Random generation of finite simple groups

Group G

The **generating graph** $\Gamma(G)$ vertices $G \setminus 1$

edges $x - y \iff \langle x, y \rangle = G$

G finite & not cyclic

Def $\mathbb{P}(G) = \mathbb{P}(2 \text{ random elements gen. } G)$

$$= \frac{\#\text{ edges in } \Gamma(G)}{|G|^2}$$

Steinberg '62: If G is FSG then $\exists\, x, y$ s.t.

$\langle x, y \rangle = G$

e.g. $\Gamma(G)$ has an edge

$\mathbb{P}(G) > 0$

Dixon '69 $\lim_{n \to \infty} \mathbb{P}(A_n) = 1$

Sketch Let $G = A_n$

$p_n :=$ proportion of pairs which gen. a primitive group

$$= 1 - \frac{1}{n} + O(n^{-2}) \xrightarrow[n \to \infty]{} 1$$

stats of random perms

Jordan: If $H \leq S_n$ primitive & H contains a q-cycle for q prime, $q \leq n-3$ then $H = A_n$ or S_n

$$Q_n := \left\{ g \in G : \begin{array}{l} g \text{ has exactly one } q\text{-cycle } \& \\ \text{other cycles coprime to } q,\ q \text{ prime}, \\ q \leq n-3 \end{array} \right\}$$

$$q_n := \frac{|Q_n|}{|G|} \sim 1 - \frac{4}{3\log\log n}$$

If $g \in Q_n$ then g^k is a q-cycle some k

Let x, y uniform in G

$$\mathbb{P}(A_n \leq \langle x,y \rangle) \geq \mathbb{P}(\langle x,y\rangle \text{ primitive } \& \ x \in Q_n) \xrightarrow[n\to\infty]{} 1$$

CFSG-free, stats of random perms.

Liebeck-Shalev '95 If G a FSG

$$\lim_{|G|\to\infty} \mathbb{P}(G) = 1$$

CFSG (non-ab)

A_n $n \geq 5$ ← Dixon

Lie type e.g. $PSL_n(q)$ $q \to \infty$, $E_8(q)$ $n \to \infty$

Sporadic ← finitely many

Idea $\langle g,h \rangle \neq G \iff \exists\, M \leq_{max} G$ s.t. $g,h \in M$

So $$1 - \mathbb{P}(G) \leq \sum_{M \leq_{max} G} \left(\frac{|M|}{|G|}\right)^2 = \sum_{\substack{R \text{ rep} \\ \text{of conj.} \\ \text{class of max. sbgps.}}} \left(\frac{|R|}{|G|}\right)^2 \frac{|G|}{|N_G(R)|}$$

$$= \sum_{R \text{ rep}} \frac{|R|}{|G|} \xrightarrow[\substack{n\to\infty \\ q\to\infty}]{\text{WTS}} 0$$

E.g. $PSL_n(q)$ Kantor–Lubotzky '90

	~ subgroup	~ # conj classes
$\mathcal{C}_1$	parabolics	$2n$
$\mathcal{C}_2$	$GL_{\frac{n}{t}}(q) \wr S_t$ $t \mid n$	$\leq n$
		$\leq n$
$\mathcal{C}_3$		
$\mathcal{C}_4$		$\leq n$
$\mathcal{C}_5$	$GL_n(\sqrt[b]{q})$ b prime	$\leq \log q$
$\mathcal{C}_6$		1
$\mathcal{C}_7$		$\log n$
$\mathcal{C}_8$		4

If $M \in \mathcal{C}_1, \dots, \mathcal{C}_8$ then $\frac{|G|}{|M|} \geq \frac{1}{2} q^{n-1}$

So
$$\sum_{\substack{R \text{ rep} \\ \mathcal{C}_1, \dots, \mathcal{C}_8}} \frac{|R|}{|G|} \leq \frac{2}{q^{n-1}} \left(5n + 5 + \log n + \log q\right)$$
$$\xrightarrow[q \to \infty]{n \to \infty} 0$$

Class $\mathcal{S}$ similar.

Menezes–Quick–Roney-Dougal '13 G is FSG

$$\mathbb{P}(G) \geq \frac{53}{90} > \frac{1}{2}$$

equality iff $A_6 = G$

Computational Galois Theory

The subgroup of G *invariably generated* by $g_1, \dots, g_k \in G$ is $\langle g_1, \dots, g_k \rangle_I = \bigcap_{h_1, \dots, h_k \in G} \langle g_1^{h_1}, \dots, g_k^{h_k} \rangle$

e.g. $\langle (12), (1234) \rangle_I \leq \langle (13), (1234) \rangle \lneqq S_4$

Kantor–Lubotzky–Shalev, Guralnick–Malle 2010s:
G is FSG. $\exists\, x, y \in G$ s.t. $\langle x, y \rangle_I = G$

e.g. $\langle SL_n(\mathbb{C}) \rangle_I \leq$ upper Δ

$$\langle SL_n(\mathbb{Q}) \rangle_I \overset{??}{=} SL_n(\mathbb{Q})$$

($\neq$)

Let $f \in \mathbb{Z}[x]_n$, $G = Gal(f/\mathbb{Q}) \leq S_n$

For p prime, the degrees of irreducible factors of f mod p form a partition of n, call it λ_p.

Frobenius Density Theorem Fix a partition λ of n

Density of primes p s.t. $\lambda_p = \lambda$ $\sim$ Density of elements in G with cycle type λ

Given $f \in \mathbb{Z}[x]_n$, is $G = S_n$?

- Pick random primes $p_1, \dots, p_k$
- Do $\lambda_{p_1}, \dots, \lambda_{p_k}$ IG S_n?

If yes $G = S_n$

If no $\mathbb{P}(G = S_n) = \mathbb{P}(k \text{ random elts do not IG } S_n)$

Def $\mathbb{P}_I(G,k) = \mathbb{P}(k \text{ random elts IG } G)$

Pemantle-Peres-Rivin '15 $\exists \varepsilon > 0 \ \forall n \ \mathbb{P}_I(S_n, 4) > \varepsilon$

Our algorithm 1-sided Monte Carlo alg.

Eberhard-Ford-Green '17 $\lim_{n\to\infty} \mathbb{P}_I(S_n, 3) = 0$

Fix rank, $q \to \infty$, 2 elements Garzoni-McK '22+

Fix q (large), $n \to \infty$, 4 elements McK '21

S_n is Weyl group of SL_n

$$X^{q^n} + aX^{q^{n-1}} + \cdots + zX$$

$\mathbb{F}_q$

$\mathrm{Gal} \leq GL_n$