Isomorphism of Graphs with Bounded Eigenvalue Multiplicity

László Babai

Department of Algebra
Eötvös University
Budapest
HUNGARY, H-1088

D. Yu. Grigoryev

Leningrad Branch of the
Mathematical Institute
of the Acad. Sci. U.S.S.R.
191 011 Leningrad, U.S.S.R.

David M. Mount[†]

Dept. of Computer Sciences
Purdue University
West Lafayette, IN 47907

ABSTRACT

We investigate the connection between the spectrum of a graph, i.e. the eigenvalues of the adjacency matrix, and the complexity of testing isomorphism. In particular we describe two polynomial time algorithms which test isomorphism of undirected graphs whose eigenvalues have bounded multiplicity. If X and Y are graphs of eigenvalue multiplicity m, then the isomorphism of X and Y can be tested by an $O(n^{4m+c})$ deterministic and by an $O(n^{2m+c})$ Las Vegas algorithm, where n is the number of vertices of X and Y.

1. Introduction

It is not known whether graph isomorphism can be decided in deterministic polynomial time. The failure to find an efficient decision procedure after extensive effort suggests that researchers should look beyond classical graph theory and investigate the relevance of techniques from other areas in mathematics. Recent developments in the graph isomorphism problem have succeeded by introducing strong theoretical tools from topology and group theory. First, isomorphism of graphs of bounded genus was shown to be polynomial time testable [H&T 73, H&W 74, FMR 79, Mil 80, F&M 80, Lic 80]. These methods capitalized on the properties of the topological embeddings of graphs.

Recently group theoretic techniques have been brought to bear on the problem. László Babai introduced the "tower of groups method" to give a polynomial time coin tossing algorithm to decide isomorphism of graphs with bounded color multiplicity [Bab 79]. This technique was applied by Hoffmann to cone graphs of bounded degree [Hof 80a] and later by Furst, Hopcroft and Luks to trivalent graphs [FHL 80a]. Furthermore, the latter paper

[†] This work has been partially supported by the National Science Foundation under Grant MCS 80-21066.

demonstrated a deterministic polynomial time algorithm for the "tower of groups method" similar to existing algorithms from computational group theory [Sim 70]. An important breakthrough was achieved by E. M. Luks in establishing a polynomial time isomorphism test for graphs of bounded valence [Luk 80, Hof 82]. Among Luks' contributions was a recursive algorithm for computing setwise stabilizers in certain permutation groups based upon the existence of systems of imprimitivity.

In this paper we introduce a new class of graphs for which isomorphism may be tested in polynomial time: graphs with bounded eigenvalue multiplicity. Consider an undirected graph X with n vertices represented by its adjacency matrix A. Viewing A as a linear transformation in $\mathbb{R}^n$, the eigenvalues of A are the roots of the characteristic polynomial, $\det(\lambda I-A)$. We say that the graph X is of eigenvalue multiplicity m if no root of the characteristic polynomial has multiplicity exceeding m. The analysis of graphs through their eigenvalues constitutes the mathematical theory of graph spectra [Big 74, CDS 80]. The special case of deciding isomorphism of graphs with distinct eigenvalues has been shown to be achievable in $O(n^3)$ time by Leighton [L&M 82b].

Two algorithms are presented here which were discovered independently. The first algorithm, due to Babai and Grigoryev, employing the "tower of groups method" decides isomorphism of graphs with eigenvalue multiplicity m in $O(n^{4m+c})$ deterministic time with an $O(n^{2m+c})$ Las Vegas version (cf. Section 4). (c is an absolute constant everywhere but it may denote different constants at different places.) This result was announced in [Bab 79, Bab 80, and Bab 81] and is given in Section 4. The second algorithm, due to Mount, runs in $O(n^{4m+c})$ deterministic time. This algorithm applies Luks' method of "recursion through systems of imprimitivity" and is given in Section 5.

In order to determine whether two connected graphs X_1 and X_2 are isomorphic, it suffices to find a set of permutations generating the automorphism group of their disjoint union, $\mathrm{Aut}(X_1 \cup X_2)$. See for instance [Mat 78, Hof 80b]. Note that if X_1 and X_2 are each of eigenvalue multiplicity m, then their disjoint union is a graph of eigenvalue multiplicity at most 2m. Both of the algorithms presented determine the automorphism group of the graph by first using the eigenspace structure to formulate the problem in group theoretic terms and then solving the group theoretic problem.

2. Notation and Background

Linear Algebra

Consider an undirected graph X on n vertices represented by its adjacency matrix A. Since A is an n×n, symmetric real valued matrix it has n real *eigenvalues*. Let $\{\lambda_1, \lambda_2, \ldots, \lambda_r\}$ be the set of distinct eigenvalues. Associated with the eigenvalue λ_i is the *eigenspace* S_i containing the *eigenvectors* associated with λ_i: $S_i = \{x \in \mathbb{R}^n \mid Ax = \lambda_i x\}$. By virtue of the symmetry of A:

1. If λ_i is an eigenvalue with multiplicity m_i then S_i has dimension m_i.
2. The direct sum $S_1 \oplus S_2 \oplus \ldots \oplus S_r = \mathbb{R}^n$.
3. If $i \neq j$ then S_i and S_j are mutually orthogonal.

Let $V = \{e_1, e_2, \ldots, e_n\}$ be the standard basis of $\mathbb{R}^n$, i.e. the unit vectors. These vectors are identified with the vertices of X as enumerated in the adjacency matrix A. The ***automorphism group*** of X is defined to be the set of permutations on V which preserve adjacency. The automorphisms of X induce orthogonal linear transformations on $\mathbb{R}^n$ by permuting the unit vectors. So the automorphism group of X may equivalently be defined as the set of permutation matrices π which commute with the adjacency matrix of X:

$$\pi \in \mathrm{Aut}(X) \text{ iff } \pi A = A\pi$$

For a subspace $S \subset \mathbb{R}^n$ let pr_S denote the orthogonal projection from $\mathbb{R}^n$ to S.

Group Theory

A ***permutation group*** G on a domain V is a subgroup of the ***symmetric group*** Sym(V). The ***order*** of a finite group G, written |G|, is the number of elements in G. If H is a subgroup of G, written $H \leq G$, we may partition G into equivalence classes of uniform size by defining, for $\psi,\pi \in G$, $\psi \equiv \pi$ iff $\psi^{-1}\pi \in H$. These equivalence classes are the ***left cosets*** of H in G. The ***index*** of H in G, written |G:H|, is the number of equivalence classes under this partition. The partition is traditionally written:

$$G = \pi_1 H+\pi_2 H+\ldots+\pi_p H$$

where + denotes the union of disjoint sets.

A permutation group G ***(setwise) stabilizes*** a set $\Delta \subset V$ (equivalently, Δ is G-***stable***) if for all $x \in \Delta$, $\pi \in G$ we have $\pi x \in \Delta$. The set $\{\pi x \mid \pi \in G\}$ is the ***orbit*** of x in G. The orbits of a permutation group partition the permutation domain. For a G-stable subset Δ, we say G acts ***transitively*** on Δ if Δ is an orbit. Consider an invariant equivalence relation on a G-stable subset Δ, that is, $x \equiv y$ implies $\pi x \equiv \pi y$ for all $\pi \in G$. We call the equivalence classes of such a relation a ***system of imprimitivity*** on Δ. Any permutation $\pi \in G$ induces a permutation of the equivalence classes of the relation. Every group contains two trivial systems of imprimitivity on Δ corresponding to the identity relation and $\Delta\times\Delta$. Groups which have no nontrivial system of imprimitivity on Δ are said to act ***primitively*** on Δ.

The ***pointwise stabilizer*** in G of a set $B \subset V$ is the group $G_B = \{\pi \in G \mid \pi x = x \text{ for each } x \in B\}$. The set B is a ***base*** for G if G_B is the trivial group containing only the identity permutation. In this case, any member of G is determined by its action on B. For instance, a basis of a subspace S is a base for the group of linear transformations on S, GL(S). If G acts on V, |V| = n, and B is a base for G then $|G| \leq n(n-1)\ldots(n-|B|+1) \leq n^{|B|}$.

We use the symbol "↾" throughout to mean "restricted to."

In general a permutation group on n points may have as many as n! elements. However any permutation group G may be represented by a set of at most n^2 *generating permutations* whose closure under multiplication is equal to G [FHL 80b]. Throughout this paper those permutation groups whose order is bounded a priori by n^m will be represented by a full list of their elements. All other groups will be represented by a set of generating elements.

3. Eigenspaces and Automorphisms

The relationship between the automorphisms of a graph and the eigenspaces of the adjacency matrix of the graph is summarized in the following well known result from the theory of graph spectra.

Lemma 3.1 Let X be an undirected graph with adjacency matrix A. A permutation matrix $\pi \in \mathrm{Aut}(X)$ if and only if the eigenspaces of A are (setwise) invariant under π.

Proof

Suppose that $\pi \in \mathrm{Aut}(X)$. Let x be an arbitrary element of S_i. Then,

$$A\pi x = \pi Ax = \pi\lambda_i x = \lambda_i\pi x$$

Hence $\pi x \in S_i$. Conversely, suppose that S_i is π invariant. Again for $x \in S_i$,

$$A\pi x = \lambda_i\pi x = \pi\lambda_i x = \pi Ax$$

Since the eigenspaces of a symmetric matrix span $\mathbb{R}^n$, $A\pi = \pi A$.

□

Lemma 3.1 characterizes Aut(X) in terms of its action on the eigenspaces of X, but provides little intuition into the structure of a graph which has bounded eigenvalue multiplicity. We relate the information offered by Lemma 3.1 to the action of Aut(X) on the vertex set of the graph by demonstrating the existence of systems of imprimitivity.

For a subspace $S \subset \mathbb{R}^n$, let Ψ_S denote the equivalence relation on V defined

$$x \, \Psi_S \, y \text{ iff } pr_S x = pr_S y$$

Lemma 3.2 Let G be group of orthogonal transformations permuting V. Suppose that $\Delta \subset V$ is G-stable, and $S \subset \mathbb{R}^n$ is a G-invariant subspace such that $pr_S\Delta$ spans S. Then:

1. The equivalence classes Δ/Ψ_S form a system of imprimitivity in G on Δ.
2. The induced action of G on Δ/Ψ_S is isomorphic to the induced action of G on $pr_S\Delta$.
3. Let $\tilde{G}$ be the induced action of G on Δ/Ψ_S. Then there exists $\hat{G} \leq Sym(\Delta/\Psi_S)$ such that $\tilde{G} \leq \hat{G}$ and $|\hat{G}| \leq |\Delta/\Psi_S|^m$ where m is the dimension of S. The elements of $\hat{G}$ may be listed in $O(n^{m+c})$ time.

Proof

It is well known that if π is an orthogonal linear transformation under which a subspace S is invariant then pr_S and π commute.

1. For $x,y \in \Delta$, $\pi \in G$, $x\Psi_S y$ iff $pr_S x = pr_S y$ iff $\pi pr_S x = \pi pr_S y$ iff $pr_S \pi x = pr_S \pi y$ iff $\pi x \Psi_S \pi y$.
2. For $x \in \Delta$, identify the equivalence class $[x] \in \Delta/\Psi_S$ with the vector $pr_S x \in pr_S\Delta$. Because $[x]$ is a block of a system of imprimitivity in G, for $\pi \in G$.

   $$\pi[x] = [\pi x] \sim pr_S \pi x = \pi pr_S x$$

   As an obvious consequence the elements of G induce permutations on the set $pr_S\Delta$.
3. The induced actions of G on Δ/Ψ_S have been shown to be isomorphic to the actions of G on $pr_S\Delta$, and the induced actions of G on pr_S are linear transformations. If S has dimension m then S has a basis B of size m in $pr_S\Delta$. To each mapping $B \to pr_S\Delta$ there corresponds exactly one linear transformation of S. Some of these transformations permute the set $pr_S\Delta$. Let $\hat{G}$ denote the group of permutations of $pr_S\Delta$ obtained in this way. Certainly $\hat{G}$ contains $\tilde{G}$ as a subgroup. Because B is a base for $\hat{G}$, $|\hat{G}| \leq |pr_S\Delta|^{|B|} \leq n^m$. Furthermore, the elements of $\hat{G}$ can be listed in $O(n^{m+c})$ time by enumerating the n^m mappings $B \to pr_S\Delta$ and selecting the resulting linear transformations which permute $pr_S\Delta$.

□

Corollary For each eigenspace of the adjacency matrix of a graph X, there exists a system of imprimitivity in Aut(X). If the eigenspace has dimension m then there are at most n^m distinct actions induced on the blocks of this imprimitivity system.

In the next section an even stronger characterization of Aut(X) will be presented.

4. Tower of Groups Approach

In this section we consider the problem of determining a set of generators of the automorphism group of a graph X with at most m-tuple eigenvalues. The results of this section unless otherwise noted are due to the first two authors.

Theorem 4.1 For graphs X with not more than m-tuple eigenvalues, generators of the automorphism group Aut(X) can be found by an $O(n^{2m+c})$ deterministic and by an $O(n^{m+c})$ Las Vegas algorithm.

(The term Las Vegas algorithm has been introduced in [Bab 79]. It means an algorithm which uses flips of a coin; and its output may be "NO ANSWER", but whenever an answer is reached it is correct, and for any particular input, the probability of receiving NO ANSWER is $\leq 1/2$.)

The algorithm consists, roughly speaking, of a "linear algebra part" and of a "group theory part". The "linear algebra part" requires high precision arithmetic; eigenvalues and coordinates of eigenvectors have to be calculated to n^c digits accuracy in order to make it possible to decide whether two occurring numbers are equal. We do not go into details here. See [L&M 82a] for more information.

The output of the "linear algebra part" is a reduction to the problem of determining the automorphism group of a "graph with restricted color-groups": the vertex set V of the graph X is split as $V = C_1 + \ldots + C_s$, explicitly listed groups $H_i \le \mathrm{Sym}(C_i)$ act on each C_i, and we wish to obtain a set of generators for $\mathrm{Aut}(X) \cap (H_1 \times \ldots \times H_s)$. A particular case of this, solved in the same way [Bab 79], is the automorphism problem of "vertex-colored graphs with bounded color-multiplicities." (These problems are particular cases of the "intersection of group cylinders" problem, also solved in [Bab 79].) The "graph with restricted color-groups" is then reduced to the "tower of groups" which in turn admits a deterministic and a faster Las Vegas solution.

Balanced sequence of systems of imprimitivity

Our first procedure concerns permutation groups subject to certain imprimitivity conditions.

The identity relation will be denoted by id: x id y iff x=y. We say that an equivalence relation is *balanced* if all equivalence classes have equal cardinality. *A sequence of equivalence relations* $\Psi_1, \ldots, \Psi_r$ (on the same base set) will be called *balanced* if each of the equivalence relations $\Psi_1 \wedge \ldots \wedge \Psi_j$ $(j=1,\ldots,r)$ is balanced. (Note that we do not require here Ψ_2 (e.g.) to be balanced.)

Let $\Psi_1, \ldots, \Psi_r$ be a balanced sequence of equivalence relations on the set Δ such that $\bigwedge_{i=1}^{r} \Psi_i =$ id. Suppose that for each j, a permutation group $G_j \le \mathrm{Sym}(\Delta/\Psi_j)$ is explicitly listed, along with a base $B_j \subset (\Delta/\Psi_j)$ for G_j $(j=1,\ldots,r)$. Note that $|G_j| \le d^{|B_j|}$ where $d = |\Delta|$

Lemma 4.2 Let $H \le \mathrm{Sym}(\Delta)$ consist of those permutations under which each Ψ_j is invariant, and the action of each permutation on Δ/Ψ_j belongs to G_j. Then

(a) $|H| \le d^m$ where $d = |\Delta|$ and $m = \max_{j=1,\ldots,r} |B_j|$.

(b) H can be listed in d^{m+c} time.

Proof

Let $\overline{\Psi}_j = \Psi_1 \wedge \ldots \wedge \Psi_j$ $(j=1,\ldots r)$ and $\overline{\Psi}_0 = \Delta \times \Delta$. Since the sequence $\Psi_1, \ldots, \Psi_r$ is balanced, each $\overline{\Psi}_{j-1}$-class splits into an equal number, say d_j, of $\overline{\Psi}_j$-classes. $\overline{\Psi}_r =$ id, hence $d_1 \cdot \ldots \cdot d_r = d$.

Let H_j denote the group of those permutations under which $\Psi_1, \ldots, \Psi_j$ are invariant and whose action on Δ/Ψ_i belongs to G_i for $i=1,\ldots,j$. Let $\widetilde{H}_j$ denote the action of H_j on $\Delta/\overline{\Psi}_j$. Clearly, $H = H_r = \widetilde{H}_r$.

We shall list the elements of $\widetilde{H}_j$ by induction on j and claim $|\widetilde{H}_j| \le (d_1 \ldots d_j)^m$. $\widetilde{H}_0$ is the trivial group acting on the singleton $\Delta/\overline{\Psi}_0$. Let now $\sigma \in \widetilde{H}_{j-1}$. We have to find the set of those $\pi \in \widetilde{H}_j$ whose action on $\Delta/\overline{\Psi}_{j-1}$ coincides with σ. (Note that this set may be empty.)

Let us select one $\overline{\Psi}_j$-class from each Ψ_j-class corresponding to the members of B_j. Let B_j' denote the set of these $\overline{\Psi}_j$-classes. Now, σ determines the $\overline{\Psi}_{j-1}$-class of the π-image of each member of B_j'. Hence for each of them there are d_j possible π-images in $\Delta/\overline{\Psi}_j$. Once we have made our choice of $\pi \restriction B_j'$ out of these $d_j^{|B_j|}$ possible maps $B_j' \to \Delta/\overline{\Psi}_j$, the permutation π is uniquely determined (if such a π exists at all). Namely, for each $\overline{\Psi}_j$-class x, the $\overline{\Psi}_{j-1}$-class of πx is determined by σ and the Ψ_j-class of πx is determined by $\pi \restriction B_j'$ since B_j is a base of G_j.

Hence for each σ, the list of the corresponding π's can be compiled in d^{m+c} time, and this list is not longer than $d_j^{|B_j|} \le d_j^m$. In particular, it follows by induction that $|H_j| \le |H_{j-1}| \cdot d_j^{|B_j|} \le (d_1 \cdot \ldots \cdot d_j)^m$. The final conclusion is that $H = H_r$ can be found in d^{m+c+1} time and $|H| \le (d_1 \cdot \ldots \cdot d_r)^m = d^m$

□

Reduction to "Graphs with restricted color-groups"

A *partition-decomposition pair* $((C_1,\ldots,C_s),(W_1,\ldots,W_r))$ consists of a partition of the vertex set $V = C_1+\ldots+C_s$ and a decomposition of $\mathbb{R}^n$ to the orthogonal sum of subspaces $W_1\oplus\ldots\oplus W_r$. Such a pair is *invariant* if each set C_i and each subspace W_j is invariant under Aut(X).

As in Section 3 we define $x\Psi_j y$ iff $\mathrm{pr}_{W_j}x = \mathrm{pr}_{W_j}y$. The above partition-decomposition pair is *stable* if the following conditions hold for each $i=1,\ldots,s$ and $j=1,\ldots,r$:

(i) all vectors in $\mathrm{pr}_{W_j}C_i$ have equal lengths;

(ii) the sequence of equivalence relations $\Psi_1\restriction C_i, \Psi_2\restriction C_i,\ldots, \Psi_r\restriction C_i$ is balanced;

(iii) either $\mathrm{pr}_{W_j}C_i = \{0\}$ or $\mathrm{pr}_{W_j}C_i$ spans W_j.

We introduce three operations of *refinement*, corresponding to violations of either condition.

(oi) We split C_i into smaller classes according to the lengths of the projections $\mathrm{pr}_{W_j}x$, $x \in C_i$.

(oii) We split C_i so that two members of C_i remain equivalent iff their equivalence classes under $\bar{\Psi}_j$ had equal size, where $\bar{\Psi}_j = \Psi_1\wedge\ldots\wedge\Psi_j$.

(oiii) Let W_j' be the span of $\mathrm{pr}_{W_j}C_i$ and let W_j'' be the orthogonal complement to W_j' in W_j. We replace W_j by $W_j'\oplus W_j''$ in our decomposition of $\mathbb{R}^n$.

Lemma 4.3 If the partition-decomposition pair $((C_1,\ldots,C_s),(W_1,\ldots,W_r))$ is invariant then the refined partition-decomposition pair obtained after executing any of the above operations remains invariant.

The proof is a straightforward application of the earlier observation, that, if π is an orthogonal transformation and W is a π-invariant subspace then π and pr_W commute.

The following is clear, too:

Proposition 4.4 By less than 2n-fold application of the above operations we arrive from any initial partition-decomposition pair at a stable one.

As an initial decomposition we choose the decomposition to eigensubspaces of the adjacency matrix of X. Hence we have $\dim(W_j) \le m$. As an initial partition, the trivial partition (everything in one class) will suffice. We note, however, that we can start from any partition into invariant subsets.

The result of the "linear algebra part" of our algorithm can be summarized in the following:

Theorem 4.5 Let X be a graph with eigenvalue multiplicity $\le m$. Then one can partition the vertex set of X as $C_1+\ldots+C_s$ in n^c time such that

(a) each C_i is invariant under Aut(X);

(b) a permutation group $H_i \le \mathrm{Sym}(C_i)$ of order $|H_i| \le n^m$ can be listed in n^{m+c} time such that $(\mathrm{Aut}\ X)\restriction C_i \le H_i$ $(i=1,\ldots,s)$.

Proof

Let $((C_1,\ldots,C_s),(W_1,\ldots,W_r))$ be a stable partition-decomposition pair; $\dim(W_j) \le m$.

Now, for a fixed value of i, let $\Delta = C_i$. Consider the equivalence relation Ψ_j restricted to Δ. $\Psi_1,\ldots,\Psi_r$ is a balanced sequence of Aut(X)-invariant equivalence relations on Δ, and $\Psi_1\wedge\ldots\wedge\Psi_r = \mathrm{id}$.

If $\mathrm{pr}_{W_j}\Delta$ spans W_j then let G_j be the group $\hat{G}$ obtained in Lemma 3.2. G_j contains the induced actions of Aut(X) on on Δ/Ψ_j as a subgroup, and $|G_j| \le n^m$. $O(n^{m+c})$ times suffices to to list G_j.

If $\mathrm{pr}_{W_j}\Delta = \{0\}$ then $\Psi_j = \Delta\times\Delta$, and G_j will be the trivial group acting on the singleton Δ/Ψ_j.

By applying Lemma 4.2 now, where the group H obtained is denoted by H_i, we have $(\mathrm{Aut}\ X)\restriction C_i \le H_i$, and the proof is complete.

□

Corollary 4.6 If C is an orbit of $\mathrm{Aut}(X)$, then $|(\mathrm{Aut}\,X)\restriction C| \le n^m$.

Reduction to "Tower of groups"

Let now X be a graph with colored vertices, the color classes forming a partition $C_1+\ldots+C_s = V$ of the vertex set. Assume that groups $H_i \le \mathrm{Sym}(C_i)$ are explicitly listed for $i=1,\ldots,s$. Their direct product $H_1\times\ldots\times H_s$ acts on V. The question about "graphs with restricted color-groups" is to determine a set of generators for $G=\mathrm{Aut}(X) \cap (H_1\times\ldots\times H_s)$.

This is a particular case of the "intersection of group-cylinders" problem, formulated and solved in [Bab 79]. For completeness and for the sake of a more accurate complexity bound, we recall the method.

Let $N = \max\{\,|H_i| : i=1,\ldots,s\}$. Let $[C_i,C_j]$ denote the bipartite subgraph of X induced between C_i and C_j. Let H_{ij} denote the restriction to C_i of the group $\mathrm{Aut}[C_i,C_j] \cap (H_i\times H_j)$, $(i\ne j)$.

Lemma 4.7 H_{ij} can be listed in Nn^c time.

(Note that listing H_{ij} in N^2n^c time would be straightforward.)

Proof

Let Θ denote the equivalence relation on C_j defined by $x\Theta y$ iff x and y are adjacent to the same vertices in C_i. Clearly Θ is invariant under $\mathrm{Aut}[C_i,C_j]\restriction C_j$. Let H_j' consist of those elements of H_j under which Θ is invariant. H_j' can be listed simply by checking each member of H_j. Let $\widetilde{H}_j$ be the induced actions of H_j' on C_j/Θ. Given $\widetilde{H}_j$ (arranged as a dictionary with an efficient FIND operation), one can decide in n^c time for any $\pi \in H_i$ whether or not $\pi \in H_{ij}$. Namely, π induces at most one permutation of C_j/Θ, and we have to check whether this permutation belongs to $\widetilde{H}_j$ or not.

□

Let now $K_i = \bigcap_{j=1}^{s} H_{ij}$, where $H_{ii} = H_i \cap (\mathrm{Aut}(X\restriction C_i))$. By Lemma 4.7, K_i can be listed in Nn^c time.

Lemma 4.8 $|K_i\times K_j : \mathrm{Aut}[C_i,C_j] \cap (K_i\times K_j)| \le N$, (for $i\ne j$).

(Again, an N^2 upper bound would be straightforward.)

Proof

If A, B, C, D are groups, $A \le B \le D$, $C \le D$, then

$$|A:A\cap C| \le |B:B\cap C|$$

Applying this inequality to $A = K_i\times K_j$, $B = K_i\times H_j$, $C = \mathrm{Aut}[C_i,C_j]$, we find that the left hand side in the Lemma does not exceed

$$|K_i\times H_j : \mathrm{Aut}[C_i,C_j] \cap (K_i\times H_j)|.$$

As $K_i \le H_{ij}$, we have $|\mathrm{Aut}[C_i,C_j] \cap (K_i\times H_j)| \ge |K_i|$. Consequently the index of this group in $K_i\times H_j$ does not exceed $|H_j| \le N$.

□

Let $pr_{ij} : K_1\times\ldots\times K_s \to K_i\times K_j$ denote the projection map and $L_{ij} = pr_{ij}^{-1}(\mathrm{Aut}[C_i,C_j] \cap (K_i\times K_j))$. (This is a group cylinder in the sense of [Bab 79].) Clearly, $G = \bigcap_{i\ne j} L_{ij}$.

We are going to trap G in a tower of recognizable groups, exactly as in [Bab 79]. Let $q = \binom{s}{2}$, and let

$$G^0 = K_1\times\ldots\times K_s$$
$$G^1 = L_{12}$$
$$G^2 = L_{12} \cap L_{13}$$
$$\ldots \quad \ldots$$
$$G^q = \bigcap_{i\ne j} L_{ij} = G$$

Then we go on taking pointwise stabilizers:

$$G^{q+1} = G_1$$
$$G^{q+2} = G_{12}$$
$$\ldots \quad \ldots$$
$$G^{q+n} = G_{12\ldots n} = \{1\}$$

We have

$$|G^{k-1}:G^k| \le N \text{ for } k=1,\ldots,q$$
$$|G^{k-1}:G^k| \le n \text{ for } k=q+1,\ldots,q+n$$

Solution of the "Tower of groups"–Deterministic and Las Vegas

The "tower of groups" problem is the following:

Let $G^0 \geq G^1 \geq \ldots \geq G^t = \{1\}$ be a tower of groups. The elements of G_0 are encoded by words in an alphabet, and group operations are performed by an oracle. Each group G^i is *recognizable*, i.e. for any $\pi \in G^0$ the question $\pi \in G^i$ is decided by an oracle.

In addition, a set of generators of G^0 is provided. The problem is to find generators for each G^i. The problem, in this form, was formulated in [Bab 79].

An algorithm essentially due to Sims and analyzed by Furst-Hopcroft-Luks [FHL 80b] solves this problem by $O(T^2)$ operations where

$$T = \sum_{j=1}^{t} (|G^{j-1}:G^j| - 1)$$

The operations occurring are division and the following:

(•) Given an element $\pi \in G^{j-1}$ and a set of elements $\{\varphi_1, \ldots, \varphi_p\}$ of G^{j-1}, decide whether π belongs to any of the cosets $\varphi_j G^j$, $(j=1,\ldots,p)$.

In the case of the tower obtained at the end of the previous section, we would need about p group operations to decide (•) where p can be as large as N. We have, however a more economical way of doing (•) in the case of the "graphs with restricted color-groups".

Let $G^h = G^{h-1} \cap L_{ij}$. Clearly, for any $\sigma, \pi \in G^{h-1}$ we have $\sigma G^h = \pi G^h$ if and only is $\sigma\{C_i, C_j\} = \pi\{C_i, C_j\}$. This way we have a natural representation of the cosets $(G^{h-1} : G^h)$ as images under members of G^{h-1} of the edge set $\{C_i, C_j\}$ which can be stored in a dictionary with an efficient FIND operation, hence (•) costs only n^c each time.

The total running time of the "tower of groups" algorithm for the "graphs with restricted color-groups" problem will then be

$$O(T^2 n^2) = O(N^2 n^{c+2})$$

In the problem of determining the automorphism group of a graph with not more than m-fold eigenvalues, we have $N \leq n^m$. The running time of the entire algorithm is asymptotically dominated by the "tower of groups" piece, giving a total of $O(n^{2m+c})$ time.

The Las Vegas algorithm of [Bab 79] for the "tower of groups" requires only O(T) operations (•). This results in an $O(Nn^c)$ Las Vegas algorithm for the "graphs with restricted color-groups" problem and an $O(n^{m+c})$ Las Vegas algorithm for the automorphism group of a graph with not more than m-fold eigenvalues. (The "linear algebra" part of the algorithm contributes another $O(n^{m+c})$.

5. Systems of Imprimitivity Approach

In this section we provide another algorithm for finding a generating set for the automorphism group of an undirected graph with eigenvalue multiplicity m in $O(n^{2m+c})$ time, for c an absolute constant. This algorithm operates essentially by considering the possible actions induced by Aut(X) on each eigenspace. It then combines this information for each eigenspace to determine the actions of Aut(X) induced on the direct sum of the eigenspaces. Unless otherwise noted, the results of this section are due to the third author.

As in the previous section we assume that we are given the orthogonal projection transformation for each eigenspace. To avoid excessive subscripting, let pr_i denote the projection transformation for the i^{th} eigenspace S_i. Consider the set of unit vector permutations under which S_i is invariant. Define G_i to be the group consisting of the induced actions of these transformations on S_i. As seen in Section 3, the elements of G_i permute the set of projected unit vectors $pr_i V$. Since $pr_i V$ spans S_i we can faithfully represent each element of G_i as a permutation of $pr_i V$. By Lemma 3.2, $|G_i| \leq n^{m_i}$ where m_i is the dimension of S_i, and the elements of G_i may be listed in $O(n^{m_i+c})$ time.

Now we extend our notation to let $\bar{S}_i$ denote the direct sum $S_1 \oplus S_2 \oplus \cdots \oplus S_i$. Similarly let $\overline{pr}_i$ denote the orthogonal projection transformation for $\bar{S}_i$: $\overline{pr}_i = pr_1 + \ldots + pr_i$. Consider the set of linear transformations permuting the unit vectors under which $S_1, S_2, \ldots, S_i$ are invariant. Define $\bar{G}_i$ to be the group consisting of the induced actions of these transformations on $\bar{S}_i$. Although $|G_i|$ is polynomially bounded, in general $|\bar{G}_i|$ may grow as the product $|G_1| \cdot |G_2| \cdot \ldots \cdot |G_i|$. Hence $\bar{G}_i$ will be represented by a set of at most n^2 *generating permutations* [FHL 80b]. By Lemma 3.1, $\bar{G}_r = Aut(X)$, where r is the number of distinct eigenvalues.

Compatible Transformations

Since $\bar{S}_i = \bar{S}_{i-1} \oplus S_i$, any transformation $\psi \in \bar{G}_i$ induces a transformation $\varphi \in \bar{G}_{i-1}$ acting on $\bar{S}_{i-1}$ and $\pi \in G_i$ acting on S_i. Two transformations, like φ and π, which are induced by the same element of $\bar{G}_i$ are said to be *compatible*. In fact given a compatible pair of elements φ and π, the transformation $\psi \subset \bar{G}_i$ inducing φ and π, called their *extension*, is uniquely determined

$$ext(\varphi, \pi) = \psi = \varphi \overline{pr}_{i-1} + \pi pr_i$$

Our approach to finding $\bar{G}_i$ is to select a permutation $\pi \in G_i$, generate the subset of permutations of $\bar{G}_{i-1}$ which are compatible with π, and then extend the result to a subset of $\bar{G}_i$. For $H \subseteq \bar{G}_{i-1}$, $\pi \subset G_i$ define:

$$comp_\pi(H) = \{\varphi \in H \mid ext(\varphi, \pi) \in \bar{G}_i\}$$

For $H \subseteq \bar{G}_{i-1}$ whose elements are compatible with π, let $ext(H, \pi)$ denote the extension of the elements of H with π. Obviously,

$$\bar{G}_i = \bigcup_{\pi \in G_i} ext(comp_\pi(\bar{G}_{i-1}), \pi)$$

Conceptually, Aut(X) is computed as follows:

```
Compute $G_1, G_2, \ldots, G_r$;
$\bar{G}_1 := G_1$;
for i := 2 to r do begin
    $\bar{G}_i := \{\}$;
    for each $\pi \in G_i$ do
        $\bar{G}_i := \bar{G}_i \cup ext(comp_\pi(\bar{G}_{i-1}), \pi)$;
end
$Aut(X) := \bar{G}_r$;
```

We will return later to explain the efficient implementation of the underlying operations on the permutation groups. Presently we turn our attention to computing $comp_\pi(\bar{G}_{i-1})$ in polynomial time.

We investigate the relationship between a transformation in G_i (alternately in $\bar{G}_i$) and the set of unit vector permutations which induce this transformation. Consider an eigenspace S_i. Let $\Gamma_1, \Gamma_2, \ldots, \Gamma_d$ be the equivalence classes of the relation defined in Section 3 on V:

$$x \Psi_i y \quad \text{iff} \quad pr_i x = pr_i y$$

Define the group $K_i = Sym(\Gamma_1) \times Sym(\Gamma_2) \times \ldots \times Sym(\Gamma_d)$. Similarly we define $\bar{K}_i$ in terms of $\bar{S}_i$, $\overline{pr}_i$ and $\bar{\Psi}_i = \Psi_1 \wedge \ldots \wedge \Psi_i$. (The groups K_i and $\bar{K}_i$ are introduced only for the purposes of proof and are not used by the algorithm.)

Lemma 5.1 Consider $\varphi \subset G_i$ (alternately $\bar{G}_i$) which is induced by the unit vector permutation φ'. The set of unit vector permutations which induce φ on S_i ($\bar{S}_i$) is $\varphi' K_i$ ($\varphi' \bar{K}_i$)

The proof is a straightforward application of basic linear algebra and group theory.

Given $\varphi \in \bar{G}_{i-1}$ and $\pi \in G_i$ the question of whether φ and π are compatible reduces to determining that:

$$\varphi' \bar{K}_{i-1} \cap \pi' K_i \neq \{\}.$$

where φ' and π' are unit vector permutations inducing φ and π respectively.

The compatibility criterion may be visualized by constructing a matrix P whose rows are indexed by the elements of $\overline{pr}_{j-1}V$ and whose columns are indexed by the elements of pr_jV. The entry $P_{x,y}$ is the set of elements of V which project both onto x and y.

$$P_{x,y} = \{z \in V \mid \overline{pr}_{j-1}z = x \text{ and } pr_jz = y\}$$

By Lemma 5.1, to induce $\varphi \in \overline{G}_{j-1}$ we must map each of the elements of V which project onto x to some element projecting onto φx. That is, we must map each element of row x to an element in row φx. Likewise to induce $\pi \in G_j$ we must map each of the elements in column y to an element in column πy. (This is exactly what the permutations of $\varphi'\overline{K}_{j-1}$ and $\pi'K_j$ do respectively.) The row and column permutations φ and π naturally induce a permutation on the entries of P mapping $P_{x,y}$ to $P_{\varphi x,\pi y}$. A permutation of V can be found which induces both φ and π if and only if the cardinality of the entries is preserved under this induced row and column permutation. Thus we have shown:

Theorem 5.2 For $\varphi \in \overline{G}_{j-1}$ and $\pi \in G_j$, φ and π are compatible if and only if $\forall x \in \overline{pr}_{j-1}V$, $\forall y \in pr_jV$, $|P_{x,y}| = |P_{\varphi x,\pi y}|$.

We have reduced the algebraic notion of compatibility for linear transformations φ and π to a predicate over permutations φ and π acting on $\overline{pr}_{j-1}V$ and pr_jV respectively. Note that the only computational objects whose construction requires the high precision representation are G_i, pr_i and $\overline{pr}_i$ for $i=1,\ldots,r$. Henceforth we identify the sets of vectors V, pr_jV and $\overline{pr}_jV$ with initial segments of the set $\{1,2,\ldots,n\}$. The groups G_i and $\overline{G}_i$ will be represented as permutation groups over these sets. As mentioned earlier, this representation is faithful. The extension of compatible permutations φ and π can be defined as the $\psi \in Sym(\overline{pr}_jV)$ such that for all $z \in \overline{pr}_jV$, $\overline{pr}_{j-1}\psi z = \varphi\overline{pr}_{j-1}z$ and $pr_j\psi z = \pi pr_jz$.

Simple Recursive Definition of $comp_\pi$

Now we modify the definition of $comp_\pi$ to restrict attention to a subset of the permutation domain. Let $H \le \overline{G}_{j-1}$, $\psi \in \overline{G}_{j-1}$, $\pi \in G_j$ and $\Delta \subset \overline{pr}_{j-1}V$ which is setwise stable in H. Define:

$$comp_\pi(\psi H,\Delta) =$$
$$\{\varphi \in \psi H \mid \forall x \in \Delta, \forall y \in pr_jV, |P_{x,y}| = |P_{\varphi x,\pi y}|\}$$

Our goal is to compute $comp_\pi(\overline{G}_{j-1},\overline{pr}_{j-1}V)$.

Standard results from computational group theory provide an efficient representation of permutation groups by means of a set of generating permutations. A coset of a permutation group, say ψH, can be represented by ψ and a generating set for H. It is crucial that all of the intermediate results of the algorithm have such a succinct representation. The following, adapted from [Luk 80], establishes this for us:

Proposition 5.3 Let $H \le \overline{G}_{j-1}$ and $\Delta \subseteq \overline{pr}_{j-1}V$ setwise stable in H. Then $comp_\pi(\psi H,\Delta)$ is either empty or is a coset of the group $comp_I(H,\Delta)$, where I is the identity transformation.

Proof

The stability of Δ in H guarantees that $comp_I(H,\Delta)$ is a group. Suppose that $comp_\pi(\psi H,\Delta)$ is not empty and φ is an element. Then $\varphi \in \psi H$ and $\forall x \in \Delta$, $y \in pr_jV$, $|P_{x,y}| = |P_{\varphi x,\pi y}|$. Let σ be any element of H. Note that for $x \in \overline{pr}_{j-1}V$, $x \in \Delta$ iff $\sigma x \in \Delta$. Hence $\forall x \in \Delta$, $y \in pr_jV$, $|P_{\sigma x,y}| = |P_{\varphi\sigma x,\pi y}|$. From this it follows that:

$$\forall x \in \Delta, y \in pr_jV, |P_{x,y}| = |P_{\varphi\sigma x,\pi y}|$$
$$\text{iff}$$
$$\forall x \in \Delta, y \in pr_jV, |P_{x,y}| = |P_{\sigma x,y}|$$

Rephrasing this gives:

$$\varphi\sigma \in comp_\pi(\psi H,\Delta) \quad \text{iff} \quad \sigma \in comp_I(H,\Delta)$$

Therefore $comp_\pi(\psi H,\Delta)$ is a coset of $comp_I(H,\Delta)$.

□

We apply Luks' recursive methods to compute $comp_\pi$. One easily verifies the following rules which guide the computation, recalling that Δ is setwise stable in H:

$\mathrm{comp}_\pi(\psi H,\Delta)$:

1. If $\Delta = \{x\}$ then:

   $$\mathrm{comp}_\pi(\psi H,\Delta) = \begin{cases} \psi H & \text{if } \forall y \in pr_i V, |P_{x,y}| = |P_{\psi x, \pi y}| \\ \{\} & \text{otherwise} \end{cases}$$

2. If $\Delta = \Gamma_1+\Gamma_2+\ldots+\Gamma_d$ and each Γ_i is setwise stable in H then:

   $\mathrm{comp}_\pi(\psi H,\Delta) = \mathrm{comp}_\pi(\ldots(\mathrm{comp}_\pi(\psi H,\Gamma_1),\ldots),\Gamma_d)$.

3. If $H = \varphi_1 H'+\varphi_2 H'+\ldots+\varphi_q H'$ then.

   $\mathrm{comp}_\pi(\psi H,\Delta) = \bigcup_{j=1}^{q} \mathrm{comp}_\pi(\psi\varphi_j H',\Delta)$.

The correctness of these rules is independent of the structure of the group H. The efficiency of these rules however depends crucially on the existence of a rich imprimitivity structure in $\overline{G}_{i-1}$.

Let S_j be an eigenspace, where $1 \le j \le i-1$. Define the equivalence relation Ψ_j on $\overline{pr}_{i-1}V$ just as before. The fundamental result giving a polynomial time algorithm relates the size of H to the size of the setwise stabilizer of the equivalence classes of Ψ_j.

Theorem 5.4 Let $H \le \overline{G}_{i-1}$ and $\Delta \subset \overline{pr}_{i-1}V$ be an orbit of H. For any eigenspace S_j $(1 \le j \le i-1)$ the equivalence classes Δ/Ψ_j form a system of imprimitivity in H. Let H' be the subgroup of H setwise stabilizing these classes. Then $|H{:}H'| \le |\Delta/\Psi_j|^{m_j}$ where m_j is the dimension of S_j.

Proof

The proof follows immediately from Lemma 3.2 with the observation that the cosets of H' in H are in 1-1 correspondence with the induced actions of H on Δ/Ψ_j.

□

We compute comp_π by investigating the action of H on the subset Δ. If this action is intransitive we recursively call comp_π on each of the orbits in Δ (rule 2). If the action is transitive we find an eigenspace S_j $(1 \le j \le i-1)$ which partitions Δ nontrivially, find the subgroup $H' \le H$ stabilizing this partition and call comp_π with each of the cosets of H' in H on each of the partitions (rule 3).

Note that for any pair of distinct vectors in $\overline{pr}_{i-1}V$, there is some eigenspace S_j $(1 \le j \le i-1)$ in which their projections are unequal. Thus if $|\Delta| > 1$ we can always find a eigenspace which partitions Δ nontrivially.

Reorganizing the Recursion

The problem with computing "comp" directly from these simple recursive rules is that relatively expensive operations, such as computing generators for the subgroup H', are performed over and over for each coset ψH and each π, when in fact these operations only depend on H and Δ. We reorganize the recursion by collecting at one time the entire set of pairs ψ and π which will appear in a call to $\mathrm{comp}_\pi(\psi H,\Delta)$ for a single H and Δ.

Given $H \le \overline{G}_{i-1}$ and $\Delta \subset \overline{pr}_{i-1}V$ which is H-stable suppose that $U \subset \overline{G}_{i-1} \times G_i$ is a set of pairs (ψ,π) for which we want to compute $\mathrm{comp}_\pi(\psi H,\Delta)$. As seen in Proposition 5.3, if nonempty then $\mathrm{comp}_\pi(\psi H,\Delta) = \hat{\psi}\mathrm{comp}_I(H,\Delta)$. We distinguish our new procedure with an upper case name. Define:

$\mathrm{COMP}(H,U,\Delta) = (K,W)$ where:

1. K is a generating set for $\mathrm{comp}_I(H,\Delta)$,
2. $W \subset \overline{G}_{i-1} \times G_i$ contains one pair $(\hat{\psi},\pi)$ corresponding to each $(\psi,\pi) \in U$ for which $\mathrm{comp}_\pi(\psi H,\Delta) = \hat{\psi}\mathrm{comp}_I(H,\Delta)$.

Those pairs $(\psi,\pi) \in U$ for which $\mathrm{comp}_\pi(\psi H,\Delta)$ is empty do not appear at all in W. Conceptually we have just run $\mathrm{comp}_\pi(\psi H,\Delta)$ in parallel for each of the $(\psi\ ,\ \pi)$ in U and have recorded the results in K and W.

To compute $\overline{G}_i$ we wish to find those elements of $\overline{G}_{i-1}$ which are compatible with each element of G_i. The initial call is $\mathrm{COMP}(\overline{G}_{i-1}, (\{I\} \times G_i), \overline{pr}_{i-1}V)$ where I denotes the identity permutation in $\overline{G}_{i-1}$. The reorganized algorithm follows:

```
COMP(H,U,Δ):
(where $H \le \bar{G}_{i-1}$, $\Delta \subseteq \overline{pr}_{i-1}V$ is H-stable, $U \subseteq \bar{G}_{i-1} \times G_i$)
begin
  if $|\Delta| = 1$ then begin
    Comment: $\Delta = \{x\}$;
    $W = \{ (\psi,\pi) \in U : \forall y \in pr_i V \; |P_{x,y}| = |P_{\psi x, \pi y}| \}$
    return(H,W);
  end
  else if H is intransitive on Δ then begin
    Find $\Gamma_1,\dots,\Gamma_d$ the orbits of H;
    return (COMP(...COMP(H,U,$\Gamma_1$),...,$\Gamma_d$));
  end
  else begin
    Consider the next $\Psi_j$ $(1 \le j \le i-1)$ where $\Psi_j$
    partitions Δ nontrivially into $\Gamma_1,\dots,\Gamma_d$;
    Find $H' \le H$ stabilizing each of the classes
    $\Gamma_1,\dots,\Gamma_d$;
    Comment: $H = \varphi_1 H' + \varphi_2 H' + \dots + \varphi_q H'$   $(q \le d^m)$;
    for each $(\psi,\pi) \in U$ do
      Replace $(\psi,\pi)$ by the q-tuple
      $[(\psi\varphi_1,\pi),\dots,(\psi\varphi_q,\pi)]$ in U
    (K,U') = COMP(...COMP(H',U,$\Gamma_1$),...,$\Gamma_d$);
    Comment: Glue cosets together;
    if $U' \ne \{\}$ then begin
      Let $[(\psi_1,\pi),\dots,(\psi_s,\pi)] \subseteq U$ be the nonempty
      remainder of any q-tuple created above;
      Add $\{\psi_1^{-1}\psi_2, \dots, \psi_1^{-1}\psi_s\}$ to K.
    end;
    for each nonempty remainder of a previous q-
    tuple $[(\psi_1,\pi),\dots,(\psi_s,\pi)] \subseteq U$ do begin
      Comment: Select an element of the tuple as
      the new representative.
      Replace the s-tuple by $(\psi_1,\pi)$;
    end.
    Convert K to a proper generating set;
    return(K,U').
  end
end
```

This reorganization was developed by Hoffmann to improve the time complexity of trivalent graph isomorphism [Hof 81]. For the most part, the correctness of this version is evident from the earlier version of "comp". The notable exception is the process of "gluing cosets together." The correctness of this operation follows from the next result, adapted from the discussion in [Hof 81] or [Hof 82, pp. 149-157].

Lemma 5.7 (Luks, Hoffmann) Suppose $H = \varphi_1 H' + \dots + \varphi_q H'$, and for some s, $1 \le s \le q$:

$$\psi_j \in comp_\pi(\psi\varphi_j H') \quad \text{for } j = 1,\dots,s$$
$$comp_\pi(\psi\varphi_j H') = \{\} \quad \text{for } j = s+1,\dots,q$$

then

$$comp_I(H) = <\psi_1^{-1}\psi_2,\dots,\psi_1^{-1}\psi_s, comp_I(H')>$$

where <K> denotes the group generated by the elements of K.

Analysis

Consider the structure of the recursive calls generated by COMP. A call to COMP(...,Δ) results in recursive calls to COMP(...,Γ_1),...,COMP(...Γ_d) for $\Gamma_1 + \dots + \Gamma_d = \Delta$. The execution sequence of recursive calls is just a depth first traversal of a tree whose vertices correspond to subsets of $\overline{pr}_{i-1}V$ and whose leaves correspond to singleton subsets. Note that each division of Δ into Γ's is nontrivial, that is, each interior vertex of this tree has at least two descendents. Thus the total number of vertices in the tree, and therefore the total number of recursive calls, is less than $2\,|\overline{pr}_{i-1}V| \le 2n$.

The complexity of each recursive call depends in part on the number of elements in U, which we now estimate:

Lemma 5.7 Suppose the call COMP(H,U,Γ) has ensued from the initial call COMP($\bar{G}_{i-1}$, $(\{1\} \times G_i)$, $\overline{pr}_{i-1}V$). Then $|U| \le n^m(|\overline{pr}_{i-1}V| / |\Gamma|)^m$.

Proof

(By induction on the depth of recursion.) Since $|G_i| \le n^m$ this is true for depth 0.

Before proving the induction step notice that the size of the coset list returned is never larger than the size of the coset list on entry. So it suffices to show that in the series of calls $\mathrm{COMP}(\ldots(\mathrm{COMP}(H,U,\Gamma_1),\ldots),\Gamma_d)$ the initial U satisfies the size criterion for each Γ_k, $k=1,\ldots,d$.

Suppose that the call to $\mathrm{COMP}(H,U,\Gamma)$ arose from $\mathrm{COMP}(G,W,\Delta)$ where $|W| \le n^m(|\overline{pr}_{i-1}V|/|\Delta|)^m$. Clearly $\Gamma \subset \Delta$. If the call to $\mathrm{COMP}(H,U,\Gamma)$ arose from the intransitive case then

$$\begin{aligned} |U| &= |W| \\ &\le n^m(|\overline{pr}_{i-1}V|/|\Delta|)^m \\ &\le n^m(|\overline{pr}_{i-1}V|/|\Gamma|)^m \end{aligned}$$

If the call arose from the transitive case then Γ is one of d equal sized blocks forming a system of imprimitivity in Δ, so $|\Delta| = d\cdot|\Gamma|$. $|U| = |W|\cdot q$ where $q = |G:H|$. By Theorem 5.4 $|G:H| \le d^m$. Therefore

$$\begin{aligned} |U| &\le |W|\cdot d^m \\ &\le n^m(|\overline{pr}_{i-1}V|/|\Delta|)^m(|\Delta|/|\Gamma|)^m \\ &\le n^m(|\overline{pr}_{i-1}V|/|\Gamma|)^m \end{aligned}$$

□

Since $|pr_{i-1}V| \le n$, in each recursive call $|U| \le n^{2m}$. At the base of the recursion the construction of W requires $O(|U|\cdot n)$ steps. The cost of expanding U into p-tuples and later contracting the returned set W' is likewise bounded by the size of the expanded set times n. We defer charging the complexity of this operation to the subsequent call to "COMP" with the expanded set. By doing this the cost of processing U is always bounded by $O(|U|\cdot n) = O(n^{2m+1})$, for each recursive call.

The other sources of effort during each recursive call are the group operations. Recall that H is represented by a list of at most n^2 generating elements. The orbits of H can be calculated in $O(n^3)$ time by existing techniques [Hof 82, p. 46]. The partition of Δ into blocks of imprimitivity requires $O(n)$ time. The set K, constructed in the transitive case, may contain as many as n^2+n^m elements after gluing the cosets together, but by the standard "sift and close" method [FHL 80b], $O(n^{\max(m+2,6)})$ time suffices to reduce K to a proper generating set.

Finally we must analyze the construction of a generating set for H' from H in the transitive case. H' is constructed by the "tower of groups" method [FHL 80b]. The time to construct a generating set is $O((T+n^2)^2n(C+n))$ where $T = |H:H'| \le n^m$ and C is the time to decide for $\varphi \in H$ whether the group tower has already encountered some $\psi \in H$ such that $\varphi H' = \psi H'$.

To bound C we provide an efficient method of recording the cosets of H' in H. These cosets are in 1-1 correspondence with the permutations of Δ/Ψ_j induced by H. By Lemma 3.2 each permutation is determined by the image of a base $B = \{b_1,\ldots,b_m\} \subset \Delta/\Psi_j$. We construct an m-dimensional matrix M indexed over Δ/Ψ_j and identify the coset φH with the entry $M[\varphi b_1,\ldots,\varphi b_m]$. The entries of M can be initialized in $O(n^m)$ time and the entry of M corresponding to φH can be located in $O(m)$ time.

With the aid of the matrix M, $C=O(m)$ so the generators for H' can be constructed in $O((n^m+n^2)^2n(m+n)) = O(n^{\max(2m+2,6)})$ time. Combining all the results of the preceding discussion $\mathrm{COMP}(\overline{G}_{i-1}, (\{I\}\times G_i), \overline{pr}_{i-1}V)$ can be computed in $O(n^{\max(2m+3,7)})$ time.

One remaining detail is the extension of $\mathrm{COMP}(\overline{G}_{i-1}, (\{I\}\times G_i), \overline{pr}_{i-1}V) = (K,W)$ to $\overline{G}_i$. By definition K is a generating set for $\mathrm{comp}_i(\overline{G}_{i-1})$. So $\overline{G}_i$ is generated from the set:

$$\mathrm{ext}(K,I) \cup \{\mathrm{ext}(\varphi,\pi) \mid (\varphi,\pi) \in W\}$$

This set may contain n^2+n^m elements and so an additional $O(n^{\max(m+2,6)})$ time is required to produce a proper generating set for $\overline{G}_i$ by the "sift and close" procedure.

After iterating over the $O(n)$ eigenspaces the cost of computing Aut(X) is clearly $O(n^{\max(2m+4,8)})$ plus the initial expense of computing the eigenvectors, the projection functions and the groups G_i. Since the linear algebra part contributes $O(n^{m+c})$ the total complexity is $O(n^{2m+c})$.

One Unbounded Multiplicity

The following interesting observation on this algorithm was pointed out to the authors by Christoph Hoffmann. Suppose an undirected graph has r-1 distinct eigenvalues each of bounded multiplicity and one eigenvalue whose multiplicity is unbounded. The automorphism group of this graph can be computed in polynomial time as follows. The group $\bar{G}_{r-1}$ can be computed as before in polynomial time, and by Lemma 5.1 the group H of unit vector permutations inducing $\bar{G}_{r-1}$ can easily be found. The group H consists of orthogonal transformations under which $\bar{S}_{r-1}$ is invariant, hence S_r, the eigenspace of unbounded dimension whose orthogonal complement is $\bar{S}_{r-1}$, is also H-invariant. By Lemma 3.1, H = Aut(X). As a consequence of this observation the isomorphism of graphs in which all but one of the eigenvalue multiplicities are bounded by a constant can be tested in polynomial time.

6. Conclusions

Two polynomial time algorithms have been presented which find the automorphism group of a graph with bounded eigenvalue multiplicity. The two algorithms presented provide an interesting continuity between the "tower of groups" type algorithms for graph isomorphism [Bab 79, FHL 80a, Hof 80a] and the "recursion through systems of imprimitivity" algorithms [Luk 80, Bab 81]. We remark that the tower of groups method was originally designed precisely in order to complete the proof of the result of this paper. On the other hand the second algorithm is interesting because it employs essentially the same group theoretic methods as Luks' algorithm for the isomorphism of graphs with bounded valence. This raises hopes for a common generalization of the problems of isomorphism for graphs of bounded valence and bounded eigenvalue multiplicity. It is a problem of considerable interest to find a more general parameter of graphs so that boundedness of this parameter would permit polynomial time isomorphism testing on the one hand, and it would generalize the boundedness of such parameters as valency, genus, and multiplicity of eigenvalues on the other hand.

Acknowledgements

It is a pleasure to thank Christoph Hoffmann for his invaluable contributions to Section 5. The authors would also like to thank Harry Lewis and Ron Graham for their many efforts in arranging this collaboration.

References

[Bab 79]
Babai, L., "Monte Carlo algorithms in graph isomorphism testing," preprint, 1979.

[Bab 80]
Babai, L., "Isomorphism testing and symmetry of graphs," *Combinatorics 79* (M. Deza and I. G. Rosenberg, eds.) Ann. Discr. Math. 8, 1980, 101-109.

[Bab 81]
Babai, L., "Moderately exponential bound for isomorphism," *Fundamentals of Computation Theory* (Proc. Conf. FCT '81, Szeged, F. Gécseg, ed.) Lect. Notes in Comp. Sci. 117, Springer, 1981, 34-50.

[Big 74]
Biggs, Norman, *Algebraic Graph Theory*, Cambridge University Press, 1974.

[CDS 80]
Cvetković, D., M. Doob and H. Sachs, *Spectra of Graphs, Theory and Application*, Academic Press, 1980.

[FHL 80a]
Furst, M., J. Hopcroft and E. M. Luks, "A subexponential algorithm for trivalent graph isomorphism," Tech. Rept. 80-426, Comp. Sci. Dept., Cornell Univ., 1980.

[FHL 80b]
Furst, M., J. Hopcroft and E. M. Luks, "Polynomial time algorithms for permutation groups," *Proc. 21st IEEE FOCS Symp.*, 1980, 36-41.

[FMR 79]
Filotti, I., G. Miller and J. Reif, "On determining the genus of a graph in $O(V^{O(g)})$ steps," *Proc. 11th ACM STOC Symp.*, 1979, 27-37

[F&M 80]
Filotti, I. and J. Mayer, "A polynomial time algorithm for determining isomorphism of graphs of fixed genus," *Proc. 12th ACM STOC Symp.*, 1980, 236-243.