Algebra and Computation Course Instructor: V. Arvind

Lecture 3: Divide-and-Conquer on Groups

Lecturer: V. Arvind *Scribe: Ramprasad Saptharishi*

1 Overview

Last lecture we studied automorphism groups motivated through graph isomorphism. This lecture we shall examine other techniques to study group theoretic properties; we shall implement a 'divide-and-conquer' approach to study groups.

2 Orbit Computation

Computing the orbit of an element is one of the basic questions in group theoretic algorithms.

We are given a group G that acts on a finite set Ω, and hence G can be thought of as a subgroup of $Sym(\Omega)$. And of course since G could be very large, a small generating set A of G is given as input. Given an element $\alpha \in \Omega$, we would like to compute the G-orbit of α, denoted by α^G. Recall that

$$\alpha^G = \{\beta \in \Omega \ : \ \exists g \in G, \beta = \alpha^g\}$$

The naive way is to try and 'reach' every element in the orbit using elements of A acting on α, which is as follows:

1: $\Delta = \{\alpha\}$
2: **while** *Delta* grows **do**
3: **for** each $a \in A$ and each $\delta \in D \in \Delta$ **do**
4: $\Delta = \Delta \cup \{\delta^g\}$
5: **end for**
6: **end while**

The running time is atleast quadratic in the $|\Omega|$. A reachability approach is much better.

Algorithm: Define a graph $X = (V, E)$ where $V = \Omega$ and $(\alpha, \beta) \in E$ if $\alpha^a = \beta$ for some a in $A \cup A^{-1}$. The connected components of this graph would correspond to the orbits.

This is a linear time algorithm to compute orbits of Ω. Note that this algorith infact gives more, given any two elements of the same orbit, one could also obtain a group element that takes one to another: look at the path from one to another, multiply the edge labels.

This gives us a step forward towards a divide-and-conquer approach. Once we have the orbit decomposition of Ω, we can study the action of the group on each orbit separately. We would then have the additional property of the action of G being transitive[1] on the set.

3 Decomposition of Transitive Groups

In order to break down transitive groups we shall study "blocks". In this section, we shall assume that the action of G is transitive.

Definition 1. *$\Delta \subseteq \Omega$ is called a block if for all $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \phi$*

Of course for any action, Ω and singletons of Ω are blocks are trivial to be interesting.

Definition 2. *G is said to be primitive if it has only trivial blocks*

Let us look at some examples.

1. When G is infact the entire $Sym(\Omega)$, it's easily seen that G is primitive.
2. Even when G is the set of even permuations over Ω, also denoted by $A_{|\Omega|}$, it has enough permuations to still remain primitive. This also can be easily checked.
3. Suppose G acts on itself, say by left multiplication, $G \leq Sym(G)$. Every subgroup of G is a block since the cosets are either identical or disjoint. Infact, any coset would also be a block.

   Thus, we have a tiling of Ω using such blocks, we shall refer to these as a *block system*

[1] any element of the set can be pushed to any other by some element of the group

Definition 3. *A block system is a partition of Ω such that each part in the partition is a block with respect to the action.*

Note that if Δ is a block, so is Δ^g for every $g \in G$. And the tiling gives a theorem very similar to Lagrange's theorem on subgroups of a group.[2]

Theorem 4. *Let G act transitively on a set Ω and let $\Delta \subseteq \Omega$ be any block. Then $|\Delta|$ divides $|\Omega|$*

And this immediately leads to the following corollary.

Corollary 5. *For any group G that acts on Ω transitively, if $|\Omega|$ is a prime, then G is primitive.*

4. Let X be the graph, a collection of some k triangles and look at its automorphism group acting on it. First note that this action is transitive, and further, each triangle would be a block.

   Thus the automorphism group is imprimitive.

   This can of course be extended to any collection of k identical graphs such that the automorphism group of the piece is transitive.

5. Look at the leaves of a complete binary tree of depth k, and let the group be the automorphism group acting on them.

   What are the blocks?

   Take any internal node in the tree, and look at the set of all descendant leaves of it, and this set of leaves form a block. Infact, all blocks are precisely such sets of leaves.

The last example infact gives a great motivation to a divide-and-conquer approach.

If G is transitive and imprimitive, let Δ be the smallest block. Now group elements of Ω corresponding to the block-system generated by Δ. Now notice that G infact acts on this block system since G moves the blocks in the system around. And let the block system be the new set Ω_1 and the group being the projected version of G and we can now ask the question "Is G' primitive/transitive ?" with respect to the smaller set Ω.

Checking if the action is transtive can be done by orbit computation, but we need to check if a group is primitive.

[2]note that you require the action to be transitive, otherwise such Δ^g blocks needn't cover all of Ω

4 Blocks and Subgroups

Observation: If Δ_1 and Δ_2 are G-blocks, then so is $\Delta_1 \cap \Delta_2$.

With this observation, we can now talk about the smallest block containing a bunch of elements of Ω.

Lemma 6. *$G \leq Sym(\Omega)$ acting transitively on Ω, is primitive if and only if G_α is a maximal subgroup of G.*

Proof. Note that α needn't be specified since G_α and G_β are conjucates of each other when G is transitive. It is easy to check that of $g \in G$ such that $g\alpha = \beta$, then $gG_\alpha g^{-1} = G_\beta$.

Suppose $\{\alpha\} < \Delta < \Omega$, a non-trivial block. Let $H = \{g \in G \ : \ \Delta^g = \Delta\}$. We will now show that $G_\alpha < H < G$, thus proving one direction of the lemma.

Clearly, since G acts transitively and $\Delta < \Omega$, H has to be a proper subgroup of G. Also, if $g \in G_\alpha$, then $\alpha \in \Delta \cap \Delta^g \neq \phi$. Since Δ is a block, this forces $\Delta = \Delta^g$ and thus $g \in H$. Since $\{\alpha\} < \Delta$ there exists a $\beta \in \Delta$ different from α. Let g be the element of the group that takes α to β. Then since $\beta \in \Delta \cap \Delta^g$, $g \in H$ but $g \notin G_\alpha$. Thus $G_\alpha < H$.

As for the other direction, let $G_\alpha < H < G$. We shall show that $\alpha^H = \Delta$ is our non-trivial block. Since $G_\alpha < H$, $\Delta \neq \{\alpha\}$. Showing $\Delta < \Omega$ is a bit more involved. Since G_α is a subgroup of G, G_α and its cosets partition G:

$$G = \bigcup_{\beta \in \Omega \ , \ g_\beta : \alpha \mapsto \beta} G_\alpha g_\beta$$

And note that if any $g_\beta \in H$, the the entire coset of $G_\alpha g_\beta$ is contained in H. Hence since $\Delta = \Omega$ would imply $H = G$, our assumption $H < G$ forces $\Delta < \Omega$.

All that's left to show is that Δ is a block. Suppose $\Delta^g \cap \Delta \neq \phi$, then for some $h, h' \in H$, $\alpha^{hg} = \alpha^{h'}$ which then forces $h'gh^{-1} \in G_\alpha < H$. Hence $g \in H$ and therefore $\Delta^g = \Delta$. □

What the above lemma established is a one-to-one correspondence between subgroups of G and blocks of Ω.

One could also think of G as acting on $\{G_\alpha g \ : \ \alpha \in \Omega\}$, by identifying each point $\alpha \in \Omega$ by the subgroup G_α and its cosets.

Lemma 7. *Let $N \lhd G$, a normal subgroup of G. Then the orbits of N form a block system.*

Proof. We want to show that α^N is a block. Suppose $\alpha^{Ng} \cap \alpha^N \neq \phi$, then for some $n_1, n_2 \in N$, $\alpha^{n_1 g} = \alpha^{n_2}$ and hence $n_1 g n_2^{-1} \in G_\alpha$. By normality of N, the above terms can be written as $n_3 g$ for some $n_3 \in N$. From this, $n_1 g n_2^{-1} \in Ng$ and hence $n_2 \in Ng$ which collapses Ng and N, thus forcing $\alpha^{Ng} = \alpha^N$. □

Corollary 8. *If G is primitive, all its normal subgroups are transitive.*

5 Finding Blocks

Problem: Given $\langle A \rangle = G \leq Sym(\Omega)$ a transitive group. Find a non-trivial block system or report PRIMITIVE.

Observe that if G is not primitive, for every $\alpha \in \Omega$, there exists a $\beta \neq \alpha$ such that G has a non-trivial block containing $\{\alpha, \beta\}$. And hence it is enough to solve the following MINBLOCK problem efficiently.
MINBLOCK: Given $\{\alpha, \beta\} \subseteq \Omega$, find the minimum block containing α and β.

The algorithm is very clever and neat. Define an undirected graph $X = (V, E)$ such that $V = \Omega$ and $E = \{(\alpha, \beta)\}^G = \{(\alpha^g, \beta^g) \ : \ g \in G\}$.

Claim 9. *The connected component C containing α is the minimum block.*

Proof. Note that $G \leq Aut(X)$ and also G is transitive on Ω. Hence connected components have to move as a whole, and thus connected components are blocks and hence C is a block.

Suppose C was not minimal, let $C_1 \subsetneq C$ be a block. Since the containment is strict, there exists an edge $(\gamma, \delta) = (\alpha^g, \beta^g)$ such that $\gamma \in C_1$ and $\delta \in C \setminus C_1$. Now $\gamma \in C_1^g \cap C_1$ but $\delta \in C_1^g \setminus C_1$ which contradicts that C_1 is a block. Hence C has to be the minimal block containing α and β. □

One can now run over all β for a given α to find solve the non-trivial block problem.

6 Membership Testing

Problem: Given $\langle A \rangle = G \leq Sym(\Omega)$ and $g \in Sym(\Omega)$, check if $g \in G$.

This problem clearly reduces to the problem of computing the order of the group given by a set of generators (to check for membership of g, throw

g into the generating set and check if the order changes). We are looking for a divide and conquer approach to solve membership.

A promising avenue is the orbit-stabilizer formula $|G| = |G_\alpha||\alpha^G|$. We know to compute α^G efficiently, and hence can recurse on the smaller subgroup G_α. But how do we get hold of a small generating set for G_α? The following marvellous idea of Schreir gives the answer.

Theorem 10 (Schreir). *Let $\langle A\rangle = G$ and $H \leq G$. Let R be the set of distinct coset representatives of H, (i.e)*

$$G = \bigsqcup_{r\in R} Hr$$

Then

$$B = \left\{r_1 a r_2^{-1} \ : \ a \in A; r_1, r_2 \in R\right\} \cap H$$

generates H

Proof. For any given $r_1 \in R$ and $a \in A$, there exists a unique r_2 such that $r_1 a r_2^{-1} \in H$ (because $Hr_1 a = Hr_2$).

$$\begin{aligned}
RA &\subseteq BR \quad (r_1 a = (r_1 a r_2^{-1})r_2) \\
&\subseteq \langle B\rangle R \\
\implies RAA &\subseteq \langle B\rangle RA \\
&\subseteq \langle B\rangle\langle B\rangle R = \langle B\rangle R \\
\therefore \forall t \geq 0,\ RA^t &\subseteq \langle B\rangle R \\
\implies G &= \langle B\rangle R
\end{aligned}$$

Now since G can be partitioned into cosets of H and there are distinct representatives of every coset in R, unless $\langle B\rangle = H$, $\langle B\rangle R$ cannot cover the group. Hence $\langle B\rangle = H$. □

One could then look at $H = G_\alpha$ and the coset representatives are $g_\beta : \alpha \mapsto \beta$ and can be found in the orbit computation itself. But this still doesn't quite solve the problem since the size of the generating set is growing rapidly ($|B| = |R||H|$) and would get to exponential size in n steps.

This can also be tackled in a very clever way. We shall just see the sketch here, the details will be worked out next class.

Idea: For any two elements π and ψ in B, if $1^\pi = 1^\psi$ (both π and ψ map 1 to the same element), replace $\{\pi, \psi\}$ by $\{\pi, \pi^{-1}\psi\}$. This would then ensure that the two elements map 1 to different images now. Repeating this

replacement process, we can ensure that the elements of B are never larger than n^2.

The details shall be worked out in the next lecture, the interested reader could take this as an easy exercise though.