L21
5/15/2020

Igor Pak

Bias of the PRA

Before: $\Gamma_k(G)$ = graph on generating k-tuples $\langle g_1 \dots g_k \rangle = G$, $k \geq d(G)$

PRA: - random walk on $\Gamma_k(G)$
- output random g_i, $i \in \{1 \dots k\} \leftarrow Q$

#vertices $|\Gamma_k(G)| = \varphi_k(G)\,|G|^k$

Idea: $k \leftarrow$ large enough so that $\varphi_k(G) > 1-\varepsilon$

e.g. Th [Lubotzky, '02] $k = d(G) + O(\log\log|G|)$

Exc $\Rightarrow |Q, U|_{TV} < \varepsilon$ $\not\Rightarrow_{\text{post Exc}}$ $\text{sep}(Q^2, U) < c\varepsilon$

Bias: Distribution $Q \leftarrow$ of g_i, i random in $\bar{g} = (g_1 \dots g_k)$ and $(g_1 \dots g_k)$ random in $\Gamma_k(G)$

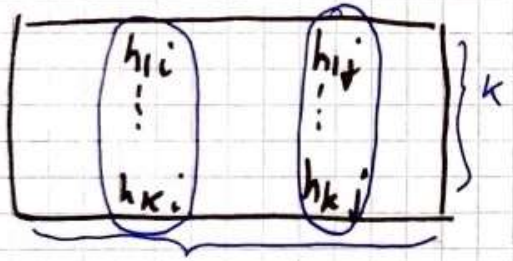
$\Rightarrow$ look for Bias only when $\varphi_k(G)$ small

Th [Hall, 1936] H – fin simple group, non-ab

$$\alpha_k(H) := \max\{m : d(H^m) = k\}$$

then $\alpha_k(H) = \#$ orbits of $Aut(H)$ acting on $\Gamma_k(H)$

▷ $G = H^m$ $\quad \langle g_1 \dots g_k \rangle = G$ $\quad g_i = (h_{i1} \dots h_{im})$

$\bar g \leftrightarrow$ 

$\bar g^{(i)} = \begin{pmatrix} h_{1i} \\ \vdots \\ h_{ki} \end{pmatrix}$

$\star\ h^{(1)} \dots h^{(m)} \in \Gamma_k(H)$ since $\langle h_{1i}, \dots h_{ki} \rangle = H$

L $(h_{ij}) \leftrightarrow \bar g \in \Gamma_k(G) \supseteq \{h^{(1)} \dots h^{(m)}\}$ lie in diff orbits of $Aut(H)$ on $\Gamma_k(H)$

$\psi : \begin{pmatrix} h_1 \\ \vdots \\ h_k \end{pmatrix} \to \begin{pmatrix} \psi(h_1) \\ \vdots \\ \psi(h_k) \end{pmatrix}$

$\Gamma_k(H) \Rightarrow \Gamma_k(H)$

Th $\Leftrightarrow$ **L** ▷ (lemma) $\Rightarrow$ obvious

since "$\in$ same orbit" is invariant under multiplication

$\Leftarrow$ direction — Suppose true for $m-1$

(By induction) $h^{(1)} \dots h^{m-1}$ < diff orbits $\Rightarrow$ gen'te H^{m-1}

Take $h^1 \dots h^{m-1} h^m = \underbrace{\left(h_{ij} \middle| \right)}_{m-1} \Big\}k \Leftrightarrow \bar{g}$

Observe $\{h^1 \dots h^m\} \Rightarrow \langle \bar{g} \rangle = \langle g_1 \dots g_k \rangle = (* * \dots * \bullet) \subset H^m$

this subgroup W contains H^{m-1} $\quad W$

Let $B = \langle (1 \dots 1 \bullet)^m \in \langle \bar{g} \rangle \rangle \subset H$

B is normal in H $\Rightarrow$ $B = 1$ or H

If $B = H$ ✓ Let $B = 1$, H-normal $\Rightarrow \exists x, y \in H$

s.t. $[x, Y] = xyx^{-1}y^{-1} \neq 1$

$\Rightarrow$ $(x\,1 \dots 1\,u) \in W$

$(y\,1 \dots 1\,v) \in W$

$(x^{-1}y^{-1}xy \dots 1\,1) \in W$

$\Rightarrow$ contradiction

Q: where the assumption was used?

Last time [L] Hall thm $\Rightarrow$ $\alpha_2(A_n) > \frac{n!}{8}$ n-large enough

$\Gamma_2(A_n) = \{(x,y) : x,y \in A_n, x \neq y, x \sim y\}$

$|\Gamma_2(A_n)| > \frac{1}{2}|A_n|^2 = \frac{n!^2}{8}$

$\alpha_2(A_n) > \frac{|\Gamma_2(A_n)|}{|Aut(A_n)|} > \frac{n!^2/8}{n!}$ n-large enough ☑

Cor $G := A_n^{n!/8}$ **then** $\varphi_k(G) \to 0$ as $k \to \infty$

$d(G) = 2$ $\forall k = o(n)$

/ $\forall n$ large enough /

$\varphi_k(A_n^{n!/8}) \leq [\varphi_k(A_n)]^{n!/8} < \left(1 - \frac{1}{n^k}\right)^{n!/8}$

$\varphi_k(A_n) = P(\langle \sigma_1, \dots \sigma_k \rangle = A_n) < 1 - P(\sigma_1(1) = \dots = \sigma_k(1) = 1) = 1 - \frac{1}{n^k}$ ☑

Thus this is a group to look for bias!

L $\varphi_k(A_n^{n!/8}) \geq [\varphi_k(A_n)]^{n!/8}\left(1 + O\left(\frac{1}{n!^{k-3}}\right)\right)$ $k \geq 4$

$\#\text{Orbits} > \frac{|A_n|^k}{|S_n|} = \frac{(n!/2)^k}{n!}$ we have $n!/8$ of them. ☑

/ BPay Paradox explained: $h^{(1)} \dots h^{(m)} \in \Gamma_k(H)$

$P(h^{(1)} \dots h^{(m)} \in$ diff orbits of $Aut(H))$

$= (1 - \frac{1}{N})(1 - \frac{2}{N}) \dots (1 - \frac{m-1}{N}) > 1 - \frac{m^2}{2N}$

$m = n!/g \qquad N = \frac{(n!/2)^k}{n!} > c(n!)^3$ if $k \geq 4$ /

$\Rightarrow \exists\, \bar{g} \leftrightarrow (h^{(1)} \dots h^{(m)})$ random in $\Gamma_k(G)$

$\bar{Q} \leftarrow$ distr of $h^{(1)}$ from $\bar{g}$

$Q \leftarrow$ distr of $h^{(1)}$ from $\Gamma_k(H)$

Then $|\bar{Q} - Q|_{TV} \leq O(\frac{1}{n^{k-3}})$

Th [Babai-PT 2004] $G = (A_n)^{n!/g}$, $k = o(n)$, $k > 4$

$Q \leftarrow$ distr of g_1 in random unif $(g_1 \dots g_k) \in \Gamma_k(G)$

Then $|Q - U| \to 1$ as $n \to \infty$

Proof of Bias

$G = A_n^{n!/8}$, $M = n!/8$

$\bar{g} \in \Gamma_k(G)$ $\quad \bar{g}_i = g(\sigma_1, \dots \sigma_M)$

$\bar{g} = (g_1 \dots g_k)$ $\quad$ If $g_1 \in G$ unif $\Rightarrow P(\sigma_1(1) = 1) = \frac{1}{n}$

$\perp$ $g_1 \in G$ from $Q \Rightarrow$ $P(\sigma_1(1) = 1) = \frac{1}{n} - \frac{1}{n^k} + O\left(\frac{1}{n^{2k-1}}\right)$

B

D $H^{(1)} = \begin{pmatrix} \sigma_{11} \\ \vdots \\ \sigma_{k1} \end{pmatrix}$ $\quad h^{(1)} \in \Gamma_k(A_n] \ (\approx)$ not all $\sigma_{i1}(1) = 1$

$P(\langle \sigma_{11} \dots \sigma_{k1} \rangle = A_n) = 1 - \frac{1}{n^k} n + \frac{1}{n(n-1)^k} \binom{n}{2}$ (Babai th)

$+ \frac{1}{2(n(n-1))^k} \binom{n}{k}$

A

Then

$P(B|A) = \frac{P(A|B)P(B)}{P(A)}$ $\quad P(B) = \frac{1}{n}$

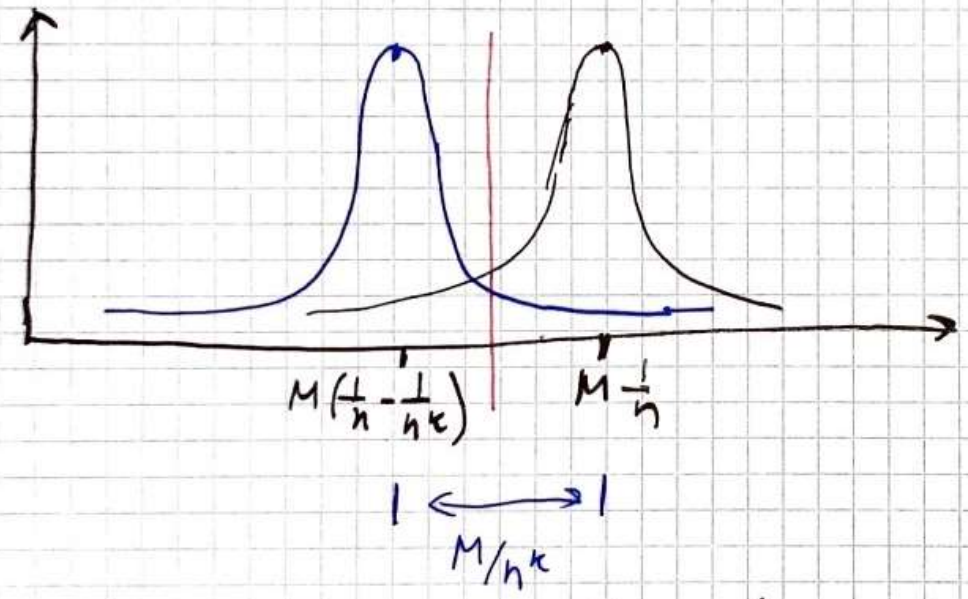
$= 1 - \frac{1}{n^{k-1}} + O\left(\frac{1}{n^{2k-2}}\right)$

$= \left(\frac{1}{n}\right) \frac{1 - 2/n^{k-1} + O(\ )}{1 - 1/n^{k-1} + O(\ )} = \frac{1}{n} - \frac{1}{n^k} + O(\ )$ ☐

$G = A_n^{n!/g}$ $\qquad g = (\sigma_1, \dots \sigma_M)$, $\quad M = n!/g$

$\mathbb{E}[\#\, \sigma_i(1) = 1] = M \cdot \frac{1}{n}$ $\qquad g$ uniform.

$\mathbb{E}[\#\, \sigma_i(1) = 1] = M \cdot [\frac{1}{n} - \frac{1}{n^k} + O(\,)]$ $\qquad g \in Q$



Use Chernoff Bound

Let $X := \{ \bar{g} \in G$ s.t. $\#\{\sigma_i(1) = 1\} > M(\frac{1}{n} - \frac{1}{2n^k})$

then $|X| \geq |G| \left(1 - \frac{n^k}{\sqrt{M}}\right)$

$Q(X) < \frac{n^k}{\sqrt{M}} \to 0$

$U(X) \to 1$

as $n \to \infty$ ▨

STORY

$(g_1 \dots g_k \textcircled{h})$