L3 (4/3/2020) Igor Pak

Probability of generation

Last time: $\varphi_k(G) = P(\langle g_1, \dots g_k \rangle = G)$, $g_i \in G$ unif, indep

Th (Dixon) $\varphi_2(A_n) \to 1$ as $n \to \infty$

Th (Babai) $\varphi_2(A_n) = 1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right)$

Prop 1 $\varphi_2(A_n) < 1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right)$

$\triangleright$ $$1 - \varphi_2(A_n) \leq \sum_{i=1}^{n} P(\sigma(i) = \omega(i) = i) - \sum_{i<j} P(\sigma(i) = \omega(i) = i,\ \sigma(j) = \omega(j) = j) - \sum_{i<j<k} + \dots$$

$$\leq n \cdot \frac{1}{n^2} - \binom{n}{2} \frac{1}{n^4} + \binom{n}{3} \frac{1}{n^6} - \dots \qquad \blacksquare$$

G - simple

Prop 2 $\varphi_k(G) \le 1 - \sum_{M} \frac{1}{[G:M]^k} = 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G:M]^{k-1}}$

M - Max subgroup of G

Conj class of Max subgroups

$\oplus$

$\overline{}$

D

$$1 - \varphi_k(G) = P(\langle g_1 \dots g_k \rangle \neq G) \le \sum_{M} P(g_1 \dots g_k \in M)$$

$$\le \sum_{M} \frac{1}{[G:M]^k} \quad \text{where} \quad [G:M] = \frac{|M|}{|G|}$$

$\mathcal{M} = \{M^G = gMg^{-1}\} = [G:M]$ bc G-simple,

M - max $\Rightarrow M \triangleleft G$

Thus

$$1 - \varphi_k(G) \le \sum_{M} \frac{1}{[G:M]^k} = \sum_{\mathcal{M}} \sum_{M \in \mathcal{M}} \frac{1}{[G:M]^k}$$

$$= \sum_{\mathcal{M}} \frac{1}{[G:M]^{k-1}} \quad \square$$

Th [Liebek-Sholev]

cc of max subgroups in A_n

$$= \frac{n}{2}\,(1+o(1))$$

/ $M_k = A_k \times A_{n-k}$ ← $\frac{n}{2}$ of them /

$$[A_n : M_k] = \frac{1}{2}\binom{n}{k}$$

Now $1-\varphi_2(A_n) \le \sum_{k=1}^{n/2} \frac{1}{\binom{n}{k}} + [\text{rest}]$

& $[\text{rest}] < c^{-n}$ uses CFSG

Example $\quad G = PSL(2,p)$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a b c d \in \mathbb{F}_p,\ ad-bc=1 \right\} \Big/ \left\{ \begin{pmatrix} \pm 1 & \\ & \pm 1 \end{pmatrix} \right\}$$

$$|PSL(2,p)| = \frac{1}{2(p-1)} (p^2-p)(p^2-1) = \frac{p(p-1)(p+1)}{2}$$

L1 $\quad M = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right\}, \quad [G:M] = p+1$

L2 $\quad [\#\ \text{conj. classes of } M] \leq 7$

Thus $\quad \varphi_2(G) > 1 - \dfrac{7}{p+1} \to 1$ as $p \to \infty$

Th [Breuillard - Gamburd]

$\approx$ such Cayley (g_1, g_2) are expanders

Back to S_n

Th [Jordan, 1873]

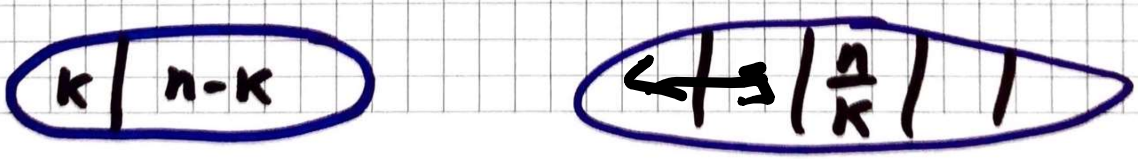
$G \leq S_n$ primitive & contains cycle of prime length $p \leq n-3$

Then $G = S_n$ or A_n

Def primitie := transitive + imprimitive

transitive := $\text{orbit}_G(1) = \{1 \dots n\}$

imprimitive := does not preserve block structures



L1 $P(\langle \sigma, w\rangle \text{ is transitive}) = 1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right)$

D $$P(\ ) < \sum_{k=1}^{n/2} \binom{n}{k} \frac{1}{\binom{n}{k}^2} = \sum_{k=1}^{n/2} \frac{1}{\binom{n}{k}} = \frac{1}{n} + \frac{O(1)}{n^2}$$ ◻

L2 $P(\langle \sigma, w\rangle \text{ is imprimitive}) = O\left(\frac{n}{2^{n/2}}\right)$

D $n = dk$, blocks of size d

\# such block structures $= \frac{1}{k!}\binom{n}{d \ldots d} = \frac{n!}{(d!)^k\, k!}$

$$\Rightarrow P(\ ) < \sum_{d \mid n} \frac{n!}{(d!)^k\, k!} \cdot \left[\frac{(d!)^k\, k!}{n!}\right]^2 < \sum_{k=2}^{n/2} \frac{(n/k)!^k\, k!}{n!}$$

$$= \frac{(n/2)!\, 2^n}{n!} + \ldots + \frac{2!\,(n/2)!^2}{n!} < \left(\frac{n}{2}\right) 2 \Big/ \binom{n}{n/2} < \frac{n}{2^{n/2}}$$ ◻

Cor $P(\langle \sigma, \omega \rangle = \text{primitive}) = 1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right)$

L3 $P\left(\begin{matrix} \sigma \text{ has no prime cycles} \\ \text{of length } \; p \le n-3 \end{matrix} \right) > 1 - \frac{c}{\log \log n}$

Cor + L3 $\Rightarrow$ Dixon's th

/By Jordan's th/ $\blacksquare$

Main L [Erdős-Turan, corrected] $\leftarrow$ 1965 + IP_{2001}

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

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

SL1 $\mathbb{E}[\#\ \ell\text{-cycles in } \sigma \in S_n] = \dfrac{1}{\ell}$

D $\mathbb{E} = \binom{n}{\ell} \cdot \dfrac{(\ell-1)!\,(n-\ell)!}{n!} = \dfrac{1}{\ell}$ $\blacksquare$

Cor $\mathbb{E}[\#\text{ cycles in } \sigma] = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$

$= \log n + \gamma + O(\frac{1}{n})$, γ - Euler-Mascheroni const

≈ 0.57721566

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

$$\mathbb{E}[(\#\text{ of } \ell\text{-cycles})(\#\ m\text{-cycles})] = \frac{1}{\ell m}$$

/ c.f. $\mathbb{E}[XY] = \mathbb{E}[X]\,\mathbb{E}[Y]$ /

X, Y - indep

$$\text{D} \quad \mathbb{E} = \sum_{\substack{A\text{-}\ell\text{-subset} \\ B\text{-}m\text{-subset}}} P\begin{pmatrix} G \text{ has cycle at } A \\ \text{and at } B \end{pmatrix}$$

$$= \binom{n}{\ell,\, m,\, n-\ell-m} \frac{(\ell-1)!\,(m-1)!\,(n-m-\ell)!}{n!}$$

$$= \frac{n!}{\ell!\, m!\, (n-\ell-m)!} \quad \text{——} \;\; '' \;\; \text{——}$$

$$= \frac{1}{\ell m}$$

■

SL3 $\mathbb{E}[(\#(\ell\text{-cycles}))^2] = \begin{cases} \frac{1}{\ell}, & 2\ell > n \\ \frac{1}{\ell} + \frac{1}{\ell^2}, & 2\ell \leq n \end{cases}$

D $\mathbb{E}[\#\,\ell\text{-cycles}] = \frac{1}{\ell}\sum_{i=1}^{n} P(i \in \ell\text{-cycle}) = \frac{1}{\ell}$

$\Rightarrow \; P(i \in \ell\text{-cycle}) = \frac{1}{n} \qquad \forall i, n, \ell$

$$\mathbb{E}[(\#\,\ell\text{-cycles})^2] = \frac{1}{\ell^2}\sum_{i=1}^{n}\sum_{j=1}^{n} P(i,j \in \ell\text{-cycle})$$

$$= \frac{1}{\ell^2}\sum_{i=1}^{n} \underset{j=i}{P(i \in \ell\text{-cycle})} + \frac{1}{\ell^2}\sum_{i \neq j} P(i \in \ell\text{-cycle}) \times P(j \in \ell\text{-cycle} \mid i \in \ell\text{-cycle})$$

$$= \underbrace{\frac{1}{\ell^2}\, n\, \frac{1}{n}}_{1/\ell^2} + \underbrace{\frac{1}{\ell^2}\, n\, \frac{1}{n}(n-1)}_{1/\ell^2 \;\; (n-1)} \cdot (*)$$

$$(*) = \frac{\ell-1}{n-1} + \frac{n-\ell}{n-1}\,\frac{1}{n-\ell}$$

$$\mathbb{E}\left[(\#\text{ of } \ell\text{-cycles})^2\right] = \begin{cases} \frac{1}{\ell^2} + \frac{1}{\ell^2}(\ell-1) & 2\ell > n \\ \frac{1}{\ell^2} + \frac{1}{\ell^2}\,\ell & 2\ell \le n \end{cases}$$

$$= \begin{cases} \frac{1}{\ell} & 2\ell > n \\ \frac{1}{\ell} + \frac{1}{\ell^2} & 2\ell \le n \end{cases}$$

E-T main result:

log order of random σ

is Normal w/ $\mathbb{E} = \frac{1}{2}(\log n)^2$