L4 (4/6/2020) Igor Pak

Probability of Generation

From last lecture:

Th [Dixon] $P(\langle \sigma, \omega \rangle = A_n \text{ or } S_n) \to 1$ as $n \to \infty$

Lemma $P(\sigma$ has no prime cycles of length $p \le n-3) > 1 - \frac{c}{\log\log n}$

$\boxed{L \Rightarrow Th}$ ← by Jordan's Th

Main Lemma [E-T]

$A = \{1 \le a_1 \le a_2 \le \ldots \le a_r \le n\}$

$P(\sigma \text{ has no cycles in } A) \le \frac{1}{\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_r}}$

Def $X_\ell :=$ # ℓ-cycles in random $\sigma \in S_n$

SL1 $\mathbb{E}[X_\ell] = \frac{1}{\ell}$

SL2 $\ell \neq m, \ \ell + m \leq n$

$\Rightarrow \mathbb{E}[X_\ell \cdot X_m] = \frac{1}{\ell m}$

SL3 $$\mathbb{E}[X_\ell^2] = \begin{cases} \frac{1}{\ell}, & 2\ell > n \\ \frac{1}{\ell} + \frac{1}{\ell^2}, & 2\ell \leq n \end{cases}$$

Now: SL1 + SL2 + SL3 $\Rightarrow$ **Main L**

Proof of Main Lemma $A = \{1 \le a_1 < \dots < a_r\}$

$X_\ell = \#\ \ell\text{-cycles}$, $Y = \#\ A\text{-cycles} = \sum_{i=1}^{r} X_{a_i}$

$$\mathbb{E}[Y] = \sum_{i=1}^{r} \mathbb{E}[X_{a_i}] = \sum_{i=1}^{r} \frac{1}{a_i}$$

$$\begin{aligned}
\mathbb{E}[Y^2] &= \sum_{i \neq j} \mathbb{E}[X_{a_i} X_{a_j}] + \sum_{i=1}^{r} \mathbb{E}[X_{a_i}^2] \\
&\le 2 \sum_{i<j} \frac{1}{a_i a_j} + \sum_{i=1}^{r} \left(\frac{1}{a_i^2} + \frac{1}{a_i} \right) \\
&\le \underbrace{\left(\sum_{i=1}^{r} \frac{1}{a_i} \right)}_{\mathrm{I}} + \underbrace{\left(\sum_{i=1}^{r} \frac{1}{a_i} \right)^2}_{\mathrm{II}}
\end{aligned}$$

$$\begin{aligned}
\mathrm{Var}(Y) = \mathbb{E}[Y^2] - \mathbb{E}[Y]^2 &\le (\mathrm{I} + \mathrm{II}) - \mathrm{II} \\
&\le \left(\sum_{i=1}^{r} \frac{1}{a_i} \right)
\end{aligned}$$

By Chebyshev ineq. $\mu := \mathbb{E}[Y] = \sum_{i=1}^{r} \frac{1}{a_i}$

$$P(Y=0) = P(Y + \underbrace{\mathbb{E}[Y]}_{\mu} \leq \underbrace{\mathbb{E}[Y]}_{\mu}) \leq \frac{Var(Y)}{\mu^2}$$

$$\leq \frac{\mu}{\mu^2} = \frac{1}{\mu} = \frac{1}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_r}} \qquad \square$$

Counting Lemma [E-R]

Fix p - prime. **Then**

$$P(p \nmid \text{order of } \sigma) = \prod_{i=1}^{\lfloor n/p \rfloor} \left(1 - \frac{1}{ip}\right)$$

Remark: Probabilistic proof??

We only know GF proof.

Proof of Counting Lemma

$\sigma \in S_n \longleftrightarrow$ cycles in $\sigma \longleftrightarrow$ partition $\lambda \vdash n$

$z_\lambda :=$ # elts in conj class of S_n corr. to λ

Prop: $$z_\lambda = \frac{n!}{(1^{m_1} m_1!)(2^{m_2} m_2!)\cdots}, \quad \lambda = (1^{m_1} 2^{m_2} \cdots), \quad n = \sum m_i \cdot i$$

Exc: prove Prop.

$$\underline{i} \to t^{m_1} / m_1! \cdot 1^{m_1}$$

We have: $$1 = \sum_{\lambda \vdash n} \frac{z_\lambda}{n!} = [t^n] \prod_{i=1}^{\infty} \left(1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \cdots\right)$$

$$P(p \nmid \text{order of } \sigma) = [t^n] \prod_{i=1,\, p \nmid i}^{\infty} \left(1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \cdots\right)$$

$$\Pi_i := \left(1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \cdots\right) = \exp(t^i / i)$$

$$z_{(n)} = \frac{n!}{n} = (n-1)!$$

$$P(p \nmid \sigma) = [t^n] \left(\prod_{p \nmid i,\ i=1}^{\infty} \pi_i(t) \right) =: Q_p(t)$$

$$Q_p(t) = \prod_{p \nmid i} e^{t^i/i} = \prod_{i=1}^{\infty} e^{t^i/i} \Big/ \prod_{k=1}^{\infty} e^{t^{pk}/pk}$$

$$= \exp\left[\sum_{i=1}^{\infty} t^i/i - \sum_{k=1}^{\infty} t^{pk}/pk \right]$$

$$= \exp\left[-\log(1-t) + \frac{1}{p} \log(1-t^p) \right]$$

$$-\log(1-z) = z + \frac{z^2}{2} + \frac{z^3}{3} + \dots$$

$$= \frac{(1-t^p)^{1/p}}{1-t} = \left(\frac{1-t^p}{1-t} \right) (1-t^p)^{\frac{1}{p}-1}$$

$$= (1+t+t^2+\dots+t^{p-1}) \times \sum_{m=0}^{\infty} t^{mp} \left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{mp}\right)$$

/ last eq.: $(1+z)^{\alpha} = 1 + \frac{\alpha}{1!} z + \frac{\alpha(\alpha-1)}{2!} z^2 + \dots$ /

<u>We have:</u>

$$P(p \nmid \text{order of } \sigma) = [t^n]\, Q_p(t)$$

$$= [t^n] \left[(1+t+\dots+t^{p-1}) \left[1 + \sum_{m=1}^{\infty} t^{mp} \left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right) \cdots \right] \right]$$

$$= \left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right) \cdots \left(1-\frac{1}{mp}\right), \quad m = \left\lfloor \frac{n}{p} \right\rfloor$$

$\blacksquare$

<u>Summary:</u> $Y = \#\, A\text{-cycles}$, $\mu = \mathbb{E}[AY]$
$= \sum \frac{1}{a_i}$

<u>Main L:</u> $P(Y=0) < \frac{1}{\mu}$

<u>Counting L:</u> $P(p \nmid \sigma) = \left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right) \cdots \left(1-\frac{1}{\lfloor \frac{n}{p} \rfloor p}\right)$

<u>**Note**</u>: p- prime never used(!)

Proof of Dixon's th

$A := \{ p\text{-prime}, (\log n)^2 < p \leq n-3 \}$

ML $\Rightarrow$ $P(G \text{ has no } A\text{-cycles}) = P(Y=0)$

$$\leq \left(\sum_{(\log n)^2 < p \leq n-3} \frac{1}{p} \right)^{-1} \sim \left(\log\log(n-3) - \log\log\left((\log n)^2\right) \right)^{-1}$$

$$\lesssim \frac{c}{\log\log n}$$

$\Rightarrow$ w/ $\Pr > 1 - \dfrac{c}{\log\log n}$ G contains a p-cycle in A

We want: $P(G$ cont. p-cycle in $A \mid G$ cont. exactly ≥ 1 p-cycle in $A)$

$P(\sigma \text{ cont. } \overbrace{\text{p-cycle}}^{\text{one}} \text{ in } A \mid \sigma \text{ cont } \cancel{\text{exactly 1}}\ {\geq 1} \text{ p-cycle in } A)$

$$= \prod_{k=1}^{\lfloor (n-p)/p \rfloor} \left(1 - \frac{1}{pk}\right) > \exp\left[\sum_{k=1}^{n/p} \log\left(1 - \frac{1}{pk}\right)\right] =$$

$$= \exp\left[-\sum_{k=1}^{n/p} \frac{1}{pk} + O(1)\right] \qquad \Big| \; p > (\log n)^2$$

$$= \exp\left[\frac{1}{p}\left(-\log(n/p) + \cancel{\log p} + O(1)\right)\right]$$

$$\geq \exp\left[\frac{1}{p}(-\log n)\right]$$

$$> \exp\left[-1/(\log n)\right] > 1 - \frac{1}{\log n}$$

In summary: $1 - P(\langle \sigma, w\rangle = S_n \text{ or } A_n) \leq$

$\leq P(\langle \sigma, w\rangle \text{ not primitive}) + P(\langle \sigma, w\rangle \text{ does not cont p-cycle}, p \leq n-3)$

$$\leq \frac{1}{n} + O\left(\frac{1}{n^2}\right) + \frac{c}{\log\log n} + \frac{1}{\log n} \to 0 \quad \blacksquare$$