L22
5/18/2020

Exhibiting the Bias

Igor Pak

Last time: $G = (A_n)^{n!/8}$, $k \geqslant 4$, $k = o(n)$

$Q_k \leftarrow$ distr of g_i in random $\bar{g} = (g_1 \dots g_k) \in \Gamma_k(G)$

Th [Babai-P] $|Q - U|_{TV} \to 1$ as $n \to \infty$

Explanation:

(1) $\varphi_k(G) < \left(1 - \frac{1}{n^k}\right)^{n!/8} \to 0$

(2) $\exists$ subset $X \subset G$ s.t. $\frac{|X|}{|G|} \to 1$, $Q_k(X) \to 0$
/explicitly constructed/

Today: We exhibit the bias.

Construct words $w = \text{word}[x_1, x_2 \dots]$

s.t. length $|w| = \text{poly}(n)$

$w[Q_k] = 1$ whp
$w[U] \neq 1$ whp

} Mistaken law in G!

Idea: Monotone formulas

$Y_1 Y_2 \ldots$ ← iid elts in G, from Q

Let us assume: $P(Y_i = 1) < \frac{1}{n}$, n- large

$\begin{cases} Y_i \equiv 1 & \leftarrow \text{Tuth} \\ Y_i \neq 1 & \leftarrow \text{False} \end{cases}$

$\Rightarrow$ $Y_i \cdot Y_j = 1 \Leftrightarrow Y_i \wedge Y_j = \text{True}$

$[Y_i \cdot Y_j] = 1 \Leftrightarrow Y_i \vee Y_j = \text{True}$

Main Ex $Q = U$ on A_n

$P(Y_i = 1) = \frac{1}{(n!/2)}$ $\qquad P([Y_i \cdot Y_j] = 1) = P(Y_i \cdot Y_j = Y_j \cdot Y_i)$

$P(Y_i \cdot Y_j = 1) = \frac{1}{(n!/2)}$ $\qquad = \frac{P(n)}{|A_n|} = \frac{e^{O(\sqrt{n})}}{(n!/2)}$

/ all factorially small $\Leftrightarrow = O(n^{-cn})$ /

Def (monotone formula)

F: $[(Y_1 \vee Y_3 \vee Y_6) \wedge (Y_2 \vee Y_4 \vee Y_7) \wedge (Y_1 \vee Y_5)] \vee [*] \dots$

$word_F \leftarrow [[[Y_1\ Y_3]\ Y_6] \cdot [[Y_2\ Y_4]\ Y_7]\ [Y_1\ Y_5],\ *] \dots$

We construct F so that $word_F$ works.

First STEP : From Q to U

L1 $\lambda \vdash n$, $C_\lambda \in$ corresp. conj. class in S_n or A_n

Then $diam\left(Cayley(A_n, C_1)\right) \leq cn$, some for S_n, $c > 1$

▷ ① $(i\,j) \in$ product of 2 ℓ-cycles (Exc)

② every $\sigma \in S_n \in$ product of $\leq (n-1)$ transpositions

②' $-\!\!\vdash\ \sigma \in A_n \in -\!\!/\!\!-\!\!-\ \leq n/2$ pairs of transp.

$\Rightarrow$ $diam < 2n$ ▨

● Exc $diam \leq (n-1)$ ● in S_n, $\leq \frac{n}{2}$ in ● A_n ● ③

L2 $R = C_\lambda$, $G = A_n$ or S_n

$\{X_t\}$ ← r.w. on Cayley $(G, R) = \Gamma(G, R)$

Then $mix = O(n^3 \log n)$

D We know: $mix = O(Diam\ N_\gamma\ |R|\ \log |G|)$

where $\gamma = \{\gamma_g : 1 \to g \ \forall g \in G\}$ paths in $\Gamma(G, R)$

Consider $\bar{\gamma} = \bigcup a^{-1} \gamma a \quad \forall a \in Aut(G) \supseteq S_n$ /

Since R ← inv under $Aut(G)$, $\bar{\gamma}$ valid collection of paths.

$\Rightarrow N_{\bar{\gamma}} \le \frac{Diam}{|R|} \Rightarrow mix = O(Diam^2 \log |G|)$

$= _{L1}\ O(n^2 n \log n) = O(n^3 \log n)$ ▨

Known: $mix = O(n \log n)$, achieved on $R = \{(i\ i)\}$ transpositions

Biased dist Q on $A_n = G$

$X_1 X_2 \ldots \leftarrow$ iid on A_n from Q

$Y_i := (z_1^{-1} X_1 z_1)(z_2^{-1} X_2 z_2) \ldots (z_\ell^{-1} X_\ell z_\ell)$

$\ell = O(n^3 \log n) \Rightarrow$ r.w. on conj. class of X_1

where $z_i \leftarrow U$ on G.

$\Rightarrow$ if $Q(1) \neq 1$ whp $\Rightarrow$ Y_i is nearly-uniform

$\text{sep}(\ ) \geq \varepsilon \Leftrightarrow P(Y_i = g) \geq \frac{1-\varepsilon}{|G|}$

$Q(1) = 1$ whp $\Rightarrow$ $Y_i = 1$ u.h.p.

u.h.p $\Leftrightarrow$ w/ $P > 1 - O(n^{-cn})$

We want: word $(X_1 X_2 \ldots)$ s.t $X_i \leftarrow U \Rightarrow$ word $\neq 1$ whp

and $X_i \leftarrow Q \Rightarrow$ word $= 1$ whp.

Thus $z_i \leftarrow X_i \leftarrow$ in U case ✓

Q irrelevant ✓

Back to $\Gamma_k(A_n^{n^{1/8}})$, $k = o(n)$

$\bar{g} = (g_1 \dots g_k) \in \Gamma_k$

$g_i = (\sigma_1, \sigma_2 \dots \sigma_M)$, $M = n^{1/8}$

$\sigma_i \leftarrow$ iid, $\sigma_i \in A_n$ unif vs. near-uniform

---

Fix $n = p \leftarrow$ prime. $x \in (g_1)^p$.

$$\begin{cases} P(\sigma_i^p = 1) = \frac{1}{p} & \forall \sigma_i \leftarrow \text{unif.} \\ P(\sigma_i^p = 1) = \frac{1}{p} + \frac{1}{p^k} + O\left(\frac{1}{p^{2k-1}}\right) \in Q_k & \text{/no fp's is slightly more likely than not/} \end{cases}$$

We now need to construct a clever word which would distinguish two possibilities.

Th (Ajtai, 1983)

Such words / formulas always exist / monotone formula of poly length /

Bios amplification

Ex $X_i \leftarrow \begin{cases} 1 & w/\ P = 2/3 \\ 0 & w/\ P = 1/3 \end{cases}$ $\quad X_i' \leftarrow \begin{cases} 0 & w/\ P = 2/3 \\ 1 & w/\ P = 1/3 \end{cases}$

$$(X_1 \vee X_2) \wedge (X_3 \vee X_3) = \left(\frac{8}{9}\right)^2 = \frac{64}{81}$$
$$(X_1' \vee X_2') \wedge (X_3' \vee X_4') = \left(\frac{4}{9}\right)^2 = \frac{16}{81}$$

} (2:1) ratio $\Rightarrow$ (4:1) ratio

$X_i \leftarrow \begin{cases} 1 & w/\ P = q \\ 0 & w/\ P = 1-q \end{cases}$ $\quad X_i' \leftarrow \begin{cases} 1 & w/\ P = q' \\ 0 & w/\ P = 1-q' \end{cases}$

Ajtai: $\exists$ Formula of length $\text{Poly}\left(\frac{1}{q'-q}\right)$

s.t. $\begin{cases} \text{Formula}(X_i) = 1 & \text{uhp} \\ \text{Formula}(X_i') = 0 & \text{uhp.} \end{cases}$

Explatation in HR terms