| | |
|---|---|
| **18.317 Combinatorics, Probability, and Computations on Groups** | 30 October 2001 |
| Lecture 31 | |
| *Lecturer: Igor Pak* | *Scribe: D. Jacob Wildstrom* |

# Bias (continued)

**Theorem 1 (P. Hall).** *For a simple group $H$ and $G = H^m$, it follows that $\langle g_1, \ldots, g_k \rangle = G$ if and only if $\langle h_j^{(1)}, h_j^{(2)}, \ldots, h_j^{(k)} \rangle = H$ for all $j$ from 1 to $m$.*

We shall henceforth work with $H = A_n$, $m = \frac{n!}{8}$, $\varkappa = o(n)$, $G = H^m$, and $Q = Q_k$, which to refresh our memory, is simply the probability distribution of $g_1$ in $\bar{g} = (g_1, g_2, \ldots, g_k) \in \Gamma_k(G)$.

**Theorem 2.** *There is a subset $B$ of $G$ such that, as $n \to \infty$, $\frac{|B|}{|G|} \to 1$ but $Q(B) \to 0$.*

That is to say that there is a huge subset (approaching the full set) of $G$ which is hardly ever generated by a $k$-tuple of generators.

We claim that, roughly, if $k \geq k$, then the values of $h_j = (h_j^{(1)}, h_j^{(2)}, \ldots, h_j^{(k)})$ are independent.

Then we have the lemma:

**Lemma 3.** $|\Gamma_k(o)| = |\Gamma_k(H)|^m|(1 - O(\frac{1}{n!}))$.

**Proof:** The number of automorphisms of $\Gamma_k(H)$ is, as we discussed earlier, $\alpha_k(G)$, which must exceed $\frac{H^k}{2|\operatorname{Aut}(H)|} = \frac{1}{2}\frac{(\frac{n}{2})^k}{n!} = N$. Now, $|\Gamma_k(G)|$ is equal to the product of $|\Gamma_k(H)|^m$ and the probability that each generated $k$-tuple is in a distinct orbit. This we can easily calculate to be $(1 - \frac{1}{N})(1 - \frac{2}{N}) \cdots (1 - \frac{m}{N})$, which exceeds $(1 - \frac{m}{N})^m$ and thus $(1 - \frac{m^2}{N})$. Using the equation $m = \frac{n!}{8}$ and $N \geq \frac{(n!)^3}{32}$, the above factor can be easily shown to exceed $1 - \frac{1}{2n!}$ ∎

Let $A_n$ be generated by $(h_1^1, h_1^2, \ldots, h_1^k)$. We know that with probability $\approx \frac{1}{n}$ (specifically, $\frac{1}{n} \pm \frac{1}{n^3}$), $h_1^1$ moves the first element. What would the specific probability tell us about $g_1$?

We start by looking at $\phi_k(A_n)$, which would be 1 minus the probability of "bad events". What sort of "bad events" might we have in mind? They can be characterized by $h_1, \ldots, h_k \in M$ for some maximal subgroup $M$ of $H$. There are really only 3 types of maximal subgroups in $H$: those with one fixed point, those with a pair of elements forming an orbit, and those with two fixed points. The probability of generating any of these is easily calculated:

$$\phi_k(A_n) = 1 - \frac{1}{n^k}n - \frac{1}{n(n-1)^k}\binom{n}{2} + \frac{1}{2(n(n-1))^k}\binom{n}{2} = 1 - \frac{1}{n^{k-1}} + O(\frac{1}{n^{2(k-1)}})$$

Let $\mathcal{A}$ be the event $(h_1, \ldots, h_k) \in \Gamma_k(H)$, and $\mathcal{B}$ be the event that $h_1 = 1$. By the above, $\Pr(\mathcal{A}) = 1 - \frac{1}{n^{k-1}} + O(\frac{1}{n^{2(k-1)}})$ and $\Pr(\mathcal{B}) = \frac{1}{n}$.

So what is $\Pr(\mathcal{B}|\mathcal{A})$? Well, it is equal to $\frac{\Pr(\mathcal{A}|\mathcal{B})}{\Pr(A)}\Pr(B)$, and we may interpret $\Pr(\mathcal{A}|\mathcal{B})$ as such; either $h_2, \ldots, h_k$ fix the first element or they fix an element not equal to the first. Calculating the probabilities, it follows that

$$\Pr(\mathcal{A}|\mathcal{B}) = 1 - \frac{2}{n^{k-1}} + O(\frac{1}{n^{2(k-1)}})$$

and thus

$$\Pr(\mathcal{B}|\mathcal{A}) = \frac{1}{n}\left(\frac{1 - \frac{2}{n^{k-1}} + O(\frac{1}{n^{2(k-1)}})}{1 - \frac{1}{n^{k-1}} + O(\frac{1}{n^{2(k-1)}})}\right) = \frac{1}{n}\left(1 - \frac{1}{n^{k-1}} + O(\frac{1}{n^{2(k-1)}})\right)$$

so $P = \frac{1}{n} - \frac{1}{nk} + O(\frac{1}{n^{2k-1}})$.

So, if we were to plot the number of generating sets giving us $h_1(1) = 1$ for $g$ uniform and $g_1 \in \Gamma_k(G)$, we wil have peaks at $\frac{1}{n}$ and $\frac{1}{n} - \frac{1}{n^k}$ respectively, and we may return to our original result by choosing $B \subset G$ such that $\{g = (h_1, \ldots, h_m)\}$ in which the number of generating sets in which $h_i(1) = 1$ exceeds $m(\frac{1}{n} - \frac{1}{2n^2})$. Using the Chernoff bounds, we find that $|B| \approx |G|(1 - \frac{1}{n!}) \to 1$, and that $Q_k(B) \approx \frac{1}{n!} \to 0$.