L19
5/11/2020

Igor Pak

Product Replacement Algorithm

Want: generate random elements in $G = \langle S \rangle$
(Black Box group) $S = \{s_1, \dots s_k\}$

We Know: Erdös-Rényi Alg to prune $|S| \to O(\log|G|)$

cost $= O(k \log|G| \mu)$

Babai Alg for $|S| = O(\log|G|)$

cost $= O(\log^4|G|)$ [Babai + P.]

Cooperman-Dixon Alg for $|S| = O(\log|G|)$

cost $= O(\log^2|G|)$

PRA ← Practical Alg by [Celler, Leedham-Green, Murray, Niemeyer, O'Brien]
(1995)

Claim in [CLMNO] : works in "100 steps"

Alg $\bar{s} \leftarrow (s_1 \dots s_k \underbrace{11 \dots 1}_{k})$, $m \leftarrow 2k$

Do: $\bar{s} = (s_1 \dots s_m) \rightarrow (s_1 \dots s_i\ s_j^{\pm 1} \dots s_m)$ ↻
or $(s_1 \dots s_j^{\pm}\ s_i \dots s_m)$ ↻

where (i,j), ± 1, ↻ chosen unif.

Repeat t steps

Output random s_i

Exc Prove that $t = 100$ is NOT enough to make $sep(Q,U) \leq \frac{1}{2}$

Our Main Goal: ① Prove that PRA does not work
② Prove that fixed version works in poly time.
③ cost = $O(k \log|G| \mu)$ time

Product Replacement Graph

$\Gamma_k(G)$, $k \geq d(G)$ ← min # gen's.

Vertices: $(g_1 \cdots g_k)$ s.t. $\langle g_1 \cdots g_k \rangle = G$, $g_i \neq 1_G$.

edges: $(g_1 \cdots g_i \cdots g_j \cdots g_k) \to (g_1 \cdots g_i g_j^{\pm 1} \cdots g_j \cdots g_k)$

or $\to (g_1 \cdots g_j^{\pm 1} g_i \cdots g_i \cdots g_k)$

Note: $|\Gamma_k(G)| = \#\text{vertices} = \varphi_k(G)\,|G|^k$

Questions about $\Gamma_k(G)$:

(1) connectivity

(2) bias

(3) expansion / mixing time

Connectivity of $\Gamma_k(G)$

Ex $G = \mathbb{Z}_p^m$, $p \leftarrow$ prime, $k = m$

$$(g_1 \cdots g_m) \leftrightarrow \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{nm} \end{pmatrix} = A \quad \leftarrow \underline{\text{vertices}}$$

$A \to A \begin{pmatrix} 1 & & \\ & \ddots & \pm 1 \\ & 0 & \ddots \end{pmatrix} = E_{ij}^{\pm 1}$ or $E_{ij}^{\pm 1} A$ $\leftarrow$ edges

$\det(A E_{ij}^{\pm 1}) = \det(A) \Rightarrow \Gamma_m(\mathbb{Z}_p^m)$ $\underline{(p-1)}$ conn. comp'ts.

Prop $\Gamma_2(S_n)$, $\Gamma_2(A_n)$ has an Bounded # conn. comp.

D (Higman) $[g_1 g_2]^G \leftarrow$ conj clas is invariant on conn. comp.

eg. $[g_1 g_2 g_2] = (g_1 g_2)(g_2)(g_2^{-1} g_1^{-1}) g_2^{-1} = [g_1 g_2]$

or $[g_2 g_1, g_2] = (g_2 g_1)(g_2)(g_1^{-1} g_2^{-1})\, g_2^{-1}$

$= g_2 (g_1 g_2 g_1^{-1} g_2^{-1}) = [g_1, g_2]^{(g_2^{-1})}$

$\Rightarrow$ one needs unbounded # gen's $\langle \sigma, \omega \rangle = A_n$ with distinct $[\sigma, \omega]$

Take $\sigma = (12\ldots n)$, $\omega = (12\ldots p)$, use Jordan's thm ▨

Note: $\exists$ exp # of conj. classes of $[\sigma, \omega] \Rightarrow$ exp # of conn. comp's

Th [Guralnick-P] Same holds for $G = SL(2, p)$, etc.

Conj $\Gamma_k(6)$ conn $\forall k \geq d(6) + 1$

Th [Dunwoody] 1970 Conj holds for G-solvable

Positive results

$d(G)$ = min # gen's , $m(G)$ = max # non-redundant gen's

Th $\Gamma_k(G)$ - conn $\forall$ $k \geq d(G) + m(G)$

▷ 1) $(g_1 \dots g_k) \to (g_1 \dots g_{i-1} \mid g_{i+1} \dots g_k)$

2) $(\dots g_i \dots g_j \dots) \to (\dots g_i \; g_j \; g_i \dots) \to (\dots \mid g_j \dots g_i)$

$\to (\dots g_j \dots g_j \dots g_i \dots) \to (\dots g_j \dots g_i \dots g_i \dots) \to (g_j \; g_i \mid \dots)$

3) $(\dots g_i \dots \mid \dots) \to (\dots g_i \dots g_i \dots) \to (\dots g_i^{-1} \dots g_i \dots) \to (\dots g_i^{-1} \dots \mid \dots)$

Now $(g_1 \dots g_k) \to (g_1' \dots g_{dm}' \mid \dots \mid) \to (g_1' \dots g_{dm}' \, h_1 \dots h_d \mid \dots \mid)$

$\to (h_1 \dots h_d \mid \dots \mid)$ $\forall \bar{g}$ and $\langle h_1 \dots h_d \rangle = G$

$\Rightarrow$ $\Gamma_k(G)$ conn. ▨

Ex $G = S_n$, $d(S_n) = 2$, $m(S_n) = n-1$

$\Rightarrow \Gamma_{n+1}(S_n)$ - conn. [Cooperman-P.]

Open: $\Gamma_3(S_n)$ - conn? / Prop true $\forall n \leq 17$ /

Ex $G = SL(2,p)$, $d(G) = 2$, $m(G) \leq 4$

$\Rightarrow \Gamma_k(G)$ conn. $\forall k \geq 6$

Def $\Gamma = (V, E)$ has "large conn. comp" if

$\exists$ conn. comp of size $(1-o(1))|V|$ as $|V| \to \infty$

Th $\Gamma_3(A_n)$ has a large conn. comp.

D $\langle g_1 g_2 g_3 \rangle \in \Gamma_3(A_n)$ $\quad = A_n$ $\quad \langle h_1 h_2 h_3 \rangle$

$(g_1 g_2 g_3) \xrightarrow{\text{uhp}} (g_1 g_2 h_3)$ $\quad \leftarrow$ Dixon Thm

$\updownarrow$ $\qquad\qquad \downarrow$ uhp

$(h_1 h_2 h_3) \xleftarrow[\text{uhp}]{} (g_1 h_2 h_3)$ $\quad \blacksquare$