COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 12 (4) (1992) 411–416

EXTENDING PARTIAL ISOMORPHISMS OF GRAPHS

EHUD HRUSHOVSKI[1]

Received June 7, 1991

Theorem. *Let X be a finite graph. Then there exists a finite graph Z containing X as an induced subgraph, such that every isomorphism between induced subgraphs of X extends to an automorphism of Z.*

The graph Z may be required to be edge-transitive. The result implies that for any n, there exists a notion of a "generic n-tuple of automorphisms" of the Rado graph R (the random countable graph): for almost all automorphisms $\sigma_1,\dots,\sigma_n$ and$\tau_1,\dots,\tau_n$ of R (in the sense of Baire category), $(R,\sigma_1,\dots,\sigma_n),\cong(R,\tau_1,\dots,\tau_n)$. The problem arose in a recent paper of Hodges, Hodgkinson, Lascar and Shelah, where the theorem is used to prove the small index property for R.

1. Introduction

The origin of the question is explained here, but none of the notions involved are in any way needed for the statement of the theorem. Let Gr be the class of all finite graphs, with graph embeddings assumed to preserve edges and non-edges. The *generic graph* is the unique countable graph R satisfying:

(1) Every element of Gr embeds into R.

(2) Given embeddings $f:M\to N$ in Gr and $g:M\to R$, there exists $h:N\to R$ with $hf=g$.

This graph (also called the Rado graph or the countable random graph) has the property that it is isomorphic to almost every graph on a countable set of vertices (edges chosen independently with probability 1/2) [3].

It is a result of Fraïssé that a generic object exists not only for the class Gr, but for any similar class of structures closed under substructures and satisfying the amalgamation property; see [2] for this story. In particular, one can consider the class Gr^+ of finite graphs Γ endowed with partial automorphisms $F_1,F_2,\dots$ (isomorphisms between induced subgraphs, considered as binary relations on Γ; it is assumed that only finitely many F_i's are nonempty on Γ.) This class satisfies the requirements and hence there exists a unique object $(R,f_1,f_2,\dots)$ satisfying (1), (2) for Gr^+. It is easy to see that the underlying graph of this object is the generic graph. The theorem proved here states that the f_i's define locally finite automorphisms of R. Note that uniqueness of $(R,f_1,f_2,\dots)$ as a structure is equivalent to the uniqueness of the sequence of automorphisms $(f_1,f_2,\dots)$ up to simultaneous conjugacy in $\mathrm{Aut}(R)$; thus we have defined a certain conjugacy class of sequences of automorphisms of R, which could be called *mutually generic* (see [7]).

AMS subject classification code (1991): 05 C 25

[1] Work supported by a Sloan Fellowship and by NSF grant DMS–8903378.

The problem arose initially in investigations of the structure of the group of automorphisms of R. The *small index conjecture* for R states that a subgroup of $\mathrm{Aut}(R)$ is of countable index if and only if it contains the stabilizer of a finite set. This is proved to be the case in [5] (see also [6]). Mutually generic automorphisms are used here, for example, in the following way. If $(f_1, f_2, \ldots)$ is such a sequence, then so is $(f_{\sigma 1}, f_{\sigma 2}, \ldots)$ for any permutation σ of $\{1, 2, \ldots\}$. Hence G-conjugation induces the full symmetric group on $Y = \{f_1, f_2, \ldots\}$. Any subset of G intersecting Y in an infinite, co-infinite subset must therefore have continuum many conjugates. This is used to show (initially) that any subset of G with less than continuum conjugates must be meager or co-meager in the sense of Baire category.

2. Proof of Theorem

We will say that a family F of subsets of a finite set Y is *statistically independent* if for all distinct $A_1, \ldots, A_m, B_1, \ldots, B_k$ in F $\mathrm{card}(A_1 \cap \ldots \cap A_m - B_1 - \ldots - B_k) = \mathrm{card}(Y) \cdot 2^{-m-k}$. For a graph X we use the same letter X to denote its set of vertices, and E^X to denote the set of edges. $X(a)$ is the set of vertices of X adjacent to a.

Claim 1. *Every finite graph X can be embedded in a finite graph Y such that $\{Y(a) : a \in X\}$ is a statistically independent collection of subsets of Y.*

Proof. We may assume the map $a \mapsto X(a)$ is one-to-one on X, since it is easy to embed X in a slightly larger graph with this property. Let Y be the set of all subsets of X, and define a graph structure on Y by:

$$(y_1, y_2) \in E^Y \text{ iff } y_1 = X(a_1) \text{ for some } a_1 \in y_2, \text{ or } y_2 = X(a_2) \text{ for some } a_2 \in y_1.$$

Note that if $y_1 = X(a_1)$ and $y_2 = X(a_2)$, then $a_1 \in y_2$ iff $a_2 \in y_1$ iff (a_1, a_2) is an edge of X; so X is embedded into Y by the map $a \mapsto a^* = X(a)$. Moreover $Y(a^*) = \{y : a \in y\}$. So $\{Y(a^*) : a \in Y\}$ is clearly statistically independent.

Let U be the set of isomorphisms between induced subgraphs of X. Let Y be as in Claim 1.

Claim 2. *Let $f \in U$. There exists $f^* \in \mathrm{Sym}(Y)$ such that f^* extends f, and $f^*[Y(a)] = Y[f(a)]$ for $a \in \mathrm{dom}(f)$. If $\mathrm{dom}(f) = \mathrm{range}(f)$ and $f^2 = 1$ then f^* may be chosen so that $f^{*2} = 1$.*

Proof. Let $D = \mathrm{dom}(f)$, $R = \mathrm{range}(f)$. For any function $\nu : D \to \{0,1\}$ let $D_\nu = \{y \in Y : \text{for } d \in D,\ (d, y) \in E^Y \text{ iff } \nu(d) = 1\}$. Let $R_\nu = \{y \in Y : \text{for } d \in D,\ (fd, y) \in E^Y$ iff $\nu(d) = 1\}$. By Claim 1, $|D_\nu| = |R_\nu| = |Y| \cdot 2^{-|D|}$. Since f is an isomorphism of D with R as graphs, $|D \cap D_\nu| = |R \cap R_\nu|$. Hence $|D_\nu - D| = |R_\nu - R|$. Let f^* be any permutation of Y extending f and mapping $D_\nu - D$ to $R_\nu - R$ for each ν. If $D = R$ and $f^2 = 1$, then $R_\nu = D_{\nu f}$, and it is easy to choose f^* with $f^{*2} = 1$.

Choose f^* for $f \in U$ in such a way that $f^{-1*} = f^{*-1}$. Let G be the group of permutations of Y generated by $U^* = \{f^* : f \in U\}$.

Notation. $f_n \ldots f_1 x = y$ (with $x, y \in Y$, $f_1, \ldots, f_n \in U$) means: there exist $x_0, \ldots, x_n \in Y$ with $x_0 = x$, $x_n = y$, $x_i \in \mathrm{dom}(f_{i+1})$, and $f_{i+1} x_i = x_{i+1}$ for $i < n$.

Define a relation $\approx$ on $G \times X$ by

$(g,x) \approx (g',x')$ if there are $h_1,\ldots,h_n \in U$ with
(i) $h_n \ldots h_1 x = x'$
(ii) $g = g' h_n^* \ldots h_1^*$ (in G).

Claim 3.
(a) $\approx$ *is an equivalence relation on* $G \times Y$.
(b) *The action of* G *on* $G \times Y$ *given by* $g(h,x) = (gh,x)$ *respects* $\approx$.

Proof. Easy. ∎

Let $Z = G \times Y/\approx$; by Claim 3 (b) there is an induced action of G on Z. Observe that if $(1,x) \approx (1,y)$ then there are $h_1,\ldots,h_n$ with $h_n \ldots h_1 x = y$ and $h_n^* \ldots h_1^* = 1$; so $x = y$. Thus Y embeds naturally into Z (as a set). Make Z into a graph by letting the edges be $\{(g,a)/\approx,(g,b)/\approx) : (a,b) \text{ is an edge of } Y,\ g \in G\}$. This makes Z into a graph, on which G acts by automorphisms, and clearly every element of U extends to one of G. We must show that Y is an induced subgraph of Z. Suppose x, $y \in Y$ and $((1,x)/\approx,(1,y)/\approx)$ if an edge of Z. Then for some $g \in G$, and some edge (x',y') of Y, we have:

$$(1,x) \approx (g,x')$$
$$(1,y) \approx (g,y')$$

So for some $h_1,\ldots,h_m$ and $f_1,\ldots,f_l$ in U,

$$h_m \ldots h_1 x' = x$$
$$f_l \cdots f_1 y' = y$$

and $h_m^* \ldots h_1^* = g = f_l^* \cdots f_1^*$.

Let $x_0,\ldots,x_m \in Y$ be such that $x_0 = x'$, $x_m = x$, $x_i \in \operatorname{dom}(h_{i+1})$, and $h_{i+1} x_i = x_{i+1}$. Then $h_{i+1}^*[Y(x_i)] = Y(x_{i+1})$, so $h_m^* \ldots h_1^*[Y(x')] = Y(x)$, hence $f_l^* \cdots f_1^*[Y(x')] = Y(x)$. Now $y' \in Y(x')$, so $f_l^* \cdots f_1^*(y') \in Y(x)$. But $f_l^* \ldots f_1^*(y') = f_1 \ldots f_1 y' = y$, so (x,y) is an edge of Y. This proves that Y is an induced subgraph of Z, and finishes the proof of the theorem. ∎

3. Discussion

3.1 A graph X is called *edge-transitive* (respectively *vertex-* or *flag-transitive*) if the automorphism group of X is transitive on edges (respectively vertices, or oriented edges). The graph Z constructed in the proof of the theorem is clearly flag-transitive. This strengthening may also be deduced from the theorem as stated. Let Z' be any graph satisfying the conclusion of the theorem. Observe that any two vertices (edges, oriented edges) of X are conjugate under $G = \operatorname{Aut}(Z')$. Let Z be the graph whose set of vertices is $\{gx : x \in X,\ g \in G\}$ and with $E^Z = \{ge : e \in E^X,\ g \in G\}$. It is then easy to verify that Z is flag-transitive and satisfies the requirements.

3.2 Suppose $|X| = n$. The present proof yields a graph Z with $|Z| \leq (2n2^n)!$. To see this follow the construction of Z:

(i) In Claim 1, X is replaced by a graph X' such that the map $a \mapsto X(a)$ is one-to-one on X'. This may be done most economically as follows: let U be a set of size $[\log_2(n)]+1$. Identify the set of vertices of X with a set of subsets of

U (disjoint from U), and containing the singleton subsets. Let $X' = X \cup U$, and let $E^{X'} = E^X \cup \{\{x,u\} : u \in X\}$. Then $|X'| = n + [\log_2(n)] + 1$.

(ii) The graph Y of Claim 1 has size $2^{|X'|} = 2n2^n$.

(iii) The group G defined in Claim 2 has size $\leq |Y|! = (2n2^n)!$. G acts transitively on Z (or Z may be so modified, as in 3.1) so the same bound holds for Z.

3.3 It is interesting to ask whether the doubly-exponential bound in 3.2 can be reduced. At all events one exponential is required. Let $n = 2m$, and let X be the graph with vertex set $\{0, \dots, n-1\}$ and edges $\{(i,j) : i+m < j\}$. Any permutation of $\{0, \dots, m-1\}$ is a partial automorphism of X, and hence must extend to an automorphism of Z. Thus for any subset S of $\{0, \dots, m-1\}$ there must exist an element b_S of Z whose set of neighbors among $\{0, \dots, m-1\}$ is precisely S. Thus Z must have cardinality at least $2^m + m$.

The same example shows that the bound $2n2^n$ on the size of the graph Y in Claim 1 cannot be substantially improved.

To be explicit, one may ask: If $|X| = n$, can Z be found with $|Z| \leq 2^{cn^2}$?

3.4 The problem may be generalized by taking the data to be a graph X together with a family F of partial automorphisms of X, and seeking a graph Z containing X as an induced subgraph, such that every element of F extends to an automorphism of Z. If F is the family of all maps on singletons, we are in effect requiring X to be embedded in a vertex-transitive graph. In this case the problem was solved with some precision in [1] (Theorem 2.4): If $g(n)$ denotes the smallest integer such that each graph with n vertices is an induced subgraph of some vertex-transitive graph of size $g(n)$, then $cn^2/\log^2 n < g(n) < c'n^2$ for some constants c, c'.

3.5 In another direction, we may consider the case where $F = \{f\}$ consists of a single partial automorphism. This case was proved in [7]. Let $g^*(n)$ denote the smallest integer such that for each pair (Γ, f), where Γ is a graph with n vertices and f is a partial automorphism, there exists a graph Γ' and an automorphism f' of Γ' such that Γ' contains Γ as an induces subgraph, and f' extends f. Let $\beta(n)$ be the number-theoretic function defined as follows. Let $P = \{(\prod_i q_i, \sum_i q_i) : q_1 \dots q_r$ are powers of distinct primes$\}$. Let $\beta(n) = \sup\{a(n-b) + b : (a,b) \in P\}$.

Claim.

a) *$c(n \log n)^{1/2} \leq \log \beta(n) \leq c'(n \log n)^{1/2}$ for some $0 < c < c'$.*

b) *For large enough n, if $n = c_1 + \dots + c_k + d_1 + \dots + d_l$ and μ is the least common multiple of the c_i's satisfying $\mu \geq 2d_j$ for each j, then $\sum c_i + l\mu \leq \beta(n)$.*

Proof. (a) An easy application of the prime number theorem. (For the upper bound, write $\beta(n) = a(n-b) + b$, $a = \prod_i q_i$, $b = \sum_i q_i$; note that at most $(n/\log(n))^{1/2}$ of the prime powers q_i belong to a prime $\geq (n \log n)^{1/2}$, or else $n - b$ would be negative. For the lower bound, consider only primes $\leq (n \log n)^{1/2}$; use the maximal power smaller than n, which must be $\geq n^{1/2}$.)

(b) If a prime p occurs in both c_i and c_j, say it occurs to a greater power in c_j; then replacing c_i by c_i/p and l by $l + (c_i - c_i/p)$ merely increases the bound; so we may assume the c_i's are powers of distinct primes. Let $(a,b) = (\prod_i c_i, \sum_i c_i)$. If $a \geq 2d_j$ for each j then $a = \mu$, so $\sum c_i + l\mu = b + la \leq b + (n-b)a \leq \beta(n)$. Otherwise

$b \le a \le 2n$ so $\mu \le 4n$ and $\sum c_i + l\mu \le 4n^2 + n$. But since n is large enough, there are four prime powers $q_1 \dots q_4$ between $\sqrt{n}$ and $(n-5)/4$, so $\beta(n) \ge 2 \cdot 3 \cdot q_1 \dots q_4 \ge 6n^2$.

Lemma. *For large enough n, $g^*(n) = \beta(n)$.*

Proof. First let f be a partial permutation of a set X of size n. Consider (X, f) as a graph, with $x, f(x)$ adjacent; a connected component is either a cycle or a "segment". Define $\mu = \mu(X, f)$ to be the least integer such that every cycle of (X, f) has order dividing μ, and every segment has size $\le \mu/2$. Let Z be a set containing X and g a permutation of Z extending f, such that:

($*$) every segment of (X, f) is contained in a cycle of (Z, g) of size μ; and every cycle of (Z, g) is a cycle of (X, f), or contains a unique segment of (X, f).

Note that the size of Z is $\sum c_i + l\mu$, where the c_i's are the sizes of the cycles of (X, f) and l is the number of segments; so by (b) above $|Z| \le \beta(n)$.

Now suppose X also has a graph structure E^X, so that f is a partial automorphism of (X, E^X). Define a graph structure on Z as follows: $\{x, y\} \in E^Z$ iff for some integer j, $\{g^j x, g^j y\} \in E^X$. Clearly g is an automorphism of Z. To see that X is an induced subgraph of Z, let x, $y \in X$ and suppose $\{g^j z, g^j y\} \in E^X$; we must show $\{x, y\} \in E^X$. Note that g^μ is the identity on Z, so we may choose j with $|j| \le (\mu/2)$. For definiteness say j is nonnegative. x, $g^j x$ lie in the same component C_Z of (Z, g), and hence by ($*$) in the same component C_X of (X, f). Suppose first C_X is a segment. It has length $\le (\mu/2)$, so $C_X \cup \{gx, \dots, g^j x\}$ has size $\le (\mu/2) + j - 1 < \mu$. Thus $C_X \cup \{gx, \dots, g^j x\} \ne C_Z$. However the two subsets C_X and $\{x, gx, \dots, g^j x\}$ of the cycle C_Z are connected and meet in two points x, $g^j x$, so they must go the same way around; i.e. $\{x, gx, \dots, g^j x\} \subseteq C_X$. Thus $g^i x \in X$ for $i \le j$, so $f^i x$ is defined for $i \le j$. If C_X is not a segment it is a cycle, in which case $f^i x$ is defined for all i. Similarly $f^i y$ is defined for $i \le j$. Since $\{f^j x, f^j y\} = \{g^j x, g^j y\} \in E^X$ we have $\{x, y\} \in E^X$ as required. This shows that $g^*(n) \le \beta(n)$.

For the other inequality, define a graph X of size n as follows. Let $\beta(n) = a(n-b) + b$, $(a, b) = (\prod_i q_i, \sum_i q_i)$, $q_1 < \dots < q_r$ powers of distinct primes. As a set X will consist of disjoint subsets C_i of size q_i and $(n-b)$ additional points e_j. For $i < r$ choose $a_i \in C_i$; also choose $a_{r,1}, \dots, a_{r,n-b}$ in C_r (it is easy to see that $q_r > (n-b)$.) Let $E^X = \{\{a_i, e_i\} : i < r,\ j = 1, \dots, n-b\} \cup \{\{a_{r,k}, e_j\} : k \le j\}$. Thus e_j is adjacent to a unique point of C_i for $i < r$, and to exactly j points of C_r. Let f be a permutation of $\cup_i C_i$ defining a cycle of order q_i on each C_i, with $f(a_{r,k}) = a_{r,k+1}$. If (Z, g) is a graph containing X as an induced subgraph, together with an automorphism g extending f, then g leaves each C_i invariant. In particular $g^k(e_j)$ is adjacent to exactly j points of C_r; so e_j, $e_{j'}$ are in distinct g-orbits if $j \ne j'$. The g-orbit of e_j must have size $m(j)$ divisible by each q_i, since $g^{m(j)} e_j = e_j$, so e_j is adjacent to $f^{m(j)} a_i$ and hence $f^{m(j)}(a_i) = a_i$. Similarly e_j is adjacent to $g^{m(j)} e_{r,k}$ for each $k \le j$, and it follows that $g^{m(j)} e_{r,1} = e_{r,1}$. Thus q_i divides $m(j)$ for each j, so $a \le m(j)$. Hence $|Z| = \sum_i q_i + \sum_j m(j) \ge b + (n-b)a = \beta(n)$, as required.

3.6 In the case of a single automorphism, the construction of 3.5 goes through for hypergraphs or other relational structures. Is the theorem also valid in this generality?

References

[1] L. Babai, and V. T. Sós: Sidon sets in groups and induced subgraphs of Cayley graphs, *Europ. J. Comb.* **6** (1985), 101–114.

[2] P. Cameron: *Oligomorphic Permutation Groups*, LMS 152, Cambridge University Press, 1990.

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

[4] R. Fraïssé: Sur l'extension aux relations de quelques proprietes des ordres, *Ann. Sci. École Norm. Sup.* **71** (1954), 361–388.

[5] W. Hodges, I. Hodkinson, D. Lascar, and S. Shelah: The small index property for omega-stable omega-categorical structures and for the random graph, preprint.

[6] D. Lascar: The group of automorphisms of a relational saturated structure, to appear in Proceedings of 1991 Banff conference on finite combinatorics.

[7] J. Truss: Generic Automorphisms of Homogeneous Structures, to appear in LMS Proceedings.

Ehud Hrushovski

Department of Mathematics, M.I.T.
Cambridge, MA 02139, U.S.A.
ehud@math.mit.edu