-w)y)\right| \\
&= \left|\sum_y \bar{\chi}(y)\sum_{u\in U}\psi(uy)\sum_{w\in W}\bar{\psi}(wy)\right| \\
&\leq \sum_y \left|\sum_{u\in U}\psi(uy)\right| \left|\sum_{w\in W}\psi(w)\right| \\
&\leq \left\{\sum_y \left|\sum_{u\in U}\psi(uy)\right|^2\right\}^{1/2} \left\{\sum_y \left|\sum_{w\in W}\psi(wy)\right|^2\right\}^{1/2} \\
&= q|U|^{1/2}|W|^{1/2},
\end{aligned}$$

with the penultimate step following from the Cauchy–Schwarz inequality and the last one from (13.9). □

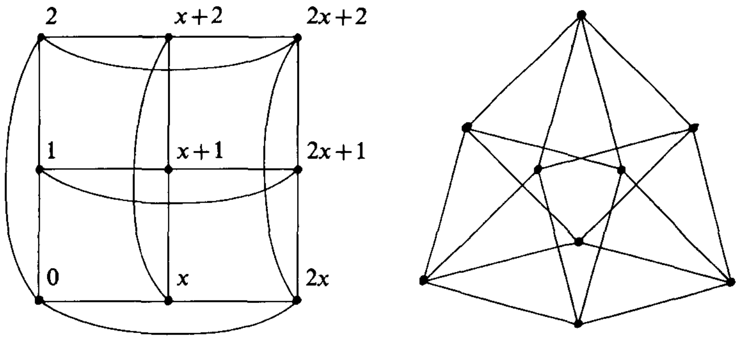


Fig. 13.1. Two drawings of the Paley graph P_9, with $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$.

13.2 The Paley Graph P_q

Let $q \equiv 1 \pmod 4$ be a prime power so that -1 is a square in the field: $\chi(-1) = 1$, where χ is the *quadratic residue character* on $\mathbb{F}_q$, i.e. $\chi(x) = x^{(q-1)/2}$. [If q is a prime, then instead of χ one tends to use the Legendre symbol $\left(\frac{x}{q}\right) = \chi(x)$.] As mentioned in the introduction, the *Paley graph* or *quadratic residue graph* P_q has vertex set $\mathbb{F}_q$ and edge set $\{xy : \chi(x-y) = 1\}$.

The condition $\chi(-1) = 1$ is needed to ensure that xy is defined to be an edge precisely when yx is defined to be an edge. [When deciding on the notation for a Paley graph, we are confronted with the uncomfortable choice of P_q or Q_q. We opted for the first because Q^n will be used for the graph of the n-dimensional cube (Chapter 14) and also because P_q looks more attractive than Q_q. Unfortunately, we shall also discuss the property P_k defined in §2 of Chapter 2, but there seems little danger of mistaking a graph for a property of graphs.] The aim of this section is to show that P_q rather closely resembles a typical graph in $\mathcal{G}(q, \frac{1}{2})$. We start with some properties of P_q which can be read out of the definition.

Theorem 13.8 *The graph P_q is a doubly transitive, self-complementary, strongly regular graph with parameters $\{(q-1)/2, (q-5)/4, (q-1)/4\}$. To spell this out: P_q is $(q-1)/2$-regular, any two adjacent vertices have $(q-5)/4$ common neighbours and any two non-adjacent vertices have $(q-1)/4$ common neighbours. For any two vertices a and b, there are precisely $(q-1)/4$ vertices $c \neq b$ joined to a and not joined to b.*

Proof Multiplication by a quadratic non-residue maps P_q into its complement, so P_q is self-complementary. Given edges uv and $u'v'$, there is a linear function $\phi : \mathbb{F}_q \to \mathbb{F}_q, \phi(x) = ax + b$, mapping u into u' and v into v'. Then $\chi(a) = \chi(a)\chi(u - v) = \chi(a(u - v)) = \chi(u' - v') = 1$, so ϕ gives an isomorphism of P_q into itself, mapping u into u' and v into v'.

Let $x \in V(P_q) = \mathbb{F}_q, U = \Gamma(x), W = V(P_q)\backslash(U \cup \{x\})$ and $q = 4k + 1$. We know that each vertex $y \in U$ is joined to the same number of vertices in W, say l, and also that each vertex $z \in W$ is not joined to precisely l vertices in U. Then

$$|U||W| = (2k)^2 = 2kl + 2kl,$$

so $l = k$. Therefore any two adjacent vertices have $k - 1$ common neighbours and any two non-adjacent vertices have k common neighbours. Since P_q is self-complementary, for any two non-adjacent vertices there are $k-1$ other vertices joined to neither of them, and for any two adjacent vertices there are k vertices joined to neither of them.

Finally, for any two vertices a and b there are $2k$ vertices, distinct from a and b, joined to precisely one of them. Since P_q has an automorphism interchanging a and b, of these $2k$ vertices k are joined to a and not to b, and k are joined to b and not to a. □

If q is a prime power congruent to 3 modulo 4, then the above construction of P_q cannot be carried out. In that case the quadratic residues define the *Paley tournament* or *quadratic residue tournament* $\vec{P}_q$: the vertex set of $\vec{P}_q$ is $\mathbb{F}_q$ and there is an arc (directed edge) from x to y iff $y - x$ is a quadratic residue. In fact, Paley (1933) constructed $\vec{P}_q$ rather than P_q. Paley's main interest in the matter was that $\vec{P}_q$ can be used to construct Hadamard matrices of order $q + 1$.

Let $A = (a_{ij}), i, j \in \mathbb{F}_q$, be the adjacency matrix of $\vec{P}_q : a_{ij} = \chi(j - i), i, j \in \mathbb{F}_q$. Set $B = A - I_q$, where I_q is the $q \times q$ identity matrix and let C be the $(q + 1) \times (q + 1)$ matrix obtained from B by adding to it a row of 1's and a column of 1's. Then the analogue of Theorem 13.8 shows that C is an *Hadamard matrix*: all entries are ± 1 and any two rows (and any two columns) are orthogonal (see also §4 of Chapter 14). Thus, for $q = 3$ the following matrices are obtained (with $+$ and $-$ instead of $+1$ and -1):

$$A = \begin{pmatrix} 0 & + & - \\ - & 0 & + \\ + & - & 0 \end{pmatrix}, B = \begin{pmatrix} - & + & - \\ - & - & + \\ + & - & - \end{pmatrix}, C = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & - & - & + \\ + & + & - & - \end{pmatrix}.$$

The Paley graph P_q can also be used to define a $(q+1) \times (q+1)$ orthogonal matrix which is close to an Hadamard matrix: all entries are ± 1 except for those on the main diagonal, which are 0. Let A be the adjacency matrix of P_q and set $B = 2A - J_q + I_q$ where, as customary, J_q is the $q \times q$ matrix of 1's. Add to B a row and a column, with 1's everywhere except for a 0 in the main diagonal: denote by C this new matrix. Thus for $q = 5$, with the earlier convention and the parentheses omitted, A, B and C are as follows

$$\begin{pmatrix} 0 & + & 0 & 0 & + \\ + & 0 & + & 0 & 0 \\ 0 & + & 0 & + & 0 \\ 0 & 0 & + & 0 & + \\ + & 0 & 0 & + & 0 \end{pmatrix} \begin{pmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{pmatrix} \begin{pmatrix} 0 & + & + & + & + & + \\ + & 0 & + & - & - & + \\ + & + & 0 & + & - & - \\ + & - & + & 0 & + & - \\ + & - & - & + & 0 & + \\ + & + & - & - & + & 0 \end{pmatrix}$$

Then, by Theorem 13.8, C is a symmetric matrix with diagonal entries 0, off-diagonal entries 1 and -1, such that the sum of the entries in each row, except the first one, is 1, and $CC^T = C^2 = qI_{q+1}$.

Theorem 13.8 shows that P_q is similar to a typical element of $\mathscr{G}(q, \frac{1}{2})$ in the sense that the degree of every vertex is about $q/2$ and for any two vertices a and b there are about $q/4$ vertices in each of the following sets: $\{x : xa \in E, xb \in E\}, \{x : xa \in E, xb \notin E\}, \{x : xa \notin E, xb \in E\}, \{x : xa \notin E, xb \notin E\}$, where $E = E(P_q)$ is the edge set of P_q. In fact, this is only the tip of the iceberg: if m is not too large, then for every set M of m vertices and for every partition $M = U \cup W$, about $2^{-m}q$ vertices are joined to all vertices in U and to none in W. The result below claiming this (Theorem 13.10) is from Bollobás and Thomason (1981) and Bollobás (1984*c*); essentially the same result had been proved much earlier by Graham and Spencer (1971).

Lemma 13.9 *Let χ be a non-principal character of $\mathbb{F}_q$ and let U and W be disjoint subsets of $\mathbb{F}_q$. Then*

$$\left| \sum_{x \notin U \cup W} \prod_{u \in U} \{1 + \chi(x-u)\} \prod_{w \in W} \{1 - \chi(x-w)\} - q \right| \le \{(m-2)2^{m-1} + 1\}q^{1/2} + m2^{m-1},$$

where $m = |U| + |W|$ and, as usual, an empty product is defined to be 1.

Proof Clearly

$$
\begin{aligned}
&\left|q - \sum_x \prod_{u\in U}\{1+\chi(x-u)\} \prod_{w\in W}\{1-\chi(x-w)\}\right| \\
&= \left|q - \sum_x \left\{\sum_{Z_1\subset U}\prod_{u\in Z_1}\chi(x-u)\right\}\left\{\sum_{Z_2\subset W}(-1)^{|Z_2|}\prod_{w\in Z_2}\chi(x-w)\right\}\right| \\
&= \left|q - \sum_x \sum_{Z\subset U\cup W}(-1)^{|Z\cap W|}\chi\left(\prod_{z\in Z}(x-z)\right)\right| \\
&= \left|\sum_x \sum_{Z\subset U\cup W_{Z\neq\varnothing}}(-1)^{|Z\cap W|}\chi(P_Z(x))\right| \\
&= \left|\sum_{Z\subset U\cup W_{Z\neq\varnothing}}(-1)^{|Z\cap W|}\sum_x \chi(P_Z(x))\right|,
\end{aligned}
$$

where $P_Z(x)$ denotes the polynomial $\prod_{z\in Z}(x-z)$.

By Theorem 13.3, we have

$$\left|\sum_x \chi(P_Z(x))\right| \le (|Z|-1)q^{1/2}.$$

Hence the sum above is at most

$$\sum_{Z\subset U\cup W_{Z\neq\varnothing}} (|Z|-1)q^{1/2} = (m2^{m-1} - 2^m + 1)q^{1/2}.$$

Finally,

$$\left|\sum_{x\in U\cup W}\prod_{u\in U}\{1+\chi(x-u)\}\prod_{w\in W}\{1-\chi(x-w)\}\right| \le m2^{m-1},$$

so the lemma follows. □

Theorem 13.10 *Let U and W be disjoint sets of vertices of the Paley graph P_q and denote by $v(U,W)$ the number of vertices not in $U\cup W$ joined to each vertex of U and no vertex of W. Then*

$$|v(U,W) - 2^{-m}q| \le \frac{1}{2}(m-2+2^{-m+1})q^{1/2} + m/2.$$

Proof Let χ be the quadratic residue character on $\mathbb{F}_q$: $\chi(x) = x^{(q-1)/2}$.

Then

$$\sum_{x \notin U \cup W} \prod_{u \in U} \{1 + \chi(x - a)\} \prod_{w \in W} \{1 - \chi(x - w)\} = 2^m v(U, W),$$

since a product above is non-zero iff x is joined to every vertex in U and to no vertex in W, in which case it is precisely 2^m. Therefore Lemma 13.9 implies our theorem. □

For brevity, call a graph *r-full* if it contains every graph of order r as an induced subgraph. Furthermore, let us say that a graph G has property $\tilde{P}_k$ if whenever U and W are disjoint sets of vertices of G with $|U| + |W| \leq k$, then $v(U, W) \geq 1$, i.e. G has a vertex not in $U \cup W$ joined to every vertex in U and to none in W. Note that $\tilde{P}_k$ is slightly different from property P_k defined in §2 of Chapter 2: clearly $P_k \to \tilde{P}_k$ and $\tilde{P}_{2k} \to P_k$. It is immediate that if G has $\tilde{P}_r$, then it is $(r + 1)$-full; in fact, every graph of order r can be embedded into G vertex by vertex.

It is easily seen that if $\varepsilon > 0$ and $n = \lceil (\log 2 + \varepsilon) r^2 2^r \rceil$, then a.e. $G_{n,1/2}$ has property $\tilde{P}_r$ and so is $(r + 1)$-full (see Ex. 4). In fact, Bollobás and Thomason (1981) proved that even for $n = \lceil r^2 2^{r/2} \rceil$ a.e. $G_{n,1/2}$ is r-full and so is P_q if q is sufficiently large.

Theorem 13.11 *Let $r \geq 2$ and let $q \equiv 1 \pmod 4$ be a prime power satisfying*

$$q > \{(r - 2)2^{r-1} + 1\} q^{1/2} + r 2^{r-1}. \tag{13.10}$$

Then the graph P_q has property $\tilde{P}_r$ and is $(r + 1)$-full.

In particular, if $q > \{2^{r-1}(r - 1) + 1\}^2$ or $q > r^2 2^{2r-2}$, then the graph P_q has property $\tilde{P}_r$ and is $(r + 1)$-full.

Proof By Theorem 13.10, $v(U, W) > 0$ whenever $|U| + |W| \leq r$. This means precisely that P_q has $\tilde{P}_r$. It is easily checked that $q > \{2^{r-1}(r - 1) + 1\}^2$ implies (13.10). □

As observed by Blass, Exoo and Harary (1981), the proof of Theorem 2.6 implies the following analogue of that result.

Corollary 13.12 *Let P be a property of graphs given by a first order sentence. Then there is a constant q_0 such that either every $P_q, q \geq q_0$, has P or else no P_q, $q \geq q_0$, has P. The first alternative holds if a.e. $G_{n,1/2}$ has P and the second holds if almost no $G_{n,1/2}$ has P.*

Let us turn to another striking property of P_q, showing that P_q is rather similar to a typical element of $\mathcal{G}(q, \frac{1}{2})$. Given disjoint sets of vertices U and W, denote by $e(U)$ the number of edges joining vertices in U and write $e(U, W)$ for the number of $U - W$ edges. We know from Theorems 2.8 and 2.11 that a.e. $G_{n,1/2}$ is such that if U and W are not too small, then $e(U)$ is close to $|U|^2/4$ and $e(U, W)$ is close to $|UW|/2$. The next result, essentially from Bollobás (1984*c*), shows that P_q has a similar property.

Theorem 13.13 *Let U and W be disjoint sets of vertices of the Paley graph P_q. Then*

$$\left|e(U) - \frac{1}{2}\binom{|U|}{2}\right| \le \frac{1}{4}|U|q^{1/2}$$

and

$$\left|e(U, W) - \frac{1}{2}|UW|\right| \le \frac{1}{2}|U|^{1/2}|W|^{1/2}q^{1/2}.$$

Proof Writing χ for the quadratic residue character, clearly

$$\left|\sum_{u,w\in U}\sum \chi(u-w)\right| = \left|2e(U) - 2\left\{\binom{|U|}{2} - e(U)\right\}\right| = \left|4e(U) - 2\binom{|U|}{2}\right|$$

and

$$\begin{aligned}\left|\sum_{u\in U}\sum_{w\in W}\chi(u-w)\right| &= |e(U,W) - (|U||W| - e(U,W))| \\ &= |2e(U,W)| - |U||W|.\end{aligned}$$

By Lemma 13.7, the first expression is at most $|U|_q^{1/2}$ and the second is at most $|U|^{1/2}|W|^{1/2}q^{1/2}$. □

All our results so far concern the existence of many vertices and edges of one kind or another. However, r.gs are used not only because they contain many subgraphs of various kinds, but also because they do not contain certain subgraphs. Thus, as a.e. $G_{n,1/2}$ has fairly small clique number, in Chapter 12 we could use it to give lower bounds for Ramsey numbers. Do Paley graphs give us good lower bounds for Ramsey numbers? In other words, do Paley graphs have small clique numbers?

On examining P_q for some small values of q, we are greatly encouraged. Thus P_5 (which happens to be the pentagon C^5) is triangle-free so shows

$R(3) \geq 5+1 = 6$, which is best possible; and P_{17} has clique number 3, so proves $R(4) \geq 17+1 = 18$, which is also best possible. It is not unreasonable, therefore, to have high hopes of the applicability of Paley graphs in Ramsey theory. Unfortunately, our high hopes are dashed by the bleak reality; as we shall see below, for a general q the Paley graph P_q cannot be guaranteed to have a small clique number.

However, let us see first a promising consequence of Theorem 13.13. Let U be the vertex set of a complete subgraph of P_q, with $u = |U| = \mathrm{cl}(P_q)$. Then, by Theorem 13.13,

$$e(U) - \frac{1}{2}\binom{u}{2} \leq \frac{1}{4} u q^{1/2}$$

so

$$\mathrm{cl}(P_q) = u \leq q^{1/2} + 1. \tag{13.11}$$

Unfortunately, Theorem 13.13 and inequality (13.11) are not nearly as deep as they seem for, as shown by Thomason (1983), the elementary Theorem 13.8, whose proof made no use of Weil's theorem for curves over finite fields, implies slightly better bounds.

Theorem 13.14 *Let U be a set of u vertices of the Paley graph P_q. Then*

$$\left| e(U) - \frac{1}{2}\binom{u}{2} \right| \leq \frac{u}{4} \frac{q-u}{\sqrt{q}}.$$

Furthermore,

$$cl(P_q) \leq \sqrt{q}.$$

Proof We may assume that $0 < u < q$. Let $d = 2e(U)/u$ be the average degree in the graph $G[U]$ and denote by $n(U)$ the number of unordered pairs of neighbouring edges (ac, bc) with $a, b \in U$. By Theorem 13.8, for each pair (a, b) of adjacent vertices of U there are $(q-5)/4$ such pairs and for each pair (a, b) of non-adjacent vertices there are $(q-1)/4$ such pairs. Hence

$$n(U) = e(U)(q-5)/4 + \left\{ \binom{cu}{2} - e(U) \right\} (q-1)/4 = \binom{cu}{2} (q-1)/4 - e(U).$$

On the other hand, there are $u[\{(q-1)/2\} - d]$ edges joining U to $V-U$ so, on average, a vertex of U is joined to d vertices in U, and a vertex in $V-U$ is joined to $d_0 = \{u/(q-u)\}[\{(q-1)/2\} - d]$ vertices in

U. Therefore

$$n(U) \geq u\binom{cd}{2} + (q-u)\binom{cd_0}{2},$$

implying

$$\frac{ud(d-1)}{2} + \frac{u}{2}\left(\frac{q-1}{2} - d\right)\left\{\frac{u}{q-u}\left(\frac{q-1}{2} - d\right) - 1\right\} \leq \frac{u(u-1)(q-1)}{8} - \frac{du}{2}.$$

Multiplying by $u(q-u)/(2q)$ and rearranging, we find that

$$\left\{\frac{du}{2} - \frac{1}{2}\binom{cu}{2}\right\}^2 \leq \frac{u^2}{16q}(u-q)^2,$$

which is precisely the first inequality to be proved.

To see the assertion about the clique number, note that if U spans a complete subgraph of P_q and $|U| = u$, then

$$e(U) - \frac{1}{2}\binom{cu}{2} = \frac{1}{2}\binom{cu}{2} \leq \frac{u}{4}\frac{q-u}{\sqrt{q}}$$

and so $u \leq \sqrt{q}$. □

Can we do better than Theorem 13.14? Not too easily. In fact, for a general prime power $q \equiv 1 \pmod 4$ Theorem 13.14 is best possible: if $q = p^2$ for some odd prime p and F_0 is the prime field of $\mathbb{F}_q$ then every element of F_0 is a square. Hence F_0 spans a complete subgraph of P_q and so $\mathrm{cl}(P_q) \geq p = q^{1/2}$. This shows that if we want P_q to have a small clique number, then q had better be a prime. Furthermore, even when q is a prime, $\mathrm{cl}(P_q)$ cannot be shown to be small by the use of general character sum estimates, for those estimates would give a proof in the case q is a square.

Suppose then that q is a prime, $q \equiv 1 \pmod 4$. Write $n(q)$ for the least natural number which is not a quadratic residue modulo q. Then the set $\{1, 2, \ldots, n(q)\}$ spans a complete subgraph of P_q, so

$$n(q) \leq \mathrm{cl}(P_q).$$

The function $n(q)$ (to be precise, its analogue for a general character χ of $\mathbb{F}_q$) has been studied extensively; for an excellent survey see Montgomery (1971, chapter 13). Extending results of Pólya (1918) and Vinogradov

(1918), Burgess (1957, 1962, 1963) proved that if $\varepsilon > 0$ and q is sufficiently large, then

$$n(q) \le q^{1/\sqrt{16e+\varepsilon}}.$$

Assuming the Riemann hypothesis for all L-functions of real characters, Ankeny (1952) improved this considerably:

$$n(q) = O\{(\log q)^2\}. \tag{13.12}$$

The original proof of (13.12) was rather involved; Montgomery (1971, chapter 13) gave a simpler proof of an extension of (13.12). Furthermore, Montgomery showed that if the Riemann hypothesis is true for all L-functions of real characters, then for some $\varepsilon > 0$ there are infinitely many primes q satisfying

$$n(q) > \varepsilon(\log q)(\log\log q). \tag{13.13}$$

It may be that (13.13) is more-or-less best possible, i.e. (13.12) can be improved to $n(q) = O((\log q)(\log\log q))$. This would be true if, as seems to be the case, for a large fixed prime q and small primes p the values $\left(\frac{p}{q}\right)$ would behave like independent Bernoulli r.vs. For when does $n(q) > x$ hold? If $\left(\frac{p}{q}\right) = 1$ for every prime $p, 2 \le p \le x$. Since there are about $x/\log x$ primes up to x, assuming independence, $n(q) > x$ holds with probability about $2^{-x/\log x}$.

If $\varepsilon > 0$ and $x > (1+\varepsilon)(\log_2 q)(\log\log q)$, then this probability is at most $q^{-1-\varepsilon'}$ for some $\varepsilon' > 0$ and large enough q. As $\sum_q q^{-1-\varepsilon'} < \infty$, by the Borel-Cantelli lemma, if q is sufficiently large, $n(q) \le (1+\varepsilon)(\log_2 q)(\log\log q)$.

In conclusion, (13.13) does dash our hopes of using Paley graphs to obtain a good general bound for Ramsey numbers. Nevertheless, it seems likely that for sporadic values of q the graphs give even better lower bounds for Ramsey numbers than do our random graphs.

13.3 Dense Graphs

In this section we shall construct several graphs resembling typical r.gs with fairly many edges, i.e. resembling typical elements of $\mathcal{G}(n, M)$ for M rather large. By imitating the proof of Theorem 13.14, one can show that a graph G satisfying $|G| = n$ and $e(G) = M \sim cn^2, 0 < c < \frac{1}{2}$, is such that $e(U)$ is about $M\binom{u}{2}/\binom{n}{2}$ for all u-sets U if u is not too small, provided $\delta(G)$ is not much smaller than $2M/n$, the average degree, and no two vertices have substantially more than $2M^2/n$ neighbours, which is about the expected number in $G_{n,M}$. Thus, to show a fair resemblance to a typical element of $\mathscr{G}(n,M)$, it suffices to prove that all degrees are about the same and all pairs of vertices have about the same number of common neighbours.

Let us start with natural generalizations of Paley graphs: Cayley graphs. Given a group H and a set X of generators of H, the *Cayley graph* $\vec{G}(H,X)$ is a directed multigraph with vertex set H in which there is an arc (directed edge) from a to b if $a^{-1}b \in X$. [The assumption that X is a set of generators is not very important and we usually ignore it; if X does not happen to be a set of generators then $\vec{G}(H,X)$ falls into isomorphic components, with each component being isomorphic to a Cayley graph of a subgroup of H.] With a slight abuse of terminology, the graph obtained from $\vec{G}(H,X)$ by forgetting the orientation and multiplicity of edges is also called a *Cayley graph* and is denoted by $G(H,X)$. There seems to be little harm in this ambiguity; in fact, usually we choose X to be self-inverse: $X = X^{-1} = \{x^{-1} : x \in X\}$ in which case $\vec{G}(H,X)$ is obtained from $G(H,X)$ by replacing each edge ab by the arcs $\vec{ab}$ and $\vec{ba}$. Clearly the Paley graph P_q is a Cayley graph: $P_q = G\{(\mathbb{F}_q,+),Q_q\}$, where Q_q is the set of non-zero squares in $\mathbb{F}_q$.

Cayley graphs give us many new models of random graphs. For example, given a sequence of groups $H_1,H_2,\ldots$, with H_n having order $2k_n+1, k_n \to \infty$, and $r_n \in \mathbb{N}$, we may define $\mathscr{G}(H_n,r_n)$ as the set of all Cayley graphs $G(H_n,X_n)$ with X_n running through all self-inverse sets of $2r_n$ elements. Thus $\mathscr{G}(H_n,r_n)$ consists of $\binom{k_n}{r_n}$ $2r_n$-regular graphs of order $2k_n+1$.

In a rather vague sense, it is clear that 'most' elements of 'most' of the spaces $\mathscr{G}(H_n,r_n)$ resemble appropriate typical (more conventional) r.gs. Our problem is, then, to choose a particular Cayley graph that we can prove to be similar to an r.g.

As a slight generalization of P_q, we can choose q and d such that q is a prime power, $d \ge 2, d$ divides $q-1$ and $-1 \in X_q = \{x^d : x \in \mathbb{F}_q, x \neq 0\}$ and then take $G\{(\mathbb{F}_q,+),X_q\}$. As another variant, we can take q and d as above, pick a subset Y_q of $\mathbb{F}_q$ and define $X_q = \{x : x^d \in Y_q, x \neq 0\}$. Methods analogous to those in §2 can be used to show that, under certain conditions, these graphs do resemble typical r.gs in $\mathscr{G}(n,p)$ for constant p.

How can we define concrete *r.gs* which are slightly less dense? Instead of $\mathbb{F}_q$, let us take $\mathbb{F}_p = \mathbb{Z}_p$ for some prime p and let $t \in \mathbb{N}, 2 \le t < p$. Let $Q(p,t)$ be the graph with vertex set $\mathbb{F}_p$ and edges set

$$\{uv : \{(u-v)^2/p\} \le t/p\},$$

where $\{x\} = x - \lfloor x \rfloor$ is the *fractional part* of x. Clearly $Q(p,t) = G\{(\mathbb{F}_q,+), X_p\}$ where $X_p = \{x : x^2 \in Y_p\}, Y_p = \{1,2,\ldots,t\}$. We shall show that a weak variant of Theorem 13.10 holds for $Q(p,t)$. First we need a simple lemma.

Let $f : \mathbb{Z}_p \to \mathbb{R}$ be defined by

$$f(s) = \begin{cases} 1, & \text{if } 0 < \{s/p\} \le t/p, \\ 0, & \text{otherwise,} \end{cases}$$

and let $(c_j)_0^{p-1}$ be the Fourier coefficients of f:

$$f(s) = \sum_{j=0}^{p-1} c_j e(sj/p) = \sum_{j=0}^{p-1} c_j \mathrm{e}^{2\pi isj/p}.$$

Thus

$$c_j = \frac{1}{p}\sum_{s=1}^{t} e(-sj/p),$$

in particular, $c_0 = t/p$.

Lemma 13.15 *If $p \ge 3$, then*

$$\sum_{j=1}^{p-1} |c_j| < \log p.$$

Proof Clearly

$$\begin{aligned}
\sum_{j=1}^{p-1} |c_j| &= \frac{1}{p}\sum_{j=1}^{p-1}\left|\sum_{s=1}^{t} e(-sj/p)\right| = \frac{2}{p}\sum_{j=1}^{(p-1)/2}\left|\sum_{s=1}^{t} e(js/p)\right| \\
&= \frac{2}{p}\sum_{j=1}^{(p-1)/2}\left|\frac{1-e(jt/p)}{1-e(j/p)}\right| \le \frac{4}{p}\sum_{j=1}^{(p-1)/2}\frac{1}{|1-e(j/p)|} \\
&\le \frac{4}{p}\sum_{j=1}^{(p-1)/2}\frac{1}{4j/p} = \sum_{j=1}^{(p-1)/2}\frac{1}{j} < \log p
\end{aligned}$$

since

$$|1 - e(j/p)| = |1 - \mathrm{e}^{2\pi ij/p}| \ge \frac{4j}{p}.$$

if $0 \le j \le p/2$. □

For large values of p, Lemma 13.15 is easily improved (see Ex. 9).

Theorem 13.16 *Let U and W be disjoint sets of vertices of $Q(p,t)$ and denote by $v(U,W)$ the number of vertices not in $U \cup W$ joined to each vertex in U and none in W. If $|U|+|W|=2$, then*

$$\left| v(U,W) - \left(\frac{t}{p}\right)^{|U|}\left(\frac{p-t}{p}\right)^{|W|} p \right| < p^{1/2}(\log p)^2.$$

Proof Let us consider the case $U=\{u,v\}$, $W=\emptyset$; the other cases being similar (see Ex. 10). Let f be as above, so that

$$\begin{aligned} u(U,\emptyset) &= \sum_{r=0}^{p-1} f\{(u-r)^2\} f\{(v-r)^2\} \\ &= \sum_{r=0}^{p-1}\sum_{j,k} c_j c_k e\{(u-r)^2 j/p\} e\{(v-r)^2 k/p\} \\ &= pc_0^2 + \sum_{(j,k)\neq(0,0)} c_j c_k \sum_{r=0}^{p-1} e\{(u-r)^2 j/p + (v-r)^2 k/p\} \\ &= pc_0^2 + R, \end{aligned}$$

say. Since $\psi(x) = e(x/p)$ is an additive character of $\mathbb{F}_p$, by (13.6) and Lemma 13.6 we have

$$\left|\sum_{r=0}^{p-1} e\{(u-r)^2 j/p + (v-r)^2 k/p\}\right| = \left|\sum_{r=0}^{p-1} \psi((j+k)r^2 + 2(ju+kv)r)\right| \le p^{1/2}.$$

Hence

$$|R| \le \sum_{j,k} |c_j c_k| p^{1/2} < p^{1/2}(\log p)^2,$$

with the second inequality following from Lemma 13.15. As $c_0 = t/p$, this proves our theorem. □

Needless to say, Theorem 13.16 is a very poor relation of Theorem 13.10; it would be good to remedy this situation.

A universal version of the graph $Q(p,t)$ was constructed by Bollobás and Erdős (1975), who also conjectured that the analogue of Theorem 13.16 holds for this graph. A proof of this conjecture, based on classical results of Hardy and Littlewood (1914, 1925), was given recently by Pinch (1985). Let α be irrational, $0 < \delta < 1$ and $n \in \mathbb{N}$. Denote by $R(n,\alpha,\delta)$ the graph with vertex set $V = \{1,2,\dots,n\}$ and edge set $\{ij : 1 \le i < j \le n, \{(i-j)^2\alpha\} < \delta\}$.

Theorem 13.17 *For every irrational α there is a function $f_\alpha : \mathbb{N} \to \mathbb{N}$ such that $f_\alpha(n) = o(n)$ and*

$$|v(n,\delta;i,j) - \delta^2 n| \le f_\alpha(n)$$

for all $0 < \delta < 1$ and $1 \le i < j \le n$, where $v(n,\delta;i,j)$ denotes the number of common neighbours of i and j in $R(n,\alpha,\delta)$.

For $r \in \mathbb{N}$, Bollobás and Thomason (1981) constructed the following very simple graph P of order 2^r. The vertex set of P is the power set $\mathscr{P}(X)$ of $X = \{1,2,\dots,r\}$, and two vertices, $A, B \in \mathscr{P}(X)$ are joined if either $|A \cap B|$ is even and $|A||B| > 0$ or $|A| + |B|$ is even and $|A||B| = 0$. This graph P is rather close to being strongly regular: every vertex has degree $2^{r-1} - 1$, every edge is in $2^{r-2} - 2$ or $2^{r-2} - 1$ triangles and in the complement every edge is in $2^{r-2} - 1$ or 2^{r-2} triangles. Furthermore, the following easy result shows that P has an important property of a typical r.g. $G_{1/2}$ (see Ex. 11).

Theorem 13.18 *The graph P is r-full.* □

Many other graphs can be obtained by elaborating on this construction. For example, given natural numbers r, s, t and i, with $r > s > t \ge i$, let $P(r,s,t,i)$ have vertex set $X^{(s)}$, the collection of s-subsets of $X = \{1,2,\dots,r\}$ and edge set $\{AB : |A \cap B| \equiv i (\text{mod } t)\}$. If t is fixed and $r, s \to \infty$ such that $s/r \to c, 0 < c < 1$, then $P(r,s,t,i)$ resembles a typical $G_{1/t}$.

Finite geometries were used to construct graphs well before it was realized that, in some sense, they imitate r.gs. The so called *problem of Zarankiewicz* asks for the maximal number of edges in a graph of given order or in a bipartite graph with given classes, provided the graph does not contain $K(s,t)$, a complete s by t bipartite graph. In order to give lower bounds for this value, Reiman (1958), Erdős and Rényi (1962) and W. G. Brown (1966) constructed graphs from finite geometries [see Bollobás (1978*a*, chapter 4.§2) for numerous results connected with the problem of Zarankiewicz, including the constructions].

Consider $PG(r,q)$, the r-dimensional projective geometry over the field $\mathbb{F}_q$, where q is a prime power. (In fact, we could take any r-dimensional projective geometry of order q, but as we are concerned with constructions, it is better to take those which are easy to describe.) Denote by $V_i(r,q)$ the set of i-dimensional spaces: $V_0(r,q)$ is the set of points, $V_1(r,q)$

is the set of lines, etc. Note that

$$v_i(r,q) = |V_i(r,q)| = \prod_{j=0}^{i} \frac{q^{r+1-j}-1}{q^{1+j}-1}.$$

For $0 \leq k < l \leq r-1$ let $G(r,q,k,l)$ be the bipartite graph with bipartition $\{V_k(r,q), V_l(r,q)\}$, with $A \in V_k(r,q)$ adjacent to $B \in V_l(r,q)$ if B contains A. Reiman (1958) was the first to consider a graph $G(r,q,k,l)$, namely $G = G(r,q,0,1)$, in connection with the problem of Zarankiewicz for $K(2,2)$. Clearly G is an m by n bipartite graph of girth 6 with $m = v_0(r,q), n = v_1(r,q)$; furthermore, it has the maximal number of edges among all m by n bipartite graphs without a quadrilateral.

The graphs $G(r,q,0,r-1)$ were considered recently by Alon (1985), who showed that they resemble a typical G_p in the sense that most subsets of vertices have 'many' neighbours (see Theorem 2.15 and Theorem 13.10). Graphs in which all subsets of vertices of certain sizes have 'many' neighbours are usually called *expanders*. There are a good many different definitions in use, some of which will be discussed here and in §4. Call a graph (a,b)*-expanding* if for any set A of a vertices.

$$|A \cup \Gamma(A)| \geq a + b, \tag{13.14}$$

i.e. if A has at least b neighbours not in A. Similarly, a bipartite graph is said to be (a,b)-expanding if (13.14) holds whenever A is a subset of one of the vertex classes. [In that case, (13.14) is equivalent to $|\Gamma(A)| \geq b$.]

Tanner (1985) showed that the expansion properties of a graph are related to the eigenvalues of various matrices associated with the graph; this connection was further exploited by Alon and Milman (1984, 1985) and then Alon (1985) proved the following theorem. The result also follows from an argument along the lines of the proof of Theorem 13.14.

Theorem 13.19 *Let q be a prime power, $r \in \mathbb{N}, n = (q^{r+1}-1)/(q-1)$ and $k = (q^r-1)/(q-1)$. Then the n by n bipartite graph $G(r,q,0,r-1)$, constructed from the projective geometry $PG(r,q)$, is k-regular and $(a, n - n^{1+1/r}/a)$-expanding for all a, $1 \leq a \leq n$.*

A generalization of $G(r,q,k,l)$ is $G(r,q,k,l,m)$, the bipartite graph with bipartition $\{V_k(r,q), V_l(r,q)\}$, in which $A \in V_k(r,q)$ is adjacent to $B \in V_l(r,q)$ if $\dim A \cap B \geq m$.

As pointed out by Erdős, Rényi and Sós (1966) and W. G. Brown (1966), the following graph $G_0(q)$ constructed by Erdős and Rényi (1962) gives a very good lower bound for the maximal number of edges in a quadrilateral-free graph of order $n = q^2 + q + 1$, where q is an odd prime power. The vertex set of $G_0(q)$ is $V_0(2,q)$ and a point $(a,b,c) \in V_0(2,q)$ is joined to another point (α,β,γ) if

$$a\alpha + b\beta + c\gamma = 0.$$

In other words, two points of $PG(2,q)$ are adjacent if one is on the polar of the other with respect to the conic $x^2 + y^2 + z^2 = 0$. This shows that a point not on this conic has degree $q + 1$, and each of the $q + 1$ points of the conic has degree q. Furthermore, $G_0(q)$ does not contain a quadrilateral since any two lines of $PG(2,q)$ meet in one point only so every vertex of $G_0(q)$ is determined by any two of its neighbours.

Another important property of $G_0(q)$ is that the diameter is 2: this follows from the fact that any two lines of $PG(2,q)$ intersect. In fact, not only is the diameter 2, but also any two points have a common neighbour, unless the line through the points is the polar of one of the points. Hence no triangle contains any of the $q + 1$ points of the conic, but every other point is in some edge-disjoint triangles.

As an application of Theorem 13.19, Alon (1985) showed that $G_0(q)$ gives a good lower bound for the generalized Ramsey number $r(C^4, K^s) = \min\{n :$ every graph of order n without a quadrilateral contains s independent vertices$\}$.

Theorem 13.20 *(i) Let q be a prime power, $n = q^2+q+1$ and $s = 2\lfloor n^{3/4} \rfloor$. Then $r(C^4, K^s) > n$.*

(ii) There is a constant $c > 0$ such that $r(C^4, K^s) > cs^{4/3}$ for all s.

Proof (i) Let $G = G_0(q)$. We know that G contains no quadrilaterals. Consider a set of $a = \lfloor n^{3/4} \rfloor = s/2$ vertices of G_0. By Theorem 13.19, the a polars of these a points of $PG(2,q)$ contain at least $n - n^{3/2}/a \geq n - n^{3/4}$ points. Hence there are at most $\lfloor n^{3/4} \rfloor$ points independent of our a points. Consequently, $\beta_0\{G_0(q)\} \leq a + \lfloor n^{3/4} \rfloor < s$.

(ii) This follows from (i) and from any of the classical theorems about the distributions of primes, say from the fact that if n is sufficiently large then there is a prime between n and $n + n^{2/3}$ [see Montgomery (1971, Chapter 14) or Bollobás (1978*a*, p. xx)]. □

Numerous other graphs can be constructed with the use of finite geometries and polynomials. One of these was used by Brown (1966) to give a good lower bound for $z(n, 3)$, the maximal number of edges in an n by n bipartite graph which does not contain $K(3,3)$. To construct this graph, take a prime power $q, q \equiv 3 \pmod 4$, say, and consider the affine geometry $AG(3, q)$. Let V_1 and V_2 be two copies of the q^3 points of $AG(3,q)$, and join a point (a, b, c) in V_1 to a point (α, β, γ) in V_2 if $a\alpha + b\beta + c\gamma = 1$. This q^3 by q^3 bipartite graph has $q^5 - q^4$ edges, and one can show that it does not contain a $K(3,3)$. Hence $z(q^3, 3) \geq q^5 - q^4$.

To conclude this section, we discuss briefly another generalization of Paley graphs, the so-called conference graphs, already encountered in §4 of Chapter 9, introduced by Belevitch (1950). Let us recall the definition: a graph of order n is said to be a *conference graph* if it is $(n-1)/2$-regular and for any two vertices there are precisely $(n-1)/2$ vertices in different relation to these vertices. Equivalently, both the graph and its complement are $(n-1)/2$-regular graphs in which every edge is in precisely $(n-5)/4$ triangles. Clearly a conference graph of order n is a strongly regular graph with parameters $\{(n-1)/2, (n-5)/4, (n-1)/4\}$ (see Biggs, 1974). If A is the adjacency matrix of a conference graph, then, putting $B = 2A - J_n + I_n$ and $C = \begin{pmatrix} 0 & j_n^T \\ j_n & B \end{pmatrix}$, as in the discussion following Theorem 13.8, with $j_n^T = (1, 1, \ldots, 1)$, the $(n+1) \times (n+1)$ matrix C is such that the diagonal entries are 0, the off-diagonal ones ± 1 and $CC^T = C^2 = nI_{n+1}$. The matrices satisfying these conditions are called *conference matrices*. It is easily seen that every conference matrices gives rise to at least one conference graph (and, possibly, to several). Conference graphs are precisely the graphs whose local asymmetry $A^*(G)$ is equal to the obvious upper bound in terms of the order (Theorem 9.12). Erdős and Rényi (1963) called them Δ graphs and wondered whether all Δ graphs were symmetric. At the time this did not seem preposterous, for the Paley graphs were the only examples of conference graphs and the Paley graphs have transitive automorphism groups. The order n of a conference graph must be a sum of two integer squares, as shown by van Lint and Seidel (1966) but, thanks to Mathon (1978), now it is known that n need not be a prime power.

In fact, conference graphs are probably not too rare. For an odd prime power q, construct a graph Q_q by taking $\mathbb{F}_q^2$ as the vertex set, selecting a set of $(q+1)/2$ lines (i.e. 1-dimensional subspaces) and joining x to y iff $x - y$ lies on one of our lines. (Needless to say, Q_q is a Cayley graph on the additive group $\mathbb{F}_q^2$.) This construction is due to Delsarte and Goethals and to Turyn (see Seidel, 1976). Further constructions are due to Goethals and Seidel (1967, 1970), Turyn (1971) and Mathon (1978); see also Thomason (1979) for several results proving similarities between random graphs and conference graphs.

Mathon (1978) was the first to construct conference graphs with trivial automorphism groups: 1152 of the 1504 conference graphs of order 45 constructed by Mathon have trivial automorphism groups. There is little doubt that many of these graphs have degree of asymmetry 22 and so show $A(45) = 22$; and it seems very likely that $A(n) = (n-1)/2$ infinitely often.

13.4 Sparse Graphs

In this section we shall concentrate on expanding bipartite graphs of bounded degree, i.e. on bipartite graphs which expand in the sense that every not too large subset of one of the classes (or both classes) has many neighbours. Let us start with a result of Chung (1978) showing the existence of such graphs by random graph methods. For $0 < x < 1$ let

$$H(x) = -x \log x - (1-x)\log(1-x)$$

be the *entropy function.*

Theorem 13.21 *Let a, b, c be natural numbers, $3 \le b \le a$, and let $0 < \alpha < 1$ be such that*

$$\frac{H(\alpha) + (b/a)H(a\alpha/b)}{bH(\alpha) - \alpha a H(b/a)} < c, \ \alpha < \frac{b(b-2)}{ab-a-b} \quad \text{and} \quad 4 < bc.$$

Then, if n is sufficiently large, there is a bipartite graph G with bipartition (U, W) such that

$$|U| = an, \quad |W| = bn,$$
$$d(u) = bc \text{ for } u \in U, \quad d(w) = ac \text{ for } w \in W$$

and if $D \subset U, |D| \le \alpha an$, then G contains a complete matching from D into W.

Proof Given a natural number n, consider the space $\mathcal{G}$ of random bipartite graphs with bipartition (U, W), such that $|U| = an, |W| = bn, d(u) = bc$ for $u \in U$ and $d(w) = ac$ for $w \in W$. All we have to show is that if n is sufficiently large then the probability that $G \in \mathcal{G}$ has the required property is positive. In fact, as expected, as $n \to \infty$, a.e. $G \in \mathcal{G}$ has the required properties.

To show this, let us generate our r.gs as we generated random graphs in §4 of Chapter 2: replace each $u \in U$ by a set X_u of bc elements and each $w \in W$ by a set Y_w of ac elements, set $X = \bigcup_{u \in U} X_u$, $Y = \bigcup_{w \in W} Y_w$, take a random matching from X into Y and, finally, by identifying the elements in each set X_u and in each set Y_w, collapse this matching to a bipartite multigraph with bipartition (U, W). Keep only those multigraphs which are, in fact, graphs.

By Exercise 12 the probability that our multigraph is a graph tends to $e^{-(ac-1)(bc-1)/2}$, so it suffices to prove that a.e. multigraph has the required property. Now if a multigraph is such that for some set $D \subset U$, $d = |D| \le \alpha an$, it fails to contain a complete matching from D into W, then by Hall's theorem there is a set $D' \subset W$, —$D'| = d$ (we are a little generous here!) such that $\Gamma(D) \subset D'$. The probability of this is clearly at most

$$S(d) = \binom{can}{d}\binom{cbn}{d}(dac)_{dbc}(abcn - bcd)!/(abcn)!.$$

With a little work one can check that the conditions imply $\sum_{d \le \alpha an} S(d) = o(1)$. $\square$

An *n by m expander graph with parameters* (λ, α, r) is a bipartite graph of maximal degree r, with bipartition $(U, W), |U| = n, |W| = m$, such that if $D \subset U$ and $|D| \le \alpha n$ or $D \subset W$ and $|D| \le \alpha m$, then $|\Gamma(D)| \ge \lambda |D|$. A proof similar to the one above shows that there is an ample supply of expander graphs.

Theorem 13.22 *Let $0 < \alpha < 1/\lambda < \lambda$ and $r \in \mathbb{N}$ be such that*

$$\alpha^{-(\lambda+1)\alpha}(1-\alpha)^{-(1-\alpha)}(1-\lambda\alpha)^{-(1-\lambda\alpha)} < \{\alpha^{-\alpha}(1-\alpha)^{-(1-\alpha)}(\lambda-1)^{(\lambda-1)\alpha}\}^r.$$

Then for every fixed k and sufficiently large n there is an n by $n+k$ expander graph with parameters (λ, α, r). $\square$

Corollary 13.23 *If $0 < \alpha < 1/\lambda < \lambda$ and k is a non-negative integer, then there is an r such that for every sufficiently large n there is an n by $n+k$ expander graph with parameters (λ, α, r).* $\square$

Although expanders are easily shown to exist, they are rather difficult to construct, so it was a real breakthrough when Margulis (1973) gave an explicit construction for an infinite family of expander graphs. It is easily seen that small sets are more likely to expand than large ones so it makes sense to take this into account when defining expanders. Thus to state the result of Margulis, it is natural to define an *(n, r, λ)-expander* as an n by n bipartite graph of maximal degree at most r, with bipartition

(U, W) such that if $D \subset U$ and $|D| \le n/\lambda$, then

$$|\Gamma(D)| \ge \{1 + \lambda(1 - |D|/n)\}|D|.$$

Theorem 13.24 *For $n \ge 4$, let U and W be two disjoint copies of $\mathbb{Z}_m \times \mathbb{Z}_m$ and define a bipartite graph G_m with bipartition (U, W) by joining $(x, y) \in U$ to $(x, y), (x+1, y), (x, y+1), (x, x+y)$ and $(-y, x)$ in W. Then G_m is an $(m^2, 5, \lambda)$-expander for some absolute constant $\lambda > 0$.* □

The proof given by Margulis, based on representation theory, is most ingenious but, unfortunately, it does not yield a lower bound on λ although, in fact, λ is likely to be fairly large (see also C. Angluin, 1979). Gabber and Galil (1979) altered slightly the graph constructed by Margulis, and used elegant methods of functional analysis to show that the λ belonging to the new graph is indeed rather large.

Theorem 13.25 *For $n \ge 4$, let U and W be disjoint copies of $\mathbb{Z}_m \times \mathbb{Z}_m$ and define a bipartite graph $\widetilde{G}_m$ with bipartition (U, W) by joining $(x, y) \in U$ to $(x, y), (x, x+y), (x, x+y+1), (x+y, y), (x+y+1, y)$ in W. Then $\widetilde{G}_m$ is an $(m^2, 5, \lambda_0)$-expander for $\lambda_0 = (2 - \sqrt{3})/4 = 0.183\ldots$.* □

Gabber and Galil (1979) constructed another variant of the graphs above which they proved to be an $(m^2, 7, 2\lambda_0)$-expander. All of these graphs were defined by a finite family $F = \{f_1, f_2, \ldots, f_r\}$ of linear functions $f_i : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \times \mathbb{Z}_m$ by joining (x, y) in one copy of $\mathbb{Z}_m \times \mathbb{Z}_m$ to $f_i(x, y)$ in the other copy. This gives rise to the natural question whether an analogue of Margulis' construction could be carried out with the use of a finite set of one-dimensional linear functions $f_i : \mathbb{Z}_m \to \mathbb{Z}_m$. Unfortunately, the answer is in the negative: Klawe (1981) proved that if F is any finite set of one-dimensional linear functions with rational coefficients and G_n is the n by n graph defined by F in the obvious way, then for every $\lambda > 0$ there is an n_0 such that for $n \ge n_0$ the graph G_n is not an $(n, |F|, \lambda)$-expander.

As we shall see in Chapter 15, expander graphs play an important role in the design of sorting algorithms. Furthermore, expander graphs are often used as building blocks of many other constructions, including concentrators, superconcentrators, nonblocking connectors and generalized connectors (see Abelson, 1979; Alon, 1985; Alon and Milman, 1985; Bassalygo and Pinsker, 1973; Chung, 1978; Ja'Ja, 1980; Lengauer and Tarjan, 1982; Paul, Tarjan and Celoni, 1977; Pippenger, 1977, 1978, 1982; Shamir, 1985; Tompa, 1980; Valiant, 1975, 1976). For example, an *n-superconcentrator* is a graph containing two disjoint sets of n vertices each, say U and W, such that for any pair of subsets $D \subset U$ and $D' \subset W$, with $|D| = |D'| = d$, the graph contains d vertex disjoint paths starting in D and ending in D'. Valiant (1975*a*) showed the existence of directed acyclic n-superconcentrators with at most $238n$ edges; Pippenger (1977) proved that about $39n$ edges suffice and F. R. K. Chung (1978) decreased this further to about $36n$. For lack of space we do not go into the details.

To conclude this chapter, we present another sparse graph somewhat resembling a r.g. This is the 4-regular graph $M(4,p)$ constructed by Margulis (1982) as an example of a 4-regular graph of large girth and small order (see Bollobás, 1986, §3).

Let $p \geq 5$ be a prime. Consider $SL_2(\mathbb{Z})$ and $SL_2(\mathbb{Z}_p)$, the multiplicative groups of unimodular 2 by 2 matrices with entries from $\mathbb{Z}$ and $\mathbb{Z}_p$, respectively. The map $\mathbb{Z} \to \mathbb{Z}_p$, given by $a \to a(\mathrm{mod}\ p)$, induces a homomorphism $\phi_p : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}_p)$. Note that $SL_2(\mathbb{Z}_p)$ has $p(p^2-1)$ elements since it contains $p^2(p-1)$ matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a \neq 0$ and $p(p-1)$ matrices with $a = 0$.

Let $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ and set $A_p = \phi_p(A), B_p = \phi_p(B)$. The *Margulis graph* $M(4,p)$ is the Cayley graph over $SL_2(\mathbb{Z}_p)$ with respect to the set $\{A_p, B_p, A_p^{-1}, B_p^{-1}\}$, i.e. $M(4,p)$ has vertex set $SL_2(\mathbb{Z}_p)$ and edge set

$$\{(C,D) : C, D \in SL_2(\mathbb{Z}_p) \text{ and } C^{-1}D \in \{A_p, B_p, A_p^{-1}, B_p^{-1}\}\}.$$

Since $A^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$, $B^{-1} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$ and $p \geq 5$, the set $\{A_p, B_p, A_p^{-1}, B_p^{-1}\}$ has four elements and so $M(4,p)$ is 4-regular.

The main property of $M(4,p)$, proved by Margulis (1982), is that if $p > 2(1+\sqrt{2})^k$ then the girth is at least $2k+1$.

Theorem 13.26 *Let $\alpha = 1 + \sqrt{2}, k \in \mathbb{N}$ and let p be a prime greater than $2\alpha^k$. Then the Margulis graph $M(4,p)$ is a 4-regular graph of order $p(p^2-1)$ and girth at least $2k+1$.*

13.5 Pseudorandom Graphs

In the previous sections we constructed numerous graphs that have many of the properties we usually associate with random graphs. Thomason (1987*a*) was the first to look for a criterion by which to decide whether a *given* graph behaves like a random graph, and to this end introduced the concept of a jumbled graph.

For $0 < p < 1 \leq \alpha$ a graph G is called *(p,α)-jumbled* if every induced subgraph H of G satisfies

$$|e(H) - p\binom{c|H|}{2}| \leq \alpha|H|.$$

Equivalently, if $d(H) = 2e(H)/|H|$ is the average degree in H then G is (p,α)-jumbled if for every induced subgraph H we have

$$|d(H) - p(|H|-1)| \leq 2\alpha.$$

Note that if G is (p,α)-jumbled than its complement $\overline{G}$ is $(1-p,\alpha)$-jumbled. Trivially, if G is (p,α)-jumbled then its independence number is at most $1 + 2\alpha/p$ and its clique number is at most $1 + 2\alpha/(1-p)$. If $pn \to \infty$ and $(1-p)n \to \infty$ then almost every $G_p \in \mathscr{G}(n,p)$ is $(p, 2(pn)^{1/2})$-jumbled—with plenty to spare.

In the definition of being jumbled, in spite of the lost example, p does not denote a probability, but merely a number. However, this number does play a role similar to the probability of an edge of G_p; in fact, one frequently takes $p = e(G)/\binom{n}{2}$ for a jumbled graph of order n.

Clearly every graph G of order n is $(p, n/2)$-jumbled, so the property of being (p,α)-jumbled start, to be interesting only when α is smaller than $n/2$. In fact, as shown by Theorem 12.18 of Erdős and Spencer (1972) (and Bollobás and Scott (2001)), if a graph of order n is (p,α)-jumbled then α is at least of order $(pn)^{1/2}$. Thus in the most restrictive case we may take α to be of order $(pn)^{1/2}$.

Thomason (1987*a*, *b*, 1989*b*) proved a variety of conditions that imply that some graph is jumbled with a certain choice of parameters. The easy result below gives a simple *local* sufficient condition for being jumbled.

Theorem 13.27 *Let G be a graph of order n, with minimal degree pn. If no pair of vertices has more than $p^2n + l$ common neighbours, where $l \geq 1$, then G is $(p, ((p+l)n)^{1/2}/2)$-jumbled.*

Proof Let H be an induced subgraph of G of order $k < n$, with average degree d. Let $v_1, \ldots, v_n$ be the vertices of G, with $v_1, \ldots, v_k$ in H, and write d_i for the number of neighbours of v_i in H. Then

$$\sum_{i=1}^{k} d_i = kd$$

and

$$\sum_{j=k+1}^{n} d_j \geq \sum_{i=1}^{k}(pn - d_i) = k(pn - d).$$

Since no two vertices have more than $p^2n + l$ common neighbours,

$$\sum_{i=1}^{n} d_i \leq \binom{ck}{2}(p^2n + l)$$

so, by the convexity of the function $\binom{x}{2}$,

$$k\binom{cd}{2} + (n-k)\binom{ck(pn-d)/(n-k)}{2} \leq \binom{ck}{2}(p^2n + l).$$

This is equivalent to

$$(d - pk)^2 \leq \frac{n-k}{n}((k-1)l + p(1-p)n),$$

which implies that

$$|d - p(k-1)| \leq ((p + l)n)^{1/2},$$

as claimed. In fact, the same inequality holds when $k = n$ and so $H = G$. □

Thomason (1987a) showed also that certain simple *global* conditions may also imply that a graph is jumbled.

Theorem 13.28 *Let $0 < p < 1$ and let h, m and n be positive integers with $2 \leq h \leq n - 2$. Let G be a graph such that for every induced subgraph H of G with h vertices we have*

$$\left| e(H) - p\binom{h}{2} \right| \leq m.$$

Then

$$|e(H) - p\binom{|H|}{2}| \leq 80\ m\ \eta^{-2}(1-\eta)^{-2}$$

for every induced subgraph H of G, where $\eta = h/n$. □

It is easily seen that under the conditions of Theorem 13.27, almost all k-sets of vertices have about p^kn neighbours, and for most choices of disjoint sets of vertices A and B, with $|A| = \alpha$ and $|B| = b$, we have about the 'right' number of vertices, namely about $p^a(1-p)^bn$, joined to every vertex in A and no vertex in B.

As the following theorem of Thomason shows, jumbled graphs also contain about the right number of copies of a fixed graph. Given graphs G and H, we write $N^*_G(H)$ for the number of labelled occurrences of H as an induced subgraph of G. For later use, we write $N_G(H)$ for the number of labelled occurrences of H as a not necessarily induced subgraph of G. Thus, if $G = H$ is a t-cycle C_t then $N^*_G(H) = N_G(H) = 2t$, while if G is the complete graph K_n then for $t \geq 4$ we have $N^*_G(C_t) = 0$ and $N_G(C_t) = (n)_4$.

Theorem 13.29 *Let H be a graph of order $h \geq 3$ with m edges, and let G be a (p, α)-jumbled graph of order n, where $p \leq 1/2$. Furthermore, suppose that $\varepsilon^2 p^h n \geq 42\, \alpha h^2$, where $0 < \varepsilon < 1$. Then*

$$(1-\varepsilon)^h p^m (1-p)^{\binom{h}{2}-m} n^h \leq N^*_G(H) \leq (1+\varepsilon)^h p^m (1-p)^{\binom{h}{2}-m} n^h. \qquad \square$$

Chung, Graham and Wilson (1989) initiated the study of a different class of graphs resembling random graphs. They imposed less stringent conditions on the graphs, and their main aim was to prove that a great variety of conditions give the same class of graphs. They called the graphs in this class *quasi-random.*

Strictly speaking, Chung, Graham and Wilson (1989) defined properties of *sequences* $\hat{G} = (G_n)$ of graphs, where G_n has n vertices. Here are the seven properties of $\hat{G} = (G_n)$ they introduced to model a sequence $(G_{n,p})$ with $p = 1/2$.

1. For $s \geq 1, P_1(s)$ is the property that for every graph H with s vertices we have
$$N^*_{G_n}(H) = (1+o(1))n^s 2^{-\binom{s}{2}}.$$
2. For $t \geq 3, P_2(t)$ is the property that $e(G_n) \geq (1+o(1))n^2/4$ and
$$N_G(C_t) \leq (1+o(1)) \left(\frac{n}{2}\right)^t.$$
3. A sequence $\hat{G} = (G_n)$ has property P_3 if $e(G_n) \geq (1+o(1))n^2/4$ and $\lambda_1 = (1+o(1))n/2$, $\lambda_2 = o(n)$, where $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of (the adjacency matrix of) G_n, with $|\lambda_1| \geq \ldots \geq |\lambda_n|$.
4. Property P_4 holds if
$$e(G_n[S]) = \tfrac{1}{4}|S|^2 + o(n^2)$$
for every subset S of $V(G_n)$.
5. Property P_5 is defined as P_4, except the condition is demanded only for sets S with $|S| = \lfloor n/2 \rfloor$.

6. For vertices u and v of G_n, let $a_n(u,v)$ be the number of vertices joined either to *both* u and v or to *neither*. Then P_6 is the property that

$$\sum_{u,v \in V(G_n)} \left| a_n(u,v) - \frac{n}{2} \right| = o(n^3).$$

7. For vertices u and v of G_n, let $b_n(u,v)$ be the number of vertices joined to *both* u and v, i.e., the number of common neighbours. Then P_7 is the property that

$$\sum_{u,v \in V(G_n)} \left| b_n(u,v) - \frac{n}{4} \right| = o(n^3).$$

Here is then the theorem of Chung, Graham and Wilson (1989) concerning these properties.

Theorem 13.30 *For $j \geq 4$ and $t \geq 4$ even, all the properties $P_1(s), P_2(t)$, $P_3, \ldots, P_7$ are equivalent.* □

Although some of the implications, like $P_1(s) \Rightarrow P_2(s)$ and $P_4 \Rightarrow P_5$, are immediate, and some others are fairly easy, much work is needed to prove the equivalence of all the properties. In particular, it is surprising that condition $P_2(4)$ is so strong, although it looks rather weak.

A graph G_n is said to be *quasi-random* if its natural sequence (G_n) satisfies any (and so all) the properties in Theorem 13.30. Clearly, one could easily define quasi-random graphs 'imitating' the properties of $G_{n,p}$ for any constant p, not only for $p = 1/2$. In this way we obtain quasi-random graphs of density p. Chung and graham (1989, 1990, 1991a,b) went considerably further: in addition to quasi-random graphs, they studied quasi-random hypergraphs, set systems and tournaments as well.

Simonovits and Sós (1991) brought to light the following fascinating connection between quasi-random graphs and Szemerédi's lemma : if a graph is quasi-random than in every Szemerédi partition all pairs are regular with density $1/2$ and, conversely, if a graph has a Szemerédi partition in which almost all pairs are regular with density $1/2$ then the graph is quasi-random. An unexpected bonus of this is that if a graph has a Szemerédi partition in which almost all pairs have density $1/2$ then there are no exceptional pairs.

It is easily shown that if $N_{G_n}(H) = (1 + o(1))n^h p^{e(H)}$ for *all* graphs H of order h, where $0 < p < 1$ is fixed, than G_n is quasi-random of density p. It would be tempting to conjecture that if $N_{G_n}(H) = (1 + o(1))n^h p^{e(H)}$ for a not too exceptional graph H of order h then G_n is quasi-random. In fact, this is for from being the case. Nevertheless, Simonovits and

Sós (1997) proved the beautiful result that quasi-randomness *is* implied by the condition that for *every* induced subgraph F of G_n we have $N_F(H) = |F|^h p^{e(H)} + o(n^{|H|})$. The proof of this result also makes use of Szemerédi's lemma. It is remarkable that the analogue of this result for induced subgraphs is false.

Exercises

13.1 Prove that if χ is a non-principal multiplicative character of $F = \mathbb{F}_q$ and ψ is a non-principal additive character, then

$$\sum_{x\in F} \chi(x) = 0 \quad \text{and} \quad \sum_{x\in F} \psi(x) = 0.$$

[Note that if $x_1 \neq 0$, then $\sum_x \chi(x) = \sum_x \chi(xx_1) = \chi(x_1)\sum_x \chi(x)$.]

13.2 Prove that if p is a prime, χ is a non-principal character of $F = \mathbb{F}_p = \{0, 1, \ldots, p-1\}$ and $1 \leq s \leq p-1$, then

$$\left|\sum_{c=1}^{s} \chi(c)\right| \leq p^{1/2} \log p.$$

[By Lemma 13.5 and relation (13.8), with $\psi(x) = e(x/p)$ we have

$$\begin{aligned} p^{1/2}\left|\sum_{c=1}^{s} \chi(c)\right| &= \left|G(\bar{\chi}, \psi)\sum_{c=1}^{s} \chi(c)\right| = \left|\sum_{c=1}^{s}\sum_{y\in F} \bar{\chi}(y)\psi(cy)\right| \\ &= \left|\sum_{y=1}^{p-1} \bar{\chi}(y)\sum_{c=1}^{s} e(cy/p)\right| \leq \sum_{y=1}^{q-1}\left|\sum_{c=1}^{s} e(cy/p)\right|. \end{aligned}$$

Apply Lemma 13.15 or an inequality from the proof of Lemma 13.15.]

13.3 Let $q \equiv 3 \pmod 4$ be a prime power. Show that the matrix C obtained from the Paley tournament $\vec{P}_q$, described after Theorem 13.8, is an Hadamard matrix.

13.4 Show that if $\varepsilon > 0$ is fixed and $n = \lceil(\log 2 + \varepsilon)r^2 2^r\rceil$ then a.e. $G_{n,1/2}$ has $\tilde{P}_r$ and so is $(r+1)$-full. [Let U and W be disjoint sets of vertices with $|U| + |W| = r$. The probability that no vertex will do for this pair (U, W) is $(1-2^{-r})^{n-r}$. Check that $\binom{n}{r} 2^r (1-2^{-r})^{n-r} \to 0$.]

13.5 Deduce from Corollary 13.12 that the following properties are not first order properties: (i) self-complementarity, (ii) regularity,

(iii) being Eulerian, (iv) being asymmetric. (Blass, Exoo and Harary, 1981.)

13.6 A tournament T is *r-full* if it contains every tournament of order r as a subtournament, and it has property $\tilde{P}_r$ if for disjoint sets of vertices U and W with $|U|+|W| = r$ there is a vertex dominating every vertex in U and dominated by every vertex in W. Show that if T has $\tilde{P}_r$ then it is $(r+1)$-full. Analogously to Ex. 4, prove that if $\varepsilon > 0$ and $n = \lceil(\log 2 + \varepsilon)r^2 2^r\rceil$, then a.e. tournament of order n has $\tilde{P}_r$. [Erdős (1963*b*), answering a problem of Schutte.]

13.7 Show that if T is a tournament of order n in which every set of at most r vertices is dominated by some vertex (in particular, if T has $\tilde{P}_r$), then $n \geq (r+2)2^{r-1} - 1$. (E. Szekeres and G. Szekeres, 1965.)

13.8 Deduce from Theorem 13.10 the analogue of Theorem 13.11: if $r \geq 2, q \equiv 3 \pmod 4$ is a prime power and $q > \{(r-2)2^{r-1} + 1\}q^{1/2} + r2^{r-1}$, then the Paley tournament $\vec{P}_q$ has $\tilde{P}_r$ and is $(r+1)$-full. (Graham and Spencer, 1971.)

13.9 Prove the following strengthening of Lemma 13.15 for large values of p: if $\varepsilon > 0$ and p is sufficiently large, then $\sum_{j=1}^{p-1} |c_j| < (2/\pi + \varepsilon)\log p$.

13.10 Define $g : \mathbb{Z}_p = \{0, 1, \dots, p-1\} \to \mathbb{R}$ by

$$g(s) = \begin{cases} 1, & \text{if } t/p < \{s/p\}, \\ 0, & \text{otherwise.} \end{cases}$$

Note that in $Q(p,t)$ we have

$$v(U,W) = \sum_{r=0}^{p-1} \prod_{u \in U} f\{(u-r)^2\} \prod_{w \in W} g\{(w-r)^2\}.$$

Use this to prove the remaining case of Theorem 13.17.

13.11 Prove Theorem 13.18. (Bollobás and Thomason, 1981.)

13.12 Let $G_k = P(k,3,3,1)$ be as defined after Theorem 13.18: the vertex set is $V_k = W_k^{(3)}$, where $W_k = \{1, 2, \dots, k\}$, and the edge set is $\{AB : A, B \in V_k, |A \cap B| = 1\}$. Note that if $\{A_1, \dots, A_l\} \subset V_k, l \geq 5$, spans a complete subgraph and $|\bigcap_1^4 A_i| = 1$, then $|\bigcap_1^l A_i| = 1$, and if $\{B_1, \dots, B_l\} \subset V_k$ is an independent set with $B_i \cap B_{i+1} \neq \emptyset, i = 1, \dots, l-1$, then $|\bigcap_1^l B_i| = 2$. Deduce that for $k \geq 18$ we have $\mathrm{cl}(G_k) = \lfloor (k-1)/2 \rfloor$ and $\mathrm{cl}(\bar{G}_k) \leq k$, with equality if $k \equiv 0 \pmod 4$. Thus G_k shows that $R(\lfloor (k+1)/2 \rfloor, k+1) \geq \binom{k}{3} + 1$. (Nagy, 1972.)

14

Sequences, Matrices and Permutations

Given a natural number n, denote by Q^n the graph whose vertices are all the 0–1 sequences $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ of length n and in which two sequences (i.e. vertices of Q^n) are adjacent iff they differ in exactly one member. Equivalently, $V(Q^n) = \{0, \ldots, 2^n - 1\}$ and i is joined to j if, when written in binary form, they differ in precisely one digit. We call Q^n the *n-dimensional cube* or simply *n-cube*. Clearly Q^n is an n-regular, n-connected bipartite graph of order 2^n.

In §1 we shall study the space $\mathscr{G}(Q^n; p)$ of random subgraphs of Q^n, an example of the probability space introduced in §1 of Chapter 2. Thus, to obtain a random element Q^n_p of $\mathscr{G}(Q^n; p)$, we delete the edges of Q^n with probability $q = 1 - p$, independently of each other. For what values of p is Q^n_p likely to be connected? As we shall see, the critical value of p is $\frac{1}{2}$, and the main obstruction to connectedness is the existence of isolated vertices.

Let $x_1, x_2, \ldots, x_n$ be random vertices of Q^n and consider each x_i as a vector in $\mathbb{R}^n$. What is the probability that these n (not necessarily distinct) vectors are linearly independent? As one would expect, this probability tends to 0 as $n \to \infty$; however, the proof, due to Komlós (1967, 1968) is surprisingly difficult. Later Komlós (1981) extended his own theorem: he showed that the probability is $O(n^{-1/2})$; our main aim in §2 is to prove this result. It is fascinating that the proof is based on a lemma of Littlewood and Offord (1938), which was also the starting point of the study of random polynomials by Littlewood and Offord, mentioned in the Preface.

The problem to be discussed in §3 seems to have nothing to do with the n-cube but, on closer examination, it reduces to a question concerning subsets of vertices of the n-cube. Given finite sets $S_1, \ldots, S_n$, split $\bigcup_{i=1}^n S_i$ into two sets, say R and B, such that each set S_i has about as many elements in R as in B. How good a splitting can we choose?

The problem can also be formulated in terms of bipartite graphs: given an n by m bipartite graph with bipartition (U, W), split W into two sets, say R and B, such that each of the n vertices of U is joined to about as many vertices in R as in B.

In §3 we shall present a beautiful theorem of Spencer (1981) about the existence of good splittings. The ingenious proof uses probabilistic arguments; among others, it makes use of the symmetric group, as a probability space.

In §4 we glance at random permutations and random elements of other finite groups. Although the topic is definitely not part of the theory of random graphs, there are several reasons for a very brief discussion of the area in this chapter. The asymmetric group was among the first combinatorial objects studied by probabilistic methods, there is a tangible kinship between results concerning random elements of groups and many of the theorems appearing in this book, and often the methods are similar to those we have been using.

Finally, §5 is about random mappings of a finite set into itself.

14.1 Random Subgraphs of the Cube

Given $p = p(n)$, what is the probability that Q_p^n, a random subgraph of the n-cube Q^n, is connected? Burtin (1977) was the first to study this question. He proved that the critical value of p is $\frac{1}{2}$: for a fixed value of p, a.e. Q_p^n is disconnected if $p < \frac{1}{2}$, and a.e. Q_p^n is connected if $p > \frac{1}{2}$. This result corresponds to the fact that if $p = p(n) = c \log n/n$ for some constant $c > 0$, then for $c < 1$ a.e. $G_{n,p}$ is disconnected and for $c > 1$ a.e. $G_{n,p}$ is connected.

Burtin's result was extended by Erdős and Spencer (1979); they proved that there is a curious double jump at $p = \frac{1}{2}$: the probability of $Q_{1/2}^n$ being connected tends to e^{-1}. This is reminiscent of the double jump discovered by Erdős and Rényi in the growth of the giant component of $G_{n,p}$ at $p = 1/n$ and, even more, of the fact that the probability of $G_{n,\log n/n}$ being connected tends to e^{-1}. As we saw in Chapters 6 and 7, both these double jumps are simply due to our rather crude point of view: by changing p at an appropriate rate we obtain continuous probability distributions. The aim of this section is to present this result, due to Bollobás (1983*b*).

The basis of the study of Q_p^n is an isoperimetric inequality in Q_p^n. What is an isoperimetric inequality in a graph G? An inequality relating a subgraph to its boundary. There are several variants of the boundary of a subgraph; we shall consider only the one we shall need here. For an induced subgraph H of G, write $b_G(H)$ for the number of edges of G joining H to the vertices not in H. Thus $b_G(H)$ is the number of edges in the *edge-boundary* or simply *boundary* of H. An *isoperimetric inequality* is a lower bound on $b_G(H)$ in terms of the order of H. Thus a best possible isoperimetric inequality is an explicit expression for

$$b_G(k) = \min\{b_G(H) : H \subset G, |H| = k\}.$$

In determining the probability of a graph in $\mathscr{G}(G;p)$ being connected, the function $b_G(k)$ is of great importance. Indeed, if G has at most $c_G(k)$ connected induced subgraphs of order k and for some $k_0 = k_0(n)$ we have

$$\sum_{k=k_0}^{\lfloor n/2 \rfloor} c_G(k)(1-p)^{b_G(k)} = o(1)$$

then almost no graph in $\mathscr{G}(G;p)$ has a component whose order is between k_0 and $n/2$. Hence, within probability $o(1)$, our random graph is connected iff it contains no component of order less than k_0. In the proof of the main theorem (Theorem 14.3) this idea will be applied with $k_0 = 2$.

Let us see then the isoperimetric inequality in the cube Q^n, proved by Hart (1976). Related results had been obtained earlier by Harper (1964, 1966*a,b*) and Bernstein (1967). Since Q^n is n-regular, for an induced subgraph $H \subset Q^n$ of order k one has

$$b_{Q^n}(H) = kn - 2e(H).$$

Therefore

$$b_{Q^n}(k) = kn - 2e_n(k),$$

where

$$e_n(k) = \max\{e(H) : H \subset Q^n, |H| = k\}.$$

Denote by $h(i)$ the sum of digits in the binary expansion of i, and set

$$f(l, l+k) = \sum_{i=l}^{l+k-1} h(i)$$

and

$$f_*(k) = f(0,k).$$

The following theorem of Harper, Bernstein and Hart solves the isoperimetric problem in the cube Q^n.

Theorem 14.1

$$e_n(k) = f_*(k) \text{ and } b_{Q^n}(k) = kn - 2f_*(k).$$

Proof Let us prepare the ground by examining the function $f(l, l+k)$. Note that

$$h(i) + h(2^r - 1 - i) = r$$

for all $i, 0 \leq i \leq 2^r - 1$, and so

$$f(l, l+k) + f(2^r - l - k, 2^r - l) = rk \tag{14.1}$$

whenever $l+k \leq 2^r$. Furthermore, for each $j \geq 1$, in the binary expansions of the numbers $0, 1, 2, \ldots$ the jth digit is 2^j times 0, then 2^j times 1, etc., Hence the sum of the jth digits of $l, l+1, \ldots, l+k-1$ is minimal if the first block of 0's is as long as possible. Therefore

$$f(l, l+k) \geq f_*(k) \tag{14.2}$$

for all $l \geq 0$ and

$$f(l, l+k) \geq f(2^r, 2^r + k) = f_*(k) + k \tag{14.3}$$

whenever $k \leq 2^r \leq l$.

Relations (14.1) and (14.2) imply that

$$f(l, l+k) \leq f(2^r - k, 2^r) \tag{14.4}$$

if $k + l \leq 2^r$.

Let us show by induction on k that (14.3) holds without the assumption $l \geq 2^r$, i.e.

$$f(l, l+k) \geq f_*(k) + k \tag{14.5}$$

whenever $k \leq l$. This is clear for $k = 1$, so let us turn to the induction step. Let $2^{r-1} \leq k < 2^r$. By (14.3) we may assume that $l < 2^r$. Then by (14.1), (14.3) and the induction hypothesis we have

$$\begin{aligned}
f(l, l+k) &= f(l, 2^r) + f(2^r, l+k) \\
&\geq \{(2^r - l)r - f_*(2^r - l)\} + \{f_*(l + k - 2^r) + l + k - 2^r\} \\
&\geq \{(2^r - l)r - f(2^r - k, 2^r - k + 2^r - l) + 2^r - l\} \\
&\qquad + f_*(l + k - 2^r) + l + k - 2^r \\
&= f(l + k - 2^r, k) + f_*(l + k - 2^r) + k = f_*(k) + k.
\end{aligned}$$

The penultimate equality followed from (14.1) since $2^{r+1} - k - l < 2^r$. This completes the proof of (14.5).

At last we are ready to prove Theorem 14.1. We know that the two equalities are equivalent; we shall prove $e_n(k) = f_*(k)$. As the set $S = \{0, 1, \ldots, k-1\}$ spans precisely $f_*(k)$ edges, $e_n(k) \geq f_*(k)$, so all we have to prove is that $e_n(k) \leq f_*(k)$.

Let us apply induction on n. The case $n = 1$ is trivial, so all we need is the induction step. Split Q^n into two $(n-1)$-dimensional cubes. Let S be a k-subset of $V(Q^n)$ with k_1 vertices in the first cube and $k_2 \geq k_1$ vertices in the second. Every vertex of the first cube is joined to exactly one vertex of the second cube, so by the induction hypothesis the number of edges spanned by S is at most

$$f_*(k_1) + f_*(k_2) + k_1 = f_*(k) - f(k_2, k_2 + k_1) + f_*(k_1) + k_1.$$

By inequality (14.5) this expression is at most $f_*(k)$. □

Corollary 14.2 *For all k and n we have*

$$e_n(k) \leq (k/2)\lceil \log_2 k \rceil$$

and

$$b_{Q^n}(k) \geq k(n - \lceil \log_2 k \rceil).$$

Proof Let $r = \lceil \log_2 k \rceil$. Then by (14.2) and (14.1) we have

$$2f_*(k) \leq f_*(k) + f(2^r - k, 2^r) = rk$$

so

$$e_n(k) = f_*(k) \leq rk/2.$$ □

Now we are ready to prove the main result of the section.

Theorem 14.3 *Let $\lambda > 0$ be a constant and let*

$$p = p(n) = 1 - \frac{1}{2}\lambda^{1/n}\{1 + o(1/n)\} = 1 - \frac{1}{2}\{\lambda + o(1)\}^{1/n}.$$

Then

$$\lim_{n\to\infty} P(Q_p^n \text{ is connected}) = e^{-\lambda}.$$

Proof Denote by $X = X(Q_p^n)$ the number of isolated vertices in Q_p^n. We show first that $X \xrightarrow{d} P_\lambda$ and so, in particular,

$$\lim_{n\to\infty} P(Q_p^n \text{ has no isolated vertex}) = e^{-\lambda}. \tag{14.6}$$

By Theorem 1.20, it suffices to show that for every fixed $r \geq 0$, the rth factorial moment of X tends to λ^r. Counting very crudely indeed, a set of r vertices is incident with at least $r(n-r)$ edges and at most rn edges. Furthermore, there are at most

$$\binom{2^n}{r-1} rn$$

sets of r vertices incident with fewer than rn edges. Hence

$$(2^n)_r q^{rn} \leq E_r(X) \leq (2^n)_r q^{rn} + 2^{n(r-1)} rnq^{r(n-r)}.$$

This gives

$$(2q)^{rn}(1 - r^2/2^n) \leq E_r(X) \leq (2q)^{rn}\{1 + 2^{-n} rnq^{-r^2}\}.$$

The condition on p is equivalent to

$$\lim_{n\to\infty} (2q)^n = \lambda,$$

so $E_r(X) \to \lambda^r$. Hence $X \xrightarrow{d} P_\lambda$, and so (14.6) does hold.

Now we turn to the essential part of the proof. We shall show that almost no Q_p^n contains a component with at least 2 and at most 2^{n-1} vertices. This is equivalent to the statement that the probability that Q_p^n is disconnected and contains no isolated vertex tends to 0. Therefore' the theorem then follows from (14.6).

In fact, we shall prove somewhat more than we have just claimed. Let $\mathscr{C}_s$ be the family of s-subsets of $V = V(Q^n)$ spanning connected subgraphs of Q^n. If Q_p^n contains a component of order s, then the vertex set S of this component belongs to $\mathscr{C}_s$ and Q_p^n contains a spanning tree of $Q^n[S]$. We shall be rather generous on two counts: we shall not use the existence of a spanning tree and we shall replace p by a smaller probability. □

Lemma 14.4 *Let $p = 1 - \frac{1}{2}(\log n)^{1/n}$. Then the probability that for some $S \in \mathscr{C}_s, 2 \leq s \leq 2^{n-1}$, no edge of Q_p^n joins S to $V \backslash S$ tends to 0.*

Proof Recall that our interest in edge boundaries of subgraphs of Q^n stemmed precisely from their use in proving the non-existence of certain components. Given a set $S \subset V$, set $b(S) = b_{Q^n}(H)$, where $H = Q^n[S]$. Then the lemma follows if we show that

$$\sum_{s=2}^{2^{n-1}} \sum_{S \in \mathscr{C}_s} q^{b(S)} = o(1) \tag{14.7}$$

where $q = 1 - p$. By Corollary 14.2, for $|S| = s$ we have

$$b(S) \geq b(s) = s(n - \lceil \log_2 s \rceil),$$

and so

$$\sum_{S \in \mathscr{C}_s} q^{b(S)} \leq |\mathscr{C}_s| q^{b(s)}.$$

In order to prove (14.7) we partition the ranges of the summations into several parts.

(i) Set $s_1 = \lfloor 2^{n/2}/n^2 \rfloor$ and suppose that $2 \leq s \leq s_1$, Our first estimate is very crude:

$$|\mathscr{C}_s| \leq 2^n n(2n) \ldots \{(s-1)n\} = (s-1)! n^{s-1} 2^n.$$

Hence

$$|\mathscr{C}_s| q^{b(s)} \leq (s-1)! n^{s-1} 2^n q^{s(n - \lceil \log_2 s \rceil)}.$$

Since $q^n = 2^{-n} \log n$, this gives

$$|\mathscr{C}_s| q^{b(s)} \leq s! n^{s-1} 2^n 2^{-sn} S^s (\log n)^s.$$

Take the logarithm of $ns^s/s!$ times the right-hand side:

$$2s \log_2 s + s \log_2 n - (s-1)n + s \log_2 \log n.$$

If n is sufficiently large, this expression is at most 0 for every s in our range. This is perhaps easiest seen by considering $s \leq n$ and $s \geq n$ separately. Hence

$$|\mathscr{C}_s| q^{b(S)} \leq s!/ns^s$$

and so

$$\sum_{s=2}^{s_1} \sum_{S \in \mathscr{C}_s} q^{b(s)} = o(1).$$

Let us turn to the range $s_1 < s \leq 2^{n-1}$. Here we shall partition $\mathscr{C}_s$ into two sets. Let $\mathscr{C}_s^-$ consist of those sets S in $\mathscr{C}_s$ for which

$$b(S) \geq s(n - \log_2 s + \log_2 n),$$

and set $\mathscr{C}_s^+ = C_s \backslash C_s^-$. We shall make use of the facts that (i) if $S \in \mathscr{C}_s^-$ then the boundary $b(S)$ is large enough to make $q^{b(S)}$ very small and (ii) most elements of $\mathscr{C}_s$ belong to $\mathscr{C}_s^-$.

(ii) Let us estimate our double sum in the range $s_1 + 1 \le s \le 2^{n-1}$ and $S \in \mathscr{C}_s^-$. Clearly

$$|\mathscr{C}_s^-| \le |\mathscr{C}_s| \le \binom{2^n}{s} \le \frac{2^{ns}}{s!} \le \left(\frac{e2^n}{s}\right)^s.$$

Hence

$$\begin{aligned}\sum_{s=s_1+1}^{2^{n-1}} \sum_{S \in \mathscr{C}_s^-} q^{b(s)} &\le \sum_{s=s_1+1}^{2^{n-1}} \left(\frac{e2^n}{s}\right)^s 2^{-s(n-\log_2 s)-s\log_2 n}(\log n)^s \\ &= \sum_{s=s_1+1}^{2^{n-1}} \left(\frac{e\log n}{n}\right)^s = o(1).\end{aligned}$$

Our final task is to show that as s runs over $s_1+1, s_1+2, \dots, 2^{n-1}$ and $S \in \mathscr{C}_s^+$, our double sum corresponding to (14.7) is $o(1)$. Here we have to be more careful. We shall need the following lemma.

Lemma 14.5 *Let G be a graph of order v and suppose that $\Delta(G) \le \Delta$, $2e(G) = vd$ and $\Delta + 1 \le u \le v - \Delta - 1$. Then there is a u-set U of vertices with*

$$|N(U)| = |U \cup \Gamma(U)| \ge v\frac{d}{\Delta}\{1 - \exp(-u(\Delta+1)/v)\}.$$

Here, as is customary, $\Delta(G)$ is the maximum degree, d is the average degree and $\Gamma(U) = \{x \in G : xy \in E(G)$ for some $y \in U\}$.

Proof What is $\mathrm{Av}(v - |N(U)|)$, the *average* of $v - |N(U)|$ as U runs over all u-sets of $V(G)$? Let $d_1, d_2, \dots, d_n$ be the degree sequence of G. Then

$$\mathrm{Av}\{v - |N(U)|\} = \sum_{i=1}^{n} \binom{v - d_i - 1}{u} \Big/ \binom{v}{u},$$

since a vertex of degree d_i does not belong to $N(U)$ for exactly $\binom{v-d_i-1}{u}$ choices of a u-set U. The function $\binom{x}{u}$ is convex for $x \ge u$ so $\sum_{i=1}^{n} d_i = vd$ implies

$$\begin{aligned}\mathrm{Av}\{v - |N(U)|\} &\le v\frac{d}{\Delta}\binom{v-\Delta-1}{u}\Big/\binom{v}{u} + v\left(1 - \frac{d}{\Delta}\right)\binom{v-1}{u}\Big/\binom{v}{u} \\ &\le v\frac{d}{\Delta}\left(\frac{v-u}{v}\right)^{\Delta+1} + v\left(1-\frac{d}{\Delta}\right) \\ &\le v\frac{d}{\Delta}\exp\left(-\frac{u(\Delta+1)}{v}\right) + v\left(1 - \frac{d}{\Delta}\right).\end{aligned}$$

Consequently for at least one u-set U we have

$$\begin{aligned}|N(U)| &\geq v - v\frac{d}{\Delta}\exp\left(-\frac{u(\Delta+1)}{v}\right) - v\left(1-\frac{d}{\Delta}\right)\\ &= v\frac{d}{\Delta}\left\{1-\exp\left(-\frac{u(\Delta+1)}{v}\right)\right\}.\end{aligned} \qquad \square$$

Let us continue the proof of Lemma 14.4.

(iii) Let us estimate the double sum corresponding to (14.7) over the range $s_1 \leq s \leq s_2 = \lfloor 2^n/(\log n)^4 \rfloor$ and $S \in \mathscr{C}_s^+$. Then

$$b(S) \leq s(n - \log_2 s + \log_2 n),$$

that is in $H = Q^n[S]$ the average degree is at least

$$\log_2 s - \log_2 n.$$

Set

$$u = \lfloor 2s/n \rfloor.$$

By Lemma 14.5 there is a u-set $U \subset S$ such that $N(U)$, the set of vertices of H within distance 1 of U, satisfies

$$|N(U)| \geq s\frac{\log_2 s - \log_2 n}{n}\left\{1-\exp\left(-\frac{u(n+1)}{s}\right)\right\} \geq s/3.$$

This shows that the sets in $\mathscr{C}_s^+$ can be selected as follows: first we select u vertices of Q^n, then $\lceil s/3 \rceil - u$ neighbours of these vertices and then $\lfloor 2s/3 \rfloor$ other vertices. Hence

$$|\mathscr{C}_s^+| \leq \binom{2^n}{u}(2^n)^u\binom{2^n}{\lfloor 2s/3 \rfloor}$$

and so

$$\sum_{s \in \mathscr{C}_s^+} q^{b(s)} \leq \left(\frac{e2^n}{u}\right)^u 2^{nu}\left(\frac{e2^n}{\lfloor 2s/3 \rfloor}\right)^{\lfloor 2s/3 \rfloor} 2^{-s(n-\log_2 s)}(\log n)^s.$$

Write $s = 2^{\beta n}$ so that $\beta \leq 1 - 4\log_2 \log n/n$. Then the sum above is at most

$$(c\log n)^s 2^{(2/3)sn(1-\beta)-sn+s\beta n} = (c\log n)^s 2^{-sn(1-\beta)/3},$$

where c is a positive constant. By our assumption on β, if n is sufficiently large, this is at most

$$(\log n)^{-s/4}.$$

Hence

$$\sum_{s=s_1}^{s_2} \sum_{S \in \mathscr{C}_s^+} q^{b(S)} = o(1).$$

(iv) Finally suppose that $\lceil 2^n/(\log n)^4 \rceil = s_2 + 1 \le s \le 2^{n-1}$ and $S \in \mathscr{C}_s^+$. Then in $H = Q^n[S]$ the average degree is at least

$$\log_2 s - \log_2 n > n - 2\log_2 n.$$

We shall find an even smaller subset U of S that 'fixes' many vertices of U. First we look for a subgraph of H with large average degree. Denote by T the set of vertices of H with degree at least $n - (\log_2 n)^2$ and set $t = |T|$. Then

$$tn + (s-t)\{n - (\log_2 n)^2\} \ge s(n - 2\log_2 n)$$

so

$$t \ge s\left(1 - \frac{2}{\log_2 n}\right).$$

Let H_1 be the subgraph spanned by $T : H_1 = Q^n[T] = H[T]$. Consider the following crude estimate of the size of H_1:

$$e(H_1) \ge e(H) - (s-t)n \ge \frac{s}{2}(n - 2\log_2 n) - \frac{2s}{\log_2 n} n.$$

Consequently the average degree in H_1 is at least

$$n - 2\log_2 n - \frac{4n}{\log_2 n} \ge n - \frac{5n}{\log_2 n}.$$

Set $u = \lfloor 2^n/n^{1/2} \rfloor$. By Lemma 14.5 there is a u-set U in T whose neighbourhood in H_1 is large:

$$\begin{aligned} |N_H(U)| \ge |N_{H_1}(U)| &\ge t\left(1 - \frac{5}{\log_2 n}\right)\{1 - \exp(-n^{1/4})\} \\ &\ge t\left(1 - \frac{6}{\log_2 n}\right) \ge s\left(1 - \frac{8}{\log_2 n}\right). \end{aligned}$$

The existence of such a u-set restricts severely the number of s-sets $S \in \mathscr{C}_s^+$. Indeed, the number of neighbourhoods $N_H(U)$ belonging to a u-set above is at most

$$\sum_{(k_i)} \prod_{i=1}^{u} \binom{n}{k_i} \le n^{u(\log_2 n)^2},$$

where the summation is over all $(k_1, k_2, \ldots, k_u)$ with $k_i \le (\log_2 n)^2$, since at most $(\log_2 n)^2$ of the n neighbours of a vertex $x \in U$ do not belong to $N_H(U)$. Consequently, with $w = \lfloor 8s/\log_2 n \rfloor$ we find that in our range

$$\sum_{S \in \mathscr{C}_s^+} q^{b(S)} \le \binom{2^n}{u} n^{u(\log_2 n)^2} \binom{2^n}{w} 2^{-s(n-\log_2 s)} (\log n)^{s\{1-(\log_2 s)/n\}} \le 2^{\varepsilon(s)},$$

where

$$\varepsilon(s) = o(s) - s\left(n - \log_2 s - \log_2 \log n + \frac{\log_2 s}{n} \log_2 \log n\right).$$

As $s \le 2^{n-1}$, we have

$$\begin{aligned} \varepsilon(s) &\le o(s) - s\left\{n - (n-1) - \log_2 \log n + \frac{n-1}{n} \log_2 \log n\right\} \\ &= o(s) - s\left\{1 - \frac{1}{n} \log_2 \log n\right\} \le -s/2 \end{aligned}$$

if n is sufficiently large. Consequently

$$\sum_{s=s_2+1}^{2^{n-1}} \sum_{S \in \mathscr{C}_s^+} q^{b(S)} = o(1),$$

as required. This concludes the proof of Lemma 14.4 and so the proof of Theorem 14.3 is complete. □

What can we say about the orders of the large components of Q_p^n for fairly small values of p? For what values of p is there a 'giant' component, if ever? As in Chapter 6, let us write $L_i(Q_p^n)$ for the order of an ith largest component of Q_p^n. Erdős and Spencer (1979) conjectured that $L_1(Q_p^n)$, with $p = c/n$, has a jump at $c = 1$. This was proved by Ajtai, Komlós and Szemerédi (1982), who remarked also that $L_2(Q_p^n)$ is almost always small. Thus a giant component emerges shortly after $p = 1/n$ and the graph becomes connected shortly after $p = \frac{1}{2}$. Note that the ratio of these probabilities is about the logarithm of the order of the graph, just as in the case of G_p, studied in Chapter 6.

Theorem 14.6 *Let c be a constant and $p = c/n$.*

(*i*) *If $0 < c < 1$, then $L_1(Q_p^n) = o(2^n)$ almost surely.*

(*ii*) *For $c > 1$ there is a constant $\gamma(c)$ such that $L_1(Q_p^n) > \gamma(c)2^n$ almost surely.*

(*iii*) *For every $c > 0, L_2(Q_p^n) = o(2^n)$ almost surely.*

14.2 Random Matrices

What is the probability that if we pick n random vertices of Q^n (with replacement, say) then the n, not necessarily distinct, vectors of $\mathbb{R}^n$ are linearly independent? Equivalently, what is the probability that a random 0–1 matrix of order n is non-singular? Komlós (1967, 1968) proved that this probability tends to 1 as $n \to \infty$, even if the entries are not necessarily independent 0–1 r.vs but independent r.vs with an arbitrary common non-degenerate distribution function. The main aim of this section is to present a more recent theorem of Komlós (1981) giving an upper bound on the probability that an n by n 0–1 matrix is singular.

We shall need four lemmas, the first of which is a classical result, the so-called *Sperner lemma* (1928). Let $X = \{1, 2, \ldots, n\}$. Call a family $\mathcal{F}$ of subsets of X a *Sperner family* if $A, B \in \mathcal{F}$ and $A \neq B$ imply $A \not\subset B$.

Lemma 14.7 *If $\mathcal{F}$ is a Sperner family, then*

$$|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}.$$

Proof A regular bipartite graph with vertex classes $V_1, V_2, |V_1| \leq |V_2|$, contains a matching from V_1 into V_2. Hence for $k < n/2$ and $l > n/2$ there are injections $f : X^{(k)} \to X^{(k+1)}$ and $g : X^{(l)} \to X^{(l-1)}$ satisfying

$$A \subset f(A) \text{ and } g(B) \subset B \text{ for } A \in X^{(k)} \text{ and } B \in X^{(l)},$$

where $X^{(j)}$ is the set of j-subsets of X. Consequently the lattice $\mathcal{P}(X)$ of all subsets of X can be covered with $\binom{n}{\lfloor n/2 \rfloor}$ chains. By definition each chain contains at most one member of $\mathcal{F}$. □

The next lemma is another famous result, a refinement of a lemma of Littlewood and Offord (1938), due to Erdős (1945).

Lemma 14.8 *Let $S \in \mathbb{R}$ and $x_i \in \mathbb{R}, |x_i| \geq 1, i = 1, \ldots, n$. Then at most*

$$\binom{n}{\lfloor n/2 \rfloor}$$

of the 2^n sums $\sum_{i=1}^n \varepsilon_i x_i$, $\varepsilon_i = \pm 1$, fall into the open interval $(S-1, S+1)$.

Proof The collection of subsets A of $\{1, \ldots, n\}$ satisfying

$$S - 1 < \sum_{i \in A} x_i - \sum_{j \notin A} x_j < S + 1$$

is a Sperner family. □

We shall need the following immediate consequence of Lemma 14.8.

Lemma 14.9 *Suppose $x_i \in \mathbb{R}, i = 1, 2, \ldots, n$, and $x_i \neq 0$ for at least t values of i. Then at most $\binom{t}{\lfloor t/2 \rfloor} 2^{n-t}$ of the 2^n sums $\sum_{i=1}^n \varepsilon_i x_i$, $\varepsilon_i = 0, 1$, have the same value.* □

It is worth remarking that Kleitman (1965, 1976), Katona (1966), Griggs (1980), Peck (1980) and Griggs *et al.* (1983) proved a great many results related to the Littlewood–Offord lemma. For example, based on a theorem of Stanley (1980), Peck (1980) sharpened Lemma 14.9 to the following result, which had been conjectured by Erdős: a set of n distinct numbers having the most linear combinations, with coefficients 0 and 1, all equal, are n integers of smallest magnitude, say $\{i - \lfloor (n+1)/2 \rfloor : i = 1, 2, \ldots, n\}$.

Let us turn to random m by n 0–1 matrices. To be precise, choose n vectors $a_1, a_2, \ldots, a_n \in Q^m$ independently of each other and then take the matrix $(a_1, a_2, \ldots, a_n)$ whose ith column is a_i.

Let us define the *strong rank* $\overline{\overline{r}}(a_1, a_2, \ldots, a_n)$ of the matrix $(a_1, a_2, \ldots, a_n)$ to be k if any k of the a_i's are independent and either $k = n$ or some $k + 1$ of the vectors are not independent. The main theorem hinges on the following lemma.

Lemma 14.10 *If $a_1, \ldots, a_n \in Q^m$ are independent random vectors, then*

$$P\{\overline{\overline{r}}(a_1, \ldots, a_n) = k - 1\} \leq \binom{n}{k} \binom{m}{k-1} p_k^{m-k+1},$$

where

$$p_k = \binom{k}{\lfloor k/2 \rfloor} 2^{-k}.$$

Proof Because of the definition of the strong rank it suffices to show that for $k \geq 1$

$$P\{\overline{\overline{r}}(a_1, \ldots, a_k) = k - 1\} \leq \binom{m}{k-1} p_k^{m-k+1}. \tag{14.8}$$

Since, if $\overline{\overline{r}}(a_1, \ldots, a_k) \geq k - 1$, some $k - 1$ of the rows of $(a_1, \ldots, a_k)$ are independent, (14.8) follows if we show that the probability Q_k that $\overline{\overline{r}}(a_1, \ldots, a_k) = k - 1$ conditional on the first $k - 1$ rows being independent is at most p_k^{m-k+1}. Let us assume therefore that the first $k - 1$ coordinates of $a_1, \ldots, a_k$ are given and the $(k - 1)$ by k matrix M formed by them has rank $k-1$. If $\overline{\overline{r}}(a_1,\dots,a_k) = k-1$, then a_k depends on $a_1,\dots,a_{k-1}$ so for some $\alpha_1,\dots,\alpha_k \in \mathbb{R}$ we have

$$\sum_1^k \alpha_j a_j = 0 \text{ and } \sum_1^k |\alpha_j| = 1.$$

Since M has rank $k-1$, the α_i are determined by M up to a factor ± 1 and none of them is 0. Hence when choosing a_{ij} for $i \geq k$ (that is the kth $(k+1)$st,$\dots$,mth coordinates of the vectors a_j), then

$$\sum_{j=1}^k \alpha_j a_{ij} = 0 \tag{14.9}$$

has to hold for every $i, i = k,\dots,m$. Applying Lemma 14.9 with $t = n = k$, we find that the probability of choosing the ith row in such a way that (14.9) is satisfied is at most p_k. Hence

$$Q_k \leq p_k^{m-k+1},$$

completing the proof. □

We are ready to prove the theorem of Komlós (1981) on singular 0–1 matrices.

Theorem 14.11 *The probability that a random n by n 0–1 matrix is singular is $O(n^{-1/2})$.*

Proof Let $a_1,\dots,a_n \in Q^n$ be independent random vectors. Set $n_0 = \lceil 3n/4 \rceil$. By Lemma 14.10 we have

$$P\{\overline{\overline{r}}(a_1,\dots,a_n) < n_0\} \leq \sum_{k=1}^{n_0} \binom{n}{k}\binom{n}{k-1} p_k^{n-k+1}.$$

Noting that

$$p_k \sim (2/\pi k)^{1/2}$$

we find that the probability above is at most 2^{-n} if n is sufficiently large.

We have to be more careful in estimating the probability that the strong rank of a random matrix is large but less than n. Write E_k for the event that $a_1,\dots,a_{k-1}$ are independent and a_k depends on them.

Clearly

$$P\{n_0 \leq \overline{\overline{r}}(a_1,\dots,a_n) < n\} \leq \sum_{k=n_0}^{n-1} P(E_k),$$

for if $n_0 \leq \bar{\bar{r}}(a_1, \ldots, a_n) < n$, then for some $k \geq n_0$ the vectors $a_1, \ldots, a_{k-1}$ are independent but a_k depends on them. Therefore to complete the proof of our theorem it suffices to show that

$$P(E_k) \leq c_1/2^{n-k} n^{1/2} \tag{14.10}$$

for some constant c_1 and every $k, n_0 \leq k < n$. Let $n_0 \leq k < n$. Denote by $b_1, \ldots, b_n$ the row vectors of the matrix $(a_1, \ldots, a_{k-1})$. By Lemma 14.10

$$P\left\{\bar{\bar{r}}(b_1, \ldots, b_n) < \frac{n}{2}\right\} \leq \sum_{l=1}^{\lceil n/2 \rceil} \binom{n}{l} \binom{k-1}{l-1} p_l^{k-l}$$

and this is again at most 2^{-n} if n is sufficiently large. Hence (14.10) follows if we prove

$$P\{E_k | \bar{\bar{r}}(b_1, \ldots, b_n) \geq n/2\} \leq c_2/2^{n-k} n^{1/2}, \tag{14.11}$$

for some constant c_2.

Let $b_1, \ldots, b_n \in Q^{k-1}$ be fixed vectors satisfying $\bar{\bar{r}}(b_1, \ldots, b_n) \geq n/2$. As $k-1$ of these vectors are independent, we may assume without loss of generality that $b_1, b_2, \ldots, b_{k-1}$ are independent. Then the other b_i's are linear combinations of these, say b_k depends on $b_1, \ldots, b_{k-1}$ as follows:

$$\sum_1^k \beta_i b_i = 0, \tag{14.12}$$

where $\beta_k = 1$. Since $\bar{\bar{r}}(b_1, \ldots, b_n) \geq n/2$, at least $n/2$ of the β_i are non-zero. If E_k holds then a_k is a linear combination of $a_1, \ldots, a_{k-1}$ so the linear relation (14.12) has to hold for the coordinates of a_k:

$$\sum_{i=1}^k \beta_i a_{ik} = 0. \tag{14.12$'$}$$

By Lemma 14.9 the probability that the first k coordinates of a_k are chosen in such a way that (14.12′) holds is at most

$$\binom{\lfloor n/2 \rfloor}{\lfloor n/4 \rfloor} 2^{-n/2} \leq 2n^{-1/2}.$$

Finally, if E_k holds, the subsequent coordinates $a_{k+1,k}, a_{k+2,k}, \ldots, a_{n,k}$ of a_k are all determined by $a_{1,k}, a_{2,k}, \ldots, a_{k-1,k}$ and the linear dependence of $b_{k+1}, b_{k+2}, \ldots, b_n$ on $b_1, \ldots, b_{k-1}$. Therefore the probability of choosing them so that E_k holds is 2^{-n+k}. This implies (14.11), so the proof of our theorem is complete. □

Theorem 14.11 tells us that almost no 0–1 matrix has 0 as an eigenvalue. What about the distribution of the eigenvalues? This question has been studied in detail for real symmetric matrices, the fundamental result in the area being Wigner's (1955, 1958) semicircle law. The following extension of it is due to Arnold (1967) (see also Arnold (1971, 1976)).

Theorem 14.12 *For $1 \le i \le j$ let a_{ij} be independent real-valued r.vs such that all $a_{ij}, i < j$ have the same distribution and all a_{ii} have the same distribution. Suppose, furthermore, that all central moments of the a_{ij} are finite and put $\sigma^2 = \sigma^2(a_{ij})$. For $i < j$ set $a_{ji} = a_{ij}$ and let $A_n = (a_{ij})_{i,j=1}^n$. Finally, denote by $W_n(x)(A_n)$ the number of eigenvalues of A_n not larger than x, divided by n. Then $W_n(x)$ is a r.v. for every $n \in \mathbb{N}$ and $x \in \mathbb{R}$, defined on the space of random matrices A_n, and $\lim_{n\to\infty} W_n(x2\sigma\sqrt{n}) = W(x)$ in distribution, where*

$$W(x) = \begin{cases} 0, & \text{if } x \le -1, \\ \dfrac{2}{\pi}\displaystyle\int_{-1}^{x} (1-x^2)^{1/2}, & \text{if } -1 \le x \le 1, \\ 1, & \text{if } x \ge 1. \end{cases}$$

Note that $W(x)$ is precisely the distribution function whose density is $2/\pi$ times the unit semicircle.

Juhász (1981) and Füredi and Komlós (1981) studied the largest and second-largest eigenvalues of a random symmetric matrix. Juhász proved that if $E(a_{ii}) > 0$, then the second-largest eigenvalue is much smaller than the largest eigenvalue. This result of Juhász was extended by Füredi and Komlós to the following theorem which, in view of the semicircle law, is essentially best possible.

Theorem 14.13 *Let K, μ, σ and ν be fixed positive numbers. Let $a_{ij}, 1 \le i \le j \le n$, be independent r.vs such that $|a_{ij}| \le K$ for all $i \le j, E(a_{ij}) = \mu$ and $\sigma^2(a_{ij}) = \sigma^2$ for all $i < j$, and $E(a_{ii}) = \nu$ for all i. For $i < j$ set $a_{ji} = a_{ij}$, and define $A = (a_{ij})_{i,j=1}^n$. Let $\lambda_1(A) \ge \lambda_2(A) \ge \ldots \ge \lambda_n(A)$ be the eigenvalues of A.*

(*i*) *If $\mu > 0$, then, as $n \to \infty$,*

$$\lambda_1(A) - \{(n-1)\mu + \nu + \sigma^2/\mu\} \xrightarrow{d} N(0, 2\sigma^2).$$

Furthermore, almost every A is such that

$$\max_{i \ge 2} |\lambda_i(A)| < 2\sigma\sqrt{n} + O(n^{1/3}\log n).$$

(*ii*) *If* $\mu = 0$, *then*

$$\max_{1 \le i \le n} |\lambda_i(A)| = 2\sigma\sqrt{n} + O(n^{1/3}\log n).$$

Note that for matrices A satisfying the conditions of Theorems 14.12 and 14.13 we must have

$$\lambda_2(A) = \{2\sigma + O(1)\}\sqrt{n}.$$

14.3 Balancing Families of Sets

Let $S_1, S_2, \dots, S_n$ be finite sets. We wish to partition $\bigcup_{i=1}^n S_i$ into two sets, say R (red) and B (blue), such that for each i about the same number of elements of S_i belong to R as to B. To formulate our problem more precisely, for a given partition (or colouring) $R \cup B$ define the *discrepancy* of a set S as

$$\text{disc } S = ||S \cap R| - |S \cap B||.$$

Then our aim is to find a partition $R \cup B$ for which the vector $(\text{disc } S_i)_{i=1}^n \in \mathbb{R}^n$ is small in some norm.

After several results concerning this problem, due to Brown and Spencer (1971), Olson and Spencer (1978) and Beck and Fiala (1981), the l_2 norm case was settled completely by Spencer (1981). Our main aim in this section is to prove Spencer's theorem (Theorem 14.21). Given n, define $f_2(n)$ as follows:

$$f_2(n) = \max_{(S_i)} \min_{(R,B)} \left\{ \sum_{i=1}^n (\text{disc } S_i)^2 \right\}^{1/2}. \tag{14.13}$$

To justify the use of the maximum above note that by splitting the atoms of a system $\{S_i\}_1^n$ as equally as possible we obtain a partition for which disc S_i is less than 2^n for every i. Hence $f_2(n) \le \sqrt{n}\, 2^n$. As we shall see later, this simple estimate is very crude indeed.

Before getting down to some mathematics, let us reformulate the definition of $f_2(n)$. Given sets $S_1, S_2, \dots, S_n \subset \{1, 2, \dots, m\}$, write

$$u_{ij} = \begin{cases} 1, & \text{if } j \in S_i, \\ 0, & \text{if } j \notin S_i. \end{cases}$$

Then $u_j = (u_{ij})_{i=1}^n$ is a vertex of the n-cube Q^n in $\mathbb{R}^n$. Thus we wish to partition the vertices $u_1, u_2, \dots, u_m$ of Q^n in such a way that each of the n faces of Q^n of the form

$$\{\varepsilon = (\varepsilon_i)_1^n : \varepsilon_j = 1\}, \qquad j = 1, 2, \dots, n.$$

has about as many blue vertices as red ones. This shows that we may assume that $m \le 2^n$, since if $u_i = u_j$ for some $i \ne j$ then putting u_i into R and u_j into B we reduce the problem to splitting $m-2$ vertices. Although this is a pleasant little fact, it does not really help us.

In terms of the vectors $u_1, u_2, \ldots, u_m$, for a partition R, B we have

$$\begin{aligned}
\sum_{i=1}^{n} (\text{disc } S_i)^2 &= \sum_{i=1}^{n} (|S_i \cap R| - |S_i \cap B|)^2 \\
&= \sum_{i=1}^{n} \left(\sum_{j \in R} u_{ij} - \sum_{j \in B} u_{ij} \right)^2 \\
&= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \varepsilon_j u_{ij} \right)^2 = \left| \sum_{j=1}^{n} \varepsilon_j u_j \right|^2,
\end{aligned}$$

where $\varepsilon_j = 1$ if $j \in R$ and $\varepsilon_j = -1$ if $j \in B$. (Here and in the sequel $|x|$ denotes the l_2 norm of the vector x.) Consequently (14.13) is equivalent to

$$f_2(n) = \max_{m} \max_{u_j \in Q^m} \min_{\varepsilon_j = \pm 1} \left| \sum_{j=1}^{m} \varepsilon_j u_j \right|. \tag{14.14}$$

As our first result we shall show that if m is small, say $m = n$, then $|\sum_1^m \varepsilon_j u_j|$ is small for some $(\varepsilon_j)_{j=1}^m$.

Theorem 14.14 *If* $S_1, S_2, \ldots, S_n \subset \{1, 2, \ldots, n\}$, *then*

$$\sum_{i=1}^{n} (\text{disc } S_i)^2 \le n^2$$

for some partition R, B.

Proof Given $u_1, \ldots, u_n \in Q^n$ we choose inductively $\varepsilon_1, \varepsilon_2, \ldots$ such that

$$\left| \sum_{1}^{h} \varepsilon_i u_i \right|^2 \le hn.$$

To do this, having chosen $\varepsilon_1, \ldots, \varepsilon_h$, choose $\varepsilon_{h+1} = \pm 1$ so that

$$\left| \sum_{1}^{h+1} \varepsilon_i u_i \right| \le \left| \sum_{1}^{h} \varepsilon_i u_i - \varepsilon_{h+1} u_{h+1} \right|.$$

Then by the parallelogram law

$$\left|\sum_1^{h+1} \varepsilon_i u_i\right|^2 \le \frac{1}{2}\left\{\left|\sum_1^{h} \varepsilon_i u_i + \varepsilon_{h+1}u_{h+1}\right|^2 + \left|\sum_1^{h} \varepsilon_i u_i - \varepsilon_{h+1}u_{h+1}\right|^2\right\}$$

$$= \left|\sum_1^{h} \varepsilon_i u_i\right|^2 + |\varepsilon_{h+1}u_{h+1}|^2 \le (h+1)n. \qquad \square$$

In order to get our first bound on $f_2(h)$ we note that Q^n is contained in the ball of radius $\sqrt{n}$ about the origin. Hence, if for an arbitrary number of vectors $u_1, u_2, \ldots, u_m$ in the unit ball of $\mathbb{R}^n$ we can find $\varepsilon_i = \pm 1$ with $|\sum_1^m \varepsilon_i u_i| \le h(n)$, say, then $f_2(n) \le \sqrt{n}h(n)$. It turns out that the best possible function $h(n)$ is easily determined.

Theorem 14.15 *Let $u_1, u_2, \ldots, u_m \in \mathbb{R}^n, |u_i| \le 1$. Then there exist $\varepsilon_i = \pm 1$ such that*

$$\left|\sum_1^m \varepsilon_i u_i\right| \le n^{1/2}.$$

The bound $n^{1/2}$ is best possible.

Proof If $u_1, \ldots, u_n$ are orthonormal then $|\sum_1^n \varepsilon_i u_i| = n^{1/2}$ for every choice of the ε_i, so the bound cannot be improved. To see that $n^{1/2}$ is an upper bound, in the first instance we choose $\alpha_1, \alpha_2, \ldots, \alpha_m$ between -1 and 1 so that most of them are exactly ± 1 and the sum $\sum_1^m \alpha_i u_i$ is 0 and then change the remaining α_i to ± 1 in such a way that the sum will not be altered by much. We state these two steps as separate lemmas.

Lemma 14.16 *Given $u_1, \ldots, u_m \in \mathbb{R}^n$ there are $(\alpha_i)_1^m$ such that*

$$\sum_1^m \alpha_i u_i = 0, \qquad -1 \le \alpha_i \le 1,$$

and $|\alpha_i| < 1$ for at most n of the indices.

Proof Set $H = \{(\alpha_1, \ldots, \alpha_m) : \sum_1^m \alpha_i u_i = 0\} \subset \mathbb{R}^m$ and let K^m be the solid cube: $K^m = \{(x_1, \ldots, x_m) : |x_i| \le 1\} \subset \mathbb{R}^m$. Let α be an extreme point of $K^m \cap H$. Then since codim $H \le n, \alpha$ is not in the interior of a face of dimension greater than n of K^m. Hence, α is in the n-dimensional skeleton of K^m, i.e. all but at most n of the α_i's are ± 1. $\square$

Lemma 14.17 *Let $u_1, \dots, u_n \in \mathbb{R}^n, |u_i| \le 1$, and let $(\alpha_1, \dots, \alpha_n) \in K^n$. Then there exist $\varepsilon_i = \pm 1$ such that*

$$\left| \sum_1^n \varepsilon_i u_i - \sum_1^n \alpha_i u_i \right| \le n^{1/2}.$$

Proof We shall need a simple fact of elementary geometry. The shortest chord of a sphere of radius $(r^2+1)^{1/2}$ through a point at distance r from the centre has length 2.

Now to prove the lemma we select inductively $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k = \pm 1$ such that

$$\left| \sum_1^k (\varepsilon_i - \alpha_i) u_i \right| \le k^{1/2}.$$

Having selected $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k$, put $a = \sum_1^k (\varepsilon_i - \alpha_i) u_i$, $b = a - (\alpha_{k+1} + 1) u_{k+1}$, $c = a - (\alpha_{k+1} - 1) u_{k+1}$. Then b and c are the endpoints of a segment of length 2 containing a. Hence by the remark above

$$\min\{|b|, |c|\} \le (|a|^2 + 1)^{1/2} \le (k+1)^{1/2}.$$

Theorem 14.15 is an immediate consequence of Lemmas 14.16 and 14.17. Indeed, first select $\alpha_1, \alpha_2, \dots, \alpha_m$ as in Lemma 14.16, say $|\alpha_{n+1}| = |\alpha_{n+2}| = \dots = |\alpha_m| = 1$. Then apply Lemma 14.17 to $(u_i)_1^n$ and $(\alpha_i)_1^n$ to find $\varepsilon_i = \pm 1, 1 \le i \le n$, with

$$\left| \sum_1^n (\varepsilon_i - \alpha_i) u_i \right| \le n^{1/2}.$$

Finally, set $\varepsilon_{n+1} = \alpha_{n+1}, \varepsilon_{n+2} = \alpha_{n+2}, \dots, \varepsilon_m = \alpha_m$. Then

$$\left| \sum_1^m \varepsilon_i u_i \right| = \left| \sum_1^m \varepsilon_i u_i - \sum_1^m \alpha_i u_i \right| = \left| \sum_1^n (\varepsilon_i - \alpha_i) u_i \right| \le n^{1/2}. \qquad \square$$

As we remarked before Theorem 14.15, our result gives some information about $f_2(n)$.

Corollary 14.18 $f_2(n) \le n$.

Proof Given $S_1, S_2, \dots, S_n$, let $u_1, u_2, \dots, u_m \in Q^n$ be the vectors determined by the S_i. Then $|u_i/n^{1/2}| \le 1$ for every i, so for some $\varepsilon_i = \pm 1$ we have

$$\left| \sum_1^m \varepsilon_i u_i / n^{1/2} \right| \le n^{1/2},$$

implying

$$\left|\sum_1^m \varepsilon_i u_i\right|^2 \leq n^2. \qquad \square$$

The above attack on $f_2(n)$ has one main deficiency. Having selected $\alpha_1, \alpha_2, \ldots, \alpha_n$, the ε_i are chosen one by one, so in the choice of ε_i we do not take into account $\alpha_{i+1}, \alpha_{i+1}, \ldots, \alpha_n$. In order to get a better bound on $f_2(n)$ we select the ε_i all at once. To do this we shall replace the ε_i by appropriate random variables X_i and will show that the expected value of $|\sum_1^n X_i u_i|^2$ is small. The existence of these random variables will be implied by the following lemma.

Lemma 14.19 *Given $\varepsilon > 0$ there is an n_0 such that if $n \geq n_0$ and $0 < p_i < 1, i = 1, \ldots, n$, then there are Bernoulli r.vs $X_1, X_2, \ldots, X_n$ satisfying*

$$P(X_i = 1) = p_i, \quad P(X_i = 0) = 1 - p_i$$

and

$$\sigma^2\left(\sum_{i \in S} X_i\right) \leq \frac{n}{16}(1 + \varepsilon) \quad \textit{for all} \quad S \subset \{1, 2, \ldots, n\}.$$

Proof We shall show first that the result is true if for some integer a we have $p_1 = p_2 = \ldots = p_n = a/n$. Consider the symmetric group S_n, acting on $\{1, 2, \ldots, n\}$, as a probability space. For $i = 1, \ldots, n$, define

$$A_i = \{\pi \in S_n : \pi(i) \leq a\} \quad \text{and} \quad Y_i = \chi_{A_i}$$

where χ denotes the indicator function. Then

$$E(Y_i^2) = E(Y_i) = P(A_i) = a/n = p$$

and

$$E(Y_i Y_j) = P(A_i \cap A_j) = \frac{a(a-1)}{n(n-1)} = p\frac{a-1}{n-1} \text{ for } i < j.$$

Hence, if $S \subset \{1, 2, \ldots, n\}$ has s elements, then

$$\begin{aligned}
\sigma^2\left(\sum_{i \in S} Y_i\right) &= \sum_{i \in S} E(Y_i^2) + 2\sum_{\substack{i<j \\ i,j \in S}} E(Y_i Y_j) - (sp)^2 \\
&= sp\left\{1 + (s-1)\frac{a-1}{n-1} - sp\right\} \\
&= sp\left\{1 - \frac{a-1}{n-1} - s\left(\frac{a}{n} - \frac{a-1}{n-1}\right)\right\}
\end{aligned}$$

$$
\begin{aligned}
&= sp\left\{1-\frac{a-1}{n-1}-s\frac{n-a}{n(n-1)}\right\} = sp\left\{1-\frac{a-1}{n-1}-\frac{sq}{n-1}\right\}\\
&= sp\left\{q-\frac{sq}{n-1}\right\}+sp\frac{n-a}{n(n-1)}\\
&\le spq\left(1-\frac{s}{n-1}\right)+1 \le \frac{n}{4}pq+1,
\end{aligned}
$$

where $q = 1-p$. Therefore

$$\sigma^2\left(\sum_{i\in S} Y_i\right) \le \frac{n}{16}+1$$

for every set S.

Now if $a/n \le p_1 \le p_2 \le \ldots \le p_n \le (a+1)/n, a \le n-1$, then define A_i and Y_i as earlier and set

$$B_i = \{\pi \in S_n : \pi(i) = a+1\} \text{ and } C_i = A_i \cup B_i.$$

Let $X_1, X_2, \ldots, X_n$ be 0–1 r.vs satisfying $P(X_i) = p_i, X_i \ge Y_i$ and

$$P(A_{i_1}\cap A_{i_2}\cap\ldots\cap A_{i_k}) \le E(X_{i_1}X_{i_2}\ldots X_{i_k}) \le P(C_{i_1}\cap C_{i_2}\cap\ldots\cap C_{i_k}).$$

Since the sets $B_1, B_2, \ldots, B_n$ are disjoint,

$$\sum_{i\in S} Y_i \le \sum_{i\in S} X_i \le \sum_{i\in S} Y_i + 1$$

for every set S.

If $\left|\sum_{i\in S} X_i - E(\sum_{i\in S} X_i)\right| \ge n^{1/3}+1$, then

$$\left|\sum_{i\in S} X_i - E\left(\sum_{i\in S} X_i\right)\right| \le (1+n^{-1/3})\left|\sum_{i\in S} Y_i - E\left(\sum_{i\in S} Y_i\right)\right|,$$

therefore, if n is large enough,

$$\sigma^2\left(\sum_{i\in S} X_i\right) \le (n^{1/3}+1)^2 + (1+n^{-1/3})^2\left(\frac{n}{16}+1\right) \le \frac{n}{16}+2n^{2/3}.$$

Finally, we shall prove the general case by putting together, rather crudely, groups of r.vs with the p_i's close to each other. Let k be defined by

$$k^3 + k(k-1) \le n < (k+1)^3 + k(k+1).$$

Partition $\{p_1, p_2, \ldots, p_n\}$ into k^2 groups of k elements and $n-k^3$ singletons in such a way that the elements in a group satisfy

$$\frac{a}{k} \le p_i \le \frac{a+1}{k}$$

for some integer a. Use the construction above to define r.vs for the p_i's in each group and make these groups of r.vs independent of each other. Since the variance is additive on independent r.vs, if n is large enough, the variance of any sum of our r.vs is at most

$$k^2\left(\frac{k}{16}+2k^{2/3}\right)+(n-k^3)\frac{1}{4}\le\frac{n}{16}+3n^{8/9}. \qquad \square$$

Note that, for once, independence is beaten handsomely : if our Bernoulli r.vs $X_1, X_2, \dots, X_n$ are independent, then $\sigma^2(\sum_{i=1}^n X_i) = \sum_{i=1}^n p_i(1-p_i)$ so all we can guarantee is that $\sigma^2(\sum_{i=1}^n X_i) \le n/4$.

If we replace X_i by $2X_i - 1$, then we obtain the following reformulation of Lemma 14.19.

Lemma 14.19′ *Given $\varepsilon > 0$, there is an n_0 such that the following holds.*

If $n \ge n_0$ and $0 < p_i < 1, 1 \le i \le n$, then there exist r.vs $X_1, X_2, \dots, X_n$ such that

$$P(X_i = 1) = p_i, \quad P(X_i = -1) = 1 - p_i$$

and

$$\sigma^2\left(\sum_{i\in S} X_i\right) \le \frac{n}{4}(1+\varepsilon)$$

for every set $S \subset \{1, 2, \dots, n\}$.

This result enables us to strengthen Lemma 14.17 considerably.

Lemma 14.20 *Given $\varepsilon > 0$, there is an n_0 such that the following holds.*

If $n \ge n_0, v_1, v_2, \dots, v_n$ are (not necessarily distinct) vertices of the n-cube Q^n and $-1 < \alpha_i < 1$ for $i = 1, 2, \dots, n$, then there exist $\varepsilon_i = \pm 1$ such that

$$\left|\sum_{i=1}^n \varepsilon_i v_i - \sum_{i=1}^n \alpha_i v_i\right|^2 \le \frac{n^2}{4}(1+\varepsilon). \tag{14.15}$$

Proof Let n_0 be as in Lemma 14.19′. Set $p_i = (1+\alpha_i)/2$ and let $X_1, X_2, \dots, X_n$ be r.vs with

$$P(X_i = 1) = p_i, \qquad P(X_i = -1) = 1 - p_i,$$

and

$$\sigma^2\left(\sum_{i\in S} X_i\right) \le \frac{n^2}{4}(1+\varepsilon)$$

for every set $S \subset \{1,2,\dots,n\}$. Then $E(X_i) = p_i - (1-p_i) = \alpha_i$. Denote by S_j the set of indices i for which the jth coordinate of v_i is 1. Then

$$E\left(\left|\sum_{i=1}^n X_i v_i - \sum_{i=1}^n \alpha_i v_i\right|^2\right) = E\left[\sum_{j=1}^n \left\{\sum_{i\in S_j}(X_i - \alpha_i)\right\}^2\right] \le \frac{n^2}{4}(1+\varepsilon)$$

since

$$E\left\{\sum_{i\in S_j}(X_i-\alpha_i)\right\}^2 = \sigma^2\left(\sum_{i\in S_j} X_i\right) \le \frac{n}{4}(1+\varepsilon)$$

for every j. Consequently (14.15) holds for some choice of the ε_i. □

Theorem 14.21 $f_2(n) = (n/2)\{1+o(1)\}$.

Proof By replacing Lemma 14.17 by Lemma 14.20 in the proof of Theorem 14.15, we find that

$$f_2(n) \le (n/2)\{1+o(1)\}.$$

To get a lower bound for $f_2(n)$, assume first that there is an Hadamard matrix of order n, i.e. there are orthogonal vectors $v_1, v_2, \dots, v_n \in \mathbb{R}^n$ with coordinates ± 1. We may also assume that $v_1 = (1,1,\dots,1)^t$. Set $u_i = \frac{1}{2}(v_1 + v_i), i = 1,2,\dots,n$, so that $u_i \in Q^n$. Then for $\varepsilon_i = \pm 1$ we have

$$\begin{aligned}\left|\sum_{i=1}^n \varepsilon_i u_i\right|^2 &= \frac{1}{4}\left|\left(\sum_{i=1}^n \varepsilon_i\right) v_1 + \sum_{i=2}^n \varepsilon_i v_i\right|^2 \\ &= \frac{n}{4}\left\{\left(\sum_{i=1}^n \varepsilon_i\right)^2 + n - 1\right\} \ge \frac{n^2}{4}\left(1 - \frac{1}{n}\right). \qquad (14.16)\end{aligned}$$

For an arbitrary value of n we just choose an Hadamard matrix of order at most n and apply (14.16). To be precise, given $\varepsilon > 0$, if n is sufficiently large, then there is an Hadamard matrix of order m for some m satisfying $(1-\varepsilon)n \le m \le n$. This follows from the fact that for all $k, l \in \mathbb{N}$ there are Hadamard matrices of order $4^k 12^l$. Hence, by (14.16),

$$f_2(n) \ge f_2(m) \ge \frac{m}{2}\left(1 - \frac{1}{m}\right)^{1/2} \ge \frac{(1-\varepsilon)n}{2}\left(1 - \frac{1}{(1-\varepsilon)n}\right).$$

Therefore $f_2(n) = (n/2)\{1+o(1)\}$, as claimed. □

The thrust of Theorem 14.21 is, of course, the upper bound which, loosely stated, claims that $f_2(n) = O(n)$. Putting it another way, given a family of n sets, for some partition of the underlying set the average of the squares of the discrepancies is $O(n^{1/2})$. Recently, Spencer (1985) greatly improved this assertion: he showed that for some colouring not only the average is $O(n)$ but even the maximum! To formulate Spencer's theorem, analogously to (14.13), define

$$f_\infty(n) = \max_{(S_i)} \min_{(R,B)} \max_{1\le i\le n} \text{ disc } (S_i).$$

Note that, by the easy part of Theorem 14.21, $f_\infty(n) \ge \{\frac{1}{2} + o(1)\}n^{1/2}$.

Theorem 14.22 $\{\frac{1}{2} + o(1)\}n^{1/2} \le f_\infty(n) = O(n^{1/2})$. □

To change the topic slightly, let $\mathscr{M}_n$ be the set of n by n matrices whose entries are ± 1. For $A = (a_{ij}) \in \mathscr{M}_n$, let $d(A) = |\sum_{i,j} a_{ij}|$. How small can we make $d(A)$ by successively changing the signs of all entries in some rows or some column? And how large can we make it? These questions were studied by Gleason (1960), Moon and Moser (1966), Komlós and Sulyok (1970) and Brown and Spencer (1971).

To formulate the results precisely, for $A, B \in \mathscr{M}_n$ let $A \approx B$ if A is obtained from B by changing the signs of all entries in a column or in a row; let $\sim$ be the equivalence relation induced by $\approx$. Define

$$d(n) = \max_{A\in\mathscr{M}_n} \min_{B\sim A} d(B)$$

and

$$D(n) = \min_{A\in\mathscr{M}_n} \max_{B\sim A} d(B).$$

It is rather surprising that $d(n)$ is very small, as shown by the following theorem of Komlós and Sulyok (1970), whose proof is probabilistic.

Theorem 14.23 *If n is sufficiently large, then*

$$d(n) = \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 2, & \text{if } n \text{ is even.} \end{cases}$$ □

Although $D(n)$ is not known with nearly as much precision as $d(n)$, the following rather tight bounds were obtained by Brown and Spencer (1971).

Theorem 14.24 $(2/\pi)^{1/2}n^{3/2} + o(n^{3/2}) \le D(n) \le n^{3/2} + o(n^{3/2})$. □

14.4 Random Elements of Finite Groups

Consider the symmetric group S_n of all $n!$ permutations of $V = \{1, 2, \ldots, n\}$. Turn S_n into a probability space by giving all elements of S_n the same probability and write P_n for the probability in S_n. The elements of the probability space S_n are said to be *random permutations* of V.

Random permutations have been studied by a great many authors, including Landau (1909), Erdős and Szekeres (1934), Goncharov (1942, 1944), Feller (1945), Chowla, Herstein and Moore (1951), Moser and Wyman (1955), Golomb (1964), Shepp and Lloyd (1966), Erdős and Turán (1965, 1967*a*,*b*, 1968), Best (1970) and Vershik and Shmidt (1977, 1978), so we shall only state some of the fundamental results and give some simple arguments, showing the flavour of the subject.

For $\sigma \in S_n$, denote by $X_k(\sigma)$ the number of k-cycles of σ. Then

$$E(X_k) = \binom{n}{k}(k-1)!(n-k)!/n! = \frac{1}{k}$$

and it is easily seen, using Theorem 1.20, that for each fixed k we have $X_k \xrightarrow{d} P_{1/k}$ (Ex. 7). In particular, the probability that a random element of S_n has no fixed point tends to e^{-1}: a rather well-known result. Also, the expected number of cycles (or orbits) is precisely $\sum_{k=1}^{n} 1/k$.

Let us have a look at some more involved r.vs on S_n. Fix a set $R \subset V = \{1, 2, \ldots, n\}, |R| = r \geq 1$. The orbits of a permutation $\sigma \in S_n$ partition V and so induce a *partition* $\pi(\sigma) = \pi(\sigma, R)$ of R. Denote by $I(\sigma) = I(\sigma, R)$ the *set of elements of* $V - R$ *in the orbits of* σ *containing elements of* R. [Thus $R \cup I(\sigma, R)$ is the minimal subset of V containing R and invariant under σ.] By definition, π and I are r.vs on S_n.

Theorem 14.25 *Let ρ be a partition of R: $\cup_1^l R_i, |R_i| = r_i \geq 1, \sum_1^l r_i = r$, and let $K \subset V - R, |K| = k$. Then*

$$\begin{aligned} P_n\{\pi(\sigma) &= \rho \text{ and } |I(\sigma)| = k\} = P_n\{\pi(\sigma) = \rho \text{ and } I(\sigma) = K\}\binom{n-r}{k} \\ &= \binom{r+k-1}{k}\left\{\prod_1^l (r_i - 1)!\right\} \Big/ (n)_r. \end{aligned} \tag{14.17}$$

Proof By symmetry

$$P_n\{\pi(\sigma) = \rho \text{ and } I(\sigma) = K\} = P_n\{\pi(\sigma) = \rho \text{ and } |I(\sigma)| = k\} \Big/ \binom{n-r}{k}.$$

There are $(m-1)!$ cyclic permutations on m given elements. Hence the probability that for given $k_1, k_2, \ldots, k_l$ a permutation $\sigma \in S_n$ contains l orbits $R_1 \cup K_1, R_2 \cup K_2, \ldots, R_l \cup K_l$ with $|K_i| = k_i$ is

$$\binom{n-r}{k_1, \ldots, k_l} \left\{ \prod_1^l (r_i + k_i - 1)! \right\} \Big/ n! = \left\{ \prod_1^l (r_i + k_i - 1)_{r_i - 1} \right\} / (n)_r$$
$$= \frac{\prod_1^l (r_i - 1)!}{(n)_r} \prod_1^l \binom{r_i + k_i - 1}{r_i - 1}.$$

Therefore

$$P\{\pi(\sigma) = \rho \text{ and } |I(\sigma)| = k\} = \frac{\prod_1^l (r_i - 1)!}{(n)_r} \sum{}' \prod_{i=1}^l \binom{r_i + k_i - 1}{r_i - 1}, \quad (14.18)$$

where $\sum'$ denotes summation over all integer sequences $(k_i)_1^l$ with $k_i \geq 0$ and $\sum_1^l k_i = k$. Note that

$$\sum{}' \prod_{i=1}^l \binom{r_i + k_i - 1}{r_i - 1} = \binom{r + k - 1}{r - 1} \quad (14.19)$$

since a summand on the left-hand side counts the number of r-sets of $\{1, 2, \ldots, r - k\}$ whose $(\sum_1^j r_i)$th element is $\sum_1^j (r_i + k_i), j = 1, 2, \ldots, l$. Relations (14.18) and (14.19) imply the assertion. □

Corollary 14.26 *$\pi(\sigma)$ and $I(\sigma)$ are independent r.vs, the distribution of $\pi(\sigma)$ is independent of n,*

$$P_n\{\pi(\sigma) = \rho\} = \frac{1}{r!} \prod_1^l (r_i - 1)!$$

and

$$P_n\{|I(\sigma)| = k\} = \binom{r + k - 1}{k} \Big/ \binom{n}{r}.$$

Proof By Theorem 14.25,

$$P_n\{\pi(\sigma) = \rho\} = \frac{\prod_1^l (r_i - 1)!}{(n)_r} \sum_{k=0}^{n-r} \binom{r + k - 1}{k}$$
$$= \frac{\prod_1^l (r_i - 1)!}{(n)_r} \binom{n}{r} = \frac{1}{r!} \prod_1^l (r_i - 1)!$$

and so

$$P_n\{\pi(\sigma) = \rho \text{ and } |I(\sigma)| = k\} / P_n\{\pi(\sigma) = \rho\} = \binom{r + k - 1}{k} \Big/ \binom{n}{r}. \quad \square$$

For $\sigma \in S_n$ define $W_1(\sigma) = 1$, and if $h \geq 2$,

$$W_h(\sigma) = \begin{cases} 1, & \text{if } h \notin I(\sigma, \{1, \dots, h-1\}), \\ 0, & \text{otherwise.} \end{cases}$$

Note that σ has $W_1 + W_2 + \cdots + W_n$ cycles.

Theorem 14.27 *The Bernoulli r.vs $W_1, \dots, W_n$ are independent and satisfy $P(W_h = 1) = 1/h, h = 1, \dots, n$.*

Proof Since $(W_1, \dots, W_h)$ is a function of $\pi(\sigma, \{1, \dots, h\})$ and W_{h+1} is a function of $I(\sigma, \{1, \dots, h\})$, the independence of the W_i follows from Corollary 14.26. Furthermore, $W_h(\sigma) = 1$ iff in the partition $\pi(\sigma, \{1, \dots, h\})$ the class containing h contains only h. By Corollary 14.26 the probability of this is precisely the probability that a random permutation on $\{1, 2, \dots, h\}$ fixes $h : P_h\{\sigma(h) = h\} = 1/h$. □

As an immediate consequence of Theorem 14.27, we see again that the expected number of cycles is $\sum_{k=1}^n 1/k$. Furthermore, the variance of the number of cycles is $\sum_{h=1}^n (h-1)/h^2 \sim \log n$, and from Theorem 14.27 one can deduce the following result of Goncharov (1944). [In fact, there are more straightforward ways of deducing this result; see Feller (1966, vol. I, p. 258).]

Theorem 14.28 *Denote by $U_n = U_n(\sigma)$ the number of cycles in σ. Then $(U_n - \log n)/(\log n)^{1/2} \xrightarrow{d} N(0, 1)$.*

Let us turn to more substantial matters. What is the expected length of a longest cycle? What is the asymptotic distribution of the order of a random permutation? The first question was answered by Golomb (1964) and Shepp and Lloyd (1966).

Theorem 14.29 *Denote by $L_n = L_n(\sigma)$ the length of a longest cycle of $\sigma \in S_n$. Then $E(L_n)/n$ is monotone decreasing and*

$$\begin{aligned} \lim_{n \to \infty} E(L_n)/n &= \int_0^\infty \exp\{-x - \int_x^\infty (\mathrm{e}^{-y}/y) \mathrm{d}y\} \mathrm{d}x \\ &= 0.62432965 \dots . \end{aligned}$$

The second question is answered by the following deep theorem of Erdős and Turán (1968).

Theorem 14.30 *Denote by $O_n = O_n(\sigma)$ the order of $\sigma \in S_n$. Then*

$$\frac{\log O_n - \frac{1}{2}\log^2 n}{(\frac{1}{3}\log^3 n)^{1/2}} \xrightarrow{d} N(0,1). \qquad \square$$

The result is rather surprising since, at the first sight, O_n hardly seems to be concentrated about $n^{(\log n)/2}$. Indeed, already Landau (1909) had proved that with $\tilde{O}_n = \max\{O_n(\sigma) : \sigma \in S_n\}$, we have

$$\lim_{n\to\infty} \frac{\log \tilde{O}_n}{\sqrt{n \log n}} = 1,$$

so S_n contains a permutation whose order is almost $e^{(n \log n)^{1/2}}$ and, on the other hand, S_n contains $(n-1)! = (1/n)n!$ cyclic permutations, each with order n.

The study of random elements of Abelian groups was initiated by Erdős and Rényi (1965). They were mostly interested in the representability of elements as sums of elements belonging to a randomly chosen small set. Let $(A_n, +)$ be an Abelian group of order n; turn A_n into a probability space by giving all elements probability $1/n$. Let us choose k random elements of A_n, say $a_1, a_2, \ldots, a_k$, and for $b \in A_n$ denote by $R(b) = R_k(b)$ the number of ways b can be represented as

$$b = \varepsilon_1 a_1 + \varepsilon_2 a_2 + \cdots + \varepsilon_k a_k,$$

where $\varepsilon_i = 0$ or 1 (memories of the cube Q^k!). How large should we choose k to guarantee that, with large probability, every b has at least one such representation. Trivially, k must be at least $\log_2 n$ since, if all n elements are representable, then $2^k \geq n$. In fact, the mean

Erdős and Rényi (1965) proved that a slightly larger k will suffice.

Theorem 14.31 *If $\omega(n) \to \infty$ and*

$$k \geq \log_2 n + \log_2 \log n + \omega(n),$$

then, almost surely, we have $R(b) \geq 1$ for all $b \in A_n$.

The resemblance of this theorem to many of the theorems in this book is not merely superficial. In fact, a weaker form of this theorem is easily proved by the familiar second moment method (Ex. 8). Many extensions and variants of this result have been proved; see, for example, Miech (1967), Hall (1972, 1977), Hall and Sudbery (1972), Wild (1973) and Erdős and Hall (1976, 1978). Here we only state a beautiful result of Erdős and Hall (1978). For $r \geq 0$, denote by $D(r)$ the number of elements b of A_n for which $R(b) = r$, and set $d(r) = D(r)/n$.

Theorem 14.32 *Suppose for each fixed positive integer r, the number of elements of A_n of order r is $o(n)$. Let $k = k(n) = \log_2 n + O(1)$ and set $\lambda = \lambda(n) = 2^k/n$. Then for each fixed integer $r \geq 0, d(r) - (\lambda^r/r!)e^{-\lambda} \to 0$ in probability.* □

14.5 Random Mappings

Although we shall work with a base set of cardinality n, it is more natural to denote it by X rather than our usual V. So let $X = \{1, 2, \dots, n\}$ and let $\mathscr{F} = X^X$ be the set of all n^n maps from X to X. Clearly the set $\mathscr{F}$ can be identified with the collection $\mathscr{D}$ of all directed graphs with loops, in which every vertex has outdegree 1. The directed graph D_f corresponding to a map $f \in \mathscr{F}$ is such that D_f has an arc (or loop) $\vec{ij}$ iff $f(i) = j$. Endow $\mathscr{F}$ (and so $\mathscr{D}$) with the uniform distribution. Then every invariant of a map $f \in \mathscr{F}$ (graph $D_f \in \mathscr{D}$) becomes an r.v. and we can speak of a *random map* or a *random function* and a *random mapping digraph* (r.m.d.).

Occasionally we shall disregard the orientation of the arc of D_f. Then we write G_f instead of D_f; the graph G_f is a *random mapping graph* (r.m.g.). Calling loops and double edges cycles, we see that every component of G_f is unicyclic.

The space of r.m.gs G_f is almost the same as $\mathscr{G}(n, \text{1-out})$. Indeed, the graphs $G_{1\text{-out}}$ are precisely the loopless graphs G_f. The number of loops has asymptotically Poisson distribution with mean 1 [see Theorem 14.33(ii)], so most results concerning the graphs G_f carry over to the graphs $G_{1\text{-out}}$, perhaps with an additional factor e (see Ex. 11).

Random mappings have been studied in great detail in a host of papers: Kruskal (1954), Rubin and Sitgreaves (1954), Katz (1955), Folkert (1955), Harris (1960), Riordan (1962), Stepanov (1969*a*, *b*, *c*, 1971), H. Frank and Frisch (1971), Proskurin (1973), Sachkov (1973), Kolchin (1977), Bagaev (1977), Gertsbakh (1977), Burtin (1980), Ross (1981) and Pittel (1983). We shall not attempt to do justice to all the results, but we shall try to give back the flavour of the investigations. In fact, we have already touched on the subject: Lemma 5.17 and Theorem 5.18 are, as we shall see, results about r.m.gs.

A random map has a good many invariants. Let $f \in \mathscr{F}$. Given $x \in X$, write $\alpha(x)$ for the number of 'descendants' of x under f and $\beta(x)$ for the number of 'ancestors':

$$\begin{aligned} \alpha(x) &= |\{f^k(x) : k = 0, 1, \dots\}|, \\ \beta(x) &= |\{y : f^k(y) = x \text{ for some } k, k = 0, 1, \dots\}|, \end{aligned}$$

where f^0 is the identity map: $f^0(x) = x$. Furthermore, let $\delta(x)$ be the number of vertices on the cycle in the component of G_f containing x. Thus $\delta(x) = 1$ if the component contains a loop and $\delta(x) = 2$ if it contains a double edge. Since the probability distributions of $\alpha(x), \beta(x)$ and $\delta(x)$ do not depend on x, we shall suppress the variable x.

Let us denote by γ the number of cycles in G_f, by $\bar{\gamma}$ the number of elements on the cycles and by γ_m the number of cycles of length m. Thus $\gamma = \sum_{m=1}^n \gamma_m$ and $\bar{\gamma} = \sum_{m=1}^n m\gamma_m$. By definition the range of the variables $\alpha, \beta, \gamma, \bar{\gamma}$ and δ is $\{1, 2, \ldots, n\}$, and the range of γ_m is $\{1, 2, \ldots, \lfloor n/m \rfloor\}$. Since the components of G_f are unicyclic, γ is not only the number of cycles, but also the number of components. The basic properties of the distributions of $\alpha, \beta, \gamma, \bar{\gamma}, \gamma_m$ and δ, proved by Rubin and Sitgreaves (1954), Katz (1955), Harris (1960), Stepanov (1969*c*) and Ross (1981), are collected in the following theorem.

Theorem 14.33

(i) $P(G_f \text{ is connected}) = P(\gamma = 1) = \frac{1}{n} \sum_{r=1}^{n} \prod_{j=0}^{r-1} \left(1 - \frac{j}{n}\right)$

$$= \frac{(n-1)!}{n^n} \sum_{j=0}^{n-1} \frac{n^j}{j!} \sim \left(\frac{\pi}{2}\right)^{1/2} n^{-1/2}.$$

(ii) *For* $1 \le r \le n$,

$$E(\gamma_r) = \frac{1}{r} \prod_{j=0}^{r-1} \left(1 - \frac{j}{n}\right).$$

For every fixed r *we have* $\gamma_r \xrightarrow{d} P_{1/r}$.

(iii)

$$E(\gamma) = \sum_{r=1}^{n} \frac{1}{r} \prod_{j=0}^{r-1} \left(1 - \frac{j}{n}\right) \sim \log n$$

and

$$\begin{aligned} \sigma^2(\gamma) &= \sum_{r=1}^{n} \frac{1}{r} \prod_{j=0}^{r-1} \left(1 - \frac{j}{n}\right) \\ &\quad + \sum_{r=1}^{n-1} \frac{1}{r} \prod_{j=0}^{r-1} \left(1 - \frac{j}{n}\right) \sum_{s=1}^{n-r} \frac{1}{S} \prod_{h=0}^{s-1} \left(1 - \frac{r+h}{n}\right) \\ &\quad - \left\{ \sum_{r=1}^{n} \frac{1}{r} \prod_{j=0}^{r-1} \left(1 - \frac{j}{n}\right) \right\}^2. \end{aligned}$$

(iv) For $1 \leq k \leq n$,

$$P(\alpha = k) = P(\bar{\gamma} = k) = \frac{k}{n}(n)_k n^{-k} = \frac{k}{n}\prod_{j=0}^{k-1}\left(1 - \frac{j}{n}\right).$$

(v) For $1 \leq l \leq n$,

$$P(\delta = l) = \frac{1}{n}\sum_{k=l}^{n}(n)_k n^{-k} = \frac{1}{n}\sum_{k=l}^{n}\prod_{j=0}^{k-1}\left(1 - \frac{j}{n}\right).$$

(vi) $E(\alpha) = E(\beta) = E(\bar{\gamma}) \sim (\pi n/2)^{1/2}$.

(vii) $E(\delta) = E(\alpha/2) + \frac{1}{2} \sim \frac{1}{4}(2\pi n)^{1/2}$.

Proof (i) The number of connected r.m.ds is $\sum_{k=1}^{n}(n)kn^{n-k-1}$, since there are $\binom{n}{k}(k-1)!$ ways of forming a directed cycle of length k and kn^{n-k-1} ways of extending this cycle to a r.m.d. (see Lemma 5.17 and Theorem 5.18). As there are n^n r.m.ds, the exact formula for $P(\gamma = 1)$ follows. To see the asymptotic formula note that, as in the proof of Theorem 5.18,

$$\frac{1}{n}\sum_{r=1}^{n}\prod_{j=0}^{r-1}\left(1 - \frac{j}{n}\right) \sim \frac{1}{n}\int_0^\infty e^{-x^2/2n}dx = \frac{1}{\sqrt{n}}\int_0^\infty e^{-y^2/2}dy = \left(\frac{\pi}{2}\right)^{1/2} n^{-1/2}.$$

(ii) and (iii). The expected number of cycles of length r is

$$E(\gamma_r) = \binom{n}{r}(r-1)!n^{-r}$$

since n^{n-r} r.m.ds contain a given oriented cycle of length r. Hence

$$\begin{aligned} E(\gamma) &= \sum_{r=1}^{n}\frac{1}{r}\prod_{j=0}^{r-1}\left(1 - \frac{j}{n}\right) \sim \int_1^\infty x^{-1}e^{-x^2/(2n)}dx = \frac{1}{2}\int_1^\infty y^{-1}e^{-y/(2n)}dy \\ &= \frac{1}{2}E_1\left(\frac{1}{2n}\right) = -\frac{1}{2}Ei\left(-\frac{1}{2n}\right) = -\frac{1}{2}li(e^{-1/2n}) \sim \log n, \end{aligned}$$

using a well-known approximation of the exponential integral [see Abramowitz and Stegun (1972, pp. 228–229) or Ryshik and Gradstein (1963, vol. II, p. 291)].

Clearly

$$E_2(\gamma) = E\{\gamma(\gamma - 1)\} = \sum_{r=1}^{n-1}\binom{n}{r}(r-1)!n^{-r}\sum_{s=1}^{n-r}\binom{n-r}{s}(s-1)!n^{-s},$$

which implies the expression for $\sigma^2(\gamma)$.

For r and s fixed, the sth factorial moment of γ_r is

$$E_s(\gamma_r) = \binom{n}{r}\binom{n-r}{r}\cdots\binom{n-(s-1)r}{r}\{(r-1)!\}^s n^{-sr} \sim \left(\frac{1}{r}\right)^s.$$

Hence by Theorem 1.20 we have $\gamma_r \xrightarrow{d} P_{1/r}$.

(iv) and (v). First we determine the joint distribution of α and δ. By definition, $\delta(x) \leq \alpha(x)$ for every function f. Furthermore, for $1 \leq l \leq k \leq n$ we have

$$\begin{aligned} P(\alpha = k, \delta = l) \;=\; & P\{f^r(x) \notin \{x, f(x), \ldots, f^{r-1}(x)\}, \\ & \qquad 0 < r \leq k-1, \text{ and } f^k(x) = f^{k-l}(x)\} \end{aligned}$$

and so

$$P(\alpha = k, \delta = l) = (n-1)_{k-1} n^{-k} = (n)_k n^{-k-1}.$$

Summing over l and k we have

$$P(\alpha = k) = k(n)_k n^{-k-1},$$

and

$$P(\delta = l) = \sum_{k=l}^{n} (n)_k n^{-k-1}.$$

As a consequence of these formulae, we see also that

$$E(\delta) = E\{(\alpha + 1)/2\}.$$

Let us turn to $\bar{\gamma}$, the number of vertices on cycles. Given a set of cycles on k vertices there are $F(n,k) = kn^{n-k-1}$ digraphs D_f in which these are exactly the cycles. Since a partition of a set into oriented cycles corresponds to a permutation of the set,

$$P(\bar{\gamma} = k) = \binom{n}{k} kn^{n-k-1} k! n^{-n} = k(n)_k n^{-k-1}.$$

(vi) and (vii). By symmetry the number of functions $f \in \mathscr{F}$ for which y is a descendant of x is equal to the number of functions for which x is a descendant of y, i.e. for which y is an ancestor of x. Hence $E(\alpha) = E(\beta)$. Perhaps the simplest way to see the approximations is to determine first the asymptotic density of $\delta/\sqrt{n}$ (see Ex. 10). $\square$

Let us introduce another invariant of G_f. Delete all edges of G_f which belong to cycles. The remaining graph is a forest consisting of $\bar{\gamma}$ trees. Call the components of G_f the *trees* of G_f. Denote by τ_m the number of trees of order m and by $\tau(m) = \sum_{k=m}^{n} \tau_k$ the number of trees of order at least m. How large a tree is G_f likely to contain? The surprising answer that with probability bounded away from 0 there are trees of order at least cn, is due to Stepanov (1969c).

Theorem 14.34 *For* $1 \le m \le n$ *we have*

$$E(\tau_m) = \frac{n!}{n^n} \frac{n^{m-1}}{m!} \sum_{k=0}^{n-m} \frac{(n-m)^k}{k!}.$$

If $\min\{n-m, m\} \to \infty$, *then*

$$E(\tau_m) \sim \frac{1}{2} \frac{n^{1/2}}{m^{3/2}}. \tag{14.20}$$

Finally, if $0 < c < 1$ *and* $m \sim cn$, *then*

$$E\{\tau(m)\} \sim c^{-1/2} - 1. \tag{14.21}$$

Proof What is the expected number of trees of order m for which the unique cycle in the component containing the tree has $r+1$ edges? There are $\binom{n}{m}$ ways of selecting the vertex set of the tree and m^{m-1} ways of selecting a rooted spanning tree on that set. There are $(n-m)_r$ ways of attaching a directed $(r+1)$-cycle to the root and $(n-m)^{n-m-r}$ ways of extending the union of our tree and cycle to a r.m.d. Hence

$$\begin{aligned} E(\tau_m) &= \sum_{r=0}^{n-m} \binom{n}{m} m^{m-1} (n-m)_r (n-m)^{n-m-r} n^{-n} \\ &= \frac{n!}{n^n} \frac{m^{m-1}}{m!} \sum_{k=0}^{n-m} \frac{(n-m)^k}{k!}. \end{aligned}$$

To see the last equality, set $k = n - m - r$.

The sum

$$\sum_{k=0}^{n-m} \frac{(n-m)^k}{k!} e^{-(n-m)}$$

is precisely the probability that a Poisson r.v. with mean $n-m$ does not exceed its mean. Since $(P_\lambda - \lambda)/\sqrt{\lambda} \xrightarrow{d} N(0,1)$ (see the remark after

Theorem 1.21),

$$\sum_{k=0}^{n-m} \frac{(n-m)^k}{k!} e^{-(n-m)} = \frac{1}{2}(1+\varepsilon_{n-m}),$$

where $\varepsilon_l \to 0$ as $l \to \infty$. Consequently

$$E(\tau_m) = (1+\varepsilon_{n-m})\frac{1}{2}\frac{n!}{n^n}\frac{m^{m-1}}{m!}e^{-(n-m)}. \tag{14.22}$$

Relation (14.20) follows from (14.22) by applying Stirling's formula.

Finally, suppose c is fixed, $0 < c < 1$, and $m \sim cn$. Then by (14.22) and (14.20)

$$\begin{aligned} E\{\tau(m)\} = E\left(\sum_{k=m}^{n} \tau_k\right) &\sim \frac{1}{2}\sum_{k=m}^{n} \frac{n^{1/2}}{k^{3/2}} = \frac{1}{2}\sum_{k=m}^{n}(k/n)^{-3/2}\frac{1}{n} \\ &\sim \frac{1}{2}\int_c^1 x^{-3/2}\mathrm{d}x = \frac{1}{\sqrt{c}} - 1. \qquad \square \end{aligned}$$

Corollary 14.35 *Denote by τ^* the maximal tree size in a r.m.g. Then for $\frac{1}{2} < c \le 1$ we have* $\lim_{n\to\infty} P(\tau^*/n \ge c) = (1/\sqrt{c}) - 1$.

Proof Clearly $\tau^*/n \ge c$ iff $\tau(\lceil cn \rceil) \ge 1$. Furthermore, a r.m.g. G_f cannot contain two trees each with more than $n/2$ vertices, so $\tau(\lceil cn \rceil)$ takes only two values, 0 and 1. Hence

$$P(\tau^*/n \ge c) = P\{\tau(\lceil cn \rceil) = 1\} = E\{\tau(\lceil cn \rceil)\} \sim (1/\sqrt{c}) - 1. \qquad \square$$

Theorem 14.33 and Corollary 14.35 show that random mappings are rather peculiar : with high probability there are exceptionally large trees, i.e. there are vertices with exceptionally many ancestors. On the other hand, the number of cyclic vertices is only of order $\sqrt{n}$.

A random mapping digraph was proposed by Gertsbakh (1977) as a model for an epidemic process: X is the population, initially a subset A of X is infected with a contagious disease and the disease spreads to other elements of X according to some rule depending on a r.m.d. D_f. There are three obvious possibilities: the disease spreads only forwards along an arc, it spreads only backwards, or it spreads in both directions. In this way we get direct, inverse and two-sided epidemic processes.

For a function $f \in \mathscr{F}$ let $f^* : X \to \mathbb{P}(X)$ be defined by

$$f^*(x) = \{f(x)\} \cup f^{-1}(x).$$

Given a set $A \subset X$, denote by $\hat{f}(A), \hat{f}^{-1}(A)$ and $\hat{f}^*(A)$ the transitive closures of A under f, f^- and f^*, respectively. Thus $\hat{f}(A)$ is the set of all descendants of elements of A and $\hat{f}^*(A)$ is the minimal subset B of X which contains A and satisfies $f^*(b) \subset B$ for every $b \in B$. Clearly

$$\xi(A) = |\hat{f}(A)|, \eta(A) = |\hat{f}^{-1}(A)| \text{ and } \zeta(A) = |\hat{f}^*(A)|$$

are the number of elements which are eventually infected if the disease is initially confined to A and then spreads according to the function f and the rules above.

Gertsbakh (1977) posed a number of interesting questions. For how large a set A are we likely to end up with at least a fixed proportion of infected elements? Is there a *threshold function* $m_0 = m_0(n)$ in the sense that if $|A| = o(m_0)$, then for a.e. function (in the usual r.g. sense) only $o(n)$ of the elements will be infected but if $|A|/m_0 \to \infty$ then for a.e. function $n - o(n)$ elements will be infected? Or, simply, what can we say about the distributions of $\xi(A), \eta(A)$ and $\zeta(A)$? As these distributions depend only on $|A|$, for $|A| = m$ we may write ξ_m, η_m and ζ_m instead of $\xi(A), \eta(A)$ and $\zeta(A)$. Note that $\xi_1 = \alpha$ and $\eta_1 = \beta$. Each of the r.vs ξ_m, η_m and ζ_m has range $\{m, m+1, \dots, n\}$.

It so happens that η_m, the r.v. associated with the inverse epidemic process, is the easiest to handle. Fortunately, as far as threshold functions are concerned, it is also the most interesting.

The probability that in an inverse epidemic process a single element infects the entire set was determined by Gertsbakh (1977).

Theorem 14.36

$$P(\eta_1 = n) = P(\beta = n) = 1/n.$$

Proof When does an element x infect the entire set? If and only if G_f is connected and x is on the unique cycle of G_f. Hence, arguing as in the proof of Theorem 14.33(i) and making use of Theorem 14.33(iv),

$$\begin{aligned} P(\eta_1 = n) &= \sum_{k=1}^{n} \frac{k}{n} \binom{n}{k} (k-1)! k n^{n-1-k} n^{-n} \\ &= \frac{1}{n} \sum_{k=1}^{n} \frac{k}{n} (n)_k n^{-k} = \frac{1}{n} \sum_{k=1}^{n} P(\alpha = k) = \frac{1}{n}. \qquad \square \end{aligned}$$

In preparation for an attack on η_m, we look at a random digraph slightly different from D_f. Let $\tilde{Y} = \{Y_1, Y_2, \dots, Y_n\}$ be a family of $n \geq 0$

independent r.vs with

$$P(Y_i = j) = \lambda_j, \quad j = 0, 1, \ldots, n \text{ and } \sum_{j=0}^{n} \lambda_j = 1.$$

Construct a random digraph $D_{\tilde{Y}}$ on $\{0, 1, \ldots, n\}$ by sending an arc from i to j whenever $Y_i = j$. For $S \subset X = \{1, 2, \ldots, n\}$ set $\lambda(S) = \sum_{i \in S} \lambda_i$. The following result is due to Ross (1981).

Theorem 14.37 $P(D_{\tilde{Y}}$ *is connected*$) = \lambda_0$.

Proof We apply induction on n. If $\lambda_0 = 1$ or $n \in \{0, 1\}$, then the result is trivial, so suppose $\lambda_0 < 1$ and $n \geq 2$.

Given a set $S \subset X$, let $D_{\tilde{Y}}/S$ be the digraph obtained from $D_{\tilde{Y}}$ by collapsing $S \cup \{0\}$ to a single vertex. Clearly

$$P(D_{\tilde{Y}} \text{ is connected } |\{i : Y_i = 0\} = S) = P(D_{\tilde{Y}}/S \text{ is connected}) = \frac{\lambda(S)}{1 - \lambda_0},$$

where the second inequality follows from the induction hypothesis, with $S \cup \{0\}$ playing the role of the distinguished vertex 0. Consequently

$$\begin{aligned}
P(D_{\tilde{Y}} \text{ is connected}) &= \sum_{\substack{S \subset X \\ S \neq \emptyset}} \lambda_0^{|S|} (1 - \lambda_0)^{n - |S|} \frac{\lambda(S)}{1 - \lambda_0} \\
&= \sum_{k=1}^{n} \sum_{\substack{S \subset X \\ |S| = k}} \lambda_0^k (1 - \lambda_0)^{n-k-1} \sum_{i \in S} \lambda_i \\
&= \sum_{i=1}^{n} \lambda_i \sum_{k=1}^{n} \binom{n-1}{k-1} \lambda_0^k (1 - \lambda_0)^{n-k-1} \\
&= \frac{\lambda_0}{1 - \lambda_0} \sum_{i=1}^{n} \lambda_i \sum_{k=1}^{n} \binom{n-1}{k-1} \lambda_0^{k-1} (1 - \lambda_0)^{n-k} \\
&= \frac{\lambda_0}{1 - \lambda_0} (1 - \lambda_0) = \lambda_0.
\end{aligned}$$

□

The exact distribution of η_m was determined by Burtin (1980); it is, in fact, a simple consequence of Theorem 14.37.

Theorem 14.38 *For* $1 \leq m \leq n$ *and* $0 \leq s \leq n - m$

$$P(\eta_m = s) = \frac{m}{m+s} \binom{n-m}{s} \left(\frac{s+m}{n}\right)^s \left(\frac{n-m-s}{n}\right)^{n-m-s}.$$

Proof Let $A \subset X, B \subset X \backslash A, |A| = m$ and $|B| = s$. Denote by C the event that, starting from A, B will be the set of infected elements in the inverse epidemic process. Furthermore, let C_1 be the event that $f(B) \subset A \cup B, C_2$ be the event that $f(X \backslash A \cup B) \subset X \backslash A \cup B$ and C_3 be the event that for every $b \in B$ there is an oriented path whose initial vertex is b and which ends in A. Clearly $C = C_1 \cap C_2 \cap C_3$ and the events C_1 and C_2 are independent. Furthermore,

$$P(C_1) = \left(\frac{m+s}{n}\right)^s \text{ and } P(C_2) = \left(\frac{n-m-s}{n}\right)^{n-m-s}.$$

What is $P(C_3|C_1 \cap C_2)$? It is the probability that the subgraph of the random mapping graph on $A \cup B$ formed by the arcs starting in B becomes connected when we collapse A to a single vertex. By Theorem 14.37 this probability is $m/(m+s)$.

Putting all these together, we find that

$$\begin{aligned} P(\eta_m = m+s) &= \binom{n-m}{s} P(C_3|C_1 \cap C_2) P(C_1) P(C_2) \\ &= \binom{n-m}{s} \frac{m}{m+s} \left(\frac{m+s}{n}\right)^s \left(\frac{n-m-s}{n}\right)^{n-m-s}. \quad \square \end{aligned}$$

Burtin (1980) used Theorem 14.38 to determine the asymptotic distribution of η_m. The standard calculations are left to the reader.

Theorem 14.39 *(i) If $m = o(n^{1/2})$ and $m \to \infty$, then n_m/m^2 converges in distribution to a r.v. with density*

$$(1/\sqrt{2\pi})x^{-3/2}e^{-1/(2x)}, \quad 0 < x < \infty.$$

(ii) If $m \sim cn^{1/2}$ for some positive constant c, then η_m/n converges in distribution to a r.v. with density

$$(c/\sqrt{2\pi})x^{-3/2}(1-x)^{-1/2}e^{-c^2(1-x)/2x}, \quad 0 < x < \infty.$$

(iii) If $m = o(n)$ and $m/n^{1/2} \to \infty$, then $(m^2/n^2)(n - \eta_m)$ converges in distribution to a r.v. with density

$$(1/\sqrt{2\pi x})e^{-x/2}, \quad 0 < x < \infty.$$

Quite crudely, Theorem 14.39 tells us that our process has a threshold function.

Corollary 14.40 *$m_0 = n^{1/2}$ is a threshold function for the inverse epidemic process.* $\square$

The asymptotic distributions of ξ_m and ζ_m were determined by Pittel (1983). These results are considerably more difficult to prove than Theorems 14.38 and 14.39; for the proofs the reader is referred to the original paper.

Theorem 14.41 *If $m = o(n)$ and $m \to \infty$, then ξ_m is asymptotically normal with mean $(2mn)^{1/2}$ and variance $n/2$ and ζ_m is asymptotically $Z^2/2$, where Z is an $N(0,1)$ r.v.* □

From this theorem we can find the threshold functions for the direct and two-sided epidemic process; in a way the results are disappointing: the threshold functions are extreme in both cases.

Corollary 14.42 *(i) If $m = o(n)$ and $m \to \infty$, then, starting with m infected elements, in the direct epidemic process the number of eventually infected elements is of order $(nm)^{1/2}$. In particular, $m_0 = n$ is a threshold function for the direct epidemic process.*

(ii) If $m \to \infty$, then in the two-sided epidemic process almost all elements will be infected, provided we start with m infected elements. In particular, $m_0 = 1$ is a threshold function for the two-sided epidemic process. □

In fact, the expected number of elements infected by a single element in a two-sided epidemic process is about $\frac{2}{3}n$ (see Exx. 14 and 15).

Exercises

14.1 Given a graph G of order n, consider a one-to-one map $f : V(G) \to \{0, 1, \ldots, n-1\}$, called a *numbering* of G, and set

$$a(f, G) = \sum \{|f(x) - f(y)| : xy \in E(G)\}.$$

Show that for the cube Q^n with $V(Q^n) = \{0, 1, \ldots, 2^n - 1\}, a(f, Q^n)$ is minimized by the natural numbering $f(i) = i, i = 0, 1, \ldots, 2^n - 1$. (Harper, 1964, 1966*a*.)

14.2 The *bandwidth* bw (G) of a graph G is

$$\mathrm{bw}(G) = \min_f \max\{|f(x) - f(y)| : xy \in E(G)\},$$

where the minimum is taken over all numberings of G (see Ex. 1). Show that the bandwidth of the cube Q^n is attained by a numbering for which $0, 1, \ldots, \sum_{i=1}^{j} \binom{n}{i} - 1$ are assigned to the vertices with at most j digits 1. (Harper, 1966*a*,*b*.)

14.3 Prove that for $\varepsilon > 0$ there is a constant $c = c(\varepsilon)$ such that a.e. $G_{c/n}$ has bandwidth at least $(1-\varepsilon)n$ (see Ex. 2). [Note that if f is a numbering of $G_{c/n}$ with $|f(x) - f(y)| < (1-\varepsilon)n$ for all $xy \in E(G_{c/n})$, then no edge joins the set $\{x : f(x) \leq (\varepsilon/2)n - 1\}$ to the set $\{y : f(y) \geq (1-\varepsilon/2)n - 1\}$. However, if c is sufficiently large, then a.e. $G_{c/n}$ is such that any two sets of $\lfloor(\varepsilon/2)n\rfloor$ vertices are joined by an edge (Ex. 12 of Chapter 7). This result is a weaker form of a theorem of de la Vega (1983*b*).]

14.4 Let X and Y be independent identically distributed random vectors in a d-dimensional Euclidean space. Use Turán's theorem for triangles to deduce that

$$P(|X+Y| \geq x) \geq \frac{1}{2}P^2(|X| \geq x).$$

14.5 By considering scalar products show that if $a_1, a_2, \ldots, a_{d+2} \in \mathbb{R}^d$ and $|a_i| \geq 1$ for each i, then $|a_i + a_j| \geq \sqrt{2}$ for some $i \neq j$. Use this and Turán's theorem to deduce that if X and Y are identically distributed random vectors in $\mathbb{R}^d$, then

$$P(|X+Y| \geq x) \geq (1/d+1)P^2(|X| \geq x/\sqrt{2}).$$

(Katona, 1977.)

14.6 For $1 \leq p < \infty$ write $\|\cdot\|_p$ for the p-norm: $\|(x_i)_1^n\|_p = (\sum_{i=1}^n x_i^p)^{1/p}$. Define $f_p(n)$ analogously to $f_2(n)$ and $f_\infty(n)$:

$$f_p(n) = \max_{(S_i)} \min_{(R,B)} \|\{\text{disc } (S_i)\}_{i=1}^n\|_p.$$

Show that the analogue of (14.14) holds:

$$f_p(n) = \max_m \max_{u_j \in Q^n} \min_{\varepsilon_j = \pm 1} \left\| \sum_{j=1}^m \varepsilon_j u_j \right\|_p.$$

Deduce from Theorems 14.21 and 14.22 that for $2 \leq p_1 < p_2 < \infty$ we have

$$f_2(n)n^{1/p_1 - 1/2} \leq f_{p_1}(n) \leq f_{p_2}(n) \leq f_\infty(n)n^{1/p_2}.$$

In particular, there are absolute constants c_1 and c_2 such that, for $2 \leq p < \infty$,

$$c_1 n^{1/2+1/p} \leq f_p(n) \leq c_2 n^{1/2+1/p}.$$

(Spencer, 1981.)

14.7 Consider a shuffling procedure for a full deck of 52 cards. Assuming that 52 is large enough for Theorem 14.29, show that with probability about $\frac{1}{2}$ we need only 2600 repetitions to return to the original order, although in the worst case we may need 180,180 shuffles.

14.8 With the notation used in the discussion of Theorems 14.31 and 14.32, prove that

$$E\left[\sum_{b\in A_n}\{R_k(b)-2^k/n\}^2\right]=2^k\left(1-\frac{1}{n}\right).$$

Use Chebyshev's inequality to deduce that if $k \leq 2\log_2 n+\omega(n)$, then, almost surely,

$$R_k(b)=(2^k/n)\{1+o(1)\} \text{ for every } b\in A_n.$$

14.9 (Ex. 8 ctd.) Suppose every non-identity element of A_n has order 2. Show that if $k-\log_2 n\to\infty$, then, almost surely,

$$R_1(b)\geq 1 \text{ for every } b\in A_n.$$

[Note that A_n is a vector space over $\mathbb{Z}_2$; set up a Markov chain whose states are dimensions of subspaces of A_n.]

14.10 Use Theorem 14.33(v) and Stirling's formula to show that the asymptotic density of $(\alpha/\sqrt{n},\delta/\sqrt{n})$ is

$$f(x,y)=\begin{cases} e^{-x^2/2}, & \text{if } 0\leq y\leq x<\infty,\\ 0, & \text{if otherwise.}\end{cases}$$

Prove that $\alpha/\sqrt{n}$ and $\delta/\sqrt{n}$ have asymptotic densities $x\,e^{-x^2/2}(x\geq 0)$ and $2\pi\{1-\Phi(x)\}(x\geq 0)$. Deduce that $E(\delta)\sim\frac{1}{4}(2\pi n)^{1/2}$, as claimed in Theorem 14.33(vii).

14.11 Deduce from Theorem 14.33(i) or from Theorem 5.18 that

$$P(G_{1\text{-out}} \text{ is connected})\sim e\left(\frac{\pi}{2}\right)^{1/2}n^{-1/2}.$$

14.12 Denote by $\gamma(s)$ the number of cycles of length at least s in an r.m.g. G_f. Prove that for $s\sim cn, 0<c<1$, we have

$$E\{\gamma(s)\}\sim\log(1/c).$$

(Stepanov, 1969*c*.)

14.13 Alter the definition of an inverse epidemic process so that loops are not allowed. Prove that the probability that a single element infects the entire set tends to e/n.

[cf. Theorem 4; Gertsbakh (1977).]

14.14 Deduce from relation (14.31) that in a two-sided epidemic process a positive proportion of the elements is expected to be infected by a single element:

$$\varliminf_{n\to\infty} E(\xi_1)/n > 0.$$

14.15 Give an explicit formula for $E(\xi_1)$ and deduce that

$$\lim_{n\to\infty} E(\xi_1)/n = \tfrac{2}{3}.$$

(Pittel, 1983.)

15

Sorting Algorithms

Random graph techniques are very useful in several areas of computer science. In this book we do not intend to present a great variety of such applications, but we shall study a small group of problems that can be tackled by random graph methods.

Suppose we are given n objects in a linear order unknown to us. Our task is to determine this linear order by as few *probes* as possible, i.e. by asking as few *questions* as possible. Each probe or question is a binary comparison: which of two given elements a and b is greater? Since there are $n!$ possible orders and k questions result in 2^k different sequences of answers, $\log_2(n!) = \{1 + o(1)\}n \log_2 n$ questions may be needed to determine the order completely. It is only a little less obvious that with $\{1 + o(1)\}n \log_2 n$ questions we can indeed determine the order. However, if we wish to use only $\{1+o(1)\}n \log_2 n$ questions, then our later questions have to depend on the answers to the earlier questions. In other words, our questions have to be asked in many *rounds*, and in each round they have to be chosen according to the answers obtained in the previous rounds.

For a sorting algorithm, define the *width* as the maximum number of probes we perform in any one round and the *depth* as the maximal number of rounds needed by the algorithm. Thus the width corresponds to the number of parallel processors we design our (parallel sorting) algorithm for and the depth is then the (parallel) time that may be required by the algorithm. The *size* of an algorithm is the number of probes; as we mentioned, this information theoretic lower bound on the size of a sorting algorithm is $\log_2(n!)$. What is then the minimal size of a sorting algorithm of given depth?

Equivalently, how many parallel processors do we need if we wish to be able to sort n objects in time r, i.e., in r rounds? It turns out that the nature of this problem depends considerably on the magnitude of r. If we restrict the depth severely, then the size has to be of considerably larger order than $n \log n$; on the other hand, with width $O(n)$ there are algorithms of size $O(n \log n)$. The problem of sorting with small depth (i.e. in few rounds) was suggested only rather recently by Roberts and was motivated by testing consumer preferences by correspondence (see Scheele, 1977). On the other hand, the problem of sorting with (relatively) small depth is a classical problem in computing (see Knuth, 1973) and there is a formidable literature on the subject.

In this chapter we shall consider only the two extreme cases: that of very small depth and that of small width. The first two sections are devoted to variants of the problem of sorting in two rounds, and the third section gives a brief description of a recent major breakthrough by Ajtai, Komlós and Szemerédi (1983*a*, *b*) concerning sorting with width $O(n)$. In the fourth section we present some recent results about bin packing.

A wider view of sorting is taken in a recent review article by Bollobás and Hell (1984), to whom the reader is referred for additional references.

15.1 Finding Most Comparisons in One Round

We wish to ask questions in one round in such a way that no matter what answer we get, we can deduce almost all comparisons, that is all but $o(n^2)$ of them. At least how many questions do we have to ask? In this section we study variants of this problem, essentially due to Hell (see Häggkvist and Hell, 1980, 1981, 1982), with bounds on the number of steps we are allowed to take in deducing a comparison.

Let us start by formulating our problems in terms of graphs. Given a graph $G = (V, E)$, let $\vec{E}$ be an orientation of the edges. We say that $\vec{E}$ is a *consistent* or *acyclic* orientation if the oriented graph $\vec{G} \sim (V, \vec{E})$ contains no directed cycle. Equivalently, $\vec{E}$ is our acyclic orientation if there is a linear order $<$ on V such that $\overrightarrow{xy} \in \vec{E}$ implies $x > y$. For an acyclic oriented graph $\vec{G} \sim (V, \vec{E})$, let $C_d(\vec{G})$ be the oriented graph whose vertex set is V and in which $\overrightarrow{xy}$ is an edge iff there are $x_0, x_1, \ldots, x_l \in V$ such that $l \leq d, x_0 = x, x_l = y$ and $\overrightarrow{x_i x_{i+1}} \in \vec{E}$ for $0 \leq i < l$. We call $C_d(\vec{G})$ the *d-step closure of* $\vec{G}$ and the edge $\overrightarrow{xy}$ above a *d-step implication.* [Note that for every d a d-step implication is both a $(d+1)$-step implication and an $(n-1)$-step implication.] A 2-step implication is said to be a *direct implication* and an n-step implication is an *implication.* The oriented graph $C_n(\vec{G}) = C_{n-1}(\vec{G})$ is the *transitive closure* of $\vec{G}$: it contains an edge $\overrightarrow{xy}$ iff

$\vec{G}$ has a directed path whose initial vertex is x and whose terminal vertex is y.

The question we investigate is this. How few edges can a graph of order n have if every acyclic orientation of it is such that its d-step closure contains $\binom{n}{2} - o(n^2)$ edges? The results we are going to present are from Bollobás and Rosenfeld (1981).

One of our concrete random graphs has relatively few edges but there are many more edges in its 2-step closure. Let p be a prime power and let G_0 be the graph constructed by Erdős and Rényi (1962) and described in §4 of Chapter 13. Thus the vertex set of G_0 is the set of points of the projective plane $PG(2,p)$ over the field of order p and a point (a,b,c) is joined to a point (α,β,γ) iff $a\alpha + b\beta + c\gamma = 0$.

Theorem 15.1 *The graph G_0 has $n = p^2+p+1$ vertices, $\frac{1}{2}p(p+1)^2 \sim \frac{1}{2}n^{3/2}$ edges and every orientation of G_0 contains at least $\frac{1}{10}(p^2-1)^2 \sim \frac{1}{10}n^2$ direct implications.*

Proof Let us recall the following facts about G_0 (see pp. 328–329): p^2 vertices have degree $p+1$, the remaining $p+1$ vertices are independent and have degree p, no triangle of G_0 contains any of these $p+1$ vertices, the graph G_0 has diameter 2 and contains no quadrilaterals.

Consequently, no pentagon of G_0 has a diagonal. Since every orientation of an odd cycle contains a directed path of length 2, every orientation $\vec{G}_0$ of G_0 is such that every pentagon of G_0 has a diagonal which is a direct implication in $\vec{G}_0$. Thus in order to prove that $C_2(\vec{G}_0)$ has many edges we shall show that G_0 has many pentagons and no pair of vertices is the diagonal of many pentagons.

At least how many pentagons contain an edge x_2x_3 of G_0? We may assume that x_3 has degree $p+1$. Let x_4 be a vertex adjacent to x_3 but not to x_2. Since G_0 has no quadrilateral, we have at least $p-1$ choices for x_4. Let x_1 be a vertex adjacent to x_2 but not to x_3. If $d(x_2) = p+1$, then, as before, we have at least $p-1$ choices for x_1. If $d(x_2) = p$, then x_2 is contained in no triangle so once again we have $p-1$ choices for x_1. Finally, since G_0 has diameter 2, there is a (unique) vertex x_5 adjacent to both x_1 and x_4. In this way we have constructed a pentagon $x_1x_2\ldots x_5$. In constructing this pentagon we started with an arbitrary edge x_2x_3, so G_0 has at least

$$\frac{1}{5}\frac{1}{2}p(p+1)^2(p-1)^2$$

pentagons.

In at most how many pentagons of G_0 can a given pair $ab \in V^{(2)}$ be a diagonal? Suppose $x_1x_2x_3x_4x_5$ is a pentagon and $x_1 = a, x_3 = b$. Since G_0 has no quadrilateral, the vertex x_2 is determined by a and b. As x_4 has to be a neighbour of x_3 different from x_2, we have at most p choices for x_4. Having chosen x_4, once again we have at most one choice for x_5. Hence at most p pentagons contain ab as a diagonal.

Finally, every orientation of a pentagon gives at least one direct implication, so no matter how we orient G_0, we obtain at least

$$\tfrac{1}{10}p(p+1)^2(p-1)^2/p = \tfrac{1}{10}(p^2-1)^2$$

direct implications, as claimed. □

Now we turn to the main result of this section.

Theorem 15.2 *Given $\varepsilon > 0$, let $C = 5\varepsilon^{-1/2}\{\log(3e/\varepsilon)\}^{1/2}$ and put $p = Cn^{-1/2}$. Then a.e. G_p is such that every consistent orientation of it contains at least $\binom{n}{2} - \varepsilon n^2$ direct implications.*

Proof Let $w_0 = n^{1/2}(\log n)^2$. By Theorem 2.14 a.e. G_p is such that if $W \subset V$, $|W| = w \geq w_0$, then

$$Z_W = \left\{z \in V - W : |\Gamma(z) \cap W| \leq \tfrac{2}{3}pw\right\}$$

has at most w_0 elements. Also, by Theorem 2.15 a.e. G_p is such that if $U \subset W$, $|U| = u \geq u_0 = \lceil(3\log(3/\varepsilon)+3)n^{1/2}/C\rceil$, then

$$T_u = \{x \in V - U : \Gamma(x) \cap U = \emptyset\}$$

has at most $(\varepsilon/3)n$ elements. Suppose a graph G_0 satisfies both conclusions above. To prove the theorem it suffices to show that every consistent orientation of G_0 contains at least $\binom{n}{2} - \varepsilon n^2$ direct implications.

Consider an acyclic orientation of G_0. Let $x_1, x_2, \ldots, x_n$ be a relabelling of the vertices such that every edge $x_ix_j, i > j$, is oriented from x_i to x_j.

Partition $V(G_0) = \{x_1, \ldots, x_n\}$ into $k = \lceil 4/\varepsilon\rceil$ consecutive blocks of roughly equal size:

$$V(G_0) = \bigcup_{i=1}^{k} W_i, \max W_i + 1 = \min W_{i+1}$$

and

$$\lfloor n/k\rfloor \leq |W_i| \leq \lceil n/k\rceil.$$

Pick a block $W_i, i \geq 3$, and write $W = W_{i-1}$. If n is sufficiently large, then $|W| \geq w_0$, so $|Z_W| \leq w_0$. Each $x \in W_i - Z_W$ is joined to a set U_x of at least $\frac{2}{3}pw \geq u_0$ vertices in W. By assumption at most $(\varepsilon/3)n$ vertices of G_0 are not joined to some vertices in U_x. Hence for such a vertex x there are at most $2\lceil n/k \rceil + (\varepsilon/3)n < \frac{6}{7}\varepsilon n$ vertices $y \in \bigcup_{j=1}^{i} W_j$ such that xy is not a direct implication. Consequently, for a fixed i there are at most $w_0 n + \lceil n/k \rceil \frac{6}{7}\varepsilon n^2 < \varepsilon n^2/k$ pairs of the form $\{x_j, x_l\}, x_l \in W_i, j < l$, for which $x_j x_l$ is not a direct implication. As there are k blocks W_i, the assertion follows. □

Corollary 15.3 *Suppose $\omega(n) \to \infty$ and $p = \omega(n)n^{-1/2}$. Then a.e. G_p is such that every consistent orientation of it contains $\{1 + 0(1)\}n^2/2$ direct implications.*

There are sequences $(\varepsilon_n)_1^\infty, (G_n)_1^\infty$ such that (i) $\varepsilon_n \to 0$, (ii) each G_n is a graph of order n and size at most $\omega(n)n^{3/2}$ whose every consistent orientation contains at least $(1 - \varepsilon_n)\binom{n}{2}$ direct implications.

Proof The first assertion is immediate from Theorem 15.2. To see the second, note simply that a.e. G_p has at most $\omega(n)n^{3/2}$ edges [in fact, at most $(1 + \varepsilon)\omega(n)n^{3/2}/2$ edges]. □

The corollary above is essentially best possible: for every constant C there is a positive constant ε such that every graph of order n and size at most $Cn^{3/2}$ has a consistent orientation with at most $\lceil (1 - \varepsilon)\binom{n}{2} \rceil$ direct implications. This follows from Theorem 15.9 in the next section.

The problem concerning k-step implications can be tackled in a similar manner. The proof of the result one obtains is omitted [see Ex. 1 for (ii)].

Theorem 15.4 (i) *Given $\varepsilon > 0$, there is a constant $C > 0$ such that with $p = Cn^{1/d-1}$ a.e. G_p is such that the d-step closure of every acyclic orientation of G_p contains at least $(1 - \varepsilon)\binom{n}{2}$ edges.*

In particular, if $\omega(n) \to \infty$, then there are graphs $G_1, G_2, \ldots$ such that G_n has n vertices, at most $\omega(n)n^{1+1/d}$ edges, and the d-step closure of every acyclic orientation of G_n has $\{1 + o(1)\}\binom{n}{2}$ edges.

(ii) *Given $C > 0$, there is an $\varepsilon > 0$ such that if n is sufficiently large, then every graph of order n and size at most $Cn^{1+1/d}$ has a consistent orientation with at most $(\frac{1}{2} - \varepsilon)n^2$ d-step implications.* □

Let us comment on a problem which seems to be rather close to the ones we have just discussed. With how few edges is there a graph of order n which is such that if we orient the edges according to a random linear order, then with probability $1 - o(1)$ almost all pairs are direct [d-step, $(n-1)$-step] implications? This question has a very easy answer.

Theorem 15.5 (i) *Let $\omega(n) \to \infty$. Then there are graphs $G_1, G_2, \ldots$ such that G_n has n vertices and at most $\omega(n)n$ edges and with probability $1 - o(1)$ a random linear order of the vertices of G_n induces an orientation of G_n whose 2-step closure has $\{1 - o(1)\}\binom{n}{2}$ edges.*

(ii) *Given a positive constant C, there is an $\varepsilon > 0$ such that for every sufficiently large n and every graph of order n and size Cn the expected number of pairs which are not in the transitive closure of a random acyclic orientation of the graph is at least $n^2/(9C^2)$.*

Proof (i) Let G_n be a graph with $k = \omega(n)$ vertices of degree $n-1$ and $n-k$ vertices of degree k. Consider a random linear order of $V(G_n)$ and the induced oriented graph $\overrightarrow{G_n}$. If a vertex y of degree $n-1$ is between two vertices x and z, say $x > y > z$, then the pair (x, z) is a direct implication in $\overrightarrow{G_n}$ since $\overrightarrow{xy}$ and $\overrightarrow{yz}$ are edges of $\overrightarrow{G_n}$. Let n_0 be the number of vertices preceding the first vertex of degree $n-1$, let n_1 be the number of vertices between the first and the second vertices of degree $n-1, \ldots,$ and finally let n_k be the number of vertices following the last vertex of degree $n-1$. Then exactly $\sum_{i=0}^{k}\binom{n_i}{2}$ pairs are not direct implications. It is easily seen that with probability $1-o(1)$ we have $\max n_i = o(n/k)$, and so $o(n^2)$ pairs are not direct implications.

(ii) Let G_n be a graph of size Cn with vertex set $\{x_1, x_2, \ldots, x_n\}$. Set $d_i = d(x_i)$. Then the probability that x_i is a maximal element in a random orientation (that is there is no vertex x_j with $\overrightarrow{x_j x_i} \in \vec{E}$) is clearly $1/(d_i+1)$. Hence the expected number of maximal vertices is

$$E(M) = \sum_{i=1}^{n} \frac{1}{d_i + 1}.$$

Since

$$\begin{aligned} \sum_{i=1}^{n} d_i &= 2Cn, \\ E(M) &\geq n\frac{1}{2C+1}, \end{aligned}$$

so

$$E\{M(M-1)/2\} \geq \binom{n/(2C+1)}{2} \geq n^2/9C^2$$

if n is sufficiently large. To complete our proof note that if $\overrightarrow{xy}$ is in the transitive closure, then y is not a maximal vertex. $\square$

15.2 Sorting in Two Rounds

Let us consider the following sorting procedure. We ask m_1 questions and having obtained the answers, we deduce all d-step implications. In the next round we ask m_2 questions and deduce again all d-step implications, and so on.

All questions within a round are formulated simultaneously. We have to choose our questions in such a way that after r rounds we know the complete order of the elements. Denote by SORT(n,r,d) the minimal value of m for which we can always distribute the questions so that $m_i \leq m$ for every $i, i = 1,2,\ldots,r$. In other words, SORT(n,r,d) is the minimal number of processors enabling us to sort a set of n elements in r time intervals, assuming that in each time interval each processor is capable of completing one binary comparison. (In this model an object may be compared with several others during the same time interval, and there are no restrictions on communication among the processors). We also put SORT(n,r) = SORT$(n,r,n-1)$. This is the corresponding minimum without any bound on the number of steps.

In this section we shall study the functions SORT(n, 2, d) and SORT(n, 2). The first results concerning SORT(n, 2) were proved by Häggkvist and Hell (1980, 1981) who showed that $C_1 n^{3/2} <$ SORT$(n,2) < C_2 n^{5/3} \log n$ for some constants C_1 and C_2. The following essentially best possible results were proved by Bollobás and Thomason (1982). The proof of the first is somewhat similar to that of Theorem 15.2, so we leave it as an exercise (Ex. 2). Although the proof of Theorem 15.7 is random graph theory at its purest, it is not very short and its details are not very attractive, so we do not reproduce it here.

Theorem 15.6 *Let*

$$\alpha = \frac{1}{3}\left(1 - \frac{\log\log n}{\log n} + \frac{\log 2}{\log n}\right)$$

and $p = n^{-\alpha}$. Then a.e. G_p is such that it has at most $\frac{1}{2}n^{5/3}(\log n)^{1/3}$ edges and every consistent orientation of it has at least $\binom{n}{2} - \frac{1}{2}n^{5/3}(\log n)^{1/3}$ direct implications. In particular, SORT$(n,2,2) \leq \frac{1}{2}n^{5/3}(\log n)^{1/3}$ if n is sufficiently large. □

Theorem 15.7 *Let $p = n^{-\alpha}$, where*

(i) *$d \geq 3$ is a fixed integer and*

$$\alpha = \frac{d-1}{2d-1} - \frac{1}{2d-1}\frac{\log\log n}{\log n} - \frac{\log 2d}{\log n}$$

or (ii)

$$d = \frac{1}{2}\frac{\log n}{\log\log n} \text{ and } \alpha = \frac{1}{2} - \frac{\log\log n}{\log n} + \frac{\log 2}{\log n}.$$

Then a.e. G_p is such that in any consistent orientation of it there are at most $n^{2-\alpha}$ pairs whose order is not given by d-step implications. □

Corollary 15.8 *If $d \geq 2$ is fixed and n is sufficiently large, then*

$$\text{SORT }(n, 2, d) \leq 2dn^{1+d/(2d-1)}(\log n)^{1/(2d-1)}$$

and

$$\text{SORT }(n, 2) \leq \tfrac{1}{2}n^{3/2}\log n. \qquad \square$$

In Bollobás and Thomason (1982) it is shown that the results above are essentially best possible. Somewhat surprisingly, one has much more difficulty with the d-step closure of a graph than with the transitive closure. A slightly weaker version of the second part of Corollary 15.10 is in Häggkvist and Hell (1981).

Theorem 15.9 *Suppose the positive integers d, n and m satisfy*

$$n^{(d+1)/d} < m < 8^{-d}n^2.$$

Then every graph G of order n and size m has a consistent orientation $\vec{G}$ for which at least

$$2^{-14}n^{(3d-1)/(d-1)}m^{-d/(d-1)}$$

edges do not belong to the d-step closure of $\vec{G}$, provided n is sufficiently large.

Proof We shall assume that n is sufficiently large, so that for the sake of simplicity the integer part signs can be safely ignored. Let H be the subgraph of G spanned by the $s = n/2$ vertices of smallest degree. Then $\Delta = \Delta(H) \leq 4m/n = 2m/s$. The consistent orientation of G we are looking for will be such that no vertex of H will be dominated by a vertex not in H. Thus for $x, y \in H$ there is a d-step implication from x to y in G if and only if there is a d-step implication in H. Hence it suffices to show that for some consistent orientation $\vec{H}$ of H at least $2^{-14}n^{(3d-1)/(d-1)}m^{-d/(d-1)}$ pairs of vertices of H do not belong to the d-step closure of $\vec{H}$.

Consider the probability space of all $s!$ orderings of the vertices of

H. We shall estimate from above the probability that there is an $(i+1)$-step implication between a and b, where a and b are given vertices and $1 \leq i \leq d-1$.

Let A_u be the event that there are exactly u vertices between a and b. Then

$$P(A_u) = \frac{2\{s-(u+1)\}}{s(s-1)}.$$

The probability that a given $a-b$ path of length $i+1$ yields an $(i+1)$-step implication, given that A_u occurs, is

$$\frac{1}{i!}\binom{u}{i} \Big/ \binom{s-2}{i} \leq \frac{1}{i!}\left(\frac{u}{s-2}\right)^i.$$

Hence the probability that there is a d-step implication between a and b, given that A_u occurs, is at most

$$\sum_{i=1}^{d-1} t_i(a,b)\frac{1}{i!}\left(\frac{u}{s-2}\right)^i, \tag{15.1}$$

where $t_i(a,b)$ denotes the number of $a-b$ paths of length $i+1$.

Let M be the expected number of non-adjacent pairs (a,b) not implied by d-step implications. We shall show that M is fairly large. By (15.1)

$$M \geq \sum_{ab \notin E(H)} \sum_{u=0}^{s-2} P(A_u)\left\{1 - \sum_{i=1}^{d-1} t_i(a,b)\frac{1}{i!}\left(\frac{u}{s-2}\right)^i\right\}_+,$$

where $x_+ = \max(x,0)$. Hence for every $0 \leq v \leq s-2$,

$$\begin{aligned} M &\geq \sum_{ab \notin E(H)} \sum_{u=0}^{v} P(A_u)\left\{1 - \sum_{i=1}^{d-1} t_i(a,b)\frac{1}{i!}\left(\frac{u}{s-2}\right)^i\right\} \\ &\geq \sum_{u=0}^{v} P(A_u)\left\{\binom{s}{2} - m - \sum_{i=1}^{d-1} T_i\frac{1}{i!}\left(\frac{u}{s-2}\right)^i\right\}, \end{aligned}$$

where T_i is the number of $(i+1)$-paths in H. Clearly

$$T_i \leq \frac{s}{2}\Delta^{i+1} \leq \frac{s}{2}\left(\frac{2m}{s}\right)^{i+1} = S_i,$$

so

$$\begin{aligned} M &\geq \sum_{u=0}^{v} P(A_u)\left\{\binom{s}{2} - m - \sum_{i=1}^{d-1} S_i\left(\frac{u}{s-2}\right)^i\right\} \\ &\geq \sum_{u=0}^{v} P(A_u)\left\{\binom{s}{2} - m - 3\max_{1\leq i\leq d-1} S_i\left(\frac{v}{s-2}\right)^i\right\}. \end{aligned}$$

Let $w = 12^{-1/(d-1)}(s-2)^{2d/(d-1)}(2m)^{-d/(d-1)}$. Then

$$(S_i/S_{i-1})\{w/(s-2)\} = \frac{m}{2s}\frac{w}{s-2} > 1$$

so

$$\max_{1\le i\le d-1} S_i\left(\frac{w}{s-2}\right)^i = S_{d-1}\left(\frac{w}{s-2}\right)^{d-1} < \frac{1}{12}\binom{s}{2}.$$

Therefore

$$M \ge \frac{1}{2}\binom{s}{2}\sum_{u=0}^{w} P(A_u) \ge \frac{1}{2}\binom{s}{2} w\frac{s}{s(s-1)} = \frac{1}{4}ws,$$

because $s-(w+1) \ge s/2$. Finally note that

$$\tfrac{1}{4}ws > 2^{-14}n^{(3d-1)/(d-1)}m^{-d/(d-1)}.$$

Choose an ordering of G in which every vertex of $G-H$ is greater than every vertex of H and the ordering induced on H has at least $M \ge \frac{1}{4}ws$ missing d-step implications in H. Then G has at least $\frac{1}{4}ws$ missing d-step implications. □

Corollary 15.10 *If $c < \sqrt{2}/3$ and n is sufficiently large, then*

$$\mathrm{SORT}(n,2,d) \ge 2^{-7}n^{1+d/(2d-1)},$$

and

$$\mathrm{SORT}(n,2) \ge cn^{3/2}.$$

Proof The first part of the corollary is proved by putting $m = 2^{-7}n^{1+d/(2d-1)}$ in Theorem 15.9. To see the second part, let G be a graph of order n with $m = (\sqrt{2}/3)n^{3/2}$ edges. Let $C_1, C_2, \ldots, C_k$ be the colour classes produced by the greedy colouring algorithm (see Bollobás, 1979*a*, p. 89). Set $n_i = |C_i|$. Then

$$\sum_1^k n_i = n \quad \text{and} \quad \sum_1^k in_i \le m.$$

Let us minimize

$$\sum_1^n x_i^2 \tag{15.2}$$

subject to the conditions

$$\sum_1^n x_i = n,\ \sum_1^n ix_i \le m \quad \text{and} \quad x_i \ge 0, i = 1,\ldots,n.$$

By the method of Lagrange multipliers (see, for example, Hadley, 1964) we obtain that at the minimum $x_i = \mu - i\lambda$ over the range $1 \leq i \leq i_0 \sim 3m/n$, $0 \leq x_{i_0} \leq \lambda$ and $x_i = 0$ for $i > i_0$, where $\lambda \sim \frac{2}{9}n^3/m^2$ and $\mu \sim \frac{2}{3}n^2/m$. Consequently the minimum in (15.2) is about $\frac{4}{9}n^3/m = 2m$. Hence the parameters of our colouring satisfy

$$\sum_1^k \binom{n_i}{2} \geq m\{1 + o(1)\}.$$

Now let us order the vertices of G in such a way that every vertex in C_i precedes every vertex in $C_{i+1}, i = 1, 2, \ldots, k-1$, and let $\vec{G}$ be the orientation of G induced by this ordering. Then for $x, y \in C_i, x \neq y$, there is no implication from x to y so at most

$$\binom{n}{2} - \sum_1^k \binom{n_i}{2} \geq \binom{n}{2} - m\{1 + o(1)\}$$

edges belong to the closure of $\vec{G}$. □

It is perhaps worth noting that the proof above gives the following assertion in extremal graph theory. Colour a graph of order n and size m by the greedy algorithm. Then there are at least $(2n^3/9m)\{1 + o(1)\}$ pairs of vertices of the same colour, provided $m/n \to \infty$ and $m/n^2 \to 0$.

To conclude this section, let us say a few words about explicitly constructed two-round sorting algorithms. Häggkvist and Hell (1981) constructed a two-round sorting problem of width $(13/30)n^2 - (13/30)n$, based on the Petersen graph and balanced incomplete block designs, and the explicit algorithm in Theorem 15.1 can be viewed as a two-round sorting algorithm of width $\frac{2}{5}n^2 + O(n^{3/2})$. The first constructive subquadratic two-round sorting algorithm is due to Pippenger (1984); the algorithm is based on Pippenger's expander graphs. Recently Alon (1986) used his expander graphs, described in §3 of Chapter 13, to give an explicit two-round sorting algorithm of width $n^{7/4}$.

15.3 Sorting with Width $n/2$

We saw in §2 that the size of a sorting algorithm of bounded depth is considerably greater than $n \log n$, the information theoretic lower bound. What happens at the other end of the spectrum? Is there a sorting algorithm of depth $O(\log n)$ and size $O(n \log n)$? This question has attracted considerable study and was answered only recently, in the affirmative, by Ajtai, Komlós and Szemerédi (1983*a*, *b*). Our aim in this section is to describe their solution.

In fact, instead of restricting the depth, in this case it is more natural to restrict the width to precisely $n/2$. Indeed, with width $n/2$ we can use a matching for the questions in each round, assuming, of course, that n is even.

One of the best-known sorting algorithms was constructed by Batcher (1968): it has depth $O\{(\log n)^2\}$ and does use matchings in each round. Valiant (1975*a*) give an algorithm of width $O(n)$ and depth $O(\log n \log\log n)$ thereby coming very close to the information theoretic bound. C. P. Kruskal (1983) extended Valiant's algorithm to obtain sorting algorithms of any width $w = O(n/\log n)$ and depth $O(n \log n/w)$. This meant that for width $O(n/\log n)$ the order of the information theoretic lower bound on the size can indeed be attained.

Numerous related results were obtained by Hirschberg (1978), Preparata (1978), Borodin and Cook (1980), Borodin et al. (1981), Reischuk (1981), Shiloach and Vishkin (1981), Borodin and Hopcroft (1982), Yao (1982) and Reif and Valiant (1983). Among others, width $O(n)$ algorithms were given which, with probability tending to 1, need only $O(\log n)$ time. Finally Ajtai, Komlós and Szemerédi (1983a, b) managed to get rid of the unwanted $O(\log n)$ factor. They proved that there is a deterministic sorting algorithm of depth $O(\log n)$ and width $n/2$ in which, for even n, the questions in each round are distributed according to a matching.

To state the result precisely, we need some definitions. Let $F_1, F_2, \ldots, F_l$ be partitions of $\{1, 2, \ldots, m\}$ into pairs and singletons, i.e. let each F_i consist of independent edges of the complete graph with vertex set $\{1, 2, \ldots, m\}$. If m is even, then the F_i's will always be chosen to be 1-factors, i.e. matchings. Denote by $\mathrm{ALG}[F_1, F_2, \ldots, F_l; m]$ the following algorithm, used for ordering m elements. Let $x_1, x_2, \ldots, x_m$ be the elements to be ordered; place them into registers marked $1, 2, \ldots, m$. In round 1 compare the contents of the registers joined by an edge of F_1: if the larger register contains the smaller element, interchange the elements, otherwise do not move them. In round 2, compare the current contents of the registers joined by an edge of F_2 and interchange the contents, whenever they are the wrong way round. In round 3 use F_3, etc., up to F_l. Thus an algorithm of the form $\mathrm{ALG}[F_1, F_2, \ldots, F_l; m]$ is a so-called *comparator network*, and one with a rather simple structure. We think of $\mathrm{ALG}[F_1, F_2, \ldots, F_l; m]$ as an algorithm which accepts a permutation of $1, 2, \ldots, m$, namely $x_1, x_2, \ldots, x_m$, and produces another of $1, 2, \ldots, m$, namely the permutation whose ith element is the element in the register labelled i. If the permutation produced by our algorithm is always the identity (i.e. if, at the end, the ith register contains precisely the ith element), regardless of the input, then our algorithm is a sorting algorithm. However, in general it is only a reordering algorithm.

Ajtai, Komlós and Szemerédi (1983*a*, *b*) proved that sorting can be accomplished by such a simple comparator network of depth $O(\log n)$.

Theorem 15.11 *There is an absolute constant C such that for every $n \in \mathbb{N}$, there is a sorting algorithm of the form $ALG[F_1, F_2, \ldots, F_l; n]$, where $l \le C \log n$.* □

Before saying a few words about the proof, we define two algorithms used in the proof: *ε-halving* and *ε-sorting.*

A permutation $\pi \in S_m$ is said to be *ε-halved* if for every initial segment $K = \{1, 2, \ldots, k\}, k \le m/2$, the inequality $\pi(i) \le m/2$ holds for all but at most $\varepsilon|K|$ members i of K, and, similarly, for every terminal segment $K = \{k, k+1, \ldots, m\}, k \ge m/2$, the inequality $\pi(i) \ge m/2$ holds for all but at most $\varepsilon|K|$ members i of K. An algorithm is said to be an *ε-halving algorithm* if it accepts an arbitrary permutation of $\{1, 2, \ldots, m\}$ and produces an ε-halved permutation.

Lemma 15.12 *For every $\varepsilon > 0$ there is a constant $l = l_1(\varepsilon)$ such that for every $m \in \mathbb{N}$ there is an ε-halving algorithm of the form $ALG[F_1, F_2, \ldots, F_l; m]$.*

Proof Let $l = l_1(\varepsilon)$ be such that for every $m \in \mathbb{N}$ there is a bipartite expander graph G_m with parameters $((1-\varepsilon)/\varepsilon, \varepsilon, l)$ and bipartition $U = \{1, 2, \ldots, \lfloor m/2 \rfloor\}$, $W = \{\lfloor m/2 \rfloor + 1, \lfloor m/2 \rfloor + 1, \ldots, m\}$. By Corollary 13.23 we know that there is such an l. Let $F_1, F_2, \ldots, F_l$ be a factorization of G_m into subgraphs of maximal degree 1. We claim that ALG$[F_1, F_2, \ldots, F_l; m]$ will suffice.

Note that if $i \in U, j \in W, ij \in E(G_m)$, then, at the end of the algorithm, the content of i is less than the content of j. Indeed, this was certainly true about the current contents when the edge ij was used in the algorithm; from then on the content of i could only decrease and the content of j could only increase.

Suppose now that $A_0 \subset \{1, 2, \ldots, k\}, |A_0| > \varepsilon k, k \le m/2$, and the elements of A_0 end up in the registers forming a set $W_0 \subset W$. Set $U_0 = \Gamma(W_0)$. Then

$$U_0 \subset U, |U_0| > (1-\varepsilon)k,$$

and by the remark above, each register in U_0 has content at most as large as the content of its neighbour in W_0 and so at most k. However, this is impossible since $|U_0 \cup W_0| > k$.

A similar argument works for terminal segments. □

Let us say that a permutation $\pi \in S_m$ is *ε-sorted* if for every $k, 1 \leq k \leq m$, we have

$$|\{i : i \leq k, \pi(i) > k\}| \leq \varepsilon m.$$

and

$$|\{i : i \geq k, \pi(i) < k\}| \leq \varepsilon m.$$

Thus π is ε-sorted, at most εm members of an initial segment are mapped outside an initial segment and at most εm members of a terminal segment are mapped outside a terminal segment.

An algorithm is said to be an *ε-sorting algorithm* if from an arbitrary permutation of $\{1, 2, \ldots, m\}$ it produces an ε-sorted permutation. The proof of Theorem 15.11 hinges on the existence of suitable ε-sorting algorithms.

Lemma 15.13 *For every $\varepsilon > 0$ there is an $l = l_2(\varepsilon)$ such that for every $m \in \mathbb{N}$ there is an ε-sorting algorithm of the form $ALG[F_1, F_2, \ldots, F_l; m]$.*

Proof By replacing ε by $\varepsilon/2$, we may assume that $m = 2^t$. Choose $\varepsilon_1 > 0$ and $r \in \mathbb{N}$ such that $\varepsilon_1 < \varepsilon/\{2\log(2/\varepsilon)\}$ and $2^{-r} < \varepsilon/4$. We claim that $l_2(\varepsilon) = l_1(\varepsilon_1)r$ will suffice.

Apply an ε_1-halver guaranteed by Lemma 15.12, of length $l_1(\varepsilon_1)$, to the whole set of registers, then apply ε_1-halvers to the top and bottom halves of the registers, then to each quarter, and so on, altogether r times, the last application being to intervals of length less than $\varepsilon m/2$. The succession of these algorithms is clearly an algorithm of the form $\mathrm{ALG}[F_1, F_2, \ldots, F_l; m]$, where $l = l_2(\varepsilon)$, and it is easily seen that it is an $(\varepsilon/2)$-sorting algorithm. □

Let us describe now the algorithm in Theorem 15.11. As in the proof of Lemma 15.13, we may assume that n is a power of 2, say $n = 2^{t_0}$, where t_0 is large. Furthermore, the 1-factors $F_1, F_2, \ldots, F_l$ claimed by Theorem 15.11 will be given in $O(\log n)$ batches, each batch consisting of at most C 1-factors for some absolute constant C. To give the tth batch of 1-factors, it is convenient to choose a partition of the set of registers, with each class of the partition corresponding to a vertex of a rooted binary tree T_t of order $2^{t+1}-1$ and height $t, t = 0, 1, \ldots, t_0$. The 1-factors in each batch are chosen with the aid of Lemma 15.13.

The partition associated with the trees T_t depend on a positive constant A, that will be chosen to be a power of 2, the algorithms associated with the partitions depend on a positive constant ε as well, which will be chosen to be considerably smaller than $1/A$. Before giving exact definitions, let us give an intuitive description of the entire algorithm.

Let $\{x_t(i,j) : 0 \leq i \leq t, 1 \leq j \leq 2^i\}$ be the vertices of T_t, with $x_t(i,j), i < t$, having two *descendants*: $x_t(i+1, 2j-1)$ and $x_t(i+1, 2j)$. Thus $x_t(0,1)$ is the root of T_t and $x_t(t,1), x_t(t,2), \ldots, x_t(t,2^t)$ are its endvertices.

What partition of the register set $\{1, 2, \ldots, n\}$ shall we associate with T_t? Say $\mathscr{I}_t(i,j)$ is the set corresponding to vertex $x_t(i,j)$. Then the union of the sets of registers corresponding to the vertices in the branch at $x_t(i,j)$ is a large subset of the interval $[(j-1)2^{-i}n + 1, j2^{-i}n]$, with the extremes of the union at $\mathscr{I}_t(i,j)$, the apex of the branch, and the middle of the union at the other endvertices. Where is the rest of the interval $[(j-1)2^{-i}n + 1, j2^{-i}n]$? At the antecedents of the vertex $x_t(i,j)$: at $x_t(i-1, \lfloor j/2 \rfloor), x_t(i-2, \lfloor j/4 \rfloor)$, etc., which contain even more extreme elements of the interval than $\mathscr{I}_t(i,j)$. Furthermore, each $\mathscr{I}_t(i,j)$ is chosen to be the union of at most two intervals.

For fixed i and j, as t increases, $\mathscr{I}(i,j)$ becomes smaller and smaller and, eventually, it becomes empty. Thus more and more registers belong to sets at higher levels. Eventually, all registers filter up (down?) to the endvertices; the partition corresponding to T_{t_0} is just the discrete partition: $\mathscr{I}_{t_0}(i,j)$ is empty unless $i = t_0$ and $\mathscr{I}_{t_0}(t_0, j) = \{j\}, 1 \leq i \leq 2^{t_0} = n$.

Putting it another way: the subgraph U_t of T_t spanned by vertices $x_t(i,j)$ for which $\mathscr{I}_t(i,j) \neq \emptyset$, is a forest: with t increasing, eventually $\mathscr{I}_t(0,1)$ will be empty so U_t will have two components, then $\mathscr{I}_t(1,1)$ and $\mathscr{I}_t(1,2)$ also become empty and the forest U_t will have four components, etc. Finally, U_{t_0} will consist of $2^{t_0} = n$ vertices, namely the endvertices of T_{t_0}. In Fig. 15.1 we show some of the partitions for $n = 128$.

To define the sequence of 1-factors associated with a tree, call a subgraph spanned by a set $\{x_t(i,j), x_t(i+1, 2j-1), x_t(i+1, 2j)\}$ a *fork*. A fork is *even* if i is even and *odd* if i is odd. Note that a fork has one or three vertices; it has only one vertex if either $i = -1$, in which case the fork is the root of the tree, or $i = t$, in which case the fork is an endvertex. Now for the 1-factors associated with T_t. Take an ε-sorting algorithm, of the kind guaranteed by Lemma 15.13, on each even fork of T_t, follow it by an ε-sorting algorithm on each odd fork of T_t, and repeat this, say, eight times. This means choosing at most $16l_2(\varepsilon)$ 1-factors on the set of registers: this is the sequence of 1-factors we associate with T_t. Altogether then we shall choose $16l_2(\varepsilon)(\log_2 n + 1) = O(\log n)$ 1-factors, as required by Theorem 15.11.

The effect of the ε-sorting algorithms is that more and more elements to be sorted will belong to the correct set of registers. During the part of the algorithm corresponding to T_t, each element moves at a distance not more than 16 on T_t, and most elements move towards the set containing the register in which they have to end up. Of course, movement from one register to another is possible only if the registers belong to the same component of U_t, so it is crucial that, at each stage, the registers in each component U_t contain, collectively, the right set of elements.

It is not too difficult to show that with an appropriate choice of A and ε, the algorithm we defined is indeed a sorting algorithm. However, for the details the reader is referred to Ajtai, Komlós and Szemerédi (1983*a*, *b*).

To conclude this section, let us give the exact partition of $[1, n]$ associated with T_t for some $A = 2^a$.

Set $X_t(j) = \lfloor A^j (2A)^{-t-1} n \rfloor$ and

$$Y_t(i) = \sum_{j=1}^{i} X_t(j).$$

For $0 \le i \le t-1, 1 \le j \le 2^i$ and j odd, define

$$\begin{aligned}\mathscr{I}_t(i,j) &= \{(j-1)2^{-i}n + [Y_t(i)+1, Y_t(i+1)]\} \cup \\ &\quad \{(j-1)2^{-i}n + [2^{-i}n - Y_t(i+1) + 1, 2^{-i}n]\}\end{aligned}$$

and for $0 \le i \le t-1, 1 \le j \le 2^i$ and j even, define

$$\begin{aligned}\mathscr{I}_t(i,j) &= \{(j-1)2^{-i}n + [1, Y_t(i+1)]\} \cup \\ &\quad \{(j-1)2^{-i}n + [2^{-i}n - Y_t(i+1) + 1, 2^{-i}n - Y_t(i)]\}.\end{aligned}$$

Now let us define the sets belonging to the endvertices of T_t. The sets are simply intervals: for $1 \le j \le 2^t$ and j odd, set

$$\mathscr{I}_t(t,j) = (j-1)2^{-t}n + [Y_t(t) + 1, 2^{-t}n],$$

and, finally, for $1 \le j \le 2^t$ and j even, define

$$\mathscr{I}_t(t,j) = (j-1)2^{-t}n + [1, 2^{-t}n - Y_t(t)].$$

The reader can easily check that the partitions in Fig. 15.1 were defined by these formulae.

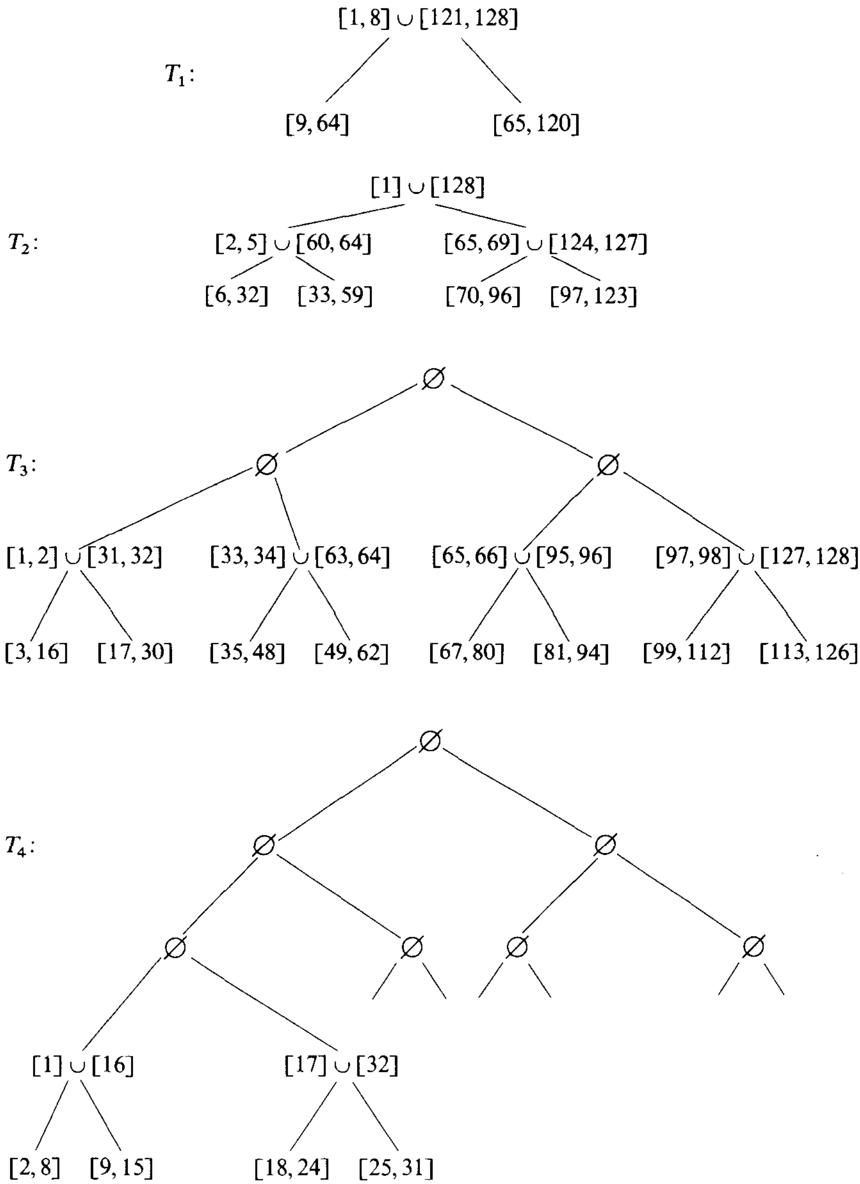


Fig. 15.1. The partitions of [1, 128] corresponding to T_1, T_2, T_3 and T_4 for $A = 4$.

Not surprisingly, the algorithm of Ajtai, Komlós and Szemerédi immediately attracted much interest and soon inspired many results (see Bilardi and Preparata, 1984*a*, *b*; Leighton, 1984; Thompson, 1985).

15.4 Bin Packing

Let L be a sequence $x_1, x_2, \ldots, x_n$ of n numbers in (0, 1]. We shall write $L = x_1 x_2 \ldots x_n$ and call L a *list* of n numbers. Given lists L_1, L_2, we write $L_1 L_2$ for the concatenation of them. A *packing* of L into unit capacity bins is a partition $\{1, 2, \ldots, n\} = \bigcup_{i=1}^{k} B_i$ such that $\sum_{x_j \in B_i} x_j \leq 1$ for every i. Thus a packing of L is a distribution of the numbers into bins B_i such that the sum of numbers in B_i is at most 1. The *bin packing problem* asks for fast algorithms packing any list into relatively few bins.

Given a list L, denote by $V(L)$ the sum of numbers in L and by L^* the minimal number of bins into which L can be packed. Clearly $V(L) \leq L^* < 2V(L)$. The problem of finding a packing of L into L^* bins may involve a solution of the NP-complete partition problem (see Karp, 1972), so instead of trying to construct an optimal packing it is sensible to look for relatively fast algorithms which arrive at nearly optimal packings. Such algorithms were found by Johnson (1973, 1974*a*), Johnson *et al.* (1974) and Yao (1980).

For any bin packing algorithm S, denote by $S(L)$ the number of bins used by S for packing a list L. Set $R_S(k) = \sup\{S(L)/L^* : L^* = k\}$ and call $R_S^\infty = \overline{\lim}_{k\to\infty} R_S(k)$ the *asymptotic performance ratio of* S. In terms of R_S^∞ the problem mentioned above asks for a fast (say at least polynomial) algorithm S for which R_S^∞ is rather close to 1. Yao (1980) asked whether for some $\varepsilon > 0$ every polynomial algorithm S has asymptotic performance ratio at least $1 + \varepsilon$. It was something of a breakthrough when recently this question was answered in the negative by de la Vega and Lueker (1981). The aim of this section is to present this beautiful result.

A *finite multiset* is a function μ on a set $\{y_1, y_2, \ldots, y_m\}$ whose values are natural numbers: $\mu(y_i) = n_i \in \mathbb{N}$. The multiset μ will be denoted by $\{y_1 \cdot n_1, y_2 \cdot n_2, \ldots, y_m \cdot n_m\}$ and we shall call n_i the *multiplicity* of y_i in μ. The *cardinality* of this multiset is $|\mu| = \sum_{i=1}^m n_i$. Suppose a list $L = x_1 x_2 \ldots x_n$ is such that its elements take m distinct values: $y_1 < y_2 < \ldots < y_m$. Then we write

$$\mu_L = \{y_1 \cdot n_1, y_2 \cdot n_2, \ldots, y_m \cdot n_m\},$$

where n_i is the number of x_j's equal to y_i. Then clearly $|\mu_L| = \sum_{i=1}^m n_i = n$.

A bin B_i used in a packing of a list L can be identified with the sublist L_i of L consisting of the elements of L in B_i. We call the multiset μ_{L_i} the *type* of B_i. If $\mu_L = \{y_1 \cdot n_1, y_2 \cdot n_2, \ldots, y_m \cdot n_m\}$, then we can represent the type of a bin by a vector $T \in \mathbb{Z}_+^m$, where $T = (t_1, t_2, \ldots, t_m)$ corresponds to the bin with exactly t_i members equal to y_i. In this way, to every packing of L corresponds a multiset of types of bins used in the packing.

If β is a multiset of types of bins corresponding to a packing of a list L and $\mu = \mu_L$, then we shall say that β is a *packing* of μ.

Note that if β is a packing of μ and $\mu = \mu_L$, then one can define in time linear in $|L|$ a packing of L using a set of bins whose types are given by β. Given a multiset μ, let μ^* be the minimal cardinality of the multisets of types of bins which are packings of μ. Thus $\mu^* = L^*$ whenever $\mu = \mu_L$.

The proof of the main theorem is based on a lemma concerning $RBP(\eta, m)$, the problem of *restricted bin packing* with parameters η and $m, 0 < \eta \leq 1$ and $m \in \mathbb{N}$. Let $M(\eta, m)$ be the collection of multisets $\mu = \{x_1 \cdot n_1, x_2 \cdot n_2, \ldots, x_m \cdot n_m\}$ with $\eta \leq x_i \leq 1, i = 1, 2, \ldots, m$. Then $RBP(\eta, m)$ asks for an algorithm constructing for every multiset $\mu \in M(\eta, m)$ a packing β of μ with $|\beta| = \mu^*$ or $|\beta|$ not much larger than μ^*.

Lemma 15.14 *Given η and m, $RBP(\eta, m)$ can be solved within an additive constant in constant time, that is there are numbers C_1, C_2, depending only on η and m, and an algorithm such that for every $\mu \in M(\eta, m)$ the algorithm constructs in time bounded by C_1 a packing β of μ satisfying $|\beta| \leq \mu^* + C_2$.*

Proof Note first that for any multiset $\mu \in M(\eta, m)$ the number of possible types of bins is bounded by a function $\tau(\eta, m)$. In fact rather crudely we may take

$$\tau(\eta, m) = (\lfloor 1/\eta \rfloor + 1)^m,$$

since a bin cannot contain more than $\lfloor 1/\eta \rfloor$ elements of the same value, and there are m distinct values.

Write $q = q(\mu) \leq \tau(\eta, m)$ for the actual number of types of bins which can be used in a packing of a multiset $\mu \in M(\eta, m)$. Let $T_1, T_2, \ldots, T_q$ be the vectors representing these types of bins, say $T_i = (t_1^i, t_2^i, \ldots, t_m^i)$.

If a packing β of μ has b_i bins of type T_i, then $|\beta| = \sum_{i=1}^q b_i$ and $\sum_{i=1}^q b_i t_j^i = n_j, j = 1, 2, \ldots, m$. We shall call a multiset $\gamma = \{T_1 \cdot c_1, T_2 \cdot c_2, \ldots, T_q \cdot c_q\}$ a loose packing of μ if

$$\sum_{i=1}^{q} c_i t_j^i \geq n_j, \quad j = 1, 2, \ldots, m.$$

A loose packing γ of μ can clearly be converted in constant time (i.e. in time depending only on q and m) to a packing β of μ with $|\beta| \leq |\gamma|$. Thus the lemma will be proved if we construct a constant time algorithm giving a loose packing of μ into $\mu^* + q \leq \mu^* + \tau(\eta, m)$ bins.

Consider the ordinary linear program P:

minimize

$$\sum_{i=1}^{q} a_i$$

subject to

$$\sum_{i=1}^{q} a_i t_j^i \geq n_j, \quad j = 1, 2, \ldots, m.$$

and

$$a_i \geq 0, \quad i = 1, 2, \ldots, q.$$

Clearly P can be solved in time depending only on q. Let $(\alpha_1, \alpha_2, \ldots, \alpha_q)$ be a solution.

Then $\sum_{i=1}^{q} \alpha_i \leq \sum_{i=1}^{q} b_i = |\beta|$ for every packing $\beta = (b_1, b_2, \ldots, b_q)$ of μ, and so $\sum_{i=1}^{q} \alpha_i \leq \mu^*$.

Furthermore, with $\alpha_i' = \lceil \alpha_i \rceil$ we have

$$\sum_{i=1}^{q} \alpha_i' \leq \sum_{i=1}^{q} \alpha_i + q \leq \mu^* + q, \sum_{i=1}^{q} \alpha_i' t_j^i \geq n_j, \quad j = 1, 2, \ldots, m$$

and

$$\alpha_i' \geq 0, \quad i = 1, 2, \ldots, q.$$

Hence the multiset $\{T_1 \cdot \alpha_1', T_2 \cdot \alpha_2', \ldots, T_q \cdot \alpha_q'\}$ defines a loose packing of μ and the number of bins used is at most $\mu^* + q \leq \mu^* + \tau(\eta, m)$. $\square$

Armed with this lemma it is fairly easy to prove the theorem of de la Vega and Lueker (1981).

Theorem 15.15 *For every* $0 < \varepsilon < 1$ *there is a bin packing algorithm* S *with* $R_S^\infty \leq 1 + \varepsilon$, *whose running time is at most* $C_\varepsilon + Cn \log(1/\varepsilon)$, *where* C_ε *depends only on* ε *and* C *is an absolute constant.*

Proof Set $\eta = \varepsilon/3$ and $m = \lceil \eta^{-2} \rceil$. Let $L = x_1 x_2 \ldots x_n$ be a list to be packed. Suppose L has l terms less than η, and define h by

$$n - l = mh + r, \quad 0 \leq r \leq m - 1.$$

If $h = 0$, then, using one bin for each of the terms at least η and packing each of the l other terms into the first bin they fit into, we obtain a packing into at most

$$m - 1 + V(L)/(1 - \eta)$$

bins. If L^* is sufficiently large, then this number is less than $L^*(1 + \varepsilon)$.

Suppose now that $h > 0$. Let $x_{j_1} \le x_{j_2} \le \ldots \le x_{j_{n-l}}$ be some increasing rearrangement of the terms of L greater than η and set

$$y_i = x_{j_{(i-1)h+1}}, \quad i = 1, 2, \ldots, m.$$

The kth largest term of a set of order n can be found in $O(n)$ time (see Blum *et al.*, 1973; Pratt and Yao, 1973). Hence, by finding first $y_{\lfloor m/2 \rfloor}$, then $y_{\lfloor m/4 \rfloor}$ and $y_{\lfloor 3m/4 \rfloor}$, and so on, all y_i's can be found in $O(n \log m) = O\{n \log(1/\varepsilon)\}$ time. Consequently in $O\{n \log(1/\varepsilon)\}$ time we can find a rearrangement $L_1 = K_0 y_1 K_1 y_2 \ldots y_m K_m R$ of L such that

(i) K_0 contains the l terms less than η,
(ii) $|K_1| = |K_2| = \ldots = |K_m| = h - 1$,
(iii) each term x_j in K_i satisfies $y_i \le x_j \le y_{i+1}$ and
(iv) the r terms in R are at least y_m.

[In fact, property (iv) is superfluous, it follows from the others.]

We shall need two more lists:

$$L_2 = K_0 y_1^h y_2^h \ldots y_m^h R$$

and

$$L_3 = K_0 y_2^h y_3^h \ldots y_m^h 1^h R.$$

Our theorem is implied by the following two assertions.

Claim 15.1 $L_3^* \le L_2^*(1+\eta) \le L^*(1+\eta)$.

Claim 15.2 *If L^* is sufficiently large, then there is a linear time packing of L_3 into not more than $L_3^*/(1-\eta) + 1$ bins.*

Indeed, every packing of L_1 gives a packing of L_2 using the same number of bins and every packing of L_3 gives a packing of L, in time linear in n. Since $L^*(1+\eta)/(1-\eta) + 1 < L^*(1 + 5\eta/2) + 1 < L^*(1+\varepsilon)$ if L^* is sufficiently large, the theorem follows from the two claims.

If we ignore the h terms $1, 1, \ldots, 1$ of L_3, then the remaining terms form a sublist of L_2. Hence $L_3^* \le L_2 + h$. Since $L_2^* \ge mh\eta \ge h/\eta$, we find that

$$L_3^* \le L_2^*(1+\eta),$$

which is Claim 1.

Let us turn to the proof of Claim 15.2. Set $Q = y_2^h \ldots y_m^h 1^h$ so that $L_3 = K_0 Q R$. Since $Q \in M(\eta, m)$, by Lemma 15.14 there is an algorithm of time at most $C(\eta, m) = C_\varepsilon$ which finds a multiset of types of bins of cardinality at most $Q^* + \tau(\eta, m)$, into which Q can be packed. This packing of Q can be performed in linear time in n. Let us extend this packing to a packing of QR by placing each element of R into a bin by itself. All we have been left to do is to add the l elements of K_0 to this packing.

We shall pack these elements one by one, always using the first available bin in which the sum of terms is at most $1-\eta$. If at the end of this process we have to start new bins then all bins, except perhaps the last one, are at least $1-\eta$ full. Hence in this case

$$S(L_3) \leq V(L_3)/(1-\eta)+1 \leq L^*/(1-\eta)+1.$$

On the other hand, if we do not start new bins, then

$$S(L) \leq Q^* + \tau(\eta, m) + |R| \leq Q^* + \tau(\eta, m) + \eta^{-2} \leq L^*/(1-\eta)$$

if $L^* \geq Q^*$ is sufficiently large. □

Exercises

15.1 Check that Theorem 15.9 implies Theorem 15.4(ii).

15.2 By imitating the proof of Theorem 15.2, prove Theorem 15.6.

15.3 For a tournament T, denote by $h(T)$ the maximal cardinality of a consistent (i.e. acyclic) set of arcs in T and set $f(n) = \min\{h(T) : T \text{ is a tournament of order } n\}$. Prove that $h(T) - \frac{1}{2}\binom{n}{2} = O\{n^{3/2}(\log n)^{1/2}\}$ for a.e. tournament T of order n and deduce that

$$0 \leq f(n) - \frac{1}{2}\binom{n}{2} = O\{n^{3/2}(\log n)^{1/2}\}.$$

[Erdős and Moon (1965); in fact, Spencer (1971, 1980) proved that for some constants $0 < c_1 < c_2$ we have

$$\frac{1}{2}\binom{n}{2} + c_1 n^{3/2} \leq f(n) \leq \frac{1}{2}\binom{n}{2} + c_2 n^{3/2},$$

and de la Vega (1983*a*) improved the upper bound by showing that a.e. tournament T of order n satisfies

$$f(n) \leq \frac{1}{2}\binom{n}{2} + 1.73n^{3/2}.]$$

16

Random Graphs of Small Order

Most of the results in the previous chapters concern spaces of random graphs of order n as $n \to \infty$: even our inequalities were claimed to hold only 'if n is sufficiently large'. Nevertheless, asymptotic results are often applied for rather small values of n, so the question arises as to how good these approximations are when n is not too large. The main aim of this chapter is to reproduce some of the tables concerning graphs of fairly small order, given by Bollobás and Thomason (1985). These tables are still far beyond the bound for which exact calculations are possible; for exact tables concerning graphs of small order (mostly general graphs of order at most 14 and trees of order at most 27), the reader should consult, among others, Bussemaker *et al.* (1976), Quintas, Stehlik and Yarmish (1979), Quintas, Schiano and Yarmish (1980), Brown *et al.* (1981) and Halberstam and Quintas (1982, 1984). For the use of information about small subgraphs see, among others, Frank and Frisch (1971), Frank (1977, 1979*a*, *b*), Frank and Harary (1980*a*, *b*), Gordon and Leonis (1976) and Quintas and Yarmish (1981).

16.1 Connectivity

We know from Theorem 7.3 that if $c \in \mathbb{R}$ is a constant, $p = (\log +n)/n$ and $M = \lfloor (n/2)(\log n + c) \rfloor$, then $\lim_{n\to\infty} P(G_p \text{ is connected}) = \lim_{n\to\infty} P(G_M \text{ is connected}) = 1 - e^{-e^{-c}}$.

Several authors have examined the probability that certain random graphs with very few vertices are connected (see Fu and Yau, 1962; Na and Rapoport, 1967). Of course, used indiscriminately, the approximations hidden in the relations above cannot be expected to be too good for small values of n (see Fillenbaum and Rapoport, 1971; Rapoport and Fillenbaum, 1972; Schultz and Hubert, 1973, 1975). However, values of

$P(n, M) = P(G_M \text{ is connected})$ have been directly calculated for small values of n. Using the formula

$$P(n, M) = 1 - \binom{N}{M}^{-1} \sum_{j=2}^{n} \frac{(-1)^j}{j} \sum{}' \frac{n!}{n_1!n_2!\dots n_j!} \binom{\sum_{k=1}^{j} \binom{n_k}{2}}{M},$$

where $\sum'$ denotes the sum over all partitions of n into exactly j parts, Ling (1973*a*, *b*, 1975) computed $P(n, M)$ for all $n \leq 16$ and Ling and Killough (1976) computed $P(n, M)$ for larger values of n. The disadvantages of this formula are clearly the occurrence of the alternating sign, requiring numbers to be stored with considerable accuracy, and the sum over all partitions, using up a lot of CPU time. Nevertheless, Ling and Killough gave extensive and accurate tables of $P(n, M)$ for $n \leq 100$.

For small values of n, Bollobás and Thomason (1985) used the recursive formula of Gilbert (1959) (see Ex. 1 in Chapter 7) to estimate the probability of connectedness, while for larger values of n they relied on the Jordan–Bonferroni inequalities (Theorem 1.10). The results are given in Table 16.1.

Table 16.2 gives values for $P(n, M)$, where M is the *nearest* integer to $n(c + \log n)/2$.

16.2 Independent Sets

It was proved in Chapter 11 that if p is constant (say $p = \frac{1}{2}$), then the independence number of $G_{n,p}$ is almost surely about $2 \log_{(1/q)} n$ (Matula, 1970, 1972, 1976; Grimmett and McDiarmid, 1975; Bollobás and Erdős, 1976*a*; Chvátal, 1977). This was done by estimating $E(X_k)$ and $\sigma(X_k)$, where X_k is the number of k-sets of independent vertices, and then applying Chebyshev's inequality Chvátal (1977) studied the complexity of algorithms determining the clique number, and Pittel (1982) investigated the probable behaviour of such algorithms. One cannot expect a fast algorithm which determines the exact clique number of a graph: Beck (1983*b*) proved that there is no algorithm which, for every 2-colouring of the edges of the complete graph on $\mathbb{N}$, constructs a monochromatic complete subgraph of order k in $2^{k/2}$ steps. (Ramsey's theorem tells us that such a subgraph can be found in 4^k steps.) For small values of n the independence number does not have a very sharp peak, but the exact values of $E(X_k)$ and $\sigma(X_k)$ still tell us a fair amount about the

Table 16.1. *The probability of $G_{n,p}$ being connected for $p = (c + \log n)/n$*

	c										
n	−0.83	−0.48	−0.19	0.000	0.087	0.367	0.672	1.03	1.50	2.25	4.61
10	0.057	0.153	0.266	0.348	0.388	0.514	0.639	0.760	0.869	0.958	0.999
20	0.083	0.192	0.306	0.384	0.421	0.536	0.647	0.753	0.852	0.940	0.998
30	0.094	0.204	0.316	0.391	0.427	0.536	0.643	0.746	0.843	0.932	0.996
40	0.099	0.209	0.319	0.393	0.428	0.535	0.639	0.740	0.837	0.927	0.995
50	0.102	0.211	0.319	0.393	0.427	0.533	0.636	0.736	0.833	0.924	0.995
60	0.103	0.211	0.319	0.392	0.426	0.531	0.633	0.733	0.830	0.921	0.994
70	0.104	0.212	0.319	0.391	0.425	0.529	0.631	0.731	0.827	0.919	0.994
80	0.104	0.212	0.319	0.390	0.424	0.527	0.629	0.729	0.825	0.918	0.994
90	0.105	0.212	0.318	0.389	0.423	0.526	0.628	0.727	0.823	0.916	0.993
100	0.105	0.212	0.318	0.389	0.422	0.525	0.626	0.725	0.822	0.915	0.993
150	0.105	0.211	0.315	0.385	0.419	0.520	0.621	0.720	0.817	0.912	0.992
200	0.105	0.210	0.314	0.383	0.416	0.518	0.618	0.717	0.814	0.910	0.992
250	0.105	0.209	0.312	0.382	0.414	0.516	0.616	0.715	0.812	0.908	0.992
300	0.105	0.208	0.311	0.380	0.413	0.514	0.614	0.713	0.811	0.907	0.991
350	0.104	0.208	0.310	0.379	0.412	0.513	0.613	0.712	0.810	0.907	0.991
400	0.104	0.207	0.310	0.379	0.411	0.512	0.612	0.711	0.809	0.906	0.991
450	0.104	0.207	0.309	0.378	0.410	0.511	0.611	0.710	0.808	0.906	0.991
500	0.104	0.206	0.308	0.377	0.410	0.510	0.610	0.709	0.808	0.905	0.991
550	0.104	0.206	0.308	0.377	0.409	0.510	0.610	0.709	0.807	0.905	0.991
600	0.103	0.206	0.308	0.376	0.409	0.509	0.609	0.708	0.807	0.904	0.991
650	0.103	0.206	0.307	0.376	0.408	0.509	0.609	0.708	0.806	0.904	0.991
700	0.103	0.205	0.307	0.375	0.408	0.508	0.608	0.707	0.806	0.904	0.991
750	0.103	0.205	0.307	0.375	0.408	0.508	0.608	0.707	0.806	0.904	0.991
800	0.103	0.205	0.306	0.375	0.407	0.508	0.607	0.707	0.806	0.904	0.991
850	0.103	0.205	0.306	0.375	0.407	0.507	0.607	0.707	0.805	0.903	0.991
900	0.103	0.205	0.306	0.374	0.407	0.507	0.607	0.706	0.805	0.903	0.991
950	0.103	0.205	0.306	0.374	0.406	0.507	0.607	0.706	0.805	0.903	0.991
1000	0.103	0.204	0.306	0.374	0.406	0.507	0.606	0.706	0.805	0.903	0.991
1500	0.102	0.203	0.304	0.373	0.405	0.505	0.605	0.704	0.804	0.902	0.990
2000	0.102	0.203	0.304	0.372	0.404	0.504	0.604	0.704	0.803	0.902	0.990
2500	0.102	0.202	0.303	0.371	0.403	0.503	0.603	0.703	0.802	0.902	0.990
3000	0.101	0.202	0.303	0.371	0.403	0.503	0.603	0.703	0.802	0.901	0.990
3500	0.101	0.202	0.302	0.370	0.403	0.503	0.603	0.702	0.802	0.901	0.990
4000	0.101	0.202	0.302	0.370	0.402	0.502	0.602	0.702	0.802	0.901	0.990
4500	0.101	0.202	0.302	0.370	0.402	0.502	0.602	0.702	0.802	0.901	0.990
5000	0.101	0.202	0.302	0.370	0.402	0.502	0.602	0.702	0.801	0.901	0.990
6000	0.101	0.201	0.302	0.370	0.402	0.502	0.602	0.702	0.801	0.901	0.990
7000	0.101	0.201	0.301	0.369	0.402	0.502	0.602	0.701	0.801	0.901	0.990
8000	0.101	0.201	0.301	0.369	0.401	0.501	0.601	0.701	0.801	0.901	0.990
9000	0.101	0.201	0.301	0.369	0.401	0.501	0.601	0.701	0.801	0.901	0.990
10,000	0.101	0.201	0.301	0.369	0.401	0.501	0.601	0.701	0.801	0.901	0.990
20,000	0.100	0.201	0.301	0.369	0.401	0.501	0.601	0.701	0.800	0.900	0.990
40,000	0.100	0.200	0.300	0.368	0.400	0.500	0.600	0.700	0.800	0.900	0.990

Table 16.2. *The probability of $G_{n,M}$ being connected where M is the nearest integer to $n(c + \log n)/2$*

	c										
n	−0.83	−0.48	−0.19	0.000	0.087	0.367	0.672	1.03	1.50	2.25	4.61
10	0.000	0.113	0.437	0.575	0.575	0.686	0.838	0.922	0.965	0.994	1.0
20	0.068	0.202	0.365	0.472	0.522	0.654	0.757	0.834	0.914	0.968	0.999
30	0.091	0.225	0.353	0.449	0.480	0.620	0.712	0.801	0.893	0.957	0.998
40	0.089	0.217	0.352	0.443	0.486	0.588	0.691	0.785	0.876	0.948	0.997
50	0.096	0.224	0.345	0.433	0.467	0.579	0.687	0.781	0.863	0.941	0.997
60	0.100	0.228	0.340	0.425	0.453	0.572	0.673	0.770	0.858	0.936	0.996
70	0.104	0.221	0.338	0.422	0.457	0.568	0.664	0.763	0.851	0.932	0.995
80	0.101	0.218	0.339	0.411	0.452	0.558	0.659	0.759	0.846	0.930	0.995
90	0.102	0.219	0.334	0.407	0.443	0.553	0.657	0.753	0.843	0.928	0.995
100	0.104	0.215	0.333	0.406	0.446	0.553	0.652	0.749	0.840	0.926	0.994
150	0.102	0.215	0.327	0.400	0.432	0.537	0.638	0.736	0.830	0.920	0.993
200	0.102	0.213	0.321	0.395	0.429	0.529	0.632	0.730	0.825	0.916	0.993
250	0.104	0.213	0.319	0.390	0.424	0.527	0.627	0.725	0.821	0.913	0.992
300	0.103	0.210	0.318	0.389	0.422	0.525	0.623	0.722	0.819	0.912	0.992
350	0.103	0.210	0.316	0.386	0.418	0.521	0.622	0.721	0.817	0.911	0.992
400	0.103	0.209	0.314	0.384	0.418	0.520	0.620	0.717	0.815	0.909	0.992
450	0.103	0.209	0.313	0.384	0.416	0.518	0.618	0.717	0.814	0.909	0.992
500	0.103	0.209	0.312	0.383	0.416	0.516	0.617	0.715	0.813	0.908	0.991
550	0.103	0.207	0.311	0.381	0.414	0.515	0.615	0.714	0.812	0.907	0.991
600	0.103	0.207	0.310	0.380	0.413	0.514	0.615	0.713	0.811	0.907	0.991
650	0.103	0.207	0.311	0.380	0.412	0.513	0.613	0.713	0.810	0.906	0.991
700	0.103	0.206	0.310	0.379	0.411	0.513	0.613	0.712	0.810	0.906	0.991
750	0.103	0.206	0.309	0.379	0.411	0.512	0.612	0.711	0.809	0.906	0.991
800	0.102	0.206	0.309	0.378	0.411	0.511	0.612	0.711	0.809	0.906	0.991
850	0.102	0.205	0.309	0.378	0.410	0.511	0.611	0.710	0.808	0.905	0.991
900	0.102	0.206	0.309	0.377	0.409	0.511	0.610	0.710	0.808	0.905	0.991
950	0.102	0.206	0.308	0.377	0.409	0.510	0.610	0.710	0.808	0.905	0.991
1000	0.102	0.205	0.308	0.377	0.409	0.510	0.610	0.709	0.807	0.905	0.991
1500	0.102	0.204	0.306	0.374	0.407	0.507	0.607	0.707	0.805	0.903	0.991
2000	0.102	0.203	0.305	0.373	0.405	0.506	0.606	0.705	0.804	0.903	0.991
2500	0.101	0.203	0.304	0.372	0.405	0.505	0.605	0.705	0.804	0.902	0.990
3000	0.101	0.203	0.303	0.372	0.404	0.504	0.604	0.704	0.803	0.902	0.990
3500	0.101	0.202	0.303	0.371	0.404	0.504	0.604	0.703	0.803	0.902	0.990
4000	0.101	0.202	0.303	0.371	0.403	0.503	0.603	0.703	0.802	0.902	0.990
4500	0.101	0.202	0.303	0.371	0.403	0.503	0.603	0.703	0.802	0.901	0.990
5000	0.101	0.202	0.302	0.371	0.403	0.503	0.603	0.703	0.802	0.901	0.990
6000	0.101	0.202	0.302	0.370	0.402	0.503	0.602	0.702	0.802	0.901	0.990
7000	0.101	0.201	0.302	0.370	0.402	0.502	0.602	0.702	0.802	0.901	0.990
8000	0.101	0.201	0.302	0.370	0.402	0.502	0.602	0.702	0.801	0.901	0.990
9000	0.101	0.201	0.301	0.370	0.402	0.502	0.602	0.702	0.801	0.901	0.990
10,000	0.101	0.201	0.301	0.369	0.402	0.502	0.602	0.701	0.801	0.901	0.990
20,000	0.100	0.201	0.301	0.369	0.401	0.501	0.601	0.701	0.801	0.900	0.990
40,000	0.100	0.200	0.300	0.368	0.401	0.501	0.601	0.700	0.800	0.900	0.990
45,000	0.100	0.200	0.300	0.368	0.400	0.500	0.600	0.700	0.800	0.900	0.990

distribution of $\beta_0(G_{n,p})$. Clearly

$$E(X_k) = \binom{n}{k} q^{\binom{k}{2}} \tag{16.1}$$

and

$$\sigma^2(X_k) = \binom{n}{k} \sum_{r=0}^{k} \binom{k}{r} \binom{n-k}{k-r} q^{k(k-1)-\binom{r}{2}} - E(X_k)^2.$$

and by Chebyshev's inequality

$$P(X_k = 0) \le \sigma^2(X_k)/E(X_k)^2 = U(X_k). \tag{16.2}$$

Table 16.3 shows the information one can derive from (16.1) and (16.2) in the case $p = \frac{1}{2}$ for all those values of k for which $E(X_k) > 0.01$ and $U(X_k) > 0.01$.

For large values of n (5000 and 10 000) let us consider four algorithms on random graphs $G_{n,c/n}$, $c = 3$ and 4, searching for large independent sets. All four algorithms choose vertices one by one. The first algorithm, called *hammer*, always chooses an available vertex of minimum degree. In the other three algorithms the vertices are ordered at the beginning, and at each stage we choose the first available vertex. In *simple greedy* the natural order is taken, in *low first (greedy)* we choose an order in which the degrees are non-decreasing and in a *high first (greedy)* we choose an order in which the degrees are non-increasing. The outcomes are shown in Table 16.4.

16.3 Colouring

Graph-colouring algorithms have been constructed and their probable behaviour analysed by numerous authors, including Brélaz (1979), Christofides (1971), Corneil and Graham (1973), Kucera (1977) and Lawler (1970). Algorithms colouring random graphs which are just about manageable on available machines were constructed by numerous authors, including Johnson (1974), Garey and Johnson (1976), Leighton (1979), Johri and Matula (1982) and Bollobás and Thomason (1985). The standard test for the efficiency of the algorithm is usually a $G_{n,p}$ with $n = 1000$ and $p = \frac{1}{2}$. Improving on previous results, Johri and Matula used an average of 95.9 colours; this was further improved by Bollobás and Thomason to an average of 86.9 colours.

For a r.g. $G_{n,p}$ with $n = 1000$ and $p = \frac{1}{2}$, with large probability we have

$$80 \le \chi(G) \le 126.$$

Table 16.3. *Independent k-sets in $G_{n,1/2}$*

n	k	$E(X_k)$	$U(X_k)$
40	5	42.58	0.181
40	6	117.13	0.601
40	7	8.89	2.577
40	8	0.29	23.502
60	6	1527.83	0.198
60	7	184.16	0.589
60	8	9.53	2.504
60	9	0.22	27.810
80	7	1514.78	0.250
80	8	107.99	0.746
80	9	3.37	4.079
80	10	0.05	84.320
100	7	7633.00	0.138
100	8	693.23	0.346
100	9	27.68	1.224
100	10	0.49	12.818
200	9	17,104.98	0.105
200	10	638.10	0.236
200	11	10.76	1.103
200	12	0.08	37.313
400	11	25,386.89	0.057
400	12	401.84	0.119
400	13	2.93	1.359
600	12	55,133.78	0.033
600	13	608.83	0.063
600	14	3.12	0.967
800	12	$> 10^5$	0.017
800	13	26,484.02	0.026
800	14	181.74	0.059
800	15	0.58	3.591
1000	13	$> 10^5$	0.015
1000	14	4228.26	0.022
1000	15	16.96	0.178
1000	16	0.03	50.685
2000	17	3.95	0.434
3000	18	5.04	0.305
4000	19	0.72	1.847
5000	19	50.62	0.031
5000	20	0.02	50.261

The expected number of colourings with k colours, namely

$$E(k) = \sum_{(a_i)} \frac{n!}{\prod a_i! \prod n_j!} 2^{-\Sigma\binom{a_i}{2}}$$

where the sum is over all sequences (a_i) of length k with $\sum a_i = n$ and

Table 16.4. *Independent sets found by greedy algorithms in random graphs of order n with probability P(edge) = c/n*

Hammer	Simple greedy	Low first	High first
	$n = 5000, c = 3$		
2574	2071	2319	1731
2541	2177	2526	1922
2548	2206	2541	1930
2550	2197	2543	1905
2524	2188	2525	1915
2522	2221	2506	1903
2564	2190	2540	1883
2539	2239	2540	1879
2541	2206	2538	1915
2540	2229	2536	1927
	$n = 5000, c = 4$		
2246	1923	2156	1630
2237	1950	2242	1697
2250	1981	2232	1682
2243	1937	2248	1716
2253	1964	2240	1673
2262	1999	2265	1685
2248	1953	2234	1698
2239	1966	2249	1732
2252	1950	2239	1714
2268	1999	2258	1702
	$n = 10{,}000, c = 3$		
5089	4101	4595	3534
5084	4363	5038	3875
5068	4398	5047	3853
5081	4391	5083	3823
5111	4452	5091	3848
5089	4421	5070	3797
5120	4421	5111	3846
5089	4410	5088	3887
5092	4409	5082	3835
5114	4413	5091	3893

Table 16.5. *Colourings of ten graphs of order 1000*

Graph number	1	2	3	4	5
Time taken	48 : 38	51 : 56	54 : 58	49 : 11	55 : 23
Colours used	87	86	87	87	87
Graph number	6	7	8	9	10
Time taken	43 : 45	50 : 16	55 : 31	56 : 46	67 : 40
Colours used	87	87	87	87	87

Mean time: 53 : 23, mean colours used: 86.9.

Table 16.6. *The diameter and girth of a random sample of s cubic graphs of order n*

$n = 30, s = 100$

$d \backslash g$	3	4
5	7	6
6	49	22
7	14	0
8	2	0

$n = 40, s = 100$

$d \backslash g$	3	4	5
6	30	9	3
7	47	6	1
8	4	0	0

$n = 50, s = 100$

$d \backslash g$	3	4	5
6	4	4	0
7	47	15	1
8	24	2	0
9	3	0	0

$n = 100, s = 100$

$d \backslash g$	3	4	5
8	20	11	4
9	48	10	2
10	5	0	0

$n = 150, s = 100$

$d \backslash g$	3	4	5	6
9	35	18	1	1
10	37	8	0	0

$n = 200, s = 100$

$d \backslash g$	3	4	5
9	2	1	1
10	71	18	11
11	5	1	0

$n = 300, s = 40$

$d \backslash g$	3	4	5
10	5	2	1
11	25	7	0

$n = 500, s = 40$

$d \backslash g$	3	4	5
11	4	6	4
12	17	7	2

$n = 1000, s = 15$

$d \backslash g$	3	4
12	1	0
13	11	3

$n = 2000, s = 2$

$d \backslash g$	3	4
14	1	1

$n = 3000, s = 2$

$d \backslash g$	3	4
15	1	1

$n = 4000, s = 2$

$d \backslash g$	3
15	2

n_j is the number of a_i which equal j, can be computed when $n = 1000$ and $k = 79$ or 80. One finds $E(79) < 10^{-12}$ and $E(80) > 10^{14}$, so $\chi \geq 80$ almost surely. [Incidentally, the expected number of equitable colourings with 80 colours, having 40 colour classes of size 12 and 40 of size 13, is less than 0.08. The 'most likely' sequence (a_i) is 26 classes each of sizes 12 and 13, 12 each of sizes 11 and 14 and two each of sizes 10 and 15.] The upper bound of 126 represents the average number of colours used by the greedy algorithm. The fact that 87 colours tend to suffice indicates the inefficiency of the greedy algorithm.

The basic strategy of the algorithm used by Bollobás and Thomason was the natural one: find the largest independent set you can, remove it, and repeat the process on the remaining graph. The difficult part is finding a large independent set. It should be noted that this procedure is very unlikely to produce a colouring with only 80 colours, even if one

Table 16.7. *The diameter and girth of a random sample of s four-regular graphs of order n*

$n = 30$,	$s = 100$,	(4, 3) 80,	(5, 3) 20	
$n = 40$,	$s = 100$,	(4, 3) 10,	(5, 3) 89,	(6, 3) 1
$n = 50$,	$s = 100$,	(5, 3) 98,	(6, 3) 2	
$n = 100$,	$s = 100$,	(6, 3) 100		
$n = 150$,	$s = 100$,	(6, 3) 58,	(6, 4) 1,	(7, 3) 41
$n = 200$,	$s = 100$,	(7, 3) 100		
$n = 300$,	$s = 40$,	(7, 3) 38,	(8, 3) 2	
$n = 500$,	$s = 40$,	(8, 3) 40		
$n = 1000$,	$s = 15$,	(8, 3) 4,	(9, 3) 11	
$n = 2000$,	$s = 2$,	(9, 3) 2		
$n = 3000$,	$s = 2$	(10, 3) 2		

Table 16.8. *The diameter and girth of a random sample of s five-regular graphs of order n*

$n = 30$,	$s = 100$,	(3, 3) 14,	(4, 3) 18
$n = 40$,	$s = 100$,	(4, 3) 100	
$n = 50$,	$s = 100$,	(4, 3) 100	
$n = 100$,	$s = 40$,	(5, 3) 40	
$n = 150$,	$s = 40$,	(5, 3) 36,	(6, 3) 4
$n = 200$,	$s = 40$,	(5, 3) 6,	(6, 3) 34
$n = 300$,	$s = 40$,	(6, 3) 40	
$n = 500$,	$s = 15$,	(6, 3) 11,	(7, 3) 4
$n = 1000$,	$s = 2$,	(7, 3) 2	
$n = 2000$,	$s = 2$,	(8, 3) 2	

could find the actual largest independent set at each stage. For lack of space, we shall not describe the various refinements incorporated into this basic strategy.

The results of colouring 10 graphs by one of the algorithms used by Bollobás and Thomason on an IBM 3081 (5 MIPS), with a program written in FORTRAN, are given in Table 16.5.

16.4 Regular Graphs

We saw in Chapter 10 that random r-regular graphs gave rather good upper bounds for the minimal diameter of an r-regular graph of order n (Theorem 10.14). Nevertheless, even if we assume that the asymptotic bounds are applicable to graphs of small order (though, of course, they are not), we end up with rather poor bounds. However, by generating

Table 16.9. *The diameter and girth of a random sample of s six-regular graphs of order n*

$n = 30,$	$s = 50,$	(3, 3) 49,	(4, 3) 1
$n = 40,$	$s = 10,$	(3, 3) 1,	(4, 3) 9
$n = 50,$	$s = 10,$	(4, 3) 10	
$n = 100,$	$s = 5,$	(4, 3) 4,	(5, 3) 1
$n = 160,$	$s = 5,$	(5, 3) 5	
$n = 200,$	$s = 18,$	(5, 3) 18	
$n = 300,$	$s = 2,$	(5, 3) 2	
$n = 500,$	$s = 1,$	(6, 3) 1	
$n = 1000,$	$s = 1,$	(6, 3) 1	
$n = 2000,$	$s = 2,$	(8, 3) 2	

random graphs as in §4 of Chapter 2, Bollobás and Thomason found that the spread of the diameters is rather small: the results are shown in Tables 16.6–16.9. Since most of the computer time is taken up by generating random graphs, and the girth of a graph is easily checked, the distribution of the girth is also included. In each subtable of Table 16.6, the entries in the first row give the girths and those in the first column give the diameters. For example, in a sample of 100 cubic graphs of order 50, 15 had diameter 7 and girth 4. In Tables 16.7–16.9 the first two numbers stand for the order and sample size and an entry $(d, g)t$ means that we found t graphs of diameter d and girth g. For example, in a sample of 100 4-regular graphs of order 30, 80 were found to have diameter 4 and girth 3.

References

Abelson, H. (1979). A note on time–space tradeoffs for computing continuous functions, *Info. Process. Lett.* **8**, 215–217.

Abramowitz, M. and Stegun, I. A. (1972). *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables.* National Bureau of Standards, Appl. Math. Series 55, xiv + 1046pp.

Achlioptas, D. and Friedgut, E. (1999). A sharp threshold for k-colorability, *Random Structures, Algorithms* **14**, 63–70.

Achlioptas, D. and Molloy, M. (1997). The analysis of a list-colouring algorithm on a random graph, *38th Annual Symposium on Foundations of Computer Science, Miami, FL (1997)*, pp. 204–212.

Achlioptas, D. and Molloy, M. (1999). Almost all graphs with $2.522n$ edges are not 3-colorable, *Electr. J. Combinatonics* **6**, Research Paper 29, 9 pp.

Aho, A. V., Hopcroft, J. E. and Ullman, J. D. (1974). *The Design and Analysis of Computer Algorithms*, Addison–Wesley, Reading, Massachusetts.

Aigner, M. (1980). *Combinatorial Theory.* Grundlehren der mathematischen Wissenschaften **234**, Springer-Verlag, Berlin, Heidelberg, New York, viii + 483pp.

Ajtai, M., Komlós, J. and Szemerédi, E. (1979). Topological complete subgraphs in random graphs, *Studia Sci. Math. Hungar.* **14**, 293–297.

Ajtai, M., Komlós, J. and Szemerédi, E. (1980). A note on Ramsey numbers, *J. Combinatorial Theory (A)* **29**, 354–360.

Ajtai, M., Komlós, J. and Szemerédi, E. (1981*a*). The longest path in a random graph, *Combinatorica* **1**, 1–12.

Ajtai, M., Komlós, J. and Szemerédi, E. (1981*b*). A dense infinite Sidon sequence, *Europ. J. Combinatorics* **2**, 1–11.

Ajtai, M., Komlós, J. and Szemerédi, E. (1982). Largest random component of a *k-cube, Combinatorica* **2**, 1–7.

Ajtai, M., Komlós, J. and Szemerédi, E. (1983*a*). *O(n log n)* sorting network, *Proc. 15th ACM Symp. on Theory of Computing*, pp. 1–9.

Ajtai, M., Komlós, J. and Szemerédi, E. (1983*b*). Sorting in *C log n parallel steps, Combinatorica* **3**, 1–19.

Ajtai, M., Komlós, J., Pintz, J., Spencer, J. and Szemerédi, E. (1982). Extremal uncrowded hypergraphs, *J. Combinatorial Theory (A)* **32**, 321–335.

Akers, S. B. (1965). On the construction of (d, k) graphs, *IEEE Trans. Comput.* **14**, 488.

Albert, R., Jeong, H. and Barabási, A.-L. (1999). Diameter of the world-wide web, *Nature* **401**, 130–131.

Albertson, M. O., Bollobás, B. and Tucker, S. (1976). The independence ratio and maximum degree of a graph, *Proc. Seventh Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, pp. 43–50.

Albertson, M. O. and Hutchinson, J. P. (1975). The maximum size of an independent set in a nonplanar graph, *Bull. Amer. Math. Soc.* **81**, 554–555.

Aldous, D. (1992). Asymptotics in the random assignment problem, *Probab. Theory, Related Fields* **93**, 507–534.

Aldous, D. (2001). The random assignment problem, *Random Structures and Algorithms*, to appear

Aleliunas, R., Karp, R. M., Lipton, R. J., Lovász, L. and Rackoff, C. (1979). Random walks, universal transversal sequences, and the complexity of maze problems, *20th Annual Symp. on Foundations of Computer Science*, October, pp. 218–223.

Alm, S. E. and Sorkin, G. B. (2001). Exact expectations and distributions for the random assignment problem, to appear.

Alon, N. (1986). Eigenvalues, geometric expanders and sorting in rounds, *Combinatorica* **6**, 207–209.

Alon, N. (1991). A parallel algorithmic version of the local lemma, *Random Structures, Algorithms* **2**, 361–378.

Alon, N., Kim, J.H. and Spencer, J. (1997). Nearly perfect matchings in regular simple hypergraphs *Israel J. Math.* **100**, 171–187.

Alon, N. and Krivelevich, M. (1997). The concentration of the chromatic number of random graphs, *Combinatorica* **17**, 303–313.

Alon, N. and Milman, V. D. (1984). Eigenvalues, expanders and superconcentrators, *Proc. 25th Annual Symp. on Foundations of Computer Science*, Florida, pp. 320–322.

Alon, N. and Milman, V. D. (1985), λ_1, isoperimetric inequalities for graphs, and superconcentrators, *J. Combinatorial Theory (B)* **38**, 73–88.

Alon, N., Rödl, V. and Ruciński, A. (1998). Perfect matchings in ε-regular graphs, *Elect. J. Combinatorics* **5**, Research Paper 13, 4pp.

Alon, N. and Spencer, J. (1992). The probabilistic method, John Wiley and Sons, New York, xvi + 254 pp.

Angluin, D. (1979). A note on a construction of Margulis, *Info. Process. Lett.* **8**, 17–19.

Angluin, D. and Valiant, L. G. (1979). Fast probabilistic algorithms for Hamilton circuits and matchings, *J. Computer, Syst. Sci.* **18**, 155–193.

Ankeny, N. C. (1952). The least quadratic non-residue, *Annls Math.* **55**, 65–72.

Arnold, L. (1967). On the asymptotic distribution of the eigenvalues of random matrices, *J. Math. Analysis Applics* **20**, 262–268.

Arnold, L. (1971). On Wigner's semicircle law for the eigenvalues of random matrices, *Z. Wahrscheinlichkeitstheorie verwand. Gebiete* **19**, 191–198.

Arnold, L. (1976). Deterministic version of Wigner's semicircle law for the distribution of matrix eigenvalues, *Linear Algebra, Applics* **13**, 185–199.

Aronson, J., Dyer, M., Frieze, A. and Suen, S. (1994). On the greedy heuristic for matching, *Proceedings of the Fifth Annual ACM–SIAM Symposium on Discrete Algorithms (Arlington, VA, 1994)*, ACM, New York, pp. 141–149.

Aronson, J., Dyer, M., Frieze, A., and Suen, S. (1995). Randomized greedy matching, II., *Random Structures, Algorithms*, 55–73.

Aronson, J., Frieze, A. and Pittel, B. G. (1998). Maximum matchings in sponse random graphs: Karp–Sipser revisited, *Random Structures, Algorithms* **12**, 111–177.

Austin, T. L., Fagen, R. E., Penney, W. F. and Riordan, J. (1959). The number of components in random linear graphs, *Annls Math. Statist.* **30**, 747–754.

Azuma, K. (1967). Weighted sums of certain dependent variables, *Tôhoku Math. J.* **3**, 357–367.

Babai, L. (1980*a*). On the complexity of canonical labelling of strongly regular graphs, *SIAM J. Comput.* **9**, 212–216.

Babai, L. (1980*b*). Isomorphism testing and symmetry of graphs. In 'Combinatorics 79' (Deza, M. and Rosenberg, I. G., Eds), *Annls Discrete Math.* **8**, 101–109.(*)

Babai, L. (1980*c*). Almost all Steiner triple systems are asymmetric, *Annls Discrete Math.* **10**, 37–39.

Babai, L. (1981). Moderately exponential bound for isomorphism. In *Fundamentals of Computation Theory* (Gécseg, F., Ed.), Lecture Notes in Comput. Sci. *117*, Springer-Verlag, pp. 34–50.

Babai, L., Erdős, P. and Selkow, S. M. (1980). Random graph isomorphisms, *SIAM J. Comput.* **9**, 628–635.

Babai, L. and Godsil, C. D. (1982). On the automorphism groups of almost all Cayley graphs, *Europ. J. Combinatorics* **3**, 9–15.

Babai, L., Grigoryev, D. Yu. and Mount, D. M. (1982). Isomorphism of graphs with bounded eigenvalue multiplicity, *Proc. 14th Annual ACM STOC Symp.*, pp. 310–324.

Babai, L. and Kučera, L. (1979). Canonical labelling of graphs in linear average time, *20th Annual IEEE Symp. on Foundations of Computational Science*, Puerto Rico, pp. 39–46.

Bagaev, G. N. (1973). Random graphs with degree of connectedness 2, *Diskret Analiz* **22**, 3–14 (in Russian).

Bagaev, G. N. (1974). Distribution of the number of vertices in a component of a connected graph with randomly eliminated edges. In *III Vsesoy. Konf. Probl. Teor. Kiber. Novosibirsk*, pp. 137–140 (in Russian).

Bagaev, G. N. (1977). The distribution of the number of vertices in a component of an indecomposable random mapping, *Dokl. Akad. Nauk BSSR* **21**, 1061–1063 (in Russian).

Baker, A. (1975). Some aspects of transcendence theory, *Astérisque* **24–25**, 169–175 (Soc. Math. de France).

Ball, M. O. (1979). Computing network reliability, *Ops Res.* **27**, 823–838.

Ball, M. O. (1980). The complexity of network reliability computations, *Networks* **10**, 153–165.

Ball, M. O. and Provan, J. S. (1981*a*). Calculating bounds on reachability and connectedness in stochastic networks, Working Paper MS/S # 81-012, College of Business and Management, University of Maryland at College Park.

Ball, M. O. and Provan, J. S. (1981*b*). Bounds on the reliability problem for shellable independence systems, Working Paper MS/S # 81-013, College of Business and Management, University of Maryland at College Park.

Bannai, E. and Ito, T. (1973). On finite Moore graphs, *J. Fac. Sci. Univ. Tokyo, Sect. IA. Math.* **20**, 191–208.

Barabási, A.-L. and Albert, R. (1999). Emergence of scaling in random networks, *Science* **286**, 509–512.

Barabási, A.-L., Albert, R. and Jeong, H. (2000). Scale-free characteristics of random networks: the topology of the world-wide web, *Physica* **A281**, 69–77.

Barbour, A. D. (1982). Poisson convergence and random graphs, *Math. Proc. Camb. Phil. Soc.* **92**, 349–359.

Barbour, A. D. and Eagleson, G. K. (1982). Poisson approximation for some statistics based on exchangeable trials. *Adv. Appl. Probab.* **15**, 585–600.

Barbour, A. D., Holst, L. and Janson, S. (1992). *Poisson Approximation*, Oxford University Press, New York, x + 277 pp.

Barlow, R. R. and Proschan, F. (1965). *Mathematical Theory of Reliability*. John Wiley and Sons, New York, London and Sydney, xiii + 256pp.

Bassalygo, L. A. and Pinsker, M. S. (1973). The complexity of an optimum non-blocking switching network without reconnections, *Problemy Peredachi Informatsii* **9**, 84–87 (in Russian). English transl. in *Problems of Information Transmission*, Plenum Press, New York (1974), pp. 64–66.

Batcher, K. (1968). Sorting networks and their applications, *AFIPS Spring Joint Conf.* **32**, 307–314.

Bauer, H., (1981). *Probability Theory and Elements of Measure Theory* (2nd English Edn). Academic Press, xiii + 460pp.

Bauer, D., Boesch, F., Suffel, C. and Tindell, R. (1981). Connectivity extremal problems and the design of reliable probabilistic networks. *The Theory of Applications of Graphs* (Chartrand, G., Ed.). John Wiley and Sons, New York.

Beck, J. (1983*a*). On size Ramsey numbers of paths, trees and cycles, I. *J. Graph Theory* **7**, 115–129.

Beck, J. (1983*b*). There is no fast method for finding monochromatic complete subgraphs, *J. Combinatorial Theory (B)* 58–64.

Beck, J. (1985). On size Ramsey numbers of paths, trees and cycles, II.

Beck, J. (1991). An algorithmic approach to the Lovász lemma; I. *Random Structures and Algorithms* **2**, 343–365.

Beck, J. and Fiala, T. (1981). 'Integer-making' theorems, *Discrete Appl. Math.* **3**, 1–8.

Békéssy, A., Békéssy, P. and Komlós, J. (1972). Asymptotic enumeration of regular matrices. *Studia Sci. Math. Hungar.* **7**, 343–353.

Belevitch, V. (1950). Theory of $2n$-terminal networks with applications to conference telephony, *Elect. Commun.* **27**, 231–244.

Bender, E. A. (1974*a*). Asymptotic methods in enumeration, *SIAM Rev.* **16**, 485–515.

Bender, E. A. (1974*b*). The asymptotic number of non-negative integer matrices with given row and column sums, *Discrete Math.* **10**, 217–223.

Bender, E. A. and Canfield, E. R. (1978). The asymptotic number of labelled graphs with given degree sequences, *J. Combinatorial Theory (A)* **24**, 296–307.

Bender, E. A., Canfield, E. R. and McKay, B. D. (1990). The asymptotic number of labeled connected graphs with a given number of vertices and edges, *Random Structures and Algorithms* **1**, 127–169.

Benson, C. T. (1966). Minimal regular graphs of girth eight and twelve, *Canad. J. Math.* **26**, 1091–1094.

Berge, C. (1958). Sur le couplage maximum d'un graphe, *C.r. Acad. Sci., Paris* **247**, 258–259.

Berge, C. (1973). *Graphs and Hypergraphs*. North-Holland Mathematical Library **6**, Amsterdam, London, xiv + 528pp.

Bermond, J.-C. and Bollobás, B. (1982). The diameter of graphs—a survey, *Proc. Twelfth Southeastern Conf. on Combinatorics, Graph Theory and Computing, Congressus Numerantium* **32**, 3–27.

Bermond, J.-C., Delorme, C. and Farhi, G. (1982). Large graphs with given degree and diameter III. In *Graph Theory* (Bollobás, B., Ed.). *Annls Discrete Math.* **13**, 23–32.

Bermond, J.-C., Delorme, C. and Farhi, G. (1984). Large graphs with given degree and diameter II, *J. Combinatorial Theory (B)* **36**, 32–48.

Bermond, J.-C., Bond, J., Paoli, M. and Peyrat, C. (1983). Graphs and intercommunication networks: diameter and vulnerability. In *Surveys in Combinatorics* (Lloyd, E. K., Ed.). Lond. Math. Soc. Lecture Notes, **82**, pp. 1–30.

Bernstein, A. J. (1967). Maximally connected arrays on the n-cube, *SIAM J. Appl. Math.* **15**, 1485–1489.

Best, M. R. (1970). The distribution of some variables on symmetric groups, *Indag, Math.* **32**, 385–402.

Biggs, N. L. (1974). *Algebraic Graph Theory*. Cambridge Tracts in Math. **67**, Cambridge University Press, vii + 170pp.

Bilardi, G. and Preparata, F. P. (1984*a*). Minimum area VLSI network for $O(\log n)$ time sorting, *Proc. 16th Annual ACM Symp. on Theory of Computing*, Washington, D.C., 64–70.

Bilardi, G. and Preparata, F. P. (1984*b*). The VLSI optimality of the AKS sorting network. Coordinated Science Laboratory Report R-1008, University of Illinois, Urbana.

Birnbaum, Z. W., Esary, J. D. and Saunders, S. C. (1961). Multicomponent systems and structures and their reliability, *Technometrics* **3**, 55–57.

Bixby, R. (1975). The minimum number of edges and vertices in a graph with edge connectivity N and MN-bounds, *Networks* **5**, 253–298.

Blass, A., Exoo, G. and Harary, F. (1981). Paley graphs satisfy all first-order adjacency axioms, *J. Graph Theory* **5**, 435–439.

Bloemena, A. R. (1964). *Sampling from a Graph*. Math. Centre Tracts, Amsterdam.

Blum, M., Pratt, V., Tarjan, R. E., Floyd, R. W. and Rivest, R. L. (1973). Time bounds for selection, *J. Computer, Syst. Sci.* **7**, 448–461.

Boesch, F. T. and Felzer, A. (1972). A general class of invulnerable graphs, *Networks* **2**, 261–283.

Boesch, F. T., Harary, F. and Kabell, J. A. (1981). Graphs as models of communication network vulnerability: connectivity and persistence, *Networks* **11**, 57–63.

Bollobás, B. (1978*a*). *Extremal Graph Theory*. Academic Press, London, New York, San Francisco, xx + 488pp.

Bollobás, B. (1978*b*). Chromatic number, girth and maximal degree, *Discrete Math.* **24**, 311–314.

Bollobás, B. (1979*a*). *Graph Theory—An Introductory Course*. Graduate Texts in Mathematics, Springer-Verlag, New York, Heidelberg, Berlin, x + 180pp.

Bollobás, B. (1979*b*). A probabilistic proof of an asymptotic formula for the number of labelled regular graphs, Preprint Series, Matematisk Institut, Aarhus Universitet.

Bollobás, B. (1979*c*). Graphs with equal edge-connectivity and minimum degree, *Discrete Math.* **28**, 321–323.

Bollobás, B. (1980*a*). The distribution of the maximum degree of a random

graph, *Discrete Math.* **32**, 201–203.
Bollobás, B. (1980*b*). A probabilistic proof of an asymptotic formula for the number of labelled regular graphs, *Europ. J. Combinatorics* **1**, 311–316.
Bollobás, B. (1981*a*). Degree sequences of random graphs, *Discrete Math.* **33**, 1–19.
Bollobás, B. (1981*b*). The diameter of random graphs, *Trans. Amer. Math. Soc.* **267**, 41–52.
Bollobás, B. (1981*c*). The independence ratio of regular graphs, *Proc. Amer. Math. Soc.* **83**, 433–436.
Bollobás, B. (1981*d*). Threshold functions for small subgraphs, *Math. Proc. Camb. Phil. Soc.* **90**, 197–206.
Bollobás, B. (1981*e*). Counting coloured graphs of high connectivity, *Canad. J. Math.* **33**, 476–484.
Bollobás, B. (1981*f*). Random graphs. In *Combinatorics* (Temperley, H. N. V., Ed.). Lond. Math. Soc. Lecture Note Series 52. Cambridge University Press, pp. 80–102.
Bollobás, B. (1982*a*). Vertices of given degree in a random graph, *J. Graph Theory* **6**, 147–155.
Bollobás, B. (1982*b*). Distinguishing vertices of random graphs, *Annls Discrete Math.* **13**, 33–50.
Bollobás, B. (1982*c*). The asymptotic number of unlabelled regular graphs, *J. Lond. Math. Soc.* **89**, 201–206.
Bollobás, B. (1982*d*). Long paths in sparse random graphs, *Combinatorica* **2**, 223–228.
Bollobás, B. (1983*a*). Almost all regular graphs are Hamiltonian, *Europ. J. Combinatorics* **4**, 97–106.
Bollobás, B. (1983*b*). The evolution of the cube. In *Combinatorial Mathematics* (Berge, C., Bresson, D., Camion, P., Maurras, J. F. and Sterboul, F., Eds). North-Holland, pp. 91–97.
Bollobás, B. (1984*a*). The evolution of sparse graphs. In *Graph Theory and Combinatorics*. Proc. Cambridge Combinatorial Conf. in honour of Paul Erdős (Bollobás, B., Ed.). Academic Press, pp. 35–57.
Bollobás, B. (1984*b*). The evolution of random graphs, *Trans. Amer. Math. Soc.* **286**, 257–274.
Bollobás, B. (1984*c*). Geodesics in oriented graphs, *Annls Discrete Math.* **20**, 67–73.
Bollobás, B. (1984*d*). Lectures on random graphs. In *Progress in Graph Theory* (Bondy, J. A. and Murty, U. S. R., Eds). Academic Press, pp. 3–41.
Bollobás, B. (1985). *Extremal graph theory, with emphasis on probabilistic methods*, CBMS Regional Conf. Ser. in Math. **62**, viii + 64 pp.
Bollobás, B. (1988*a*). The chromatic number of random graphs, *Combinatorica* **8**, 49–56.
Bollobás, B. (1988*b*). Martingales, isoperimetric inequalities and random graphs, in *Combinatorics*, Proceedings, Eger 1987 (Hajnal, A., Lovász, L. and Sós, V. T., Eds), Colloq. Math. Soc. János Bolyai **52**, north - Holland, Amsterdam, pp. 113–139.
Bollobás, B., Borgs, C., Chayes, J. T., Kim, J. H. and Wilson, D. B. (2001). *Random Structures and Algorithms*, to appear.
Bollobás, B. and Catlin, P. (1981). Topological cliques of random graphs, *J. Combinatorial Theory (B)* **30**, 224–227.
Bollobás, B., Catlin, P. A. and Erdős, P. (1980). Hadwiger's conjecture is true for

almost every graph, *Europ. J. Combinatorics* **1**, 195–199.
Bollobás, B., Cooper, C., Fenner, T. I. and Frieze, A. M. (2000). Edge disjoint Hamilton cycles in random graphs of minimum degree at least k, *J. Graph Theory* **34**, 42–59.
Bollobás, B. and Erdős, P. (1975). An extremal problem of graphs with diameter 2, *Math. Mag.* **48**, 281–283.
Bollobás, B. and Erdős, P. (1976*a*). Cliques in random graphs, *Math. Proc. Camb. Phil. Soc.* **80**, 419–427.
Bollobás, B. and Erdős, P. (1976*b*). On a Ramsey–Turán type problem, *J. Combinatorial Theory (B)* **21**, 166–168.
Bollobás, B., Fenner, T. I. and Frieze, A. M. (1984). Long cycles in sparse random graphs. In *Graph Theory and Combinatorics*. Proc. Cambridge Combinatorial Conf. in honour of Paul Erdős (Bollobás, B., Ed.). Academic Press, pp. 59–64.
Bollobás, B., Fenner, T. I. and Frieze, A. M. (1987). An algorithm for finding Hamilton paths and cycles in random graphs, *Combinatorica* **7**, 327–341.
Bollobás, B., Fenner, T. I. and Frieze, A. M. (1990). Hamilton cycles in random graphs of minimal degree at least k, *A Tribute to Paul Erdős*, Cambridge Univ. Press, pp. 59–95.
Bollobás, B. and Frieze, A. M. (1985). On matchings and Hamiltonian cycles in random graphs See Q3
Bollobás, B., Frank, O. and Karoński, M. (1983). On 4-cycles in random bipartite tournaments, *J. Graph Theory* **7**, 183–194.
Bollobis, B., Grimmett, G. and Janson, S. (1996). The random-cluster model on the complete graph, *Probab. Theory, and Related Fields* **104**, 283–317.
Bollobás, B. and Hell, P. (1984). Sorting and graphs. In *Graphs and Order* (Rival, I., Ed.). NATO ASI Series, Reidel, Dordrecht, Boston, Lancaster, pp. 169–184.
Bollobás, B. and Klee, V. (1984). Diameters of random bipartite graphs, *Combinatorica* **4**, 7–19.
Bollobás, B. and McKay, B. D. (1986). The number of matchings in random regular graphs and bipartite graphs, *J. Combinatorial Theory (B)* **41**, 80–91.
Bollobás, B. and Rasmussen, S. (1989). First cycles in random directed graph processes, *Discrete Math.* **75**, 55–68.
Bollobás, B. and Riordan, O. (2000). Linearized chord diagrams and an upper bound for Vassiliev invariants. *J. Knot Theory Ramifications* **7**, 847–853.
Bollobás, B. and Riordan, O. (2002). The diameter of a scale-free random graph, to appear.
Bollobás, B., Riordan, O., Spencer, J. and Tusnády, G. (2001). The degree sequence of a scale-free random graph, *Random Structures and Algorithms*, to appear.
Bollobás, B. and Rosenfeld, M. (1981). Sorting in one round, *Israel J. Math.* **38**, 154–160.
Bollobás, B. and Sauer, N. (1976). Uniquely colourable graphs with large girth, *Canad. J. Math.* **28**, 1340–1344.
Bollobás, B. and Scott, A. (2001). Discrepancies of graphs and hypergraphs, *Contemporary Combinatorics*, to appear.
Bollobás, B. and Simon, I. (1993). Probabilistic analysis of disjoint set union algorithms, *SIAM J. Comput.* **22**, 1053–1074.
Bollobás, B. and Thomason, A. G. (1977). Uniquely partitionable graphs, *J. Lond. Math. Soc. (2)* **16**, 403–410.

Bollobás, B. and Thomason, A. G. (1981). Graphs which contain all small graphs, *Europ. J. Combinatorics* **2**, 13–15.
Bollobás, B. and Thomason, A. G. (1983). Parallel sorting, *Discrete Appl. Math.* **6**, 1–11.
Bollobás, B. and Thomason, A. G. (1985). Random graphs of small order. In *Random Graphs*, Annals of Discr. Math., pp. 47–97.
Bollobás, B. and Thomason, A. G. (1987). Threshold functions, *Combinatorica* **7**, 35–58.
Bollobás, B. and de la Vega, W. F. (1982). The diameter of random regular graphs, *Combinatorica* **2**, 125–134.
Bombieri, E. (1966). On exponential sums in finite fields, *Amer. J. Math.* **88**, 71–105.
Bombieri, E. (1973*b*). Counting points on curves over finite fields, Seminaire Bourbaki, 25e année, 1972/73, No. 430, 1–8.
Bonferroni, C. E. (1936). Teorie statistiche delle classi e calcolo delle probabilitá, *Publ. Inst. Sup. Sc. Ec. Comm. Firenze* **8**, 1–62.
Borodin, A. and Cook, S. A. (1980). A time-space tradeoff for sorting on a general sequential model of computation, *Proc. 12th ACM Symp. on Theory of Computing*, pp. 294–301.
Borodin, A. and Hopcroft, J. E. (1982). *Proc. 14th ACM Symp. on Theory of Computing*, pp. 338–344.
Borodin, A., Fischer, M. J., Kirkpatrick, D. G., Lynch, N. A. and Tompa, M. (1981). A time-space tradeoff for sorting on non-oblivious machines, *J. Computer, Syst. Sci.* **22**, 351–364.
Breiman, L. (1968). *Probability*. Addison–Wesley, Reading, Massachusetts, ix + 421pp.
Brélaz, D. (1979). New methods to colour the vertices of a graph, *Commun. ACM* **22**, 251–256.
Broadbent, S. R. and Hammersley, J. M. (1957). Percolation processes. I. Crystals and maizes, *Proc. Cambridge Philos. Soc.* **53**, 629–641.
Brooks, R. L. (1941). On colouring the nodes of a network, *Proc. Camb. Phil. Soc.* **37**, 194–197.
Brown, P., Quintas, L. V., Schiano, M. D. and Yarmish, J. (1981). Distributions of small order 4-trees and some implications for large orders, Mathematics Department, Pace University, New York.
Brown, T. A. and Spencer, J. (1971). Minimization of ± 1 matrices under line shifts, *Colloq. Math. (Poland)* **23**, 165–171.
Brown, W. G. (1966). On graphs that do not contain a Thomsen graph, *Canad. Math. Bull.* **9**, 281–285.
de Bruijn, N. D., Knuth, D. E. and Rice, S. O. (1972). The average height of planted trees. In *Graph Theory and Computing* (Read, R. C., Ed.). Academic Press, New York, pp. 15–27.
Buell, D. A. and Hudson, R. H. (1984). On runs of consecutive quadratic residues and quadratic nonresidues, *BIT* **24**, 243–247.
Buell, D. A. and Williams, K. S. (1978). Maximal difference sets residue, *p*, *Proc. Amer. Math. Soc.* **69**, 205–209.
Burgess, D. A. (1957). The distribution of quadratic residues and non-residues, *Mathematika* **4**, 106–112.
Burgess, D. A. (1962). On character sums and primitive roots, *Proc. Lond. Math. Soc. (3)* **12**, 179–192.
Burgess, D. A. (1963). A note on the distribution of residues and non-residues,

J. Lond. Math. Soc. **38**, 253–256.

Burr, S. A. and Erdős, P. (1975). On the magnitude of generalized Ramsey numbers for graphs. In 'Infinite and Finite Sets', vol. I (Hajnal, A., Rado, R. and Sós, V. T., Eds). *Colloq. Math. Soc. J. Bolyai* **10**, North-Holland, Amsterdam, London, pp. 214–240.

Burr, S. A., Erdős, P., Faudree, R. J., Rousseau, C. C. and Schelp, R. H. (1980). An extremal problem in generalized Ramsey theory, *Ars Combinatoria* **10**, 193–203.

Burtin, Yu. D. (1973*a*). Asymptotic estimates of the degree of connectivity of a random graph, *Kibernetika* **3**, 118–122 (in Russian).

Burtin, Yu. D. (1973*b*). Asymptotic estimates of the diameter, independence and domination numbers of a random graph, *Soviet Mat. Doklady* **14**, 497–501.

Burtin, Yu. D. (1974). On extreme metric characteristics of a random graph, I, Asymptotic estimates, *Theory Probab. Applics* **19**, 711–725.

Burtin, Yu. D. (1975). On extreme metric characteristics of a random graph, II, Limit distributions, *Theory Probab. Applics* **20**, 83–101.

Burtin, Yu. D. (1977). On the probability of connectedness of a random subgraph of the *n*-cube, *Problemy Pered. Inf.* (Problems of Information Transmission) **13**, 90–95 (in Russian).

Burtin, Yu. D. (1980). On a simple formula for random mappings and its applications, *J. Appl. Probab.* **17**, 403–414.

Bussemaker, F. C., Cobeljic, S., Cvetković, D. M. and Seidel, J. J. (1976). Computer investigation of cubic graphs, T.H. Report 76-WSK-01, Department of Mathematics, Technological University, Eindhoven, The Netherlands; also see *J. Combinatorial Theory (B)* **23** (1977), 234–235.

Buzacott, J. A. (1980). A recursive algorithm for finding reliability measures related to connection of nodes in a graph, *Networks* **10**, 311–328.

de Caen, D. (1983). A note on the probabilistic approach to Turán's problem, *J. Combinatorial Theory (B)* **34**, 340–349.

Cameron, P. J. (1980). On graphs with given automorphism group, *Europ. J. Combinatorics* **1**, 91–96.

Cameron, P. J. (1984). Aspects of the random graph. In *Graph Theory and Combinatorics* (Bollobás, B., Ed.). Academic Press, London, pp. 65–79.

Capobianco, M. F. (1970). Statistical inference in finite populations having structure, *Trans. N. Y. Acad. Sci.* **32**, 401–413.

Capobianco, M. F. (1972). Estimating the connectivity of a graph. *Graph Theory and Applications* (Alari, Y., Lick, D. R. and White, A. T., Eds). Springer-Verlag, Berlin, pp. 65–74.

Capobianco, M. and Frank, O. (1983). Graph evolution by stochastic additions of points and lines, *Discrete Math.* **46**, 133–143.

Carlitz, L. (1954). Congruences for the number of *n*-gons formed by *n* lines, *Amer. Math. Monthly* **61**, 407–411.

Carlitz, L. (1960). Congruences for the number of *n*-gons formed by *n* lines, *Amer. Math. Monthly* **67**, 961–966.

Catlin, P. A. (1979). Hajós's graph colouring conjecture: variations and counter-examples, *J. Combinatorial Theory (B)* **26**, 268–274.

Cayley, A. (1889). A theorem on trees, *Q. J. Pure Appl. Math.* **23**, 376–378. See also *The Collected Papers of A. Cayley*, Cambridge, 1897, vol. 13, pp. 26–28.

Chen, L. H. Y. (1975). Poisson approximation for dependent trials, *Annls Probab.* **3**, 534–535.

Chernoff, H. (1952). A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, *Annls Math. Statist.* **23**, 493–509.

Chowla, S., Herstein, I. N. and Moore, K. (1951). On recursions connected with symmetric groups, *Canand, J. Math.* **3**, 328–334.

Christofides, N. (1971). An algorithm for the chromatic number of a graph, *Comput. J.* **14**, 38–39.

Chung, F. R. K. (1978). On concentrators, superconcentrators, generalizers and nonblocking networks, *Bell Syst. Tech. J.* **58**, 1765–1777.

Chung, F. R. K. (1981). A note on constructive methods for Ramsey numbers, *J. Graph Theory* **5**, 109–113.

Chung, F. R. K. and Graham, R. L. (1978). On graphs that contain all small trees, *J. Combinatorial Theory (B)* **24**, 14–23.

Chung, F. R. K. and Graham, R. L. (1989). Quasi-random hypergraphs, *Proc. Nato. Acad. Sci. U.S.A.* **86**, 8175–8177.

Chung, F. R. K. and Graham, R. L. (1990). Quasi-random hypergraphs, *Random Structures and Algorithms* **1**, 105–124.

Chung, F. R. K. and Graham, R. L. (1991*a*). Quasi-random set systems, *J. Amer. Math. Soc.* **4**, 151–196.

Chung, F. R. K. and Graham, R. L. (1991*b*). Quasi-random tournaments, *J. Graph Theory* **15**, 173–198.

Chung, F. R. K., Graham, R. L. and Wilson, R. M. (1989). Quasi-random graphs, *Combinatorica* **9**, 345–362.

Chung, F. R. K. and Grinstead, C. M. (1983). A survey of bounds for classical Ramsey numbers, *J. Graph Theory* **7**, 25–37.

Chung, F. R. K., Erdős, P., Graham, R. L., Ulam, S. M. and Yao, F. F. (1979). Minimal decompositions of two subgraphs into pairwise isomorphic subgraphs, *Proc. Tenth Southeastern Conf. on Combinatorics, Graph Theory and Computing*, vol. I, Congressus Numerantium XXIII, Utilitas Math., Winnipeg, 1979, pp. 3–18.

Chung, K. L. (1974). *A course in Probability Theory* (2nd Edn). *Probability and Mathematical Statistics* **21**. Academic Press, New York, London.

Chvátal, V. (1977). Determining the stability number of a graph, *SIAM J. Comput.* **6**, 643–662.

Chvátal, V. (1991). Almost all graphs with 1.44 n edges are 3-colourable, *Random Structures, Algorithms* **2**, 11–28.

Chvátal, V., Rödl, V., Szemerédi, E. and Trotter, W. T. (1983). The Ramsey number of a graph with bounded maximum degree, *J. Combinatorial Theory (B)* **34**, 239–243.

Clarke, L. E. (1958). On Cayley's formula for counting trees, *J. Lond. Math. Soc.* **33**, 471–474.

Cohen, J., Komlós, J. and Mueller, T. (1979). The probability of an interval graph, and why it matters, *Proc. Symp. Pure Math.* **34**, 97–115.

Comtet, L. (1974). *Advanced Combinatorics.* D. Reidel, Dordrecht, Holland, vii + 343pp.

Cooper and Frieze (1994). Hamilton cycles in a class of random directed graphs, *J. Combinatorial Theory* (B) **62**, 151–163.

Cooper, C. and Frieze, A. (1995). On the connectivity of random k-th nearest neighbour graphs, *Combinatonics, Probab., Computing* **4**, 343–362.

Cooper, C. and Frieze, A. (2000). Hamilton cycles in random graphs and directed graphs, *Random Structures, and Algorithms* **16**, 369–401.

Cooper, C., Frieze, A. and Molloy, M. (1994). Hamilton cycles in random regular digraphs, *Combinatorics, Prob. Computing* **3**, 39–49.

Cooper, C., Frieze, A., Molloy, M. and Reed, B. (1996). Perfect matchings in random r-regular, s-uniform hypergraphs, *Combinatorics, Prob. Computing* **5**, 1–14.

Coppersmith, D. and Sorkin, G. (1999). Constructive bounds and exact expectations for the random assignment problem, *Random Structures and Algorithms* **15**, 113–144.

Coppersmith, D. and Sorkin, G. B. (2001). On the expected incremental cost of a minimum assignment, *Contemporary Combinatorics*, to appear.

Corneil, D. G. and Graham, B. (1973). An algorithm for determining the chromatic number of a graph, *SIAM J. Comput.* **2**, 311–318.

Cornuejols, G. (1981). Degree sequences of random graphs, unpublished preprint.

Damerell, R. M. (1973). On Moore graphs, *Math. Proc. Camb. Phil. Soc.* **74**, 227–236.

Delorme, C. (1985). Large bipartite graphs with given degree and diameter, *J. Graph Theory* see Q3.

Delorme, C. and Farhi, G. (1984). Large graphs with given degree and diameter, *IEEE Trans. Comput.* **33**, 857–860.

Donath, W. E. (1969). Algorithm and average – value bounds for assignment problems, *IBM J. Res. Dev.* **13**, 380–386.

Doyle, J. and Rivert, R. (1976). Linear expected time of a simple union–find algorithm, Info. *Process. Lett.* **5**, 146–148.

Dvoretzky, A. and Erdős, P. (1959). Divergence of random power series, *Michigan Math. Journal* **6**, 343–347.

Dyer, M., and Frieze, A. (1991). Randomized greedy matching, *Random Structures, Algorithms* **2**, 29–45.

Dyer, M., Frieze, A. and Jerrum, M. (1998). Approximately counting Hamilton paths and cycles in dense graphs, *SIAM J. Comput.* **27**, 1262–1272.

Dyer, M. E., Frieze, A. M. and McDiarmid, C. J. H. (1986). On linear programs with random costs, *Math. Program.* **35**, 3–16.

Dyer, M., Frieze, A. and Pittel, B. (1993). The average performance of the greedy matching algorithm, *Ann. of Appl. Prob.* **3**, 526–552.

Ebert, W. and Hafner, R. (1971). Die asymptotische Verteilung von Koinzidenzen, *Z. Wahrscheinlichkeitstheorie verwand. Gebiete* **18**, 322–332.

Edwards, C. S. and Elphick, C. H. (1983). Lower bounds for the clique and the chromatic numbers of a graph, *Discrete Appl. Math.* **5**, 51–64.

Egorychev, G. P. (1980*a*). New formulae for the permanent, *Dokl. Akad. Nauk SSSR* **254**, 784–787 (in Russian).

Egorychev, G. P. (1980*b*). A solution of a problem of van der Waerden for permanents, Inst. Fiziki im. L.V. Kirenskogo, S.S.S.R. Akad. Nauk, Siberian Branch, preprint IFSO-13M, Krasnoyarsk (in Russian).

Eigen, M. and Schuster, P. (1979). *The Hypercycle—A Principle of Natural Selforganization*, Springer-Verlag, Heidelberg.

Elspas, B. (1964). Topological constraints on interconnection limited logic, *Switching Circuit Theory, Logical Design* **5**, 133–147.

Epihin, V. V. (1972). An estimate of the probability of connectedness of a graph, *Systems for the Distribution of Information*. Izdat. Nauka, Moscow, pp. 124–127 (in Russian).

Erdős, P. (1945). On a lemma of Littlewood and Offord, *Bull. Amer. Math. Soc.* **51**, 898–902.

Erdős, P. (1947). Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.* **53**, 292–294.

Erdős, P. (1957). Some remarks on a theorem of Ramsey, *Bull. Res. Council Israel, Section F* **7**, 21–24.

Erdős, P. (1959). Graph theory and probability, *Canad. J. Math.* **11**, 34–38.

Erdős, P. (1961). Graph theory and probability II, *Canad. J. Math.* **13**, 346–352.

Erdős, P. (1962). On circuits and subgraphs of chromatic graphs, *Mathematika* **9**, 170–175.

Erdős, P. (1963*a*). Some applications of probability to graph theory and combinatorial problems. In *Theory of Graphs and Applications*, Proc. Symp. held in Smolenice, June 1963. Academia, Praha (1964), pp. 133–136.

Erdős, P. (1963*b*). On a problem in graph theory, *Math. Gaz.* **47**, 220–223.

Erdős, P. (1967). Some remarks on chromatic graphs, *Coll. Math.* **16**, 253–256.

Erdős, P. (1970). Topics in combinatorial analysis, *Proc. Louisiana Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, pp. 2–19.

Erdős, P. (1974*a*). Problems and results on finite and infinite graphs. In *Recent Advances in Graph Theory*, Proc. Symp. Prague. Academia, Praha (1975), pp. 183–192.

Erdős, P. (1974*b*). Some new applications of probability methods to combinatorial analysis and graph theory, *Proc. Fifth Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, pp. 39–51.

Erdős, P. (1978). Problems and results in combinatorial analysis and combinatorial number theory, *Proc. Ninth Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Congressus Numerantium XXI, Utilitas Math., Winnipeg, pp. 29–40.

Erdős, P. (1979). Some old and new problems in various branches of combinatorics, *Proc. Tenth Southeastern Conf. on Combinatorics, Graph Theory and Computing*, vol. 1. *Congressus Numerantium* **XXIII**, Utilitas Math., Winnipeg, pp. 19–37.

Erdős, P. (1981*a*). Problems and results in graph theory. *The Theory and Applications of Graphs* (Chartrand, G., Ed.). John Wiley & Sons.

Erdős, P. (1981*b*). Solved and unsolved problems in combinatorics and combinatorial number theory, *Congressus Numerantium* **32**, 49–62.

Erdős, P. and Fajtlowicz, S. (1981). On the conjecture of Hajós, *Combinatorica* **1**, 141–143.

Erdős, P., Fajtlowicz, S. and Hoffman, A. J. (1980). Maximum degree in graphs of diameter 2, *Networks* **10**, 87–90.

Erdős, P. and Hall, R. R. (1976). Probabilistic methods in group theory, II, *Houston J. Math.* **2**, 173–180.

Erdős, P. and Hall, R. R. (1978). Some new results in probabilistic group theory, *Comment. Math. Helv.* **53**, 448–457.

Erdős, P. and Kaplansky, I. (1946). The asymptotic number of Latin rectangles, *Amer. J. Math.* **68**, 230–236.

Erdős, P., Kleitman, D. J. and Rothschild, B. L. (1976). Asymptotic enumeration of K_n-free graphs. In *Teorie Combinatorie*, vol. II. Accademia Naz. dei Lincei, Rome, pp. 19–27.

Erdős, P. and Lovász, L. (1975). Problems and results on 3-chromatic hypergraphs and some related results. *Infinite and Finite Sets* (Hajnal, A., Rado, R. and Sós, V. T., Eds). Coll. Math. Soc. J. Bolyai, vol. 11, Budapest, pp. 609–627.

Erdős, P. and Moon, J. W. (1965). On sets of consistent arcs in a tournament,

Canad. Math. Bull. **8**, 269–271.
Erdős, P. and Pach, J. (1983). On a quasi-Ramsey problem, *J. Graph Theory* **7**, 137–147.
Erdős, P. and Palka, Z. (1983). Trees in random graphs, *Discrete Math.* 145–150; Addendum: **48**, 31 (1984).
Erdős, P., Palmer, E. M. and Robinson, R. W. (1983). Local connectivity of a random graph, *J. Graph Theory* **7**, 411–417.
Erdős, P. and Rényi, A. (1959). On random graphs I, *Publ. Math. Debrecen* **6**, 290–297.
Erdős, P. and Rényi, A. (1960). On the evolution of random graphs, *Publ. Math. Inst. Hungar. Acad. Sci.* **5**, 17–61.
Erdős, P. and Rényi, A. (1961*a*). On the evolution of random graphs, *Bull. Inst. Int. Statist. Tokyo* **38**, 343–347.
Erdős, P. and Rényi, A. (1961*b*). On the strength of connectedness of a random graph, *Acta Math. Acad. Sci. Hungar.* **12**, 261–267.
Erdős, P. and Rényi, A. (1962). On a problem in graph theory, *Publ. Math. Inst. Hungar. Acad. Sci.* **7**, 215–227 (in Hungarian).
Erdős, P. and Rényi, A. (1963). Asymmetric graphs, *Acta Math. Sci. Hungar.* **14**, 295–315.
Erdős, P. and Rényi, A. (1964). On random matrices, *Publ. Math. Inst. Hungar. Acad. Sci.* **8**, 455–461.
Erdős, P. and Rényi, A. (1965). Probabilistic methods in group theory, *J. d'Anal. Math.* **14**, 127–138.
Erdős, P. and Rényi, A. (1966). On the existence of a factor of degree one of a connected random graph, *Acta Math. Acad. Sci. Hungar.* **17**, 359–368.
Erdős, P. and Rényi, A. (1968). On random matrices II, *Studia Sci. Math. Hungar.* **3**, 459–464.
Erdős, P., Rényi, A. and Sós, V. T. (1966). On a problem of graph theory, *Studia Sci. Math. Hungar.* **1**, 215–235.
Erdős, P. and Spencer, J. (1972). Imbalances in k-colorations, *Networks* **1**, 379–385.
Erdős, P. and Spencer, J. (1974). *Probabilistic Methods in Combinatorics.* Academic Press, New York, London.
Erdős, P. and Spencer, J. (1979). Evolution of the n-cube, *Comput. Math. Applics* **5**, 33–39.
Erdős, P. and Szekeres, G. (1934). Über die Anzahl der Abelschen Gruppen gegebener Ordnung, *Acta Litt. Sci. Szeged* **7**, 95–102.
Erdős, P. and Szekeres, G. (1935). A combinatorial problem in geometry, *Compositio Math.* **2**, 463–470.
Erdős, P. and Turán, P. (1965). On some problems of statistical group theory I, *Z. Wahrscheinlichkeitstheorie verwand. Gebiete* **4**, 175–186.
Erdős, P. and Turán, P. (1967*a*, 1967*b*, 1968). On some problems of statistical group theory II, III and IV, *Acta Math. Acad. Sci. Hungar.* **18**, 151–163; **18**, 309–320; **19**, 413–435.
Erdős, P. and Wilson, R. J. (1977). On the chromatic index of almost all graphs, *J. Combinatorial Theory (B)* **23**, 255–257.
Essam, J. W. (1971). Graph theory and statistical physics, *Discrete Math.* **1**, 83–112.
Even, S. and Tarjan, R. E. (1975). Network flow and testing graph connectivity, *SIAM J. Comput.* **4**, 507–518.
Fagin, R. (1976). Probabilities on finite models, *J. Symbolic Logic* **41**, 50–58.

Fajtlowicz, S. (1977). The independence ratio for cubic graphs, *Proc. Eighth South-eastern Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, pp. 273–277.

Fajtlowicz, S. (1978). On the size of independent sets in graphs, *Proc. Ninth South-eastern Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, pp. 269–274.

Falikman, D. I. (1981). A proof of van der Waerden's conjecture on the permanent of a doubly stochastic matrix, *Mat. Zametki* **29**, 931–938 (in Russian).

Fararo, T. J. and Sunshine, M. (1964). *A Study of a Biased Friendship net*, Syracuse Univ. Press, Syracuse, New York.

Feller, W. (1945). The fundamental limit theorems in probability, *Bull. Amer. Math. Soc.* **51**, 800–832.

Feller, W. (1966). *An Introduction to Probability Theory and its Applications*, vols I and II. John Wiley and Sons, New York, London, Sydney.

Fenner, T. I. and Frieze, A. M. (1982). On the connectivity of random m-orientable graphs and digraphs, *Combinatorica* **2**, 347–359.

Fenner, T. I. and Frieze, A. M. (1983). On the existence of Hamiltonian cycles in a class of random graphs, *Discrete Math.* **45**, 301–305.

Fenner, T. I. and Frieze, A. M. (1984). Hamiltonian cycles in random regular graphs, *J. Combinatorial Theory (B)* **37**, 103–112.

Fillenbaum, S. and Rapoport, A. (1971). *Subjects in the Subjective Lexicon.* Academic Press, New York.

Filotti, I. S., Miller, G. L. and Reif, J. (1979). On determining the genus of a graph in $O(v^{O(g)})$ steps, *Proc. Eleventh Annual ACM Symp. on Theory of Computing*, Atlanta, Georgia, pp. 27–37.

Flajolet, P., Knuth, D. E. and Pittel, B. (1989). The first cycles in an evolving graph, *Discrete Math.* **75**, 167–215.

Folkert, J. E. (1955). The distribution of the number of components of a random mapping function, Ph.D. Dissertation, Michigan State University.

Ford, G. W. and Uhlenbeck, G. E. (1957). Combinatorial problems in the theory of graphs, *Proc. Natn. Acad. Sci. U.S.A.* **43**, 163–167.

Frank, H. and Frisch, I. (1971). *Communication, Transmission and Transportation Networks.* Addison–Wesley, Reading, Massachusetts.

Frank, H., Kahn, R. E. and Kleinrock, L. (1972). Computer communication network design—experience with theory and practice, *AFIPS Conf. Proc.* **40**, 255–270.

Frank, O. (1977). Survey sampling in graphs, I, *Statist. Plan. Info.* **1**, 235–264.

Frank, O. (1978). Estimation of the number of connected components in a graph by using a sampled subgraph, *Scand. J. Statist.* **5**, 177–188.

Frank, O. (1979*a*). Estimating a graph from triad counts, *J. Statist. Comput. Simul.* **9**, 31–46.

Frank, O. (1979*b*). Moment properties of subgraph counts in stochastic graphs, *Annls N. Y. Acad. Sci.* **319**, 207–218.

Frank, O. (1981). A survey of statistical methods for graph analysis. In *Sociological Methodology 1981* (Leinhardt, S., Ed.). Jossey–Bass, San Francisco, pp. 110–115.

Frank, O. and Harary, F. (1980*a*). Balance in stochastic signed graphs, *Social Networks* **2**, 155–163.

Frank, O. and Harary, F. (1980*b*). Maximum triad counts in graphs and digraphs, *J. Combinatorics, Info. Systems Sci.* **5**, 1–9.

Fréchet, M. (1940). Les probabilités associées à un système d'événements compatibles et dépendants, Actualité Scient. et Ind., Hermann, Partie 1, No. 859, Paris.

Frenk, J. B. G., van Houweninge, M. and Rinnooy Kan, A. H. G. (1987). Order statistics and the linear assignment problem, *Computing* **39**, 165–174.

Friedgut, E. (1999). Sharp thresholds for graph properties, and the k-sat problem, with an appendix by Jean Bourgain, *J. Amer. Math. Soc.* **12**, 1017–1054.

Friedland, S. (1979). A lower bound for the permanent of a doubly stochastic matrix, *Annls Math.* (2) **111**, 167–176.

Friedman, H. D. (1966). A design for (d,k) graphs, *IEEE Trans. Comput.* **15**, 253–254.

Friedman, H. D. (1971). On the impossibility of certain Moore graphs, *J. Combinatorial Theory (B)* **10**, 245–252.

Frieze, A. M. (1985*a*). On the value of a random minimum spanning tree problem, *Discrete Appl. Math.* **10**, 47–56.

Frieze, A. M. (1985*b*). Limit distribution for the existence of Hamilton cycles in random bipartite graphs, *Europ. J. Combinatorics* **6**, 327–334.

Frieze, A. M. (1985*c*). Maximum matchings in a class of random graphs (to appear).

Frieze, A. M. (1985*d*). On large matchings and cycles in sparse random graphs see Q3.

Frieze, A. M. (1987). Parallel algorithms for finding Hamilton cycles in random graphs, *Info. Process. Letters* **25**, 111–117.

Frieze, A. M. (1988). Finding Hamilton cycles in sparse random graphs, *Combinatorial Theory (B)* **44**, 230–250.

Frieze, A. M. (1990). On the independence number of random graphs, *Discrete Math.* **81**, 171–175.

Frieze, A., and Janson, S. (1995). Perfect matchings in random s-uniform hypergraphs, *Random Structures and Algorithms* **7**, 41–57.

Frieze, A., Jerrum, M., Molloy, M., Robinson, R. and Wormald, N. (1996). Generating and counting Hamilton cycles in random regular graphs, *J. Algorithms* **21**, 176–198.

Frieze, A., Karoński, M. and Thomo, L. (1999). On perfect matchings and Hamilton cycles in sums of random trees, *SIAM J. Discrete Math.* **12**, 208–216.

Frieze, A. M. and Luczak, T. (1990). Hamiltonian cycles in a class of random graphs: one step further, *Proceedings of Random Graphs 187* (Karoński, M., Jaworski, J. and Ruciński, A., Eds), John Wiley, Chichester, 53–59.

Frieze, A. M. and Luczak, T. (1992). On the independence and chromatic numbers of random regular graphs, *J. Combinatorial Theory (B)*, **54**, 123–132.

Frieze, A. M. and McDiarmid, C. J. H. (1989). On random minimum length spanning trees, *Combinatorica* **9**, 363–374.

Frieze, A., Radcliffe, A. J. and Suen, S. (1995). Analysis of a simple greedy matching algorithm on random cubic graphs, combinatorics, *Prob. Computing* **4**, 47–66.

Frieze, A. and Suen, S. (1992). Counting the number of Hamilton cycles in random digraphs, *Random Structures and Algorithms* **3**, 235–241.

Frieze, A. and Suen, S. (1994). On the independence number of random cubic graphs, *Random Structures and Algorithms* **5**, 649–664.

Frucht, R. (1949). Graphs of degree 3 with given abstract group, *Canad. J. Math.* **1**, 365–378.

Fu, Y. and Yau, S. S. (1962). A note on the reliability of communication networks, *J. Soc. Ind. Appl. Math.* **10**, 469–474.

Füredi, Z. and Komlós, J. (1981). The eigenvalues of random symmetric matrices, *Combinatorica* **1**, 233–241.

Furst, M., Hopcroft, J. and Luks, E. (1980). Polynomial-time algorithms for permutation groups, *21st Annual IEEE Symp. on Foundations of Computer Science.*

Gabber, O. and Gabil, Z. (1979). Explicit constructions of linear superconcentrators, *IEEE* 364–370.

Gaifman, H. (1964). Concerning measures of first-order calculi, *Israel J. Math.* **2**, 1–17.

Galambos, J. (1966). On the sieve methods in probability theory I, *Studia Sci. Math. Hungar.* **1**, 39–50.

Galambos, J. and Rényi, A. (1968). On quadratic inequalities in probability theory, *Studia Sci. Math. Hungar.* **3**, 351–358.

Garey, M. R., Graham, R. L. and Ullman, J. D. (1972). Worst-case analysis of memory allocation algorithms, *Proc. 4th Annual ACM Symp. on the Theory of Computing*, pp. 143–150.

Garey, M. R. and Johnson, D. S. (1976). The complexity of near-optimal graph colouring, *J. Ass. Comput. Machinery* **23**, 43–49.

Gazmuri, P. G. (1984). Independent sets in random sparse graphs, *Networks* **14**, 367–377.

Gertsbakh, I. B. (1977). Epidemic processes on a random graph: some preliminary results, *J. Appl. Probab.* **14**, 427–438.

Gilbert, E. N. (1956). Enumeration of labelled graphs, *Canad. J. Math.* **8**, 405–411.

Gilbert, E. N. (1959). Random graphs, *Annls Math. Statist.* **30**, 1141–1144.

Gilbert, E. N. (1961). Random plane networks, *J. Soc. Ind. Appl. Math.* **9**, 533–543.

Gilbert, E. N. (1964). Random minimal trees, *J. Soc. Ind. Appl. Math.* **13**, 376–387.

Gimadi, E. H. and Perepelica, V. A. (1973). A statistically effective algorithm for finding a Hamilton path (cycle), *Diskret. Anal.* **22**, 15–28 (in Russian).

Gleason, A. M. (1960). A search problem on the n-cube, *Proc. Symp. Appl. Math.* vol. X. American Mathematical Society, Providence, pp. 175–179.

Göbel, F. (1963). *Mutual Choices.* Stichtung Mathematisch Centrum Amsterdam, S317 (VP22).

Göbel, F. and Jagers, A. A. (1974). Random walks on graphs, *Stochastic Process. Applics* **2**, 311–336.

Godehardt, E. (1980). Eine Erweiterung der Sätze vom Erdős–Rényi-Typ auf ungerichtete, vollständig indizierte Zufallsmultigraphen. Inaugural Dissertation, Universität Düsseldorf, ii + 128 pp.

Godehardt, E. (1981). An extension of the theorems of Erdős–Rényi-type to random multigraphs. In *Proceedings Sixth Conference on Probability Theory* (Bereanu, B., Grigorescu, S., Josifescu, M. and Postelnicu, T., Eds). Editura Academiei, Bucharest, pp. 417–425.

Godehardt, E. and Steinbach, J. (1981). On a lemma of P. Erdős and A. Rényi about random graphs, *Publ. Math. Debrecen* **28**, 271–273.

Goethals, J. M. and Seidel, J. J. (1967). Orthogonal matrices with zero diagonal, *Canad. J. Math.* **19**, 1001–1010.

Goethals, J. M. and Seidel, J. J. (1970). Strongly regular graphs derived from combinatorial designs, *Canad. J. Math.* **22**, 597–614.

Golomb, S. W. (1964). Random permutations, *Bull. Amer. Math. Soc.* **70**, 747.

Goncharov, V. L. (1942). Sur la distribution des cycles dans les permutations, *C.r. Acad. Sci. USSR (N.S.)* **35**, 267–269.

Goncharov, V. L. (1944). From the realm of combinatorics, *Izv. Akad. Nauk SSSR, Ser. Matem.* **8**, 3–48 (in Russian). (Translated as On the field of combinatory analysis, *Transl. Amer. Math. Soc. Ser.* **2** (1962), 1–46.)

Goemans, M. X. and Kodiabam, M. S. (1993). A lower bound on the expected cost of an optimal assignment, *Math. Oper. Res.* **18**, 267–274.

Gordon, M. and Leonis, C. G. (1976). Combinatorial short-cuts to statistical weights and enumeration of chemical isomers, *Proc. Fifth British Combinatorial Conf. Congressus Numerantium*, **XV**, Utilitas Math., Winnipeg, Manitoba, pp. 231–238.

Gould, H. W. (1972). *Combinatorial Identities* (Revised Edn). Morgantown, Morgantown, West Virginia, p. 15.

Goulden, I. P. and Jackson, D. M. (1983). *Combinatorial Enumeration.* Wiley–Interscience Series in Discrete Math., John Wiley and Sons, New York, Chichester, Brisbane, Toronto, Singapore, xxiv + 569 pp.

Gradshteyn, I. S. and Ryzhik, I. M. (1980). *Table of Integrals, Series and Products* (Corrected and enlarged Edn). Academic Press, New York, London, Toronto, Sydney, San Francisco, xiv + 1160 pp.

Graham, R. L. and Spencer, J. H. (1971). A constructive solution to a tournament problem, *Canad. Math. Bull.* **14**, 45–48.

Graham, R. L., Rothschild, B. L. and Spencer, J. H. (1980). *Ramsey Theory.* Wiley–Interscience Series in Mathematics, John Wiley and Sons, New York, Chichester, Brisbane, Toronto, ix + 174 pp. Second Edn. 1990, xii + 196 pp.

Graver, J. E. and Yackel, J. (1968). Some graph theoretic results associated with Ramsey's theorem, *J. Combinatorial Theory* **4**, 125–175.

Gray, P. M. D., Murray, A. M. and Young, N. A. (1977). Wright's formulae for the number of connected sparsely edged graphs, *J. Graph Theory* **1**, 331–334.

Greenwell, D. L. and Hoffman, D. G. (1981). On a probabilistic method in graph theory, *J. Combinatorial Theory (B)* **31**, 344–347.

Greenwood, R. E. and Gleason, A. M. (1955). Combinatorial relations and chromatic graphs, *Canad. J. Math.* **7**, 1–7.

Griggs, J. R. (1980). The Littlewood–Offord problem: tightest packing and an M-part Sperner theorem, *Europ. J. Combinatorics* **1**, 225–234.

Griggs, J. R. (1983*a*). Lower bounds on the independence number in terms of the degrees, *J. Combinatorial Theory (B)* **34**, 22–39.

Griggs, J. R. (1983*b*). An upper bound on the Ramsey numbers $R(3,k)$, *J. Combinatorial Theory (A)* **35**, 145–153.

Griggs, J. R., Lagarias, J. C., Odlyzko, A. M. and Shearer, J. B. (1983). On the tightest packing of sums of vectors, *Europ. J. Combinatorics* **4**, 231–236.

Grimmett, G. R. (1980). Random graphs. *Further Selected Topics in Graph Theory* (Beineke, L. and Wilson, R. J., Eds). Academic Press, London, New York, San Francisco.

Grimmett, G. (1999). *Percolation*, 2nd edn, grundlehren der Mathematischen Wissenschaften, vol. **321**, Springer-Verlag, Berlin, xiv + 444 pp.

Grimmett, G. R. and McDiarmid, C.J.H. (1975). On colouring random graphs,

Math. Proc. Camb. Phil. Soc. **77**, 313–324.
Gurevich, Y. and Shelah, S. (1987). Expected computation time for Hamiltonian path problem, *SIAM J. Comput.* **16**, 486–502.
Györi, E., Rothschild, B. and Ruciński, A. (1985). Every graph is contained in a sparsest possible balanced graph, *Math. Proc. Comb. Phil. Soc.* **98**, 397–401.
Hadley, G. (1964). Nonlinear and dynamical programming. *Series in Management Science and Economics*, vol. 2. Addison–Wesley, Reading, Massachusetts, xi + 484 pp.
Hadwiger, H. (1943). Streckenkomplexe, *Vierteljschr. Naturforsch. Ges. Zürich* **88**, 133–142.
Hafner, R. (1972*a*). Die asymptotische Verteilung von mehrfachen Koinzidenzen, *Z. Wahrscheinlichkeitstheorie verwand. Gebiete* **21**, 96–108.
Hafner, R. (1972*b*). The asymptotic distribution of random clumps, *Computing* **10**, 335–351.
Häggkvist, R. and Hell, P. (1980). Graphs and parallel comparison algorithms, *Proc. Eleventh Southeastern Conf. on Combinatorics, Graph Theory and Computing, Congressus Numerantium* **29**, 497–509.
Häggkvist, R. and Hell, P. (1981). Parallel sorting with constant time for comparisons, *SIAM J. Comput.* **10**, 465–472.
Häggkvist, R. and Hell, P. (1982). Sorting and merging in rounds, *SIAM J. Algebra, Discrete Meth.* **3**, 465–473.
Halberstam, F. Y. and Quintas, L. V. (1982). Distance and path degree sequences for cubic graphs. Mathematics Department, Pace University, New York.
Halberstam, F. Y. and Quintas, L. V. (1984). A note on tables of distance and path degree sequences for cubic graphs, Mathematics Department, Pace University, New York.
Hall, R. R. (1972). On a theorem of Erdős and Rényi concerning Abelian groups, *J. Lond. Math. Soc. (2)* **5**, 143–153.
Hall, R. R. (1977). Extensions of a theorem of Erdős–Rényi in probabilistic group theory, *Houston J. Math.* **3**, 225–234.
Hall, R. R. and Sudbery, A. (1972). On a conjecture of Erdős and Rényi concerning Abelian groups, *J. Lond. Math. Soc. (2)* **6**, 177–189.
Harary, F. and Palmer, E. M. (1973). *Graphical Enumeration.* Academic Press, New York, London, xiv + 271 pp.
Harary, F. and Palmer, E. M. (1979). The probability that a point of a tree is fixed, *Math. Proc. Camb. Phil. Soc.* **85**, 407–415.
Harary, F. and Robinson, R. W. (1979). Labelled bipartite blocks, *Canad. J. Math.* **31**, 60–68.
Hardy, G. H. and Littlewood, J. E. (1914). Some problems of Diophantine approximation II, trigonometrical series associated with the elliptic θ-functions, *Acta Math.* **37**, 193–238.
Hardy, G. H. and Littlewood, J. E. (1925). Some problems of Diophantine approximation: an additional note on the trigonometrical series associated with the elliptic θ-functions, *Acta Math.* **47**, 189–198.
Harper, L. H. (1964). Optimal assignments of numbers to vertices, *SIAM J. Appl. Math.* **12**, 131–135.
Harper, L. H. (1966*a*). Optimal numberings and isoperimetric problems on graphs, *J. Combinatorial Theory* **1**, 385–394.
Harper, L. H. (1966*b*). Minimal numberings and isoperimetric problems on cubes. In *Theory of Graphs, International Symposium*, Rome, 1966. Gordon and Breach, New York, Dunod, Paris (1967), pp. 151–152.

Harris, B. (1960). Probability distributions related to random mappings. *Annls Math. Statist.* **31**, 1045–1062.

Hart, S. (1976). A note on the edges of the *n*-cube, *Discr. Math.* **14**, 157–163.

Hartwell, B. L. (1979). The optimum defence against random subversions in a network, *Proc. Tenth Southeastern Conf. on Combinatorics, Graph Theory and Computing*, vol. II. *Congressus Numerantium* **XXIII**, Utilitas Math., Winnipeg, pp. 493–499.

Heap, B. R. (1966). Random matrices and graphs, *Num. Mathematik* **8**, 114–122.

Held, M. and Karp, R. (1962). A dynamic programming approach to sequencing problems, *SIAM J. Appl. Math.* **10**, 196–210.

Hirschberg, D. S. (1978). Fast parallel sorting algorithms, *Commun. ACM* **21**, 657–661.

Hoeffding, W. (1963). Probability inequalities for sums of bounded random variables, *J. Amer. Statist. Ass.* **58**, 13–30.

Hoffman, A. J. and Singleton, R. R. (1960). On Moore graphs with diameters 2 and 3, *IBM J. Res. Dev.* **4**, 497–504.

Hoffmann, C. M. (1980). Testing isomorphism of cone graphs, *Proc. Twelfth Annual Symp. on Theory of Computing*, pp. 244–251.

Hoffmann, C. M. (1982). *Group-Theoretic Algorithms and Graph Isomorphism.* Lecture Notes in Computer Science 136. Springer-Verlag, Berlin, Heidelberg, New York, 311 pp.

Holgate, P. (1969). Majorants of the chromatic number of a random graph, *J. R. Statist. Soc.* **31**, 303–309.

Hopcroft, J. E. and Tarjan, R. E. (1972). Isomorphism of planar graphs. In *Complexity of Computations* (Miller, R. E. and Thatcher, J. W., Eds). Plenum Press, New York, pp. 131–152.

Hopcroft, J. E. and Tarjan, R. E. (1974). Efficient planarity testing. *Ass. Comput. Machinery* **21**, 549–568.

Hopcroft, J. E. and Wong, J. K. (1974). Linear time algorithm for isomorphism of planar graphs, *Proc. Sixth Annual ACM Symp. on Theory of Computing*, Seattle, Washington, pp. 172–184.

Hopkins, G. W. and Staton, W. (1982). Girth and independence ratio, *Canad. Math. Bull.* **25**, 179–186.

Huber, P. J. (1963). A remark on a paper of Trawinski and David entitled: 'Selection of the best treatment in a paired-comparison experiment', *Annls Math. Statist.* **34**, 92–94.

Huberman, B. A. and Adamic, L. A. (1999). Growth dynamics of the world-wide web, *Nature* **401**, 131.

Hunt, G. A. (1951). Random Fourier transforms. *Trans. Amer. Math. Soc.* **71**, 38–69.

Ivchenko, G. I. (1973*a*). On the asymptotic behaviour of the degrees of vertices in a random graph, *Theory Probab. Applics* **18**, 188–195.

Ivchenko, G. I. (1973*b*). The strength of connectivity of a random graph, *Theory Probab. Applics* **18**, 396–403.

Ivchenko, G. I. (1975). Unequally probable random graphs, *Trudy Mosk. Inst. Electr. Mas.* **44**, 34–66 (in Russian).

Ivchenko, G. I. and Medvedev, I. V. (1973). The probability of connectedness in a class of random graphs, *Vopr. Kibernetiki, Moscow*, 60–66 (in Russian).

Ja'Ja, J. (1980). Time space tradeoffs for some algebraic problems, *Proc. 12th Annual ACM Symp. on Theory of Computing*, pp. 339–350.

Janson, S. (1987). Poisson convergence and Poisson processes with applications to random graphs, *Stochastic Process. Appl.* **26**, 1–30.

Janson, S. (1995). Random regular graphs: asymptotic distributions and contiguity, *Combinatorics, Probab. and Computing* **4**, 369–405.

Janson, S. (2001). On concentration of probability, *Contemporary Combinatorics*, to appear.

Janson, S., Knuth, D. E., Luczak, T. and Pittel, B. (1993). The birth of the giant component, *Random Structures, Algorithms* **3**, 233–358.

Janson, S., Luczak, T. and Ruciński, A. (1990). An exponential bound for the probability of nonexistence of a specified subgraph in a random graph, in *Random Graphs '87*, Proceedings, Poznań, 1987 (Karoński, M., Jaworski J. and Ruciński, A. Eds), John Wiley and Sons, Chichester, 73–87.

Janson, S., Luczak, T. and Ruciński, A. (2000). *Random Graphs*, John Wiley and Sons, New York, xi and 333 pp.

Jerrum, M. and Skyum, S. (1984). Families of fixed degree graphs for processor interconnection, *IEEE Trans. Comput.* **C-33**, 190–194.

Johansson, A. R. (2000). Asymptotic choice number of triangle-free graphs, to appear.

Johnson, D. S. (1973). *Near-optimal bin packing algorithms*, Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts.

Johnson, D. S. (1974*a*). Fast algorithms for bin packing, *J. Computer, Syst. Sci.* **8**, 272–314.

Johnson, D. S. (1974*b*). Worst case behaviour of graph colouring algorithms, *Fifth Southeastern Conf.*, pp. 513–527.

Johnson, D. S., Demers, A., Ullman, J. D., Garey, M. R. and Graham, R. L. (1974). Worst-case performance bounds for simple one-dimensional packing algorithms, *SIAM J. Comput.* **3**, 299–325.

Johri, A. and Matula, D. W. (1982). Probabilistic bounds and heuristic algorithms for coloring large random graphs, Tech. Rep., Dept. of Computer Science and Engineering, Southern Methodist University.

Jordan, Ch. (1926). Sur la probabilité des épreuves répétées, *Bull. Soc. Math. France* **54**, 101–137.

Jordan, Ch. (1927). Sur un cas généralisé de la probabilité des épreuves répétées, *Acta Sci. Math. (Szeged)* **3**, 193–210.

Jordan, Ch. (1934). La théorème de probabilité de Poincaré généralisé au cas de plusiers variables indépendantes, *Acta Sci. Math. (Szeged)* **7**, 103–111.

Jordan, K. (1927*a*). The basic concepts of probability theory, *Math. és Phys. Lapok* **34**, 101–136 (in Hungarian).

Juhász, F. (1981). On the spectrum of a random graph. In *Algebraic and Discrete Methods in Graph Theory* (Lovász, L. and Sós, V. T., Eds). Proc. Coll. Math. Soc. J. Bolyai 25, vol. I, pp. 313–316.

Kac, M. (1949). Probability methods in some problems of analysis and number theory, *Bull. Amer. Math. Soc.* **55**, 641–665.

Kahane, J.-P. (1963). Séries de Fourier Aléatoires, *Séminaire de Mathématique Supérieure*, Université de Montréal, vii + 174 pp.

Kahane, J.-P. (1968). *Some Random Series of Functions*. D. C. Heath and Co., Lexington, Massachusetts, viii + 184 pp.

Kahn, J., and Kim, J. H. (1998). Random matchings in regular graphs, *Combinatorica* **18**, 201–226.

Kalbfleisch, J. G. (1967). Upper bounds for some Ramsey numbers, *J. Combinatorial Theory* **2**, 35–42.

Kalbfleisch, J. G. (1971). On Robillard's bounds for Ramsey numbers, *Canad.*

Math. Bull. **14**, 437–440.
Kalbfleisch, J. G. (1972). Complete subgraphs of random hypergraphs and bipartite graphs, *Proc. Third Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, pp. 297–304.
Kalnins, A. A. (1970). Statistical estimate for the chromatic number of the graphs of some class, *Latvijskij Mat. Jez.* **7**, 111–125 (in Russian).
Karoński, M. (1982). A review of random graphs, *J. Graph Theory* **6**, 349–389.
Karoński, M. and Palka, Z. (1980). On the size of a maximal induced tree in a random graph, *Math. Slovaca* **30**, 151–155.
Karoński, M. and Palka, Z. (1981). Addendum and erratum to the paper 'On the size of a maximal induced tree in a random graph', *Math. Slovaca* **31**, 107–108.
Karoński, M. and Ruciński, A. (1983). Problem 4 in *Graphs and Other Combinatorial Topics*, Proceedings of the Third Czech. Symp. on Graph Theory, Prague, 1982, Teubner-Texte Math. **59**, Teubner, Leipzig.
Karp, R. M. (1972). Reducibility among combinatorial problems. In *Complexity of Computer Computations* (Miller, R. E. and Thatcher, J. W., Eds). Plenum Press, New York, pp. 85–104.
Karp, R. M. (1979). Probabilistic analysis of a canonical numbering algorithm for graphs, *Proc. Symposia in Pure Mathematics*, vol. 34. American Mathematical Society, Providence, Rhode Island, pp. 365–378.
Karp, R. M. (1987). An upper bound on the expected cost of an optimal assignment, *Discrete Algorithms and Complexity: Proceedings of the Japan–US Joint Seminar* (D.S. Johnson *et al*, Eds), Perspectives in Compating 15, Academic Press, pp. 1–4.
Karp, R. M. (1990) The transitive closure of a random digraph, *Random Structures, Algorithms* **1**, 73–93.
Karp, R. M., Rinnooy Kan, A. H. G. and Vohra, R. V. (1994). Average case analysis of a heuristic for the assignment problem, *Math. of Op. Res.* **19**, 513–522.
Karp, R. M. and Sipser, M. (1981). Maximum matchings in sparse random graphs, *IEEE Conf. on Computing*, pp. 364–375.
Katona, G. O. H. (1966). On a conjecture of Erdős and a stronger form of Sperner's theorem, *Studia Math. Sci. Hungar.*, 59–63.
Katona, G. O. H. (1969). Graphs, vectors and inequalities in probability theory, *Mat. Lapok* **20**, 123–127 (in Hungarian).
Katona, G. O. H. (1977). Inequalities for the distribution of the length of random vector sums, *Theory Probab. Applics* **22**, 450–464.
Katona, G. O. H., Nemetz, T. and Simonovits, M. (1964). On a problem of Turán in the theory of graphs, *Mat. Lapok* **15**, 228–238.
Katz, L. (1955). The probability of indecomposability of a random mapping function, *Annls Math. Statist.* **26**, 512–517.
Kelly, D. G. and Oxley, J. G. (1981). Threshold functions for some properties of random subjects of projective spaces, Math. Res. Rep. No. 7, Australian National University.
Kelly, D. G. and Oxley, J. G. (1982). Asymptotic properties of random subsets of projective spaces, *Math. Proc. Camb. Phil. Soc.* **91**, 119–130.
Kelly, D. G. and Tolle, J. W. (1978). Expected simplex algorithm behaviour for random linear programs, *Meth. Ops Res.* **31**. *Proc. Third Symp. on Operations Research*, Athenäum/Hain/Scriptor/Hanstein.
Kelmans, A. K. (1965). Some problems of the analysis of reliability of nets,

Automatika i Telemech. **26**, 567–574 (in Russian).
Kelmans, A. K. (1967*a*). On the connectedness of random graphs, *Automatika i Telemech.* **28**, 98–116 (in Russian).
Kelmans, A. K. (1967*b*). On some properties of the characteristic polynomial of a graph. In *Kibernetika na Sluzbu Kommunizma.* **4**, Gosenergoizdat, Moscow, Leningrad, 27–41 (in Russian).
Kelmans, A. K. (1970). Bounds on the probability characteristics of random graphs, *Automation, Remote Control* **31**, 1833–1839.
Kelmans, A. K. (1971). Problems in the analysis and synthesis of probabilistic networks, *Adaptive Systems, Large Systems.* Nauka, Moscow, pp. 264–273 (in Russian).
Kelmans, A. K. (1972*a*). Asymptotic formulas for the probability of k-connectedness of random graphs, *Theory Probab. Applics* **17**, 243–254.
Kelmans, A. K. (1972*b*). The connectivity of graphs having vertices which drop out randomly, *Automation, Remote Control* **33**, 316–620.
Kelmans, A. K. (1976*a*). Comparison of graphs by their number of spanning trees, *Discrete Math.* **16**, 241–261.
Kelmans, A. K. (1976*b*). Operations over graphs that increase the number of their spanning trees, *Issled. po Diskret. Optim* Nauka, Moscow, pp. 406–424 (in Russian).
Kelmans, A. K. (1977). Comparison of graphs by their probability of connectedness, *Kombinator. i Asimpt. Analiz, Krasnoyarsk* 69–81 (in Russian).
Kelmans, A. K. (1979). The graph with the maximum probability of remaining connected depends on the edge-removal probability, *Graph Theory Newsl.* **9**(1), 2–3.
Kelmans, A. K. (1980). Graphs with an extremal number of spanning trees, *J. Graph Theory* **4**, 119–122.
Kelmans, A. K. (1981). On graphs with randomly deleted edges, *Acta Math. Acad. Sci. Hungar.* **37**, 77–78.
Kelmans, A. K. and Chelnokov, V. M. (1974). A certain polynomial of a graph with the extremal number of trees, *J. Combinatorial Theory* (B) **16**, 197–214.
Kendall, M. G. and Babington-Smith, B. (1940). On the method of paired comparisons, *Biometrika* **33**, 239–251.
Kennedy, J. W. (1978). Random clumps, graphs and polymer solutions. *Theory and Applications of Graphs* (Alari, Y. and Lick, D. R., Eds). Lecture Notes in Mathematics, vol. 642. Springer-Verlag, New York, Berlin, Heidelberg, pp. 314–329.
Kim, J. H. (1995*a*). On Brooks' theorem for sparse graphs, *Combinatorial, Probab. Computing* **4**, 97–132.
Kim, J. H. (1995*b*). The Ramsey number $R(3, t)$ has order of magnitude $t^2/\log t$, *Random Structures and Algorithms* **7**, 173–207.
Kirousis, L. M., Kranakis, E., Krizanc, D. and Stamation, Y. (1998). Approximating the unsatisfiability threshold of random formulas, *Random Structures and Algorithms* **12**, 253–269.
Klawe, M. M. (1981). Non-existence of one-dimensional expanding graphs, *Proc. 22nd Annual Symp. on the Foundations of Computer Science*, Nashville, pp. 109–113.
Klawe, M. M., Corneil, D. G. and Proskurowski, A. (1982). Isomorphism testing in hookup classes, *SIAM J. Algebraic, Discrete Methods* **3**, 260–274.
Klee, V. L. and Larman, D. G. (1981). Diameters of random graphs. *Canad. J.*

Math. **33**, 618–640.
Klee, V. L., Larman, D. G. and Wright, E. M. (1980). The diameter of almost all bipartite graphs, *Studia Sci. Math. Hungar.* **15**, 39–43.
Klee, V. L., Larman, D. G. and Wright, E. M. (1981). The proportion of labelled bipartite graphs which are connected, *J. Lond. Math. Soc.* **24**, 397–404.
Kleinberg, J. (2000). A small-world phenomenon: an algorithmic perspective, to appear.
Kleitman, D. J. (1965). On a lemma of Littlewood and Offord on the distribution of certain sums, *Math. Z.* 251–259.
Kleitman, D. J. (1976). Some new results on the Littlewood–Offord problem, *J. Combinatorial Theory* (*A*) 89–113.
Kleitman, D. J. and Rothschild, B. L. (1975). Asymptotic enumeration of partial orders on a finite set, *Trans. Amer. Math. Soc.* **205**, 205–220.
Knuth, D. E. (1967). Improved constructions for the Floyd–Bose–Nelson sorting problem. Preliminary report. *A.M.S. Notices* **14**.
Knuth, D. E. (1973). *The Art of Computer Programming*, vol. 3, *Sorting and Searching*. Addison–Wesley, Reading, Massachusetts, xi + 723 pp.
Knuth, D. E. (1981). A permanent inequality, *Amer. Math. Monthly* **88**, 731–740.
Knuth, D. E. (2000), *Selected Papers on Analysis of Algorithms*, CSLI Lecture notes., **102**, CSLI Publications, Stanford, California, *xvi* + 621 pp.
Knuth, D. E. and Floyd, R. W. (1967). Improved constructions for the Bose–Nelson sorting problem, *A.M.S. Notices* **14**, 283.
Knuth, D. E. and Schönhage, A. (1978). The expected linearity of a simple equivalence algorithm, *Theor. Comput. Sci.* **6**, 281–315.
Kolchin, V. F. (1977). Branching processes, random trees and a generalized occupancy scheme, *Mat. Zametki* **21**, 386–394 (in Russian).
Komlós, J. (1967). On the determinant of (0, 1)-matrices, *Studia Sci. Math. Hungar.* **2**, 7–21.
Komlós, J. (1968). On the determinant of random matrices, *Studia Sci. Math. Hungar.* **3**, 387–399.
Komlós, J. and Sulyok, M. (1970). On the sum of elements of ± 1 matrices, *Combinatorial Theory and its Applications* (Erdős, P., Rényi, A. and Sós, V. T., Eds). Colloq. Math. Soc. J. Bolyai, vol. 4. North-Holland, pp. 721–728.
Komlós, J. and Szemerédi, E. (1975). Hamiltonian cycles in random graphs. *Infinite and Finite Sets* (Hajnal, A., Rado, R. and Sós, V. T., Eds). Colloq. Math. Soc. J. Bolyai, vol. 10. North-Holland, Amsterdam, pp. 1003–1011.
Komlós, J. and Szemerédi, E. (1983). Limit distributions for the existence of Hamilton cycles in a random graph, *Discrete Math.* **43**, 55–63.
Kordecki, W. (1973). Probability of connectedness of random graphs, *Prace Nauk. Inst. Mat. Fiz. Teor. Pol. Wroclaw* **9**, 55–65 (in Russian).
Korn, I. (1967). On (d, k) graphs, *IEEE Trans. Electron. Computers* **16**, 90.
Korshunov, A. D. (1970). On the power of some classes of graphs, *Soviet Mat. Dokl.* **11**, 1100–1104.
Korshunov, A. D. (1971*a*). Number of nonisomorphic subgraphs in an n-point graph, *Mat. Zametki* **9**, 263–273 (in Russian). English transl. *Math. Notes* **9**, 155–160.
Korshunov, A. D. (1971*b*). On the diameter of random graphs, *Soviet Mat. Dokl.* **12**, 302–305.
Korshunov, A. D. (1976). Solution of a problem of Erdős and Rényi on Hamilton cycles in non-oriented graphs, *Soviet Mat. Dokl.* **17**, 760–764.
Korshunov, A. D. (1977). A solution of a problem of P. Erdős and A. Rényi

about Hamilton cycles in non-oriented graphs, *Metody Diskr. Anal. Teoriy Upr. Syst., Sb. Trudov Novosibirsk* **31**, 17–56 (in Russian).

Kostochka, A. V. (1982). A lower bound for the Hadwiger number of a graph as a function of the average degree of its vertices, *Diskret. Analiz. Novosibirsk* **38**, 37–58 (in Russian).

Kostochka, A. V. and Masurova, N. P. (1977). An estimate in the theory of graph colouring, *Diskret. Analiz No.* 30, *Metody Diskret. Anal. Resenii, Kombinatornyk Zadac* 23–29, 76 (in Russian).

Kovalenko, I. N. (1971). Theory of random graphs, *Kibernetika* **4**, 1–4 (in Russian). English transl. *Cybernetics* **7**, 575–579.

Kovalenko, I. N. (1975). The structure of random directed graphs. *Theory Probab. Math. Statist.* **6**, 83–92.

Kozyrev, V. P. and Korshunov, A. D. (1974). On the size of a cut in a random graph, *Problems Cybernet.* **29**, 27–62 (in Russian). Corrections **30**, (1975), 342.

Kruskal, C. P. (1983). Searching, merging, and sorting in parallel computation, *IEEE Trans. Comput.* **C-32**, 942–946.

Kruskal, J. B. (1954). The expected number of components under random mapping functions, *Amer. Math. Monthly* **61**, 392–397.

Kruskal, J. B. (1956). On the shortest spanning subtree of a graph and the travelling salesman problem, *Proc. Amer. Math. Soc.* **7**, 48–50.

Kućera, L. (1977). Expected behaviour of graph colouring algorithms. *Fundamentals of Computation Theory.* Lecture Notes in Computer Science, No. 56. Springer-Verlag, Berlin, pp. 447–451.

Kuhn, W. W. (1972). A random graph generator, *Proc. Third Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, pp. 311–313.

Landau, E. (1909). *Handbuch der Lehre von der Verteilung der Primzahlen*, Bd I. B. G. Teubner, Leipzig, Berlin, xviii + 564 pp.

Lawler, E. L. (1970). A note on the complexity of the chromatic number problem, *Info. Process. Lett.* **5**, 66–67.

Lazarus, A. J. (1993). Certain expected values in the random assignment problem, *Op. Res. Lett.* **14**, 207–214.

Leighton, F. T. (1979). A graph colouring algorithm for large scheduling problems, *J. Res. Natn. Bur. Stand.* **84**, 489–496.

Leighton, F. T. (1984). Tight bounds on the complexity of parallel sorting, *Proc. 16th ACM Symp. on Theory of Computing*, pp. 71–80.

Leland, W. (1981). Dense intercommunication graphs with small degree.

Leland, W. and Solomon, M. (1982). Dense trivalent graphs for processor interconnection, *IEEE Trans. Comput.* **31**, 219–222.

Leland, W., Finkel, R., Qiao, L., Solomon, M. and Uhr, L. (1981). High density graphs for processor interconnection, *Info. Process. Lett.* **12**, 117–120.

Lengauer, T. and Tarjan, R. E. (1982). Asymptotically tight bounds on time–space tradeoff in a pebble game, *J. ACM* **29**, 1087–1130.

Lev, G. and Valiant, L. G. (1983). Size bounds for superconcentrators, *Theor. Comput. Sci. (Netherlands)* **22**, 233–251.

Lévy, P. (1935). Sur la sommabilité des séries aléatoires divergentes, *Bull. Soc. Math. France* **63**, 1–35.

Lichtenstein, D. (1980). Isomorphism of graphs embeddable in the projective plane, *Proc. Twelfth Annual ACM Symp. on Theory of Computing*, pp. 218–224.

Lifschitz, V. and Pittel, B. (1981). The number of increasing subsequences of the random permutation, *J. Combinatorial Theory (A)* **31**(1).

Lindeberg, J. W. (1922). Eine neue Verteilung des Exponentialgesetzes in der Wahrscheinlichkeitsrechnung, *Math. Z.* **15**, 221–225.

Ling, R. F. (1973*a*). The expected number of components in random linear graphs, *Annls Probab.* **1**, 876–881.

Ling, R. F. (1973*b*). A probability theory of cluster analysis, *Annls Am. Statist. Ass.* **68**, 159–164.

Ling, R. F. (1975). An exact probability distribution on the connectivity of random graphs, *J. Math. Psychol.* **12**, 90–98.

Ling, R. F. and Killough, G. G. (1976). Probability tables for cluster analysis based on a theory of random graphs, *J. Amer. Statist. Ass.* **71**, 293–300.

van Lint, J. H. (1981). Notes on Egoritsev's proof of the van der Waerden conjecture. *Linear Algebra and its Applications* (Brualdi, R. A. and Schneider, H., Eds), vol. 39, pp. 1–8.

van Lint, J. H. and Seidel, J. J. (1966). Equilateral point sets in projective geometry, *Indag. Math.* **28**, 335–348.

Lipton, R. J. (1978). The beacon set approach to graph isomorphism. Yale University, preprint.

Liskovec, V. A. (1975). On the number of maximal vertices of a random acyclic digraph, *Theory Probab. Applics* **20**.

Littlewood, J. E. (1969). On the probability in the tail of a binomial distribution, *Adv. Appl. Probab.* **1**, 43–72.

Littlewood, J. E. and Offord, A. C. (1938). On the number of real roots of a random algebraic equation, *J. Lond. Math. Soc.* **13**, 288–295.

Lomonosov, M. V. (1974). Bernoulli scheme with closure, *Problems Info. Transmission* **10**, 73–81.

Lomonosov, M. V. and Polesski, V. P. (1971). An upper bound for the reliability of information networks, *Problems Info. Transmission* **7**, 337–339.

Lomonosov, M. V. and Polesski, V. P. (1972*a*). Lower bound for the reliability of networks, *Problems Info. Transmission* **8**, 47–53.

Lomonosov, M. V. and Polesski, V. P. (1972*b*). The maximum of the probability of connectivity, *Problems Info. Transmission* **8**, 68–73.

Lovász, L. and Vesztergombi, K. (1976). Restricted permutations and Stirling Numbers. In *Combinatorics*, vol. II (Hajnal, A. and Sós, V. T., Eds). North-Holland, New York, pp. 731–738.

Łuczak, T. (1987). On matchings and Hamiltonian cycles in subgraphs of random graphs. *Random graphs '85 (Poznań, 1985)*, North-Holland math. studies 144, Noth-Holland, Amsterdam–New York, 171–185.

Łuczak, T. (1990*a*). On the number of sparse connected graphs, *Random Structures and Algorithms* **1**, 171–174.

Łuczak, T. (1990*b*). Component behavior near the critical point of the random graph process, *Random Structures and Algorithms* **1**, 287–310.

Łuczak, T. (1991*a*). Cycles in a random graph near the critical point, *Random Structures and Algorithms* **2**, 421–440.

Łuczak, T. (1991*b*). The chromatic number of random graphs, *Combinatonica* **11**, 45–54.

Łuczak, T. (1991*c*). The chromatic number of random graphs, *Combinatonica* **11**, 45–54.

Łuczak, T., Pittel, B. and Wierman, J. C. (1994). The structure of a random graph near the point of the phase transition, *Trans. Amer. Math. Soc.* **341**,

721–748.
Łuczak, T. and Wierman, J. C. (1989). The chromatic number of random graphs at the double-jump threshold, *Combinatorica* **9**, 39–49.
Lueker, G. S. (1981). Optimisation problems on graphs with independent random edge weights, *SIAM J. Comput.* **10**, 338–351.
Luks, E. M. (1980). Isomorphism of graphs of bounded valence can be tested in polynomial time, *21st Annual IEEE Symp. on Foundations of Computer Science*, pp. 42–49.
McDiarmid, C. J. H. (1979*a*). Colouring random graphs badly, *Graph Theory and Combinatorics* (Wilson, R. J., Ed.). Pitman Research Notes in Mathematics, vol. 34, 76–86.
McDiarmid, C. J. H. (1979*b*). Determining the chromatic number of a graph, *SIAM J. Comput.* **8**, 1–14.
McDiarmid, C. J. H. (1980*a*). Clutter percolation and random graphs. *Combinatorial Optimization* (Rayward-Smith, V. J., Ed.). Mathematical Programming Study, vol. 13. North-Holland, Amsterdam, New York, Oxford, pp. 17–25.
McDiarmid, C. J. H. (1980*b*). Percolation on subsets of the square lattice, *J. Appl. Probab.* **11**, 278–283.
McDiarmid, C. J. H. (1981). General percolation and random graphs, *Adv. Appl. Probab.* **13**, 40–60.
McDiarmid, C. J. H. (1982). Achromatic numbers of random graphs, *Math. Proc. Camb. Phil. Soc.* **92**, 21–28.
McDiarmid, C. J. H. (1983*a*). On the chromatic forcing number of a random graph, *Discrete Appl. Math.* **5**, 123–132.
McDiarmid, C. J. H. (1983*b*). General first-passage percolation, *Adv. Appl. Probab.* **15**, 149–161.
McDiarmid, C. (1990). On the chromatic number of random graphs, *Random Structures and Algorithms* **4**, 435–442.
McKay, B. D. and Wormald, N. C. (1984). Automorphisms of random graphs with specified vertices, *Combinatorica* **4**, 325–338.
McKay, B. D. and Wormald, N. C. (1990*a*). Uniform generation of random regular graphs of moderate degree, *J. Algorithms* **11**, 52–67.
McKay, B. D. and Wormald, N. C. (1990*b*). Asymptotic enumeration by degree sequence of graphs of high degree, *Europ. J. Combinatorics* **11**, 565–580.
McKay, B. D. and Wormald, N. C. (1991). Asymptotic enumeration by degree sequence of graphs with degrees $o(n^{1/2})$, *Combinatorica* **11**, 369–382.
McKay, B. D. and Wormald, N. C. (1997). The degree sequence of a random graph. I. The models, *Random Structures and Algorithms* **11**, 97–117.
McLeish, D. L. (1979). Central limit theorems for absolute deviations from the sample mean and applications, *Canad. Math. Bull.* **22**, 391–396.
Mader, W. (1967). Homomorphieeigenschaften und mittlere Kantendichte von Graphen, *Math. Annln* **174**, 265–268.
Maehera, H. (1980). On random simplices in product distributions, *J. Appl. Probab.* **17**, 553–558.
Maehera, H. (1985). On the number of induced subgraphs of a random graph, *Discrete Math.* See Q4.
Margulis, G. A. (1973). Explicit constructions of concentrators, *Problemy Peredachi Informatsii* **9**(4), 71–80 (in Russian). English transl. in *Problems Info. Transmission* **9** (1975), 325–332. Plenum Press, New York.
Margulis, G. A. (1974). Probabilistic characteristics of graphs with large

connectivity, *Problems Info. Transmission* **10**, 101–108 (in Russian). English transl. in *Problems Info. Transmission*, Plenum Press, New York (1977).
Margulis, G. A. (1982). Explicit constructions of graphs without short cycles and low density codes, *Combinatorica* **2**, 71–78.
Marshall, C. W. (1971). *Applied Graph Theory.* Wiley–Interscience, New York, London, Sydney, Toronto, xiii + 322 pp.
Mathon, R. (1978). Symmetric conference matrices of order pq^{2+1}, *Canad. J. Math.* **30**, 321–331.
Mathon, R. (1979). A note on the graph isomorphism counting problem, *Info. Process. Lett.* **8**, 131–132.
Matula, D. W. (1970). On the complete subgraph of a random graph. *Combinatory Mathematics and its Applications.* Chapel Hill, North Carolina, pp. 356–369.
Matula, D. W. (1972). The employee party problem, *Notices A.M.S.* **19**, A-382.
Matula, D. W. (1976). The largest clique size in a random graph, Tech. Rep., Dept. Comput. Sci., Southern Methodist University, Dallas.
Matula, D. (1987). Expose-and-merge exploration and the chromatic number of a random graph, *Combinatorics* **7**, 275–284.
Matula, D. and Kučera, L. (1990). An expose-and-merge algorithm and the chromatic number of a random graph, *Proceedings of Random graphs '87* (Karoński, M., Jaworski, J. and Ruciński, A., Eds), Wiley, Chichester, pp. 175–188.
Matula, D. W., Marble, G. and Isaacson, J. D. (1972). Graph colouring algorithms. In *Graph Theory and Computing* (Read, R. C., Ed.). Academic Press, New York, London, pp. 109–122.
Mauldin, R. D. (Ed.) (1979). *The Scottish Book.* Birkhäuser Verlag, Boston, Basel, Stuttgart, xiii + 268 pp.
Meir, A. and Moon, J. W. (1968). On nodes of degree two in random trees, *Mathematika* **15**, 188–192.
Meir, A. and Moon, J. W. (1970*a*). Cutting down random trees, *J. Austral. Math. Soc.* **11**, 313–324.
Meir, A. and Moon, J. W. (1970*b*). The distance between points in random trees, *J. Combinatorial Theory* **8**, 99–103.
Meir, A. and Moon, J. W. (1973*a*). Random packings and coverings in random trees, *Aequationes Math.* **9**, 107–114.
Meir, A. and Moon, J. W. (1973*b*). The expected node-independence number of random trees, *Nederl. Akad. Wetensch. Proc. Ser. Indag. Math.* **35**, 335–341.
Meir, A. and Moon, J. W. (1974). The expected node-independence number of various types of trees. *Recent Advances in Graph Theory* (Proc. Second Czechoslovak Symp., Prague), pp. 351–363.
Meir, A., Moon, J. W. and Pounder, J. R. (1980). On the order of random channel networks, *SIAM J. Algebra, Discrete Meth.* **1**, 25–33.
Memmi, G. and Raillard, Y. (1982). Some results about the (d,k) graph problem, *IEEE Trans. Comput.* **31**, 784–791.
Mézard, M. and Parisi, G. (1985). Replicas and optimization, *J. Phys. Lett.* **46**, 771–778.
Mézard, M. and Parisi, G. (1987). On the solution of the random link matching problems, *J. Phys. Lett.* **48**, 1451–1459.
Miech, R. J. (1967). On a conjecture of Erdős and Rényi, III, *J. Math.* **11**, 114–127.
Milgram, S. (1967). A small world problem, *Psychology Today* **1**, 61.

Miller, G. L. (1978). On the $n^{\log n}$ isomorphism technique, *Proc. 10th SIGACT Symp. on the Theory of Computing*, pp. 51–58.
Miller, G. L. (1979). Graph isomorphism, general remarks, *J. Computer, Syst. Sci.* **18**, 128–142.
Miller, G. L. (1980). Isomorphism testing for graphs of bounded genus. *Proc. Twelfth Annual ACM Symp. on Theory of Computing*, pp. 225–235.
Molloy, M. (1996). A gap between the appearances of a k-core and a $(k+1)$-chromatic graph, *Random Structures and Algorithms* **8**, 159–160.
Molloy, M., and Reed, B. (1999). Critical subgraphs of a random graph, *Electr. J. Combinatorics* **6**, Research Paper 35, 13 pp.
Molloy, M. S. O., Robalewska, H., Robinson, R. W. and Wormald, N. C. (1997). 1-factorizations of random regular graphs, *Random Structures, Algorithms* **10**, 305–321.
Montgomery, H. L. (1971). *Topics in Multiplicative Number Theory*. Lecture Notes in Mathematics, vol. 227. Springer-Verlag, Berlin, Heidelberg, New York, ix + 178 pp.
Moon, J. W. (1965). On the distribution of crossings in random complete graphs, *J. Soc. Ind. Appl. Math.* **13**, 506–510.
Moon, J. W. (1968*a*). On the maximum degree in a random tree, *Michigan J. Math.* **15**, 429–432.
Moon, J. W. (1968*b*). *Topics in Tournaments*. Holt, New York.
Moon, J. W. (1970*a*). *Counting Labelled Trees*. Canadian Mathematics Congress, Montreal, x + 113 pp.
Moon, J. W. (1970*b*). Climbing random trees. *Aequationes Math.* **5**, 68–74.
Moon, J. W. (1971*a*). A problem on random trees, *J. Combinatorial Theory (B)* **10**, 201–205.
Moon, J. W. (1971*b*). The lengths of limbs of random trees, *Mathematika* **18**, 78–81.
Moon, J. W. (1972*a*). Almost all graphs have a spanning cycle, *Canad. Math. Bull.* **15**, 39–41.
Moon, J. W. (1972*b*). Random exchanges of information, *Nieuw Archief voor Wiskunde (3)* **XX**, 246–249.
Moon, J. W. (1972*c*). The variance of the number of spanning cycles in a random graph, *Studia Sci. Math. Hungar.* **7**, 281–283.
Moon, J. W. (1972*d*). Two problems on random trees. Lecture Notes in Mathematics, vol. 303. Springer-Verlag, pp. 197–206.
Moon, J. W. (1973*a*). Random walks on random trees, *J. Austral. Math. Soc.* **15**, 42–53.
Moon, J. W. (1973*b*). The distance between nodes in recursive trees. *Combinatorics* (Proc. British Combinatorics Conf., 1973). London Math. Soc. Lecture Note Series 13. Cambridge University Press, 1974, pp. 125–132.
Moon, J. W. (1979). A note on disjoint channel networks, *Math. Geol.* **11**, 337–342.
Moon, J. W. and Moser, L. (1962). On the distribution of 4-cycles in random bipartite tournaments, *Canad. Math. Bull.* **5**, 5–12.
Moon, J. W. and Moser, L. (1966*a*). Almost all (0, 1) matrices are primitive, *Studia Sci. Math. Hungar.* **1**, 153–156.
Moon, J. W. and Moser, L. (1966*b*). An external problem in matrix theory, *Matem, Vesnik* **3**, 209–211.
Moore, E. F. and Shannon, C. E. (1956). Reliable circuits using less reliable relays, Parts I and II, *J. Franklin Inst.* **262**, 201–218; **262**, 281–297.

Moser, L. and Wyman, M. (1955). On the solutions of $x^d = 1$ in symmetric groups, *Canad. J. Math.* **7**, 159–188.

Murty, U. R. S. and Vijayan, K. (1964). On accessibility in graphs, *Sankhya Ser. A* **26**, 299–302.

Na, H. S. and Rapoport, A. (1967). A formula for the probability of obtaining a tree from a graph constructed randomly except for 'exogenous bias'. *Annls Math. Statist.* **38**, 226–241.

Na, H. S. and Rapoport, A. (1970). Distribution of nodes of a tree by degree, *Math. Biosci.* **6**, 313–329.

Nagy, Zs. (1972). A constructive estimation of Ramsey numbers, *Mat. Lapok* **23**, 301–302 (in Hungarian).

Naus, J. I. and Rabinowitz, L. (1975). The expectation and variance of the number of components in random linear graphs, *Annls Probab.* **3**, 159–161.

Nemetz, T. (1971). On the number of Hamilton cycles of the complete graph with a given number of edges in a given Hamilton cycle, *Mat. Lapok* 65–81 (in Hungarian).

Newman, M. E. J., Strogatz, S. H. and Watts, D. J. (2000). Random graphs with arbitrary degree distribution and their applications, to appear.

Nilli, A. (2000). Triangle-free graphs with large chromatic numbers, *Discrete Math.* **211**, 261–262.

Oberschelp, W. (1967). Kombinatorische Anzahlbestimmungen in Relationen, *Math. Annln* **174**, 53–78.

Okamoto, M. (1958). Some inequalities relating to the partial sum of binomial probabilities, *Ann. Just. Statist. Math.* **10**, 29–35.

Olin, B. (1992). Asymptotic properties of random assignment problems, Ph. D. Thesis, Kangl. Tekniska Höyskolan, Stockholm, Sweden.

Olson, J. and Spencer, J. (1978). Balancing families of sets, *J. Combinatorial Theory (A)* **25**, 29–37.

O'Neil, P. E. (1969). Asymptotics and random matrices with row–sum and column–sum restrictions, *Bull. Amer. Math. Soc.* **75**, 1276–1282.

Palásti, I. (1963). On the connectedness of bichromatic random graphs, *Publ. Math. Inst. Hungar. Acad. Sci.* **8**, 431–440.

Palásti, I. (1966). On the strong connectedness of directed random graphs, *Studia Sci. Math. Hungar.* **1**, 205–214.

Palásti, I. (1968). On the connectedness of random graphs. In *Studies in Mathematical Statistics and Applications.* Akad. Kiadó, Budapest, pp. 105–108.

Palásti, I. (1969*a*). A recursion formula for the number of Hamilton cycles having one edge in common with a given Hamilton cycle, *Mat. Lapok* **20**, 289–305 (in Hungarian).

Palásti, I. (1969*b*). On the common edges of the Hamilton cycles of a linear complete graph, *Mat. Lapok* **20**, 71–98 (in Hungarian).

Palásti, I. (1971*a*). On the threshold distribution function of cycles in a directed random graph, *Studia Sci. Math. Hungar.* **6**, 67–73.

Palásti, I. (1971*b*). On Hamilton cycles of random graphs, *Per. Math. Hungar.* **1**, 107–112.

Paley, R. E. A. C. (1933). On orthogonal matrices, *J. Math. Phys.* **12**, 311–320.

Paley, R. E. A. C. and Zygmund, A. (1930*a*). On some series of functions (1), *Proc. Camb. Phil. Soc.* **26**, 337–357.

Paley, R. E. A. C. and Zygmund, A. (1930*b*). On some series of functions (2), *Proc. Camb. Phil. Soc.* **26**, 458–474.

Paley, R. E. A. C. and Zygmund, A. (1932). On some series of functions (3), *Proc. Camb. Phil. Soc.* **28**, 190–205.

Paley, R. E. A. C., Wiener, N. and Zygmund, A. (1932). Notes on random functions, *Math. Zeitschrift* **37**, 647–668.

Palka, Z. (1982). On the number of vertices of given degree in a random graph, *J. Graph Theory* See Q4

Palmer, E. M. and Schwenk, A. J. (1979). On the number of trees in a random forest, *J. Combinatorial Theory (B)* **27**, 109–121.

Parisi, G. (1998). A conjecture on random bipartite matching, Physics e-Print archive, http://xxx.lanl.gov/ps/cond-mat/9801176

Paul, W. J., Tarjan, R. E. and Celoni, J. R. (1977). Space bounds for a game on graphs, *Math. Systems Theory* **10**, 239–251.

Pavlov, Yu. L. (1977). The asymptotic distribution of maximum tree size in a random forest, *Theory Probab. Applics* **22**, 509–520.

Pavlov, Yu. L. (1977). Limit theorems for the number of trees of a given size in a random forest, *Mat. Sbornik* **32**, 335–345 (in Russian).

Pavlov, Yu. L. (1979). Limit distribution of a maximal order of a tree in a random forest—a special case, *Math. Notes* **25**, 387–392.

Payan, C. (1986). Graphes équilibrés et arboricité rationalle, *Europ. J. Combinatonics* **7**, 263–270.

Peck, G. W. (1980). Erdős conjecture on sums of distinct numbers, *Studies in Appl. Math.* **63**, 87–92.

Penrose, M. D. (1997). The longest edge of a random minimal spinning tree, *Ann. Appl. Probab.* **7**, 340–361.

Penrose, M. D. (1999). On k-connectivity for a geometric random graph, *Random Structures and Algorithms* **15**, 145–164.

Perepelica, V. A. (1970). On two problems from the theory of graphs, *Soviet Math. Dokl.* **11**, 1376–1379.

Peterson, W. W. (1961). *Error-Correcting Codes.* M.I.T. Press and John Wiley and Sons, New York, London, pp. 245–248; Appendix A.

Pinch, R. G. E. (1985). A sequence well distributed in the square, *Math. Proc. Camb. Phil. Soc.* (to appear).

Pinsker, M. S. (1973). On the complexity of a concentrator, *Proc. 7th Int. Teletraffic Conf.*, Stockholm, pp. 318/1–318/4.

Pippenger, N. (1977). Superconcentrators, *SIAM J. Comput.* **6**, 298–304.

Pippenger, N. (1978). Generalized connectors, *SIAM J. Comput.* **7**, 510–514.

Pippenger, N. (1982). Advances in pebbling, *Int. Coll. on Automation, Language and Programming*, pp. 407–417.

Pippenger, N. (1984). Explicit constructions of highly expanding graphs, preprint.

Pittel, B. (1982). On the probable behaviour of some algorithms for finding the stability number of a graph, *Math. Proc. Camb. Phil. Soc.* **92**, 511–526.

Pittel, B. (1983). On distributions related to transitive closures of the random finite mappings, *Ann. Probab.* **11**, 428–441.

Pittel, B., Spencer, J. and Wormald, N. (1996). Sudden emergence of a giant k-core in a random graph, *J. Combinatorial Theory (B)* **67**, 111–151.

Polesski, V. P. (1971*a*). A certain lower bound for the reliability of information networks, *Problems Info. Transmission* **7**, 165–179.

Polesski, V. P. (1971*b*). Relationship between chromatic numbers and branch connectivity in a finite graph, *Problems Info. Transmission* **7**, 85–87.

Pólya, G. (1918) Über die Verteilung der quadratischen Reste und Nichtreste, *Nachr. Akad. Wiss. Göttingen Math. Phys.* 21–29.
Pólya, G. (1937). Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**, 145–254.
Pósa, L. (1976). Hamiltonian circuits in random graphs, *Discrete Math.* **14**, 359–364.
Pratt, V. R. and Yao, F. F. (1973). On lower bounds for computing the ith largest element, *Proc. 14th Annual IEEE Symp. on Switching and Automata Theory*, IEEE Comput. Soc., Northridge, California, pp. 70–81.
Preparata, F. P. (1978). New parallel-sorting schemes, *IEEE Trans. Comput.* **C-27**, 669–673.
Preparata, F. P. and Vuillemin, J. (1979). The cube-connected cycles: a versatile network for parallel computation, *Proc. 20th Annual IEEE Symp. on Foundations of Computer Science*, pp. 140–147.
Proskurin, G. V. (1973). On the distribution of the number of vertices in the strata of a random mapping, *Theory Probab. Applics* **18**, 803–808.
Provan, J. S. and Bull, M. O. (1981). The complexity of counting cuts and computing the probability that a graph is connected. Working Paper MS/S #81-002, College of Business and Management, University of Maryland at College Park.
Quintas, L. V., Schiano, M. D. and Yarmish, J. (1980). Degree partition matrices for identity 4-trees. Mathematics Department, Pace University, New York.
Quintas, L. V., Stehlik, M. and Yarmish, J. (1979). Degree partition matrices for 4-trees having specified properties, *Proc. Tenth Southeastern Conf. on Combinatorics, Graph Theory and Computing, Congressus Numerantium* **XXIV**, Utilitas Math., Winnipeg, Manitoba.
Quintas, L. V. and Yarmish, J. (1981). Valence isomers for chemical trees, *MATCH* **12**, 75–86.
Rado, R. (1964). Universal graphs and universal functions, *Acta Arith.* **9**, 331–340.
Ramanujacharyulu, C. (1966). On colouring a polygon and restricted random graphs. In *Theory of Graphs, International Symposium*, Rome, 1966, Gordon and Breach, New York, Dunod, Paris (1967), pp. 333–337.
Ramsey, F. P. (1930). On a problem of formal logic, *Proc. Lond. Math. Soc. (2)* **30**, 264–286.
Rapoport, A. and Fillenbaum, S. (1972). An experimental study of semantic structures. In *Multidimensional Scaling* (Romney, A. K., Shephard, R. N. and Nerlove, S. B., Eds), vol. II. Seminar Press, New York, pp. 93–131.
Read, R. C. (1959). The enumeration of locally restricted graphs (I), *J. Lond. Math. Soc.* **34**, 417–436.
Read, R. C. (1960). The enumeration of locally restricted graphs (II), *J. Lond. Math. Soc.* **35**, 344–351.
Read, R. C. and Corneil, D. G. (1977). The graph isomorphism disease, *J. Graph Theory* **1**, 339–363.
Recski, A. (1979). Some remarks on the arboricity of tree-complements, *Proc. Fac. Sci. Tokai Univ.* **15**, 71–74.
Reed, B. and McDiarmid, C. J. H. (1992). The strongly connected components of 1-in 1-out, *Combinatorics, Probability and Computing* **1**, 265–274.
Reif, J. H. and Valiant, L. G. (1983). A logarithmic time sort for linear size networks, *Proc. 15th ACM Symp. on Theory of Computing*, pp. 10–16.
Reiman, I. (1958). Über ein Problem von K. Zarankiewicz, *Acta Math. Acad.*

Sci. Hungar. **9**, 269–279.
Reischuk, R. (1981). A fast probabilistic parallel sorting algorithm, *Proc. 22nd IEEE Symp. on Foundations of Computer Science*, pp. 211–219.
Rényi, A. (1958). Quelques remarques sur les probabilités des événements dépendants, *J. Math. Pures, Appl.* **37**, 393–398.
Rényi, A. (1959*a*). Some remarks on the theory of trees, *Publ. Math. Inst. Hungar. Acad. Sci.* **4**, 73–85.
Rényi, A. (1959*b*). On connected graphs I, *Publ. Math. Inst. Hungar. Acad. Sci.* **4**, 385–387.
Rényi, A. (1961). On random subsets of a finite set, *Mathematica, Cluj* **3**, 355–362.
Rényi, A. (1970*a*). *Foundations of Probability*. Holden—Day, San Francisco, Cambridge, London, Amsterdam.
Rényi, A. (1970*b*). On the number of endpoints of a k-tree, *Studia Sci. Math. Hungar.* **5**, 5–10.
Rényi, A. and Szekeres, G. (1967). On the height of trees, *J. Austral. Math. Soc.* **7**, 497–507.
Richardson, D. (1973). Random growth in a tessellation, *Proc. Camb. Phil. Soc.* **74**, 515–528.
Richmond, L. B., Robinson, R. W. and Wormald, N. C. (1985). On Hamiltonian cycles in 3-connected cubic maps, in *Cycles in Graphs* (Burnaby, B.C., 1985), North-Holland Math. Stud. **115**, North-Holland, Amsterdam, pp. 141–149.
Riddell, R. J., Jr and Uhlenbeck, G. E. (1953). On the virial development of the equation of state of monoatomic gases, *J. Chem. Phys.* **21**, 2056–2064.
Riordan, J. (1962). Enumeration of linear graphs for mappings of finite sets, *Annls Math. Statist.* **33**, 178–185.
Riordan, J. (1968). *Combinatorial Identities*. John Wiley and Sons, New York, London, Sydney, xii + 256 pp.
Robbins, H. (1955). A remark on Stirling's formula, *Amer. Math. Monthly* **62**, 26–29.
Roberts, F. D. K. (1968). Random minimal trees, *Biometrika* **55**, 255–258.
Robinson, R. (1951). A new absolute geometric constant? *Amer. Math. Monthly* **58**, 462–469; see also Robinson's constant (editorial note), *Ibid.* **59** (1952), 296–297.
Robinson, R. W. and Schwenk, A. J. (1975). The distribution of degrees in a large random tree, *Discrete Math.* **12**, 359–372.
Robinson, R. W. and Wormald, N. C. (1984). Existence of long cycles in random cubic graphs, in *Enumeration and Design* (Jackson D. M. and Vaustone, S. A., Eds), Academic Press, Toronto, pp. 251–270.
Robinson, R. W. and Wormald, N. C. (1992). Almost all cubic graphs are hamiltonian, *Random Structures and Algorithms* **3**, 117–125.
Robinson, R. W. and Wormald, N. C. (1994). Almost all regular graphs are hamiltonian, *Random Structures and Algorithms* **5**, 363–374.
Rosenthal, A. (1975). A computer scientist looks at reliability computations. In *Reliability and Fault Tree Analysis* (Barlow, R. E., Fussell, J. B. and Singpurwalla, N. P., Eds). SIAM, Philadelphia, pp. 133–152.
Ross, S. M. (1981). A random graph, *J. Appl. Probab.* **18**, 309–315.
Rota, G. C. (1964). On the foundations of combinatorial theory **I**: theory of Möbius functions, *Z. Wahrscheinlichkeitsrechnung verwand. Gebiete* **2**, 340–368.
Rubin, M. and Sitgreaves, R. (1954). Probability distributions related to random

transformations of a finite set. Tech. Rep. 19A, Applied Mathematics and Statistics Laboratory, Stanford University.
Ruciński, A. (1981). On k-connectedness of an r-partite random graph, *Bull. Acad. Polon. Sci., Ser. Sci. Math.* **29**, 321–330.
Ruciński, A. (1982). Matchings and k-factors in a random graph, *Studia Sci. Math. Hungar.* **17**, 335–340.
Ruciński, A. and Vince, A. (1985). Balanced graphs and the problem of subgraphs of a random graph, *Congressus Numerantium* **49**, 181–190.
Ruciński, A. and Vince, A. (1993). The solution to an extermal problem on balanced extensions of graphs, *J. Graph Theory* **17**, 417–431.
Ryshik, I. M. and Gradstein, I. S. (1963). *Tables of Series, Products and Integrals.* VEB Deutscher Verlag der Wissenschaften, Berlin.
Sachkov, V. N. (1973). Random mappings with bounded height, *Theory Probab. Applics* **1**, 120–130.
Sachs, H. (1962). Über selbstkomplementäre Graphen, *Publicationes Math.* **9**, 270–288.
Salem, R. and Zygmund, A. (1954). Some properties of trigonometric series whose terms have random signs, *Acta Math.* **91**, 245–301.
Sauer, N. and Spencer, J. (1978). Edge disjoint placements of graphs, *J. Combinatorial Theory (B)* **25**, 295–302.
Scheele, S. (1977). Final Report to Office of Environmental Education, Department of Health, Education and Social Welfare, Social Engineering Technology, Los Angeles, Calif.
Schmidt-Pruzan, J. (1985*a*). Probabilistic analysis of strong hypergraph coloring algorithms and the strong chromatic number, unpublished manuscript.
Schmidt, J. and Shamir, E. (1981). The existence of d-dimensional matchings in random hypergraphs, unpublished manuscript.
Schmidt, J. and Shamir, E. (1983). A threshold for perfect matchings in random d-pure hypergraphs, *Discrete Math.* **45**, 287–295.
Schmidt-Pruzan, J. and Shamir, E. (1985). Component structure in the evolution of a random hypergraph, *Combinatorica* **5**, 81–94.
Schmidt-Pruzan, J., Shamir, E. and Upfal, E. (1985). Random hypergraph coloring algorithms and the weak chromatic number, *J. Graph Theory* **9**, 347–362.
Schmidt, W. M. (1973). Zur Methode von Stepanov, *Acta Arith.* **24**, 347–367.
Schmidt, W. M. (1976). *Equations over Finite Fields, An Elementary Approach.* Lecture Notes in Mathematics, vol. 536. Springer-Verlag, Berlin, Heidelberg, New York, ix + 267 pp.
Schrijver, A. (1980). On the number of edge colourings of regular bipartite graphs, A and E Report 18/80, University of Amsterdam.
Schrijver, A. and Valiant, W. G. (1979). On lower bounds for permanents. ZW 131-79, Mathematisch Centrum, Amsterdam.
Schultz, J. W. and Hubert, L. (1973). Data analysis and the connectivity of random graphs, *J. Math. Psychol.* **10**, 421–428.
Schultz, J. W. and Hubert, L. (1975). An empirical evaluation of an approximate result in random graph theory, *Brit. J. Math. Statist. Psychol.* **28**, 103–111.
Schur, I. (1916). Über die Kongruenz $x^m + y^m = z^m \pmod p$, *Jahresber. Dt. Math. Vereinigung* **25**, 114–116.
Schürger, K. (1974). Inequalities for the chromatic number of graphs, *J. Combinatorial Theory* **16**, 77–85.
Schürger, K. (1976). On the evolution of random graphs over expanding square

lattices, *Acta Math. Sci. Hungar.* **27**, 281–292.
Schürger, K. (1979*a*). On the asymptotic geometrical behaviour of a class of contact interaction processes with a monotone infection rate, *Z. Wahrscheinl.* **48**, 35–48.
Schürger, K. (1979*b*). Limit theorems for complete subgraphs of random graphs, *Per. Math. Hungar.* **10**, 47–53.
Schwenk, A. J. (1977). An asymptotic evaluation of the cycle index of a symmetric group, *Discrete Math.* **18**, 71–78.
Seidel, J. J. (1976). A survey of two-graphs, *Colloquio Int. sulle Teorie Combinatorie*, Atti dei Convegni Lincei 17, Accad. Naz. Lincei, Roma I, pp. 481–511.
Shamir, E. (1983). How many random edges make a graph Hamiltonian? *Combinatorica* **3**, 123–132.
Shamir, E. (1985). A sharp threshold for Hamilton paths in random graphs, unpublished manuscript.
Shamir, E., and Spencer, J. (1987). Sharp concentration of the chromatic number of random graphs $G_{n,p}$, *Combinatonica* **7**, 121–129.
Shamir, E. and Upfal, E. (1981*a*). On factors in random graphs, *Israel J. Math.* **39**, 296–302.
Shamir, E. and Upfal, E. (1981*b*). Large regular factors in random graphs, preprint.
Shamir, E. and Upfal, E. (1982). One-factors in random graphs based on vertex choice, *Discrete Math.* **41**, 281–286.
Shapiro, H. N. (1983). *Introduction to the Theory of Numbers.* John Wiley and Sons, New York, Chichester, Brisbane, Toronto, Singapore, xii + 459 pp.
Shearer, J. B. (1981). A counterexample to a bin packing conjecture. *SIAM J. Algebraic, Discrete Methods* **2**, 309–310.
Shearer, J. B. (1982). A note on the independence number of triangle-free graphs, see Q1.
Shearer, J. B. and Kleitman, D. (1979). Probabilities of independent choices being ordered, *Studies Appl. Math.* **60**, 271–276.
Shearer, (1985). On a problem of spaces, *Combin.* **5**, (1985) 241–245. See Q1.
Sheehan, J. (1967). On Pólya's theorem, *Canad. J. Math.* **19**, 792–799.
Sheehan, J. (1968). The number of graphs with a given automorphism group, *Canad. J. Math.* **20**, 1068–1076.
Shepp, L. A. and Lloyd, S. P. (1966). Ordered cycle lengths in random permutations, *Trans. Amer. Math. Soc.* **121**, 340–357.
Shiloach, Y. and Vishkin, U. (1981). Finding the maximum, merging and sorting in a parallel computation model, *J. Algorithms* **2**, 88–102.
Simonovits, M. and Sós, V. T. (1991). Szemerédi's partition and quasirandomness, *Random Structures and Algorithms* **2**, 1–10.
Simonovits, M. and Sós, V. T. (1997). Hereditarily extended properties, quasi-random graphs and not necessarily induced subgraphs, *Combinatorica* **17**, 577–596.
Skolem, T. (1933). Ein Kombinatorische Satz mit Anwendung auf ein Logisches Entscheidungsproblem, *Fundamenta Math.* **20**, 254–261.
Spencer, J. (1971). Optimal ranking of tournaments, *Networks* **1**, 135–138.
Spencer, J. (1974). Random regular tournaments, *Periodica Math. Hungar.* **5**, 105–120.
Spencer, J. (1975). Ramsey's theorem—a new lower bound, *J. Combinatorial Theory (A)* **18**, 108–115.

Spencer, J. (1976). Maximal asymmetry of graphs, *Acta Math. Acad. Sci. Hungar.* **27**, 47–53.
Spencer, J. (1977). Asymptotic lower bounds for Ramsey functions, *Discrete Math.* **20**, 69–76.
Spencer, J. (1980). Optimally ranking unrankable tournaments, *Per. Math. Hungar.* **11**, 131–144.
Spencer, J. (1981). Discrete ham sandwich theorems, *Europ. J. Combinatorics* **2**, 291–298.
Spencer, J. (1985). Six standard deviations suffice, *Trans. Amer. Math. Soc.* **289**, 679–706.
Sperner, E. (1928). Ein Satz über Untermengen einer endlichen Menge, *Math. Z.* **27**, 544–548.
Spiegel, M. R. (1974). *Complex Variables.* Schaum's Outline Series. McGraw-Hill, New York, London, Düsseldorf, 313 pp.
Stanley, R. P. (1980). Weyl groups, the hard Lefschetz theorem, and the Sperner property, *SIAM J. Algebra Discrete Meth.* **1**, 168–184.
Staton, W. (1977). Independence in graphs with maximum degree three, *Proc. Eighth Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, pp. 615–617.
Staton, W. (1979). Some Ramsey-type numbers and the independence ratio, *Trans. Amer. Math. Soc.* **256**, 353–370.
Steele, J. M. (1981). Growth rates of minimal spanning trees of multivariate samples. Research Report, Stanford University Department of Statistics.
Steele, J. M. (1987). On Frieze's $\zeta(3)$ limit for lengths of minimal spanning trees, *Discrete Appl. Math.* **18**, 99–103.
Stein, C. (1970). A bound for the error in the normal approximation to the distribution of a sum of dependent random variables, *Proc. Sixth Berkeley Symp. Math. Statist. Probab.* **2**, 583–602.
Stein, S. (1968). Random sample closed paths in a random linear graph, *Amer. Math. Monthly* **7**(A5), 751–752.
Steinhaus, H. (1930). Über die Wahrscheinlichkeit dafür, dass der Konvergenzkreis einer Potenzreihe ihre natürlich Grenze ist, *Math. Zeitschrift* **31**, 408–416.
Stepanov, S. A. (1969). The number of points of a hyperelliptic curve over a prime field, *Izv. Akad. Nauk SSSR Ser. Mat.* **33**, 1171–1181 (in Russian).
Stepanov, S. A. (1970). Elementary method in the theory of congruences for a prime modulus, *Acta Arith.* **17**, 231–247.
Stepanov, S. A. (1971). Estimates of rational trigonometric sums with prime denominators, *Trudy Akad. Nauk* **62**, 346–371 (in Russian).
Stepanov, S. A. (1972*a*). An elementary proof of the Hasse–Weil Theorem for hyperelliptic curves, *J. Number Theory* **4**, 118–143.
Stepanov, S. A. (1972*b*). Congruences in two variables, *Izv. Akad. Nauk SSSR, Ser. Mat.* **36**, 683–711 (in Russian).
Stepanov, S. A. (1974). Rational points on algebraic curves over finite fields, Report of a 1972 conference on analytic number theory in Minsk, USSR, pp. 223–243 (in Russian).
Stepanov, V. E. (1969*a*). Combinatorial algebra and random graphs, *Theory Probab. Applics* **14**, 373–399.
Stepanov, V. E. (1969*b*). On the distribution of the number of vertices in strata of a random tree, *Theory Probab. Applics* **14**, 65–78.
Stepanov, V. E. (1969*c*). Limit distributions of certain characteristics of random

mappings, *Theory Probab. Applics* **14**, 612–626.
Stepanov, V. E. (1970*a*). Phase transitions in random graphs, *Theory Probab. Applics* **15**, 187–203.
Stepanov, V. E. (1970*b*). On the probability of connectedness of a random graph $G_m(t)$, *Theory Probab. Applics* **15**, 55–67.
Stepanov, V. E. (1971). Random mappings with a single attracting centre, *Theory Probab. Applics* **16**, 155–161.
Stepanov, V. E. (1972). Structure of random graphs $G_m(x|h)$, *Theory Probab. Applics* **17**, 227–242.
Stoimenow, A. (1998). Enumeration of chord diagrams and an upper bound for Vassiliev invariants, *J. Knot Theory Ramifications* **7**, No. 1, 93–114.
Storwick, R. (1970). Improved construction techniques for (d,k) graphs, *IEEE Trans. Comput.* **19**, 1214–1216.
Szekeres, E. and Szekeres, G. (1965). On a problem of Schütte and Erdős, *Math. Graz.* **49**, 290–293.
Szekeres, G. and Binet, F. E. (1957). On Borel fields over finite sets, *Annls Math. Statist.* **28**, 494–498.
Szele, T. (1943). Combinatorial investigations concerning complete directed graphs, *Mat. es Fiz. Lapok* **50**, 223–236 (in Hungarian).
Tanner, R. M. (1985). Explicit construction of concentrators from generalized N-gons, *SIAM J. Alg. Discr. Meth.* **5**, 287–293.
Tarjan, R. E. (1972). Finding a maximum clique. Technical Rep. 72-123, Computer Science Department, Cornell University, Ithaca, New York.
Tarjan, R. E. (1974). Testing graph connectivity, *Proc. Sixth ACM Symp. on Theory of Computing*, Seattle, pp. 185–193.
Tarjan, R. E. and Trojanowski, A. E. (1977). Finding a maximum independent set, *SIAM J. Comput.* **6**, 537–546.
Temperley, H. N. V. (1981). Graph Theory and Applications, Ellis Horwood, Chichester, 130 pp.
Thanh, LeCong (1977). Estimates of some parameters of finite graphs with applications, *Elekt. Info. Kyber.* **13**, 505–521 (in Russian).
Thanh, LeCong (1979). On the problem of finding a shortest path in a finite graph, *Elekt. Info. Kyber.* **15**, 445–453.
Thomason, A. G. (1979). Partitions of graphs. Ph.D. Thesis, Cambridge, England, vi + 107 pp.
Thomason, A. G. (1983). Paley graphs and Weil's theorem. Talk at the British Combinatorial Conference, Southampton (unpublished).
Thomason, A. G. (1984). An extremal function for contractions of graphs, *Math. Proc. Camb. Phil. Soc.* **95**, 261–265.
Thomason, A. (1987*a*). Pseudo-random graphs, in 'Proceedings of Random Graphs, Poznań '1985' (Karoński, M., ed.), *Anns Discrete Math.* **33**, 307–331.
Thomason, A. (1987*b*). Random graphs, strongly regular graphs and pseudo-random graphs, in *Surveys in Combinatorics, 1987* (Whitehead C., ed.), London Math. Soc. Lecture note series **123**, Cambridge University Press, pp. 173–195.
Thomason, A. (1989*a*). A simple linear time algorithm for finaling a Hamilton path, *Graph Theory, and Combinatorics* **75**, 373–379.
Thomason, A. (1989*b*). Dense expanders and pseudo-random bipartite graphs, *Discrete Math.* **75**, 381–386.
Thompson, C. D. (1983). The VLSI complexity of sorting. *IEEE Trans. Comput.*, vol. C-32.

Titchmarsh, E. C. (1964). *The Theory of Functions.* Oxford University Press, London, x + 454 pp.
Tompa, M. (1980). Time space tradeoffs for computing functions using connectivity properties of their circuits, *J. Comput., Syst. Sci.* **20**, 118–132.
Trakhtenbrot, B. A. and Barzdin, Ya. M. (1973). *Finite Automata: Behavior and Synthesis.* Fundamental Studies in Computer Science, vol. 1. North-Holland and American Elsevier, New York, xi + 321 pp.
Truss, J. K. (1985). The group of the countable universal graph. See Q4.
Turyn, R. J. (1971). On C-matrices of arbitrary powers, *Canad. J. Math.* **23**, 531–535.
Tutte, W. T. (1947). The factorization of linear graphs, *J. Lond. Math. Soc.* **22**, 107–111.
Valiant, L. G. (1975*a*). Parallelism in comparison problems, *SIAM J. Comput.* **4**, 348–355.
Valiant, L. G. (1975*b*). On nonlinear lower bounds in computational complexity, *Proc. 7th Annual ACM Symp. on Theory of Computing*, Albuquerque, pp. 45–53.
Valiant, L. G. (1976). Graph theoretic properties in computational complexity, *J. Comput., Syst. Sci.* **13**, 278–285.
Valiant, L. G. (1979). The complexity of enumeration and reliability problems, *SIAM J. Comput.* **8**, 410–421.
Valiant, L. G. and Brebner, G. J. (1981). Universal schemes for parallel communication, *STOC (Milwaukee)*, 263–277.
Van Slyke, R. M. and Frank, H. (1972). Network reliability analysis I, *Networks* **1**, 279–290.
Vaught, R. L. (1954). Applications of the Lowenheim–Skolem–Tarski theorem to problems of completeness and decidability, *Indag. Math.* **16**, 467–472.
de la Vega, W. F. (1979). Long paths in random graphs, *Studia Sci. Math. Hungar.* **14**, 335–340.
de la Vega, W. F. (1982). Sur la cardinalité maximum des couplages d'hypergrahes aleatoires uniformes, *Discrete Math.* **40**, 315–318.
de la Vega, W. F. (1983*a*). On the maximum cardinality of a consistent set of arcs in a random tournament, *J. Combinatorial Theory (B)* **35**, 328–332.
de la Vega, W. F. (1983*b*). On the bandwidth of random graphs, *Combinatorial Mathematics*, North-Holland Math. Studies **75**, North-Holland, Amsterdam, 633–638.
de la Vega, W. F. (1985). Random graphs almost optimally colorable in polynomial time, *Random Graphs '83. (Poznań, 1983)*, North-Holland Math. Studies **118**, North-Holland, Amsterdam–New York, 311–317.
de la Vega, W. F. and Lueker, G. S. (1981). Bin packing can be solved within $1 + \varepsilon$ in linear time, *Combinatorica* **1**, 349–355.
Vershik, A. M. and Schmidt, A. A. (1977, 1978). Limit measures arising in the asymptotic theory of asymmetric groups I, *Theory Probab. Applics* **22**, 70–85; **23**, 36–49.
Vesztergombi, K. (1974). Permutations with restriction of middle length, *Studia Sci. Math. Hungar.* **9**, 181–185.
Vinogradov, I. M. (1918). Sur la distribution des résidues et non résidues de puissances, *Permski J. Phys. Isp. Ob.* **1**, 18–28, 94–98.
Waerden, B. L., van der (1926). Problem, *Jahresber. Dt. Math. Vereinigung* **25**, 117.
Waerden, B. L. van der (1927). Beweis einer Baudetschen Vermutung, *Nieuw*

Arch. Wisk. **15**, 212–216.
Walkup, D. W. (1979). On the expected value of a random assignment problem, *SIAM J. Comput.* **8**, 440–442.
Walkup, D. W. (1980). Matchings in random regular bipartite digraphs, *Discrete Math.* **31**, 59–64.
Walsh, T. R. S. (1979). Counting three-connected graphs, *Dokl. Akad. Nauk. SSSR* **247**, 297–302 (in Russian).
Walsh, T. R. S. and Wright, E. M. (1978). The k-connectedness of unlabelled graphs, *J. Lond. Math. Soc. (2)* **18**, 397–402.
Watts, D. J. (1999). *Small Worlds*, Princeton Univ. Press, xvi + 262 pp.
Watts, D. and Strogatz, S. (1998). Collective dynamics of small-world networks, *Nature* **393**, 440.
Wei, V. K. (1980). Coding for a multiple access channel. Ph.D. Thesis, University of Hawaii, Honolulu.
Wei, V. K. (1981). A lower bound on the stability number of a simple graph. Bell Laboratories Tech. Memor. No. 81-11217-9.
Weide, B. W. (1980). Random graphs and optimization problems, *SIAM J. Comput.* **9**, 552–557.
Weil, A. (1940). Sur les fonctions algébriques à corps de constantes fini, *C. R. Acad. Sci., Paris* **210**, 592–594.
Weil, A. (1948). Sur les courbes algébriques et les variéstés qui s'en déduisent, *Actualités Sci. Ind. No.* 1041.
Welsh, D. J. A. (1976). *Matroid Theory.* Lond. Math. Soc. Monogr. No. 8. Academic Press, London, New York, San Francisco, xi + 433 pp.
Whitworth, W. A. (1901). *DCC Exercises in Choice and Chance.* Bell: see also *Choice and Chance, With One Thousand Exercises.* Hafner, New York (1948), viii + 342 pp.
Wigner, E. P. (1955). Characteristic vectors of bordered matrices with infinite dimensions, *Annls Math.* **62**, 548–564.
Wigner, E. P. (1958). On the distribution of the roots of certain symmetric matrices, *Annls Math.* **67**, 325–327.
Wild, K. (1973). A theorem concerning products of elements of Abelian groups, *Proc. Lond. Math. Soc. (3)* **27**, 600–616.
Wilkow, R. S. (1972). Analysis and design of reliable computer networks, *IEEE Trans. Commun.* **20**, 660–678.
Wormald, N. C. (1981*a*). The asymptotic connectivity of labelled regular graphs, *J. Combinatorial Theory (B)* **31**, 156–167.
Wormald, N. C. (1981*b*). The asymptotic distribution of short cycles in random regular graphs, *J. Combinatorial Theory (B)* **31**, 168–182.
Wright, E. M. (1970). Asymptotic enumeration of connected graphs, *Proc. R. Soc. Edinb., Sect. A* **68**, 298–308.
Wright, E. M. (1971). Graphs on unlabelled nodes with a given number of edges, *Acta Math.* **126**, 1–9.
Wright, E. M. (1972). The probability of connectedness of an unlabelled graph can be less for more edges, *Proc. Amer. Math. Soc.* **35**, 21–25.
Wright, E. M. (1973*a*). For how many edges is a digraph almost certainly Hamiltonian? *Proc. Amer. Math. Soc.* **41**, 383–388.
Wright, E. M. (1973*b*). The probability of connectedness of a large unlabelled graph, *Bull. Amer. Math. Soc.* **79**, 767–769.
Wright, E. M. (1974*a*). Graphs on unlabelled nodes with a large number of edges, *Proc. Lond. Math. Soc. (3)* **28**, 577–594.

Wright, E. M. (1974*b*). For how many edges is a graph almost certainly Hamiltonian? *J. Lond. Math. Soc. (2)* **8**, 44–48.
Wright, E. M. (1974*c*). Two problems in the enumeration of unlabelled graphs, *Discrete Math.* **9**, 289–292.
Wright, E. M. (1975*a*). The probability of connectedness of a large unlabelled graph, *J. Lond. Math. Soc. (2)* **11**, 13–16.
Wright, E. M. (1975*b*). Large cycles in labelled graphs, *Math. Proc. Camb. Phil. Soc.* **78**, 7–17.
Wright, E. M. (1976). The evolution of unlabelled graphs, *J. Lond. Math. Soc. (2)* **14**, 554–558.
Wright, E. M. (1977*a*). The number of connected sparsely edged graphs, *J. Graph Theory* **1**, 317–330.
Wright, E. M. (1977*b*). Large cycles in large labelled graphs II, *Math. Proc. Camb. Phil. Soc.* **81**, 1–2.
Wright, E. M. (1978*a*). Asymptotic formulas for the number of oriented graphs, *J. Combinatorial Theory (B)* **24**, 370–373.
Wright, E. M. (1978*b*). The number of connected sparsely edged graphs II, Smooth graphs and blocks, *J. Graph Theory* **2**, 299–305.
Wright, E. M. (1980). The number of connected sparsely edged graphs III, Asymptotic results, *J. Graph Theory* **4**, 393–407.
Wright, E. M. (1982). The *k*-connectedness of bipartite graphs, *J. Lond. Math. Soc. (2)* **25**, 7–12.
Wright, E. M. (1983). The number of connected sparsely edged graphs IV, Large nonseparable graphs, *J. Graph Theory* **7**, 219–229.
Yackel, J. (1972). Inequalities and asymptotic bounds for Ramsey numbers, *J. Combinatorial Theory* **13**, 56–68.
Yao, A. C. (1976). On the average behavior of set merging algorithms, *Proc. Eighth Annual ACM Symposium on Computing*, pp. 192–195.
Yao, A. C. (1980). New algorithms for bin packing, *J. Ass. Comput. Machinery* **27**, 207–227.
Yao, A. C. (1982). On the time–space tradeoff for sorting with linear queries, *Theor. Comput. Sci.* **19**, 203–218.
Zemlyachenko, V. N. (1975). On algorithms of graph identification, *Questions Cybernet.* **15**. Proc. 2nd All-Union Seminar on Combinatorial Maths, Moscow, pp. 33–41 (in Russian).

Index

This is a new edition of the now classic text. The already extensive treatment given in the first edition has been heavily revised by the author. The addition of two new sections, numerous new results and over 150 references means that this represents an up to date and *comprehensive account of random graph theory.* *One of the aims of the* theory (founded by Erdös and Rényi in the late fifties) is to estimate the number of graphs of a given order that exhibit certain properties. This is achieved with the use of probabilistic ideas as opposed to an exact deterministic approach. This theory not only has numerous combinatorial applications, but also serves as a model for the probabilistic treatment of more complicated random structures. This book, written by an acknowledged expert in the field, can be used by mathematicians, computer scientists and electrical engineers, as well as people working in biomathematics. It is self-contained, and with numerous exercises in each chapter, is ideal for advanced courses or self study.

Béla Bollobás is Chair of Excellence at the University of Memphis and Fellow of Trinity College, Cambridge.

Cambridge Studies in Advanced Mathematics

CAMBRIDGE
UNIVERSITY PRESS
www.cambridge.org
ISBN 0-521-79722-5
9 780521 797221