18.317 Combinatorics, Probability, and Computations on Groups	12 September 2001
Lecture 3	
Lecturer: Igor Pak	*Scribe: T. Chiang*

Probabilistic Generation

In this lecture, we will prove the following Theorem with contemporary mathematics:

Theorem 1 (Dixon)

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

We first recall that a simple group G is a group with no proper normal subgroups. Let G be simple; then the following proposition is valid:

Proposition 2

$$\varphi_k(G) \leq 1 - \sum_M \frac{1}{[G:M]^k} = 1 - \sum_{M \subset \mu} \frac{1}{[G:M]^{k-1}}, \tag{2}$$

where M is a maximal subgroup of G and μ is the conjugacy classes of M.

Proof: It is clear that $1 - \varphi_k(G) \leq \sum_M \frac{1}{[G:M]^k}$. Now, because M is the maximal subgroup of G, we can define $N_G(M)$ as the maximal subgroup of G such that $M \triangleleft G$. The only solution must be in the set $\{M, G\}$, and since G is simple, this implies that $N = M$. Now if we define the term $M^G = gMg^-1$ as the conjugacy class of M, we can readily verify that $|\{M^G\}| = \frac{|G|}{|N_G(M)|} = [G:M]$. ■

Theorem 3 (O'nan -Scott) *Let $G \subset S_n$ be primitive. Then G is*

A. Affine
B. Product Type
C. Diagonal Type
D. Almost Simple

Proof: Implicit from the Classification of Finite Simple Groups. ■

From here we deduce Theorem 1.

Proof: We begin with some Group Theoretic terminology. First we suppose that $G \subset S_n$ and that $G = \{\sigma_1 \ldots \sigma_k\}$. We call a group G - transitive if $\forall i, j \in \{i \ldots n\}$ then there exists an element $\sigma \in G$ such that $\sigma(i) = j$. Next we call a group G - primitive if the following occur:

$(R_1)(R_2)\cdots(R_m)$

where $|R_i| = d$ and $n = md$ so that $\forall \sigma \in G$; $\forall i, j \in R_\alpha$, there exists $\beta : \sigma(i), \sigma(j) \in R_\beta$. Now if we use the O'nan-Scott Theorem with these two facts, we see that the 4 properties of G are exactly the conjugacy classes which gives us the proof to the theorem. ■

We also give another Theorem concerning the number of conjugacy classes of the maximal subgroups of S_n.

Theorem 4 (Liebeck-Shalev) *The number of conjugacy classes of maximal subgroups of S_n is of the order:* $\frac{n}{2}(1 + O(1))$.

From here we can also deduce Theorem 1 :

Proof: First we preface the proof by noting that the maximal subgroups of S_n are of the form $S_k \times S_{n-k}$ for $k \leq \frac{n}{2}$. First we see that

$$\begin{aligned}\varphi_2(A_n) &\geq 1 - \sum_{M \subset \mu} \frac{1}{[G:M]} \\ &= 1 - \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{\binom{n}{k}} + O(\frac{1}{e^{cn}}) \\ &= 1 - \frac{1}{n} + O(\frac{1}{n^2}).\end{aligned}$$

■

We end this lecture with an example and a corollary.

Suppose that $G = PSL(2,p)$ - simple. Then

$$|G| = \frac{1}{2(p-1)}(p^2-1)(p^2-p) = \frac{p(p-1)(p+1)}{2}. \tag{3}$$

Now if H is a maximal subgroup in $PSL(2,p)$, then H has the form

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : ac = 1 \right\} \tag{4}$$

Thus $|H| = \frac{p(p-1)}{2}$. So we see that $[G:H] = p+1$ which is roughly p. It was never shown, but is told to be true that the number of conjugacy classes of maximal subgroups is ≤ 7 when the index $\geq p$. Hence $\varphi_2 > 1 - \frac{7}{p}$.

Corollary 5 *As* $p \to \infty$, $\varphi_2\left(PSL(2,p)\right) \to 1$.