Igor Pak

Probability of generation

G – finite group

$d(G) = \min \#$ gen's

$\varphi_k(G) := P(\langle g_1 \ldots g_k \rangle = G)$, $k \geq d(G)$

$\varkappa(G) := \min\{k : \varphi_k(G) \geq \frac{1}{2}\}$

Problem given G, find $\varkappa(G)$
/estimate, math/

Main Th (Dixon, 1969, conj by Netto, 1892)

$\varphi_2(S_n) \to \frac{3}{4}$ as $n \to \infty$

$\varphi_2(A_n) \to 1$ — " —

Preliminaries

(1) $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \dots \times \mathbb{Z}_p$, $d(G)=1$

$$\varphi_1(G) = \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdot\ldots\cdot\left(1-\frac{1}{p}\right) \to 0$$

as $p \to \infty$

D $$\varphi_1(G) = \exp\left[\sum_{\substack{q<p \\ q\text{-prime}}} \log\left(1-\frac{1}{q}\right)\right]$$

up to a const

$$\approx \exp\left[-\sum_{\substack{q<p \\ \text{prime}}} \frac{1}{q}\right] \to 0$$

$\blacksquare$

(2) $$\varphi_2(G) = \left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\cdots\left(1-\frac{1}{p^2}\right)$$

$$> \prod_{n=2}^{\infty}\left(1-\frac{1}{n^2}\right) > 0$$

const

(3) $G = \mathbb{Z}_2^m$, $d(G) = m$

$$\varphi_m(G) = \left(1 - \frac{1}{2^m}\right)\left(1 - \frac{1}{2^{m-1}}\right) \cdots \left(1 - \frac{1}{2}\right)$$

$$> \prod_{n=1}^{\infty} \left(1 - \frac{1}{2^n}\right) = 1 - \frac{1}{2} - \frac{1}{4} + \frac{1}{32} + \frac{1}{128} - \cdots$$

const $\nearrow$

Exc $\varphi_{m+1}(G) > \frac{1}{2} \implies \varkappa(G) = m+1$

Random graph process (on n vert)

$G_0 = \emptyset$, $\quad G_{i+1} = G_i + e$, $\quad e \leftarrow$ random edge in K_n

$\tau \leftarrow$ stopping time, until

- G - connected
- G has a Δ
- G has a component of size n^{ε}
- G has a HG

⋮

Erdős - Renyi +++ resolved a lot of these questions

Random group process (in G)

$H_0 = 1$, $H_{i+1} = \langle H_i, g \rangle$, $g \in G$ unif.

$\tau :=$ first time i, $H_i = G$

$\varphi_k(G) = P(\tau \le k) \iff P(\tau > k) = 1 - \varphi_k(G)$

Prop 1 $\varkappa(G) \le 2\, E[\tau]$

▷ $P(\tau > 2\, E[\tau]) < \frac{1}{2}$ ☒

Prop 2 $E[\tau] \le 2 \log_2 |G|$

▷ $t < \tau \Rightarrow P(H_{t+1} \neq H_t) = 1 - \frac{|H_t|}{|G|} \geq \frac{1}{2}$

Thus expected time to at least double H_t is ≤ 2

$\Rightarrow E[\tau] \le 2 \log_2 |G|$ ☒

For $G = S_n$, $\log |S_n| = n \log n + O(n)$

so $\varkappa(S_n) = O(n \log n)$

D $\varkappa \leq 2 E[\tau] \leq 4 \log_2 |S_n|$ $\square$

<u>Prop 3</u> $E[\tau] \leq 2 \ell(G)$, where

$\ell(G) = \max$ length of $1 = H_0 \subsetneq H_1 \subsetneq H_2 \cdots G$

<u>Lemma</u> $\ell(S_n) = O(n \log \log n)$.

$\Rightarrow \varkappa(S_n) = O(n \log \log n)$

D $O_p := \max\{k : p^k \mid n!\}$

<u>Then</u> $O_p = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots$

$$\leq \frac{n}{p(1-\frac{1}{p})} = \frac{n}{p-1}$$

Then

$$\ell(S_n) \leq \sum_{\substack{p \leq n \\ p\text{-prime}}} O_p \leq n \sum_{\substack{p \leq n \\ p\text{-prime}}} \frac{1}{p-1}$$

$$\leq n \log\log n + O(n)$$

Indeed

$$\sum_{\substack{p < n \\ p\text{-prime}}} \frac{1}{p-1} \sim \int_1^n \frac{dx}{x \log x}$$

$$= \int_1^n \frac{d \log x}{\log x} = \log\log x \Big|_1^n$$

$\blacksquare$

Remark $\ell(S_n) \leq \frac{3}{2} n$

Th [Cameron - Solomon - Turull, 1989]

$$\ell(S_n) = \left\lfloor \frac{3n-1}{2} \right\rfloor - b_n \quad , \text{ where}$$

$b_n :=$ # of 1s in binary exp. of n

/ uses CFSG /

Def $m(G) :=$ max size of non-redundant gen set S, $\langle S \rangle = G$

Then $d(G) \leq m(G) \leq \ell(G) \leq \log_2 |G|$

Th (Whiston, 2000)

$m(S_n) = n-1$. / uses CFSG /

// $S_n = \langle (12), (23) \dots (n-1, n) \rangle$ //

Exc $m(SL(2,p)) = O(1)$

Exc $E[\tau] \le \ell(G) + C$, $C \leftarrow$ univ. const

Exc $|G| \le 2^m$ **Then**

$$\varphi_k(G) \ge \varphi_k(\mathbb{Z}_2^m) \quad \forall\, k \ge m$$

Exc $\varkappa(G) \ge E[\tau]/2$

(a companion to $\varkappa \le 2E[\tau]$)

What's coming

Th [Dixon]

$$\varphi_2(A_n) = 1 - O\left(\frac{1}{\log\log n}\right) \quad ✓$$

Th [Babai, 1989]

$$\varphi_2(A_n) = 1 - \frac{1}{n} - O\left(\frac{1}{n^2}\right)$$

/uses CFSG/