18.317 Combinatorics, Probability, and Computations on Groups 21 September 2001

Lecture 6

Lecturer: Igor Pak *Scribe: C. Goddard*

Probabilistic Generation

In this lecture, we will complete the classical proof for Dixon's theorem on the probabilistic generation of S_n, based on the work by Erdős and Turán. Reiterating from the previous lectures, here is Dixon's theorem:

Theorem 1 (Dixon)

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

We will use Lemma 2, proved last lecture, and Jordan's theorem (Theorem 3) and combine them with Lemma 4, proved here, to prove Dixon's theorem (Theorem 1) classically.

Thus, Lemma 2 and Jordan's theorem are merely stated here:

Lemma 2 (Erdős-Turán) *Let $1 \le a_1 < a_2 < a_r \le n$. Then*

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

Theorem 3 (Jordan 1873) *If $G \subset S_n$ 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.*

Now continuing from the previous lecture, we will prove the following lemma.

Lemma 4 (Erdős-Turán) *For a fixed prime p (or prime power),*

$$\Pr(\sigma \in S_n, p \nmid \text{order}(\sigma)) = \prod_{i=1}^{\lfloor \frac{n}{p} \rfloor} \left(1 - \frac{1}{p \cdot i}\right)$$

Proof: Let

$$z_\lambda = \frac{n!}{1^{m_1}\, m_1!\, 2^{m_2}\, m_2! \ldots} = \#\text{ elements in conjugacy class } (\lambda)$$

where $\lambda = (1^{m_1} 2^{m_2} \ldots)$ and $\sum m_i \cdot i = n$.

Now

$$\begin{aligned} 1 = \sum_{\lambda \vdash n} \frac{z_\lambda}{n!} &= \text{coeff } [t^n] \prod_{i=1}^{\infty} \left(1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \frac{t^{3i}}{3! \cdot i^3} + \ldots\right) \\ \Pr(\sigma \in S_n, p \nmid \text{order}(\sigma)) &= \text{coeff } [t^n] \prod_{i=1,\ p \nmid i}^{\infty} \left(1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \frac{t^{3i}}{3! \cdot i^3} + \ldots\right) \end{aligned}$$

Now denote $\Pi = 1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \frac{t^{3i}}{3! \cdot i^3} + \dots$

$$\begin{aligned}
\text{So } \Pi &= \prod_{p \nmid i, i=1}^{\infty} \exp\left(\frac{t^i}{i}\right) \text{ (since } e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots) \\
&= \frac{\prod_{i=1}^{\infty} \exp\left(\frac{t^i}{i}\right)}{\prod_{\alpha=1}^{\infty} \exp\left(\frac{t^{p\alpha}}{p\alpha}\right)} \\
&= \exp\left(\sum_{i=1}^{\infty} \frac{t^i}{i} - \sum_{\alpha=1}^{\infty} \frac{t^{\alpha p}}{\alpha p}\right) \\
&= \exp\left(-\log(1-t) + \frac{1}{p}\log(1-t^p)\right) \text{ (using } -\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \dots) \\
&= \frac{(1-t^p)^{\frac{1}{p}}}{1-t} \\
&= \frac{1-t^p}{1-t} \cdot (1-t^p)^{\frac{1}{p}-1} \\
&= \frac{1-t^p}{1-t} \cdot \left(\frac{1}{1-t^p}\right)^{1-\frac{1}{p}} \\
&= (1 + t + \dots + t^{p-1}) \cdot \left\{1 + \sum_{m=1}^{\infty} t^{mp} \cdot \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{2p}\right) \cdot \ldots \cdot \left(1 - \frac{1}{mp}\right)\right\}
\end{aligned}$$

(Note: $(1+x)^\alpha = 1 + \frac{\alpha}{1!}x + \frac{\alpha(\alpha-1)}{2!}x^2 + \dots$)

So to find coeff$[t^n]$, take $m = \lfloor \frac{n}{p} \rfloor$ above, and we're done. ■

Now we are ready to prove Dixon's theorem (Theorem 1).

Proof: $\Pr(\sigma \text{ has } p-\text{cycle}) \longrightarrow 1$ as $n \to \infty, p < n-2$.

Let $A = \{\log^2 n < p < n-2, p \ -\text{prime}\}$.

Using Lemma 2,

$\Rightarrow \Pr(\sigma \text{ has no } A \ -\text{cycles})$

$$\begin{aligned}
\leq \frac{1}{\sum_{p=\log^2 n}^{n-2} \frac{1}{p}} &\sim \frac{1}{\log\log(n-2) - \log\log(\log^2 n)} \\
&\quad \text{(Using Euler's theorem: } \sum_{p<x} \frac{1}{p} \sim \log\log x) \\
&\sim c \cdot (\log\log n)^{-1} \text{ where c is a constant}
\end{aligned}$$

$\Rightarrow$ with $\Pr > 1 - \frac{c}{\log\log n}$, $\exists\, p \ -$cycle with $p \in A$ for some prime p .

Now from Lemma 4, since $p > \log^2 n$, we have:

$$\Pr(\sigma \text{ contains exactly one } p\text{-cycle} \,|\, \sigma \text{ contains at least one } p\text{-cycle}) = \prod_{i=1}^{n-p} \left(1 - \frac{1}{p \cdot i}\right)$$

$$> \exp\left(\sum_{i=1}^{n} \log\left(1 - \frac{1}{p \cdot i}\right)\right) = \exp\left(-\sum_{i=1}^{n} \frac{1}{p \cdot i} + \mathrm{o}(1)\right) = \exp\left(\frac{-\log n + \log p + \mathrm{o}(1)}{p}\right)$$

$$> \exp\left(\frac{-\log n}{p}\right) > \exp\left(\frac{-1}{\log n}\right) > 1 - \frac{1}{\log n}$$

■

Finally, for the Pr as in Theorem 1, we obtain

$$\Pr > \left(1 - \frac{c}{\log\log n}\right)\left(1 - \frac{1}{\log n}\right) \to 1 \text{ as } n \to \infty$$

■