18.317 Combinatorics, Probability, and Computations on Groups	7 September 2001

Lecture 1

Lecturer: Igor Pak *Scribe: R. Radoičić*

Probability of Generating a Group

Let G be a finite group and let $|G|$ denote the order of G. Let $d(G)$ denote the minimum number of generators of G and $l(G)$ the length of the longest subgroup chain $1 = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq \ldots \subsetneq G_l = G$. Also, let $m(G)$ denote the maximal size of a *non-redundant* generating set, where a generating set $\langle g_1, g_2, \ldots, g_k \rangle$ is called *redundant* if there exists an i such that $\langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_k \rangle = G$. Furthermore, let

$$\varphi_k(G) = Pr(\langle g_1, g_2, \ldots, g_k \rangle = G),$$

where g_i are elements of G, chosen independently and uniformly at random from G. The main topic of the lecture today is to give a good estimate on $\varphi_k(G)$. More precisely, for every group G, we would like to find the smallest k for which $\varphi_k(G) \geq \frac{1}{3}$ or some other positive constant. Trivially, $\varphi_k(G) = 0$ for $k < d(G)$.

Let's look at several examples to understand the meaning of the notions above.

For example, let's take $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \ldots \times \mathbb{Z}_p$. Then, clearly,

$$\varphi_1(G) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\cdots\left(1 - \frac{1}{p}\right),$$

which tends to 0 as $p \to \infty$. Indeed,

$$\varphi_1(G) = \exp\left(\sum_{i<p, i\text{ prime}} \log\left(1 - \frac{1}{i}\right)\right) \approx \exp\left(-\sum_{i<p, i\text{ prime}} \frac{1}{i}\right),$$

which converges to 0 since $\sum \frac{1}{i}$ diverges. On the other hand,

$$\varphi_2(G) = \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\cdots\left(1 - \frac{1}{p^2}\right)$$

is strictly positive since $\sum \frac{1}{i^2}$ converges.

If G is ${\mathbb{Z}_2}^r$, i.e an r-dimensional vector space on $\{0, 1\}$-vectors, then $d(G) = m(G) = l(G) = r$. But this is not always the case.

If G is $\mathbb{Z}_{2^r}$, then $d(G) = m(G) = 1$, but $l(G) = r$, since $1 = \mathbb{Z}_1 \subsetneq \mathbb{Z}_2 \subsetneq \mathbb{Z}_4 \subsetneq \ldots \mathbb{Z}_{2^r}$.

Now, let $G = S_n$, the permutation group on n letters. Since $G = \langle (1, 2), (1, 2, \ldots, n) \rangle$ and since S_n is not a cyclic group, then $d(G) = 2$. Because there are $n - 1$ adjacent transpositions $(1, 2), (2, 3), \ldots, (n - 1, n)$, we have $m(G) \geq n - 1$. Actually, Whiston [W00] showed that $m(G) = n - 1$.

What about $l(S_n)$? Well, for any group G we have the following trivial bounds:

Proposition 1

$$d(G) \leq m(G) \leq l(G) \leq \log_2 |G|$$

Proof: The first and the last inequality are obvious, while the middle inequality follows from the implication: $m(G) = k$ and $\langle g_1, g_2, \ldots, g_k\rangle$ is the maximal non-redundant generating set $\Rightarrow \langle g_1\rangle \subsetneq \langle g_1, g_2\rangle \subsetneq \ldots \subsetneq \langle g_1, g_2, \ldots, g_k\rangle$. ■

One of the serious theorems in this subject shows that $l(S_n) \approx \frac{3}{2}n$, but its proof is quite involving and uses the classification theorems [B86], [CST89]. We are going to show a weaker but elegant statement:

Theorem 2

$$l(S_n) = O(n \log\log n)$$

Proof: We will use $\bigcirc_p$ to denote the highest power of p dividing $n!$. Then we have

$$\bigcirc_p = \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \ldots = \sum_i \lfloor\frac{n}{p^i}\rfloor \leq \frac{n}{p\left(1-\frac{1}{p}\right)} = \frac{n}{p-1}.$$

Then clearly:

$$l(S_n) \leq \sum_{p\leq n, p \text{ prime}} \bigcirc_p \leq n \sum_{p\leq n} \frac{1}{p-1} \leq n\log\log n + O(n),$$

where the last inequality follows from the Prime Number Theorem:

$$\sum_{p\leq n} \frac{1}{p-1} \sim \int_1^n \frac{dx}{x\log x} = \int \frac{d\,\log x}{\log x} = \log\log x\Big|_1^n.$$

■

Definition 3 *We define the random group process $\{B_t\}$:*

$B_0 = 1$ and for $t > 0$, $B_{t+1} = \langle B_t, g_{t+1}\rangle$, where $g_{t+1} \in G$ is a random element chosen at moment $t+1$. We obtain the chain of subgroups $B_0 \subset B_1 \subset B_2 \subset \ldots \subset B_t \subset \ldots \subset G$. Let $\tau(G)$ denote the stopping time of $\{B_t\}$, i.e.

$$\tau := \min\{t : B_t = G\}$$

Proposition 4

$$\mathbf{E}[\tau] \leq 2\log_2|G|$$

Proof: Given that $t < \tau$ (i.e. $B_t \neq G$), we have

$$Pr(B_{t+1} \neq B_t) = 1 - \frac{|B_t|}{|G|} \geq \frac{1}{2}.$$

Thus, the expected time for the random group process to increase the order of the current subgroup is ≤ 2. Hence, $\mathbf{E}[\tau] \leq 2\log_2|G|$. ■

If $G = {\mathbb{Z}_2}^r$, then the inequality in the previous proof is an equality, so, in a sense, ${\mathbb{Z}_2}^r$ is the worst to generate. Notice that we actually proved the following stronger statement:

Proposition 5

$$\mathbf{E}[\tau] \leq 2l(G)$$

However, $l(G)$ in the proposition above cannot be replaced by $m(G)$, which is clear, e.g. when $G = {\mathbb{Z}_2}^r$. Still, the result is not the best possible. Clearly, $\mathbf{E}[\tau] \geq l(G)$, but we will show today that the multiplicative constant factor in front of $l(G)$ can be shed.

Theorem 6 *Let $|G| \leq 2^r$. Then for all k, $\varphi_k(G) \geq \varphi_k({\mathbb{Z}_2}^r)$.*

Proof: Fix k and a subgroup $A \subsetneq G$. Let B_t and B'_t be the random group processes for G and ${\mathbb{Z}_2}^r$, respectively. Let $\tau_1, \tau_2, \ldots, \tau_L = \tau$ denote times t for which $B_t \neq B_{t-1}$. Similarly, define $\tau'_1, \tau'_2, \ldots, \tau'_R = \tau'$. We will use the induction on $|G|$. When $|G| = 1$, the theorem is trivial. Let $s := \tau_{L-1}$. We need to show that

$$Pr(\tau_L - \tau_{L-1} \leq k \big| B_s = A) \geq Pr(\tau'_R - \tau'_{R-1} \leq k)$$

Indeed, the lefthand side is equal to $1 - (\frac{|A|}{|G|})^k$, and the righthand side is equal to $1 - Pr(\tau'_R - \tau'_{R-1} > k) = 1 - \frac{1}{2^k}$.

Now $\frac{|A|}{|G|} \leq \frac{1}{2}$ and the claim above follows.

This claim, combined with the induction assumption $Pr(\tau_{L-1} \leq k) \geq Pr(\tau'_{R-1} \leq k)$, gives

$$Pr(\tau_L \leq k \big| B_s = A) \geq Pr(\tau'_R \leq k) = \varphi_k({\mathbb{Z}_2}^r).$$

This holds for any fixed k and A, so the theorem follows. ∎

References

[W00] J. Whiston: Maximal independent generating sets of the symmetric group, *Journal of Algebra* 232 (2000), 255–268.

[B86] L. Babai: On the length of subgroup chains in the symmetric group, *Comm. Algebra* 14 (1986), 1729–1736.

[CST89] P. J. Cameron, R. Solomon, A. Turull: Chains of subgroups in symmetric groups, *Journal of Algebra* 127 (1989), 340–352.