18.317 Combinatorics, Probability, and Computations on Groups 14 September 2001

Lecture 4

Lecturer: Igor Pak *Scribe: Ben Recht*

Even if a paper is famous and written by very famous individuals, that does not necessarily mean that it is correct. In this lecture, we will look at a proof of the probabilistic generation of S_n by Dixon, based on results of Erdős and Turan. Then we discuss the lemmas which they proved incorrectly in their paper.

Our goal will be to prove

Theorem 1

$$Pr(\langle \sigma_1, \sigma_2 \rangle = A_n \text{ or } S_n) \to 1 \text{ as } n \to \infty$$

The idea of the proof is a follows. First we will prove that the probability that $\langle \sigma_1, \sigma_2 \rangle$ is primitive goes to 1 as n goes to infinity. Next, we can show that the probability that $\langle \sigma_1, \sigma_2 \rangle$ contains a cycle of length p, where p is a prime less than $n-3$ also goes to 1 as n goes to infinity. Then the theorem follows immediately by the following result of Jordan

Theorem 2 (Jordan 1873) *If $G \leq S_n$ is primitive and contains a cycle of length p where p is a prime less than $n-3$ the G is equal to A_n or S_n.*

The proof of Jordan's theorem can be found in many classic texts on group theory.

We'll proceed with the following

Lemma 3 $Pr(\langle \sigma_1, \sigma_2 \rangle \text{ is transitive}) = 1 - \frac{1}{n} + O(\frac{1}{n^2})$

Proof: Let $p = Pr(\langle \sigma_1, \sigma_2 \rangle$ is transitive). Then

$$\begin{aligned}
1 - p &< \sum_{k=1}^{n/2} \binom{n}{k} Pr(\sigma_1 \text{ and } \sigma_2 \text{ fix blocks of size } k \text{ and } n-k) \\
&= \sum_{k=1}^{n/2} \binom{n}{k} \frac{1}{\binom{n}{k}^2} \\
&= \sum_{k=1}^{n/2} \frac{1}{\binom{n}{k}} \\
&= \frac{1}{n} + O(\frac{1}{n^2})
\end{aligned}$$

∎

We'll now prove a result about when $\langle \sigma_1, \sigma_2 \rangle$ is primitive.

Theorem 4 $Pr(\langle \sigma_1, \sigma_2 \rangle \text{ is imprimitive}) = O(\frac{n}{2^{n/4}})$

Proof: The probability that σ has a fixed block structure with block size d ($md = n$) is equal to $\frac{d!^m m!}{n!}$ as we can permute the blocks and the elements within the blocks. The number of block structures with block size d is equal to

$$\frac{\binom{n}{d\ldots d}}{m!} = \frac{n!}{d!^m m!}\,.$$

Here is is clear that the multinomial coefficient is over m d's.

Now

$$\begin{aligned} Pr(\langle\sigma_1,\sigma_2\rangle \text{ is imprimitive}) &< \sum_{d|n} \frac{n!}{d!^m m!}\left(\frac{d!^m m!}{n!}\right)^2 \\ &< \sum_{m=2}^{n/2} \frac{(\frac{n}{m})!^m m!}{n!} \\ &= \frac{(n/2)!2^n}{n!} + \ldots + \frac{2!(n/2)!^2}{n!} \end{aligned}$$

The last term in this sum is a dominating term, there are $n/2$ such terms and $\binom{n}{n/2} > 2^{n/2}$, thus completing the proof. ■

Corollary 5 *$Pr(\langle\sigma_1,\sigma_2\rangle$ is primitive $) = 1 - \frac{1}{n} + O(\frac{1}{n^2})$*

We now will attempt to prove

Theorem 6 *Let $\sigma \in S_n$ and p be a prime less than $n-2$. Then $Pr(\sigma = \sigma_p \prod_i \gamma_i)$, where σ_p is a p-cycle and γ_i are c_i-cycles with $p \nmid c_i$, goes to 1 as n goes to infinity.*

This result will imply Dixon's theorem. To prove this result, we will prove the following two lemmas next time.

Lemma 7 *(**Erdős -Turan**) Let $1 \leq a_1 \leq a_2 \leq a_r \leq n$. Then*

$$Pr(\sigma \in S_n \textit{ does not contain any cycles of length } a_i) \leq \sum_{i=1}^{r} \frac{1}{a_i}\,.$$

Lemma 8 *Let $\sigma \in S_n$ and $p < n$ be a prime. Then $Pr(p \nmid order(\sigma)) = \prod_{k=1}^{n/p}(1 - \frac{1}{pk})$.*

Erdős and Turan published a famous proof of these lemmas. We will construct correct proofs in the next lecture.