Algebra and Computation Course Instructor: V. Arvind

Lecture 2

Lecturer: V. Arvind *Scribe: Ramprasad Saptharishi*

1 Motivation

Last lecture we had a brush up of group theory to set up the arsenal required to study Graph Isomorphism. This lecture we shall see how group theory motivates graph isomorphism, and some more theorems on group theory that we would require for later lectures.

2 Graph Isomorphism and Automorphism Groups

Recall that two graphs G_1 and G_2 are isomorphic if there is a re-numbering of vertices of one graph to get the other, or in other words, there is an automorphism of one graph that sends it to the other.

And clearly, $Aut(G) \leq S_n$, the symmetric group on n objects, which represent the permuation group on the vertices. And since it is a subgroup of the permutation group, $|Aut(G)| \leq n!$

Of course, providing the entire automorphism group as output would take exponential time but what about a small generating set? Which then leads us to, does there exist a small generating set?

Lemma 1. *For any group H of size n, there exists a generating set of size* $\log n$.

Proof. Let $H_0 = \{e\}$. If $H_0 = H$ we are done. Otherwise, let $x = H \setminus H_0$. Let $H_1 = \langle H_0, x\rangle$ and in general, $x \in H \setminus H_i$ and $H = \langle H_i, x\rangle$ and since x forms two distinct cosets of H_i, $|H_{i+1}| = 2|H_i|$. And hence, in $\log n$ steps one would hit H. □

Now we can ask the question, can we output a small generating set of the automorphism group of a graph G? We shall refer to this problem as $Graph - Aut$. We shall now show that $Graph - Iso$ and $Graph - Aut$ are polynomial time equivalent.

Theorem 2. *With $Graph - Iso$ as an oracle, there is a polynomial time algorithm for $Graph - Aut$ and vice-versa.*

Proof. First we shall show that we can solve $Graph - Iso$ with $Graph - Aut$ as an oracle. We are given two graphs G_1 and G_2 and we need to create a graph G using the two such that the generating set of the automorphism should tell us if they are isomorphic or not.

Let $G = G_1 \cup G_2$. Suppose additionally we knew that G_1 and G_2 are connected, then a single oracle query would be sufficient. If any of the generators of $Aut(G)$ interchanged a vertex in G_1 with one in G_2, then connnectivity should force $G_1 \cong G_2$.

But what if they are not connected? We then have this vey neat trick, $G_1 \cong G_2 \Longleftrightarrow \overline{G}_2 \cong \overline{G}_2$, and either G_1 or $\overline{G}_1$ has to be connected and hence one can check for connectivity and then ask the appropriate query.

The other direction is a bit more involved. The idea is to see that any group is a union of cosets. Hence, suppose

$$H = a_1K \cup a_2K \cup \cdots a_nK$$

then $\{a_1, a_2, \ldots, a_n\}$ along with a generating set for K form a generating set for H. Hence once we have a subgroup K with small index, we can then recurse on K.

Hence we are looking for a tower of subgroups

$$Aut(G) = H \geq H_1 \geq H_2 \geq \cdots \geq H_m = \{e\}$$

such that $[H_i : H_{i+1}]$ is polynomially bounded.

For our graph G, let $Aut(G) = H \leq S_n$. We shall use Weilandt's notation where i^π denotes the image of i under π. In this notation, composition becomes simpler: $(i^\pi)^\tau = i^{\pi\cdot\tau}$.

Define $H_i = \{\pi \in H : 1^\pi = 1, 2^\pi = 1, \cdots i^\pi = 1\}$. And this gives the tower

$$H_0 = H \geq H_1 \geq H_2 \geq \cdots \geq H_{n-1} = \{e\}$$

with the additional property that $[H_i : H_{i+1}] \leq n - i$ since there are atmost $n - i$ places to go to when the first i are fixed by H_i.

Now look at the tablaeu

Picture supposed to come here, needs to be completed

□

3 The Set Stabilizer Problem

The Problem Statement: $H \leq S_n$, given by a small generating set. Also given is a subset $\Delta \subseteq [n]$. Find the

$$stab_{\Delta}(H) = \{\pi \in H : \Delta^{\pi} = \Delta\}$$

Though this problem has nothing to do with graphs directly, graph isomorphism reduces to this.

Theorem 3.

$$Graph - Iso \leq_P Set - Stab$$

Proof. By our earlier theorem, it is enough to show that $Graph - Aut$ reduces to $Set - Stab$.

One simply needs to note that an automorphism can be thought of as acting on the edges as well. Given a graph $G = (V, E)$, a permutation of the vertices induces a permutation of the edges. Hence,

$$\phi : Sym(V) \longrightarrow Sym\binom{V}{2}$$

is injective.

Thus, all we need to do is find the set of elements in $Sym(V)$ that stabilizes E. Our set H is $\phi(Sym(V)) \subseteq Sym\binom{V}{2}$ and $\Delta = E \subseteq \left[\binom{n}{2}\right]$ and the automorphism group is precicely $stab_{\Delta}(H)$. □

4 More Group Theory: Sylow Theorems

We will need some more tools for the lectures that follow, the Sylow Theorems in particular. Before that, we need the Orbit-Stabilizer theorem.

Definition 4. *Let G act on a set S. Let $s \in S$*

- *The orbit of s (s^G), is the set of all possible images of s under the action of G.*

$$s^G = \{t \in S : \exists g \in G, gs = t\}$$

- *The stabilizer of $s(G_s)$ is the set of all elements of G that fix s*

$$G_s = \{g \in G : gs = s\}$$

Theorem 5 (Orbit-Stabilizer Theorem)**.** *For any finite group G that acts on a set S. For every $s \in S$,*

$$|G| = |s^G| \cdot |G_s|$$

Proof. This is just Lagrange's theorem, all we need to see is that the stabilizer G_s is a subgroup of G and that $[G : G_s] = |s^G|$, should be a trivial exercise to the reader. □

Theorem 6 (Sylow Theorems)**.** *Let G be a group, $|G| = p^m r$, where p is a prime and $gcd(r, p) = 1$. Then*

1. *there exists a subgroup P such that $|P| = p^m$ (p-sylow subgroup)*

2. *for any p-subgroup[1]H of G, one of its conjucates is contained in P*

3. *the number of p-sylow subgroups of G is $1 \pmod p$*

Proof. We shall prove the subdivisions one after another.

Subdivision 1*:*

Let Ω be the set of subsets of G of size p^m. Note that $|\Omega| = \binom{p^m r}{p^m}$. Lucas' theorem tells us that $\binom{p^m r}{p^m}$ is not divisible by p by our choice of r. Let G act on Ω by left multiplication.

The action decomposes Ω into orbits, and since $p \nmid |\Omega|$, there exists $A \in \Omega$ such that $p \nmid |A^G|$. And since $p^m r |G| = |A^G||G_A|$, and by the choice of A, $p^m \mid |G^A|$.

And since the elements $ga \in A$ for $a \in A$ are distinct under the action of G_A, it follows that $|A| \geq |G_A|$ and hence forcing $|G_A| = p^m$. Hence G_A is our desired p-sylow subgroup.

Subdivision 2*:*

Let Ω be the set of left cosets of P, our p-sylow subgroup. And let H be a p-subgroup of G, which induces an action on Ω by left multiplication.

Since $|H| = p^a$, every non-trivial orbit of Ω is has cardinality a multiple of p. Hence, the number of points of Ω that are fixed by H is modulo p is the same as $|\Omega|$. Hence in particular, since $p \nmid |\Omega|$, the set of points fixed by H is non-zero. Hence, there exists a gP that is fixed by H.

Hence $hgP \subseteq gP$ or $g^{-1}hgP \subseteq P \implies g^{-1}hg \in P$ for all $h \in H$. Thus $g^{-1}Hg \subseteq P$

[1] subgroup of order p^a for some a

Note that this also tells us that all p-sylow subgroups are conjucates of each other.

Subdivision 3*:*

Let P be a p-sylow subgroup and let Ω be the set of p-sylow subgroups of G on which P acts by conjucation. For any $Q \in \Omega$, the stabilizer of Q under conjucation is called the normalizer of Q, denoted by $N_G(Q)$.

Suppose $Q \in \Omega$ is fixed by P on conjucation, then $P \leq N_G(Q)$. But subdivision 2 tells us that P and Q are conjucate to each other in $N_G(Q)$, which then forces $P = Q$. Hence the only fixed point is P itself and hence $|\Omega| = 1 \pmod{p}$. □

We also did the proof of Lucas' Theorem, has to be TEX-ed out