Random Graphs, Strongly Regular Graphs and Pseudo-random Graphs

Andrew Thomason†
Department of Mathematics
University of Exeter
North Park Road
Exeter EX4 4QE
England

1. Introduction.

Despite the title this article is not an attempt to be all things to all men. For although random graphs and strongly regular graphs are often thought of as opposite ends of a spectrum, the one being chaotic and disordered, the other being structured and symmetric, there are certain occasions on which they might bear similarities. These occasions are broadly of two kinds:

(i) there are extremal graph theory problems where both random graphs and strongly regular graphs provide the extremal configurations, or, at least, the best known approximations, and

(ii) there are instances where graphs with certain desired properties can be shown to exist by random methods, but where the best constructed examples are strongly regular, or close to strongly regular.

(Of course, these two instances overlap somewhat.) On these occasions both types of graph may be thought of as being covered by the umbrella term 'pseudo-random graph'. The purpose of this paper is to try and make precise this similarity and to offer the elements of a common treatment for both types of graph.

Caveat. Let it be said at once that we can prove nothing about random graphs which cannot be proved better by standard methods, and our methods are of little effect in sparse graphs anyway. Likewise we tackle only a restricted class of strongly regular graphs, namely those with parameters (k, λ, μ) where $\lambda \approx \mu$ (or equivalently those whose two non-trivial eigenvalues are opposite in sign and approximately equal in magnitude). However for this class it is possible to obtain some new results.

The aim of a common treatment for the different types of graph in case (i) above would be to attempt a characterisation of the extremal graphs for the given problem, and so perhaps help to compute the extremal function. This approach was successful in the proof of Theorem 2.3 below and in establishing new upper bounds for ramsey numbers; it also produced unexpected results about another problem

† *Current address*: Department of Pure Mathematics and Mathematical Statistics, 16, Mill Lane, Cambridge CB2 1SB, England.

Reprinted from Surveys in Combinatorics, 1987
(ed. C Whitehead) LMS Lecture Note series 123

(discussed in section 6). The aim in case (ii) would be to provide a way to check whether a given construction is 'pseudo-random', and so has the desired property. Some results of this kind are discussed in section 5.

At present this discussion may appear a bit vague, but in section 3 we will give a precise definition of a class of graphs (*jumbled* graphs) which will be our class of pseudo-random graphs, and show that both random graphs and certain types of strongly regular graphs fall into this class. In section 4 we develop some properties of jumbled graphs and in section 6 look at some of the consequences. To begin with, though, we look at some of the instances of the problems mentioned at the outset.

For matters concerning random graphs we refer to the recent treatise of Bollobás [**12**]. The material in chapter 13 of that work is of particular relevance. The notation $\mathcal{G}(n,p)$ will refer to the probability space of labelled graphs on n vertices where the edges are chosen independently and at random with probability p. We shall use the phrase 'a random graph has property P', where P is a graph property, to mean that a graph in $\mathcal{G}(n,p)$ has P almost surely, that is, $\Pr(G \in \mathcal{G}(n,p) \text{ has } P) \to 1$ as $n \to \infty$.

2. Some examples.

Here we give some examples of occasions when random graphs and strongly regular graphs appear similar.

RAMSEY THEORY.

The best illustration is provided by the first ever result on random graphs. Let $r(K_t)$ be the ramsey number of K_t, that is, the smallest value of n such that every colouring of the edges of the complete graphs K_n of order n with two colours yields a monochromatic K_t.

Theorem 2.1. (Erdős [28], 1947) $\quad r(K_t) > 2^{t/2}$.

This lower bound is obtained because there is only a very small probability of finding a K_t in a random graph of order $2^{t/2}$ or its complement. Remarkably, there is no known constructive lower bound which is provably of exponential order, the best being $r(K_t) > \exp((1+o(1))(\log t)^2/4\log\log t)$ by Frankl and Wilson [**35**]. When it comes to exact values, though, strongly regular graphs appear. The only exact values known are $r(K_3) = 6$ and $r(K_4) = 18$, the extremal colourings being provided by the Paley graphs Q_5 and Q_{17}. The *Paley graph* Q_n of order n has vertex set the finite field $\mathbf{F}_n$, $n \equiv 1 \pmod 4$, with $xy \in E(Q_n)$ if $x-y$ is a square in $\mathbf{F}_n$. Elementary character sums show that Q_n is a conference graph; that is, it is $(n-1)/2$-regular, each edge is in $(n-5)/4$ triangles, and that the same holds for the complement. A conference graph is strongly regular with parameters $((n-1)/2, (n-5)/4, (n-1)/4)$.

Conference graphs resemble random graphs with edge probability $1/2$ in that each vertex has degree around $n/2$ and each pair of vertices has around $n/4$ common neighbours. This suggests that lower bounds for ramsey numbers are provided by random-like graphs. (Indeed, by considering the extremal graphs for the function $r(K_t)$ as being pseudo-random it is possible to obtain a new upper bound for $r(K_t)$, as described in section 6.) More generally it would suggest that if n is large, a colouring of K_n with few monochromatic K_t's is random-like, leading to the following conjecture. Let $k_t(G)$ denote the number of complete subgraphs in G of order t, and let $\overline{G}$ denote the complement of G. Let

$$c_t(n) = \min\{\, k_t(G) + k_t(\overline{G})\,;\ |G| = n \,\} \binom{n}{t}^{-1}$$

where $|G|$ is the order of G. (We use the notation of [11].) So $c_t(n)$ is the minimum proportion of monochromatic K_t's in a colouring of K_n. Then $r(K_t) = \min\{n; c_t(n) > 0\}$. It is easily shown that $c_t(n)$ increases with n so $c_t = lim_{n\to\infty} c_t(n)$ exists.

Conjecture. (Erdős [29], 1962). $\quad c_t = 2^{1-\binom{t}{2}}$.

Note that $2^{1-\binom{t}{2}}$ is the proportion of monochromatic K_t's in a random colouring. In fact it will be shown later (Theorem 4.8) that a conference graph yields the same proportion of monochromatic K_t's. This suggests that the extremal graphs for the function $c_t(n)$ are 'pseudo-random', and so might be those characterised in section 3. Indeed the corresponding conjecture involving complete bipartite subgraphs of bipartite graphs has been completely proved by Erdős and Moon [30]. (The corresponding conjecture is that the minimum proportion of monochromatic subgraphs is the same as the average proportion.) Surprisingly, it turns out Erdős' conjecture is *false*; counterexamples can be constructed by modifying certain pseudo-random graphs. We will return to this in section 6.

THE PROBLEM OF ZARANKIEWICZ.

This extremal problem (or a typical case of it) is that of computing the function $Z(n,t)$, the greatest number of edges in a graph of order n which contains no complete bipartite subgraph $K_{t,t}$. For a general discussion see Bollobás [11]. Upper bounds on $Z(n,t)$ are due to Kövári, Sós and Turán [49] and Znám [72].

Theorem 2.2. $\quad \frac{1}{2}n^{2-2/(t+1)} < Z(n,t) < \frac{1}{2}(t-1)^{1/t}n^{2-1/t} + \frac{1}{4}(t-1)n.$

The general lower bound is obtained from random graphs with the appropriate number of edges. For $t = 2$ a better lower bound is obtained by considering graphs constructed from finite geometries. The graph constructed with vertex set

$PG(2,q)$ by joining $a{:}b{:}c$ to $\alpha{:}\beta{:}\gamma$ if $a\alpha + b\beta + c\gamma = 0$ (Erdős and Rényi [31]), shows $Z(n,2) = \frac{1}{2}n^{3/2}(1+o(1))$ if n is large. This graph is not strongly regular, but the degrees differ by at most one and the number of common neighbours of a pair of vertices varies by at most one. In a similar vein Brown [22] constructed from $AG(3,q)$ bipartite graphs with n vertices and order $n^{5/3}$ edges, containing no $K_{3,3}$. The vertices of this graph consist of two copies of $AG(3,q)$, with (x_1,x_2,x_3) joined to (y_1,y_2,y_3) if $\sum_{i=1}^{3}(x_i-y_i)^2 = -s$, where s is some fixed quadratic non-residue. The graph is (q^2-q)-regular and no pair of vertices has more than $q+1$ common neighbours. At least to this extent the extremal graphs for the Zarankiewicz problem are pseudo-random.

SUBCONTRACTIONS.

The fundamental extremal problem involving subcontractions is to determine the greatest number of edges in a graph G of given order which does not contract to a complete graph of order t; we write $G \not\succ K_t$. It is not hard to show that the function

$$b(t) = \lim_{n\to\infty} \inf\{\, b\,;\ |G| = n \text{ and } e(G) \geq b|G| \text{ implies } G \succ K_t \,\}$$

exists, and is at most 2^{t-3}. Mader [51] proved $t-2 \leq b(t) \leq 8(t-2)\lfloor \log_2(t-2)\rfloor$ for $t \geq 4$. Only recently it was noticed that random graphs show $b(t) \geq \frac{1}{4}t\sqrt{\log_2 t}(1+o(1))$ (de la Vega [68], Kostochka [48], Thomason [61]), and the latter two references contain proofs that $t\sqrt{\log t}$ is the correct order for $b(t)$. The next result is from [61].

Theorem 2.3. $0{\cdot}265t\sqrt{\log_2 t}(1+o(1)) \leq b(t) \leq 2{\cdot}68t\sqrt{\log_2 t}(1+o(1))$.

It might be expected that the extremal graphs for this problem are pseudo-random, and it was by examining subcontractions in pseudo-random graphs that the simple proof in [61] was discovered.

THE DIAMETER.

The function $n(D,\Delta)$, the greatest number of vertices in a graph of maximum degree Δ and diameter D seems very hard to determine. It is easily shown that $n(D,\Delta) \leq (\Delta(\Delta-1)^D - 2)/(\Delta-2)$. From below the de Bruijn graphs show $n(D,\Delta) \geq \lfloor \Delta/2 \rfloor^D$. The vertices of the de Bruijn graph $dB(k,d)$ are the k^d vectors with d coordinates which are integers between 1 and k. Two vectors are adjacent in the graph if the first $k-1$ coordinates of one agree with the last $k-1$ coordinates of the other. Most of the best results about $n(D,\Delta)$ are quite recent. For good surveys covering different aspects of this area see Bermond and Bollobás [7], Bermond, Bond, Paoli and Peyrat [8] and Bollobás [12]. From our point of view we note that random regular graphs provide the best known bounds for many instances of $n(D,\Delta)$. This

is natural in that the paths from a vertex in an extremal graph must spread out as much as possible, and that is a property of random regular graphs. The extremal graphs are pseudo-random but this is a case where the methods of section 3 do not apply easily, because the edge density is too low, and so we can make no worthwhile contribution.

EXPANDER GRAPHS.

A bipartite graph with vertex classes X and Y each of order n is (n, a, b)-*expanding* if every subset $A \subset X$ of order a has at least b neighbours in Y. It is an (n, k, β)-*expander* if it is $(n, x, x(1+\beta(1-x/n)))$-expanding for all $x \leq n/2$. Much interest has been shown lately in graphs with few edges which are good expanders. They are used for instance in the construction of concentrators and superconcentrators (Margulis [**52**], Valiant [**67**], Chung [**25**]), and the expanding properties of graphs are used implicitly or explicitly in the construction of parallel sorting algorithms (Häggkvist and Hell [**43**], Bollobás and Thomason [**19**], Ajtai, Komlós and Szemerédi [**1**], Alon [**3**]). Random graphs provide the best upper bounds known for the size of expanders (see Chung [**25**]). Many constructions have been found, some such as that of Margulis [**52**] requiring deep techniques for proof. The construction of concentrators requires expanders whose sizes are linear in the number of vertices, and such graphs are again too sparse for our techniques to be amenable. But sometimes a dense expander needs to be constructed (say for sorting applications) and here we can make some contribution. We will return to this in section 5.

3. Jumbled graphs.

In a random graph in $\mathcal{G}(n,p)$, each induced subgraph H satisfies $e(H) \approx p\binom{|H|}{2}$, where $e(H)$ is the number of edges of H. The least we might require of a graph which mimics a random graph of edge probability p is that the same property holds. To this end, we call the quantity $\left|e(H) - p\binom{|H|}{2}\right|$ the *error* of the subgraph H, and we will define a pseudo-random graph to be one in which no induced subgraph has large error. It is the choice of error term which determines the usefulness of the definition; the one we choose was described in [**62**].

Definition. *Let p, α be real numbers with $0 < p < 1 \leq \alpha$. A graph G is said to be* (p, α)-jumbled *if every induced subgraph H satisfies*

$$\left|e(H) - p\binom{|H|}{2}\right| \leq \alpha|H|.$$

The reason for choosing this form of error term is first of all that it depends only on H, so implying

(a) if G is (p, α)-jumbled then $\overline{G}$ is $(1-p, \alpha)$-jumbled, and

(b) if G is (p, α)-jumbled and G' is an induced subgraph of G then G' is (p, α)-jumbled.

The form of error term also enables us to prove Theorems 3.1 and 3.2 below, which we will discuss later.

What is the significance of the parameter α? Of course, every graph of order n is $(p, n/2)$-jumbled but if a graph is known to be $(p, o(n))$-jumbled quite a lot can be said about its properties, as we shall see. A conference graph of order n is $(p, \sqrt{n})$-jumbled by Theorem 3.1 below; in fact a theorem of Erdős and Spencer [32] (or more precisely a theorem proved by a method similar to a proof in [32]) shows that if G is (p, α)-jumbled then $\alpha \neq o(\sqrt{pn})$. Observe that the definition permits us to say nothing useful about subgraphs H of G if $p|H| = O(\alpha)$. Since we often need information about the neighbourhood of a vertex, which will usually have order around pn, we mostly need $\alpha = o(p^2 n)$. Because of this inequality and the relation $\alpha \neq o(\sqrt{pn})$ our methods will be most easily applied to dense graphs, that is with $p \geq n^{-1/3}$. From time to time we shall use the term 'jumbled graph' by itself, without specifying the values of p and α, to mean a (p, α)-jumbled graph where α is suitably small (say $\alpha = o(p^2 n)$). The word 'jumbled' is intended to convey the fact that the edges are evenly spread through the graph.

We aim to show that jumbled graphs mimic in many ways the *large scale* properties of random graphs with edge probability p. But before describing the properties of jumbled graphs, let us see some examples of them. There are essentially two ways to test whether a graph is (p, α)-jumbled for some small α. First of all, each subgraph H might be tested against the definition. In this way it can be shown that a random graph is $(p, 2\sqrt{pn})$-jumbled; this is fortunate, for otherwise our class of pseudo-random graphs would not contain random graphs themselves. However we are not always put to so much trouble.

Theorem 3.1. *Let G be a graph of order n, with minimum degree pn. If no pair of vertices has more than $p^2 n + l$ common neighbours, G is $(p, \sqrt{(p+l)n})$-jumbled.*

This is a remarkable (though simply proved) result, since it shows that the condition on vertex degrees and common neighbours, which we noticed in earlier examples, is actually sufficient to make a graph behave like a random graph. This theorem is very useful for showing that specific constructions, such as Paley graphs and others in the following list, are jumbled. The need to examine all induced subgraphs is removed, and all that remains is a simple degree check. (The proof of the theorem is indeed simple, depending only on the Cauchy-Schwartz inequality or second moment method, and so is probably implicit in several earlier works by other authors. In fact the conditions in the theorem imply a somewhat stronger

conclusion, namely that the error of an induced subgraph H is at most $(1+\sqrt{pn}+\sqrt{l|H|})|H|$. Under certain circumstances this would yield information about H when the conclusion of Theorem 3.1 was too weak, for instance if $l \approx \sqrt{n}$ and $|H| \approx n^{5/8}$. Of course we could modify our definition of a jumbled graph to take account of this extra strength, for instance by calling a graph (p, α, β)-jumbled if the error of any induced subgraph H is at most $(\alpha+\beta\sqrt{|H|})|H|$. Our reason for not doing so, apart from the extra complication that would arise with a fancier error term, is that no correspondingly stronger version of Theorem 3.2 below would be obtained. In any case no occasion has arisen so far where the full strength of the proof of Theorem 3.1 was needed. *N.b.* A gap in the proof of Theorem 3.1 given in [**62**] is filled in [**66**].)

SOME JUMBLED GRAPHS.

(a) A random graph in $\mathcal{G}(n,p)$ is $(p, 2\sqrt{pn})$-jumbled.

(b) A random graph in $\mathcal{G}(n,p)$, with edges added to form a clique of order $\sqrt{pn}$, is $(p, 3\sqrt{pn})$-jumbled.

(c) The vertex disjoint union of a random graph in $\mathcal{G}(n,p)$ and a clique $K_{\sqrt{pn}}$ is $(p, 3\sqrt{pn})$-jumbled.

The above examples show that the small subgraphs of a jumbled graph may be far from random.

(d) The Paley graphs Q_n are $(1/2, \sqrt{n})$-jumbled.

(e) Let $n = 2kr+1$ be a prime power. The graph whose vertices are the elements of the finite field $\mathbf{F}_n$, with x joined to y if $x-y$ is a k'th power, is $(1/k, 2n^{3/4})$-jumbled. This follows from Theorem 3.1 and estimates of Weil [**70**] for character sums. This graph is not strongly regular unless $k=2$, when it is the Paley graph. If we let xy be an edge if $x-y$ is in one of j specified cosets of the k'th powers we obtain a graph which is $(j/k, 2n^{3/4})$-jumbled.

Hence we have specific constructions which emulate graphs in $\mathcal{G}(n,p)$ for any fixed rational value of p.

(f) The previous construction works if we join x to y whenever $x+y$ is a k'th power. This graph is not strongly regular even if $k=2$. The example is interesting, though, because an obvious generalisation enables us to construct pseudo-random hypergraphs. This subject is explored further by Haviland and Thomason [**44**].

(g) Let the vertices of a graph be the vectors of the space $\mathrm{AG}(2,q)$, and partition the set of $q+1$ lines in this space into two sets P and N, with $|P|=k$. Join $\mathbf{x}$ to $\mathbf{y}$ if $\mathbf{x}-\mathbf{y}$ is parallel to a line in P. Then G is strongly regular with parameters $(k(q-1), (k-1)(k-2)+q-2, k(k-2))$, as recorded by Hubaut [**45**] and Seidel [**57**], and is $(k/q, n^{3/4})$-jumbled.

(h) Let the vertices of the graph T_k^+ be the $n = 2^{2k}$ vectors in AG$(2k, 2)$, with $\mathbf{x}$ joined to $\mathbf{y}$ if $q^+(\mathbf{x} - \mathbf{y}) \neq 0$, where

$$q^+((x_1, x_2, \ldots, x_{2k})) = x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}.$$

The graph T_k^- is defined similarly by using q^-, where $q^-(\mathbf{x}) = x_1 + x_2 + q^+(\mathbf{x})$. The graphs $T_k^\pm$ are strongly regular with parameters $(2^{2k-1} \mp 2^{k-1}, 2^{2k-2} \mp 2^{k-1}, 2^{2k-2} \pm 2^{k-1})$ (see for example Thomason [63], Seidel [57] or Hubaut [45]), and so are $(1/2, n^{3/4})$-jumbled.

(i) Let the vertices of G be the elements of PG(k, q). Join the vertex $x_0{:}x_1{:}\ldots{:}x_k$ to the vertex $y_0{:}y_1{:}\ldots{:}y_k$ if $x_0y_0 + \cdots + x_ky_k = 0$. This graph is $(1/q, 2\sqrt{n/q})$-jumbled. When k=2 this graph is the Erdős-Rényi graph mentioned in section 2. Note that $q \sim n^{1/k}$, so we have a way to model graphs in $\mathcal{G}(n, n^{-1/k})$.

(j) The previous example may be viewed, when $q = 2$, as the graph whose vertices are the non-empty subsets of a set of order $k+1$, two vertices being adjacent if their intersection has even order. Let G be the subgraph spanned by the subsets of even order. Then G is $(1/2, 2\sqrt{n})$-jumbled, where $n = 2^k - 1$. In fact if k is even then G is strongly regular, with parameters $((n-3)/2, (n-11)/4, (n-3)/4)$.

(k) In the previous example we could have looked at the subgraph spanned by the vertices of odd order. This is also $(1/2, 2\sqrt{n})$-jumbled.

(l) Let the vertices of the graph $B(n, t)$ be the elements of the field $\mathbf{F}_n$, where n is prime, and let t be an integer, $1 < t < n$. Join x to y if the fractional part of $(x - y)^2/n$ is at most t/n. A theorem of Bollobás quoted in section 5 implies this graph is $(t/n, 3n^{3/4} \log n)$-jumbled.

(m) Let G be a graph of order r, and let $m \geq 1$ be an integer. Denote by $m \circ G$ the graph of order mr obtained by taking r disjoint sets of vertices V_x, $x \in G$, with $|V_x| = m$, and joining $v_x \in V_x$ to $v_y \in V_y$ if x is joined to y in G. Note that $m_1 \circ (m_2 \circ G) = (m_1 m_2) \circ G$. If G is (p, α)-jumbled then $m \circ G$ is $(p, m\alpha + m)$-jumbled.

(n) The graph $2 \bullet G$ is formed from two disjoint copies G_1 and G_2 of G; if $x_1 \in G_1$ and $y_2 \in G_2$ then $x_1y_2 \in E(2 \bullet G)$ if $x = y$ or $xy \notin E(G)$. For suitable choices of G this graph provides good lower bounds for ramsey numbers, as Mathon [53] showed. However there is no profit in iterating the operation $2\bullet$, since $2 \bullet (2 \bullet G)$ is isomorphic to $2 \bullet (2 \circ G)$.

These are just a few graphs we have selected, either because they are well known, or because they will be used as examples later, or simply to illustrate how easy it is to find examples of jumbled graphs. There are many others. Some more are given in [62], and there are many more strongly regular graphs with $\lambda \approx \mu$,

such as those listed in [45] or some new ones of Brouwer [21]. The point is that Theorem 3.1 gives a very easy way of checking whether a given graph is jumbled.

From the point of view of describing the extremal graphs for certain problems, the following theorem from [62] gives a property of graphs which are *not* jumbled.

Theorem 3.2. *Let G be a graph of order n, let ηn be an integer between 2 and $n-2$, and let $\omega > 1$ be a real number. Suppose each induced subgraph H of order ηn satisfies $\left|e(H) - p\binom{\eta n}{2}\right| \leq \eta n \alpha$. Then G is $(p, 7\sqrt{n\alpha/\eta}/(1-\eta))$-jumbled. Moreover G contains an induced subgraph G^* of order at least $\left(1 - \frac{880}{\eta(1-\eta)^2\omega}\right)n$ which is $(p, \omega\alpha)$-jumbled.*

The proof is by no means as straightforward as that of Theorem 3.1. To see how this theorem might be used, let $G_1, G_2, \ldots$ be a sequence of graphs with $|G_n| = n$, and let η be a constant between zero and one. Let $\alpha(n)$ be any function of n satisfying $\alpha(n) = o(n)$, and choose $\omega(n)$ so that $\omega(n)\alpha(n) = o(n)$ and $\omega(n) \to \infty$. Then the theorem shows that there is a constant $\delta = \delta(\eta)$ such that either G_n contains an induced subgraph G_n^* of order $(1 + o(1))n$ which is $(p, o(n))$-jumbled (which is often as good as G_n itself being jumbled), or G_n contains an induced subgraph H of order $\lfloor \eta n \rfloor$ with $\left|e(H) - p\binom{|H|}{2}\right| > \delta n^2$. An example of the use of this theorem occurs in section 6.

4. Properties of jumbled graphs.

Here we give some properties of jumbled graphs which illustrate their claim to be pseudo-random. The first few are basic properties of vertex degrees.

Theorem 4.1. *Let G be a (p, α)-jumbled graph of order n, and let $0 < \epsilon < 1$. Then at least $(1-\epsilon)n$ of the vertex degrees of G lie in the range $p(n-1) \pm 10\alpha\epsilon^{-1}$.*

Theorem 4.2. *Let G be a (p, α)-jumbled graph of order n, and let $0 < \epsilon < 1$. Let H be an induced subgraph of G of order k. Then at least $n - \epsilon k$ of the vertices of G have between $pk - 21\alpha\epsilon^{-1}$ and $pk + 21\alpha\epsilon^{-1}$ neighbours in H.*

Under the degree conditions of Theorem 3.1 (by which phrase we shall speak of a graph, such as a conference graph, with minimum degree pn, in which no pair of vertices has more than $p^2n + l$ common neighbours for some small l), it is possible to show that almost all sets of k vertices have around $p^k n$ common neighbours. For general graphs these conditions don't apply, but we do have the following result. In this the number of vertices joined to every vertex in a set U_1 and to no vertex in a set U_2 is denoted $v(U_1, U_2)$.

Theorem 4.3. *Let G be a (p,α)-jumbled graph of order n, let $k,l \geq 0$ be integers and let $0 < \epsilon < 1$. Then $|v(U_1,U_2) - p^k q^l n| < 21(k+l)^2\alpha\epsilon^{-1}$ for at least $(1-\epsilon)\binom{n}{k}\binom{n-k}{l}$ choices of sets U_1 and U_2 with $|U_1| = k$ and $|U_2| = l$. (Here $q = 1-p$.)*

These degree conditions and the definition of a (p,α)-jumbled graph enable us to establish many analogues of well known random graph properties for jumbled graphs. We list just a few of the more obvious ones.

THE DIAMETER.

It is easily seen that a random graph in $\mathcal{G}(n,p)$ has diameter 2 if $p^2n - 2\log n \to \infty$. For jumbled graphs we come fairly close.

Theorem 4.4. *Let G be a (p,α)-jumbled graph. Let $u,w \in G$ be vertices with degree at least d. If $pd > 4\alpha$ there is a u-v path of length at most 3 in G. In particular, if $\delta(G) > 4\alpha p^{-1}$ then G has diameter at most 3.*

THE CONNECTIVITY.

For a random graph in $\mathcal{G}(n,p)$ the vertex connectivity equals the minimum degree (see Bollobás and Thomason [**20**]).

Theorem 4.5. *Let G be a (p,α)-jumbled graph of order n. Then $\kappa(G) > \delta(G) - 4\alpha p^{-1} + 1$.*

For graphs satisfying the degree conditions of Theorem 3.1 this can be improved to $\kappa(G) = \delta(G)$.

HAMILTON CYCLES.

A random graph is hamiltonian if $pn - \log n - \log\log n \to \infty$ (this is not easy to prove; see [**12**]). The same is certainly not true for a jumbled graph if p is small, even if we impose a minimum degree condition; consider example (c). But if p is larger we can make progress.

Theorem 4.6. *Let G be a (p,α)-jumbled graph of order n, with minimum degree at least pn. If $(p-k/n)^2 n \geq 6(\alpha+2k)$, where k is a non-negative integer, then G has a set of $k+1$ edge disjoint hamilton cycles.*

Theorem 4.7. *Let G be a (p,α)-jumbled graph of order n, with minimum degree $pn \geq m = \lceil 6\alpha p^{-1}\rceil$. Then G has at least $\frac{1}{2}(pn)!/m!$ hamilton cycles.*

These theorems show for instance the existence of an exponentially large number of hamilton cycles, and a set of $(n/100)$ edge disjoint hamilton cycles, in the Paley graphs. This answers a question of Calkin [**24**]. Theorems 4.6 and 4.7 are proved using the Chvátal-Erdős theorem [**26**] to generate hamilton cycles, rather than applying the flipping method commonly used in random graph results. This

method has also been applied to find a linear expected time hamilton cycle algorithm for graphs in $\mathcal{G}(n,p)$ if $p \geq 12n^{-1/3}$; see [64].

INDUCED SUBGRAPHS, CLIQUES AND THE CHROMATIC NUMBER.

We turn now to induced subgraphs, since one of our original aims was to investigate the apparently extremal graphs for Erdős' conjecture. Previous methods for estimating complete subgraphs have been rather *ad hoc*. Several authors (Blanchard [9], Bollobás and Thomason [18], Graham and Spencer [39]) have shown that $k_t(Q_n) = 2^{-\binom{t}{2}}\binom{n}{t}(1+O(n^{-1/2}))$ by using Weil's estimates [70] for character sums. For $t = 4$ the exact result, $k_4(Q_n) = n(n-1)((n-5)(n-17)+4(a^2-1))/1536$, where $n = a^2+b^2$ and a is odd and coprime to n, was obtained by Evans, Pulham and Sheehan [34] and Thomason [60]. The only general result so far was due to Giraud [37] who shows that $k_4(G)+k_4(\overline{G}) = \frac{1}{32}\binom{n}{4}(1+O(n^{-1/2}))$ if G is a conference graph. The following theorem extends this to a much larger class of graphs, and for all values of t.

Theorem 4.8. *Let G be a (p,α)-jumbled graph of order n, where $p \leq 1/2$. Let F be a graph of order $r \geq 3$ with m edges, and let A be the order of its automorphism group. Suppose ϵ satisfies $0 < \epsilon < 1$ and $\epsilon^2 p^r n \geq 42\alpha r^2$. Then the number of induced subgraphs of G isomorphic to F lies between $(1-\epsilon)^r p^m q^{\binom{r}{2}-m} A^{-1} n^r$ and $(1+\epsilon)^r p^m q^{\binom{r}{2}-m} A^{-1} n^r$, where $q = 1-p$.*

Rosenfeld asked if a strongly regular graph could be found containing a given graph F as an induced subgraph. A graph containing *every* graph of order r as an induced subgraph was called *r-full* by Bollobás and Thomason [18], who showed that the Paley graphs of large order are r-full. Theorem 4.8 combined with Theorem 3.1 offers a great many more examples.

Theorem 4.8 shows that in a $(1/2, O(\sqrt{n}))$-jumbled graph the number of complete subgraphs is around $2^{-\binom{t}{2}}\binom{n}{t}$ for t up to about $\frac{1}{2}\log_2 n$. It would be reasonable to hope to push this up to $\log_2 n$. But although this may be true for the Paley graphs, as we see at the end of section 6, it is in general untrue. In the graph of example (j) the number of K_t's constructed by first choosing $k/2$ independent mutually orthogonal vectors and then choosing $r = t-k/2$ more in the space spanned by the first $k/2$ is of order $2^{-\binom{t}{2}+\binom{r}{2}}\binom{n}{t}$, as shown in [62]. So Theorem 4.8 cannot be improved in general.

If we ask for the clique number of a $(1/2, O(\sqrt{n}))$-jumbled graph, Theorem 4.8 shows it is at least $\frac{1}{2}\log_2 n$. No example is known where it is so small, but the clique number of example (k) is only $\log_2 n$. On the other hand the clique number may be as large as $\sqrt{n}$, as many of our examples show. Of course it will not be much larger since it follows directly from the definition that the clique number

of a (p, α)-jumbled graph is at most $1 + 2\alpha(1-p)^{-1}$. This contrasts with random graphs in $\mathcal{G}(n, 1/2)$, where the clique number is known always to within one and usually exactly (see Matula [54] or Bollobás and Erdős [17]). Estimates for the chromatic number are related to those of the clique number, so by a greedy algorithm we can colour a $(1/2, O(\sqrt{n}))$-jumbled graph with at most $2n/\log_2 n$ colours, the corresponding value for random graphs being $n/\log_2 n$ (Grimmett and McDiarmid [40]). However, there is a lower bound of $n/2\log_2 n$ for the chromatic number of a random graph, whereas the chromatic number of a $(1/2, O(\sqrt{n}))$-jumbled graph may be as low as $\sqrt{n}$. This is the case, for example, in the Paley graph Q_n if n is a perfect square.

SUBCONTRACTIONS AND TOPOLOGICAL CLIQUES.

The *contraction clique number* $ccl(G)$ of a graph G is the largest value of t for which $G \succ K_t$. The *topological clique number* $tcl(G)$ is the largest value of t for which G contains a subdivision of K_t. Of course, $ccl(G) \geq tcl(G)$. The values of $ccl(G)$ and $tcl(G)$ were investigated by Bollobás, Catlin and Erdős [15] and by Bollobás and Catlin [14] in relation to the conjectures of Hadwiger and Hajós. (The former conjectured $ccl(G) \geq \chi(G)$, which holds for almost every graph, the latter speculated that $tcl(G) \geq \chi(G)$, which fails for almost every graph.) They found $ccl(G) = n/\sqrt{\log_b n}(1 + o(1))$, where $b = 1/(1-p)$, and $tcl(G) = 2\sqrt{n/(1-p)}(1 + o(1))$ almost surely, for $G \in \mathcal{G}(n, p)$, with p constant. Use of the theorems at the beginning of this section and the techniques of [61] gives the following.

Theorem 4.9. *Let p, C be constants, let G_n be a $(p, C\sqrt{n})$-jumbled graph of order n, and let $b = 1/(1-p)$. Then, as $n \to \infty$,*

$$ccl(G_n) \geq (1 + o(1))n/\sqrt{\log_b n}$$

and

$$2(1+C)(1-p)^{-1}\sqrt{n} \geq tcl(G_n) \geq (1 + o(1))\sqrt{pn}.$$

A more general result for $tcl(G)$ is available in [62]. We give no upper bound for $ccl(G)$. For consider the graph G with vertex set $\{x_i, y_i; 1 \leq i \leq n/2\}$, where $x_i y_i \in E(G)$ and for each pair $1 \leq i < j \leq n/2$ the vertex x_i is joined to exactly one of x_j and y_j chosen at random, and so is y_i. Then G is $(1/2, 2\sqrt{n})$-jumbled, and indeed the graphs spanned by $\{x_1, \ldots, x_{n/2}\}$ and $\{y_1, \ldots, y_{n/2}\}$ are randomly chosen members of $\mathcal{G}(n/2, 1/2)$. But $ccl(G) \geq n/2$. In fact $ccl(G)$ cannot be much bigger than this since the clique number must be at least $ccl(G) - n/2$.

5. Other techniques.

The methods used to obtain results in sections 3 and 4 were elementary though complicated. Other techniques have been used on jumbled graphs, apart

from those alluded to so far. Here we describe briefly one or two of them. For the Paley graphs, Bollobás used the method of Gauss sums to obtain the following.

Theorem 5.1. (Bollobás [13]) *The number of edges between a set of k vertices of the Paley graph Q_n and another disjoint set of l vertices lies between $\frac{1}{2}kl - \frac{1}{2}\sqrt{kln}$ and $\frac{1}{2}kl + \frac{1}{2}\sqrt{kln}$.*

This improves on Theorem 4.3 for this particular graph. In particular if n is large, we see $v(U_1, U_2) \neq 0$. This implies that every first order graph property is either possessed by almost every graph in $\mathcal{G}(n,p)$ and by Q_n for all large n or is possessed by almost no graph in $\mathcal{G}(n,p)$ nor by Q_n for all large n (see for instance [12]).

The theorem also shows that Theorem 3.1 cannot be significantly improved if we require say every three vertices to have around p^3n common neighbours. For Q_n contains complete subgraphs of order $\sqrt{n}$ if n is a perfect square, and so is not $(1/2, \alpha)$-jumbled for $\alpha < \sqrt{n}/2$. Moreover none of the other results of section 4 can be improved significantly for this graph.

Recall the graph $B(n,t)$ of example (l). This graph is clearly regular of degree $d = |\{x \in \mathbf{F}_n; x^2 \in \{1, \ldots, t\}\}|$. If $t \gg n^{1/4} \log n$ then $d/t \to 1$; in fact the Pólya-Vinogradov inequality (see Ayoub [6]) states $|d - t| < \sqrt{n} \log n$, and a deep improvement by Burgess [23] reduces the $\sqrt{n}$ to $At^{1-1/(r+1)}n^{1/4r}$, where A is an absolute constant and r is any positive integer. The following theorem of Bollobás gives bounds on the number of common neighbours a pair of vertices might have. The pleasing proof is based on that of Pólya.

Theorem 5.2. (Bollobás [12]) *No two vertices of the graph $B(n,t)$ have more than $t^2/n + \sqrt{n} \log^2 n$ common neighbours.*

Consequently the graph $B(n,t)$ can be shown to be $(p, 3n^{3/4} \log n)$-jumbled by Theorem 3.1. A universal analogue of this graph has been constructed by Bollobás and Erdős [16]. Denote by $R(n, \alpha, \delta)$ the graph with vertex set $\{1, \ldots, n\}$, in which ij is an edge if the fractional part of $(i-j)^2\alpha$ is less than δ; here we require α to be irrational and $0 < \delta < 1$ but n need no longer be prime. Pinch used classical results of Hardy and Littlewood to prove a conjecture of Bollobás and Erdős about $R(n, \alpha, \delta)$, which shows that it is $(\delta, o(n))$-jumbled.

Theorem 5.3. (Pinch [56]) *For every irrational α there is a function $f_\alpha : \mathbf{N} \to \mathbf{N}$ such that $f_\alpha(n) = o(n)$, and such that no two vertices in any graph $R(n, \alpha, \delta)$ have more than $\delta^2 n + f_\alpha(n)$ common neighbours.*

Quite a few techniques have been developed for use on expander graphs. (Recall the definitions of section 2.) Margulis was the first to construct a family of

linear expanders as follows. The vertex classes X and Y are both copies of $\mathbf{Z}_m \times \mathbf{Z}_m$. Join (a,b) in X to (a,b), $(a+1,b)$, $(a,b+1)$, $(a,a+b)$ and $(-b,a)$ in Y, and call the resulting graph $M(m)$. Using fairly deep techniques from representation theory, Margulis proved an expansion property for these graphs.

Theorem 5.4. (Margulis [52]) *There is an absolute constant β_0 such that $M(m)$ is an $(m^2, 5, \beta_0)$-expander.*

Unfortunately no lower bound is provided for β_0. However variants of this construction have been shown to be good expanders by some authors, and Gabber and Galil [36] were able to give explicit values of β, using fourier analysis. These have been further refined; see for example Alon and Milman [5], Jimbo and Maruoka [46] and Alon, Galil and Milman [4] (among many others. The papers cited contain many references to the literature). A useful idea of Tanner [59], developed by Alon [2], gives a valuable sufficient condition for a graph to be a good expander. Alon was able to go considerably further, though, and show the necessity of the condition. A graph is a *strong (n,k,β)-expander* if it is $(n, x, x(1+\beta(1-x/n)))$-expanding for all $x \leq n$. Given a graph G we define $\lambda(G)$ to be the second smallest eigenvalue of the matrix $D - A$, where D is the diagonal matrix of vertex degrees and A is the adjacency matrix. It is easily checked that if G is regular the smallest eigenvalue is 0 and $\lambda(G) > 0$.

Theorem 5.5. (Alon [2]) *Let G be a k-regular bipartite graph. If G is a strong (n,k,β)-expander then $\lambda \geq \beta^2/(1024 + 2\beta^2)$. If $\beta \leq (2d\lambda - \lambda^2)/d^2$ then G is a strong (n,k,β)-expander.*

This is a very useful result, especially since the best expanders are generated randomly and we can estimate the expansion properties very quickly by this method, though to compute the expansion properties exactly is known to be coNP-complete; see Blum, Karp, Vornberger, Papadimitriou and Yannakakis [10]. It is also possible to verify explicit constructions.

For the purposes of constructing superconcentrators very sparse (in fact linear) expanders are needed. But some applications, notably parallel sorting in few rounds, make use of dense expanders, and here the ideas of section 3 start to bear fruit. To sort n objects which are ordered in some unknown way in just two rounds using m parallel processors, m pairs of objects, determined by some algorithm (which of course is just a graph of order n and size m) are compared. All possible deductions are made by transitivity, and any pairs whose relative order is still hidden are then compared. The algorithm is successful if it leaves at most m pairs to be compared in the second round. After Häggkvist and Hell [43] constructed an algorithm, Bollobás

and Thomason [19] found the correct order for the minimal value of m by showing that a random graph with $n^{3/2}\log n$ edges produces a succesful algorithm. Moreover a random graph with $n^{5/3}\log^{1/3} n$ edges produces a successful algorithm even if we allow only two step deductions between rounds (that is, we can deduce $a < b$ only if the first round yields $a < c$ and $c < b$ for some c). Once again, this is the correct order of magnitude. Known constructions for algorithms are less efficient. Alon [3] used eigenvalue methods to show that the bipartite graph whose vertex classes are the points and the hyperplanes of $\mathrm{AG}(d,q)$, adjacency in the graph reflecting incidence in the geometry, is $(n,x,n-n^{1+1/d}/x)$-expanding for all x. In the case $d=4$ it is straightforward to take such an expander and construct a two round sorting algorithm with two step deductions using only $(22/3+o(1))n^{3/4}$ edges, not far from optimal. The expanding properties of this graph can also be verified by the following analogue of Theorem 3.1 for bipartite graphs.

Theorem 5.6. *Let G be a bipartite graph with vertex classes X and Y, both of order n. Suppose each vertex in X has degree at least pn and that no two vertices of X have more than p^2n+l common neighbours. Then G is $(n,x,n-(lx+pn)/p^2x)$-expanding for all x.*

This allows the construction of many dense expanders to be verified. For example, the graph due to Brown [22] described in section 2 is $(n,x,n-6n^{1/2}-n^{4/3}/x)$-expanding for all x, and, as already mentioned, the graphs described in the previous paragraph are $(n,x,n-n^{1+1/d}/x)$-expanding for all x. The proof of the theorem can also be used to show the existence of a two round sorting algorithm with two step deductions using only $(3+o(1))n^{3/4}$ edges. Further details are given in [65].

Theorem 5.6 was used by Dyer and Frieze [27] along with Theorem 3.1 to develop a polynomial expected time algorithm for a minimum cut. The algorithm seeks to find the minimum number of edges in a cut which partitions the vertices into two equal-sized subsets. The graphs are uniformly distributed among those of order 2n which have a 'small cut', that is, a cut with at most $(\frac{1}{2}-\epsilon)e(G)$ edges for some fixed $\epsilon > 0$. The theorems above are needed to prove that the cut, once found, is indeed minimum.

6. Ramsey theory.

In this final section we examine some consequences of the previous work for ramsey theory. Recall Erdős' conjecture from section 1, that $c_t = 2^{1-\binom{t}{2}}$. This conjecture is trivially true for $t=2$, and for $t=3$ follows at once from a result of Goodman [38]. However this case is much easier than $t \geq 4$ since, as Lorden

[50] showed, the number of monochromatic triangles depends only on the degree sequence. For $t \geq 4$ very little is known, the only general result being due to Giraud [37] who showed that $c_4 > \frac{1}{46}$.

It turns out this conjecture is false. Recall the definition of $m \circ G$ from example (m) of section 3.

Lemma 6.1. $k_t(m \circ G) + k_t(\overline{m \circ G}) = \sigma_t(G) 2^{1-\binom{t}{2}} \binom{n}{t} (1 + o(1))$,

where $$\sigma_t(G) = 2^{\binom{t}{2}-1} p^{-t} \left\{ t! k_t(G) + \sum_{j=1}^{t} j! S(t,j) k_j(\overline{G}) \right\}.$$

Here G has order p, $n = mp = |m \circ G|$, and the $o(1)$ term is with p,t fixed and $m \to \infty$. $S(t,j)$ is a Stirling number of the second kind and represents the number of ways of partitioning t labelled objects into j non-empty parts.

A consequence of this lemma is that any graph G provides an upper bound for c_t, namely $c_t \leq 2^{1-\binom{t}{2}} \sigma_t(G)$. To find counterexamples to Erdős' conjecture we need graphs with $\sigma_t < 1$. These are by no means easy to find; certainly $\sigma_4(Q_n) > 1$ for the Paley graphs, as the calculation of $k_4(Q_n)$ cited in section 4 shows. But the graphs T_k^- from example (h) do the trick. The graph spanned by the neighbours of the zero vector in T_k^- is denoted P_k^-. The next results are from [63].

Theorem 6.2. $\sigma_4(P_4^-) < 0{\cdot}976$ *and* $\sigma_t(T_t^-) < 0{\cdot}936$ *for* $t \geq 5$.

Corollary 6.3. $c_t < 2^{1-\binom{t}{2}}$ *for* $t \geq 4$.

A modification of $2 \circ P_4^-$ can be used to show $c_4 < \frac{1}{33}$.

The failure of Erdős' conjecture is a considerable surprise, since it has always been thought that the best ramsey colourings for complete graphs were, roughly speaking, symmetric with respect to the two colours and such that the edges of any given colour were spread evenly through the graph. This is not true, in the following sense. Let us call a sequence $G_1, G_2, \ldots$ of graphs such that $|G_n| = n$ and $k_t(G_n) + k_t(\overline{G}_n) = c_t(n)\binom{n}{t}$ an *extremal sequence* for K_t. Clearly Corollary 6.3 means we cannot characterise the graphs of an extremal sequence as pseudo-random graphs, as we had once intended. But we can still uncover some properties of the extremal sequence. Theorem 4.8 shows that G_n is not itself $(\frac{1}{2}, o(n))$-jumbled, nor indeed can it contain an induced subgraph of order $n + o(n)$ which is $(\frac{1}{2}, o(n))$-jumbled. The remarks following Theorem 3.2 now have the following consequence.

Theorem 6.4. *Let $G_1, G_2, \ldots$ be an extremal sequence for K_t, and let η be a constant with $0 < \eta < 1$. Then there is a positive constant $\delta = \delta(\eta)$ such that G_n contains an induced subgraph H_n of order $\lfloor \eta n \rfloor$ with $\left| e(H) - \frac{1}{2}\binom{|H|}{2} \right| > \delta n^2$.*

In other words, the graphs of an extremal sequence contain large subgraphs with a significant bias towards one colour. Unfortunately this does not imply that the graphs themselves are biased toward one colour, since for example the complete bipartite graph $K_{n/2,n/2}$ contains large biased subgraphs.

These results have some bearing on the actual ramsey numbers for complete graphs. Székely defined the quantity

$$k(n) = \min\left\{ \sum_{t>0} k_t(G) + k_t(\overline{G}) \,;\ |G| = n \right\}$$

and showed that estimates for $k(n)$ could be used to estimate ramsey numbers, as follows. Let $r(G,H)$ denote the ramsey number which is the smallest value of n such that any colouring of the edges of K_n with red and blue yields a red G or a blue H. The number $r(G,G)$ is abbreviated $r(G)$. This coincides with our earlier definition of $r(K_t)$. The term $r(k,l)$ stands for $r(K_k, K_l)$. Székely's theorem gives lower bounds for ramsey numbers in terms of the function $k(n)$.

Theorem 6.5. (Székely, [58]) *Given $\epsilon > 0$ there is an n_0 such that if $n > n_0$ then*

$$\text{both} \quad n^{(1/2-\epsilon)s} \leq k(n) \leq \frac{1}{(k-2)!} r(k,2)r(k,3)\dots r(k,k-3)r(k,k-2)r(k,k)^2$$

$$\text{and} \quad n^{0.2275 \log n} \leq k(n) \leq n^{0.7214 \log n},$$

where $s = \max\{l; r(l,l) \leq \sqrt{n}\}$.

Another function for which we can obtain a better bound is the ramsey number $r(C_4, K_n)$, where C_4 is a 4-cycle. It is easily checked that no two vertices of the Erdős-Rényi graph have two common neighbours. This means first that the graph contains no C_4, and secondly that we can apply Theorem 3.1 with $p = n^{-1/2} + O(n^{-1})$ and $l < n^{-1/2}$. Thus the graph is $(n^{-1/2}, 2n^{3/4})$-jumbled, and so contains no independent set of order $4n^{3/4}$. In fact, as remarked after Theorem 3.1, the proof yields somewhat more, namely that the independence number is at most $n^{3/4} + n^{1/2}$.

Theorem 6.6. $r(C_4, K_n) > (1 + o(1))n^{4/3}$.

This result was also obtained by Alon [3], using his eigenvalue method.

We conclude with some remarks about the ramsey numbers $r(K_n)$ themselves. The usual proof of the existence of ramsey numbers involves a local argument, that is, it is based on a discussion on vertex degrees. In this paper we have been looking at how a more global approach might be fruitful. In this context it is interesting to note some recent work of Gyárfás, Lehel, Schelp and Tuza [41], extended

by Gyárfás, Lehel, Nešetřil, Rödl, Schelp and Tuza [42]. For a given graph G they define $r_k^{\text{loc}}(G)$ to be the smallest value of n for which any colouring of the edges of K_n with any number of colours yields a monochromatic G provided no more than k colours appear at any vertex. (Of course, the first thing they have to do is show that $r_k^{\text{loc}}(G)$ exists.) We will then want to compare $r_2^{\text{loc}}(K_t)$ with $r(K_t)$. In general $r_2^{\text{loc}}(G)/r(G)$ can be arbitrarily large, though it is shown in [41] that if G is connected then $r_2^{\text{loc}}(G)/r(G) < 3/2$. For complete graphs there is the following sharper result, in which the graph $K_m + \overline{K}_n$ consists of n vertices each joined to every vertex of a K_m.

Theorem 6.7. (Gyárfás, Lehel, Schelp and Tuza [41]) $r_2^{\text{loc}}(K_m + \overline{K}_n) = r(K_m + \overline{K}_n)$ *if* $m \geq n-1$.

In particular, $r(K_t)=r_2^{\text{loc}}(K_t)$. There are many other interesting comparisons and contrasts between local and global ramsey numbers contained in [41] and [42].

As for the ramsey number $r(K_m + \overline{K}_n)$, it was conjectured in [60] to be at most $2^m(m+n-2)+2$. This was backed up by a heuristic argument which *in vacuo* has some appeal but now appears hopeless, especially in view of the failure of Erdős' conjecture. The conjecture is true for $m = 1$ (trivially) and $m = 2$ (by Goodman's theorem, as is implicit in Walker [69]), but is indeed false for $m = 3$. It is shown in [66] that P_k^- contains no $K_3 + \overline{K}_n$ if $n > 4^{k-2}$.

Theorem 6.8. $r(K_3 + \overline{K}_n) \geq 8n + 2\sqrt{n-1} - 7$ *if* $n = 4^k + 1$.

We mentioned earlier that the extremal colourings for $r(K_3)$ and $r(K_4)$ were provided by Paley graphs, and most of the hitherto best known bounds for small ramsey numbers were derived from these graphs (though recently Mathon [53] has improved these bounds considerably with other constructions, as mentioned in section 3). The actual clique number $cl(Q_n)$ in a Paley graph is unknown if n is prime (though if n is a perfect square the clique number is $\sqrt{n}$). Of course it is at least as large as the smallest non-residue, which value is sometimes at least $\epsilon \log n \log\log n$ for some $\epsilon > 0$ (Montgomery [55] assuming the Riemann hypothesis for all L-functions of real characters). In order to improve the lower bound for $r(K_t)$ given by Theorem 1.1 it would be necessary to show that $cl(Q_n) < 2\log_2 n$ infinitely often. As for lower bounds on $cl(Q_n)$, the results of [9],[18] and [39], or Theorem 4.9, show that $cl(Q_n) > \frac{1}{2}\log_2 n$, though this follows from the fact that Q_n is self-complementary and $r(K_t) < 4^t$. Perhaps it would be possible to improve the methods of [9],[18] and [39] by replacing the estimates of Weil by the more recent estimates of Deligne (see Katz [47]), and so obtain $cl(Q_n) > \log_2 n$, but this would

be a formidable undertaking. However we have the following general result from [66].

Theorem 6.9. *Let G be a (p,α)-jumbled graph of order n. Then G contains $K_u + \overline{K}_w$, provided $w = \lceil p^u n - 2\alpha/(1-p)\rceil \geq 1$.*

If, in this theorem, G is such that $w \geq r(t-u,t)$, then G contains a monochromatic K_t. Use of the classical bound $r(k,l) < \binom{k+l-2}{k-1}$ due to Erdős and Szekeres [33] yields the next theorem, which in particular can be applied to Q_n.

Theorem 6.10. *Let $G_1, G_2, \ldots$ be a sequence of graphs in which G_n has order n and is $(p, O(\sqrt{n}))$-jumbled. Then $k_t(G_n) + k_t(\overline{G}_n) > 0$ if $t < \frac{5}{8}\log_2 n(1+o(1))$.*

This theorem means that if the extremal colourings for the ramsey number of K_t are pseudo-random then $r(K_t) < (3{\cdot}05)^t$. In general no upper bound of the form $r(K_t) < (4-\epsilon)^t$, for fixed ϵ, has been proved; the best is $r(K_t) < C\frac{\log\log t}{\log t}\binom{2t-2}{t-1}$ claimed by Yackel [71]. Now the Erdős-Szekeres bound derives from the inequality $r(k,l) \leq r(k-1,l) + r(k,l-1)$. An examination of this proof reveals that any extremal colouring for $r(k,l)$ on anything approaching $r(k-1,l)+r(k,l-1)$ vertices is jumbled. We can then apply Theorem 6.9 to show the existence of a red K_k or a blue K_l, so giving a better upper bound for $r(k,l)$. Certainly this approach gives some improvement over the classical result. At the time of writing, the following theorem at least seems quite likely. The details will be given in [66].

Theorem 6.11. *There is an absolute positive constant ϵ such that if $(1-\epsilon)k < l \leq k$ then $r(k,l) < (k+l)^{-\epsilon}\binom{k+l-2}{k-1}$.*

References

[1] M. Ajtai, J. Komlós and E. Szemerédi, Sorting in $C\log n$ parallel steps, *Combinatorica* **3**, 1–19.

[2] N. Alon, Eigenvalues and expanders, (preprint).

[3] N. Alon, Eigenvalues, geometric expanders, sorting in rounds and ramsey theory, (preprint).

[4] N. Alon, Z. Galil and V.D. Milman, Better expanders and superconcentrators, (preprint).

[5] N. Alon and V.D. Milman, Eigenvalues, expanders and superconcentrators, in 'Proc. 25th Annual Symp. on Foundations of Computer Science', Florida pp. 320–322.

[6] R. Ayoub, 'An introduction to the analytic theory of numbers', American Mathematical Society (1963).

[7] J.-C. Bermond and B. Bollobás, The diameter of graphs – a survey, in 'Proc. Twelfth Southeastern Conf. on Combinatorics, Graph Theory and Computing', *Congressus Numerantium* **32**, pp. 3–27.

[8] J.-C. Bermond, J. Bond, M. Paoli and C. Peyrat, Graphs and intercommunication networks: diameter and vulnerability, in 'Surveys in Combinatorics' (E.K. Lloyd, ed.) London Math. Soc. Lecture Notes **82** pp. 1–30.

[9] A. Blanchard, quoted by G. Giraud, Nouvelles majorations des nombres de Ramsey binaires-bicolores, *C.R. Acad. Sci. Paris Sér. A* **268** (1969), 5–7.

[10] M. Blum, R.M. Karp, O. Vornberger, C.H. Papadimitriou and M. Yannakakis, The complexity of testing whether a graph is a superconcentrator, *Infor. Process. Letters* **13** (1981), 164–167.

[11] B. Bollobás, 'Extremal Graph Theory', Academic Press, London (1978).

[12] B. Bollobás, 'Random Graphs', Academic Press, London (1985).

[13] B. Bollobás, Geodesics in oriented graphs, *Annals Discrete Math.* **20** (1984), 67–73.

[14] B. Bollobás and P. Catlin, Topological cliques of random graphs, *J. Combinatorial Theory Ser. B.* **30** (1981), 224–227.

[15] B. Bollobás, P. Catlin and P. Erdős, Hadwiger's conjecture is true for almost every graph, *European J. Combinatorics* **1** (1980), 195–199.

[16] B. Bollobás and P. Erdős, An extremal problem of graphs with diameter 2, *Math. Mag.* **48** (1975), 281–283.

[17] B. Bollobás and P. Erdős, Cliques in random graphs, *Math. Proc. Camb. Phil. Soc.* **80** (1976), 419–427.

[18] B. Bollobás and A. Thomason, Graphs which contain all small graphs, *European J. Combinatorics* **2** (1981), 13–15.

[19] B. Bollobás and A. Thomason, Parallel Sorting, *Discrete Appl. Math.* **6** (1983), 1–11.

[20] B. Bollobás and A. Thomason, Random graphs of small order, in 'Random Graphs', *Annals Discrete Math.* (1985), pp. 47–97.

[21] A.E. Brouwer, Some new two-weight codes and strongly regular graphs, *Discrete Applied Math.* **10** (1985), 111-114.

[22] W.G. Brown, On graphs that do not contain a Thomsen graph, *Canad. Math. Bull.* **9** (1966), 281–285.

[23] D.A. Burgess, On character sums and primitive roots, *Proc. London Math. Soc.* **12** (1962), 179–192.

[24] N. Calkin, personal communication.

[25] F.R.K. Chung, On concentrators, superconcentrators, generalizers and nonblocking networks, *Bell Syst. Tech. J.* **58** (1978), 1765-1777.

[26] V. Chvátal and P. Erdős, A note on hamiltonian circuits, *Discrete Math.* **2** (1972), 111-113.

[27] M.E. Dyer and A.M. Frieze, Fast solution of some random NP-hard problems (preprint).

[28] P. Erdős, Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.* **53** (1947), 292–294.

[29] P. Erdős, On the number of complete subgraphs contained in certain graphs, *Publ. Math. Inst. Hung. Acad. Sci., VII, Ser. A* **3** (1962), 459–464.

[30] P. Erdős and J.W. Moon, On subgraphs of the complete bipartite graph, *Canad. Math. Bull.* **7** (1964), 35–39.

[31] P. Erdős and A. Rényi, On a problem in graph theory, *Publ. Math. Inst. Hungar. Acad. Sci.* **7** (1962), 215–227 (in Hungarian).

[32] P. Erdős and J. Spencer, Imbalances in k-colorations, *Networks* **1** (1972), 379–385.

[33] P. Erdős and G. Szekeres, A combinatorial problem in geometry, *Compositio Math.* **2** (1935), 463–470.

[34] R.J. Evans, J.R. Pulham and J. Sheehan, On the number of complete subgraphs contained in certain graphs, *J. Combin. Theory Ser. B* **30** (1981), 364–371.

[35] P. Frankl and R.M. Wilson, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357–368.

[36] O. Gabber and Z. Galil, Explicit constructions of linear superconcentrators, *J. Comp. and Sys. Sci.* **22** (1981), 407–420.

[37] G. Giraud, Sur le problème de Goodman pour les quadrangles et la majoration des nombres de Ramsey, *J. Combin. Theory Ser. B* **27** (1979), 237–253.

[38] A.W. Goodman, On sets of acquaintances and strangers at any party, *Amer. Math. Monthly* **66** (1959), 778–783.

[39] R.L. Graham and J.H. Spencer, A constructive solution to a tournament problem, *Canad. Math. Bull.* **14** (1971), 45–48.

[40] G.R. Grimmett and C.J.H. McDiarmid, On colouring random graphs, *Math. Proc. Cambridge Phil. Soc.* **77** (1975), 313–324.

[41] A. Gyárfás, J. Lehel, R.H. Schelp and Zs. Tuza, Ramsey numbers for local colorings, (preprint).

[42] A. Gyárfás, J. Lehel, J. Nešetřil, V. Rödl, R.H. Schelp and Zs. Tuza, Local k-colorings of graphs and hypergraphs, (preprint).

[43] R. Häggkvist and P. Hell, Parallel sorting with constant time for comparisons, *SIAM J. Comput.* **10** (1981), 465–472.

[44] J. Haviland and A. Thomason, Pseudo-random hypergraphs (to appear).

[45] X.L. Hubaut, Strongly regular graphs, *Discrete Math.* **13** (1975), 357–381.

[46] Sh. Jimbo and A. Maruoka, Expanders obtained from affine transformations, in 'Proc. 17th Annual ACM Symp. on Theory of Computing' (1985), pp. 88–97.

[47] N.M. Katz, 'Sommes exponentielles', *astérisque* **79**, Société Mathématique de France (1980).

[48] A. Kostochka, A lower bound for the Hadwiger number of graphs by their average degree, *Combinatorica* **4** (1984), 307–316.

[49] P. Kövári, V.T. Sós and P. Turán, On a problem of K. Zarankiewicz, *Colloq. Mat.* **3** (1954), 50–57.

[50] G. Lorden, Blue-empty chromatic graphs, *Amer. Math. Monthly* **69** (1962), 114–120.

[51] W. Mader, Homomorphiesätze für Graphen, *Math. Ann.* **178** (1968), 154–168.

[52] G.A. Margulis, Explicit constructions of concentrators, *Problemy Peredachi Informatsii* **9**(4) (1973), 71–80 (in Russian). English translation in *Problems Info. Transmission*, Plenum Press (1975), 325–332.

[53] R. Mathon, Lower bounds for ramsey numbers and assosciation schemes, *J. Combinatorial Theory, Ser. B* **42** (1987), 122–127.

[54] D.W. Matula, On the complete subgraph of a random graph, in 'Combinatory Mathematics and its Applications', Chapel Hill, N.C., pp. 356–369.

[55] H.L. Montgomery, Topics in multiplicative number theory. *Lecture Notes in Mathematics* **227**, Springer-Verlag (1971).

[56] R.G.E. Pinch, A sequence well distributed in the square, *Math. Proc. Cambridge Phil. Soc.* **99** (1986), 19–22.

[57] J.J. Seidel, A survey of two-graphs, in 'Colloquio Internazionale sulle Teorie Combinatorie', Atti dei Convegni Lincei **17**, Accad. Naz. Lincei, Roma (1976), pp. 481–511.

[58] L.A. Székely, On the number of homogeneous subgraphs of a graph, *Combinatorica* **4** (1984), 363–372.

[59] R.M. Tanner, Explicit construction of concentrators from generalized N-gons, *SIAM J. Alg. Discr. Meth.* **5** (1985), 287–293.

[60] A. Thomason, On finite ramsey numbers, *European J. Combinatorics* **3** (1982), 263–273.

[61] A. Thomason, An extremal function for contractions of graphs, *Math. Proc. Cambridge Phil. Soc.* **95** (1984), 261–265.

[62] A. Thomason, Pseudo-random graphs, in 'Proceedings of Random Graphs, Poznań 1985', (M. Karonski, ed.) *Annals of Discrete Math.* (1987).

[63] A. Thomason, A disproof of a conjecture of Erdős in ramsey theory, (submitted)

[64] A. Thomason, A linear expected time hamilton cycle algorithm, (submitted).

[65] A. Thomason, Dense expanders, (to appear).

[66] A. Thomason, Upper bounds for ramsey numbers, (to appear).

[67] L.G. Valiant, Graph theoretic properties in computational complexity, *J. Comp. and Sys. Sci.* **13** (1976), 278–285.

[68] W.F. de la Vega, On the maximum density of graphs which have no subcontraction to K^s, *Discrete Math.* **46** (1983), 109–110.

[69] K. Walker, Dichromatic graphs and ramsey numbers, *J. Combinatorial Theory* **5** (1968), 238–243.

[70] A. Weil, Sur les courbes algébrique et les variétés qui s'en déduisent, *Actualités Sci. Ind. No. 1041* (1948).

[71] J. Yackel, Inequalities and asymptotic bounds for ramsey numbers, *J. Combinatorial Theory Ser. B* **13** (1972), 56–68.

[72] Š. Znám, On a combinatorial problem of K. Zarankiewicz, *Colloq. Math.* **11** (1963), 81–84.