

# The Countable Random Graph

Michael Watson

March 14th, 2015

## Abstract

In this paper, we give a probabilistic existence proof of the countable random graph  $R$  and discuss some of its graph theoretic properties. A more constructive existence proof will also be given. We will see that the graph is *indestructible*, in that a finite number of changes to its vertices or edge set result in a graph isomorphic to  $R$ . Furthermore, we will explore the automorphism group of  $R$ , and will show that this group is simple and has cardinality  $2^{\aleph_0}$ .

## 1 Introduction

We will introduce the concept of a countable random graph, and show that there is such a graph  $R$  which is unique up to isomorphism. First, a probabilistic existence proof is given, followed by a more constructive proof. Property (\*), as defined below, is fundamental to the existence proof, and later we will be interested in showing that certain graphs satisfy this property. If property (\*) is satisfied in these graphs, this is enough to show that our graph in question is isomorphic to the unique graph  $R$ .

**Definition 1.** *A countable random graph is a simple graph with countably many vertices, where we choose the edges independently and with probability  $\frac{1}{2}$  for each pair of vertices.*

**Theorem 1.** *There exists a graph  $R$  with the following property: If we select a countable graph at random, by selecting the edges independently with probability  $1/2$ , then with probability 1, this graph is isomorphic to  $R$ .*

It seems unintuitive that a graph that is chosen at random has a predictable outcome. Before we explore the proof, we define the following property:

- (\*) Given finitely many vertices  $u_1, \dots, u_m, v_1, \dots, v_n$ , there exists a vertex  $z$  which is adjacent to  $u_1, \dots, u_m$ , but not adjacent to any of  $v_1, \dots, v_n$ .

In the future, we will say that a vertex  $z$  satisfying property (\*) is "correctly joined". The proof of this theorem will follow from two facts:

**Fact 1.** *With probability 1, a countable random graph satisfies (\*).*

**Fact 2.** *Any two countable graphs satisfying (\*) are isomorphic.*

*Proof of Fact 1.* Our goal is to show that the probability that a countably random graph fails to satisfy property (\*) is 0. Or equivalently, we must show that the set of all random graphs not satisfying (\*) is null. This proof will follow from an elementary result from measure theory: the countable union of null sets is null. There are countably many ways to choose integers  $m$  and  $n$ , and so countably many ways to choose our vertices  $u_1, \dots, u_m, v_1, \dots, v_n$ . Now let  $z_1, z_2, \dots, z_N$  be a set of vertices distinct from  $u_1, \dots, v_n$ . The probability that any one of these vertices is not correctly joined is  $1 - \frac{1}{2^{m+n}}$ . Since the probability of being correctly joined is independent of our choices of  $z_i$ , then the probability that none of these vertices is correctly joined is  $(1 - \frac{1}{2^{m+n}})^N$ . As  $N$  tends to infinity, this probability tends to 0. Therefore almost surely (with probability 1), a countable random graph satisfies (\*). □

*Proof of Fact 2.* Let  $G_1$  and  $G_2$  be two countable graphs satisfying property (\*). We must show these graphs are isomorphic. We start with an isomorphism  $\varphi$  which maps a finite set of vertices  $\{x_1, \dots, x_n\} \subset G_1$  into a finite set of vertices in  $G_2$ . We must extend  $\varphi$  to incorporate a new point,  $x_{n+1}$ . Let  $U$  be the set of neighbors of  $x_{n+1}$  within  $\{x_1, \dots, x_n\}$ , and let  $V = \{x_1, \dots, x_n\} \setminus U$ . The potential image  $\varphi(x_{n+1})$  must be adjacent to the images of  $U$ , and nonadjacent to the images of  $V$ . Fact 1 guarantees that there exists some such vertex which is correctly joined in this sense.

Now we must construct an isomorphism between  $G_1$  and  $G_2$ . Enumerate the vertices of  $G_1$  and  $G_2$  as  $\{x_1, x_2, \dots\}$  and  $\{y_1, y_2, \dots\}$ , respectively. Start with  $\varphi_0 = \emptyset$ . Now suppose that  $\varphi_n$  has been constructed. If  $n$  is even, then pick the smallest index  $m$  such that  $x_m$  is not in the domain of  $\varphi_n$ , and extend  $\varphi_n$  to  $\varphi_{n+1}$  which has  $x_m$  in its domain. If  $n$  is odd, then we work backwards. Pick the smallest indexed element  $y_m$  in  $G_2$  which is not in the image of  $\varphi_n$ . Since  $G_1$  satisfies property (\*), we extend our map  $\varphi_n$  to  $\varphi_{n+1}$  which has  $y_m$  in its image. We continue this back and forth method, and take  $\varphi$  to be the union of these maps. Then  $\varphi$  gives the desired isomorphism  $G_1 \cong G_2$ . □

So far, we have only given a non-constructive existence proof of  $R$ . Therefore, it may be desirable to have an explicit construction of  $R$ . The following theorem can be attributed to Cameron [1] and his students.

**Theorem 2.** *The following construction produces a countable graph  $R$  with property (\*). Let the vertices of  $R$  be enumerated by  $v_0, v_1, \dots$ . Consider the (unique) triadic representation of  $j$ :*

$$j = \sum_{k=0}^{n-1} a_k 3^k \text{ with } a_k \in \{0, 1, 2\} \forall k \text{ and } a_{n-1} \neq 0.$$

*Then the vertex  $v_j$  is joined exactly to those  $v_i$  with  $i < j$  for which  $a_i = 1$  in the above representation.*

*Proof.* We give an algorithm for constructing  $R$  which shows that it satisfies property  $(*)$ . Then the above formula is verified. The graph  $R$  is determined if we specify, for each vertex, to which of the vertices of lower index it is joined. The algorithm produces  $R$  inductively. There is no information needed for  $v_0$ . So we have already one vertex. Now we add new vertices (with certain edges to the vertices with lower index), such that the property  $(*)$  is satisfied for  $U$  and  $V$ , which are subsets of  $\{0, 1, 2, \dots, n-1\}$  where  $n$  runs inductively through the natural numbers. To enumerate all possibilities of choosing  $U$  and  $V$  disjoint in  $\{0, 1, \dots, n-1\}$  we look at the triadic representations  $(a_{n-1}, a_{n-2}, \dots, a_1, a_0)$  of the  $2 * 3^{n-1}$  numbers from  $3^{n-1}$  to  $3^n - 1$ , which all start with 1 or 2.  $a_i = 1$  in this representation means that  $i \in U$ ,  $a_i = 2$  means  $i \in V$  and  $a_i = 0$  means that  $i$  is not in  $U$  or  $V$ . We only need those configurations where  $n-1$  lies in  $U$  or  $V$ . For  $k$  running through these numbers, we add a new vertex, joined to exactly those vertices  $v_i$  for which  $a_i = 1$ . So the property  $(*)$  is satisfied for  $U$  and  $V$  in  $\{0, 1, 2, \dots, n-1\}$ . As  $n$  grows arbitrarily large, the property  $(*)$  is satisfied in  $R$ , because every  $(U, V)$  of disjoint finite subsets of the natural numbers is contained in some  $\{0, 1, 2, \dots, n-1\}$ .

This algorithm produces exactly the graph which is described in the above formula, because if  $j = \sum_{k=0}^{n-1} a_k 3^k$  with  $a_k \in \{0, 1, 2\}$  and  $a_{n-1} \neq 0$  the algorithm describes the edges from  $v_j$  to  $v_i$  with  $i < j$  exactly in the  $n$ th step, when we look at the triadic representation of  $j$ .  $\square$

## 2 A construction

**Theorem 3.** *Let  $M$  be a countable model of set theory. Define a graph  $M^*$  by the rule that  $x \sim y$  if and only if either  $x \in y$  or  $y \in x$ . Then  $M^*$  is isomorphic to  $R$ .*

*Proof.* Let  $u_1, \dots, u_m, v_1, \dots, v_n$  be distinct elements of  $M$ . Let  $x = \{v_1, \dots, v_n\}$  and  $z = \{u_1, \dots, u_m, x\}$ . We claim that  $z$  is a witness to condition  $(*)$ . Clearly  $u_i \sim z$  for all  $i$ . Suppose that  $v_j \sim z$ . If  $v_j \in z$ , then either  $v_j = u_i$  (contradicting our assumption), or  $v_j = x$  (thus  $x \in x$ , contradicting the Axiom of Foundation). If  $z \in v_j$ , then  $x \in z \in v_j \in x$ , again contradicting the Axiom of Foundation.  $\square$

A set  $S$  of positive integers is called universal if, given  $k \in \mathbb{N}$  and  $T \subseteq \{1, \dots, k\}$ , there is an integer  $N$  such that, for  $i = 1, \dots, k$ ,

$$N + i \in S \text{ if and only if } i \in T.$$

We will later be interested in binary sequences instead of sets. There is a bijection, under which the sequence  $\sigma$  and the set  $S$  correspond when  $(\sigma_i = 1) \Leftrightarrow (i \in S)$ .

Now let  $S$  be a universal set. Let  $G$  be a graph, and let its vertex set be  $\mathbb{Z}$ . Let vertices  $x$  and  $y$  be adjacent if and only if  $|x - y| \in S$ . We claim that this graph is then isomorphic to  $R$ . We must verify that property  $(*)$  holds. So, let  $u_1, \dots, u_m, v_1, \dots, v_n$  be distinct integers. Define  $l$  and  $g$  to be the least and

greatest of these integers. Let  $k = g - l + 1$  and  $T = \{u_i - l + 1 : i = 1, \dots, m\}$ . Now we can choose an integer  $N$ , by the definition of universality, such that  $z = l - 1 - N$ . Then  $z$  is witness to property (\*).

**Definition 2.** A binary sequence  $\sigma$  is universal if and only if it contains every finite binary sequence as a consecutive subsequence.

### 3 Universality

One of the most important properties of the infinite random graph  $R$  is that it is *universal*:

**Proposition 1.** Every finite or countable graph can be embedded as an induced subgraph of  $R$ .

*Proof.* This proof is almost identical to the proof of Fact 2, except that instead of constructing our map in a back-and-forth manner, we need only go forwards. That is, property (\*) only needs to hold in the target graph.

Let a graph  $G$  have vertex set  $\{x_1, x_2, \dots\}$ . Now suppose that we already have an isomorphism of induced subgraphs,  $\varphi_n : \{x_1, x_2, \dots, x_n\} \rightarrow R$ . Let  $U$  and  $V$  be the sets of neighbors and non-neighbors, respectively, in the set  $\{x_1, \dots, x_n\}$ . Then define  $\varphi_{n+1}(x_{n+1})$  to be the vertex in  $R$  that is adjacent to every vertex in  $\varphi_n(U)$ , and not adjacent to every vertex in  $\varphi_n(V)$ . Take  $\varphi = \bigcup(\varphi_n)$ . Then  $\varphi$  gives us the desired embedding.  $\square$

**Proposition 2.** A countable graph  $G$  is isomorphic to a spanning subgraph of  $R$  if and only if, given any finite set  $\{v_1, \dots, v_n\}$  of vertices in  $G$ , there is a vertex  $z$  joined to none of  $v_1, \dots, v_n$ .

*Proof.* We use the back-and-forth method to construct our desired isomorphism, but when going backwards, we only require that nonadjacencies be preserved.  $\square$

### 4 Indestructibility

The Graph  $R$  has some amazing properties. If we make a finite number of changes to  $R$ , our result is still isomorphic to  $R$ . We shall start this discussion with the following proposition.

**Proposition 3.** Let  $u_1, \dots, u_m, v_1, \dots, v_n$  be distinct vertices of  $R$ . Then the set  $Z = \{z : z \sim u_i \text{ for } i \in \{1, \dots, m\}; z \not\sim v_j, \text{ for } j \in \{1, \dots, n\}\}$  is infinite, and the induced subgraph on this set is isomorphic to  $R$ .

*Proof.* It is sufficient to verify that property (\*) holds in  $Z$ . Let  $u'_1, \dots, u'_l, v'_1, \dots, v'_k$  be distinct vertices of  $Z$ . Then there exists a vertex  $z$  adjacent to  $u_1, \dots, u_m, u'_1, \dots, u'_l$  and nonadjacent to  $v_1, \dots, v_n, v'_1, \dots, v'_k$ . Thus  $Z$  satisfies property (\*).  $\square$

We define the operation of *switching* a graph with respect to a set  $X$  of vertices as follows: every edge in  $X$  becomes a non-edge in our new graph, and every non-edge in  $X$  will become an edge. We leave fixed all of the edges and non-edges that do not correspond to vertices in  $X$ . Now we are able to prove the *indestructibility* of  $R$ .

**Proposition 4.** *The result of any of the following operations on  $R$  is isomorphic to  $R$ :*

- (a) *deleting a finite number of vertices;*
- (b) *changing a finite number of edges to non-edges or vice-versa;*
- (c) *switching with respect to a finite set of vertices.*

*Proof.* Part (a) follows from proposition 3 if we take our set  $Z$  to be the vertices that are not adjacent to those that have been deleted. Part (b) follows similarly. In case (c), suppose we perform a switching operation with respect to a set  $X$ . Let  $U = \{u_1, \dots, u_m\}$ ,  $V = \{v_1, \dots, v_n\}$ ; then we can find a vertex outside of  $X$  which is adjacent to  $U \setminus X$  and  $V \cap X$ , and non-adjacent to  $U \cap X$  and  $V \setminus X$ .  $\square$

Now we see that every graph obtained from  $R$  by switching is isomorphic to  $R$ . If we were to switch with respect to the neighbors of a vertex  $v$ , then  $v$  is an isolated point in our new graph. If we delete  $v$ , then our result is again isomorphic to  $R$ .

$R$  satisfies the *pigeonhole principle*:

**Proposition 5.** *If the vertex set of  $R$  is partitioned into a finite number of parts, then the induced subgraph on one of these parts is isomorphic to  $R$ .*

*Proof.* Suppose that the conclusion is false for partition  $X_1 \cup \dots \cup X_k$  of the vertex set. Then, for each  $i$ , property (\*) fails in  $X_i$ , so there are finite disjoint subsets  $U_i, V_i$  of  $X_i$  such that no vertex of  $X_i$  is "correctly joined" to all vertices of  $U_i$  and to none of  $V_i$ . Setting  $U = U_1 \cup \dots \cup U_k$  and  $V = V_1 \cup \dots \cup V_k$ , we find that condition (\*) fails in  $R$  for the sets  $U$  and  $V$ , a contradiction.  $\square$

**Proposition 6.** *The only countable graphs  $G$  which have the property that, if the vertex set is partitioned into two parts, then one of those parts induces a subgraph isomorphic to  $G$ , are the complete and null graphs and  $R$ .*

*Proof.* Suppose that  $G$  has this property but is not complete or null. Since any graph can be partitioned into a null graph and a graph with no isolated vertices, we see that  $G$  has no isolated vertices. Similarly, it has no vertices joined to all others.

Now suppose that  $G$  is not isomorphic to  $R$ . Then we can find  $u_1, \dots, u_m$  and  $v_1, \dots, v_n$  such that (\*) fails, with  $m + n$  minimal subject to this. by the preceding paragraph,  $m + n > 1$ . So the set  $\{u_1, \dots, v_n\}$  can be partitioned into two non-empty subsets  $A$  and  $B$ . Now let  $X$  consist of  $A$  together with all vertices (not in  $B$ ) which are not "correctly joined" to the vertices in  $A$ ; let  $Y$

consist of  $B$  together with all vertices (not in  $X$ ) which are not "correctly joined" to the vertices in  $B$ . By assumption,  $X$  and  $Y$  form a partition of the vertex set. Moreover, the induced subgraphs on  $X$  and  $Y$  fail instances of condition  $(*)$  with fewer than  $m + n$  vertices; by minimality, neither is isomorphic to  $G$ , a contradiction. □

**Proposition 7.**  *$R$  is isomorphic to its complement*

*Proof.* Property  $(*)$  is clearly self-complementary. □

## 5 Homogeneity

**Definition 3.** A structure is a set equipped with a collection of relations, functions and constants. If there are no functions or constants, then we have a relational structure.

**Definition 4.** A relational structure  $M$  is homogeneous if every isomorphism between finite induced substructures of  $M$  can be extended to an automorphism of  $M$ .

**Proposition 8.**  *$R$  is homogeneous*

*Proof.* This proof follows from the proof of Fact 2. Taking  $G_1 = G_2 = R$ , we start with an isomorphism between finite substructures of  $R$ , and proceed in the back-and-forth manner to derive an automorphism of  $R$ . □

In the terminology of Fraïssé, we have the following definitions.

**Definition 5.** The age of a structure  $M$  is the class of all finite structures embeddable in  $M$ .

**Definition 6.** A class  $\zeta$  of finite structures has the amalgamation property if, given  $A, B_1, B_2 \in \zeta$  and embeddings  $f_1 : A \rightarrow B_1$  and  $f_2 : A \rightarrow B_2$ , there exists  $C \in \zeta$  and embeddings  $g_1 : B_1 \rightarrow C$  and  $g_2 : B_2 \rightarrow C$  such that  $g_1 \circ f_1 = g_2 \circ f_2$ . Loosely speaking, if two structures  $B_1$  and  $B_2$  have isomorphic substructures  $A$ , then  $B_1$  and  $B_2$  can be "glued together" so that the substructures coincide, and such that the resulting structure  $C$  resides in  $\zeta$ .

**Theorem 4.** (a) A class  $\zeta$  of finite structures (over a fixed relational language) is the age of a countable homogeneous structure  $M$  if and only if  $\zeta$  is closed under isomorphism, closed under taking induced substructures, contains only countably many non-isomorphic structures, and has the amalgamation property.

(b) If the conditions of (a) are satisfied, then the structure  $M$  is unique up to isomorphism.

**Definition 7.** A class  $\zeta$  having the properties of the previous theorem is called a Fraïssé class, and the countable homogeneous structure  $M$  whose age is  $\zeta$  is its Fraïssé limit. The class of all finite graphs is a Fraïssé class, and its Fraïssé limit is  $R$ .

The Fraïssé limit of a class  $\zeta$  is characterized by a condition generalizing property (\*): If  $A$  and  $B$  are members of the age of  $M$  with  $A \subseteq B$  and  $|B| = |A| + 1$ , then every embedding of  $A$  into  $M$  can be extended to an embedding of  $B$  into  $M$ .

It is possible that when  $B_1$  and  $B_2$  are embedded into a structure  $C$  that their overlap in  $C$  may be larger than  $A$ , their isomorphic subgroup. This motivates the following definition.

**Definition 8.** A class  $\zeta$  has the strong amalgamation property if  $\zeta$  has the amalgamation property, and  $g_1[B_1] \cap g_2[B_2] = (g_1 \circ f_1)[A] = (g_2 \circ f_2)[A]$ . Informally,  $\zeta$  has the strong amalgamation property if when two given structures  $B_1$  and  $B_2$  are "glued together", the overlap is not larger than  $A$ .

**Proposition 9.** Let  $M$  be the Fraïssé limit of the class  $\zeta$ , and  $G = \text{Aut}(M)$ . Then the following are equivalent:

- (a)  $\zeta$  has the strong amalgamation property;
- (b)  $M \setminus A \cong M$  for any finite subset  $A$  of  $M$ ;
- (c) the orbits of  $G_A$  on  $M \setminus A$  are infinite for any finite subset  $A$  of  $M$ , where  $G_A$  is the setwise stabiliser of  $A$ .

**Definition 9.** A structure  $M$  is called  $\aleph_0$  categorical if any countable structure satisfying the same first-order sentences as  $M$  is isomorphic to  $M$ .

Here, it is necessary to specify that a structure be countable. By the Löwenheim-Skolem theorem, there are structures of arbitrarily large cardinality which satisfy the same first-order sentences as  $M$ .

**Proposition 10.**  $R$  is  $\aleph_0$  categorical

*Proof.* We need only translate property (\*) into a countable set of first-order sentences  $\sigma_{m,n}$  (for  $m, n \in \mathbb{N}$ ), where  $\sigma_{m,n}$  is the sentence

$$(\forall u_1, \dots, u_m, v_1, \dots, v_n)((u_1 \neq v_1) \& \dots \& (u_m \neq v_n)) \rightarrow (\exists z)((z \sim u_1) \& \dots \& (z \sim u_m) \& (z \not\sim v_1) \& \dots \& (z \not\sim v_n))$$

□

**Theorem 5.** If  $M$  is either  $\aleph_0$ -categorical or homogeneous, then it is universal.

## 6 First-order theory of random graphs

**Theorem 6.** *Let  $\theta$  be a first-order sentence in the language of graph theory. Then the following are equivalent:*

- (a)  $\theta$  holds in almost all finite random graphs;
- (b)  $\theta$  holds in the graph  $R$ ;
- (c)  $\theta$  is a logical consequence of  $\{\sigma_{m,n} : m, n \in \mathbb{N}\}$ .

*Proof.* The equivalence of (b) and (c) follows from the Gödel-Henkin completeness theorem for first-order logic, and the fact that the sentences  $\sigma_{m,n}$  axiomatize  $R$ . Now we show that (c) implies (a). We must first show that  $\sigma_{m,n}$  holds in almost all finite random graphs. The probability that it fails in an  $N$ -vertex graph is not greater than  $N^{m+n}(1 - \frac{1}{2^{m+n}})^{N-m-n}$ , since there are at most  $N^{m+n}$  ways of choosing  $m+n$  distinct points, and  $(1 - \frac{1}{2^{m+n}})^{N-m-n}$  is the probability that no further point is correctly joined. This probability tends to 0 as  $N$  tends to  $\infty$ .

Now let  $\theta$  be an arbitrary sentence satisfying (c). Since proofs in first-order logic are finite, the deduction of  $\theta$  involves only a finite set  $\Sigma$  of sentences  $\sigma_{m,n}$ . It follows from the last paragraph that almost all finite graphs satisfy the sentences in  $\Sigma$ ; so almost all satisfy  $\theta$  too.

Finally, we must show that not (c) implies not (a). If (c) fails, then  $\theta$  doesn't hold in  $R$ , so  $(\neg\theta)$  holds in  $R$ , so  $(\neg\theta)$  is a logical consequence of the sentences  $\sigma_{m,n}$ . By the preceding paragraph,  $(\neg\sigma)$  holds in almost all random graphs.  $\square$

**Corollary 1.** *Let  $\theta$  be a sentence in the language of graph theory. Then either  $\theta$  holds in almost all finite random graphs, or it holds in almost none.*

## 7 Measure and category

Here we discuss an alternative argument for the existence of  $R$  using Baire category theory. We begin by reviewing one of the Baire category theorems.

**Definition 10.** *A Baire space is a topological space with the following property: for each countable collection of open dense sets  $U_n$ , their intersection  $\cap U_n$  is dense.*

**Theorem 7** (Baire Category Theorem 1). *Every complete metric space is a Baire space. More generally, every topological space which is homeomorphic to an open subset of a complete pseudometric space is a Baire space. Thus every completely metrizable topological space is a Baire space.*

**Definition 11.** *In a topological space, a set is dense if it meets every nonempty open set; a set is residual if it contains a countable intersection of open dense sets.*

According to the Baire category theorem:

**Theorem 8.** *In a complete metric space, any residual set is non-empty.*

We are concerned with the space  $2^{\mathbb{N}}$  of all infinite sequences of zeros and ones. This is a probability space with the coin-tossing measure. It is a complete metric space with  $d(x, y) = \frac{1}{2^n}$  if the sequences  $x$  and  $y$  agree in positions  $0, 1, \dots, n-1$  and disagree in position  $n$ . We say that a set  $S$  of sequences is open if and only if it is finitely determined, i.e., any  $x \in S$  has a finite initial segment such that all sequences with this initial segment are in  $S$ . A set  $S$  is dense if and only if it is "always reachable", i.e., any finite sequence has a continuation lying in  $S$ . We say that "almost all sequences of property  $P$  (in the sense of Baire category)" if the set of sequences which have property  $P$  is residual. We now describe countable graphs by binary sequences. Take a fixed enumeration of the edge set of a graph; then we can view a sequence as the characteristic function of the edge set of a graph. This gives meaning to the phrase "almost all graphs (in the sense of Baire category)". Now analogous to Fact 1, we have the following:

**Fact 3.** *Almost all countable graphs (in the sense of either measure or Baire category) have property (\*).*

## 8 The automorphism group

### 8.1 General properties

In this section, we will explore the automorphism group of the infinite random graph,  $G = \text{Aut}(R)$ . Clearly,  $G$  acts transitively on vertices, edges, non-edges, etc. So  $G$  is a rank 3 permutation group on the vertex set. This holds because it has three orbits of vertices: equal, adjacent, and non-adjacent pairs.

**Proposition 11.**  $|\text{Aut}(R)| = 2^{\aleph_0}$ .

In fact, the automorphism group of any countable first-order structure is either at most countable or of cardinality  $2^{\aleph_0}$ .

**Definition 12.** *A countable structure  $M$  has the small index property if any subgroup of  $\text{Aut}(M)$  with index less than  $2^{\aleph_0}$  contains the pointwise stabilizer of a finite set of points of  $M$ ; it has the strong small index property if any such subgroup lies between the pointwise and setwise stabiliser of a finite set.*

**Theorem 9.**  *$R$  has the strong small index property.*

This result was shown by Hodges et al. [3], and Cameron [2].

**Corollary 2.** *Let  $\Gamma$  be a graph with fewer than  $2^{\aleph_0}$  vertices, on which  $\text{Aut}(R)$  acts transitively on vertices, edges and non-edges. Then  $\Gamma$  is isomorphic to  $R$ .*

## 8.2 Simplicity of $\text{Aut}(R)$

The aim of this section is to prove the following theorem, which can be attributed to Truss [4]:

**Theorem 10.**  *$\text{Aut}(R)$  is simple.*

Let  $C$  be a set with at least two, and at most  $\aleph_0$  members, and let  $[X]^2$  denote the set of 2-element subsets of a set  $X$ . If  $\Gamma$  is a countable set, and  $F_C$  is a function from  $[\Gamma]^2$  into  $C$ , then the structure  $\Gamma_C = (\Gamma, F_C)$  is called the countable universal C-coloured graph if the following condition is satisfied: Whenever  $\alpha$  is a map from a finite subset of  $\Gamma$  into  $C$ , there is  $x \in \Gamma \setminus \text{Dom}(\alpha)$  such that  $(\forall y \in \text{Dom}(\alpha), F_c\{x, y\} = \alpha(y))$ . Now let  $G_C$  be the group of automorphisms of  $\Gamma_C$ .

Let  $\Sigma$  be the set of all  $\sigma \in G = \text{Aut}(R)$ , which are an infinite product of disjoint infinite cycles (with no finite cycles) and such that the following property holds: Whenever  $\alpha$  is a map from a finite subset of  $\Gamma$  into  $C$ , there is  $x \in \Gamma \setminus \text{Dom}(\alpha)$  such that  $\forall n \in \mathbb{Z}, \sigma^n(x) \notin \text{Dom}(\alpha)$  and  $\forall y \in \text{Dom}(\alpha), F\{x, y\} = \alpha(y)$ . In this case, we say that  $x$  is a witness for the formula.

Simplicity of  $G = \text{Aut}(R)$  follows from two theorems:

**Theorem 11.** *Let  $\sigma_1, \sigma_2$  be non-identity members of  $G$ . Then there is a conjugate  $\tau$  of  $\sigma_1$  such that  $\sigma_2\tau \in \Sigma$ .*

**Theorem 12.** *Let  $\sigma_1, \sigma_2, \sigma_3 \in \Sigma$ . Then there are conjugates  $\tau_1, \tau_2, \tau_3$  of  $\sigma_1, \sigma_2, \sigma_3$ , respectively, such that  $\tau_1\tau_2\tau_3 = 1$ .*

The simplicity of  $\text{Aut}(R)$  follows. By the first theorem, there are conjugates  $\sigma_1$  and  $\sigma_2$  of  $\sigma^{-1}$  such that  $\sigma^{-1}\sigma_1, \tau\sigma_2 \in \Sigma$ . By the second theorem, there are conjugates  $\tau_1, \tau_2$  of  $\sigma^{-1}\sigma_1$  and  $\tau_3$  of  $\tau\sigma_2$  such that  $\tau_3\tau_2\tau_1 = 1$ . Therefore,  $\tau_3 = \tau_1^{-1}\tau_2^{-1}$ , so  $\tau_3$  is a product of four conjugates of  $\sigma$ . Hence so is  $\tau\sigma_2$ , and  $\tau$  is the product of five conjugates of  $\sigma$ .

## 8.3 Topology

Given an infinite set  $X$ , the symmetric group  $\text{Sym}(X)$  has a topology in which a neighborhood basis of the identity is given by pointwise stabilizers of finite tuples. Let  $m(g)$  be the smallest point moved by the permutation  $g$ . Define the distance between the identity and  $g$  to be  $\max\{2^{-m(g)}, 2^{-m(g^{-1})}\}$ . This metric is translation-invariant:  $d(f, g) = d(fg^{-1}, 1)$ .

**Proposition 12.** *Let  $G$  be a subgroup of the symmetric group on a countable set  $X$ . Then the following are equivalent:*

- (a)  $G$  is closed in  $\text{Sym}(X)$ ;
- (b)  $G$  is the automorphism group of a first-order structure on  $X$ ;
- (c)  $G$  is the automorphism group of a homogeneous relational structure on  $X$ .

Thus, we see that  $\text{Aut}(R)$  is a topological group with a topology derived from a complete metric.

The following was proved by Truss [4]:

**Theorem 13.** *There is a conjugacy class which is residual in  $\text{Aut}(R)$ . Its members have infinitely many cycles of each finite length, and no infinite cycles.*

**Proposition 13.**  *$R$  has  $2^{\aleph_0}$  non-conjugate cyclic automorphisms.*

*Proof.* In section 2, we took a universal set  $S \subseteq \mathbb{N}$ , and showed that this induced a graph  $G$  with vertex set  $\mathbb{Z}$ , where  $x$  and  $y$  are adjacent whenever  $|x - y| \in S$ , and  $G$  is isomorphic to  $R$ . Now clearly, this graph admits the shift automorphism defined by  $x \mapsto x + 1$ .

Now, let  $\phi$  be a cyclic automorphism of  $R$ . Index the vertices of  $R$  so that  $\phi(x) = x + 1$ , for every vertex  $x$ . If we take  $S = \{n \in \mathbb{N} : n \sim 0\}$ , then  $x \sim y$  if and only if  $|x - y| \in S$ , where  $S$  is universal. It can be proven that two cyclic automorphisms are conjugate in  $\text{Aut}(R)$  if and only if they give rise to the same set  $S$ . Since there are  $2^{\aleph_0}$  universal sets, the result is proved.  $\square$

## References

- [1] P. J. Cameron (1999) Permutation Groups. London Mathematical Society, p 134
- [2] P. J. Cameron (2005), The random graph has the strong small index property, *Discrete Math.* 291, 41-43
- [3] W. A. Hodges, I. M. Hodkinson, D. Lascar and S. Shelah (1993), The small index property for  $\omega$ -stable and  $\omega$ -categorical structures and for the random graph, *J. London Math. Soc.* (2) 48, 204-218
- [4] J. K. Truss (1985). The group of the countable universal graph. Mathematical Proceedings of the Cambridge Philosophical Society, 98, pp 213-245 doi:10.1017/S0305004100063428