Topics in Graph Automorphisms

Derrick Stolee
University of Nebraska-Lincoln
s-dstolee1@math.unl.edu

February 15, 2010

Abstract

The symmetry of a graph is measured by its automorphism group: the set of permutations of the vertices so that all edges and non-edges are preserved. There are natural questions which arise when considering the automorphism group and there are several interesting results in this area that are not well-known. This talk presents some of these results and maybe even proves one or two. First, we will prove that almost all graphs have trivial automorphism group. Second, we will briefly discuss the relation of the graph automorphism and group intersection problems. Then, we will discuss Babai's constrcution that any finite group with n elements can be represented by a graph on $2n$ vertices (other than three exceptions). Finally, we will mention there exists a subgroup of S_n that is the automorphism group of no graph of size less than $\frac{1}{2}\binom{n}{\frac{1}{2}n}$.

1 Almost all graphs are rigid

Before we can begin the proof of this fact, recall the Chernoff-Hoeffding bounds.

Theorem 1.1 ([DP09]). *Let $X = \sum_{i=1}^{n} X_i$ be a sum of identically distributed independent random variables X_i where $\Pr(X_i = 1) = p, \Pr(X_i = 0) = q = 1 - p$. Then, we have the following* relative Chernoff-Hoeffding bound *for all $\varepsilon > 0$:*

$$\Pr[X < (1-\varepsilon)np] \leq e^{-np\varepsilon^2/2}, \qquad \Pr[X > (1+\varepsilon)np] \leq e^{-np\varepsilon^2/2}$$

1.1 Properties of $G(n,p)$

Lemma 1.2. *Let ε be a function on n with $\varepsilon(n) > 0$. Then, the probability that G, distributed as $G(n+1,p)$, has all vertices of degree $\deg v \in ((1-\varepsilon)np, (1+\varepsilon)np)$ is at least $1 - 2(n+1)e^{-\frac{np\varepsilon^2}{2}}$.*

Proof. Let $X_{i,j}$ be the indicator variable for the edge $\{i,j\}$ appearing in $G(n+1,p)$ $(1 \leq i < j \leq n+1)$. The expected value is p. By linearity of expectation,

$$\mathbb{E}[\deg i] = \sum_{j \neq i} \mathbb{E}[X_{i,j}] = np.$$

By the Chernoff bound,

$$\Pr[\deg i < (1-\varepsilon)np] \leq e^{-np\varepsilon^2/2}.$$

And similarly,

$$\Pr[\deg i > (1+\varepsilon)np] \leq e^{-np\varepsilon^2/2}.$$

Hence,

$$\Pr[\deg i \notin ((1-\varepsilon)np, (1+\varepsilon)np)] \leq 2e^{-np\varepsilon^2/2}.$$

Thus, the probability that all vertices have degree within the requested bounds is at least

$$1 - \sum_i 2e^{np\varepsilon^2/2} = 1 - 2(n+1)e^{-\frac{np\varepsilon^2}{2}}. \qquad \square$$

1.2 Rigidity of $G(n,p)$

Theorem 1.3 ([Bol01]). *Let $G \sim G_{n,p}$ for constant p and let $\varepsilon > 0$. The graph G is rigid with probability*

$$\Pr[\mathrm{Aut}(G) \cong I] \geq 1 - 2ne^{-(n-1)p\varepsilon^2/2} - n^2 2^{1-(n-1)p(1-\varepsilon)},$$

which tends to 1 as n tends to infinity.

Proof. Consider G having the property that all vertices $v \in V(G)$ have degree bounds $(1-\varepsilon)np \leq \deg v \leq (1+\varepsilon)np$. If G has automorphism group $\Gamma \leq S_n$, then Γ acts on the pairs of vertices. This partitions them in to *pair orbits* that either consist entirely of edges or have no edges at all. If this partition has k parts, then at most 2^k graphs have this partition and as such has automorphism group Γ.

We will argue that if Γ is non-trivial, then k is at most $\binom{n}{2} - (n-1)p(1-\varepsilon) + 1$. Most clearly, a non-trivial group has a partition σ that moves some vertex x to a different vertex y. By this action, the edges of x are mapped to edges of y. These edges are therefore not in singleton partitions (except possibly for the edge xy if it exists). But since there are at least $(n-1)p(1-\varepsilon) - 1$ edges incident to y that do not form their own orbits, the number of orbits is at most $\binom{n}{2} - (n-1)p(1-\varepsilon) + 1$.

So, the portions of graphs with an automorphism that takes x to y is at most

$$\frac{2^{\binom{n}{2}-(n-1)p(1-\varepsilon)+1}}{2^{\binom{n}{2}}} = 2^{1-(n-1)p(1-\varepsilon)}.$$

The sum over all pairs x, y gives the portion with non-trivial automorphisms is at most $n^2 2^{1-(n-1)p(1-\varepsilon)}$ (using $\binom{n}{2} \leq n^2$). This probability is conditioned on the bounded degree. Removing the condition gives a probability of rigidity being at least

$$\begin{aligned}\left[1 - 2ne^{-(n-1)p\varepsilon^2/2}\right] \cdot \left[1 - n^2 2^{1-(n-1)p(1-\varepsilon)}\right] &= 1 - 2ne^{-(n-1)p\varepsilon^2/2} - n^2 2^{1-(n-1)p(1-\varepsilon)} \\ &\quad + 2n^2 e^{\ln 2 - (n-1)p[\varepsilon^2/2 + \ln 2(1-\varepsilon)]} \\ &\geq 1 - 2ne^{-(n-1)p\varepsilon^2/2} - n^2 2^{1-(n-1)p(1-\varepsilon)}. \qquad \square\end{aligned}$$

2 Group Intersection and Graph Automorphism

The problem of finding the intersection of two groups is at least as hard as finding the automorphism group of a graph. Showing the reverse hardness is very difficult, if possible at all. This section defines these problems and discuss how hardness may be shown.

2.1 Group Intersection

Let X be a set of elements in S_m, the permutation group on ms elements. This set X generates a group $\langle\, X \,\rangle$ as the set of all finite products of elements in X and their inverses. Note that this includes the empty product which is taken to be the identity element. Here, X is a *generating set* and the group $\langle\, X \,\rangle$ is the group *generated by X*.

Given two generating sets X_1, X_2, the groups $\langle\, X_1 \,\rangle$ and $\langle\, X_2 \,\rangle$ intersect at least at the identity element. Checking if the intersection is trivial defines the following decision problem.

Definition 1 ([Hof82]). The decision problem of Group Intersection is the language GrpInt_D defined as

$$\mathrm{GrpInt}_D = \{[0^m, X_1, X_2] : \langle X_1 \rangle \cap \langle X_2 \rangle \neq \{\varepsilon\}\}.$$

Here, the input is interpreted as generating sets $X_1, X_2 \subseteq S_m$ and its size is $n = m + (|X_1| + |X_2|) \log m$.

A polynomial on the input of GrpInt_D is taken as a function in $\mathrm{poly}(m, |X_1|, |X_2|)$. This decision problem has a simple NPalgorithm: non-deterministically choose a non-trivial element x in S_m and use the polynomial-time algorithm for group ownership to check that $x \in \langle X_1 \rangle$ and $x \in \langle X_2 \rangle$. If x in both, accept.

While the decision problem has a clear NPalgorithm, the problem of *producing* explicit generators X_3 that generate $\langle X_1 \rangle \cap \langle X_2 \rangle$ seems much harder.

Definition 2. Producing generators for the intersection of a group is the problem GrpInt_P:

$$[0^m, X_1, X_2] \overset{\mathrm{GrpInt}_P}{\longrightarrow} [X_3],$$

with the condition that $\langle X_3 \rangle = \langle X_1 \rangle \cap \langle X_2 \rangle$.

The simplest non-deterministic algorithm for this problem requires alternation. First, non-deterministically choose X_3 and test that $X_3 \subseteq \langle X_1 \rangle \cap \langle X_2 \rangle$. This can be done using an NP process. However, to show that $\langle X_3 \rangle \supseteq \langle X_1 \rangle \cap \langle X_2 \rangle$, an element x of S_m must be chosen non-deterministically, verified to be in $\langle X_1 \rangle \cap \langle X_2 \rangle$, and then verified to be in $\langle X_3 \rangle$. If the first verification fails, return failure (not reject or accept). If the first verification succeeds, reject if the second verification fails. This is a coNP process as all choices of x will return failure or accept if X_3 generates the intersection, but at least one path will reject if it does not.

Hence, $\mathrm{GrpInt}_P \in \mathrm{NP}^{\mathrm{coNP}}$.

2.2 Graph Automorphism

Given a graph G, the *automorphism group* $\mathrm{Aut}(G)$ is the set of permutations on the vertex set $V(G)$ that preserve adjacencies and non-adjacencies. Explicitly,

$$\mathrm{Aut}(G) = \{\sigma \in \mathrm{Sym}(V(G)) : \forall v, u \in V(G), \{\sigma(v), \sigma(u)\} \in E(G) \Leftrightarrow \{v, u\} \in E(G)\}.$$

This gives an immediate decision problem on all graphs.

Definition 3 ([Hof82]). The decision problem of Graph Automorphism is GA_D defined as

$$\mathrm{GA}_D = \{[G] : \mathrm{Aut}(G) \neq \{\varepsilon\}\}.$$

Here, the input is a graph G given as an adjacency matrix. The input size is the number of vertices $n = |V(G)|$, even though the encoding is size n^2.

Again, this problem is clearly in NP. Non-deterministically choose a non-trivial element $\sigma \in \mathrm{Sym}(V(G))$ and check if it preserves adjacencies and non-adjacencies in G. If so, $\sigma \in \mathrm{Aut}(G) \neq \{\varepsilon\}$. This leads directly to the production version of the problem.

Definition 4. Producing generators for the automorphism of a graph is the problem GA_P:

$$[G] \overset{\mathrm{GA}_P}{\longrightarrow} [X],$$

where $\langle X \rangle = \mathrm{Aut}(G) \subseteq \mathrm{Sym}(V(G))$.

Note that these definitions are very similar to those of GrpInt_D and GrpInt_P. Also, it seems GrpInt_D has the same upper bound on its complexity. However, GA_P has a different complexity. In fact, GA_P is polynomial-time Turing reducible to the decision problem of graph isomorphism, GI_D.

2.3 Reductions

A *many-one reduction* from a decision problem A to a decision problem B is a function $f : \Sigma^* \to \Sigma^*$ so that $f(\mathbf{x}) \in B$ if and only if $\mathbf{x} \in A$. This can be interpreted as an input manipulation function. Propose that a solver for B is given. The function f can be used to convert the input $\mathbf{x}$ for problem A into input $f(\mathbf{x})$ suitable for the B-solver. This solver then computes an answer for $f(\mathbf{x})$ on B which is the correct answer for $\mathbf{x}$ on A. This proves that the complexity of A is *at most* the complexity of f plus the complexity of B. If f is computed in log-space, then the ordering of their complexity is denoted $A \leq_m^{\mathrm{L}} B$. If f is computed in polynomial time, then the ordering is denoted $A \leq_m^{\mathrm{P}} B$.

A many-one reduction from a production problem A to a production problem B is a pair of functions $f, g : \Sigma^* \to \Sigma*$ so that $f(\mathbf{x}) \xrightarrow{B} \mathbf{y}$ implies $\mathbf{x} \xrightarrow{A} g(\mathbf{y})$. The function f acts as an input converter, similar to the decision reduction. However, the outputs of a B-solver may not fit exactly the format of an A-solver, so the function g converts the B output into format fit for A. Hence, if a B-solver exists, the following chain will solve A:

$$\begin{tikzcd}
\mathbf{x} \arrow[r] \arrow[rrr, bend right, "A"'] & f(\mathbf{x}) \arrow[r, "B"] & \mathbf{y} \arrow[r] & g(\mathbf{y})
\end{tikzcd}$$

The complexity of the function f will give the same orderings $\leq_m^{\mathrm{L}}$ and $\leq_m^{\mathrm{P}}$ as before. The use of the function g could be a method for "cheating." Instead of allowing computation to be done in g, it will need to be considered a well-defined injection (with respect to equivalence classes on both sides of the function). This enforces that the reduction needs to use the problem B to produce an answer that *almost immediately* gives an answer to A.

Consider the following theorem as a common use of these reductions.

Theorem 2.1 ([Hof82]). $\mathrm{GA}_P \leq_m^{\mathrm{L}} \mathrm{GrpInt}_P$.

Ridiculously poor sketch of proof. $f([G]) = [0^{\binom{n}{2}}, \mathrm{Sym}(V(G))', \mathrm{Sym}(E(G)) \times \mathrm{Sym}(\overline{E(G)})]$. $g : \mathrm{Sym}(V(G))' \to \mathrm{Sym}(V(G))$. □

3 Graphs with Given Automorphism Group

Definition 5 ([Fru39]). Given a group Γ generated by elements $S = \{\sigma_i\}_{i \in I}$, the *Cayley graph* $C(\Gamma, S) = (\Gamma, E)$ is the edge-labeled directed graph with vertex set Γ and an edge $x \to y$ with label σ if $\sigma \in S$ and $y = \sigma x$.

Theorem 3.1. *Let Γ be a finite group generated by S with $n = |\Gamma|$. The Cayley graph $C(\Gamma, S)$ has automorphism group Γ. The labeled edges can be replaced with simple undirected gadgets to form a graph $C'(\Gamma, S)$ of order $O(|\Gamma| \log |S|)$ with automorphism group isomorphic to Γ.*

For a while, this stood as the best upper bound on the size of an undirected graph with given automorphism group. Then, Sabidussi presented in 1958 a complete characterization of the minimum-order graphs with a k-order cyclic automorphism group for each $k \geq 2$.

Definition 6. Let Γ be a finite group. We define the minimum graph order $\alpha(\Gamma)$ to be

$$\alpha(\Gamma) = \min\{n(G) : G = (V, E), \mathrm{Aut}(G) \cong \Gamma\},$$

the minimum order of a simple graph with automorphism group isomorphic to Γ.

Lemma 3.2 ([Sab59]). *Let $m \geq 2$ be an integer.*

$$\alpha(\mathbb{Z}_m) = \begin{cases} 2 & \text{if } m = 2, \\ 3m & \text{if } m \in \{3, 4, 5\}, \\ 2m & \text{if } m = p^3 \geq 7, p \text{ prime}, \\ \sum_{i=1}^{t} \alpha(\mathbb{Z}_{p_i^{e_i}}) & \text{where } m = \prod_{i=1}^{t} p_i^{e_i} \text{ for } p_1, \dots, p_t \text{ distinct primes.} \end{cases}$$

Proof. We skip the minimality, but instead focus on constructions that achieve these bounds.

Note that $\mathbb{Z}_2 \cong \mathrm{Aut}(K_2)$. Moreover, if $G_1, \ldots, G_t$ are graphs with $\mathrm{Aut}(G_i) \cong \mathbb{Z}_{p_i^{e_i}}$ and $|V(G_i)| = \alpha(\mathbb{Z}_{p_i^{e_i}})$, for distinct primes $p_1, \ldots, p_t$, then their union $G = \cup_{i=1}^t G_i$ has automorphism group

$$\mathrm{Aut}(G) \cong \prod_{i=1}^t \mathbb{Z}_{p_i^{e_i}} \cong \mathbb{Z}_{p_1^{e_1} \cdots p_t^{e_t}}.$$

Set $m \in \{3, 4, 5\}$. We construct G with $\mathrm{Aut}(G) \cong \mathbb{Z}_m$ and $|V(G)| = 3m$. Start with the cycle C_m. Subdivide each edge and insert $L(C_m) \cong C_m$ as the induced subgraph of these new vertices. Now, the original cycle has length $2m$. Subdivide every other edge of this cycle, and connect these m new vertices in an m-cycle. The vertices in the outer cycle of length $3m$ can be labeled $x_1y_1z_1x_2y_2z_2 \ldots x_my_mz_m$ in order. This gives that the vertices x_i have degree two, the y_i are in a cycle $Y = y_1 \ldots y_m$ and the z_i are in a cycle $Z = z_1 \ldots z_m$. By the rotation $x_i \mapsto x_{i+1}$, we see that all indices are adjusted by one, giving the cyclic action of $\mathbb{Z}_m$.

Consider the induced cycles Y and Z and an automorphism $\pi \in \mathrm{Aut}(G)$. If $\pi(Y) = Y$, then π induces an action on Y from D_m, the dihedral group on m points. However, if π is a reflection in D_m, then π does not extend to G.

Now, if $m = p^e \geq 7$, we can construct G from an m-cycle $C = c_1 \ldots c_m$ and and m-independent set $X = x_1 \ldots x_m$. Consider all indices modulo m.

Note that the edges c_ic_{i+1} are in C. Also add these edges:

$$c_ix_i, \quad c_{i+2}x_i, \quad c_{i+3}x_i.$$

Since $m \geq 7$, we see that each of $i, i+2$, and $i+3$ define unique vertices. Also, $c_{i+1}x_i$ is *not* an edge in G.

Now, all vertices in X have degree three while each in C has degree five. Hence, X and C are stabilized by $\mathrm{Aut}(G)$. Moreover, since C is stabilized and $G[C] \cong C_m$, $\mathrm{Aut}(G)$ is isomorphic to a subgroup of D_m, the dihedral group on m elements. Note that the construction gives an automorphism $c_i \mapsto c_{i+1}$ and $x_i \mapsto x_{i+1}$. So, $\mathbb{Z}_m \leq \mathrm{Aut}(G) \leq D_m$.

The vertex x_i acts as an orientation on the quadruple $c_ic_{i+1}c_{i+2}c_{i+3}$, since the induced subgraph of $N[x_i]$ is a triangle with a leaf. Hence, we can determine an orientation on each edge c_ic_{i+1}, as c_{i+1} is the vertex between c_i (the leaf in $N[x_i]$) and c_{i+2} (one of the vertices in the triangle of $N[x_i]$) and recover the increasing order of the indices. Hence, $\mathrm{Aut}(G) \cong \mathrm{Aut}(\vec{C}_m) \cong \mathbb{Z}_m$, where $\vec{C}_m$ is the directed cycle on m vertices. □

It wasn't until 1974 when László Babai proved that those three cyclic groups were the only finite groups that required three vertices per element. All other finite groups with n elements are representable by a graph of order $2n$.

Theorem 3.3 ([Bab74])**.** *If Γ is a finite group not isomorphic to $\mathbb{Z}_3, \mathbb{Z}_4$, or $\mathbb{Z}_5$, then there exists a graph G with $\mathrm{Aut}(G) \cong \Gamma$ and $|V(G)| \leq 2|\Gamma|$.*

Proof. If Γ is cyclic, we are done by Sabidussi's theorem.

If $\Gamma \cong V_4$, we have $V_4 \cong \mathrm{Aut}(K_4 - e)$.

Now, assume $|\Gamma| > 6$. Let $S = \{\alpha_1, \ldots, \alpha_t\}$ be a minimal generating set of Γ. Create two graphs $G_1 = (\Gamma, E_1), G_2 = (\Gamma, E_2)$.

In G_1, for each element $\gamma \in \Gamma$ and each $i \in \{1, \ldots, t-1\}$, place an edge between $\alpha_i\gamma$ and $\alpha_{i+1}\gamma$. Note that each vertex set $\{\alpha_1\gamma, \ldots, \alpha_t\gamma\}$ is a path in G_1. If there exists an edge between $\alpha_i\gamma$ and $\alpha_j\gamma$ with $j > i+1$, this contradicts minimality of S, since there exists $\gamma' \in \Gamma, \ell \in \{1, \ldots, t-1\}$ so that

$$\alpha_i\gamma = \alpha_\ell\gamma', \quad \alpha_j\gamma = \alpha_{\ell+1}\gamma'.$$

This gives $\gamma' = \alpha_{\ell+1}^{-1}\alpha_j\gamma$ and hence $\alpha_i = \alpha_\ell\alpha_{\ell+1}^{-1}\alpha_j$.

In G_2, for each element $\gamma \in \Gamma$, place an edge between γ and $\alpha_1\gamma$.

Both G_s ($s \in \{1, 2\}$) are regular with degree d_s. We have $d_2 = 2$. If $d_1 = d_2$, then these graphs have the same degree.

Define G_3 by case: if $d_1 \neq d_2$, then $G_3 = G_2$; if $d_1 = d_2$, then $G_3 = \overline{G_2}$. Note that G_3 is regular with degree $d_3 \neq d_1$, since if $d_1 = d_2$, then $d_3 = n - 1 - d_2 = n - 3 > 6 - 3 = 4 > d_2 = d_1$.

Define $G = (\Gamma \times \{1, 3\}, E)$ where $E = E'_1 \cup (E_3 \times \{3\}) \cup E'$, where

$$\begin{aligned} E'_s &= \{\{(\gamma, s), (\delta, s)\} : \{\gamma, \delta\} \in E_s\}, \\ E' &= \{\{(\gamma, 1), (\gamma, 3)\} : \gamma \in \Gamma\} \\ &\quad \cup \{\{(\gamma, 3), (\alpha_i\gamma, 1)\} : \gamma \in \Gamma, i \in \{1, \ldots, t\}\}. \end{aligned}$$

Claim 3.1. $\mathrm{Aut}(G) \cong \Gamma$.

First, note that Γ is isomorphic to a subgroup of $\mathrm{Aut}(G)$. Given $\delta \in \Gamma$, $\pi_\delta : V(G) \to V(G)$ is defined as

$$\pi_\delta(\gamma, s) = (\gamma\delta, s) \qquad\qquad \forall \gamma \in \Gamma, s \in \{1, 3\}$$

Note that π_δ defines a bijection on each edge set E'_1, E'_3, E' as

$$\begin{aligned} \{(\alpha_i\gamma, 1), (\alpha_{i+1}\gamma, 1)\} &\xmapsto{\pi_\delta} \{(\alpha_i\gamma\delta, 1), (\alpha_{i+1}\gamma\delta, 1)\} && (E'_1) \\ \{(\gamma, 3), (\alpha_1\gamma, 3)\} &\xmapsto{\pi_\delta} \{(\gamma\delta, 3), (\alpha_1\gamma\delta, 3)\} && (E'_3 \text{ or } \overline{E'_3}) \\ \{(\gamma, 1), (\gamma, 3)\} &\xmapsto{\pi_\delta} \{(\gamma\delta, 1), (\gamma\delta, 3)\} && (E') \\ \{(\gamma, 3), (\alpha_i\gamma, 1)\} &\xmapsto{\pi_\delta} \{(\gamma\delta, 3), (\alpha_i\gamma\delta, 1)\} && (E') \end{aligned}$$

It remains to show any permutation in $\mathrm{Aut}(G)$ is represented by π_δ for some $\delta \in \Gamma$.

Let $\gamma \in \Gamma$ be any element. Define the subgraph A_γ be the induced subgraph of G given by $(\gamma, 3), (\gamma, 1), (\alpha_1\gamma, 1), \ldots, (\alpha_t\gamma, 1)$. As mentioned previously, the vertices $(\alpha_1\gamma, 1), \ldots, (\alpha_t\gamma, 1)$ induce a path in G. It is also true that there is no edge from $(\gamma, 1)$ to $(\alpha_i\gamma, 1)$ for any $i \in \{1, \ldots, t\}$. If such an i existed, then there exists an $\ell \in \{1, \ldots, t-1\}$ and $\gamma' \in \Gamma$ ($\gamma' \neq \gamma$) so that

$$\gamma = \alpha_\ell\gamma', \quad \alpha_i\gamma = \alpha_{\ell+1}\gamma'.$$

However, this implies $\alpha_i = \alpha_{\ell+1}\alpha_\ell^{-1}$, which contradicts minimality of S.

Hence, $(\gamma, 1)$ is a leaf in A_γ.

Let $\pi \in \mathrm{Aut}(G)$ be a permutation of $V(G)$. Consider an element $\gamma \in \Gamma$ and $\gamma' = \pi(\gamma)$. Since $\pi(A_\gamma) = A_{\gamma'}$, and $(\gamma, 1)$ is the only leaf in A_γ, $\pi(\gamma, 1) = \pi(\gamma', 1)$ since $(\gamma', 1)$ the only leaf in $A_{\gamma'}$.

So, π can be considered as a permutation of Γ that also acts on G. Let π be such a permutation given by a non-trivial automorphism of G.

Now, let γ be any element with $\pi(\gamma) \neq \gamma$ and define $\delta = \gamma^{-1}\pi(\gamma)$.

Claim 3.2. *For any element $\gamma' \in \Gamma$, $\pi(\gamma') = \gamma'\delta$.*

It is sufficient to prove that if $\pi(\gamma) = \gamma\delta$, then for all $i \in \{1, \ldots, t\}$ has $\pi(\alpha_i\gamma) = \alpha_i\gamma\delta$. If this is true, then for all $\gamma' \in \Gamma$, the sequence of generators $\alpha_{j_1} \cdots \alpha_{j_k} = \gamma'\gamma^{-1}$ gives $\gamma' = \alpha_{j_1} \cdots \alpha_{j_k}\gamma$ and iteration on the number of generators in the right-hand-side product gives $\pi(\gamma') = \gamma'\delta$.

Since the only vertex $(\alpha_i\gamma, 1)$ in A_γ that has $(\alpha_i\gamma, 3)$ adjacent to $(\gamma, 3)$ is $(\alpha_1\gamma, 1)$. Hence, $\pi(\alpha_1\gamma) = \gamma\delta$. Moreover, the path $(\alpha_1\gamma, 1)(\alpha_2\gamma, 1)\ldots(\alpha_t\gamma, 1)$ in A_γ is now embedded uniquely into $\pi(A_\gamma) = A_{\gamma\delta}$ as $(\alpha_1\gamma\delta, 1)(\alpha_2\gamma\delta, 1)\ldots(\alpha_t\gamma\delta, 1)$. This proves the claim. □

4 Other Automorphism Results

Based on this construction of Babai, the worst-case order of a graph G with automorphism group Γ is $O(n)$ where $n = |\Gamma|$. Unfortunately, we cannot hope for better asymptotics than that (or much better constants, even), since there is a very close lower bound for the alternating group.

Theorem 4.1 ([Lie83]). *If $n \geq 23$, then the minimum order of a graph with automorphism group isomorphic to A_n is at least $\frac{1}{2}\binom{n}{\lfloor n/2 \rfloor}$.*

Corollary 4.2. *By Stirling's approximation, the above lower bound is approximately $\frac{2^n}{\sqrt{2\pi n}}$.*

The following result is very recent and interesting. We know the complexity of graph isomorphism is in NP but it is not known to be in coNP. However, the planar case has a linear-time algorithm.

Even more surprising is the following.

Theorem 4.3 ([DLN$^+$09]). PlanarIsomorphism *is in* L.

This theorem states there is a log-space algorithm to solve isomorphism for planar graphs. This result finished a series of several papers in the past four years attempting to tackle this problem. It uses the fact that a 3-connected planar graph has a unique embedding in the plane. Then, the graph G is decomposed into 3-connected components, forming a tree-like structure. An older algorithm of canonizing labeled trees is used to canonize G based on this decomposition.

References

[Bab74] László Babai. On the minimum order of graphs with given group. *Canadian Mathematical Bulletin*, 17:467–470, 1974.

[Bol01] Béla Bollobás. *Random graphs*, volume 73 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2001.

[DLN$^+$09] Samir Datta, Nutan Limaye, Prajakta Nimbhorkar, Thomas Thierauf, and Fabian Wagner. Planar graph isomorphism is in log-space. In *Proceedings of the 24th Conference on Computational Complexity*, 2009.

[DP09] Devdatt Dubhashi and Alessandro Panconesi. *Concentration of Measure for the Analysis of Randomized Algorithms*. Cambridge University Press, New York, NY, USA, 2009.

[Fru39] R. Frucht. Herstellung von Graphen mit vorgegebener abstrakter Gruppe. *Compositio Math.*, 6:239–250, 1939.

[Hof82] Christoph M. Hoffmann. *Group-Theoretic Algorithms and Graph Isomorphism*. Springer-Verlag, 1982.

[Lie83] Martin W. Liebeck. On graphs whose full automorphism group is an alternating group or a finite classical group. *Proceedings of the London Mathematical Society*, 3:337–362, 1983.

[Sab59] Gert Sabidussi. On the minimum order of graphs with a given automorphism group. *Monatsh. Math.*, 63:124–127, 1959.