18.317 Combinatorics, Probability, and Computations on Groups 28 November 2001

Lecture 30

Lecturer: Igor Pak *Scribe: Michael Korn*

Bias in the Product Replacement Algorithm

Here is the algorithm:

The input to the algorithm is a k-tuple $\overline{g} = (g_1, g_2, \ldots, g_r, 1, \ldots, 1)$, where the elements $g_1, \ldots, g_r$ generate the group G.

We then run a random walk on $\Gamma_k(G)$ starting at $\overline{g}$ for L steps, putting us at the point $\overline{g'}$. We choose i randomly from $1, \ldots, k$, and output the group element g'_i.

This algorithm is supposed to generate random group elements.

Here are some questions which can be asked about this algorithm:

Q1: Is $\Gamma_k(G)$ connected?

Q2: How do we choose the values for k and L?

Q3: Is there bias in the output? (Are all group elements equally represented in generating k-tuples?)

In this lecture we will try to answer question 3.

Definition 1 *Suppose G is a finite group, and $k \geq d(G)$. (Recall that $d(G)$ is the minimum number of generators necessary to generate G.)*

Let Q be the probability distribution of the first component of $(g_1, \ldots, g_k)$, where $(g_1, \ldots, g_k)$ is selected uniformly at random from among all k-tuples which generate G. So $Q(a)$ is the probability that $g_1 = a$.

Proposition 2 *Let $\phi_k(G)$ be the probability that a random k-tuple $(g_1, \ldots, g_k)$ generates G.*

If $\phi_{k-1}(G) \geq 1/2$, then $sep(Q) \leq 1/2$.

Proof:

We need to show that for all $a \in G$, $Prob(g_1 = a) \geq \frac{1}{2|G|}$, where $(g_1, \ldots, g_k)$ is a random generating k-tuple. This probability is equal to the number of generating k-tuples of the form $(a, g_2, \ldots, g_k)$, divided by the total number of generating k-tuples. The total number of generating k-tuples is at most $|G|^k$. Since $\phi_{k-1}(G) \geq 1/2$, the $(k-1)$-tuple $(g_2, \ldots, g_k)$ generates G at least half the time. So $(a, g_2, \ldots, g_k)$ is a generating k-tuple at least half the time, for any a. So there are at least $\frac{|G|^{k-1}}{2}$ generating k-tuples which have first element a. So the probability is at least $\frac{1}{2|G|}$. ■

Question: Are there finite groups G with very small $\phi_k(G)$ for $k \geq d(G)$?

The answer will turn out to be yes. Let G_n be the group $(A_n)^{n!/8}$. Then $d(G_n) = 2$ for n large enough. This fact follows from the following theorem.

Theorem 3 *(P. Hall, 1938)*

Let H be a nonabelian simple group. Let $\alpha_k(H) = \max\{m : d(H^m) = k\}$. Then $\alpha_k(H)$ is the number of $Aut(H)$ orbits of action on $\Gamma_k(H)$.

Let us see why this implies the earlier fact. We let $H = A_n$ and let $k = 2$. For $n > 6$, it is a fact that $Aut(A_n) = S_n$. (This is not true for $n = 6$, but this is not for normal people to understand why.) We will assume that $\phi_2(A_n) \geq 1/2$ (so two random elements of A_n generate A_n at least half the time). Thus there are at least $\frac{1}{2}(\frac{n!}{2})^2$ vertices in $\Gamma_2(A_n)$. Since $Aut(A_n) = S_n$, the size of an orbit is $n!$, so the number of orbits is at least $\frac{1}{2}(\frac{n!}{2})^2 \frac{1}{n!} = \frac{n!}{8}$. So $\alpha_2(A_n) \geq \frac{n!}{8}$, so $d((A_n)^{n!/8}) = 2$, which proves the fact from above.

We will now give a proof of Hall's Theorem.

Proof:

Let $G = H^m$. Take $\langle g_1, \ldots, g_k \rangle = G$, and let $g_i = (h_1^{(i)}, h_2^{(i)}, \ldots, h_m^{(i)}) \in G$, where $h_j^{(i)} \in H$. Let us write these elements in a k-by-m array as shown:

$$\begin{aligned}
g_1 &= \quad h_1^{(1)}, h_2^{(1)}, \ldots, h_j^{(1)}, \ldots, h_m^{(1)} \\
g_2 &= \quad h_1^{(2)}, h_2^{(2)}, \ldots, h_j^{(2)}, \ldots, h_m^{(2)} \\
&\vdots \\
g_k &= \quad h_1^{(k)}, h_2^{(k)}, \ldots, h_j^{(k)}, \ldots, h_m^{(k)}
\end{aligned}$$

Now look at the columns of this array. For all j, we must have $\langle h_j^{(1)}, h_j^{(2)}, \ldots, h_j^{(k)} \rangle = H$.

Claim 4 $\langle g_1, \ldots, g_k \rangle = G$ *iff* $(h_j^{(1)}, \ldots, h_j^{(k)})$ *are generating k-tuples in different $Aut(H)$ orbits.*

Proving this claim is enough to prove the theorem.

The "only if" direction is obvious; if two such k-tuples were in the same orbit, then it would be impossible for $(g_1, \ldots, g_k)$ to generate all of H^m, since the two columns would always be bound by the isomorphism between them.

For the "if" direction, assume the columns of the array are generating k-tuples which are in different orbits. Let $B = \langle g_1, \ldots, g_k \rangle$, and suppose B does not equal G. We will use an inductive argument. So assume that for a k-by-$(m-1)$ array, if the columns are generating k-tuples in different orbits, then the rows generate all of G. In our situation, this means that the projection of B onto the first $m-1$ coordinates is onto. (In other words, for any choice of the first $m-1$ coordinates, there is an element of B which attains those values, though we can't say what its last coordinate will be.) Of course, there is nothing special about the first $m-1$ coordinates; this statement holds for any collection of $m-1$ coordinates.

Now consider the subset $C \subset B$ consisting of points whose first $m-1$ coordinates are all equal to 1 (the identity element). This is a normal subgroup of H, hence it is either H itself, or 1, since H is simple. Suppose $C = H$. Then B would have to equal G, since we can find an element of B which sets the first $m-1$ coordinates to whatever we want, and then multiplying this by an appropriate member of C will yield any element of G at all. So we must assume $C = 1$. Again, there is nothing special about the last coordinate. So any element of B which has the value 1 for $m-1$ of its coordinates must have value 1 in the remaining coordinate as well.

Recall that we assumed H is nonabelian. Hence there are elements x and y with $xyx^{-1}y^{-1} \neq 1$. Since we can set any $m-1$ coordinates any way we like, it follows that $(x, 1, \ldots, 1, z) \in B$, for some z. Similarly, we have

$(y, 1, \ldots, 1, w, 1) \in B$, for some w. Multiplying these gives $(xy, 1, \ldots, 1, w, z) \in B$ and $(yx, 1, \ldots, 1, w, z) \in B$. Dividing these last two gives $(xyx^{-1}y^{-1}, 1, \ldots, 1, 1) \in B$. But this contradicts the result of the previous paragraph.

This completes the proof of Hall's Theorem.

■

Now back to the situation with A_n. As it turns out, for A_5 we have $\alpha_2(A_5) = 19$, which is greater than $\frac{5!}{8} = 15$, as we claimed that it should be for n large enough.

Claim 5 *$\phi_k((A_n)^{n!/8}) \to 0$ very rapidly as $n \to \infty$.*

Proof:

Recall that

$$Prob(\langle \sigma_1, \sigma_2, \ldots, \sigma_k \rangle \neq A_n) > \frac{1}{n^k}$$

(This is true since each permutation will fix the point 1 with probability $1/n$, hence with probability $1/n^k$ all k permutations will fix the point 1.) So

$$Prob\left(\langle g_1, \ldots, g_k \rangle = (A_n)^{n!/8}\right) \leq \left(1 - \frac{1}{n^k}\right)^{n!/8} \leq e^{-n!/8n^k}$$

which is very small for n large.

■