

L9 (4/17/2020)

Igor Pak

Testing group properties

- Recall:
- (1) testing abelian, nilpotent, solvable
under random elts oracle (REO)
 - (2) REO for permutation groups $G \leq S_n$
 - (3) testing abelian w/out REO
(using random subproducts)

- Today:
- (4) testing nilpotent, solvable
using random subproducts
 - (5) testing $G \cong S_n, A_n$ under REO



Random subproducts

$$G = \langle S \rangle, \quad S = \{s_1, \dots, s_k\}$$

$$h \leftarrow s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}, \quad \varepsilon_i \in \{0, 1\} \text{ unig, indep.}$$

Th 1 $H \subsetneq G$ proper subgroup

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

Th 2 $k > 2 \log_2 |G| + O(\log \frac{1}{\varepsilon})$

$$P(\langle h_1, \dots, h_k \rangle = G) > 1 - \varepsilon$$

This is all we need to test

$G \leftarrow$ nilpotent(?), solvable(?)



[For $G \leftarrow$ abelian(?) only Th 1 was used.]

Nilpotent & solvable groups

Def

$G \in \text{fin. group}$

$[G, G] = \langle [g, h] = g^{-1}h^{-1}gh, g, h \in G \rangle$, $G/[G, G]$ - ab
commutator subgroup, $[G, G] \trianglelefteq G$ (normal subgroup)

Def

G - nilpotent if

$$G \supset G_1 \supset G_2 \supset \dots \supset G_e = 1,$$

where $G_{i+1} = [G_i, G]$

$$[A, B] = \langle [a, b], a \in A, b \in B \rangle$$

Def

G - solvable if

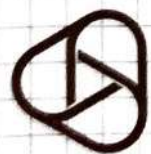
$$G \supset G_1 \supset G_2 \supset \dots \supset G_e = 1$$

where $G_{i+1} = [G_i, G_i]$

Obs

$$Ab \subsetneq Nilp \subsetneq Solv$$

Examples: $[S_n, S_n] = A_n$, $[A_n, A_n] = A_n \in \text{non-solv}$, $n \geq 5$



$$\left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, * \in \mathbb{F}_q \right\} \in \text{nilp}$$

$$\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, * \in \mathbb{F}_q, * \neq 0 \right\} \in \text{solv}$$

Proof $\rightarrow$ EXC

③

Commutator subgroup gen'n

$$G = \langle S \rangle, \quad S = \{s_1, \dots, s_k\}, \quad G' := [G, G]$$

Warning: $G' \neq \langle [s_i, s_j] \rangle$

ex $S_n = \langle (12), (12 \dots n) \rangle$

Th $A = \langle a_1, \dots, a_k \rangle, \quad B = \langle b_1, \dots, b_m \rangle, \quad A, B \leq G$

Then $[A, B] = \langle [a_i, b_j] \rangle^G$ normal closure

/smallest normal subgroup which contains

Warning: $G' \neq \langle [a_i, b_j]^{S_k} \rangle$

$hg := g^{-1}hg$

Exc Find an example.



$$\underline{L} \quad \left\{ \begin{array}{l} G = \langle S \rangle, S = \{s_1, \dots, s_k\} \\ H = \langle T \rangle, T = \{t_1, \dots, t_e\} \end{array} \right\} \quad \text{Suppose } H \neq H^G, H \leq G.$$

Then $P(h^g \notin H) \geq \frac{1}{4}$, where
$$\begin{aligned} h &= t_1^{\varepsilon_1} \dots t_e^{\varepsilon_e} \\ g &= s_1^{\alpha_1} \dots s_k^{\alpha_k} \\ \varepsilon_i, \alpha_i &\in \{0, 1\} \text{ unif indep} \end{aligned}$$

D $N_G(H) := \{g \in G : g^{-1}Hg = H\}$
normalizer of H in G

(1) $H \neq H^G \Rightarrow H \not\leq G \Rightarrow N_G(H) \neq G$

By Th 1 $P(g \notin N_G(H)) \geq \frac{1}{2}$

(2) Let $g \notin N_G(H) \Rightarrow H^g \cap H \neq H$

Note
$$\begin{aligned} h^g &= (t_1^{\varepsilon_1} \dots t_e^{\varepsilon_e})^g = g^{-1} t_1^{\varepsilon_1} \dots t_e^{\varepsilon_e} g = (t_1^g)^{\varepsilon_1} \dots (t_e^g)^{\varepsilon_e} \\ &= (t_1^{g_1})^{\varepsilon_1} \dots (t_e^{g_e})^{\varepsilon_e} \leftarrow \text{random subproduct on } H^g \\ H^g &= \langle t_1^g \dots t_e^g \rangle \end{aligned}$$

$\Rightarrow P(h^g \notin H) = P(h^g \notin H^g \cap H) \geq \frac{1}{2}$

(1) + (2) $\Rightarrow P(h^g \notin H) \geq \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$

Commutator Subgroup Alg

$$G = \langle S \rangle, \quad S = \{s_1, \dots, s_k\}, \quad G' := [G, G] = ?$$

Alg $R_0 = \{s_i^{-1} s_j^{-1} s_i s_j\}$

$$H_0 \leftarrow \langle [s_i, s_j] \rangle = \langle R_0 \rangle \quad \underline{L := c(\log |G|)}$$

Repeat $i = 1 \dots L$

$$L \leftarrow 4 \log |G| + 4 \log \frac{1}{\epsilon}$$

$$H_{i+1} \leftarrow \langle H_i, h^g \rangle = \langle R_{i+1} \rangle$$

$$R_{i+1} \leftarrow \{R_i \cup h^g\}, \quad \text{where}$$

$$\left\{ \begin{array}{l} g = s_1^{\epsilon_1} \dots s_k^{\epsilon_k} \\ h = r_1^{d_1} \dots r_n^{d_n} \end{array} \right\} \quad R_i = \{r_1, \dots, r_n\}$$

Output $H_L = \langle R_L \rangle \rightarrow G'$

Cost

Th Output = G' w.h.p
 $p > 1 - \epsilon$

$$O(k^2 L^2 n)$$



Testing for Nilp, Solv

Alg $G = \langle S \rangle$, $S = \{s_1, \dots, s_k\}$

$G_1 \leftarrow \text{CSA}[G, G]$, $G_1 = \langle R_1 \rangle$

$G_2 \leftarrow \text{CSA}[G, G]$, $G_2 = \langle R_2 \rangle$

$\vdots$

$G_L \leftarrow \text{CSA}[G_{L-1}, G]$, $G_L = \langle R_L \rangle$

Test $x = ?$ $\forall x \in R_L$

Yes $\Rightarrow$ Nilp uhp

No $\Rightarrow$ NOT Nilp.

Hidden issue

$|R_i|$ explodes

Thus at each stage prune

$|R_i| = O(\log |G|)$

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

Total cost $(k^2 L) \cdot (L \text{ iterations}) \mu$

$O((\log |G|)^4 \mu)$ $\leftarrow$ almost!

$\times \log \log |G|$

we want uhp. so $\varepsilon = O(\frac{1}{L})$



Alg for solv $\leftarrow$ same

$$G_i \leftarrow \text{CSA}[G_{i-1}, G_{i-1}]$$

What did we get?

One-sided Monte-Carlo Alg

If No $\Rightarrow$ True claim / NOT Nilp/Solv.

If yes $\Rightarrow$ Maybe claim / Nilp/Solv u.h.p.



Testing for S_n using REO

Input $G = \langle R \rangle$, $R = \{r_1, \dots, r_k\}$ Black Box group
 $n \in \mathbb{N}$

Output: yes if $G \cong S_n$
no $G \not\cong S_n$

say n - even

(0) Find $p+q=n$, p, q -prime, $p'+q'=n-2$, p', q' -prime. ≥ 2

(1) $g, h \leftarrow \text{random in } G$.
 $g^{pq} \stackrel{?}{=} 1 \Rightarrow g = \underbrace{\quad}_p \underbrace{\quad}_q$ } Repeat until found

(2) $h^{2p'q'} \stackrel{?}{=} 1 \Rightarrow h = \frac{1}{2} \underbrace{\quad}_{p'} \underbrace{\quad}_{q'}$ } Repeat until found

(3) $a \in h^{p'q'} = \left(\frac{1}{2}\right)$, $b \leftarrow \text{random in } G$
 $a^b \leftarrow \text{random transp.}$

$[a^b, g] \neq 1? \Rightarrow$ Output $S = \{a^b, a^b g\}$



Analysis

IF $\exists p, q, p', q' \Rightarrow$ Prob of success $> \frac{1}{pq} + \frac{1}{2pq} = \Omega(\frac{1}{n})$
random transp $\Omega(\frac{1}{n})$

Validity check

$$S_n = \langle x = (12), y = (12 \dots n) \rangle$$

check relations: $s_i^2 = (s_i, s_{i+1})^2 = (s_i, s_j)^2 = 1$
 $s_i := (\bar{y}^i x, y^i)$
 $(i-j) > 2$

Bonus story: Goldbach Conjecture

$n < 10^{14}$
Bratus - P.

Odd GC
 $n > 10^{40,000}$

Helpgo41 ✓

