18.317 Combinatorics, Probability, and Computations on Groups 22 October 2001

Lecture 18

Lecturer: Igor Pak *Scribe: Christopher Malon*

Testing Solvability and Nilpotence

How to Reduce Generating Sets

Let $G = \langle g_1, \dots, g_k \rangle$, and consider a random subproduct $h = g_1^{\epsilon_1} \cdots g_k^{\epsilon_k}$, where the $\epsilon_i \in \{0, 1\}$ are chosen independently, uniformly. Last time, we showed:

Lemma 1 *If $H < G$ is a proper subgroup, then $\Pr(h \notin H) \geq \frac{1}{2}$.*

From the first lecture of the semester, we know that a nonredundant generating set cannot have more than $\log_2 |G|$ elements. Let L be an upper bound on $\log_2 |G|$, and c be a constant to be determined.

Theorem 2 *A set of cL independently chosen random subproducts $\{h_1, \dots, h_{cL}\}$ generates G with high probability.*

(The cost of forming this generating set is $O(kL)$.)

Proof: Let $H_i = \langle h_1, \dots, h_i \rangle$. Either $H_i = G$, or $\Pr(h_{i+1} \notin H_i) \geq \frac{1}{2}$, by the lemma above. Let τ be the first time i when $H_i = G$. Then $E(\tau) \leq 2L$. If we take L to be the length of the maximal subgroup chain, and $c = 4$, then this algorithm succeeds with probability at least $\frac{1}{2}$, by the Markov inequality. ■

The Chernoff bound (stated in lecture 10, October 1) provides another estimate of the value of c sufficient to ensure a certain probability of success. We omit the details.

Commutator Subgroups

Fix $k = O(\log |G|)$.

In order to test a black box group for solvability or nilpotence, we want to construct generators for a commutator group $[G, G]$ from generators for G.

Suppose $G = \langle g_1, \dots, g_k \rangle$. $[G, G]$ is *not* necessarily generated by the set of $[g_i, g_j]$. For example, a simple alternating group can be generated by two elements g_1, g_2. Since $[G, G]$ is normal in G and G is simple, $[G, G] = G$. The single element $[g_1, g_2]$ can generate only a cyclic subgroup.

The following *is* true:

Theorem 3 *If $A = \langle a_1, \dots, a_k \rangle$ and $B = \langle b_1, \dots, b_m \rangle$ are normal subgroups of G, then $[A, B]$ is the normal closure of the group generated by $[a_i, b_j]$, $1 \leq i \leq k$, $1 \leq j \leq m$.*

The *normal closure* of a subgroup H of G, denoted $\langle H\rangle^G$, is the smallest normal subgroup of G containing H. Since $[A, B]$ is normal, it must contain the normal closure of the group generated by the $[a_i, b_j]$. The equality given by the theorem wasn't proven in class, but I've sketched the easy proof at the end of the notes.

Lemma 4 *Let $H = \langle h_1, \ldots, h_m\rangle$ be a subgroup of $G = \langle g_1, \ldots, g_k\rangle$. Suppose $H \neq \langle H\rangle^G$. Then $\Pr(h^g \notin H) \geq \frac{1}{4}$, where h and g are random subproducts of the given generators for H and G, respectively.*

Proof: Let

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

denote the normalizer of H in G. Since $H \neq \langle H\rangle^G$, we know H is not normal in G, and $N_G(H) \neq G$. Let g be a random subproduct of the generators for G. By Lemma 1, $\Pr(g \notin N_G(H)) \geq \frac{1}{2}$.

Assume $g \notin N_G(H)$. Then $H^g \cap H$ is a proper subgroup of H. Let h be a random subproduct in H. Then

$$h^g = (h_1^{\epsilon_1} \cdots h_m^{\epsilon_m})^g = (h_1^g)^{\epsilon_1} \cdots (h_m^g)^{\epsilon_m}$$

is a random subproduct on $H^g = \langle h_1^g, \ldots, h_m^g\rangle$. Over h, $\Pr(h^g \notin H) = \Pr(h^g \notin H^g \cap H) \geq \frac{1}{2}$, again by Lemma 1. Over h and g, $\Pr(h^g \notin H) \geq \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. ■

Our algorithm to construct a generating set for $[A, B]$ proceeds as follows. Let V_0 be the group generated by all $[a_i, b_j]$. For each $r > 0$, form V_r by adding the element v^g to the set of generators for V_{r-1}, where v is a random subproduct of the generators for V_{r-1} and g is a random subproduct of the generators for G. Then $V_{cL} = [G, G]$ with high probability, by Theorem 3, Lemma 4, and the Markov Inequality.

To test whether a black box group is solvable, we just take its commutator repeatedly, using the algorithm above:

$$G \to [G, G] \to [[G, G], [G, G]] \to \cdots$$

We keep doing this for as many iterations as the longest possible subgroup chain in G (logarithmic in the size of G, which is given). We answer that it is solvable (with high probability) if all the generators are equal to the identity at the end of the algorithm. Otherwise, we say that it is not solvable (with certainty).

If we follow the algorithm literally, the number of generators we are considering will blow up as we take more commutators. To avoid this, we apply the generating set reduction algorithm from the beginning of the lecture. Thus, we can test for solvability in polynomial time in k and $\log_2 |G|$.

Similarly, we can test whether a group is nilpotent, by considering commutators of the form

$$G \to [G, G] \to [G, [G, G]] \to \cdots .$$

Appendix

To prove Theorem 3, we show that if $N < G$ is a normal subgroup containing all $[a_i, b_j]$, then it contains $[A, B]$. The proof can be broken into two lemmas:

Lemma 5 *N contains all $\left[a_i^{\pm 1}, b_j^{\pm 1}\right]$.*

Proof: Observing that $[x, y] = [y, x]^{-1}$, we obtain

$$\begin{aligned}
\left[a_i^{-1}, b_j\right] &= a_i^{-1}[a_i, b_j]^{-1}a_i \\
\left[a_i, b_j^{-1}\right] &= b_j^{-1}[a_i, b_j]^{-1}b_j \\
\left[a_i^{-1}, b_j^{-1}\right] &= b_j^{-1}a_i^{-1}\,[a_i, b_j]\,a_i b_j
\end{aligned}$$

■

Lemma 6 *Let $N < G$ be normal. If $x, y, z \in G$ and $[x, z], [y, z] \in N$, then $[xy, z] \in N$.*

Proof:

$$\begin{aligned}
[xy, z] &= xyzy^{-1}x^{-1}z^{-1} \\
&= x(yzy^{-1}z^{-1})zx^{-1}z^{-1} \\
&= x(yzy^{-1}z^{-1})x^{-1}xzx^{-1}z^{-1} \\
&= (x\,[y, z]\,x^{-1})([x, z])
\end{aligned}$$

■

The theorem follows by considering expansions of arbitrary elements of A and B in terms of the a_i and b_j, and applying the two lemmas.