The Random Graph Revisited

Peter J. Cameron

Abstract. The random graph, or Rado's graph (the unique countable homogeneous graph) has made an appearance in many parts of mathematics since its first occurrences in the early 1960s. In this paper I will discuss some old and new results on this remarkable structure.

1. The Random Graph

Consider the following two countably infinite graphs.

For the first graph, take any countable model of the Zermelo-Fraenkel axioms for set theory. (The existence of such models, the so-called *Skolem paradox*, follows from the downward Löwenheim-Skolem theorem of first-order logic.) Abstractly, this is a countable set with an asymmetric membership relation. Now form an undirected graph by symmetrising the relation; that is, x and y are adjacent (written $x \sim y$) if either $x \in y$ or $y \in x$.

For the second graph, the vertices are the primes congruent to 1 mod 4. Let $p \sim q$ hold if p is a quadratic residue mod q. By the law of quadratic reciprocity, this relation is already symmetric.

Remarkably, these two graphs are isomorphic.

To see this, we first note that each of them has the following property: if U and V are finite disjoint sets of vertices, then there exists a vertex z such that $u \sim z$ for all $u \in U$, while $v \not\sim z$ for all $v \in V$. (We write $v \not\sim z$ to indicate that v and z are not adjacent.) In the first graph, this property is demonstrated using the Pairing, Union, and Foundation axioms. In the second graph, the proof uses the Chinese Remainder Theorem and Dirichlet's Theorem on primes in arithmetic progression.

This property of a graph G can be stated another way. If A and B are finite graphs with A an induced subgraph of B, then every embedding of A into G extends to an embedding of B into G. The stated property asserts this when $|B| = |A|+1$, and the general case follows by induction. We call this the *I-property*, because it is a form of injectivity.

Now any two countable graphs having the I-property are isomorphic. This is a standard application of the *back-and-forth* technique from model theory. If G_1 and G_2 are countable graphs with the I-property, we build successively larger finite partial isomorphisms between them by going alternately from G_1 to G_2 and from G_2 to G_1; the result after countably many steps is an isomorphism.

The argument shows more. If we take $G_1 = G_2 = G$, and begin with a given finite partial isomorphism, we see that *every isomorphism between finite subgraphs of G extends to an automorphism of G*. We call a graph with this property *homogeneous*; we have shown that a graph with the I-property is homogeneous. The converse also holds, provided that we formulate the I-property correctly: we require that the two finite graphs A and B must belong to the *age* of G, the class of all finite graphs embeddable in G.

So the two graphs with which we started this section, despite appearances, are isomorphic, and are homogeneous, although no symmetries are visible to the casual observer.

There are several more features of this story. First, Fraïssé [11] showed that two countable homogeneous graphs with the same age are isomorphic (essentially by the argument given above); he also characterised the ages of homogeneous graphs. They are the classes of finite graphs which are closed under isomorphism, closed under taking induced subgraphs, and have the *amalgamation property.* (This asserts that, if two members of the age have isomorphic induced subgraphs, then they can be embedded in another graph in the class in such a way that the isomorphism becomes equality.) If these conditions are satisfied by the class $\mathcal{C}$ of finite graphs, then the unique countable homogeneous graph G whose age is $\mathcal{C}$ is called the *Fraïssé limit* of $\mathcal{C}$.

Subsequently, all the countable homogeneous graphs were determined by Lachlan and Woodrow [18]:

Theorem 1.1. *The countably infinite homogeneous graphs are the following:*

(a) *the disjoint union of m complete graphs of size n, where m and n are finite or countable (and at least one is infinite);*
(b) *the complements of the graphs under (a);*
(c) *the Fraïssé limit of the class of graphs containing no complete subgraph of size r, for given finite $r \geq 3$;*
(d) *the complements of the graphs under (c);*
(e) *the Fraïssé limit of the class of all finite graphs.*

The graphs in case (c) were first constructed and studied by Henson [12]. The unique graph under (e) is the one with which we began this section. It is called the *random graph* (for reasons which will shortly appear) or *Rado's graph* (since the first explicit construction of it was given by Rado [19]).

We digress to give Rado's construction. Let us first define an asymmetric relation $\to$ on the set of non-negative integers by the rule that $x \to y$ if the xth digit in the base-2 expression of y is 1 (that is, when y is written as a sum of distinct powers of 2, then 2^x is one of these powers). Now the symmetrised form of $\to$ defines a graph on $\mathbb{N}$ which is the graph R. For the relation $\to$ just defined is a model of the Zermelo-Fraenkel axioms (including the Axiom of Choice) except for the Axiom of Infinity: every finite set X of natural numbers is represented by the single natural number $y = \sum_{x \in X} 2^x$, and $x \to y$ if and only if $x \in X$. Now the Axiom of Infinity was not used in our proof that the symmetrised membership relation defines the graph R.

Fraïssé also observed that there is nothing special about graphs: the relation between homogeneity, the I-property, and the amalgamation property holds for arbitrary relational structures. (We need to include one extra condition in the statement of Fraïssé's Theorem in general, namely that there are only countably many structures in the class $\mathcal{C}$, up to isomorphism. This is to rule out the possibility of, for example, infinitely many unary relations, any subset of which might hold on a particular element of the domain; by Cantor's Theorem, a countable set does not contain enough elements for all possibilities to be realised.)

The homogeneous relational structures of various types have been determined by various authors: partially ordered sets by Schmerl [20]; tournaments by Lachlan [17], simplified by Cherlin [7]; directed graphs by Cherlin [8]. Remarkably, there are only three countable homogeneous tournaments: the linear order $\mathbb{Q}$; the *circular tournament*, otherwise known as the *local order* or *locally transitive tournament*, and has arisen in diverse areas such as permuutation groups [4] and computer science [16]; and the analogue of R, the *random tournament*, which admits a construction similar to our second construction of the random graph, but using primes congruent to -1 mod 4 instead. On the other hand, there are uncountably many countable homogeneous directed graphs (this had been pointed out earlier by Henson [13]).

There is no need to stick to relational structures. The argument essentially extends to all lofally finite first-order structures, and even beyond this class with care. For a recent treatment of these ideas in group theory, see Higman and Scott [14].

Finally, we come to the reason for the term *random graph*. We use the simplest possible model for the random graph on a given finite or countable vertex set: we decide, with probability 1/2, whether a given pair of vertices is an edge or a non-edge, independently of all other choices. If the vertex set is finite, then every possible graph occurs, with probability inversely proportional to the order of its automorhism group; indeed, graphs with no symmetry at all predominate. On the other hand, Erdős and Rényi [9] showed the following:

Theorem 1.2. *There is a countable graph R such that, with probability* 1*, the random graph on a countable vertex set is isomorphic to R.*

Of course, R is the graph we met above, the Fraïssé limit of the class of all finite graphs. The proof is simple: we have to show that the I-property holds with probability 1. SInce the union of countably many null sets is null, and there are only countably many pairs of finite disjoint sets of vertices, it suffices to show that, for given finite disoint sets U and V, the probability that no vertex z with the correct joins exists is zero.

But the probability that a given vertex z is not correctly joined is $(1 - 1/2^n)$, where $n = |U \cup V|$; by independence, the probability that no vertex is correctly joined is

$$\lim_{k\to\infty}(1-1/2^n)^k = 0\,.$$

The result of Erdős and Rényi was described, in their account of it by Erdős and Spencer [10], as demolising the theory of countable random graphs. In its place, we have the theory of *the* countable random graph! A survey of some of the remarkable properties of R and their generalisations to other classes of structures is given in [5]. In the remainder of this paper, some recent results will be mentioned.

2. The Pigeonhole Property

If a countably infinite set is partitioned into two parts, then at least one of the two is countable, and hence is isomorphic to the original set. We say that a structure has the *pigeonhole property* if, whenever it is partitioned into two parts, one of the parts is isomorphic to the original structure.

Theorem 2.1. *The only countable graphs with the pigeonhole property are the complete and null graphs and the random graph.*

For the proof, see [5]. The proof that the random graph has the pigeonhole property is very short, and goes as follows. Suppose that it has a partition such that neither of the two parts X_1 and X_2 is isomorphic to R. Then there exist finite disjoint subsets U_i and V_i of X_i such that no vertex of X_i is joined to all vertices in U_i and none in V_i, for $i = 1, 2$. But then no vertex of R is joined to all vertices in $U_! \cup U_2$ and to none in $V_1 \cup V_2$, a contradiction.

This remarkable characterisation of R suggests either weakening the definition of the pigeonhole property or considering other classes of structures. The first approach ahs not yielded much yet. I merely pose a question:

> Which countable graphs G have the property that, whenever G is partitioned into two parts, one of the parts has an induced subgraph isomorphic to G?

More is known about the second case. Bonato and Delic [2, 3] determined the tournaments with the pigeonhole property. Note that there are no complete or null tournaments.

Theorem 2.2. *Let T be a countable tournament with the pigeonhole property. Then either*

(a) *T or its converse is an ordinal power of ω; or*
(b) *T is the random tournament.*

Some results are known about more general binary relations such as directed graphs, but there is not yet a complete classification of these.

3. Automorphism Groups

The random graph R is homogeneous. Hence, its automorphism group $\mathrm{Aut}(R)$ is transitive on finite subgraphs of any given isomorphism type; in particlar, it is transitive on vertices, edges, and non-edges, and so is a primitive permutation group of rank 3 on vertices.

A number of properties of this group are known:

(a) It has cardinality $2^{\aleph_0}$.
(b) It is simple [21].
(c) It has the strong small index property (see below) [15].

A permutation group on a countable set X is said to have the *small index property* if every subgroup of index less than $2^{\aleph_0}$ contains the pointwise stabiliser of a finite set; it has the *strong small index property* if every such subgroup lies between the pointwise and setwise stabilisers of a finite set.

Truss [21] found all the cycle structures of automorphisms of R. In particular, R has cyclic automorphisms. The easiest way to see this is as follows. Choose a set S of positive integers independently at random. Construct a graph $\Gamma(S)$ with vertex set $\mathbb{Z}$ by joining x and y if and only if $|x - y| \in S$. The resulting graph admits the cyclic shift $x \mapsto x + 1$ as an automorphism; and, with probability 1, it is isomorphic to R. Similarly it follows from Truss's classification that R admits an automorphism with one fixed vertex v and two infinite cycles (necessarily the neighbours and the non-neighbours of v).

Bhattacharjee and Machperson [1] settled a question of Peter Neumann by the following remarkable combination of the two types of automorphisms just described.

Theorem 3.1. *There exist automorphisms f, g of R such that*

(a) *f, g generate a free subgroup of* $\mathrm{Aut}(R)$,
(b) *f has a single cycle on R, which is infinite,*
(c) *g fixes a vertex v and has two cycles on the remaining vertices (namely, the neighbours and non-neighbours of v),*
(d) *the group $\langle f, g\rangle$ is oligomorphic, and transitive on vertices, edges, and non-edges of R, and each of its non-identity elements has only finitely many cycles on R.*

The existence of cyclic auutomorphisms of R shows that in fact it is a Cayley graph for the infinite cyclic group. Cameron and Johnson [6] generalised this as follows.

Theorem 3.2. *Let G be a countable group which cannot be expressed as the union of finitely many translates of square-root sets of non-identity elements. Then, with probability* 1, *a random Cayley graph for G is isomorphic to R.*

Here, the *square-root set* of an element g is $\{x : x^2 = g\}$.

Wielandt called a group G a *B-group* if every primitive permutation group containing the regular representation of R is doubly transitive. The B stands for

Burnside, who gave the first examples: the finite cyclic groups of prime-power (non-prime) order. In fact, it follows from the Classification of Finite Simple Groups that, for almost all n (that is, all but a set of density zero), every group of order n is a B-group. (However, the finite non-B-groups have not been determined.) In the infinite case, things are very different: *no countable B-group is known*, although many groups are known not to be B-groups.

It follows from the above theorem of Cameron and Johnson that, if a countable group G is not the union of finitely many translates of square-root sets of non-identity elements, then G is not a B-group; for it is a regular subgroup of the primitive but not doubly transitive group $\mathrm{Aut}(R)$. Other countable homogeneous structures have been examined in the hope of finding further non-B-groups, but this has not been successful. (Note however that the above result does not exhaust the list of groups which are not B-groups. For example, any group which is the direct product of two countable subgroups is a non-B-group, since it is contained in the primitive group $S_\omega \wr S_2$ (in its product action).) The two results together show that no countable abelian group is a B-group. For let G be a countable abelian group. If the subgroup A_2 of involutions has infinite index in A, then A satisfies the hypotheses of the Cameron-Johnson theorem. If not, it has finite exponent, and so is a direct product of two infinite factors.

I mention an unsolved problem arising from the search for regular groups of automorphisms of countable structures. Recall Henson's construction [12] of countable homogeneous graphs H_r, where H_r is the Fraïssé limit of the class of finite graphs containing no complete subgraph of size r. Henson showed in that paper that H_3 has cyclic automorphisms but H_r does not for $r \geq 4$. His argument in fact shows more:

Theorem 3.3. *For $r \geq 4$, H_r is not a normal Cayley graph of any countable group.*

A Cayley graph for G is *normal* if it admits both left and right translation by G, in other words, if the set of neighbours of the identity is a normal subset. Now we can pose the open problem: *Is the Henson graph H_r for $r \geq 4$ a Cayley graph?*

References

[1] M. Bhattacharjee and H. D. Macpherson, Strange permutation representations of free groups, *J. Austral. Math. Soc.*, to appear.

[2] A. Bonato and D. Delic, A pigeonhole property for relational structures, *Mathematical Logic Quarterly* **45** (1999), 409–413.

[3] A. Bonato and D. Delic, Tournaments and orders with the pigeonhole property, *Canad. Math. Bull.*, to appear.

[4] P. J. Cameron, Orbits of permutation groups on unordered sets, II, *J. London Math. Soc.* (2) **23** (1981), 249–265.

[5] P. J. Cameron, The random graph, pp. 331–351 in *The Mathematics of Paul Erdős*, (J. Nešetřil and R. L. Graham, eds.), Springer, Berlin, 1996.

[6] P. J. Cameron and K. W. Johnson, An essay on countable B-groups, *Math. Proc. Cambridge Philos. Soc.* **102** (1987), 223–232.

[7] G. Cherlin, Homogeneous tournaments revisited, *Geometriae Dedicata* **26** (1988), 231–239.

[8] G. Cherlin, The classification of countable homogeneous directed graphs and countable homogeneous n-tournaments, *Memoirs Amer. Math. Soc.* **621**, American Mathematical Society, Providence, RI, 1998.

[9] P. Erdős and A. Rényi, Asymmetric graphs, *Acta Math. Acad. Sci. Hungar.* **14** (1963), 295–315.

[10] P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, New York/Akad. Kiadó, Budapest, 1974.

[11] R. Fraïssé, Sur certains relations qui généralisent l'ordre des nombres rationnels, *C. R. Acad. Sci. Paris* **237** (1953), 540–542.

[12] C. W. Henson, A family of countable homogeneous graphs, *Pacific J. Math.* **38** (1971), 69–83.

[13] C. W. Henson, Countable homogeneous relational structures and $\aleph_0$-categorical theories, *J. Symbolic Logic* **37** (1972), 494–500.

[14] G. Higman and E. A. Scott, *Existentially Closed Groups*, Oxford University Press, Oxford, 1988.

[15] W. A. Hodges, I. M. Hodkinson, D. Lascar and S. Shelah, The small index property for ω-stable, ω-categorical structures and for the random graph, *J. London Math. Soc.* (2) **48** (1993), 204–218.

[16] D. E. Knuth, *Axioms and Hulls*, Lecture Notes in Computer Science **606**, Springer, Berlin, 1992.

[17] A. H. Lachlan, Countable homogeneous tournaments, *Trans. Amer. Math. Soc.* **284** (1984), 431–461.

[18] A. H. Lachlan and R. E. Woodrow, Countable ultrahomogeneous undirected graphs, *Trans. Amer. Math. Soc.* **262** (1980), 51–94.

[19] R. Rado, Universal graphs and universal functions, *Acta Arith.* **9** (1964), 331–340.

[20] J. H. Schmerl, Countable homogeneous partially ordered sets, *Algebra Universalis* **9** (1979), 317–321.

[21] J. K. Truss, The group of the countable universal graph, *Math. Proc. Cambridge Philos. Soc.* **98** (1985), 213–245.

School of Mathematical Sciences,
Queen Mary and Westfield College,
London E1 4NS, U.K.
E-mail address: `p.j.cameron@qmw.ac.uk`