L5 (4/8/2020) Igor Pak

Probality on Finite Groups

G - fin. group, $|G|$ - order of G

$C_G(x) = \{ y \in G : yx = xy \}$ - centralizer of x

$Z(G) = \bigcap_{x \in G} C_G(x)$ - center of G

$K(g) = \{ a^{-1} g a, \ a \in G \}$ - conj class of $g \in G$

$k(G)$ = # conj classes in G

Ex $G = S_n$

$Z(S_n) = 1$, $k(S_n) = p(n)$ - # part $\vdash n$

$K(\sigma) = \{$ all $\omega \in S_n$ w/ same cycle part'n as $\sigma \}$

Exc (1) $|K(g)| = 1 \iff g \in Z(G)$

(2) G - non abelian $\Rightarrow$ $G/Z(G)$ is not cyclic

(3) $|G/Z(G)|$ is never prime

Def $\psi(G) := P(xy = yx)$

Prop $\psi(G) = \dfrac{k(G)}{|G|}$

$\triangleright$ $$\psi(G) = \sum_{g \in G} \frac{|C_G(g)|}{|G|^2} = \frac{1}{|G|^2} \sum_{g \in G} \frac{|G|}{|K(g)|}$$

$$= \frac{1}{|G|} \sum_{\text{conj class } K} \sum_{g \in K} \frac{1}{|K(g)|} = \frac{k(G)}{|G|}$$

$\blacksquare$

<u>Th</u> G - non-abelian [MacHale, 1974](?)

<u>Then</u> $\psi(G) \leq \frac{5}{8}$

$\triangleright$ By Exc (3) $|G/Z(G)| \neq 1, 2, 3$

$\Rightarrow |Z(G)| \leq \frac{|G|}{4}$

$\Rightarrow |\xi_G(g)| \geq 2$ for $\geq \frac{3|G|}{4}$ elts $g \in G$

$\Rightarrow k(G) \leq \frac{|G|}{4} + \frac{1}{2} \cdot \frac{3}{4} |G| = \frac{5}{8} |G|$

$\Rightarrow$ By Prop $\psi(G) \leq \frac{k(G)}{|G|} \leq \frac{5/8\ |G|}{|G|}$

$\leq \frac{5}{8}$ $\boxtimes$

<u>Exc</u> Check that MacHale Thm is sharp

Alg consequences

Suppose $\exists$ alg A for generating ε-uniform random $g \in G$, $\forall \varepsilon > 0$

Then testing G for abelian can be done in $O(\text{time of } A)$

▷ **Alg**

- Pick random $x, y \in G$
- check $xy = yx$

Repeat $O(1)$ times

By MacHale Thm if G - non-ab then $\mathbb{E}\,\#$ tries until $xy \neq yx$ is $O(1)$ $\blacksquare$

Remark

Th [Guralnick-Wilson, 2000]

(1) G - not nilpotent

$\Rightarrow P(\langle x,y\rangle \text{ - non-nilp}) \geq \frac{1}{2}$

(2) G - not solvable

$\Rightarrow P(\langle x,y\rangle \text{ - non-solv}) \geq \frac{19}{30}$

Proof based on CFSG

Exc Check that (1), (2) are sharp.

Erdős - Rényi random subproducts

$G = \langle g_1 \dots g_k \rangle$, so $S = \{g_1 \dots g_k\}$ is a generating set

Def (E-R subproducts)

$h \leftarrow g_1^{\varepsilon_1} \cdot \ldots \cdot g_k^{\varepsilon_k}$, $\varepsilon_1 \dots \varepsilon_k \in \{0,1\}$ indep unif. random

Main idea: $h \leftarrow$ pseudo-random

Th $P(h h' \neq h' h) \geq \frac{1}{4}$ $\forall$ G - non-abelian

[P, 2011]

Cor testing if G - abelian can be done in $O(k)$ steps.

L $G = \langle g_1 \dots g_k \rangle$, $H \subsetneq G$ subgroup.

Then $P(h \notin H) \geq \frac{1}{2}$

▷ $i \Leftarrow \min g_i \notin H$.

$$h = \underbrace{(g_1^{\varepsilon_1} \cdots g_{i-1}^{\varepsilon_{i-1}})}_{H} \, g_i^{\varepsilon_i} \, (g_{i+1}^{\varepsilon_{i+1}} \cdots g_k^{\varepsilon_k})$$

2 Cases: ① $h = (x) \cdot g_i^{\varepsilon_i} \cdot (y)$, $x, y \in H$

$\Rightarrow h \notin H$ w/ $P = \frac{1}{2}$

② $h = (x) \, g_i^{\varepsilon_i} \, (y)$, $x \in H$, $y \notin H$

$\Rightarrow h \notin H$ w/ $P \geq \frac{1}{2}$ ∎

Proof of Thm G - non - abelian

1) $Z(G) \neq G$, $H \leftarrow Z(G)$

$$P(h \notin Z(G)) \geq \frac{1}{2} \quad \text{by } \leq$$

---

2) Fix $h \notin Z(G)$, $H' \leftarrow C_G(h) \neq G$

$$P(h' \notin C_G(h)) \geq \frac{1}{2} \quad \text{by } \leq$$

Thus $P(h h' \neq h' h) \geq \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ $\blacksquare$

Remark By MacHale Thm

$$P(g g' \neq g' g) \geq \frac{3}{8} > \frac{1}{4}$$

Matrix groups

$G < GL(n, \mathbb{F}_q)$, q - fixed (say, 2)

$G = \langle g_1 \dots g_k \rangle$, $g_i \in GL(n, \mathbb{F}_q)$

Alg [testing G - abelian]

$h, h' \leftarrow g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k}$

$h h' =? \; h' h$

Repeat $O(1)$ times

cost of Alg

$O(k\omega)$, where

$\omega = O(n^{2.37\dots})$

mat mult cost

Q: Can one do better?

A: Yes! No need for ω

Freivals trick (1979)

Th $O(n^2 k)$ time suffice

D $h, h' \in GL(n, \mathbb{F}_q)$ fixed

Want: $h h' =? h' h$

Idea: $h h' v =? h' h v$, $v \in \mathbb{F}_q^n$ random

L $M \neq 1 \Rightarrow P(Mv \neq v) \geq \frac{1}{2}$ $\blacksquare$ ← **Exc**

Alg
$$\begin{cases} h, h' \leftarrow \text{random subproducts} \\ v \in \mathbb{F}_q^n \leftarrow \text{random vector} \\ \text{check } h h' v =? h' h v \end{cases}$$
Repeat $O(1)$ times

Exc: G - non-ab $\Rightarrow P(\neq) \geq \frac{1}{8}$

$\blacksquare$

Next time

Q: Can this alg be derandomized?

$\Leftrightarrow$ $O(k)$ possible for determ. alg?

A: No!

We prove that* $\Omega(k^2)$ for determ. alg's.

* Oracle model