L8 (4/15/2020) **Igor Pak**

Random generation in permutation groups

Problem: Given $G = \langle s_1, \ldots s_k \rangle$ output random $g \in G$

More precisely: $S = \{s_1, \ldots s_k\} \subset S_N$, $GL(n, \mathbb{F}_q)$, etc.

Want: probab. alg. which outputs from Q on G

s.t. $\frac{1-\varepsilon}{|G|} < Q(g) < \frac{1+\varepsilon}{|G|} \quad \forall g \in G$

$\boxed{\forall \varepsilon > 0}$

We will solve Problem in the future.

Today: the case $G \subseteq S_N$

Last L: ε-R Thm

$g_1 \dots g_k \leftarrow$ uniform random in G

$h = g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k}$, $\quad \varepsilon_i \in \{0,1\}$ random subproducts

$Q(h) \leftarrow$ prob. of h

Then $\left[\frac{1-\varepsilon}{|G|} < Q(h) < \frac{1+\varepsilon}{|G|} \quad \forall h \in G \right]$ w/ Prob $> 1-\delta$

$$k > 2 \log_2 |G| + 2 \log_2 \frac{1}{\varepsilon} + \log \frac{1}{\delta} + 1$$

Thus: if $\varkappa \leftarrow$ cost of gen'n $\underline{1}$ random el't

Then generating $\underline{m}$ random el'ts in

$$O(\varkappa \log_2 |G| + m k \mu)$$

where $\mu \leftarrow$ cost of mult in G.

Permutation groups

$G = \langle R \rangle$, $R = \langle s_1 \dots s_k \rangle$, $s_i \in S_N$

Th (1) $|G|$ and random $g \in G$ can be computed
[Sims, 1971] in time $\mathrm{poly}(N, k)$

(2) Moreover group membership $x \overset{?}{\in} G$, $x \in S_N$
can be decided in $\mathrm{poly}(N, k)$

Sims (197) $\leftarrow N^6$, Knuth (1991) $\leftarrow N^5$ Deterministic

[Cooperman-Finkelstein $\leftarrow N^4$ Probab]

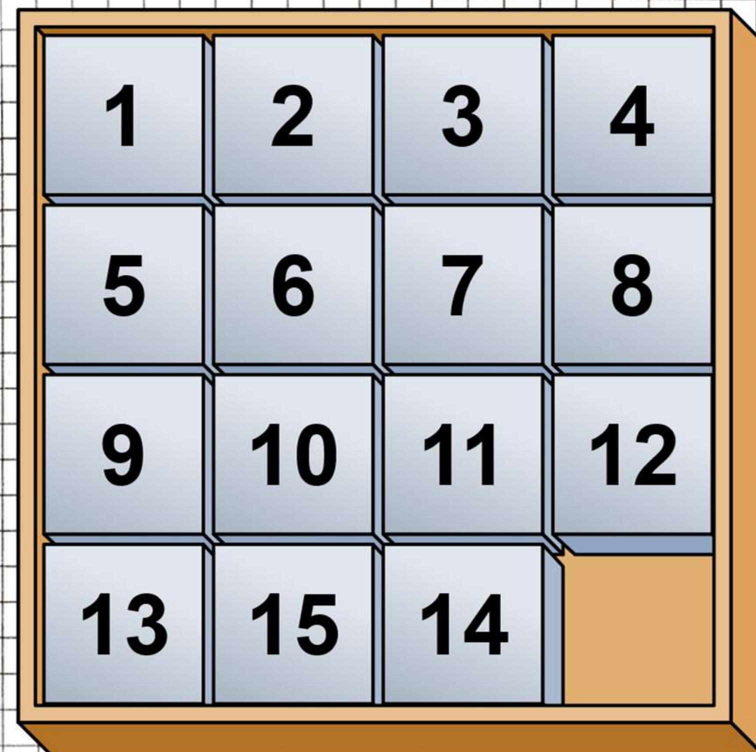
↑

Coming UP

Examples of Pemutation groups

① Rubik's cube ++

② Game 15



EXC (1) Understand why Sims Th $\Rightarrow$ $n \times n \times n$ Rubik's cube can be solved in poly(n) time

(2) Why is "Game (n^2-1)" a problem on perm. groups

Schreier's Lemma

① $G = \langle s_1 \dots s_k \rangle \quad , \quad s_j \in S_N$

Orbit of 1 $:= \{ i,\ 1 \le i \le N,\ \sigma(1) = i \text{ some } \sigma \in G \}$

$X_0 \leftarrow \emptyset \quad , \quad X_1 \leftarrow \{1\}$

$X_{i+1} = \bigcup_j \{ s_j(i) \ , \ i \in X_i \}$

$\le N$ steps

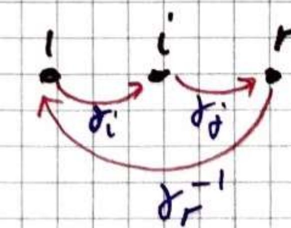
/easy to compute/

② $St_G(1) = \{ \sigma \in G \ : \ \sigma(1) = 1 \} < G$

Schreier's L (1928) $\quad \Gamma < G \ , \ \Gamma = \{ \gamma_i \ , \ i \in O_G(1) \ , \ \gamma_i(1) = i \}$ ①

Then

$$St_G(1) = \langle \sigma = \gamma_r^{-1} \gamma_j \gamma_i \ , \ i j r \in O_G(1) \text{ s.t. } \sigma(1) = 1 \Leftrightarrow \gamma_j(i) = r \rangle$$



Think of RC : [Do smth] → [minor change] → [UNDO]

Sims Alg $\left[G = \langle s_1 \ldots s_k \rangle \subset S_N \right]$

① Compute $O_G(1)$ as $\Gamma = \{ \gamma_i , \; i \in O_G(1) \}$

② Compute $St_G(1)$ via Schreier's Lemma

as $St_G(1) = \langle \gamma_r^{-1} \gamma_j \gamma_i \; : \; \gamma_j(i) = r \rangle$

$G \leftarrow St_G(1)$, Repeat until done.

$$G \supseteq St_G(1) \supseteq St_G(1,2) \supseteq \cdots \supseteq St_G(1,2,\ldots N) = 1$$

$|\Gamma_1| = O_G(1)$, $|\Gamma_2| = O_{St(1)}(2)$, $\ldots$, $|\Gamma_\ell| = O_{St(1\ldots \ell-1)}(\ell), \ldots$

Output ① $|G| \leftarrow |\Gamma_1| \cdot |\Gamma_2| \cdot \ldots$

② $g \leftarrow (\text{rand } \gamma_i \in \Gamma_1)(\text{rand } \gamma_j \in \Gamma_2) \cdot \ldots$

③ given $\sigma \in S_N$, check $i = \sigma(1) \in ? \; O_G(1)$. No $\Rightarrow$ "NO"
yes $\Rightarrow$ $\sigma \leftarrow \gamma_i^{-1} \sigma$, repeat w/ $St_G(1)$

Exc Fill in details for ①, ②, ③.

Major issue w/ Sims Alg

Number of gen's (!)

of $St_G(1 2 \ldots \ell)$ can (and does) explode

$k \to k^3 \to k^9 \to \cdots$

What to do?

Sims, Knuth + clever bookeping

[Cooperman-Finkelstein]

Reducing number of gen's

Alg $G = \langle S \rangle$, $S = \{s_1, \ldots, s_k\} \longrightarrow G = \langle R \rangle$ w.h.p., $|R| = O(\log |G|)$

$R \leftarrow \{h_1, h_2, \ldots, h_\ell\}$, $h_i \leftarrow s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$, $\varepsilon_i \in \{0,1\}$

random subproducts.

Th/L $\ell = 2\log_2 |G| + O(\log \frac{1}{\varepsilon}) \Rightarrow G = \langle R \rangle$ w/ $\Pr > 1 - \varepsilon$

$\triangleright$ $H_0 = 1$, $H_{i+1} = \langle H_i, h_{i+1} \rangle$

Recall: w/ $\Pr \geq \frac{1}{2}$ $h_{i+1} \notin H_i$

+ Exc $\blacksquare$

Back to Sims Alg

$G = \langle R \rangle$, $R = \{s_1 \dots s_k\} \subset S_N$, $\underline{\ell} := \log(N!) \geq \log|G|$
$= N\log N + O(N)$

(0) k gen's $\xrightarrow[CF]{}$ $O(\ell)$ gen's

cost $O(k\ell\mu)$

(1) compute $O_G(1)$, Γ_1

cost $O(\ell N\mu)$

(2) compute $\{\gamma_r^{-1}\gamma_j\gamma_i\}$

cost $O(N^2\mu)$

One more issue (!?!)

Error term $\varepsilon \leq \frac{1}{N}$

$\Rightarrow$ multiply cost by $(\log\frac{1}{\varepsilon})$
$= O(\log N)$

Repeat N times

$k \leftarrow O(N^2)$

Total cost

$$O(k\ell\mu + N^2\ell\mu \times N + \ell N\mu \times N + N^2\mu \times N)$$

$$= O(k\ell\mu + N^3\ell\mu)$$

$$= O(kN\log N\,\mu + N^4\log N\,\mu)$$

$\times\ O(\log N)$ ▨

How good is this S-C-F Alg?

Cost: $\leftarrow \quad O(N^4 (\log N)^2 \mu + \dots)$

Outputs: $\leftarrow \quad \Gamma_1, \Gamma_2, \dots, \Gamma_N$

w/ Pr: $\quad > 1 - \varepsilon$

$|G| = |\Gamma_1| \cdot |\Gamma_2| \cdots$

w/ Pr $> 1 - \varepsilon$

reliable?

Imp. Remark: we can check if Answer correct

Note: $|\Gamma_1| \cdot |\Gamma_2| \cdots \le |G|$ always

$(=) \iff$ we obtained all of $St_G(1 \dots \ell)$

NOT a subgroup.

Alg $\quad G = \langle s_1, \dots, s_k \rangle$

check group membership (3) $\forall s_i$

Yes $\Rightarrow$ (=) ✓

No $\Rightarrow$ try again

$\Rightarrow$ SCF Alg is in ZPP

/ zero error, but probab. exp time /

RC Exc (cont'd)

① Take $n \times n \times n$ RC. Here $N = O(n^2)$

Choose a smart order of Stab's so that no need for N iteration.

Q: Is $O(1)$ iterations enough in this case?

② Find $G = \langle S \rangle$, $G \neq S_n, A_n$ s.t. $\Omega(N)$ iterations

③ Read about M_{24} ← Mathieu group $\subset S_{24}$

How many iter do you need for M_{24}?