Combinatorics and Probability (Math 285)

Igor Pak, UCLA

Zoom Lecture 1 (March 30, 2020)

What this class is about?

Assorted recent and classical results in Combinatorial Probability.

Special emphasis on S_n and uniform random sampling of combinatorial objects.

Examples of subjects:

- Probability of generation, *Dixon's theorem*: $P(\langle \sigma, \omega \rangle = S_n) \to 3/4$ as $n \to \infty$,
- Random walks on $\mathbb{Z}^d$, special walks on the grid such as Gessel walk, Kreweras walk, etc.
- Random walks on groups such as S_n, $GL(n, q)$, $U(n, q)$, coupling and stopping time arguments
- Testing group properties (abelian, nilpotent, solvable) via Erdős–Renyi subproducts
- Testing finiteness of linear groups via random walks
- Random walk on linear extensions, approximation in polynomial time
- 1/3–2/3 conjecture for Young tableaux via random walks
- Random walk on contingency table, Burnside walks
- Wilson's LERW, uniform random trees, Aldous–Broder algorithm

L2 (4/1/2020) Igor Pak

Probability of generation

G – finite group

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

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

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

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

Main Th (Dixon, 1968, conj by Netto, 1892)

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

$\varphi_2(A_n) \to 1$ — " —

Preliminaries

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

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

as $p \to \infty$

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

up to a const

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

$\boxtimes$

(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

<u>Exc</u> $\varphi_{m+1}(G) > \frac{1}{2} \Rightarrow \varkappa(G) = m+1$

3

Random graph process (on n vert)

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

$\tau \leftarrow$ stopping time, until

- G - connected
- G has a $\triangle$
- G has a component of size n^{ε}
- G has a HC

⋮

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

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

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

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

Thus expected time to at least double H_t is ≤ 2

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

5

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

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

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

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

$\ell(G) = \underline{\max}$ $\underline{\text{length}}$ 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> $O_p = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \dots$

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

6

Then

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

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

Indeed

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

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

$\boxtimes$

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 /

// $S_n = \langle (1\,2), (2\,3) \ldots (n-1, n) \rangle$ //

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 $\varkappa \le 2E[\tau]$)

9

What's coming

Th [Dixon]

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

Th [Babai, 1989]

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

/uses CFSG/

10

L3 (4/3/2020) Igor Pak

Probability of generation

Last time: $\varphi_k(G) = P(\langle g_1 \dots g_k \rangle = G)$, $g_i \in G$ unif. indep

Th (Dixon) $\varphi_2(A_n) \to 1$ as $n \to \infty$

Th (Babai) $\varphi_2(A_n) = 1 - \frac{1}{n} + O(\frac{1}{n^2})$

Prop 1 $\varphi_2(A_n) < 1 - \frac{1}{n} + O(\frac{1}{n^2})$

D $1 - \varphi_2(A_n) \le \sum_{i=1}^{n} P(\sigma(i) = \omega(i) = i) - \sum_{i<j} P(\sigma(i) = \omega(i) = i, \sigma(j) = \omega(j) = j) - \sum_{i<j<k} + \dots$

$\le n \cdot \frac{1}{n^2} - \binom{n}{2} \frac{1}{n^4} + \binom{n}{3} \frac{1}{n^6} - \dots$ $\square$

1

G - simple

Prop 2 $\varphi_k(G) \le 1 - \sum_{M} \frac{1}{[G:M]^k} = 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G:M]^{k-1}}$

M - max subgroup of G Conj class of max subgroups

Φ

D $1 - \varphi_k(G) = P(\langle g_1 \dots g_k \rangle \ne G) \le \sum_{M} P(g_1 \dots g_k \in M)$

$\le \sum_{M} \frac{1}{[G:M]^k}$ where $[G:M] = \frac{|M|}{|G|}$

$\mathcal{M} = \{M^G = g M g^{-1}\} = [G:M]$ ie G - simple, M - max $\Rightarrow M \triangleleft G$

Thus

$1 - \varphi_k(G) \le \sum_{M} \frac{1}{[G:M]^k} = \sum_{\mathcal{M}} \sum_{M \in \mathcal{M}} \frac{1}{[G:M]^k}$

$= \sum_{\mathcal{M}} \frac{1}{[G:M]^{k-1}}$ $\square$

(2)

Th [Liebeck-Shalev]

$\#$ cc of max subgroups in A_n

$$= \frac{n}{2}\left(1+o(1)\right)$$

/ $M_k = A_k \times A_{n-k}$ ← $\frac{n}{2}$ of them /

$[A_n : M_k] = \frac{1}{2}\binom{n}{k}$

Now $1-\varphi_2(A_n) \leq \sum_{k=1}^{n/2} \frac{1}{\binom{n}{k}} + [\text{rest}]$

L $[\text{rest}] < c^{-n}$ uses CFSG

3

Example $\quad G = PSL(2,p)$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a,b,c,d \in \mathbb{F}_p,\ ad-bc=1 \right\} \Big/ \left\langle \begin{pmatrix} \pm 1 & \\ & \pm 1 \end{pmatrix} \right\}$$

$$|PSL(2,p)| = \frac{1}{2(p-1)}(p^2-p)(p^2-1) = \frac{p(p-1)(p+1)}{2}$$

L1 $M = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right\}, \quad [G:M] = p+1$

L2 $[\#\text{ conj. classes of } M] \leq 7$

Thus $\quad \varphi_2(G) > 1 - \frac{7}{p+1} \to 1$ as $p \to \infty$

Th [Breuillard - Gamburd]

$\approx$ such Cayley (g_1, g_2) are expanders

4

Back to S_n

Th [Jordan, 1873]

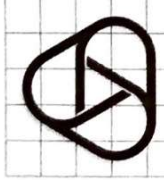
$G \leq S_n$ primitive & contains cycle of prime length $p \leq n-3$

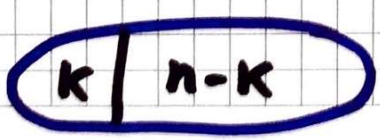
Then $G = S_n$ or A_n

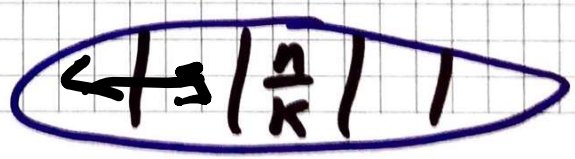
Def primitie := transitive + imprimitive

transitive := $\mathrm{orbit}_G(1) = \{1 \dots n\}$

imprimitive := does not preserve block structures







L1 $P(\langle \sigma, \omega \rangle \text{ is transitive}) = 1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right)$

D $P(\ ) < \sum_{k=1}^{n/2} \binom{n}{k} \frac{1}{\binom{n}{k}^2} = \sum_{k=1}^{n/2} \frac{1}{\binom{n}{k}} = \frac{1}{n} + \frac{O(1)}{n^2}$ ◻

L2 $P(\langle \sigma, \omega \rangle \text{ is imprimitive}) = O\left(\frac{n}{2^{n/2}}\right)$

D $n = dk$, blocks of size d

$\#$ such block structures $= \frac{1}{k!}\binom{n}{d \cdots d} = \frac{n!}{(d!)^k\, k!}$

$$\Rightarrow P(\ ) < \sum_{d \mid n} \frac{n!}{(d!)^k\, k!} \cdot \left[\frac{(d!)^k\, k!}{n!}\right]^2 < \sum_{k=2}^{n/2} \frac{(n/k)!^k\, k!}{n!}$$

$$= \frac{(n/2)!\, 2^n}{n!} + \dots + \frac{2!\,(n/2)!^2}{n!} < \left(\frac{n}{2}\right) 2 \Big/ \binom{n}{n/2} < \frac{n}{2^{n/2}}$$ ◻

(6)

Cor $P(\langle \sigma, \omega \rangle = \text{primitive}) = 1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right)$

L3 $P\left(\begin{array}{c}\sigma \text{ has no prime cycles} \\ \text{of length } p \le n-3\end{array}\right) > 1 - \frac{c}{\log\log n}$

$=$

Cor + L3 $\Rightarrow$ Dixon's th

/By Jordan's th/ $\blacksquare$

$=$

Main L [Erdös-Turan, corrected] $\leftarrow$ 1965+ (1 Proof)

$A = \{1 \le a_1 < a_2 < \dots < a_r \le n\}$

$P(\sigma \text{ has no cycles in } A) < \dfrac{1}{a_1 + a_2 + \dots + a_r}$

7

SL1 $\mathbb{E}[\#\ \ell\text{-cycles in } \sigma \in S_n] = \frac{1}{\ell}$

D $\mathbb{E} = \binom{n}{\ell} \cdot \frac{(\ell-1)!\,(n-\ell)!}{n!} = \frac{1}{\ell}$ ∎

Cor $\mathbb{E}[\#\text{ cycles in } \sigma] = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$

$= \log n + \gamma + O(\frac{1}{n})$, γ - Euler-Mascheroni const

≈ 0.57721566

SL2 $\ell \neq m$, $\ell + m \leq n$

$$\mathbb{E}[(\#\text{ of } \ell\text{-cycles})(\#\ m\text{-cycles})] = \frac{1}{\ell m}$$

/ c.f. $\mathbb{E}[XY] = \mathbb{E}[X]\,\mathbb{E}[Y]$ /

X, Y - indep

8

$$\mathbb{D}\ \mathbb{E} = \sum_{\substack{A\text{-}\ell\text{-subset} \\ B\text{-}m\text{-subset}}} P\left(\begin{array}{c}\sigma \text{ has cycle at } A \\ \text{and at } B\end{array}\right)$$

$$= \binom{n}{\ell, m, n-\ell-m} \frac{(\ell-1)!\,(m-1)!\,(n-m-\ell)!}{n!}$$

$$= \frac{n!}{\ell!\,m!\,(n-\ell-m)!} \text{ — } \text{ll} \text{ —}$$

$$= \frac{1}{\ell m}$$

$\blacksquare$

SL3 $\mathbb{E}\left[\left(\#(\ell\text{-cycles})\right)^2\right] = \begin{cases} \frac{1}{\ell}, & 2\ell > n \\ \frac{1}{\ell} + \frac{1}{\ell^2}, & 2\ell \le n \end{cases}$

D $\mathbb{E}[\#\ \ell\text{-cycles}] = \frac{1}{\ell}\sum_{i=1}^{n} P(i \in \ell\text{-cycle}) = \frac{1}{\ell}$

$\Rightarrow P(i \in \ell\text{-cycle}) = \frac{1}{n} \quad \forall i, n, \ell$

$$\mathbb{E}\left[(\#\ \ell\text{-cycles})^2\right] = \frac{1}{\ell^2}\sum_{i=1}^{n}\sum_{j=1}^{n} P(i, j \in \ell\text{-cycle})$$

$$= \frac{1}{\ell^2}\sum_{i=1}^{n} P(i \in \ell\text{-cycle}) + \frac{1}{\ell^2}\sum_{i \neq j} P(i \in \ell\text{-cycle}) \times P(j \in \ell\text{-cycle} \mid i \in \ell\text{-cycle})$$

$j = i$

$$= \underbrace{\frac{1}{\ell^2}\, n\, \frac{1}{n}}_{1/\ell^2} + \underbrace{\frac{1}{\ell^2}\, n\, \frac{1}{n}(n-1)}_{1/\ell^2\ (n-1)} \cdot (*)$$

10

$$(*) = \frac{\ell-1}{n-1} + \frac{n-\ell}{n-1}\,\frac{1}{n-\ell}$$

$$\mathbb{E}\left[(\#\text{ of } \ell\text{-cycles})^2\right] = \begin{cases} \frac{1}{\ell^2} + \frac{1}{\ell^2}(\ell-1) & 2\ell > n \\ \frac{1}{\ell^2} + \frac{1}{\ell^2}\,\ell & 2\ell \le n \end{cases}$$

$$= \begin{cases} \frac{1}{\ell} & 2\ell > n \\ \frac{1}{\ell} + \frac{1}{\ell^2} & 2\ell \le n \end{cases}$$

E-T main result:

log order of random σ is Normal w/ $\mathbb{E} = \frac{1}{2}(\log n)^2$

L4 (4/6/2020) Igor Pak

Probability of Generation

From last lecture:

Th [Dixon] $P(\langle \sigma, \omega \rangle = A_n \text{ or } S_n) \to 1$ as $n \to \infty$

Lemma $P(\sigma$ has no prime cycles of length $p \le n-3) > 1 - \frac{c}{\log\log n}$

$\boxed{L \Rightarrow Th}$ ← By Jordan's Th

Main Lemma [E-T]

$A = \{1 \le a_1 \le a_2 \le \dots \le a_r \le n\}$

$$P(\sigma \text{ has no cycles in } A) \le \frac{1}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_r}}$$

Def $X_\ell := \#\ \ell$-cycles in random $\sigma \in S_n$

SL1 $\mathbb{E}[X_\ell] = \frac{1}{\ell}$

SL2 $\ell \neq m$, $\ell + m \leq n$

$\Rightarrow \mathbb{E}[X_\ell \cdot X_m] = \frac{1}{\ell m}$

SL3 $\mathbb{E}[X_\ell^2] = \begin{cases} \frac{1}{\ell}, & 2\ell > n \\ \frac{1}{\ell} + \frac{1}{\ell^2}, & 2\ell \leq n \end{cases}$

Now: SL1 + SL2 + SL3 $\Rightarrow$ **Main L**

Proof of Main Lemma

$A = \{1 \le a_1 < \dots < a_r\}$

$X_\ell = \#\ \ell\text{-cycles}$, $Y = \#\ A\text{-cycles} = \sum_{i=1}^{r} X_{a_i}$

$$\mathbb{E}[Y] = \sum_{i=1}^{r} \mathbb{E}[X_{a_i}] = \sum_{i=1}^{r} \frac{1}{a_i}$$

$$\mathbb{E}[Y^2] = \sum_{i \neq j} \mathbb{E}[X_{a_i} X_{a_j}] + \sum_{i=1}^{r} \mathbb{E}[X_{a_i}^2]$$

$$\le 2 \sum_{i<j} \frac{1}{a_i a_j} + \sum_{i=1}^{r} \left(\frac{1}{a_i^2} + \frac{1}{a_i} \right)$$

$$\le \underbrace{\left(\sum_{i=1}^{r} \frac{1}{a_i} \right)}_{\mathrm{I}} + \underbrace{\left(\sum_{i=1}^{r} \frac{1}{a_i} \right)^2}_{\mathrm{II}}$$

$$\mathrm{Var}(Y) = \mathbb{E}[Y^2] - \mathbb{E}[Y]^2 \le (\mathrm{I} + \mathrm{II}) - \mathrm{II}$$

$$\le \left(\sum_{i=1}^{r} \frac{1}{a_i} \right)$$

③

By Chebyshev ineq. $\mu := \mathbb{E}[Y] = \sum_{i=1}^{r} \frac{1}{a_i}$

$$P(Y=0) = P(Y + \underbrace{\mathbb{E}[Y]}_{\mu} \le \underbrace{\mathbb{E}[Y]}_{\mu}) \le \frac{Var(Y)}{\mu^2}$$

$$\le \frac{\mu}{\mu^2} = \frac{1}{\mu} = \frac{1}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_r}} \qquad \boxtimes$$

<u>Counting Lemma</u> [E-R]

Fix p - prime. <u>Then</u>

$$P(p \nmid \text{order of } \sigma) = \prod_{i=1}^{\lfloor n/p \rfloor} \left(1 - \frac{1}{ip}\right)$$

<u>Remark</u>: Probabilistic proof??

We only know GF proof.

Proof of Counting Lemma

$\sigma \in S_n \longleftrightarrow$ cycles in $\sigma \longleftrightarrow$ partition $\lambda \vdash n$

$z_\lambda :=$ # elts in conj class of S_n corr. to λ

Prop: $$z_\lambda = \frac{n!}{(1^{m_1} m_1!)(2^{m_2} m_2!)\cdots}, \quad \lambda = (1^{m_1} 2^{m_2} \cdots), \quad n = \sum m_i \cdot i$$

Exc: prove Prop.

$i \to t^{m_i}/m_i! \cdot i^{m_i}$

We have: $$1 = \sum_{\lambda \vdash n} \frac{z_\lambda}{n!} = [t^n] \prod_{i=1}^{\infty} \left(1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \cdots\right)$$

$$P(p \nmid \text{order of } \sigma) = [t^n] \prod_{i=1,\, p \nmid i} \left(1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \cdots\right)$$

$$\Pi_i := \left(1 + \frac{t^i}{1! \cdot i} + \frac{t^{2i}}{2! \cdot i^2} + \cdots\right) = \exp(t^i/i)$$

$$z_{(n)} = \frac{n!}{n} = (n-1)!$$

5

$$P(p \nmid \sigma) = [t^n]\left(\prod_{p \nmid i,\ i=1}^{\infty} \Pi_i(t)\right) = Q_p(t)$$

$$Q_p(t) = \prod_{p \nmid i} e^{t^i/i} = \prod_{i=1}^{\infty} e^{t^i/i} \Big/ \prod_{k=1}^{\infty} e^{t^{pk}/pk}$$

$$= \exp\left[\sum_{i=1}^{\infty} t^i/i - \sum_{k=1}^{\infty} t^{pk}/pk\right]$$

$$-\log(1-z) = z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots$$

$$= \exp\left[-\log(1-t) + \frac{1}{p}\log(1-t^p)\right]$$

$$= \frac{(1-t^p)^{1/p}}{1-t} = \left(\frac{1-t^p}{1-t}\right)(1-t^p)^{\frac{1}{p}-1}$$

$$= (1+t+t^2+\cdots+t^{p-1}) \times$$

$$\sum_{m=0}^{\infty} t^{mp}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{mp}\right)$$

(6)

/ last eq.: $(1+z)^\alpha = 1 + \frac{\alpha}{1!} z + \frac{\alpha(\alpha-1)}{2!} z^2 + \cdots$ /

<u>We have</u>:

$$P(p \nmid \text{order of } \sigma) = [t^n]\, Q_p(t)$$

$$= [t^n]\left[(1+t+\cdots+t^{p-1})\left[1+\sum_{m=1}^{\infty} t^{mp}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\right]\right]$$

$$= \left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{mp}\right), \quad m = \left\lfloor \frac{n}{p} \right\rfloor$$

$\boxed{}$

<u>Summary</u>: $Y = \#$ A-cycles, $\mu = \mathbb{E}[Y] = \sum \frac{1}{a_i}$

<u>Main L</u>: $P(Y=0) < \frac{1}{\mu}$

<u>Counting L</u>: $P(p \nmid \sigma) = \left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{\lfloor \frac{n}{p} \rfloor p}\right)$

<u>Note</u>: p-prime never used(!)

7

Proof of <u>Dixon's th</u>

$A := \{ p\text{-prime},\ (\log n)^2 < p \le n-3 \}$

<u>ML</u> $\Rightarrow$ $P(\sigma \text{ has no } A\text{-cycles}) = P(Y=0)$

$$\le \left(\sum_{(\log n)^2 < p \le n-3} \frac{1}{p} \right)^{-1} \sim \left(\log\log(n-3) - \log\log((\log n)^2) \right)^{-1}$$

$$\lesssim \frac{c}{\log\log n}$$

$\Rightarrow$ w/ $Pr > 1 - \dfrac{c}{\log\log n}$ σ contains a p-cycle in A

<u>We want</u>: $P(\sigma \text{ cont. } p\text{-cycle in } A \mid \sigma \text{ cont. exactly } \ge 1 \ p\text{-cycle in } A)$

$P(\sigma$ cont. one p-cycle in $A \mid \sigma$ cont ~~exactly~~ ≥ 1 p-cycle in $A)$

$$= \prod_{k=1}^{\lfloor (n-p)/p \rfloor} \left(1 - \frac{1}{pk}\right) > \exp\left[\sum_{k=1}^{n/p} \log\left(1 - \frac{1}{pk}\right)\right] =$$

$$= \exp\left[-\sum_{k=1}^{n/p} \frac{1}{pk} + O(1)\right]$$

$p > (\log n)^2$

$$= \exp\left[\frac{1}{p}\left(-\log(n/p) + \cancel{\log p} + O(1)\right)\right]$$

$$\geq \exp\left[\frac{1}{p}(-\log n)\right]$$

$$> \exp\left[-1/(\log n)\right] > 1 - \frac{1}{\log n}$$

In summary: $1 - P(\langle \sigma, w \rangle = S_n \text{ or } A_n)$

$\leq P(\langle \sigma, w \rangle \text{ not primitive}) + P(\langle \sigma, w \rangle \text{ does not cont } p\text{-cycle}, p \leq n-3)$

$$\leq \frac{1}{n} + O\left(\frac{1}{n^2}\right) + \frac{c}{\log \log n} + \frac{1}{\log n} \to 0 \quad \blacksquare$$

9

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 $\lambda \vdash n$

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

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

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

$\blacksquare$

Th G - non-abelian [MacHale, 1974](?)

Then $\psi(G) \leq \frac{5}{8}$

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

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

$\Rightarrow |C_G(g)| \geq 2$ for $\geq \frac{3}{4}|G|$ 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 $\psi(G) = \frac{k(G)}{|G|} \leq \frac{5/8\,|G|}{|G|}$

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

Exc Check that MacHale Thm is sharp

3

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 $O(\text{time of } A)$

D Alg
$$\left[\begin{array}{l}\text{Pick random } x, y \in G \\ \text{check } xy = yx\end{array}\right.$$
Repeat $O(1)$ times

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

$\blacksquare$

4

Remark

Th [Gurevich-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.

5

Erdős - Rényi random subproducts

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

Def (ε-R subproducts)

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

Main idea: $h \leftarrow$ pseudo-random

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

[P, 2011]

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

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

<u>Then</u> $P(h \notin H) \geq \frac{1}{2}$

▷ $i \Leftarrow \min g_i \notin H$.

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

<u>2 Cases</u>: 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) $Z(G) \neq G$, $H \leftarrow Z(G)$

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

---

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

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

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

Remark By MacHale Thm

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

Matrix groups

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

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

Alg [testing G-abelian]

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

$hh' =? h'h$

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: $hh' =? h'h$

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

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

Alg
- $h, h' \leftarrow$ random subproducts
- $v \leftarrow \mathbb{F}_q^n$ ← random vector
- check $hh'v =? h'hv$

Repeat $O(1)$ times

Exc: 6-non-ab $\Rightarrow P(\neq) \geq \frac{1}{8}$

▨

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

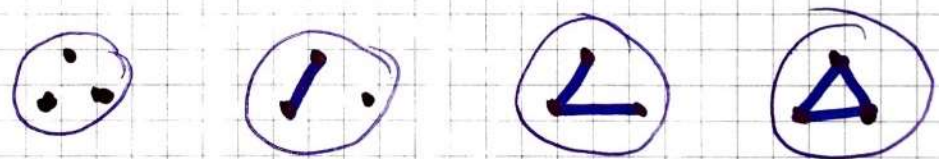
L6 (4/10/2020) Igor Pak

I. Rough Asymptotic Counting

① $\{a_n\}$, $a_n = \#$ graphs on n unlabeled vertices

OEIS A000088: 1, 2, 4, 11, 34, 156, 1044, ...

Ex $a_3 = 4$



Th (Erdös-Renyi, 1963)

$$a_n \sim \frac{1}{n!} 2^{\binom{n}{2}}$$

Exc Prove E-R thm.

ML: w.h.p. # edges to be changed to have symmetries is $> \frac{n}{2}(1-o(1))$

①

Cor 1 $a_n = 2^{\frac{n^2}{2}(1+o(1))}$

▷ trivially $\frac{1}{n!} 2^{\binom{n}{2}} \le a_n \le 2^{\binom{n}{2}}$ ▨

---

② $\{b_n\}$, $b_n = \#$ matroids on n elts

Th [Bansal-Pendavich-van der Pol, 2014]

$$\log \log b_n = n - \frac{3}{2}\log n + \frac{1}{2}\log\frac{2}{\pi} + O(1)$$

Cor 2 $b_n = 2^{2^n n^{\Theta(1)}}$ // $b_n = 2^{(2^n/n^{3/2})\cdot\Theta(1)}$ //

OEIS A055545 2, 4, 8, 17, 38, 98, 306, 1724, →
→ 383.172

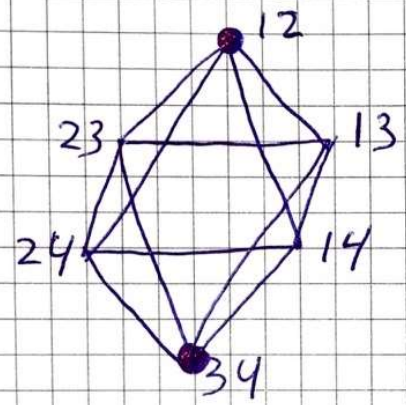
/hard to compute/

Def <u>Johnson graph</u> $J(n,k)$

<u>vertices</u>: $\binom{[n]}{k} = \{k\text{-subsets of } [n] = \{1 \dots n\}\}$

<u>edges</u>: $(A,B) \in \binom{[n]}{k}$ s.t. $|A \cap B| = k-1$.

Ex $J(4,2)$



ind $J(4,2) = 2$

Th [Piff-Welsh, 1970]

matroids on n elts of rank k

① ≥ 2 ind $J(n,k)$

② $\geq 2^{2^n} n^{-5/2} \log n$

Note $\Rightarrow$ <u>cor 2</u>

③

Key exc: Read def of a matroid.
Prove ① of P-W Thm.

Proof of ② by Knuth (1974), Graham-Sloane (1980)

L/Idea: $\exists$ indep set of size $\geq \frac{1}{n}\binom{n}{k}$

$\triangleright$ $A \in \binom{[n]}{k} \longrightarrow$ 0-1 vectors in $\mathbb{R}^n$ w/ exactly k 1's

$\varphi : \{0,1\}^n \to \mathbb{Z}_n$

$\varphi(x_1 \ldots x_n) := \sum_{i=1}^{n} i x_i \bmod n$

Observe $(A,B) \in J(n,k) \Rightarrow \varphi(A) \neq \varphi(B)$ $\boxtimes$

$\Rightarrow$ ind $J(n,k) \geq \frac{1}{n}\binom{n}{k}$

Let $k = n/2 \Rightarrow b_n \underset{PW}{\geq} 2^{\frac{1}{n}\binom{n}{n/2}} \underset{KGS}{=} 2^{2^n/n^{3/2}\,\Theta(1)}$ $\boxtimes$

④

③ $\{c_n\}$, $c_n = \#$ groups of order n

<u>OEIS</u>: <u>A000001</u> $1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, \ldots$

<u>Ex</u> $c_4 = 2$: $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$ | $c_p = 1$, p-prime

$c_6 = 2$: $\mathbb{Z}_6$, S_3

$c_{128} = 2328$, $c_{256} = 56092$,

$c_{512} = 10.4.94.213$, $c_{1024} = 49.487.365.422$

$c_{2048} = ??$ [Besche-Eick-O'Brien, 2002]

<u>Conj</u> $c_{2^k} / c_1 + c_2 + \ldots + c_{2^k} \to 1$ as $k \to \infty$

"almost all groups are 2-groups"

<u>$k=10$</u> $c_{2^{10}} / c_1 + \ldots + c_{2^{10}} > 0.99$

Th [Pyber, 1993]

$$c_1 + \dots + c_n = n^{\frac{2}{27}(1+o(1))} (\log n)^2$$

/ $\log(\#\text{ groups of order} \le n) \sim \frac{2}{27} (\log n)^3$ /

$\approx$ **Cor** $c_{2^k} \geq 2^{\Omega(k^3)}$

[Higman, 1960]

Proof of Cor (#2-groups)

$$G_k := \langle x_1 \dots x_k \rangle / \langle x_i^2 = [x_i, x_j]^2 = [x_i, [x_j, x_r]] = 1 \rangle$$

$$g \in G_k \Rightarrow g = x_1^{\varepsilon_1} \cdot \dots \cdot x_k^{\varepsilon_k} [x_1, x_2]^{\alpha_{12}} [x_1, x_3]^{\alpha_{13}} \dots$$

where $\varepsilon_i, \alpha_{ij} \in \{0, 1\}$

6

Let $W \subseteq F_2^{\binom{k}{2}} = \langle \alpha_{ij} \rangle$ ← m-dim subspace of $\mathbb{F}_2^{\binom{k}{2}}$

$H_W := G_k / W$

$$\#\{H_W / \text{isom}\} \geq \frac{\#\ m\text{-subspaces of } \mathbb{F}_2^{\binom{k}{2}}}{\#\, GL(m, \mathbb{F}_2)}$$

$$\geq \binom{\binom{k}{2}}{m}_2 \, 2^{-k^2}$$

$$\geq 2^{m\left(\binom{k}{2} - m\right) - k^2}$$

$\underline{m := k(k-1)/2 - k}$

$$\geq 2^{k\left(\frac{k(k-1)}{2} - k\right) - k^2}$$

$$\geq 2^{\Theta(k^3)}$$ groups of order 2^{2k} ▨

Back to commutivity testing

Def Black Box group $G = \langle s_1 \dots s_k \rangle$

1. can $x, y \to xy$ in time μ
2. can $x \to x^{-1}$ — " —
3. can answer $x \overset{?}{=} 1$ in time ν

From CS pov: this is an oracle model

Th [P, 2011]

Testing $G \overset{?}{=}$ abelian for black box group G requires $\Omega(k^2 \mu) + \binom{k}{2} \nu$

Proof (via adversary)

$A_0 = \mathbb{Z}_2^k \qquad B_0 = G_k = \langle x_1 \dots x_k \rangle / (x_i^2 = [x_i, x_j]^2 = \dots)$

Q1 $\text{word}_1 = ?\ 1$

$A_1 := A_0, \quad B_1 = B_0$ if yes in B_0

$B_1 = B_0 / \text{word}_1$ if NO in B_0

Q2 $\text{word}_2 = ?\ 1$

$A_2 := A_0, \quad B_2 = B_1$ is yes in B_1

$B_2 = B_1 / \text{word}_2$ if NO in B_1

$\vdots$

Need $\geq \binom{k}{2}$ Q's to distinguish A vs B

$\blacksquare$

9

L7 (4/13/2020)

Igor Pak

Erdös - Renyi Theorem

$g_1 \dots g_k \in G$ unif. random

$\Gamma_k = \Gamma(g_1 \dots g_k)$ ← random Cayley graph

Def G - finite group, $S \subseteq G$

$\Gamma = \Gamma_G(S)$ Cayley graph

Vertices $g \in G$

Edges (g, gs), $g \in G$, $s \in S$

Note: $\langle G \rangle = G$, $\Gamma_G(G) = K_{|G|}$

$\langle S \rangle = G$, $\Gamma_G(S)$ - conn.

$S = S^{-1}$, $\Gamma_G(S)$ - undirected

$G = \mathbb{Z}_n$, $S = \{\pm 1\}$, $\Gamma = C_n$

$G = D_n$, $S = \{\alpha, \beta\}$, $\alpha^2 = \beta^2 = 1$, $\Gamma = C_{2n}$

From L2: $\varphi_k(G) > 1-\varepsilon$, $k = (\log_2 |G|)\, O\left(\frac{1}{\varepsilon}\right)$

Exc1 $O\left(\frac{1}{\varepsilon}\right) \to O\left(\log \frac{1}{\varepsilon}\right)$

Exc2 Use Exc in L2 $\Rightarrow$ $k = (\log_2 |G|) + O\left(\log \frac{1}{\varepsilon}\right)$

$\Longleftrightarrow$ Random Cayley graphs Γ_k are conn. w.h.p.

Th [Erdős - Renyi, 1965] $\forall \varepsilon > 0$

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

Then Γ_k have diam $\leq k$ w/ Prob $> 1-\varepsilon$

Note: Harder ε-R Thm $2 \to 1$.

We prove original version which implies more.

Def $\bar{g} = (g_1 \dots g_k)$ fixed

$$\boxed{Q_{\bar{g}}(h) := P_{\bar{\varepsilon}}(g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = h)}, \quad h \in G, \quad \varepsilon_i \in \{0,1\} \text{ unif \& indep}$$

/distribution of random subproducts/

Th [ε-R, "real deal"]

$\forall \varepsilon, \delta > 0$, G - finite group

$$P\left(\max_{h \in G} \left| Q_{\bar{g}}(h) - \frac{1}{|G|} \right| < \frac{\varepsilon}{|G|} \right) > 1 - \delta$$

So $\forall \varepsilon < 1$ $\operatorname{diam} \Gamma(\bar{g}) \leq K$ w/ $P > 1 - \delta$

Meaning of max condition:

$$\Leftrightarrow \| Q_{\bar{g}} - U \|_\infty < \frac{\varepsilon}{|G|} \Leftrightarrow \frac{1-\varepsilon}{|G|} < Q_{\bar{g}}(h) < \frac{1+\varepsilon}{|G|} \quad \forall h \in G$$

Proof idea: First moment method (cf. Alon-Spencer)

Main Lemma $\forall\, G,\ k \geq 1$

$$\mathbb{E}_{\bar{g}}\left[\sum_{h\in G}\left(Q_{\bar{g}}(h)-\frac{1}{|G|}\right)^2\right] = \frac{1}{2^k}\left(1-\frac{1}{|G|}\right)$$

▷ $X \leftarrow$ r.v., $\mu = \mathbb{E}[X] \Rightarrow \mathbb{E}[(X-\mu)^2] = \mathbb{E}[X^2]-\mu^2$

L1 $$\mathbb{E}_{\bar{g}}\left[\sum_h\left(Q_{\bar{g}}(h)-\frac{1}{|G|}\right)^2\right] = \mathbb{E}_{\bar{g}}\left[\sum_h Q_{\bar{g}}(h)^2\right] - \frac{1}{|G|}$$

▷ $X_h \leftarrow Q_{\bar{g}}(h)$ $\forall h \leftarrow$ fixed. $\mu_h = \mathbb{E}_{\bar{g}}[X_h] = \frac{1}{|G|}$

$$\mathbb{E}_{\bar{g}}\left[\left(X_h-\frac{1}{|G|}\right)^2\right] = \mathbb{E}_{\bar{g}}[X_h^2] - \frac{1}{|G|^2}$$

$$\mathbb{E}_{\bar{g}}\left[\sum_h\left(X_h-\frac{1}{|G|}\right)^2\right] = \sum_{h\in G}\left[\mathbb{E}_{\bar{g}}[X_h^2] - \frac{1}{|G|^2}\right]$$

$$= \mathbb{E}_{\bar{g}}\left[\sum_{h\in G} X_h^2\right] - \frac{|G|}{|G|^2}$$

$$= \mathbb{E}_{\bar{g}}\left[\sum_{h\in G} Q_{\bar{g}}(h)^2\right] - \frac{1}{|G|} \quad \blacksquare$$

L2 $\mathbb{E}_{\bar g}\left[\sum_{h\in G} Q_{\bar g}(h)^2\right] = \frac{1}{2^k}\left(1-\frac{1}{|G|}\right)+\frac{1}{|G|}$

<u>Note</u> **L1 + L2 ⇒ ML**

▷ $\mathbb{E}_{\bar g}\left[\sum_{h\in G} Q_{\bar g}(h)^2\right] = \frac{1}{2^{2k}} \sum_{\bar\varepsilon,\bar\varepsilon'\in\{0,1\}^n} P(\bar g^{\bar\varepsilon} = \bar g^{\bar\varepsilon'})$

where $\bar g^{\bar\varepsilon} = g_1^{\varepsilon_1}\cdots g_k^{\varepsilon_k}$, $\bar\varepsilon = (\varepsilon_1,\dots,\varepsilon_k)$

<u>Indeed</u> $Q_{\bar g}(h) = \frac{1}{2^k}\sum_{\bar\varepsilon:\,\bar g^{\bar\varepsilon}=h} 1$

$\Rightarrow \sum_{h\in G} Q_{\bar g}(h)^2 = \frac{1}{2^{2k}} \sum_{\bar\varepsilon,\bar\varepsilon':\,\bar g^{\bar\varepsilon}=\bar g^{\bar\varepsilon'}=h} 1$ $\Big\}\ \forall \bar g$

$\mathbb{E}[\ \Sigma\ ] = \frac{1}{2^{2k}} P(\bar g^{\bar\varepsilon} = \bar g^{\bar\varepsilon'})$

$P_{\bar g}(\bar g^{\bar\varepsilon} = \bar g^{\bar\varepsilon'}) = \begin{cases} 1, & \bar\varepsilon = \bar\varepsilon' \\ \frac{1}{|G|}, & \bar\varepsilon \neq \bar\varepsilon' \end{cases}$

$(g_1\ g_3\ g_4\ g_7 \cdots)$
vs $(g_1\ g_3\ g_7 \cdots)$

$\bar g^{\bar\varepsilon} = \bar g^{\bar\varepsilon'}$
$= g_1 \cdots$

(Proof of L2 cont'd)

L1 $$\mathbb{E}_{\bar{g}}\left[\sum_{h\in G}\left(Q_{\bar{g}}(h)-\frac{1}{|G|}\right)^2\right] = \mathbb{E}_{\bar{g}}\left[\sum_{h\in G} Q_g(h)^2\right] - \frac{1}{|G|}$$

$$\rightarrow \mathbb{E}_g\left[\sum_h Q_g(h)^2\right] = \frac{1}{2^{2k}} \sum_{\bar{\varepsilon},\bar{\varepsilon}'} P_{\bar{g}}\left(\bar{g}^{\bar{\varepsilon}} = \bar{g}^{\bar{\varepsilon}'}\right)$$

$$= \frac{1}{2^{2k}}\left(\sum_{\bar{\varepsilon}=\bar{\varepsilon}'} 1 + \sum_{\bar{\varepsilon}\neq\bar{\varepsilon}'} \frac{1}{|G|}\right)$$

$$= \frac{1}{2^{2k}}\left(2^k + \left(2^{2k}-2^k\right)\frac{1}{|G|}\right)$$

$$= \frac{1}{2^{2k}}\, 2^k + \frac{2^{2k}}{2^{2k}|G|} - \frac{2^k}{2^{2k}|G|}$$

$$= \frac{1}{2^k}\left(1-\frac{1}{|G|}\right) + \frac{1}{|G|}$$

$\blacksquare$

$\Rightarrow$ ML

Proof of ε-R Thm

$$\max_{h\in G}\left(Q_{\bar g}(h)-\frac{1}{|G|}\right)^2 \le \sum_{h\in G}\left(Q_{\bar g}(h)-\frac{1}{|G|}\right)^2 \quad \checkmark$$

$$\Rightarrow P_{\bar g}\left[\max\left|Q_{\bar g}(h)-\frac{1}{|G|}\right| > \frac{\varepsilon}{|G|}\right]$$

$$\le P_{\bar g}\left(\sum_{h\in G}\left(Q_{\bar g}(h)-\frac{1}{|G|}\right)^2 > \frac{\varepsilon^2}{|G|}\right) \le (*)$$

$$Z := \sum_{h\in G}\left(Q_{\bar g}(h)-\frac{1}{|G|}\right)^2, \quad \mathbb{E}[Z] \underset{\text{ML}}{=} \frac{1}{2^k}\left(1-\frac{1}{|G|}\right)$$

$$P(Z > \lambda\,\mathbb{E}[Z]) < \frac{1}{\lambda}, \quad \text{Markov ineq}, \quad \lambda := \frac{\varepsilon^2}{|G|^2\,\mathbb{E}[Z]}$$

$$(*) \le \frac{|G|^2\,\frac{1}{2^k}\left(1-\frac{1}{|G|}\right)}{\varepsilon^2} \le \frac{|G|^2}{2^k\,\varepsilon^2} < \delta$$

for $k > 2\log_2|G| - 2\log_2\varepsilon - \log_2\delta + 1$

$\boxtimes$

Future directions

① mix time on $\Gamma_k = O(\log|G|)$, $k = O(\log|G|)$
/stronger than diam/

② Γ_k are expanders, $k = \Omega(\log|G|)$

③ iterated random subproducts $\Longrightarrow$ $\mathcal{U}$
(Babai + Dixon)

L8 (4/15/2020) Igor Pak

Random generation in permutation groups

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

More precisely: $S = \{s_1, \dots s_k\} \subset S_N$, $GL(n, \mathbb{F}_q)$, 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 $G \subseteq S_N$

Lost L: ε-R Thm

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

$h = g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k}$, $\varepsilon_i \in \{0,1\}$ 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 $\mathcal{L} \leftarrow$ cost of gen'n 1 random elt

Then generating m random elts in

$$O(\mathcal{L}\log_2|G| + mk\mu)$$

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 poly(N, k)

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

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

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

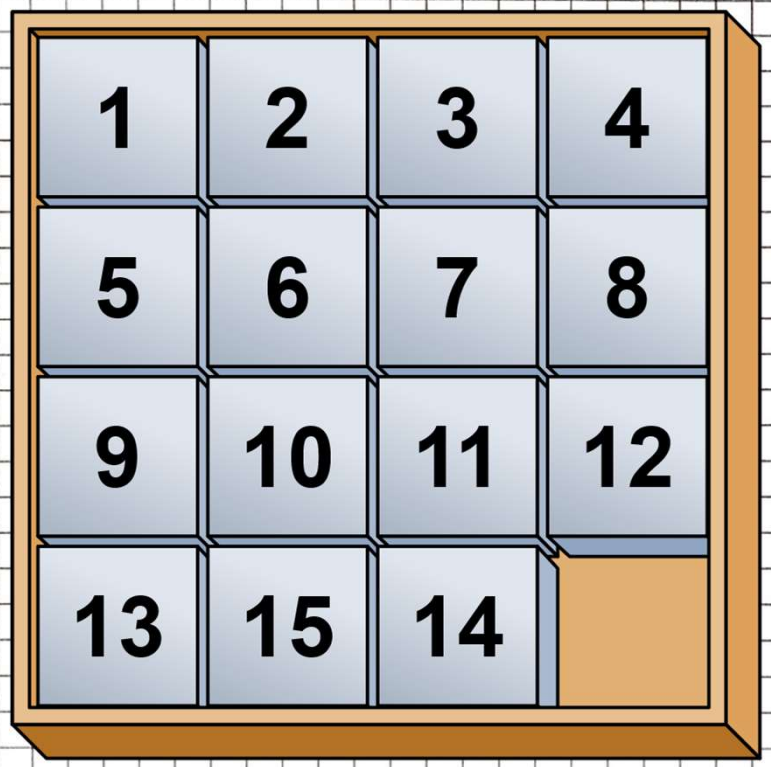
$\uparrow$

Coming UP

Examples of Permutation 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

④

Schreier's Lemma

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

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

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

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

$\le N$ steps

/easy to compute/

---

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

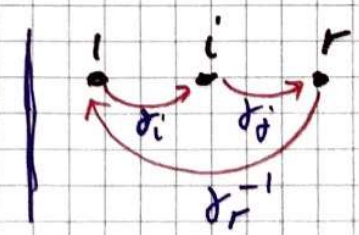
<u>Schreier's L</u> (1928) $\Gamma \subset G$, $\Gamma = \{ \gamma_i,\ i \in O_G(1) \}$ ①

$\gamma_i(1) = i$

<u>Then</u>

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

$\sigma(1) = 1 \iff \gamma_j(i) = r$



<u>Think</u> <u>of</u> <u>RC</u> : [Do smth] → [minor change] → [UNDO]

⑤

Sims Alg $\quad [G = \langle s_1 \dots s_k \rangle \subset S_N]$

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.

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

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

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

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

③ $\left[\begin{array}{l} \text{given } \sigma \in S_N, \text{ check } i = \sigma(1) \in ?\ O_G(1). \text{ No} \Rightarrow \text{"NO"} \\ \text{yes} \Rightarrow \sigma \leftarrow \gamma_i^{-1}\sigma, \text{ repeat w/ } St_G(1) \end{array}\right.$

Exc Fill in details for ①, ②, ③.

Major issue w/ Sims Alg

Number of gen's (!)

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

$K \to K^3 \to K^9 \to \dots$

What to do?

Sims, Knuth ← clever bookeping

Reducing number of gen's

[Cooperman-Finkelstein]

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

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

random subproducts.

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

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

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

+ Exc ▨

Back to Sims Alg

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

(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 $O(N^2 \mu)$

Repeat N times

$k \leftarrow O(N^2)$

Total cost

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

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

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

$\times\ O(\log N)$ ▨

One more issue (!?!)

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

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

8

How good is this S-C-F Alg?

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

Outputs: $\leftarrow$ $\Gamma_1, \Gamma_2, \ldots, \Gamma_N$

w/ Pr: $> 1-\varepsilon$

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

w/ $Pr > 1-\varepsilon$

reliable?

Imp. Remark: we can check if Answer correct

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

$\textcircled{=} \iff$ we obtained all of $St_G(1 \ldots \ell)$

NOT a subgroup.

Alg $G = \langle S_1, \ldots S_k \rangle$

check group membership $\textcircled{3}$ $\forall S_i$

yes $\Rightarrow$ $\textcircled{=}$ ✓

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}?

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 $G \subset S_N$

(3) testing abelian w/out REO (using random subproducts)

Today: (4) testing nilpotent, solvable using random subproducts

(5) testing $G \simeq S_n, A_n$ under REO

Random subproducts

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

$h \leftarrow s_1^{\varepsilon_1} \cdot \ldots \cdot s_k^{\varepsilon_k}$, $\varepsilon_i \in \{0,1\}$ unif. indep.

<u>Th 1</u> $H \subsetneq G$ proper subgroup

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

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

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

This is <u>all</u> we need to test

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

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

Nilpotent & solvable groups

Def $G \leftarrow$ 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

$G \rhd G_1 \rhd G_2 \rhd \dots \rhd G_\ell = 1$,

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

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

Def G - solvable if

$G \rhd G_1 \rhd G_2 \rhd \dots \rhd G_\ell = 1$

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

Obs

$Ab \subsetneq Nilp \subsetneq Solv$

Examples: $[S_n, S_n] = A_n$, $[A_n, A_n] = A_n \leftarrow$ non-solv, $n \geq 5$

$\left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix},\ * \in \mathbb{F}_q \right\} \leftarrow$ nilp $\quad \left\{ \begin{pmatrix} \circledast & * \\ 0 & \circledast \end{pmatrix},\ \begin{matrix} * \in \mathbb{F}_q \\ \circledast \neq 0 \end{matrix} \right\} \leftarrow$ solv

Proof $\rightarrow$ $\boxed{\text{EXC}}$

3

Commutator subgroup gen'n

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

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

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

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

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

/smalest normal subgroup which cont<?/

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

$\boxed{h^g := g^{-1} h g}$

Exc Find an example.

$\underline{L}$ $\left\{ \begin{array}{l} G = \langle S \rangle, \ S = \{s_1 \dots s_k\} \\ H = \langle T \rangle, \ T = \{t_1 \dots t_\ell\} \end{array} \right\}$ <u>Suppose</u> $H \neq H^G$, $H \leq G$.

<u>Then</u> $P(h^g \notin H) \geq \frac{1}{4}$, where $\underline{h = t_1^{\varepsilon_1} \dots t_\ell^{\varepsilon_\ell}}$

$\underline{g = s_1^{\alpha_1} \dots s_k^{\alpha_k}}$

$\varepsilon_i, \alpha_i \in \{0,1\}$ unif indep

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

normalizer of H in G

---

(1) $H \neq H^G \Rightarrow H \ntrianglelefteq G \Rightarrow N_G(H) \neq G$

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

---

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

<u>Note</u> $hg = (t_1^{\varepsilon_1} \dots t_\ell^{\varepsilon_\ell})^g = g^{-1} t_1 \dots t_\ell g = (t_1^{\varepsilon_1})^g \dots (t_\ell^{\varepsilon_\ell})^g$

$= (t_1^g)^{\varepsilon_1} \dots (t_\ell^g)^{\varepsilon_\ell}$ ← random subproduct on H^g

$H^g = \langle t_1^g \dots t_\ell^g \rangle$

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

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

Commutator Subgroup Alg

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

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

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

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

Repeat $i = 1 \dots L$

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

$R_{i+1} \leftarrow \{ R_i \cup h^g \}$, where $\begin{cases} g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} \\ h = r_1^{\alpha_1} \cdots r_N^{\alpha_N} \end{cases}$ | $R_i = \{ r_1, \dots r_N \}$

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

Th Output $= G'$ w.h.p

$p > 1 - \varepsilon$

Cost

$O(k^2 L \mu)$

$O((k^2 + L)^2 L \mu)$

Testing for Nilp, Solv

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

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

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

$\vdots$

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

Test $x =? 1 \quad \forall x \in R_L$

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

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

$\times \log \log |G|$

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

Alg for solv ← same

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

What did we get?

One-sided Monte-Carlo Alg

If No ⇒ True. claim / NOT Nilp / Solv.

If yes ⇒ Maybe claim / Nilp / Solv w.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 $G \simeq S_n$

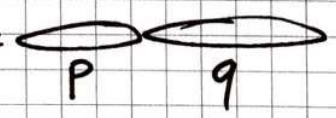
No $G \not\simeq S_n$

---

say n – even

(0) Find $p+q=n$, p,q - prime, $p'+q'=n-2$, p',q' – prime >2

(1) $g, h \leftarrow$ random in G.] Repeat until found

$g^{pq} \overset{?}{=} 1 \Rightarrow g =$ 

(2) $h^{2p'q'} \overset{?}{=} 1 \Rightarrow h =$

] Repeat until found

(3) $a \leftarrow h^{p'q'} = (\overline{2})$, $b \leftarrow$ random in G

$a^b \leftarrow$ random transp.

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

9

Analysis

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

random transp $\Omega(\frac{1}{n})$

Validity check

$S_n = \langle X = (12), Y = (12 \ldots n) \rangle$

check relations: $s_i^2 = (s_i s_{i+1})^3 = (s_i s_j)^2 = 1$ $|i-j| > 2$

$s_i := (Y^{-i} X Y^{i})$

Bonus story: Goldbach Conjecture

$n < 10^{14}$

Bratus-P.

Odd GC

$n > 10^{40,000}$

Helfgott ✓

Igor Pak

Cayley graphs

$G = \langle S \rangle$, $S = \{s_1, \dots s_k\}$, $S = S^{-1}$ /$\Leftrightarrow$ $\forall s \in S$, $s^{-1} \in S$/

$\Gamma = \Gamma(G, S)$ ← Cayley graph

vertices $g \in G$

edges (g, gs), $g \in G$, $s \in S$

Questions about Cayley graphs

(1) $\mathrm{diam}(\Gamma) = ??$

(2) $\mathrm{mix}(\Gamma) = ??$

(3) $\mathrm{eig}(\Gamma) = ??$

¿expander?

(4) Γ - planar?

(5) Γ - edge-transitive?

(6) Γ - Hamiltonian?

...

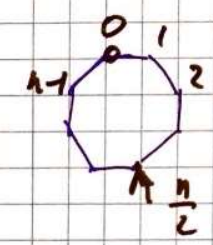
Today: some overview before (1) → (2) → (3) direction

Note $\mathrm{diam}(\Gamma) = \max_{x, y \in G} |x, y|_\Gamma$

Diameter of Cayley graphs

(0) $S = G \Rightarrow \Gamma(G,G) = K_{|G|}$, so $\operatorname{diam} \Gamma = 0$

(1) $G = \mathbb{Z}_n$, $S = \{\pm 1\}$, $\operatorname{diam} \Gamma(G,S) = \lfloor \frac{n}{2} \rfloor$



(2) general graphs $G = (V, E)$, $|V| = n$

$$\operatorname{diam} = O\left(\frac{\log n}{\log\log n} \cdot r(G)\right), \quad r(G) = \sum_{v \in V} \frac{1}{\deg(v)}$$

[Erdős Pach Spencer 1988]

for us $\deg(v) = |S|$, so $r() = |G|/|S| \to$ angul.

(3) $G = S_n$, $G = \langle R \rangle$

<u>Prop</u> 1 $R_n = \{(12), (12\ldots n)^{\pm 1}\} \Rightarrow \operatorname{diam} \Gamma(S_n, R_n) = \Theta(n^2)$

D we'll give one later using LA

<u>Prop 2</u> $R_n = \{(12), (23), \ldots (n-1, n)\} \Rightarrow \operatorname{diam} \Gamma(S_n, R_n) = \binom{n}{2}$

D $\operatorname{dist}(1, \sigma) \le \operatorname{dist}((123\ldots n), (n\, n{-}1 \ldots 1)) = \binom{n}{2}$
$= \operatorname{inv}(\sigma)$

Conj $\forall R_n$, $\langle R_n \rangle = S_n$, $\operatorname{diam}(S_n, R_n) = O(n^2)$
/say $\leq 3n^2$/

Th [Babai, Seress, 1988]
$$\operatorname{diam}(S_n, R_n) = e^{O(\sqrt{n \log n})}$$

Th [Helfgott-Seress, 2014] ← Annals Math
$$\operatorname{diam}(S_n, R_n) = e^{O((\log n)^4 \log\log n)}$$

---

(4) Lower Bounds

Prop $\operatorname{diam}\Gamma(G,S) \geq \log_{|S|} |G| - 1$

D # $g \in G$ at dist $0 \leftarrow 1$
— " — $1 \leftarrow |S|$
— " — $2 \leq |S|^2$
- - - -
$\operatorname{diam} \leq |S|^{\operatorname{diam}}$

$1 + |S| + |S|^2 + \dots + |S|^{\operatorname{diam}} \geq |G|$

$\boxtimes$

Q: what about S_n?

Th $\exists\, R_n$, $|R_n| = O(1)$, $\langle R_n \rangle = S_n$

s.t. $\operatorname{diam} \Gamma(S_n, R_n) = O(\log n!) = O(n \log n)$

▷ **Let** $n = p+1$, p - prime

$S_n \leftrightarrow$ perm's of $\{0, 1, 2, \dots, p-1, \infty\} \leftarrow \mathbb{P}\mathbb{F}_p$

α :	$a \to a+1 \ (p)$	$(1, 2, 3, \dots, 0, \infty)$	$R_n = \{\alpha^{\pm 1}, \beta^{\pm 1}, \gamma\}$
β :	$a \to 2a \ (p)$	$(0, 2, 4, \dots, p-2, \infty)$	
γ :	$a \to \frac{1}{a} \ (p)$	$(\infty, 1, \dots, 0)$	

L1 $\operatorname{dist}_\Gamma(i\,j) = O(\log n)$, $\Gamma = \Gamma(S_n, R_n)$

▷ $i \xrightarrow[\alpha^{-1},\, \beta^{-1}]{} \dots \xrightarrow{} 1 \xrightarrow[\alpha^{-1}]{} 0 \xrightarrow[\gamma]{} \infty$ $\quad O(\log n)$ steps

$j \to \dots \to 0$ $\quad$ — " —

$\gamma : \langle i \leftrightarrow j \rangle$

Repeat in rererse ▨

L2 $R_n = \{(i\,j),\ 1 \le i < j \le n\}$

$\operatorname{diam}(S_n, R_n) = O(n)$ ▨ Exc

▨ (4)

(5) Linear groups

Conj [Babai] $G = PSL(n, q)$, n fixed, $q \to \infty$

$\operatorname{diam} \Gamma(G, R) = O_c(\log |G|)^c$, $c = c(n)$

Note: mostly proved by now (Bourgain, Gamburd, Breuillard, Green, Tao, etc)

---

(6) $U(n, q)$ $q \leftarrow$ fixed (say $q = 2$)

$$G_n = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}, \quad * \in \mathbb{F}_q \right\} \qquad R_n = \left\{ \begin{array}{c} \begin{pmatrix} 1 & & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \begin{array}{c} \\ \\ \\ \end{array} \\ \begin{array}{ccc} & j & \end{array} \end{array} \begin{array}{c} \\ \\ i \end{array} = E_{ij}, \quad 1 \le i < j \le n \right\}$$

Prop $\operatorname{diam} \Gamma(G_n, R_n) = O(n^2)$

$\triangleright$ each row $= O(n)$ ▨

Lower Bound: $\operatorname{diam} \Gamma \geq \log_{\binom{n}{2}} 2^{\binom{n}{2}} = \dfrac{\log 2^{\binom{n}{2}}}{2 \log n} = c \dfrac{n^2}{\log n}$

Q/Conj $\operatorname{diam} = \Theta(n^2)$

5

Th [Ellenberg, 1993]

$G_n = U(n,2)$, $R_n = \{ E_{i\,i+1},\ 1 \le i \le n-1 \}$

Then $\operatorname{diam} \Gamma(G_n, R_n) = \Theta(n^2)$

D **UB**

$$A = \begin{pmatrix} 1 & * & * & * & * & * \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & 0 & & & 1 & \\ & & & & & 1 \end{pmatrix}$$

Case 1 $(1\,1\,*\,*\,\cdots\,*)$
$(1\,*\,*\,\cdots\,*)$ ↑ +

Case 2 $(1\,0\,*\,*\ \ *)$
$(1\,0\,0\ \ 0)$ ↑] **now**

$a(n) = \operatorname{dist}(1, A) \le (n-1) + a(n-1) + a(n-1)$ ← terrible(!)
$\le e^{O(n)}$

$a(n) \le a(n-1) + \underbrace{O(1)}_{2}$ ✓

$\le 2n$

cleanup idea

$\Rightarrow$ $\operatorname{diam} \le a(1) + \cdots + a(n) = O(n^2)$ ▲

LB **Need** to improve trivial $\Omega(n^2/\log n)$ to $\Omega(n^2)$

Heaps of pieces

Alphabet: $A = \{a_1, \dots, a_k\}$, $k = n-1$

words: $A^* = \{a_{i_1} a_{i_2} \dots a_{i_\ell}\}$

Commutativity relations $a_i a_j = a_j a_i \quad \forall\ |i-j| \geq 2$

Main Lemma: $\left(\#\text{ words of length} \leq \ell\right) \leq c^\ell$ some $c > 1$
/ modulo c.r. / $\approx w(\ell)$

Ex $k=3$

ℓ	1	2	3	4	...	ℓ
$w(\ell)$	3	8	21	55	...	?

OEIS A001906

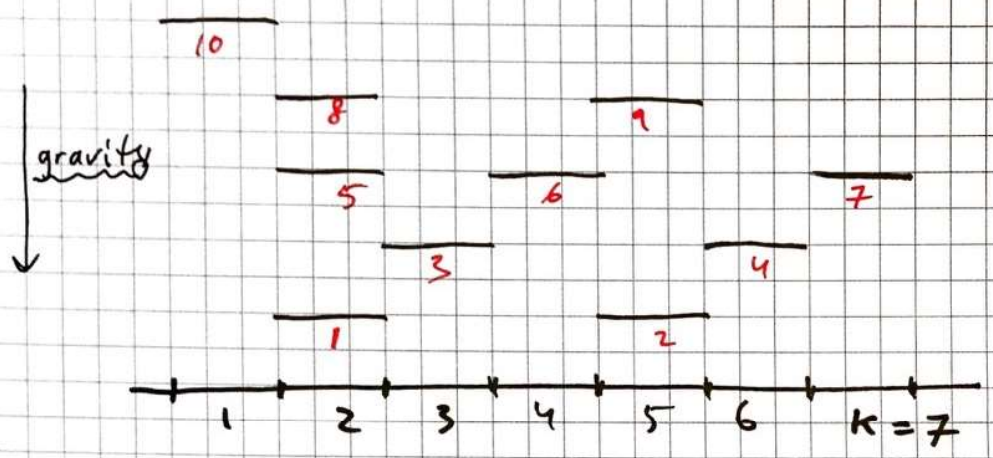
$a_1 a_3 = a_3 a_1$

$a_1 a_1 a_3 = a_1 a_3 a_1 = a_3 a_1 a_1$

$w(\ell) = 3\, w(\ell-1) - w(\ell-2)$

7

Heaps visualized



$\Longleftrightarrow$ $a_2\, a_5\, a_3\, a_6\, a_2\, a_4\, a_7\, a_2\, a_5\, a_1$

word in $A = \{a_1 \dots a_7\}$

Def word is simple if all letters commute.

Ex $a_2\, a_5\, a_7$

L/Th (Viennot, 1986)

$\Leftrightarrow$ (Cartier-Foata, 1969)

$$\sum_{w \in \text{words in } A/CR} w = \left(\sum_{\substack{w \in \text{simple words} \\ \text{in } A}} (-1)^{|w|}\, w \right)^{-1}$$

Ex $k = 3$

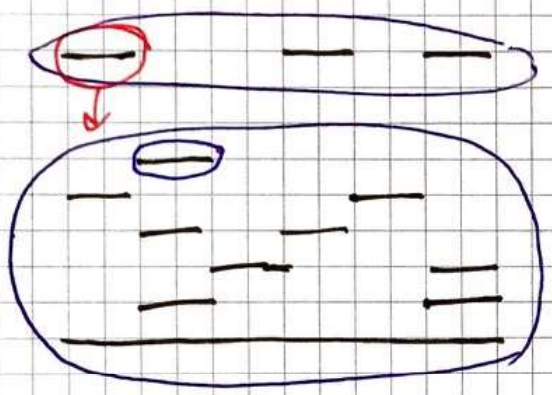
$$\sum \omega(\ell)\, t^{\ell} = \frac{1}{1 - 3t + t^2}$$

simple words:

$\emptyset,\ a_1, a_2, a_3,\ a_1 a_3$

D (visual proof)

$(\sum \text{words})(\sum \pm \text{simple words}) = 1$



simple word

word

Idea

1) find smallest movable piece

2) move ↓ if possible, ↑ otherwise.

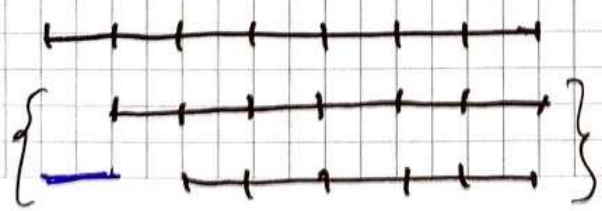
only $\emptyset$ word remains ▨

Def $P_k(t) := \sum_{w \in \text{simple word}} (-t)^{|w|}$

Prop (1) $P_k(t) = P_{k-1}(t) - t\,P_{k-2}(t)$

(2) $P_k(t) = \sum_{m=0}^{\lfloor k/2 \rfloor} (-1)^m \binom{k-m+1}{m} t^m$

D



P_{k-1}

P_{k-2}

▨

9

$$\begin{cases} P_0(t) = 1, \quad P_1(t) = 1-t \\ P_k = P_{k-1} - t\,P_{k-2} \end{cases}$$

$$\Rightarrow P_k(t) \equiv \frac{1}{2}\left(1 + \frac{1-2t}{\sqrt{1-4t}}\right)\left(\frac{1+\sqrt{1-4t}}{2}\right)^k$$

$$+ \frac{1}{2}\left(1 - \frac{1-2t}{\sqrt{1-4t}}\right)\left(\frac{1-\sqrt{1-4t}}{2}\right)^k \qquad z \leftarrow \sqrt{1-4t}$$

$$\equiv \frac{1}{2^{k+2}\,z}\left[(1+z)^{k+2} - (1-z)^{k+2}\right]$$

$$i\tan\left(\frac{\pi r}{n+2}\right) \quad \text{roots}, \ 1 \le r \le n+1$$

calculation /Exc/

$\Rightarrow$ roots of $P_k(t)$ are $\geq \frac{1}{4}$

$$\Rightarrow \sum_{w \text{ words}} t^{|w|} = \sum \omega_k(\ell)\, t^\ell = \frac{1}{P_k(t)} \quad \text{has poles at } \geq \frac{1}{4}$$

$$\Rightarrow \omega_k(\ell) \le 4^\ell (k+2)$$

$\blacksquare$

Back to $U(n,2)$

$U(n,2) = \langle E_i, 1 \le i \le n-1 \rangle$

$k = n-1$

Improved LB:

$\#$ words in E_i of length $\ell \le w_k(\ell) \le 4^\ell (k+2)$
$\le 4^\ell (n+1)$

$$\Rightarrow \operatorname{diam} \Gamma(U(n,2), \{E_i\}) \ge c \log \left[2^{\binom{n}{2}} / n+1 \right]$$
$$= \Omega(n^2)$$

$\blacksquare$

Ex $G = S_n$, $R = \{(12), \dots (n-1, n)\}$

$$LB = \frac{\log n!}{\log n} = \Theta(n)$$

Improved LB $\quad \log n! = \Theta(n \log n)$

True $\quad \Theta(n^2)$

4/22/2020

Igor Pak

Random walks

$G = \langle S \rangle$ - fin. group, $S = \{s_1, \dots s_k\}$, $S = S^{-1}$

$$\begin{cases} X_0 \leftarrow 1 \\ X_{t+1} \leftarrow X_t \cdot s_i, \quad s_i \in S, \text{ unif at random} \end{cases}$$

$\{X_t\} \leftarrow$ random walk on $\Gamma(G, S)$

$Q^t(g) = P(X_t = g) \leftarrow$ distr. of $\{X_t\}$ after t steps

Prop $\forall\, S = S^{-1}$, $1 \in S$

$Q^t(g) \to \frac{1}{|G|} \quad \forall g \in G$ $\leftarrow$ Exc

Note: this means $\{X_t\}$ is ergodic

Mixing time

Def 1 $\quad mix_1 := \min\{t : |Q^t - U|_{TV} \le \frac{1}{4}\}, \quad U(g) = \frac{1}{|G|}$

$$|P - Q|_{TV} := \frac{1}{2}|P - Q|_{\ell_1} := \frac{1}{2}\sum_{g \in G} |P(g) - Q(g)|$$

$$:= \max_{A \subseteq G} |P(A) - Q(A)| \qquad \| \leftarrow \text{Exc}$$

Note: if $\frac{1}{4} \leftrightarrow (\varepsilon < \frac{1}{4}) \Rightarrow mix_1' < C(\varepsilon)\, mix_1 \quad \| \text{Exc}$

Def 2 $\quad mix_2 := \min\{t : sep(Q^t, U) \le \frac{1}{2}\}$

$$sep(Q^t, U) := |G| \max_{g \in G} \left(\frac{1}{|G|} - Q^t(g)\right)$$

$$sep(Q^t, U) < \varepsilon \iff Q^t(g) > \frac{1-\varepsilon}{|G|} \quad \forall g \in G$$

Note: Our main <u>def</u> for today.

(2)

Prop (1) $\mathrm{sep}(t+1) \le \mathrm{sep}(t)$

(2) $\mathrm{sep}(t+s) \le \mathrm{sep}(t)\,\mathrm{sep}(s)$

(3) $\mathrm{sep}(t) \sim C\rho^t$ as $t \to \infty$, $0 \le \rho \le 1$

D of (1): $\mathrm{sep}(t) = \varepsilon \Rightarrow Q^t = (1-\varepsilon)U + \varepsilon N$ ← "noise"

$Q^{t+1} = Q^t * \underset{\sim P}{Q^1}$ where $Q^1(g) \doteq \begin{cases} 1/|S|, & g \in S \\ 0, & \text{oth.} \end{cases}$

$$\Rightarrow Q^{t+1} = ((1-\varepsilon)U + \varepsilon N) * P$$
$$= (1-\varepsilon)U * P + \varepsilon N * P$$
$$= (1-\varepsilon)U + \varepsilon(N * P) \quad \blacksquare$$

of (2) $Q^t = (1-\varepsilon)U + \varepsilon N_1$, $Q^s = (1-\delta)U + \delta N_2$

$$Q^{t+s} = Q^t * Q^s = ((1-\varepsilon)U + \varepsilon N_1) * ((1-\delta)U + \delta N_2)$$
$$= (1-\varepsilon\delta)U + \varepsilon\delta(N_1 * N_2)$$
$$\Rightarrow \mathrm{sep}(t+s) \le \varepsilon\delta = \mathrm{sep}(t)\,\mathrm{sep}(s) \quad \blacksquare$$

③

(3) $A = (a_{gh})_{|G|\times|G|}$, $a_{gh} = \begin{cases} 1/|S| , & hg^{-1} \in S \\ 0 , & \text{o.t.h} \end{cases}$

<u>Obs</u> $Q^t(g) = A^t \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_g = \frac{1}{|G|}\underbrace{\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}}_{= v_0} + \lambda_1^t v_1 + \dots + \lambda_{|G|-1}^t v_n$

$\{ (v_i, \lambda_i) \}$ ← eig. vectors, eig. values of A

as $t \to \infty$ $Q^t(g) \simeq \frac{1}{|G|} + (\rho^t \cdot c) + o(\rho^t c)$

$\Rightarrow$ $\text{sep}(t) \sim \rho^t c'$ ▨

<u>Exc</u> $\exists\, c_1, c_2 > 0$ s.t. $c_1(\text{mix}_1) < (\text{mix}_2) < c_2(\text{mix}_1)$

<u>Q</u>: how do you bound mix ← mix_2 ??

<u>Prop</u> $\text{mix} < c\left(\frac{1}{1-\lambda_1}\right) \log|G|$ ▨ | ← <u>Exc</u>

(4)

Ex $G = \mathbb{Z}_m$, $S = \{\pm 1\}$

$$A = \begin{pmatrix} 0 & 1/2 & & & & 1/2 \\ 1/2 & 0 & 1/2 & & & \\ & 1/2 & 0 & 1/2 & & \\ & & 1/2 & 0 & \ddots & \\ & & & \ddots & \ddots & 1/2 \\ 1/2 & & & & 1/2 & 0 \end{pmatrix}$$

Exc $\lambda_j = \cos(2\pi j/m)$

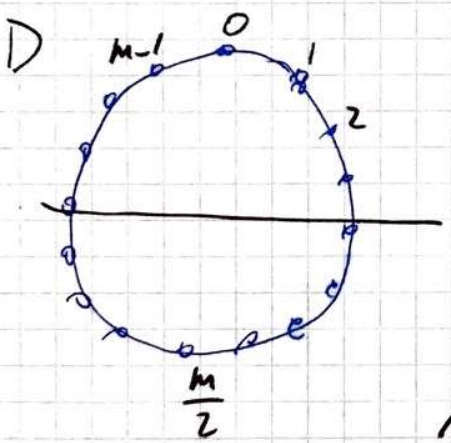
$$\Rightarrow \lambda_0 = 1, \quad \lambda_1 = 1 - \frac{(2\pi)^2}{m^2} + \cdots$$

$$= 1 - \frac{c}{m^2} + O\left(\frac{1}{m^4}\right)$$

$\Rightarrow$ mix $= O(m^2 \log m)$ | **Th** mix $= \Theta(m^2)$

Prop mix $= \Omega(m^2)$

D



after t step $X_t \in [-c\sqrt{t}, +c\sqrt{t}]$ w.h.p.

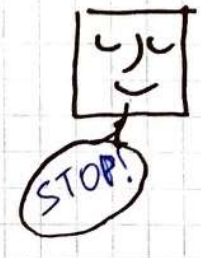
$\Rightarrow$ to reach $\frac{m}{2}$ w/ $Q^t(\frac{m}{2}) > \frac{1}{2m}$

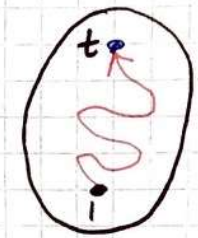
need $\Omega(m^2)$ steps $\boxed{}$

Note for TV dist $Q^t(\text{bottom half}) > \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$ $\boxed{}$

5

Strong uniform time





Def $\tau \leftarrow$ (prob.) stopping time is called strong uniform if

$$P(X_t = g \mid \tau = t) = \frac{1}{|G|} \quad \forall g \in G \quad \forall t \geq 0$$

Th [Aldous-Diaconis, 1987]

(1) $G = \langle S \rangle$, $S = S^{-1}$, $1 \in S$, $\tau \leftarrow$ strong unif.

Then $\mathrm{sep}(t) \leq P(\tau > t) \quad \forall t$

(2) $\exists\, \tau$ s.t. $\circledcirc$ $\forall t$.

Cor $\mathrm{mix} < 2 \cdot \mathbb{E}[\tau]$

D By Markov ineq $P(\tau \geq 2\mathbb{E}[\tau]) \leq \frac{1}{2}$

$$\mathrm{sep}(2\mathbb{E}[\tau]) \leq P(\tau > 2\mathbb{E}[\tau]) \leq \frac{1}{2} \qquad \blacksquare$$

(6)

Proof of (1)

$$Q^t = \sum_{k \le t} U \cdot P(\tau = k) + N\, P(\tau > t)$$

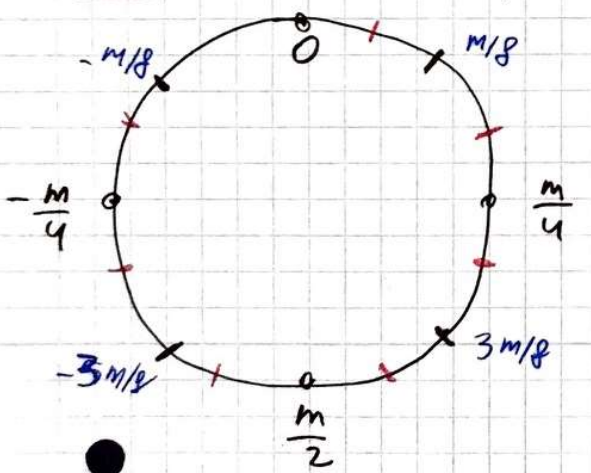
$$= U \cdot P(\tau \le t) + N\, P(\tau > t)$$

$$\Rightarrow \quad sep(Q^t, U) \le P(\tau > t) \qquad \blacksquare$$

Proof of (2) | ← Exc

clue: $\boxed{\tau}$ can flip coins (!)

Ex $G = \mathbb{Z}_m$, $S = \{0, 1, -1\}$, $m = 2^r$



Alg $\boxed{\tau}$

- walk until $\pm m/4$
- — // — $\pm m/4 \pm m/8$
- — // — $\pm m/4 \pm m/8 \pm m/16$
- . . .
- wal until odd.
- one more step

7

$\underline{L}$ τ is strong uniform.

D (1) either of $\pm\frac{m}{4}$ is unif cond. t

(2) — // — $\pm\frac{m}{4} \pm \frac{m}{8}$ — // —

⋮

(r-1) — // — odd — // — // —

(r) all unif. cond. t ▨

$$\Rightarrow \quad \text{Mix} \le 2\,\mathbb{E}[\tau] = c\left(\frac{m}{4}\right)^2 + c\left(\frac{m}{8}\right)^2 + c\left(\frac{m}{16}\right)^2 + \cdots$$

$$\le c\left(\frac{m}{4}\right)^2\left(1 + \frac{1}{4} + \frac{1}{16} + \cdots\right)$$

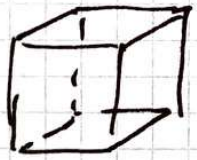
$$\le \underline{\underline{c' m^2}}$$ ▨

8

Random walk on $\mathbb{Z}_2^m$ ← hypercube

$G = \mathbb{Z}_2^m$, $|G| = 2^m$

$S = \{(0 \cdots 1_i \cdots 0),\ 1 \le i \le m\}$



lazy random walk $X_0 = 1$, $X_{t+1} = X_t \cdot s_i^{\varepsilon}$, $\varepsilon \in \{0,1\}$

$\{X_t\}$ ← choose a coord. i, flip a coin
if H, change coord. i

Th $\quad mix = m \log m + O(m)$

▷ Stopping time: mark coord. i when chosen
stop when all coord's are marked.

$(0 \cdots * \quad 0)$
$(0 \cdots * \cdots * 0)$
$(0 \quad * \quad * \quad * 0)$
$\vdots$
$(* * * \cdots * *)$

$\le \tau$ is strong uniform $\square$

$\Rightarrow mix \le 2\, \mathbb{E}[\tau] = 2 m \log m + O(m)$

coupon collector's problem

9

L12 (4/24/2020) Igor Pak

Strong Uniform Times

Last time: $\{X_t\} \leftarrow$ r.w. on $\Gamma(G,S)$

$\tau \leftarrow$ stopping time $\boxed{\tau}$

τ is strong uniform if

$$P(X_t = g \mid \tau = t) = \frac{1}{|G|} \quad \forall t \geq 0, \ \forall g \in G$$

Th [A-D]

$\tau \leftarrow$ strong uniform

$\Rightarrow$ $\operatorname{sep}(t) \leq P(\tau > t) \ \forall t$

where $\operatorname{sep}(t) = |G| \max_{g \in G} \left(\frac{1}{|G|} - Q^t(g) \right)$

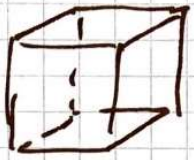
Prop $\operatorname{mix} \leq C \cdot \mathbb{E}[\tau]$, where $\operatorname{mix} := \min\{t : \operatorname{sep}(t) \leq \frac{1}{2}\}$

(1)

Random walk on $\mathbb{Z}_2^m$ ← hypercube

$G = \mathbb{Z}_2^m$, $|G| = 2^m$

$S = \{(0 \cdots 1_i \cdots 0),\ 1 \le i \le m\}$



lazy random walk $X_0 = 1$, $X_{t+1} = X_t \cdot s_i^{\varepsilon}$, $\varepsilon \in \{0,1\}$

$\{X_t\}$ ← choose a coord. i, flip a coin
if H, change coord. i

Th $\quad mix = m \log m + O(m)$

▷ Stopping time: mark coord. i when chosen
stop when all coord's are marked.

$(0 \cdots * \quad 0)$
$(0 \cdots * \cdots * 0)$
$(0 \quad * \quad * \quad * 0)$
$\vdots$
$(* * * \cdots * *)$

$\le \tau$ is strong uniform $\square$

$\Rightarrow mix \le 2\, \mathbb{E}[\tau] = 2 m \log m + O(m)$

coupon collector's problem

→

2-9

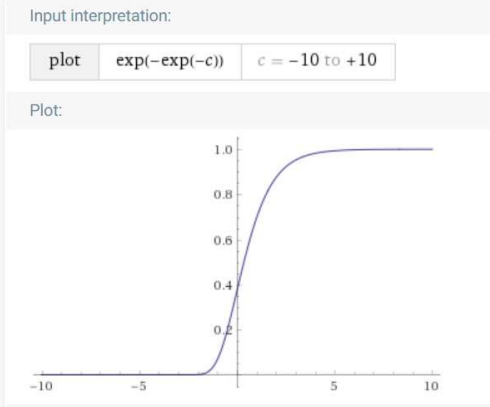
Coupon Collector's Problem

Setup: n coupons, collected one-by-one w/ replacement (unif at random)

$X \leftarrow$ r.v. time to collect all n coupons

Th [Erdös-Renyi, 1961]

$$P(X < n\log n + cn) \to e^{-e^{-c}}$$



Prop

1) $\mathbb{E}[X] = n\log n + \gamma n + O(1)$

where $\gamma = 0.5772\ldots$ Euler-Mascheroni const

2) $Var(X) = \Theta(n^2)$

Cor $P(X > n\log n + \lambda n) = O\left(\frac{1}{\lambda^2}\right)$

3

Proof of 1) $\quad X_k \leftarrow$ time to get k-th coupon

$X = X_1 + \dots + X_n$,

$X_k = \mathrm{Geo}(p_k)$, $p_k = \frac{n-k+1}{n}$

$\mathbb{E}[X_k] = \underbrace{\frac{n}{n-k+1}}_{1/p_k}$, $\mathrm{Var}(X_k) = \frac{1-p_k}{p_k^2} \le \frac{1}{(p_k)^2}$

$$\mathbb{E}[X] = \mathbb{E}[X_1] + \dots + \mathbb{E}[X_n]$$
$$= \sum_{k=1}^{n} \frac{n}{n-k+1}$$
$$= n\left(1 + \frac{1}{2} + \dots + \frac{1}{n}\right)$$
$$= n \log n + \gamma n + O(1) \quad \blacksquare$$

Proof of 2)

$$\mathrm{Var}(X) = \mathrm{Var}(X_1) + \dots + \mathrm{Var}(X_n)$$
$$\le \sum_{k=1}^{n} \left(\frac{n}{n-k+1}\right)^2$$
$$\le n^2 \sum_{k=1}^{n} \frac{1}{k^2} = O(n^2) \quad \blacksquare$$

4

Trading coupons (Newman-Shepp [1960], Erdös-Renyi [1961])

$X^{(k)} \leftarrow$ time to collect k copies of each coupons

Th $P(X^{(k)} < n\log n + (k-1)n\log\log n + cn)$
$\longrightarrow e^{-e^{-c}}$ as $n \to \infty$ $\forall k \leftarrow$ fixed

Cor $\mathbb{E}[X^{(k)}] = n\log n + n\log\log n \times (k-1) + O(n)$

Random graphs applications $G(n,p)$ [1959]

Cor $P(G(n,p)\text{-conn}) \to 0$ for $p < \frac{\log n}{n} - \frac{w(1)}{n}$ | $w(1) \to \infty$ as $n \to \infty$
$P(G(n,p)$ has PM$)$ — // —

Cor $P(G(n,p)$ is Hamiltonian$) \to 0$ for $p < \frac{\log n + \log\log n}{n} - \frac{w(1)}{n}$

5

Back to r.w. on $\mathbb{Z}_2^n$

$T_n \leftarrow$ time to collect n coupons

$\{X_t\} \leftarrow$ lazy r.w. on $\mathbb{Z}_2^n$

We have $\quad sep(t) \leq P(T_n > t)$

Note $\quad P(X_t = (1 \cdots 1)) = \frac{1}{2^n} P(T_n < t) = \frac{1}{2^n} - \frac{P(T_n > t)}{2^n}$

$$sep(t) \geq 2^n \left(\frac{1}{2^n} - P(X_t = (1 \cdots 1)) \right)$$

$$\geq P(T_n > t)$$

$$\Rightarrow \quad \boxed{sep(t) = P(T_n > t)}$$

Cutoff phenomenon

/cf. phase transition/

$$\Rightarrow \begin{cases} \forall \varepsilon > 0 \quad \exists c(\varepsilon) \text{ s.t.} \\ sep(t) > 1 - \varepsilon \qquad t < n \log n - c(\varepsilon) n \\ sep(t) < \varepsilon \qquad t > n \log n + c(\varepsilon) n \end{cases}$$

6

Random walk on $(\mathbb{Z}_p)^n$ $\qquad p = \text{const}$

Idea: indep run stoppin time $\forall\, \mathbb{Z}_p$
stop when all of these stopped. $\Big\}\ \tau$

Claim $\tau \leftarrow$ strong uniform. $\quad | \leftarrow$ Exc.

Cor 1 $\text{mix} = n \log n + O(p^2 n \log\log n)$ $\quad | \leftarrow$ Exc

Cor 2 $p = O(1) \Rightarrow$ cutoff (phenomenon)

Note $n = 1$, $p \to \infty$ $\quad$ no cutoff

Random walk on $U(n, \mathbb{F}_2)$

$$U(n,\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \; * \in \mathbb{F}_2 \right\} \qquad R_n = \left\{ E_{ij} = \begin{pmatrix} 1 & & & \\ & 1 & & 1 \\ & & 1 & \\ 0 & & & 1 \end{pmatrix} \; 1 \le i < j \le n \right\}$$

$\{X_t\} \leftarrow$ lazy rw on $U(n,\mathbb{F}_2)$

<u>Th</u> $\quad mix \le n^2 \log n + O(n^2)$

<u>Note</u> $\quad mix \geq diam\, \Gamma(U(n), R_n) = \Omega(n^2/\log n)$

<u>Proof</u>: [strong uniform time τ construction]

<u>Def</u> write $X_{t+1} = X_t \cdot (E_{ij})^{\varepsilon}$, $\varepsilon \in \{0,1\}$ unif

stop when all (ij) are used.

(8)

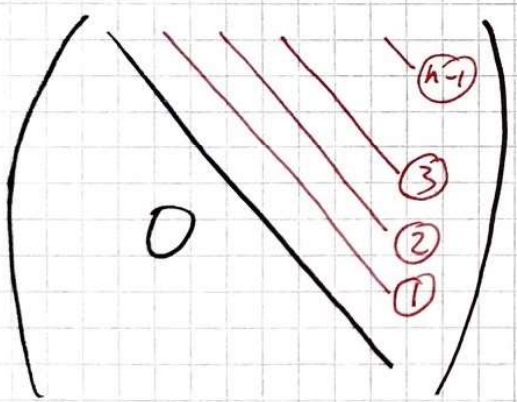
<u>Lemma</u> τ defined above is strong uniform

D $X_t = (E_{i_1 j_1})^{\varepsilon_1} (E_{i_2 j_2})^{\varepsilon_2} \cdots (E_{i_t j_t})^{\varepsilon_t}$

$/gh = hg \cdot [g,h]/$

$$= \left(E_{12}^{\alpha_{12}} E_{23}^{\alpha_{23}} \cdots E_{n-1\,n}^{\alpha_{n-1\,n}}\right)_{①} \left(E_{13}^{\alpha_{13}} E_{24}^{\alpha_{24}} \cdots\right)_{②} \cdot (*)_{[12]}$$

$$\cdot \left(E_{14}^{\alpha_{14}} E_{25}^{\alpha_{25}} \cdots\right)_{③} (*)_{[123]} \cdots \quad (*)_{[1\ldots n]}$$



$\Rightarrow$ coupon collectors problem on $\{(i,j),\ 1 \le i < j \le n\}$ $\square$

D $\mathbb{E}[\tau] = \binom{n}{2} \log \binom{n}{2} + O\left(\binom{n}{2}\right)$

$= n^2 \log n + O(n^2)$ $\square$

L13
(4/27/2020)

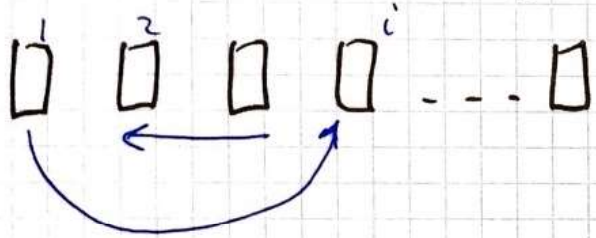
Card Shuffling

Igor Pak

$\text{mix} = O(\mathbb{E}[\tau]) = O(n \log n)$

(1) Top to random

$G = S_n$, $R = \{1, (21), (231), \ldots, (234\ldots n1)\}$



$\longleftrightarrow (23\ldots i1)$

Alg (for τ)

* Wait until n goes to the top
* Do 1 step. STOP

Th [Aldous-Diaconis]

τ - strong uniform

$\underline{L}$ $\forall t$, the relative order of cards below n is uniform.

$\triangleright$ induction $\blacksquare$

$L \Rightarrow Th \Rightarrow \text{mix} = n \log n + O(n)$

$\Rightarrow$ cutoff

1

Def $\{X_t\} \leftarrow$ r.w. on $\Gamma_n = \Gamma(G_n, S_n)$

has cutoff if $\forall \varepsilon > 0,\ \varepsilon < \frac{1}{2}$

$$\frac{t_\varepsilon^{(n)} - t_{1-\varepsilon}^{(n)}}{t_\varepsilon^{(n)}} \to 0 \quad \text{as} \quad n \to \infty$$

$$\boxed{\begin{array}{l} \mathrm{sep}(t) = |G| \max_{g \in G} \left(\frac{1}{|G|} - Q^t(g) \right) \end{array}}$$

where $t_\varepsilon^{(n)} := \min\{ t : \mathrm{sep}(t) < \varepsilon \}$

for r.w. on Γ_n

Ex 1) r.w. on $\mathbb{Z}_2^n$

2) r.w. on S_n (top to random)

Non-Ex $\mathbb{Z}_n$

Conj Ex $\Gamma(S_n, \{(i\ j),\ 1 \le i < j \le n\}) \leftarrow$ But has one in TV

(2)

(2) <u>Star transpositions</u>

$G = S_n$, $R_n = \{(1), (12), (13), \ldots, (1n)\}$

<u>PROP</u> $\operatorname{diam} \Gamma(S_n, R_n) = \frac{3}{2} n + O(1)$

D $\sigma = (1, 3,2, 5,4, 7,6, \ldots 2m+1, 2m)$

$\operatorname{dist}_\Gamma(1, \sigma) = 3m$ ▨

<u>Th</u> $\operatorname{mix} \Gamma(S_n, R_n) = O(n \log n)$

<u>Alg</u> (for τ)

* Mark (n)
* If X_t at $\underline{1}$ unmarked <u>and</u> $(1\ i) \in R$, $i \in \{1\} \cup$ marked, mark it.
* <u>STOP</u> when <u>all</u> <u>marked</u>

<u>L</u> $\forall t$, relative order of marked cards is uniform.

D (□ ... * * * x) □

$\Leftrightarrow$ τ is strong uniform.

(3)

$\underline{L}$ $\mathbb{E}[\tau] = O(n \log n)$

D 1) k marked cards, 1-st unmarked.

$$\mathbb{E}[\text{time until 1-st is marked}] = \frac{1}{(k+1)/n} = \frac{n}{k+1}$$

2) k marked cards, 1-st marked.

$$\mathbb{E}[\text{time until 1-st is unmarked}] = \frac{1}{(n-k)/n} = \frac{n}{n-k}$$

$$\mathbb{E}[\tau] \leq \sum_k \left(\frac{n}{k+1}\right) + \left(\frac{n}{n-k}\right)$$

$$\leq 2n \left(\sum_{k=1}^{n} \frac{1}{k}\right) = O(n \log n) \qquad \blacksquare$$

D $\text{mix}\{X_t\} = O(\mathbb{E}[\tau]) = O(n \log n)$ $\blacksquare$

<u>Note</u> ¿No? cutoff (from this proof)

4

Lower bound

mix $= \Omega(n \log n)$

D $\sigma = (2\,3 \ldots n\,1)$ has no f pts

By coupon collector's problem
not all i's are used after $< n \log n - O(n)$ steps
w.h.p. $\square$

Markov scan

$X_0 = 1$, $X_{t+1} = X_t \cdot (t \bmod n, i)$, $i \in \{1..n\}$ unif.

Th [Mossel - Peres - Sinclair, 2004]

Markov scan has mix $= \Theta(n \log n)$

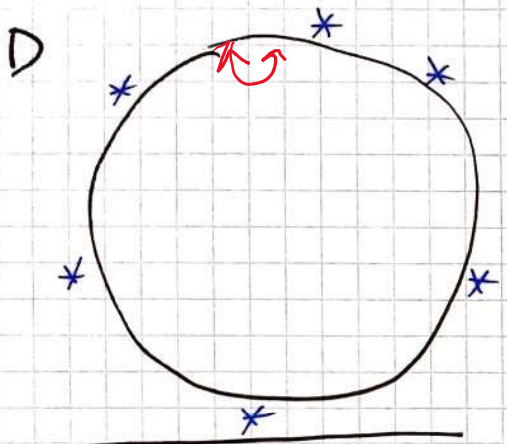
D upper bound $\leftarrow$ same strong unif. time argument
lower bound $\leftarrow$ hard. $\square$

5

(3) $G = S_n$ $\quad R = \{(12), (123\ldots n)^{\pm 1}\}$

<u>Prop/th</u> mix $= O(n^3 \log n)$

<u>Idea</u>



* Mark cards as before for top to random
* slow marking to $\left(\frac{1}{n^2}\right)$ pace ▨

<u>Th</u> [Wilson]

mix $= \Omega(n^3 \log n)$ ← hard.

<u>Exc</u> mix $= \Omega(n^3)$

Cover Time

Def $\{X_t\} \leftarrow$ r.w. on $\Gamma = (V, E)$

CT = (max over all start in $v \in V$) time to visit all vertices.

Th [Matthews]

$$\mathbb{E}[CT] = O(\text{mix} \cdot n \log n), \quad n = |V|$$

D Coupon collector's problem again! ☑

Ex $\Gamma = \Gamma(\mathbb{Z}_2^m, R)$, $n = |\Gamma| = 2^m$, mix $= m \log m$

$$\mathbb{E}[CT] = O((n \log n)\ \text{mix}) = O(2^m \log 2^m\ m \log m)$$

$$= O(2^m m^2 \log m)$$

$$= \Omega(2^m)$$

7

Two Bonus Parts

(4) $G = S_n$, $R_n = \{1, (21), (321), (4321), \ldots (n\,n-1 \ldots 1)\}$

Th [Gates - Papadimitriu, 1979]

$$\operatorname{diam} \Gamma(S_n, R_n) \le \frac{5}{3} n + O(1)$$

/recently improved/

Open $\operatorname{diam} \Gamma > (1+\varepsilon) n$??

---

(5) $X_{n+1} = aX_n + b \bmod p$

prime numper generator.

Mix time? A $O(p \log p)$? No

$\boxed{O(\log p \cdot \log\log p)}$

L14
(4/29/2020)

Random Random Walks

Igor Pak

G – fin. group. $S \subseteq G$ random subset of size k

We know: ① $\varphi_k(G) \geq 1-\varepsilon \quad \forall\, k > \log_2 |G| + O(\log \frac{1}{\varepsilon})$

$\varphi_k(G) = P(\Gamma(G,S) \text{ is connected})$

② $\operatorname{diam} \Gamma(G,S) \leq k \quad \forall\, k > 2\log_2 |G| + O(\log \frac{1}{\varepsilon})$
w/ $P_r > 1-\varepsilon$

Today: ③ $\operatorname{mix} \Gamma(G,S) \leq C \log |G| \quad \forall\, k > c' \log |G| + O(\log \frac{1}{\varepsilon})$
w/ $P_r > 1-\varepsilon$

Random random walks $\Leftrightarrow$ random walks w/ random gen. set. Cf. random walks in random environment

Generalized Random Subproducts

Let $g_1 \ldots g_k$ – unif indep in G, $\bar{g} = (g_1 \ldots g_k)$

$h \leftarrow g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ random subproduct

$Q_{\bar{g}} \leftarrow$ distr. of h.

$Q_k \leftarrow \frac{1}{|G|^k} \sum_{\bar{g} \in G^k} Q_{\bar{g}}$ distr. of random subproducts.

Cor/Th (ε-R) $k > 2\log_2|G| + 2\log_2 \frac{1}{\varepsilon} + \log \frac{1}{\delta}$

$sep(Q_k, U) < \varepsilon + \delta$

D εR Thm $\Rightarrow$ $sep(Q_{\bar{g}}, U) < \varepsilon$ for $1-\delta$ choices.

$\Rightarrow Q_k(g) > (1-\delta)\frac{(1-\varepsilon)}{|G|} > \frac{1-\varepsilon-\delta}{|G|}$ ☒

Plan: we now generalize Q_k to allow repetitions of g_i

2

Fix $x \in G$. $\quad h' := g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} x = hx = Q_k \cdot x$

$\Rightarrow \quad sep(Q_k') = sep(Q_k)$

$$h' := g_1^{\varepsilon_1} \cdots g_i^{\varepsilon_i} x \, g_{i+1}^{\varepsilon_{i+1}} \cdots g_k^{\varepsilon_k}$$

$$= x (x^{-1} g_1^{\varepsilon_1} x)(x^{-1} g_2^{\varepsilon_2} x) \cdots (x^{-1} g_i^{\varepsilon_i} x) \, g_{i+1}^{\varepsilon_{i+1}} \cdots g_k^{\varepsilon_k}$$

$$= x ((g_1^x)^{\varepsilon_1})((g_2^x)^{\varepsilon_2}) \cdots ((g_i^x)^{\varepsilon_i}) \, g_{i+1}^{\varepsilon_{i+1}} \cdots g_k^{\varepsilon_k}$$

$$= x \, v_1^{\varepsilon_1} v_2^{\varepsilon_2} \cdots v_k^{\varepsilon_k}$$, where $v_i = (g_i)^x$ – unif indep

$\Rightarrow \quad sep(Q_k') = sep(Q_k)$

$$h' := (g_1^{\varepsilon_1} \cdots g_i^{\varepsilon_i}) x_1 \cdot (g_{i+1}^{\varepsilon_{i+1}} \cdots) x_2 (\cdots) \cdot x_3 \cdots (\cdots g_k^{\varepsilon_k})$$

$x_1, x_2 \ldots \leftarrow$ all fixed.

$\Rightarrow \quad sep(Q_k') = sep(Q_k)$

Now, what if $x_i \leftarrow$ not fixed? $\quad$ ¡Same!

3

Lazy R-R walk

$S = \{g_1 \dots g_k\}$ ← $\{g_i\}$ are indep, unif in G.

$X_0 = 1$, $X_{t+1} = X_t \cdot g_i^{\varepsilon_i}$, $1 \le i \le k$ random unif
$\varepsilon \in \{0,1\}$ —//—

$X_t = g_{i_1}^{\varepsilon_1} \cdot \dots \cdot g_{i_t}^{\varepsilon_t}$ ← what used to be $\underline{\underline{h'}}$

L $\forall \varepsilon$ $\forall d$ $\exists C, C$ s.t. for $k = c \log|G|$, $t = c' \log|G|$
at least $(1-\varepsilon)$ fraction of
$\bar{i} = (i_1 \dots i_t)$ contain $> d(\log|G|)$
elts which are not repeated

εR Thm + L $\Rightarrow$ $\mathrm{sep}(t) < O(\varepsilon)$ for $t = k + O(\log \frac{1}{\varepsilon})$
w/ $Pr > 1-\varepsilon$

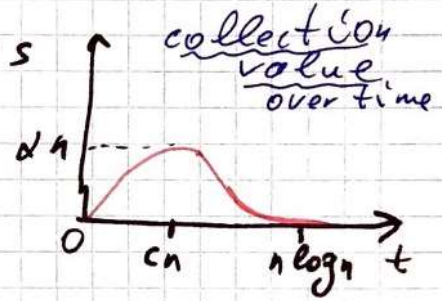
$\Rightarrow$ mix time $= O(\log|G|)$ w/ $Pr > 1-\varepsilon$ ☑

4

Strange coupon collecting

n coupons

Art: Coupon collecting whose value evaporates when repeated.



Q1: At what pt it's still worth expanding your collection?

A1: Until $n/2$ coupons are collected. $\leftarrow \tau$

$$\mathbb{E}[\tau] = \frac{n}{n} + \frac{n}{n-1} + \dots + \frac{n}{n/2} = n\left(\log n - \log \frac{n}{2}\right) \sim n(\log 2)$$

c

Q2: What's worth of your collection at time τ?

A2: Since prob of rep $\leq \frac{1}{2}$ $\Rightarrow$ # non-rep's $\gtrsim \frac{cn}{2}$ $\leftarrow \alpha$

More precisely, # rep $> (\frac{1}{2} + \varepsilon)\, cn$ w/ $\Pr < e^{-cn\varepsilon^2/2}$

/Chernoff Bound/

$\Rightarrow \boxed{\Sigma} \begin{cases} n \leftarrow K \\ d \leftarrow \alpha n \end{cases}, t \leftarrow cn$

5

Notes on the result

① Th ← P. (1996)

G ← Abelian ← cutoff (Hermon-Thomas '19)

using the same tools

/ resolves Conj of Aldous-Diaconsis in this case /

---

② For general g'ps everything is hard.

Th [Lubotzky, proving P. conj]

$k > d(G) + O_\varepsilon(\log\log|G|)$

$\Rightarrow \varphi_k(G) > 1-\varepsilon$

More results on mix time, diam, etc.

Diameter Problems

① Rubik's Cube $\quad |\Gamma| \approx 4.3 \cdot 10^{19}$

Th $\quad \mathrm{diam}(\Gamma) = 20$

[Rokicki et. al, 2014]

AKA "God's number"

1 bil sec of CPU Google

Note: [Kunkle-Cooperman] in 2007

$\mathrm{diam} \le 26$

In 90's $\quad \mathrm{diam} \le 29$

---

② Th [Even-Goldreich, 1981]

$\Gamma = \Gamma(G, S)$, $G \subseteq S_n$ $\Rightarrow$ diam Γ is NP-hard.

Th [Jerrum 1984] $\quad$ diam Γ = PSPACE-c

---

③ $G = U(n, \mathbb{F}_2)$, $S = \{E_{i\,i+1}\}$

$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ Th diam $= \Theta(n^2)$

[Ellenberg 1993]

Open Problem

Find $g \in G$ s.t. $\mathrm{dist}(1, g) = \Omega(n^2)$

Known only for $\Omega(n \log\log n)$

⑦

Two Bonus Parts

(4) $G = S_n$, $R_n = \{1, (21), (321), (4321), \ldots (n\,n-1 \ldots 1)\}$

Th [Gates – Papadimitriu, 1979]

$$\operatorname{diam} \Gamma(S_n, R_n) \le \frac{5}{3} n + O(1)$$

/recently improved/

Open $\operatorname{diam} \Gamma > (1+\varepsilon) n$??

L18

5/8/2020

Dirichlet forms & R.E. Oracle

Igor Pak

G - finite group, $V = \mathbb{R}[G]$

$$\langle \varphi, \psi \rangle := \sum_{x \in G} \varphi(x)\psi(x) = |G| \, \mathbb{E}_{x \in G \text{ uniform}} [\varphi(x)\psi(x)]$$

$$\mathcal{E}_\pi(\varphi, \varphi) := \langle (1 - P_\pi)\varphi, \varphi \rangle = |G| \cdot \mathbb{E}\left[(\varphi(X_0) - \varphi(X_1))\varphi(X_0)\right]$$

where $X_0 \leftarrow \text{unif}, \quad X_1 = X_0 \pi$

$$[P_\pi \varphi](x) := \sum_{y \in G} \varphi(xy)\pi(y)$$

L $\pi, \tilde{\pi} \leftarrow$ dist on G s.t.

$$\mathcal{E}_{\tilde{\pi}}(\varphi, \varphi) \le A \, \mathcal{E}_\pi(\varphi, \varphi) \quad \forall \varphi$$

Then $(1 - \tilde{\lambda}_i) \le A(1 - \lambda_i)$

$\Rightarrow$ r.w. applications via D&S-C Thm

Formally $\quad G = \langle S \rangle \Rightarrow \pi(x) = \frac{1}{|S|} \quad \forall s \in S$

$$M_\pi = \left(a_{xy} \right)_{x,y \in G} \qquad a_{xy} = \pi(x^{-1}y)$$

$$\pi(x) = \pi(x^{-1}) \ \forall x \in G \Rightarrow M = M^T \Rightarrow \lambda_i \in \mathbb{R}$$

$$/ \Leftrightarrow S = S^{-1} /$$

Eigenvalues $\quad 1 = \lambda_0 > \lambda_1 > \dots > \lambda_{|G|-1} \geq -1$

$\pm f \quad 1 \in S \Rightarrow \lambda_{|G|-1} > -1$

$\pi(1) \geq \frac{1}{2} \Rightarrow \lambda_i \geq 0$

Operators $\quad Q := 1 - P_\pi \quad$ on V

Prop $\quad \forall \ Q = Q^T$

$$\min_{\varphi \in V} \frac{\langle Q\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle} = \text{smallest eig of } Q$$

2

$\triangleright$ $$\max_{\varphi} \frac{\langle P_\pi \varphi, \varphi\rangle}{\langle \varphi, \varphi\rangle} = \max \text{ eig of } P_\pi = \lambda_0$$

$$\min_{\varphi} \frac{\langle Q\varphi, \varphi\rangle}{\langle \varphi, \varphi\rangle} = \min_{\varphi:\ \sum_x \varphi(x)=0} \frac{\langle Q\varphi, \varphi\rangle}{\langle \varphi, \varphi\rangle} = \lambda_1 \qquad \boxtimes$$

<u>Th</u> $Q = Q^T$ symm operator on V

[min-max principle] $q_0 \le q_1 \le \dots \le q_n$ eig.

$$m(W) := \min \left\{ \frac{\langle Qf, f\rangle}{\langle f, f\rangle},\ f \in W \subseteq V \right\}$$

<u>Then</u>

$$q_i = \max \{ m(W) : \dim W = i \}$$

$\triangleright$ <u>Exc</u> Hint: take $W = \langle v_0\, v_1 \dots v_{i-1} \rangle$ $\boxtimes$

<u>Th</u> $\Rightarrow$ $(1-\tilde{\lambda}_i) \le A\,(1-\lambda_i)$

Random Elements Oracle

$G = \langle S \rangle$ ← black box group

$S = \{s_1 \dots s_k\}$, $s_i \in S_N$, $GL(n, \mathbb{F}_q)$, etc.

Want: random elts $x \in G$

$\Leftrightarrow$ Probab distr $Q(x)$ on G s.t.

$sep(Q, U) < \varepsilon$, $\varepsilon > 0$ / $\varepsilon = 1/2$ V /

Alg [Babai, 1991]

$R \leftarrow S \cup S^{-1}$

$x \leftarrow$ Lazy random walk for L steps

$R \leftarrow R + x$

Repeat ℓ times

Output last x

Th [Babai]

$L = O((\log |G|)^4)$

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

works

Note: $4 \to 3$ [P]

4

Proof Outline $\Gamma = \Gamma(G, S)$

$X \subseteq G$ subset, $|X| \leq \frac{|G|}{2}$

Main L after $t = O(\mathrm{diam}_\Gamma(X)\, N\, |S| \log |G|)$ steps

lazy r.w. $\notin X$ w/ $P_r > \frac{1}{2}$

Here $\mathrm{diam}_\Gamma(X)$, N defined as in D-SC thm

D $\leftarrow$ Exc on using Dirichlet forms.

Hint: take $\pi(x) = \frac{1}{|X|}$ $\forall x \in X$, $\pi(x) = 0$ o.w. ∎

Consider ε R-cube

$C_S = \{ s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k},\ \varepsilon_i \in \{0,1\} \} \subseteq G$

$X := C^{-1} C$, $g \in G$ s.t. $g \notin C^{-1} C$

$\Rightarrow C_{S \cup g} = \{ s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} g^{\alpha},\ \alpha \in \{0,1\} \} = C_S \sqcup C_S g$

5

$\Rightarrow$ By <u>ML</u> each iteration $\in C_S^{-1} C_S$ w/ $P_1 > \frac{1}{2}$

for $t = O(\underset{\text{dian}}{k} \cdot \underset{N}{2} \cdot \underset{|R|}{k} \cdot \log|G|)$

Using random subproducts $\rightarrow$ $k \leq O(\log|G|)$

after $\ell = O(\log|G|)$ iterations ε R-cube

will double $\Omega(\log|G|)$ times until

$C_R^{-1} C_R > |G|/2$ $\Rightarrow$ $|R| = O(\log|G|)$ $\forall$ times

$\Rightarrow$ $t = O((\log|G|)^3)$

<u>Exc</u> $|X| > |G|/2$ $\Rightarrow$ $X^2 = G$

Moreover distr. $\approx$ uniform.

<u>Why</u> $3 < 4$? (in our case)

Cooperman - Dixon Alg

Alg (G, S) ← Black Box

$R \leftarrow S$

$h \leftarrow s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$, $R = \{s_1 \ldots s_k\}$

$R \leftarrow R + h$

Repeat ℓ times

Th [Dixon, 2006] / Conj By Cooperman '02

$\ell = O(\log |G|)$ works

PROOF IDEA:

0) $X \subset G$, $X^2 \approx X \Rightarrow X \approx$ subgroup

1) $s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} \cdot h^d = C \cup C^2$ w/ $Pr \geq \frac{1}{2}$ ← similar

2) $P(h \notin \text{subgroup}) \geq \frac{1}{2}$

4/1/+ 2) ⇒ doubling w/ $P > \text{const} > 0$

7

L19
5/11/2020

Igor Pak

Product Replacement Algorithm

Want: generate random elements in $G = \langle S \rangle$
(Black Box group) $S = \{s_1, \dots s_k\}$

We Know: Erdös-Renyi Alg to prune $|S| \to O(\log|G|)$

cost $= O(k \log|G| \, \mu)$

Babai Alg for $|S| = O(\log|G|)$

cost $= O(\log^4|G|)$ [Babai + P.]

Cooperman-Dixon Alg for $|S| = O(\log|G|)$

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

PRA ← Practical Alg by [Celler, Leedham-Green, Murray, Niemeyer, O'Brien]
(1995)

Claim in [CLMNO] : works in "100 steps"

Alg $\bar{s} \leftarrow (s_1 \ldots s_k \underbrace{11 \ldots 1}_{k})$, $m \leftarrow 2k$

Do: $\bar{s} = (s_1 \ldots s_m) \rightarrow (s_1 \ldots s_i s_j^{\pm 1} \ldots s_m)$
or $(s_1 \ldots s_j^{\pm} s_i \ldots s_m)$

where (ij) , ± 1 , $\updownarrow$ chosen unif.

Repeat t steps

Output random s_i

Exc Prove that $t = 100$ is NOT enough to make $sep(Q, U) \leq \frac{1}{2}$

Our Main Goal: ① Prove that PRA does not work

② Prove that fixed version works in poly time.

③ cost $= O(k \log |G| \mu)$ time

Product Replacement Graph

$\Gamma_k(G)$, $k \geq d(G)$ ← min # gen's.

Vertices: $(g_1 \cdots g_k)$ s.t. $\langle g_1 \cdots g_k \rangle = G$, $g_i \in G$.

edges: $(g_1 \cdots g_i \cdots g_j \cdots g_k) \to (g_1 \cdots g_i g_j^{\pm 1} \cdots g_j \cdots g_k)$

or $\to (g_1 \cdots g_j^{\pm 1} g_i \cdots g_j \cdots g_k)$

Note: $|\Gamma_k(G)| = \#\text{vertices} = \varphi_k(G)\, |G|^k$

$\boxed{\text{Questions: about } \Gamma_k(G)}$

(1) connectivity

(2) bias

(3) expansion / mixing time

Connectivity of $\Gamma_k(G)$

Ex $G = \mathbb{Z}_p^m$, $p \leftarrow$ prime, $k = m$

$$(g_1 \cdots g_m) \leftrightarrow \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{nm} \end{pmatrix} = A \quad \leftarrow \text{vertices}$$

$$A \to A \underbrace{\begin{pmatrix} 1 & & \\ & \ddots & \pm 1 \\ 0 & & 1 \end{pmatrix}}_{= E_{ij}^{\pm 1}} \quad \text{or} \quad E_{ij}^{\pm 1} A \quad \leftarrow \text{edges}$$

$\det(A E_{ij}^{\pm 1}) = \det(A) \Rightarrow \Gamma_m(\mathbb{Z}_p^m)$ $\underline{(p-1)}$ conn. comp'ts.

Prop $\Gamma_2(S_n)$, $\Gamma_2(A_n)$ has unbounded # conn. comp.

D (Higman) $[g_1 g_2]^G \leftarrow$ conj clas is invariant on conn. comp.

eg. $[g_1 g_2 g_2] = (g_1 g_2)(g_2)(g_2^{-1} g_1^{-1}) g_2^{-1} = [g_1 g_2]$

4

or $[g_2 g_1, g_2] = (g_2 g_1)(g_2)(g_1^{-1} g_2^{-1})\, g_2^{-1}$

$$= g_2 (g_1 g_2 g_1^{-1} g_2^{-1}) = [g_1, g_2]^{(g_2^{-1})}$$

$\Rightarrow$ One needs unbounded # gen's $\langle \sigma, \omega \rangle = A_n$ with distinct $[\sigma, \omega]$

<u>Take</u> $\sigma = (12 \ldots n)$, $\omega = (12 \ldots p)$, use Jordan's thm $\boxtimes$

<u>Note</u>: $\exists$ exp # of conj. classes of $[\sigma, \omega] \Rightarrow$ exp # of conn. comp's

<u>Th</u> [Guralnick-P]
Same holds for $G = SL(2,p)$, etc.

<u>Conj</u> $\Gamma_k(G)$ conn $\forall k \geq d(G) + 1$

<u>Th</u> [Dunwoody] Conj holds for G-solvable
1970

Positive results

$d(G) = \min \#$ gen's , $m(G) = \max \#$ non-redundant gen's

Th $\Gamma_k(G)$ - conn $\forall\ k \geq d(G) + m(G)$

$\triangleright$ 1) $(g_1 \cdots g_k) \to (g_1 \cdots g_{i-1}\ 1\ g_{i+1} \cdots g_k)$

2) $(\cdots g_i \cdots g_j \cdots 1 \cdots) \to (\cdots g_i\ g_j\ g_i \cdots) \to (\cdots 1\ g_j \cdots g_i)$

$\to (\cdots g_j \cdots g_j \cdots g_i \cdots) \to (\cdots g_j \cdots g_i \cdots g_i \cdots) \to (\cdots g_j \cdots g_i \cdots 1 \cdots)$

3) $(\cdots g_i \cdots 1 \cdots) \to (\cdots g_i \cdots g_i \cdots) \to (\cdots g_i^{-1} \cdots g_i \cdots) \to (\cdots g_i^{-1} \cdots 1 \cdots)$

Now $(g_1 \cdots g_k) \to (g_1' \cdots g_m' 1 \cdots 1) \to (g_1' \cdots g_m' h_1 \cdots h_d 1 \cdots 1)$

$\to (h_1 \cdots h_d 1 \cdots 1)$ $\forall \bar{g}$ and $\langle h_1 \cdots h_d \rangle = G$

$\Rightarrow \Gamma_k(G)$ conn. $\square$

6

Ex $G = S_n$, $d(S_n) = 2$, $m(S_n) = n-1$

$\Rightarrow \Gamma_{n+1}(S_n)$ - conn. [Cooperman-P.]

Open: $\Gamma_3(S_n)$ - conn? / Prop true $\forall n \leq 17$ /

Ex $G = SL(2,p)$, $d(G) = 2$, $m(G) \leq 4$

$\Rightarrow \Gamma_k(G)$ conn. $\forall k \geq 6$

Def $\Gamma = (V, E)$ has "large conn. comp" if

$\exists$ conn. comp of size $(1-o(1))|V|$ as $|V| \to \infty$

Th $\Gamma_3(A_n)$ has a large conn. comp.

D $\langle g_1\ g_2\ g_3 \rangle \in \Gamma_3(A_n)$

$\overset{\shortparallel}{A_n}$

$\langle h_1\ h_2\ h_3 \rangle$

$$\begin{tikzcd}
(g_1\ g_2\ g_3) \arrow[r, "uhp"'] \arrow[d, leftrightarrow] & (g_1\ g_2\ h_3) \arrow[d, "uhp"] \\
(h_1\ h_2\ h_3) & (g_1\ h_2\ h_3) \arrow[l, "uhp"]
\end{tikzcd}$$

← Dixon Thm

$\blacksquare$

7

5/13/2020

Product Replacement graphs

Igor Pak

Def $G = \langle S \rangle$, $d = d(G)$, $k \geq d(G)$

$\Gamma_k(G) = (V, E)$, $V = \{(g_1 \dots g_k) : \langle g_1 \dots g_k \rangle = G\}$

$$E = \left\{ \begin{array}{l} (g_1 \dots g_i \dots g_k) \in V \leftrightarrow (g_1 \dots g_i' \dots g_k) \in V \\ g_i' = g_i g_j^{\pm 1}, \quad i \neq j, \quad g_i' = g_j^{\pm 1} g_i \end{array} \right\}$$

Conj $k \geq d(G)+1 \Rightarrow \Gamma_k(G)$ conn

Th $k \geq d(G) + m(G) \Rightarrow$ — 〃 —, $m(G) =$ max non-red gen. set.

Th $G = A_n, S_n, SL(2,P)$, etc, $k \geq 3$

$\Rightarrow \Gamma_3(G)$ has a large conn. comp.

Th [Babai, '96] $k \geq 2 \log_2 |G|$

Then $\operatorname{diam} \Gamma_k(G) = O(\log^2 |G|)$

Proof 0) $(g_1 \dots g_k) \xrightarrow[O(k^2)]{} (g_1' \dots g_\ell' \; 1 \dots 1)$ $\qquad \ell = \frac{1}{2}k = \log_2|G|$

1) $(s_1 s_2 \dots s_\ell \; 1 \dots 1) \to (s_1 s_2 \dots s_\ell \; h_1 1 \dots 1)$

$\to (s_1 s_2 \dots s_\ell \; h_1 h_2 1 \dots 1) \to \dots$

$\to (s_1 s_2 \dots s_\ell \; h_1 h_2 \dots h_\ell)$ $\qquad \boxed{\ell \cdot O(\ell)}$

$h_i \in$ random subproduct

$h_i = g_1^{\varepsilon_1} s_2^{\varepsilon_2} \dots s_k^{\varepsilon_k} \times h_1^{\alpha_1} \dots h_{i-1}^{\alpha_{i-1}}$

2) $\to (1 \; 1 \dots 1 \; h_1 h_2 \dots h_\ell)$ $\qquad \boxed{O(\ell^2)}$

s.t. $C(h) = \{ h_1^{\varepsilon_1} \dots h_\ell^{\varepsilon_\ell} \} = G$

$s_i = h_1^{\varepsilon_1} \dots h_\ell^{\varepsilon_\ell}$

3) $(1 1 \dots 1 \; h_1 h_2 \; h_\ell) \to (h_1 h_2 \dots h_\ell \; 1 \dots 1) \to (h_1 \dots h_\ell \; h_1' \dots h_\ell')$

$\to (1 \dots 1 \; h_1' \dots h_\ell')$ $\qquad \boxed{O(\ell^2)}$

In summary: $\bar{g} \xrightarrow[1)]{} \bar{s} \xrightarrow[2)]{} h \xrightarrow[3)]{} h' \xleftrightarrow[2)']{} \bar{s}' \xleftarrow[1)']{} \bar{g}'$

Total: $O(\ell^2)$

Analysis? $\longrightarrow$

2

$\boxed{\text{I}}$ Assuming Cooperman-Dixon Thm

$k \geq c \cdot \ell$, $\ell = \log_2 |G|$ /where $c = 10$ /

$\Rightarrow \underbrace{h_{m+1} \cdots h_{m+2\ell}}_{\bar{h}}$ $\leftarrow$ ≈unif in G $m = k - 2\ell$

$\Rightarrow$ ER th $C(\bar{h}) = \{ h_{m+1}^{\varepsilon_1} \cdots h_{m+2\ell}^{\varepsilon_\ell} \} = G$ $\Rightarrow$ ▨

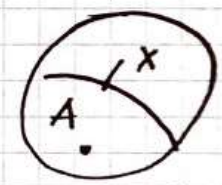
$\boxed{\text{II}}$ Babai way (w/ out C-D thm)

$(s_1 \ldots s_\ell \; h_1 \ldots h_{i-1} 1 \ldots 1) \to (s_1 s_2 \ldots s_\ell \; h_1 \ldots h_{i-1} \; \underline{\underline{h_i}} \; 1 \ldots 1)$?

We choose $h_1 \ldots h_i$ s.t $C(h_1 \ldots h_i) = 2^i$

Let $A = \underset{\shortparallel C(h_1 \ldots h_{i-1})}{C} \cdot C^{-1} \subset G$. If $A \neq G$

$\exists x \in \partial_S A$



Cay(G, S)

Take $h_i \leftarrow x$

$\Rightarrow C(h_1 \ldots h_i) = C(h_1 \ldots h_{i-1}) \cup C(h_1 \ldots h_{i-1}) h_i$

Same argument : $\exists h_1 \ldots h_\ell$, $A = G$. ▨

3

Bias in the PRA

Th [Hall]

$H \leftarrow$ non-ab simple group

$\alpha_k(H) = \max\{m : d(H^m) = k\}$

Then $\alpha_k(H) = \#$ orbits of $\mathrm{Aut}(H)$ action on $\Gamma_k(G)$

Cor $\alpha_2(A_n) > \frac{n!}{8}$ for n large enough

/th $\forall n \geq 5$ /

Ex (Hall) $\alpha_2(A_5) = 19 > \frac{5!}{8} = 15$

$\triangleright$ (of Cor) $\mathrm{Aut}(A_n) = S_n$ $\forall n = 5, \geq 7$

Exc Find $\mathrm{Aut}(A_6) \neq S_6$

$$|\Gamma_2(A_n)| > \frac{1}{2}|A_n|^2 = \frac{n!^2}{8}$$

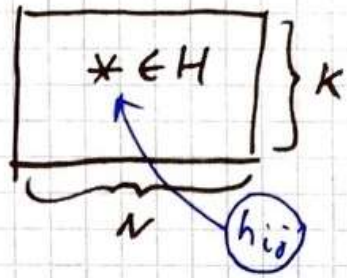
$$\Rightarrow \# \text{ orbits} > \frac{n!}{8}$$

$\blacksquare$

Proof of Hall thm (abridged)

$G = H^N$

$(g_1 \cdots g_k) \in G^k$



$g_i = (h_{i1} \ldots h_{iN})$

Note: $\forall j \quad \langle h_{1j} \ldots h_{kj} \rangle = H$

$\underline{\subseteq}$ (Hall)

$(h_{ij}) \in \Gamma_k(G) \iff$ all $(h_{1j} \ldots h_{kj})$ lie in diff. orbits of $\mathrm{Aut}(H)$

$\Rightarrow$ obvious since oth. $O_j \overset{\omega}{\simeq} O_j \quad \omega \in \mathrm{Aut}(H)$

$\Leftarrow$ Exc

$\blacksquare$

L21
5/15/2020

Igor Pak

Bias of the PRA

Before: $\Gamma_k(G)$ = graph on generating k-tuples $\langle g_1 \dots g_k \rangle = G$, $k \geq d(G)$

PRA: - random walk on $\Gamma_k(G)$
- output random g_i, $i \in \{1 \dots k\} \leftarrow Q$

#vertices $|\Gamma_k(G)| = \varphi_k(G)\, |G|^k$

Idea: $k \leftarrow$ large enough so that $\varphi_k(G) > 1 - \varepsilon$

e.g. Th [Lubotzky, '02] $k = d(G) + O(\log\log|G|)$

Exc $\Rightarrow |Q, U|_{TV} < \varepsilon$ $\quad / \Rightarrow_{\text{post Exc}}$ $\text{sep}(Q^2, U) \ll \varepsilon$

Bias: Distribution $Q \leftarrow$ of g_i, $i \in$ random in $\bar{g} = (g_1 \dots g_k)$ and $(g_1 \dots g_k)$ random in $\Gamma_k(G)$

$\Rightarrow$ look for Bias only when $\varphi_k(G)$ small

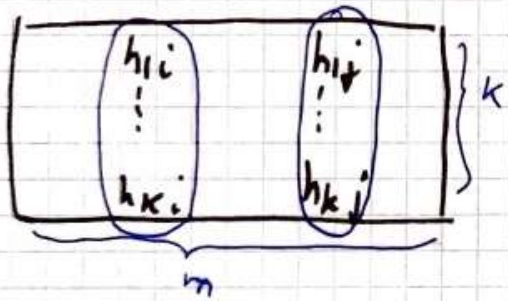
1

Th [Hall, 1936] H – fin simple group, non-ab

$$\alpha_k(H) := \max\{m : d(H^m) = k\}$$

then $\alpha_k(H) = \#$ orbits of $\mathrm{Aut}(H)$ acting on $\Gamma_k(H)$

$\triangleright$ $G = H^m$ $\quad \langle g_1 \dots g_k \rangle = G \quad g_i = (h_{i1} \dots h_{im})$

$\bar{g} \leftrightarrow$ 

$\bar{h}^{(i)} = \begin{pmatrix} h_{1i} \\ \vdots \\ h_{ki} \end{pmatrix}$ $\quad h^{(1)} \dots h^{(m)} \in \Gamma_k(H)$

since $\langle h_{1i}, \dots h_{ki} \rangle = H$

$\psi : \begin{pmatrix} h_1 \\ \vdots \\ h_k \end{pmatrix} \to \begin{pmatrix} \psi(h_1) \\ \vdots \\ \psi(h_k) \end{pmatrix}$

$\Gamma_k(H) \Rightarrow \Gamma_k(H)$

L $(h_{ij}) \leftrightarrow \bar{g} \in \Gamma_k(G) \Leftrightarrow \{h^{(1)} \dots h^{(m)}\}$ lie in diff orbits of $\mathrm{Aut}(H)$ on $\Gamma_k(H)$

Th $\Leftrightarrow$ **L** $\quad \triangleright$ (lemma) $\Rightarrow$ obvious

since "$\in$ same orbit" is invariant under multiplication

2

$\Leftarrow$ direction Suppose true for $m-1$

(By induction) $h^{(1)} \dots h^{m-1}$ $\in$ diff orbits $\Rightarrow$ gen'te H^{m-1}

Take $h^1 \dots h^{m-1} h^m = \underbrace{\left(h_{ij} \right)}_{m-1} \Big\} k \Leftrightarrow \bar{g}$

Observe $\{h^1 \dots h^m\} \Rightarrow \langle \bar{g} \rangle = \langle g_1 \dots g_k \rangle = (* * \dots * \bullet) \subset H^m$
$\qquad\qquad\qquad

Last time $\boxed{L}$ Hall thm $\Rightarrow$ $\alpha_2(A_n) > \frac{n!}{8}$ n - large enough

D $|\Gamma_2(A_n)| > \frac{1}{2}|A_n|^2 = \frac{n!^2}{8}$

$$\alpha_2(A_n) > \frac{|\Gamma_2(A_n)|}{|\mathrm{Aut}(A_n)|} > \frac{n!^2/8}{n!}$$ n - large enough $\boxtimes$

Cor $G := A_n^{n!/8}$ then $\varphi_k(G) \to 0$ as $n \to \infty$

$d(G) = 2$ $\forall k = o(n)$

/ $\forall n$ large enough /

D $\varphi_k(A_n^{n!/8}) \leq [\varphi_k(A_n)]^{n!/8} < \left(1 - \frac{1}{n^k}\right)^{n!/8}$

$\varphi_k(A_n) = P(\langle \sigma_1, \dots \sigma_k \rangle = A_n) < 1 - P(\sigma_1(1) = \dots = \sigma_k(1) = 1) = 1 - \frac{1}{n^k}$ $\boxtimes$

Thus this is a group to look for bias!

L $\varphi_k(A_n^{n!/8}) \geq [\varphi_k(A_n)]^{n!/8}\left(1 + O\left(\frac{1}{n!^{k-3}}\right)\right)$ $k \geq 4$

D #orbits $> \frac{|A_n|^k}{[S_n]} = \frac{(n!/2)^k}{n!}$ we have $n!/8$ of them. $\longrightarrow$

• N'' • $\oplus$ B Day • Paradox $\boxtimes$ • 4

/ <u>BDay Paradox explained</u>: $h^{(1)} \ldots h^{(m)} \in \Gamma_k(H)$

$$P(h^{(1)} \ldots h^{(m)} \in \text{diff orbits of } Aut(H))$$

$$= \left(1 - \frac{1}{N}\right)\left(1 - \frac{2}{N}\right) \ldots \left(1 - \frac{m-1}{N}\right) > 1 - \frac{m^2}{2N}$$

$m = n!/g \qquad N = \frac{(n!/2)^k}{n!} > c\,(n!)^3$ by $k \geq 4$ /

$\Rightarrow \underline{L}\ \bar{g} \leftrightarrow (h^{(1)} \ldots h^{(m)})$ random in $\Gamma_k(G)$

$\bar{Q} \leftarrow$ distr of $h^{(1)}$ from $\bar{g}$

$Q \leftarrow$ distr of $h^{(1)}$ from $\Gamma_k(H)$

<u>Then</u> $|\bar{Q} - Q|_{TV} \leq O\left(\frac{1}{n^{k-3}}\right)$

<u>Th</u> [Babai-PT2004] $G = (A_n)^{n!/g}$, $k = o(n)$, $k > 4$

$Q \leftarrow$ distr of g_1 in random unif $(g_1 \ldots g_k) \in \Gamma_k(G)$

<u>Then</u> $|Q - U| \to 1$ as $n \to \infty$

5

Proof of Bias

$G = A_n^{n!/g}$, $M = n!/g$

$\bar{g} \in \Gamma_k(G)$ $\qquad \bar{g}_i = g(\sigma_1 \dots \sigma_M)$

$\bar{g} = (g_1 \dots g_k)$ $\qquad$ If $g_1 \in G$ unif $\Rightarrow P(\sigma_1(1) = 1) = \frac{1}{n}$

$\underline{\text{L}}$ $\quad g_1 \in G$ from $Q \Rightarrow P(\underbrace{\sigma_1(1) = 1}_{B}) = \frac{1}{n} - \frac{1}{n^k} + O\left(\frac{1}{n^{2(k-1)}}\right)$

D

$h^{(1)} = \begin{pmatrix} \sigma_{11} \\ \vdots \\ \sigma_{k1} \end{pmatrix}$ $\qquad h^{(1)} \in \Gamma_k(A_n) \Leftrightarrow$ not all $\sigma_{i1}(1) = 1$

$$P(\underbrace{\langle \sigma_{11} \dots \sigma_{k1} \rangle = A_n}_{A}) \underset{\text{Babai th}}{=} 1 - \frac{1}{n^k} n + \frac{1}{(n(n-1))^k}\binom{n}{2} + \frac{1}{2(n(n-1))^k}\binom{n}{k}$$

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

Then

$$P(B|A) = \frac{P(A|B)\,\overset{=\frac{1}{n}}{P(B)}}{P(A)}$$

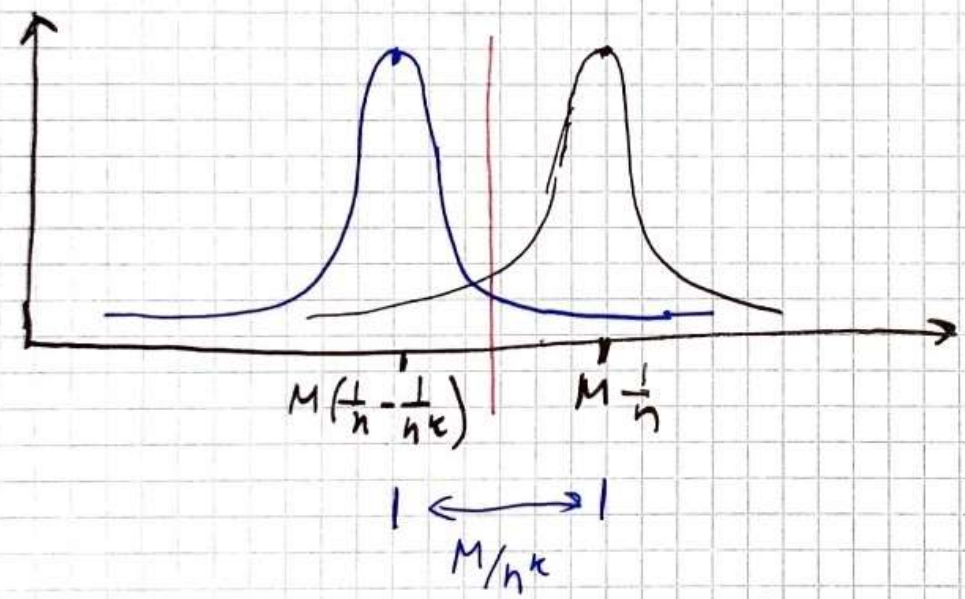
$$= \left(\frac{1}{n}\right) \frac{1 - 2/n^{k-1} + O(\ )}{1 - 1/n^{k-1} + O(\ )} = \frac{1}{n} - \frac{1}{n^k} + O(\ ) \quad \square$$

6

$G = A_n^{n!/8}$ $\qquad g = (\sigma_1, \dots \sigma_M)$, $\quad M = n!/8$

$\mathbb{E}[\# \sigma_i(1) = 1] = M \cdot \frac{1}{n}$ $\qquad g \in$ uniform.

$\mathbb{E}[\# \sigma_i(1) = 1] = M \cdot \left[\frac{1}{n} - \frac{1}{n^k} + O(\,)\right]$ $\qquad g \in Q$



Let $X := \{ \bar{g} \in G$ s.t. $\#\{\sigma_i(1) = 1\} > M(\frac{1}{n} - \frac{1}{2n^k})$

then $|X| \geq |G| \left(1 - \frac{n^k}{\sqrt{M}}\right)$

$Q(X) < \frac{n^k}{\sqrt{M}} \to 0$

$U(X) \to 1$

as $n \to \infty$

$\blacksquare$

Use Chernoff Bound

$(g_1 \dots g_k h)$

$\boxed{\text{STORY}}$

7

L22
5/18/2020

Igor Pak

Exhibiting the Bias

Last time: $G = (A_n)^{n!/8}$, $k \geq 4$, $k = o(n)$

$Q_k \leftarrow$ distr of g_i in random $\bar{g} = (g_1 \ldots g_k) \in \Gamma_k(G)$

Th [Babai-P] $|Q - U|_{TV} \to 1$ as $n \to \infty$

Explanation: (1) $\varphi_k(G) < \left(1 - \frac{1}{n^k}\right)^{n!/8} \to 0$

(2) $\exists$ subset $X \subset G$ s.t. $\frac{|X|}{|G|} \to 1$, $Q_k(X) \to 0$
/explicitly constructed/

Today: We exhibit the bias.

Construct words $w = \text{word}[x_1, x_2 \ldots]$
s.t. length $|w| = \text{poly}(n)$

$w[Q_k] = 1$ whp
$w[U] \neq 1$ w.h.p

} Mistaken law in G!

1

Idea: Monotone formulas

$Y_1\ Y_2 \ldots$ ← iid elts in G, from Q

Let us assume: $P(Y_i = 1) < \frac{1}{N}$, N- large

$$\begin{cases} Y_i = 1 & \leftarrow \text{Tuth} \\ Y_i \neq 1 & \leftarrow \text{False} \end{cases}$$

$\Rightarrow$ $Y_i\ Y_j = 1 \Leftrightarrow Y_i \wedge Y_j = \text{True}$

$[Y_i\ Y_j] = 1 \Leftrightarrow Y_i \vee Y_j = \text{True}$

Main Ex $Q = U$ on A_n

$P(Y_i = 1) = \frac{1}{(n!/2)}$

$P(Y_i\ Y_j = 1) = \frac{1}{(n!/2)}$

$P([Y_i\ Y_j] = 1) = P(Y_i\ Y_j = Y_j\ Y_i)$

$= \frac{P(n)}{|A_n|} = \frac{e^{O(\sqrt{n})}}{(n!/2)}$

/all factorially small $\Leftrightarrow$ $= O(n^{-cn})$ /

2

Def (monotone formula)

$F: \quad [(Y_1 \vee Y_3 \vee Y_6) \wedge (Y_2 \vee Y_4 \vee Y_7) \wedge (Y_1 \vee Y_5)] \vee [*] \ldots$

$\text{word}_F \leftarrow [[[Y_1\ Y_3]\ Y_6] \cdot [[Y_2\ Y_4]\ Y_7]\ [Y_1\ Y_5],\ *] \ldots$

We construct F so that word_F works.

First STEP : From Q to U

L1 $\lambda \vdash n$, $C_\lambda \leftarrow$ corresp. conj. class in S_n or A_n

Then $\text{diam}(\text{Cayley}(A_n, C_\lambda)) \leq cn$, some for S_n, $c > 1$

▷ ① $(ij) \in$ product of 2 ℓ-cycles (Exc)

② every $\sigma \in S_n \in$ product of $\leq (n-1)$ transpositions

②' —"— $\sigma \in A_n \in$ —"— $\leq n/2$ pairs of transp.

$\Rightarrow$ diam $< 2n$ ▨

● Exc diam $\leq (n-1)$ ● in S_n, $\leq \frac{n}{2}$ in ● A_n ● ③

L2 $R = C_\lambda$, $G = A_n$ or S_n

$\{X_t\} \leftarrow$ r.w. on Cayley $(G, R) = \Gamma(G, R)$

Then mix $= O(n^3 \log n)$

D We know: mix $= O(\text{Diam } N_\gamma \, |R| \log |G|)$

where $\gamma = \{\gamma_g : 1 \to g \ \forall g \in G\}$ paths in $\Gamma(G, R)$

Consider $\bar{\gamma} = \bigcup a^{-1} \gamma a \quad \forall a \in \text{Aut}(G) / = S_n /$

Since $R \leftarrow$ inv under $\text{Aut}(G)$, $\bar{\gamma}$ valid collection of paths.

$\Rightarrow N_{\bar{\gamma}} \leq \dfrac{\text{Diam}}{|R|} \Rightarrow$ mix $= O(\text{Diam}^2 \log |G|)$

$=_{L1} O(n^2 \cdot n \log n) = O(n^3 \log n)$ ▨

Known: mix $= O(n \log n)$, achieved on $R = \{(i\,i)\}$ transpositions

Biased dist Q on $A_n = G$

$X_1 X_2 \ldots \leftarrow$ iid on A_n from Q

$Y_i := (z_1^{-1} X_1 z_1)(z_2^{-1} X_2 z_2) \ldots (z_\ell^{-1} X_\ell z_\ell)$

$\ell = O(n^3 \log n) \Rightarrow$ r.w. on conj. clas of X_1

where $z_i \leftarrow U$ on G.

$\Rightarrow$ if $Q(1) \neq 1$ uhp $\Rightarrow$ Y_i is nearly-uniform

sep( ) $\leq \varepsilon \Leftrightarrow P(Y_i = g) > \frac{1-\varepsilon}{|G|}$

$Q(1) = 1$ uhp $\Rightarrow$ $Y_i = 1$ u.h.p.

u.h.p $\Leftrightarrow$ w/ $P > 1 - O(n^{-c_n})$

We want: word $(X_1 X_2 \ldots)$ s.t. $X_i \leftarrow U \Rightarrow$ word $\neq 1$ uhp

and $X_i \leftarrow Q \Rightarrow$ word $= 1$ uhp.

Thus $z_i \leftarrow X_i \leftarrow$ in U case ✓

Q irrelevant ✓

5

Back to $\Gamma_k(A_n^{n^{1/8}})$, $k = o(n)$

$\bar{g} = (g_1 \dots g_k) \in \Gamma_k$

$g_1 = (\sigma_1, \sigma_2 \dots \sigma_m)$, $m = n^{1/8}$

$\sigma_i \leftarrow$ iid, $\sigma_i \in A_n$ unif vs. near-uniform

---

Fix $n = p \leftarrow$ prime. $x \leftarrow (g_1)^p$.

$$\begin{cases} P(\sigma_i^p = 1) = \frac{1}{p} \quad \forall \sigma_i \leftarrow \text{unif.} \\ P(\sigma_i^p = 1) = \frac{1}{p} + \frac{1}{p^k} + O\left(\frac{1}{p^{2k-1}}\right) \leftarrow Q_k \end{cases}$$

/no fp's is slightly more likely than not/

We now need to construct a clever word which would distinguish two possibilities.

Th (Ajtai, 1983)

Such words / formulas always exist / monotone formula of poly length /

6

Bias amplification

Ex $X_i \leftarrow \begin{cases} 1 & w/\ P = 2/3 \\ 0 & w/\ P = 1/3 \end{cases}$ $\qquad X_i' \leftarrow \begin{cases} 0 & w/\ P = 2/3 \\ 1 & w/\ P = 1/3 \end{cases}$

$$\left.\begin{aligned} (X_1 \vee X_2) \wedge (X_3 \vee X_3) &= \left(\frac{8}{9}\right)^2 = \frac{64}{81} \\ (X_1' \vee X_2') \wedge (X_3' \vee X_4') &= \left(\frac{4}{9}\right)^2 = \frac{16}{81} \end{aligned}\right\} \quad (2:1) \text{ ratio} \Rightarrow (4:1) \text{ ratio}$$

$X_i \leftarrow \begin{cases} 1 & w/\ P = q \\ 0 & w/\ P = 1-q \end{cases}$ $\qquad X_i' \leftarrow \begin{cases} 1 & w/\ P = q' \\ 0 & w/\ P = 1-q' \end{cases}$

Ajtai: $\exists$ Formula of length $\mathrm{poly}\log\frac{1}{q'-q}$)

s.t. $\begin{cases} \text{Formula}(X_i) = 1 \text{ whp} \\ \text{Formula}(X_i') = 0 \text{ whp.} \end{cases}$

$\boxed{\text{Exploitation in HR terms}}$

7

L23 PRA **Mixes in Poly Time** Igor Pak

5/20/20

Recall: $G = \langle S \rangle$ fin group, $S = \{s_1, \dots s_k\}$

$\Gamma_k(G)$ - graph on gen'g k-tuples $(g_1 \dots g_k)$

$k > d(G) \underset{\text{conj}}{\Rightarrow} \Gamma_k(G)$ conn.

PRA: Run RW on $\Gamma_k(G)$ starting w/ $(s_1 \dots s_k)$

mix time of this RW? / on conn. comp of $\Gamma_k(G) \ni s$ /

Main Th: $k = \Omega(\log|G| \log\log|G|)$

[P. FOCS'00] **then** mix $= \mathrm{Poly}(k, \log|G|)$

/ $k = \Theta(\log|G| \log\log|G|)$

$\Rightarrow$ mix $= O(\log^6|G| (\log\log|G|)^5)$

1

Embedding REO into PRA

Babai Alg

$$(s_1 \ldots s_k \; 1 \ldots 1)$$
$$\downarrow$$
$$(s_1 \ldots s_k \; * \; 1 \ldots 1)$$
$$\downarrow$$
$$\ldots$$
$$(s_1 \ldots s_k \; \underbrace{* \; * \ldots *}_{O(\log|G|)})$$

Note: works even if we start w/ $(s_1 \ldots s_k \; \underbrace{\circ \; \circ \ldots \circ}_{\text{any}})$

Cooperman–Dixon Alg — // — — // —

We want: Collection of paths $\Gamma = \{ \gamma : \bar{g} \to \bar{g}' \;\; \bar{g}, \bar{g}' \in \Gamma_k(G) \}$

s.t. $\Delta = \max |\gamma| = \text{poly}(k, \log|G|)$

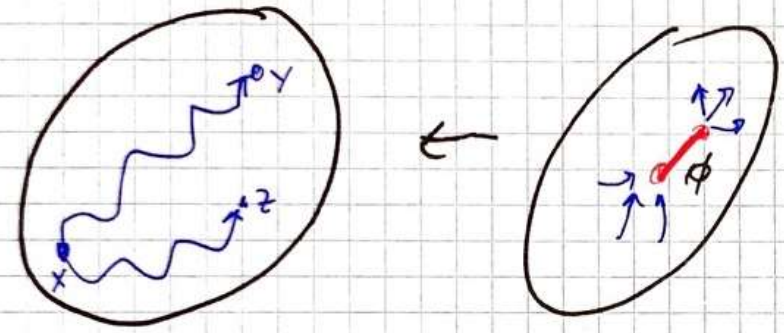
congestion through every edge $\phi = \text{poly}(k, \log|G|)$

$$\Rightarrow \text{mix} = O(\Delta^2 \phi \binom{k}{2} \underbrace{\log|\Gamma_k(G)|}_{O(k \log|G|)}).$$

②

Multicommodity flow explanation

Γ



$\Gamma = (V, E)$ ← regular graph degree d / ← $\binom{k}{2}$ 8 /

$\gamma = \{ (\gamma_{xy} : x \to y, \forall xy \in V, w_{xy}) \}$

s.t. $\sum_{\gamma} w_{xy}(\gamma) = 1 \quad \forall x, y \in V$

$$\phi = \min_{e \in E} \left[\sum_{x,y} \sum_{\gamma_{xy} \ni e} w_{xy}(\gamma) \right]$$ ← congestion through e

---

Th $\quad mix = poly(d, \phi, \log|V|)$

/ ① $O(\phi^2 d \log|V|)$, diam already in ϕ /

② $O(\Delta \phi d \log|V|)$, if extra symmetries enforce even load /

Proof ← exactly the same Dirichlet form argument

Now $\boxed{\text{No}}$ averaging over G $\quad$ $\boxed{\text{Yes}}$ weighted average over γ

③

Babai Aly $\to$ Multicomm. flow

$k > c \log_2|G|$, c - fixed, large enough.

$\Rightarrow$ every $\bar{g} \in \Gamma_k(G)$ is redundant

$\bar{g} = (\bullet \ \bullet \ s_1 \ \bullet \ s_2 \ \bullet \ \bullet \ \ldots \ \bullet \ s_\ell \ \bullet \ \bullet \ \ldots \ \bullet)$ $\qquad \ell = \log_2|G|$

$\langle s_1 \ldots s_\ell \rangle = G.$

$\bar{g}' = (\bullet \ s_1' \ s_2' \ \bullet \ \bullet \ \ldots \ \bullet \ \bullet \ \bullet \ s_\ell' \ \bullet)$

Run Babai Aly $\quad \bar{g} \to (* \ * \ s_1 \ * \ s_2 \ * \ \ldots \ *) = \bar{h}$

$\bar{g} \to (* \ s_1' \ * \ *) = \bar{h}'$

$\sigma \in S_k \qquad \bar{h} \to \sigma(\bar{h})$

If $\bar{g} \rightsquigarrow \bar{h}' = \sigma(\bar{h}) \Rightarrow \gamma : \bar{g} \to \bar{h} \to \sigma(\bar{h}) = \bar{h}' \to \bar{g}'$ ✓

Otherwise No path.

Lemma 1) $\Delta = \text{poly}(k, \log|G|) \leftarrow$ Babai th $\quad O(\log^3|G| \, k)$

2) $\phi =$ —//— //— —//— ④ Symmetry prop.

④ $\varphi_k(G) = 1 - \frac{c'}{(\log|G|)^c}$ ④

Congestion

Step t $(s_1 \ldots s_e \; * \ldots * \; \circ \; \cdot \ldots \cdot) = \bar{a}$ $\quad (g_i \leftarrow g_i \, g_j^{\pm 1}) \leftarrow R_{ij}^{t}$

Recall only combin. seq of path.

$$\left[R_{i_1 j_1}^{\varepsilon_1} \quad R_{i_2 j_2}^{\varepsilon_2} \ldots \underset{\substack{\uparrow \\ t}}{R_{i_t j_t}^{\varepsilon_t}} \; R_{i_m j_m}^{\varepsilon_m} \right]$$

m = mix time / length of Babai Alg.

$$\bar{g} \underset{t-1}{\curvearrowright} \bar{a} \underset{R_{i_t j_t}^{\varepsilon_t}}{\rightarrow} \bar{a}' \underset{m-t}{\curvearrowright} \bar{g}'$$

$\leftarrow$ part of some Babai Alg path alp

---

whp $\leftarrow \left(1 - \frac{1}{(\log |G|)^c}\right)$

$\Rightarrow$ in mix time of Babai $\quad \varepsilon = (\log |G|)^{-c}$

$\Rightarrow (\log \log |G|)$ terms in k.

$\underline{L} \Rightarrow \underline{Th}$ $\quad \blacksquare$ $\boxed{\text{Done}}$

Back to Basics

$G = \mathbb{Z}_p^m$, p - prime. $\quad d(G) = m$.

$\Gamma_m(G) \leftrightarrow GL(m, \mathbb{F}_p)$ $\quad$ det $\in$ const, $\Gamma' \in$ conn. comp w/ det $= 1$

PRA $\leftrightarrow$ RW on $SL(m, \mathbb{F}_p)$ $\quad$ w/ $R = \left\{ E_{ij} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \pm 1 \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ j \end{matrix} \right\}$

L diam $\Gamma' = O(m^2 p^2)$

$\triangleright$ $SL = \bigcup_{\sigma \in S_m} (\triangleright^0)(\sigma)(\triangleright^0)$ $\quad \square$

L' diam $\Gamma' = O(m^2 (\log p)^2)$

Exc

Th mix $\Gamma' = \text{poly}(m, \log p)$

$\triangleright$ mix $= O(\text{diam}^2 \cdot \log|\Gamma'|)$

$= O(m^4 (\log p)^2 (m^2 \log p))$

$= O(m^6 (\log p)^3)$ $\quad \square$

Better bounds??

Next time

$O(m^9 \log p)$

6

Th (D, S-C ⟷ Inventiones)
c. 1998

$$\min \Gamma_k(G) = \mathrm{poly}(k, \log G, D)$$

D = max diam of all
cayley graphs $\Gamma(G, S)$
$|S| = k$

L24 Expander graphs

Igor Pak

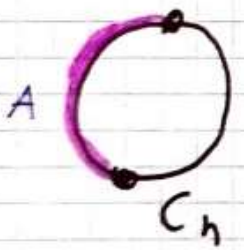
Def $G=(V,E)$ ← conn. graph, d-regular, $\varepsilon>0$

G is ε-expander if $\forall\, A\subset V$, $A\neq\emptyset$

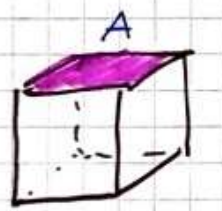
$\#E(A, V-A) \geq \varepsilon |A|$, $|A| \leq \frac{|V|}{2}$

$n=|V|$, $\{G_n\}$ ← expander if $d=\text{const}$, $\exists\, \varepsilon>0$ s.t. G_n is ε-expander $\forall n$.

Ex 1) n-cycle C_n is $\left(\frac{4}{n}\right)$-expander ← Exc



2) d-hypercube is 1-expander ← Exc



3) random 3-regular graph is $> \frac{1}{100}$-expander w.h.p. ← Exc*

← uniform

← sum of 3 random matchings

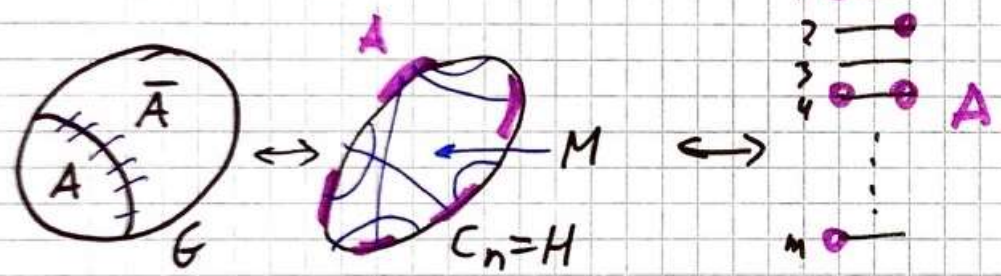
①

Th $G=(V,E) \leftarrow$ random 3-regular graph, $|V|=n=2m$

formed by $G = H \cup M$, $H = n$-cycle, $M \leftarrow$ uniform PM

then G is ε-expander whp $\varepsilon =$

D (sketch)



$|A| = k$ $\quad \mathbb{E}[\#\bullet\!-\!\!-] = 2\,\frac{k(n-k)}{n(n-1)}\,m$

$1 \le k \le m$ $\quad \geq 2\,\frac{k}{n}\,\frac{n}{2} = k$

$$P\Big[\underset{\forall A}{E(A,\bar{A}) \geq \tfrac{k}{2}}\Big] > 1 - n^{-ck}$$

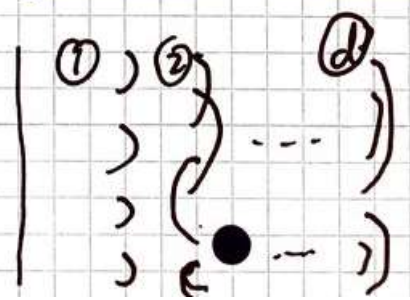
$$\Rightarrow \quad P\Big[\underset{\substack{\forall A \subset V \\ 1 \le |A| \le n/2}}{E(A,\bar{A}) \geq \tfrac{|A|}{2}}\Big] \geq 1 - \sum_{k=1}^{m} \binom{n}{k} n^{-ck} > 1-\delta > 0$$

$\boxtimes$

Motivation: [AKS] $\leftarrow$ Ajtai-Komlós-Szemerédi (1983)

Sorting network

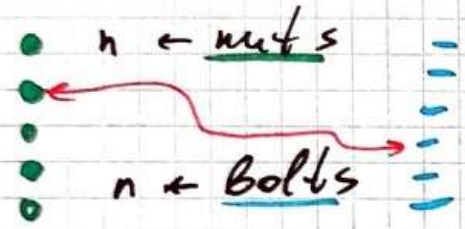
$O(n \log)$ sorting w/ depth $O(\log n)$



deterministic algorithm.

2

Nuts & Bolts [Alon-Blum-Fiat-Kannon-Naor-Ostrovsky] 1994



Random Alg

1) pick random bolt, compare w/ all nuts
2) compare matching nut w/ all bolst

split the problem into 2 roughly $\frac{n}{2}$ size

cost $O(n \log n) \leftarrow f(n) = 2n + 2f(\frac{n}{2}) =$
$= 2n + 2n + 4f(\frac{n}{2}) = \dots$

Th [Alon ++]

$\exists\ O(n (\log n)^{3+\varepsilon})$ deterministic Alg

[AKS], [Alon++] required

Th [Margulis, 1973]

$\exists$ explicit construction of ε-expanders, d, ε-fixed

$n \to \infty$

Def $G=(V,E)$ has an explicit construction if $V \subseteq \{0,1\}^{\ell}$, $\ell = O(\log n)$

$\forall v_i \in V, (v_i, v_j) \overset{?}{\in} E$ in Poly($\log n$) time

3

Nuts & Bolts det Alg

1) compare all bolts w/ corr. nuts
2) delete half nuts whose rank far from $\frac{d}{2}$

Repeat until middle nut is found.
Split the problem.

Exc get $O(n(\log n)^4)$ alg.

Margulis - Gabber-Galil expanders

$G_p = (V_p, E_p)$

$V_p = \mathbb{Z}_p^2$

$d = 8$

$E_p = \{ (a,b) \leftrightarrow (a \pm 1, b), (a, b \pm 1), (a, b \pm a), (a \pm b, b) \}$

Th [M, G-G'81]

$\{ G_p = (V_p, E_p) \} \leftarrow \frac{1}{100}$-expanders.

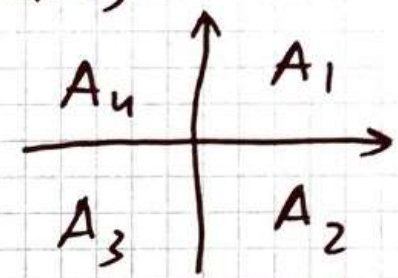
Margulis '73 ← Algebraic proof using Kazhdan (T)

Gabber-Galil ← first "elementary proof"

D $\quad S(a,b) := (a, a+b) \qquad T(a,b) := (a+b, b)$

$\underline{L}$ $\quad \forall\ A \subset \mathbb{Z}^2 \setminus O = (0,0)$

$$|E(A, \bar{A})| \geq \frac{1}{7}|A|$$



$A_1 := A \cap Q_1$
$-(0,\mathbb{Z})$
$-(\mathbb{Z},0)$
$A_0 :=$
$-A \cap -\text{"}-$

$\boxed{D\underline{L}}$ $|S(A_1)| = |T(A_1)| = |A|$ since S, T ← perm's

$S(A_1) \cap T(A_1) = \emptyset \quad \leftarrow \quad (a, a+b) = (a'+b', b') \Rightarrow b = -b'$ ×

$S(A_1), T(A_1) \subset Q_1 \Rightarrow$ at least $\frac{1}{2}$ of $E(A_1, *) \ni A$

$\Rightarrow$ <u>claim 1</u> $\quad \#E[A - A_0, \bar{A}] \geq |A - A_0| = |A| - |A_0|$

<u>claim 2</u> $\quad \#E[A_0, \bar{A}] \geq 4|A_0| - 3|A - A_0| = 7|A_0| - 3|A|$

<u>Exc</u>

<u>claim 1</u> + <u>claim 2</u> $\Rightarrow \underline{L}$ (By balancing ineq's) ☒

<u>Now</u> $\quad \mathbb{Z}^2 \to \mathbb{Z}_p$ is difficult but routine ☒

5

<u>Th</u> (Margulis '73) $\forall k$

Cayley $(G_p, R_p) \leftarrow$ expander

$G_p = SL(k, \mathbb{F}_p)$, $R_p = \left\{ \begin{pmatrix} 1 & & \pm 1 \\ & 1 & \\ & & 1 \\ & & & \ddots \end{pmatrix}_{k \times k} \right\}$

G-G $\Leftarrow$ Margulis $k = 3$

$\left(SL(3,p)\right) \begin{pmatrix} a \\ b \\ c \end{pmatrix} \leftarrow$ exp , $\oplus$ proj onto (a,b) , $\underline{c=1}$

<u>Cor</u> $\Gamma_k(\mathbb{Z}_p^k)$ are expanders $\forall k$

$\Rightarrow$ mix time of PRA on $\Gamma_k(\mathbb{Z}_p^k)$

$= c_k (\log p)$

<u>vs</u> $O(k^6 (\log p)^3)$ lost time.

<u>Th</u> [P-Zuk $\oplus$ Kossobov]

mix $= O(k^3 \log p)$

6

Next week:

Cor/Th [Kaluba-Kielak-Nowak-Ozawa '17 + '18]

$\forall k$ PRA mixes on $\Gamma_k(G)$ $\forall k \geq 5$

in $O_k(\log|G|)$ time.

Real Th $\Gamma_k(G)$ are ε_k-expanders $\forall k \geq 5$

/ Conjecture Lubotzky-P '01 /

Note: 1) every conn. comp. of $\Gamma_k(G)$

2) proof ← computer-assisted

7

L25
5/27/2020

Expanders & PRA

Igor Pak

Last time: $\Gamma = (V, E)$ ← d-regular graph, $|V| = n$

$$\phi(\Gamma) := \min_{\substack{X \subset V \\ 1 \le |X| \le \frac{n}{2}}} \frac{E(X, \overline{X})}{d\,|X|}$$ /edge expansion conductance/

Γ ← ε-expander if $\phi(\Gamma) > \varepsilon$, $\varepsilon > 0$ fixed

d - fixed, $n \to \infty$

Th [Kaluba et al. '17, '18]

$\forall\, k \geq 5\ \exists\, \varepsilon = \varepsilon(k)$ s.t. $\Gamma_k(G)$ are ε-expanders

/here $|G| \to \infty$, $\varepsilon(k)$ not known, $d = 4k(k-1)$ /

since $\Gamma_k(G)$ can be disconn, $\forall$ conn. comp -||-

Today: I will explain what's going on

Cheeger inequality

$\Gamma = (V, E)$ ← d-regular graph (conn)

$M_\Gamma := (m_{vw})$, $m_{vw} = \begin{cases} \deg(v) & , v = w \\ -1 & , (vw) \in E \\ 0 & , \text{oth.} \end{cases}$ /Laplacian/

$1 = \lambda_0 > \lambda_1 \geq \lambda_2 \geq \ldots \geq -1$ eigenvalues of $\frac{1}{d} M_\Gamma$

P-F Th

Th $\frac{1-\lambda_1}{2} \leq \phi(\Gamma) \leq \sqrt{2(1-\lambda_1)}$

/Alon, Alon-Milman, Jerrum-Sinclair, Lawler, Cheeger, ... /

Cor $\text{mix} = O\left(\log n \cdot \frac{1}{1-\lambda_1}\right) = \boxed{O\left(\frac{1}{\phi(\Gamma)^2} \log n\right)}$

relaxation time

compare with P-SC Bound $\text{mix} = \boxed{O(\Delta^2 |S| \log |G|)}$

2

Proof of Cheeger ineq (sketch)

① $\frac{1-\lambda_1}{2} \le \phi(\Gamma)$

Idea: take bad X
$\Rightarrow$ construct small $(1-\lambda_1)$ eig.

---

② $\phi(\Gamma) < \sqrt{2(1-\lambda_1)}$

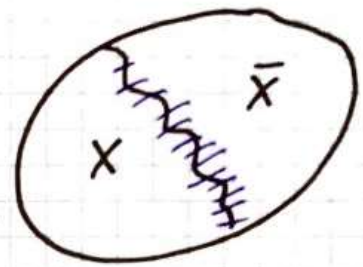
Idea: take bad eig. f
$\Rightarrow$ construct bad X

Moral: $\lambda_1(\Gamma) < 1-\varepsilon$
and $\phi(\Gamma) > \varepsilon$
are equivalen def's of expanders

Take $f \in \mathbb{R}[\Gamma]$

$f(v) = \frac{|X|}{n}, \; v \in X$

$f(v) = -\frac{n-|X|}{n}, \; v \notin X$



$E(X, \bar{X})$ = small

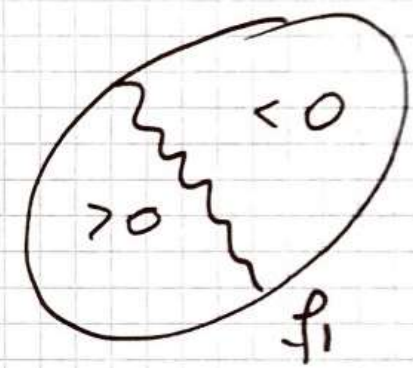
Note $\langle f, 1 \rangle = 0$

compute $\langle \frac{1}{d} M_\Gamma \cdot f, f \rangle = 1 - \text{small}$

use max principle. $1 - \text{small} < \lambda_1$

Take $f_1 \in \mathbb{R}[\Gamma]$
corr to eig. λ_1

Let $X := \left\{ \begin{matrix} v \in V \\ f_1(v) > 0 \end{matrix} \right\}$



Estimate $E[X, \bar{X}]$
using CS ineq.

Exc finish those proofs(!)

Last time: explicit construction (Margulis-Gaber-Galil)

CS implications

L ← log-space
SL ← sym log-space (undirected s-t conn ← complete)
NL ← nondet sym log-space (directed —//—)

Easy: $L \underset{①}{\subseteq} SL \underset{②}{\subseteq} NL$

① make graph out of state space
② cover time = poly(n)

Conj $NL \neq L$

Th [Reingold '04] $L = SL$

/ ⟺ one can create universal traversing sequence of length poly(n) /

Proof idea: ① turn any $\Gamma = (V, E)$ into expander by powering
② find UTS for expanders

• [Hoory-Wigderson '93]

Back to M-G-G graphs

Last time: we sketched why they are expanders after G-G. What did Margulis do?

Def [Kazhdan's Property (T)]

$G = \langle S \rangle$ ← fin. or inf. group

G has (T) if $\forall\ \pi : G \to U(V)$ unitary rep, V ← Hilbert space

w/ $\varepsilon = \varepsilon(S)$ $\quad \forall\ v \in V$, $\|v\| = 1$

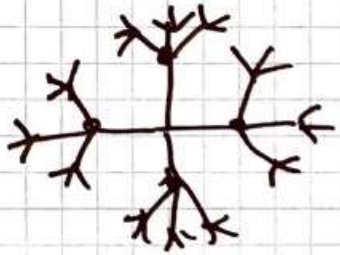
$\forall\ s \in S$ $\quad \|\pi(s)v - v\| > \varepsilon$

Ex ① G - finite $\quad (1 - \lambda_1) \geq \dfrac{\varepsilon(S)}{2|S|}$ ← Exc

---

② $G = F_2$ does NOT have (T) ← Exc

Hint: Take $V = L^2(F_2)$



5

More examples of (T) and NOT-(T)

(3) Th [Kazhdan '67] $\forall k \geq 3$ ← NOT Exc
$SL(k, \mathbb{Z})$ has (T) /uses structural prop./

---

(4) Cor [Margulis '73] $\forall k \geq 3$ $R = \{ E_{ij}(\pm 1) = \begin{pmatrix} 1 & & \pm 1 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \}$
$SL(k, \mathbb{Z}/p\mathbb{Z}) = SL(k, \mathbb{F}_p)$ has (T)
with same $\varepsilon(k)$ ← indep of p!
$\Rightarrow$ Cayley & Schreier graphs of $SL(3,p)$ are ε-expanders

Exc show that construction of MGG is ε-exp.

---

(5) $SL(2, \mathbb{Z})$ does NOT have (T) ← Exc
Hint: $SL(2, \mathbb{Z})$ contains F_2 of finite index

Th $SL(2,p)$ w/ $R = \{ \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix} \}$ are expanders
/hard result based on Langlands Th/ (6)

⑥ $\mathrm{Aut}(F_k) \leftarrow$ group of Aut of F_k

<u>Th</u> [Nielsen, 1924]

$\mathrm{Aut}(F_k)$ is generated by

$$\begin{cases} R_{ij}^{\pm} : (x_1 \dots x_i \dots x_k) \to (x_1 \dots x_i x_j^{\pm 1} \dots x_k) \\ L_{ij}^{\pm} : (x_1 \dots x_i \dots x_k) \to (x_1 \dots x_j^{\pm 1} x_i \dots x_k) \end{cases}$$

classical result in <u>combin Group Theory</u>

<u>Old</u> <u>Problem</u>: $\mathrm{Aut}(F_k)$ has (T) ?

$k=2$ – NO, maps onto $SL(2,\mathbb{Z}) \in Exc$

$k=3$ – NO, maps onto F_2 [Lubotzky Grunewald]

$k=4$ – Open

$\begin{cases} k=5 & \text{– 2017 [Kaluba et al]} \\ k \geq 6 & \text{– 2018 [— ⊢]} \end{cases}$

Proof of $k \geq 5$ are computer assisted

⑦

Back to PRA

Observation [Lubotzky-P. '01]

$\mathrm{Aut}(F_k)$ has (T) for $k \Rightarrow \Gamma_k(G)$ are exp.

w/ some $\varepsilon = \varepsilon(k)$ $\quad / \Rightarrow \mathrm{mix} \doteq O(\varepsilon^{-2} \log |G| \cdot k)$

Th [L-P] Aut (Free Nilp on k-gen of ~~index~~ class ℓ)

has (T)

$\Rightarrow \forall\, G$ - Nilp, class ℓ

$$\mathrm{mix}\ \Gamma_k(G) = O(\varepsilon^{-2}(k,\ell) \cdot \log |G| \cdot k)$$

Obs follows from viewing $\Gamma_k(G)$ as Schreier graphs of $\mathrm{Aut}(F_k)$

Question: how $\varepsilon = \varepsilon(k)$??

$\boxed{\text{Next time}}$

8

L26
5/29/2020

Igor Pak

Bounds on Kazhdan Const

Last time:

Def $G = \langle S \rangle$ has (T) w/ $\varepsilon = \varepsilon(G,S) > 0$ if
$\forall\, \pi : G \to U(V)$ unitary rep*, V – Hilb. space
$\forall\, v \in V$, $\|v\| = 1$
$\exists\, s \in S$ s.t. $\|\pi(s)v - v\| > \varepsilon$

* ← no invariant vectors

Th [Kazhdan, Margulis, etc.] (G,R) have (T)

1) $G = SL(k,\mathbb{Z})$, $R = \{ E_{ij}^{\pm} = \begin{pmatrix} 1 & & \\ & \ddots & \pm 1 \\ & & 1 \end{pmatrix},\ 1 \le i \ne j \le k \}$

2) $G = \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix} \simeq SL(2,\mathbb{Z}) \ltimes \mathbb{Z}^2$, $R = \left\{ \begin{pmatrix} 1 & \pm 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ \pm 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \pm 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \pm 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}$

Cor $G = SL(k, \mathbb{F}_p)$, $R = -\,''\,-$
$\text{Mix} = O_k(\log p)$

Q How does const depend on k?

Bounded generation

Th [Carter-Keler, 1983] $\underline{k \geq 3}$

$G = SL(k, \mathbb{Z})$, $R = \{E_{ij}\}$

$\forall g \in G \quad \exists \; g = E_{i_1 j_1}^{a_1} E_{i_2 j_2}^{a_2} \cdots E_{i_\ell j_\ell}^{a_\ell}$

where $a_i \in \mathbb{Z}$, $\ell \leq \frac{3n^2 - n}{2} + 36$

Exc False for $SL(2, \mathbb{Z})$

Proof $\leftarrow$ elementary modulo Dirichlet thm ($\forall$ arithm. progr. $\exists$ primes ...)

Th $G = SL(k, \mathbb{Z}/p\mathbb{Z})$, $R = \{E_{ij}\}$

— // — $\ell = O(k^2)$

} all we want for now

$\triangleright$ $G = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & 1 & \\ * & & & 1 \end{pmatrix} \begin{pmatrix} \sigma \in S_k \end{pmatrix} \begin{pmatrix} 1 & & & * \\ & 1 & & \\ & & 1 & \\ 0 & & & 1 \end{pmatrix}$

Recall ① diam $U(k, \mathbb{Z}/p\mathbb{Z})$ wrt R $= O(k^2)$ ✓

② diam S_k in $\{(ij)\} = O(k)$ ✓

③ $\left(\begin{array}{cc|c} 0 & 1 & \\ -1 & 0 & 0 \\ \hline & 0 & 1 \end{array}\right)$ = const dist in R $\forall k \geq 3$

Exc Hint: check $k=3$ ∎

②

Th [Shalom, 1999]

$G = SL(k, \mathbb{Z})$, $R = \{E_{ij}\}$ has (T)

w/ $\varepsilon = \varepsilon(k) > c/k^2$ for some $c > 0$

Proof idea

LO $\pi : G \to U(V)$ unitary, $V \leftarrow$ Hilb. space

suppose $\|\pi(g)v - v\| < 1 \quad \forall g \in G$

Then $\exists\, w \in V$, $w \neq 0$ invariant vector: $/\pi(g)w = w \quad \forall g \in G/$

D Let $Q := \{\pi(g)v,\ g \in G\} \subset V$

Then $Q \leftarrow$ bounded, $0 \notin Q$, $Q \leftarrow G$-invariant

$w :=$ unique pt in V s.t. $f_Q(w) = \sup\{\|w - q\| \mid q \in Q\}$ is minimized

$\Rightarrow w \neq 0$

$\Rightarrow w$ is desired invariant vector ▨

3

Proof of Shalom Th (idea, cont'd)

OBS1/L1 Every $E_{ij}^{a} \in$ some $SL(2,\mathbb{Z}) \ltimes \mathbb{Z}^2 / SL(2,\mathbb{F}_p) \ltimes \mathbb{F}_p^2$

D (for p) E_{ij}^{a} are all conjugate $\leftarrow \in$ one conjugacy class / ▨

OBS2/L2 if $\forall \|E_{ij}^{a} v - v\| < \varepsilon \Rightarrow \|gv - v\| < O(k^2)\varepsilon$

D $g = \underbrace{E_{i_1 j_1}^{a_1}}_{s_1} \underbrace{E_{i_2 j_2}^{a_2}}_{s_2} \cdots \underbrace{E_{i_\ell j_\ell}^{a_\ell}}_{s_\ell}$ By C-K Thm

$\|gv - v\| = \|s_1 s_2 \cdots s_\ell v - v\| = \leq \sum_{i=1}^{\ell} \|s_1 \ldots s_i v - s_1 \ldots s_{i-1} v\| < O(k^2)\varepsilon$ ▨

$L0 + L1 + L2 \Rightarrow \exists E_{ij}$ s.t. $\|E_{ij} v - v\| > \frac{c}{k^2}$ ▨

Last time: $(1-\lambda_1) \geq \frac{\varepsilon(G,R)^2}{2|R|} \Rightarrow 1-\lambda_1 \geq \frac{c}{2(k^2)^2 k^2} = \Omega(k^{-6})$

$\Rightarrow \mathrm{mix}(SL(k,\mathbb{F}_p), R) = O(k^6 \log |SL(k,\mathbb{F}_p)|)$

$= O(k^8 \log p)$

4

Th [P-Żuk, 2002]

$G = \langle S \rangle$ has (T) w/ Kazhdan const $\varepsilon(G,S) > 0$

Suppose S ← transitive ($\forall s, s' \in S \ \exists h \in \mathrm{Aut}(G)$ s.t $s = h(s')$)

Then $(1-\lambda_1) > \dfrac{\varepsilon(G,S)^2}{2}$

D (proof idea)

$\pi : G \to U(V)$ unitary rep

Let $\bar{\pi} : G \to U(V^N)$, $N = \#$ elts in $\Phi \subset \mathrm{Aut}(G)$ preserving S

$\pi(g)v \to (\pi \circ \phi_1(g)\, v, \dots \pi \circ \phi_N(g) v)$ $\quad \Phi = \{\phi_1 \dots \phi_N\}$

This reduces usual $(1-\lambda_1) > \dfrac{\varepsilon(G,S)^2}{2|S|}$ to [>] as desired ■

Cor $\mathrm{mix}(SL(k, \mathbb{F}_p), R) = O(\underline{k}^6 \log p)$

in place of k^8

Th [Kassabov, 2005]

$G = SL(k, \mathbb{Z})$, $R = \{E_{ij}^{\pm}\}$ has (T) w/ $\varepsilon(G,R) > \frac{1}{64\sqrt{k}+285}$
$= \Omega(\frac{1}{\sqrt{k}})$

Proof idea: combination of Sholom + G-G proof
in place of $\{E_{ij}^{a}\}$ ← (◬°), (S_k), ⊕ careful bookeping

---

Cor $\text{mix}(\underset{\substack{\uparrow \\ SL(k,\mathbb{F}_p)}}{G}, R) = O(\frac{\varepsilon(G,R)^2}{2} \log|G|) = O(k^3 \log p)$
/current best/

Exc $\varepsilon(G,R) = O(\frac{1}{\sqrt{k}})$ so Th is tight up to a const

---

Back TO PRA

Cor (from P-Z) $G = \text{Aut}(F_k)$ has (T) w/ $\varepsilon(G,\{R,L\}) = \varepsilon(k)$

$\Rightarrow$ $\text{mix}\ \Gamma_k(H) = O(\frac{1}{\varepsilon(k)^2} \log|H^k|) = O(\frac{k \log|H|}{\varepsilon(k)^2})$

6

Combinatorial approach

Conj / Near-Th [Bourgain-Gamburd, 2008]

$G = SL(2, \mathbb{F}_p)$, $G = \langle S \rangle$, $|S| \leq 4$

Then $\operatorname{diam} \operatorname{Cayley}(G, S) = O(\log p)$

Moreover — " ← expanders

w/ ε universal const

Recall

$m(G) \leq 4$

← proved for const fraction of primes

Th [Gamburd-P, 2006]

Conj $\Rightarrow$ $\Gamma_k(H)$ are expanders, $k \geq 8$, $k = O(1)$

L27
6/11/2020

PRA - Final Chapter

Igor Pak

Last time: $\left\{ \begin{array}{l} (G,S) \text{ has Kazhdan's property (T) w/} \\ \quad \varepsilon = \varepsilon(G,S) > 0 \Rightarrow \text{mix} = O(\varepsilon^{-2} \log \Gamma) \\ \text{where } \Gamma \leftarrow \text{Schreier graph}, \ S \leftarrow \text{transitive} \end{array} \right.$

$\Gamma_k(H)$ is a Schreier graph of $\mathrm{Aut}(F_k)$
$\Rightarrow$ need bounds on $\varepsilon(\mathrm{Aut}(F_k), \text{Nielsen gen's})$

Today:
- graph theory methods
- semi-definite programming

Th [Gamburd - P. + Bourgain - Gamburd]

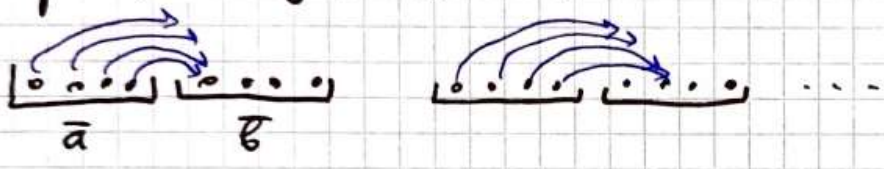
[BG]: $H = SL(2,p)$, $H = \langle S \rangle$, $|S| \leq 4 \Rightarrow \mathrm{Cayley}(H,S)$ - expander w/ $\varepsilon > 0$ universal

[GP]: $\Rightarrow \Gamma_k(H)$ - expander $\forall k \geq 8$ fixed

1

Proof of [GP] Fix $k=8$. Recall $m(H) \le 4$

Split $\Gamma_8(H)$ into union of products of Cayley graphs

$\Gamma_{\bar a}$ 

$\bar a = (h_1\, h_2\, h_3\, h_4)$

$\bar b = (h_5\, h_6\, h_7\, h_8)$

$\Gamma_{\bar a} = \mathrm{Cayley}(H, \bar a)^4$

$\Gamma'_{\bar b}$

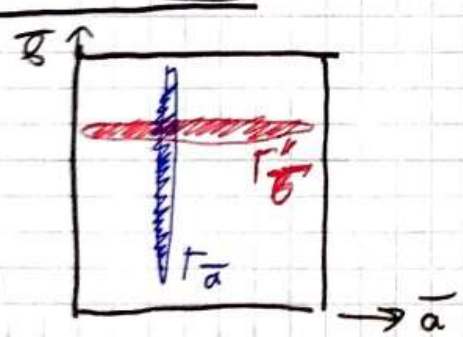
$\Gamma'_{\bar b} = \mathrm{Cayley}(H, \bar b)^4$

L1 $\langle \bar a \rangle = H \Rightarrow \Gamma_{\bar a}$ - expander.

L2 Γ, Γ' - expanders $\Rightarrow \Gamma \times \Gamma'$ - expander] $L2 \Rightarrow L1$

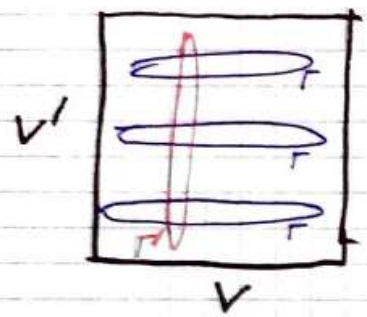
L3 $\Gamma_8 = \bigsqcup_{\bar a} \Gamma_{\bar a} \bigsqcup_{\bar b} \Gamma'_{\bar b}$, each $\Gamma_{\bar a}$ - expander
$(1-\varepsilon)$ fraction of $\Gamma'_{\bar b}$ - exp

Then Γ_8 - expander



Idea prove L2 which extends to proof of L3.

Proof of L2 $\quad \Gamma = (V, E)$, $\Gamma' = (V', E')$, $|V| = n$, $|V'| = n'$, deg $= d$



$\hat{\Gamma} := \Gamma \times \Gamma' = (V \times V', \hat{E})$

$A \subset V \times V'$, $\quad |A| < |V| \cdot |V'|/2 = \frac{nn'}{2}$

Consider $\quad A(v') = A \cap \{(*, v')\}, v' \in V'\}$

$$\hat{E}(A, \bar{A}) \geq \sum_{v'} E(A(v'), \overline{A(v')})$$

incorrect $\rightarrow$

$$\geq \sum_{v'} d\,|A(v')|\,\phi(\Gamma) = d|A|\,\phi(\Gamma)$$

Recall $\quad \phi(\Gamma) = \min\limits_{\substack{A \subset V,\, A \neq \emptyset \\ |A| \leq n/2}} \dfrac{E(A, \bar{A})}{d \cdot |A|}$ $\quad$ | Sometimes $|A(v')| > \frac{n}{2}$ (!)

Real argument: two types of $A(v')$

① $|A(v')| > \frac{3}{4} n$

② $|A(v')| \leq \frac{3}{4} n$

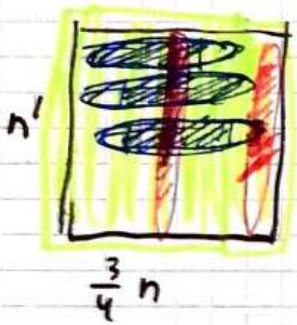
one of the types has $> \frac{|A|}{2}$

---

case ② $\quad \hat{E} \geq \frac{1}{2} \boxed{d\,\phi(\Gamma)} \frac{|A|}{2} \geq \frac{\phi(\Gamma)}{8} (2d)\,|A| \Rightarrow \phi(\hat{\Gamma}) \geq \frac{\phi(\Gamma)}{8}$

③

Case 1



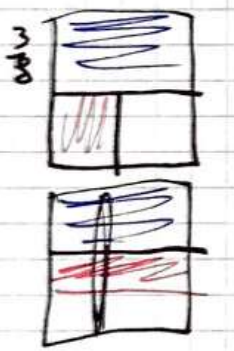
Consider now

$$A'(v) = A \cap \{(v,x)\}, \quad v \in V$$

$A(v')$ w/ $\geq \left(\frac{3}{4} n\right)$ elts take up $> \frac{|A|}{2}$ elts

we have $< \frac{|A|}{2} < \frac{n n'}{4}$ elts remain

In summary



$A'(v)$ have $\leq \frac{3}{4}|A|/n \leq \frac{3}{8} n'$

④ $\frac{1}{4} n n'$ distributed outside of $[A(v')$ w/ $\geq \frac{3}{4} n]$

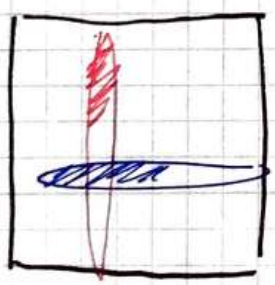
$\left(\frac{1}{4} n' n\right) / \left(5/8\, n'\right) = \frac{2}{5} n$ best case

$\left(\frac{3}{8} + \frac{1}{4}\right) n' = \frac{5}{8} n'$ worst case

$\Rightarrow$ same as case ① w/ $\frac{3}{4} \leftarrow \frac{5}{8}$ $\boxtimes$

For L3

Some idea



Key obs: ① never used row/column is a

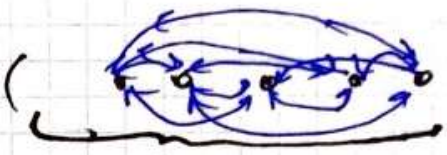
② proof robust to ignore ε-fractions of columns. $\Rightarrow$ $\boxtimes$

④

Th [Kaluba-Nowak-Ozawa '17]

$\mathrm{Aut}(F_5)$ has (T) w/ $\varepsilon > 0.18$

Cor all $\Gamma_k(H)$, $k \geq 5$ are expanders

Proof idea $\Gamma_k = \bigsqcup_{5\text{-subsets } B} \Big(\underbrace{\quad}_{k} \Big)$ 

Now apply similar argument + symmetrization.
graph theoretic

$$\Rightarrow \phi(\Gamma_k(H)) \geq \Omega\left(\frac{1}{k^2}\right)$$

$$\Rightarrow \mathrm{mix}\, \Gamma_k(H) = O(k^5 \log H) \qquad \blacksquare$$

Th [Kaluba-Kielak-Nowak '18]

$G = \mathrm{Aut}(F_k)$ has (T) w/ $\varepsilon(G, R) > \sqrt{\dfrac{1.388\,(k-2)}{6\,(k^2-k)}}$

$$= \Omega\left(\frac{1}{\sqrt{k}}\right)$$

$$\Rightarrow \mathrm{mix}\, \Gamma_k(H) = O(k^3 \log |H|) \qquad \blacksquare$$

5

Proof idea of (T) $\leftarrow$ SDP argument by Brawa '16

Th [Netzer–Thom '15]

$G = SL(3, \mathbb{Z})$ has (T) w/ $\varepsilon = \varepsilon(G, R) > \frac{1}{6}$

Cor $\min \Gamma(SL(3,p), R) = O(\log p)$ and $O(\ )$ can be computed now: $1 - \lambda_1 \geq \frac{1}{72}$ (via P-Z) improving $1/15{,}000 \leftarrow$ Burgin + PZ

Idea $G = \langle R \rangle$

Consider $\mathbb{R}[G] \leftarrow *$-algebra $(\sum c_g g)^* = \sum \bar{c}_g g^{-1}$

$R =$ usual transvections $\{E_{ij}^{\pm}\}$, $|R| = 12$

$$\Delta := 12 - \left[\sum_{M \in R} M\right] = \frac{1}{2} \sum_{M \in R} (1-M)^*(1-M)$$

Let $\mathcal{A}_\varepsilon := \Delta^2 - \varepsilon \Delta$

L1 $\varepsilon = \frac{1}{6} \Rightarrow \mathcal{A}_\varepsilon \succeq \sum_{i=1}^{n} B_i^* B_i$ for $n = 121$

L2 $\simeq \Rightarrow \geq$ ∎ 6

Making S_N into expanders

Q [Lubotzky, 1980s] $\exists ? \langle R_N \rangle = S_N$ s.t. $|R_N| = O(1)$
Cayley (S_N, R_N) are expanders

Non-example. $R = \{(12), (1 \ldots n)^{\pm 1}\}$, $\langle R \rangle = S_n$
$\Rightarrow (1 - \lambda_1) = \Theta(\frac{1}{n^2})$

Positive indication: $\exists R$ s.t. diam $= O(n \log n)$
/ we proved long ago /

Prop [Lubotzky-P.'07] $\mathrm{Aut}(F_k)$ has (T) some k
$\Rightarrow \{S_N\}$ can be made into expanders
w/ $|R_N| \leq 4k(k-1)$

Proof $H \leftarrow$ simple group, e.g. $PSL(2,p)$, $A_n, n \geq 5 \ldots$
$G := H^m$, where $m = |H|^k \varphi_k(H)$ / as in Hall thm /
$\Gamma := \Gamma_k(H^m)$. Gilman thm says $\mathrm{Aut}(F_k)$ acts as S_m
/ $k = 5$ we have $4 \cdot 5 \cdot 4 = 80$ generators /

7

Prop + th [Kalu Ba +] $\Rightarrow$ S_N can be made into expanders

---

th [Kassabov, '07]

$N = (2^{3k}-1)^6$, S_N —"— w/ $|R| < 156$

Proof uses: $\begin{cases} S_n\text{-character estimates} \\ \text{Kazhdan const for } SL(3k, \mathbb{F}_2) \\ \text{random walk estimates.} \end{cases}$

vs. $\begin{cases} \text{Gilman's proof is algebraic} \\ \text{+ th [Kalu Ba +] computational.} \end{cases}$

L28
6/3/2020

Deciding finiteness

Igor Pak

Problem: $G = GL(k, \mathbb{Z})$, $H = \langle S \rangle$, $S = \{s_1, \dots s_k\} \subset G$

Is H - infinite or finite?

Th [Babai - Beals - Rockmore, 1993]

Finiteness problem is in ZPP

Proof idea: construct two algorithms

Alg1: Probab (Monte Carlo) testing in expected poly time s.t. Yes ← True
No ← w/ Prob $> 1-\varepsilon$

Alg2: Same but Yes ← w/ Prob $> 1-\varepsilon$
No ← True

Now: Run Alg1 & Alg2 in parallel. ∎ (1)

Norms of matrices

Th! [Minkowski, Burnside + Feit]

$H \subset GL(n, \mathbb{Z})$ finite $\Rightarrow$ $|H| \le (2n)!$ [Burnside, Minkowski]
u/o CFSG

$\Rightarrow$ $|H| \le 2^n n!$, $n \geq 10$ [Feit 1996]
using CFSG

L [BBR] $H \subset GL(n, \mathbb{Z})$ finite

$M := \max\{\|s_i\|, i = 1..k\}$

then $\|h\| \le M^{n^2} e^{O(n^2 \log n)}$ / $\leftarrow n^{2n^2+3}$ more precise

---

Alg! Use Babai or Cooperman-Dixon Alg to obtain elts $h \in H$ outside of larger & larger ε-R cubes.

STOP when $\|h\| > M^{n^2} n^{(2n^2+3)}$

2

Analysis of Alg 1

$s_1 \dots s_k \; h_1 \; h_2 \dots h_\ell$, $\ell = O(\log (2n)!) = O(n \log n)$

$\langle$C-D$\rangle$ $h_{i+1} = s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k} h_1^{\alpha_1} \dots h_i^{\alpha_i}$ $\alpha_j, \varepsilon_j \in \{0,1\}$ random

(Babai) $h_{i+1} =$ RW on $\{ s_1 \dots s_k \; h_1 \dots h_i \}$ for $\underset{\text{steps}}{L} = O(n \log n)^3$
$= O(n^3 \log^3 n)$

For Alg 1 $X \subset GL(n, \mathbb{Z})$, $X := \{ \|X\| \le M^{n^2} n^{2n^2+3} \}$

$|X| = O\left((M^{n^2} n^{2n^2+3})^{n^2} \right) = O(M^{n^4} n^{2n^4+3n^2})$

$\ell \leftarrow O(\log |X|) = O(n^4 (\underbrace{\log M}_{\text{input}} + \log n))$

$L \leftarrow \ell^3$

$C_\ell^{-1} C_\ell \neq H$

If STOP $\Rightarrow$ $h_\ell \notin X \Rightarrow_L$ H inf.

If NOT $\Rightarrow$ $H \subset X$ uhp. $\boxtimes$

3

Invariant Matrices

Th [Burnside] $H \subset GL(n, \mathbb{Z})$ is finite

if and only if $\exists B \subset Mat(n, \mathbb{R})$ s.t.

B - positive definite, symmetric $B^T = B$

and $h^T B h = B \quad \forall h \in H$

Exc $\Rightarrow$ follows from $B := \frac{1}{|H|} \sum_{h \in H} h^T h$

Alg2 [Use REO (Babai, C-D or PRA) to obtain ε-uniform $h \in H$.

Do this ℓ times to obtain $h_1 \ldots h_\ell$

For $i = 1 \ldots \ell$

$B_{i+1} \leftarrow \frac{1}{2}\left[h_i^T B_i h_i + B_i\right]$

$B_0 \leftarrow I$

$\ell = poly(n)$

STOP if $B \approx$ Burnside matrix

4

Analysis of Alg2

$$B_\ell = \sum_{\bar{\alpha}=(\alpha_1 \dots \alpha_\ell)} (h^T h)\frac{1}{2^\ell}, \quad h = h_1^{\alpha_1} \dots h_\ell^{\alpha_\ell}$$

$\alpha_i \in \{0,1\}$ uniform

$$= \mathbb{E}[h^T h]$$

By ε-R Thm $\forall h_i \leftarrow \varepsilon$-unif, $\ell > 2\log|H| + \log\frac{1}{\varepsilon} + 2\log\frac{1}{\delta} + \log\frac{1}{\gamma}$

$$\boxed{\operatorname{sep}(B_\ell, B) < \gamma \text{ w/ } Pr > 1-\delta}$$

where $B = \sum_{h \in H} h^T h / |H|$

Take $\gamma \le \frac{1}{2(2n)!}$ / to be precise $\frac{1}{2n M^2 (2n)!}$ /

so the rounding over $\mathbb{Z}$ gives exact B, note: $\log(\frac{1}{\gamma}) = \text{poly}(n \log M)$

Testing $B_\ell \stackrel{?}{=} B$: check $s_i^T B s_i = B \quad \forall i = 1 \dots k$.

$\Rightarrow h^T B h = B \quad \forall h \in H$ ▨

(5)

Putting Alg1 + Alg2 together

Fix $\varepsilon = \frac{1}{2}$. After poly$(n + \log M)$ we have:

$$\begin{cases} \text{If } |H| < \infty & \text{Alg2 stops w/ } Pr > 1-\varepsilon \\ \quad\;\; |H| = \infty & \text{Alg1 stops w/ } Pr > 1-\varepsilon \end{cases} \Bigg\} \text{ proves result}$$

outputs inf/fin certificates

Repeat $O(1)$ times. Done.

Generalizations: [BBR]

1) $G = GL(n, \mathbb{Q})$, $GL(n, F)$, $F \leftarrow$ algebraic number field

2) deterministic alg using ellipsoid method

Q: Why is this astonishing?

A: Many problems for inf groups are undecidable

Th [Adian-Rabin, 1955, 1958] $G := \langle x_1 \ldots x_n \rangle / R$

$G \simeq 1$, G-fin, $G \simeq F_2$, ... $\leftarrow$ all undecidable.

6

Th [Mihailova, 1958] $n \geq 4$

$G = SL(n, \mathbb{Z})$, $H = \langle S \rangle$, $S = \{s_1, \dots s_k\}$, $g \in G$

Then $g \in ? H$ is undecidable

L $M_1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $M_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, $M_1, M_2 \in SL(2, \mathbb{Z})$

Then $\langle M_1^{\pm 1}, M_2^{\pm 1} \rangle = F_2$ / Sanov subgroup /

Exc $\langle M_1^{\pm 1}, M_2^{\pm 1} \rangle$ is a subgroup of $SL(2, \mathbb{Z})$ of index 12

Proof idea of L: $X = \mathbb{Z}^2$, $\mathcal{A} = \{(p, q) \in \mathbb{Z}^2 \mid |p| > |q|\}$

$\mathcal{B} = \{(p, q) \in \mathbb{Z}^2, |q| > |p|\}$

Check that $\boxed{M_2^n \mathcal{A} \in \mathcal{B}, \ M_1^n \mathcal{B} \in \mathcal{A}}$

$\Rightarrow$ result follows by ping-pong lemma

$\blacksquare$

Proof idea of Mihailova Thm $\quad n=4$

$\left(\begin{array}{c|c} F_2 & 0 \\ \hline 0 & F_2 \end{array}\right) \subset SL(4, \mathbb{Z})$ $\quad$ Consider $S_i = \left(\begin{array}{c|c} u_i & 0 \\ \hline 0 & v_i \end{array}\right)$ $\quad u_i, v_i \in F_2$, $i = 1..k$

$$\text{word}(S_1 .. S_k) = \text{word}(u_1 .. u_k) * \text{word}(v_1 .. v_k)$$

Th [PCP = Post correspondence problem, E. Post '46]

$\alpha_1 \dots \alpha_N$ $\leftarrow$ words over $X = \{x_1 .. x_k\}$
$\beta_1 .. \beta_N$

Then $\exists ?$ word $\in$ alphabet $\{y_1 .. y_N\}$ s.t. $\text{word}(\alpha_1 .. \alpha_N) = \text{word}(\beta_1 .. \beta_N)$ is undecidable

---

Exc Prove PCP Thm via reduction to halting problem

D(Mih) idea $\quad$ take any $x_1 .. x_k \in F_2$, $u_i \leftarrow \alpha_i$, $v_i \leftarrow \beta_i$

include in S extra "parity" gen's.

Exc $\quad$ Take $y = \begin{pmatrix} x_1^2 & \\ & x_1^2 \end{pmatrix}$

$\blacksquare$ $\quad$ 8

L29
6/5/2020

Swan Song

Igor Pak

Before: Random sampling from
- groups (Cayley graphs)
- homogeneus spaces (Schreier graphs)

Idea: use RW w/ group generators
repeatedly add/modify gen's if
necessary (Babai, C-D, PRA)

Today: Random sampling from orbits
of a particular group action

Examples:
1) k-subsets of $\{1..n\}$ ← homog. space
$\leftrightarrow S_n / S_k \times S_{n-k}$, can use S_n RW
2) $\Gamma_k(G)$ ← generating k-tuples of G ← hom. space
$\leftrightarrow \mathrm{Aut}(F_k)/(\text{Aut of } G)$, can use $\mathrm{Aut}(F_k)$ RW
3) partitions $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_\ell > 0$ ← orbits of S_n ①

More precisely, let $S(n,k)$ = set of <u>unordered</u> k-tuples of subsets $(X_1 \dots X_k)$

$$\bigcup_{i=1}^{k} X_i = \{1 \dots n\}, \quad X_i \cap X_j = \emptyset, \quad X_i \neq \emptyset$$

<u>Ex</u> $|S(4,2)| = 7$, $n=4, k=2$

1234, 1342, 1243, 2343, 1234, 1324, 1423

<u>Exc</u> - $|S(n,k)|$ = Stirling #'s second kind

- $A \in S(n,k)$ can be sampled in poly time.

<u>Observe</u>: partitions $\lambda_1 \geq \dots \geq \lambda_k$ are orbits of S_n acting on $S(n,k)$ / $\lambda_1 + \dots + \lambda_k = n$ /

<u>General</u> <u>Problem</u>

count, approximately count, sample from the set of orbits

<u>Exc</u> For $k \leq n$, $\lambda_1 \geq \dots \geq \lambda_k$ compute #/sample in poly-time.

2

Burnside Processes

$G = \langle S \rangle$ finite group, $S = \{s_1 .. s_k\}$

G acts on X $\leftarrow$ $\forall i \ \exists \sigma_i \in S_X$ $i = 1..k$

s.t. $\varphi : G \to S_X$ is homom.

$\varphi(s_i) = \sigma_i$

Problem $\#X^G :=$ # orbits of G acting on X $\leftarrow$??

BP [Jerrum'93] step $X \to Y$

1) Choose unif. random $g \in St_G(x) := \{g \in G : g \cdot x = x\}$
2) — // — $Y \in Fix(g) := \{Y \in X : gY = Y\}$

Th/Obs [Jerrum]

BP is ergodic w/ stat dist $\propto \frac{1}{\#X^G}$

D 1) $X \to 1 \to Y$ $\forall Y \in X$ w/ some (small) prob.

2) stat dist ~~deg~~ $(x) = |St_G(x)| = |G| / |Gx|$ $\leftarrow$ size of the orbit ■ (3)

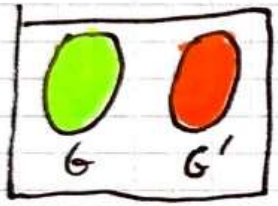
at X

Exc Formulate BP on partitions
Prove that it works in poly-time.

Warning: Even when $G = S_n$ step 1) can be hard

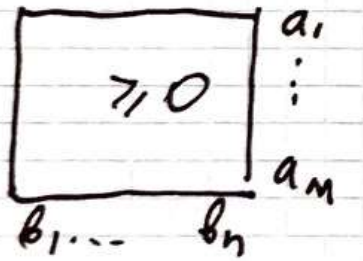
Ex $a_n :=$ # non-isom. graphs $=$ # orbits of S_n on all graphs on n vert.

Then $\#St_{S_n}(G)$, $G \subset K_n$ is as hard as graph-isom.



$\leftarrow \exists ?\ \sigma \in St_{S_{2n}}(G \sqcup G')$ which swaps $G \leftrightarrow G'$

Main example: Contingency tables

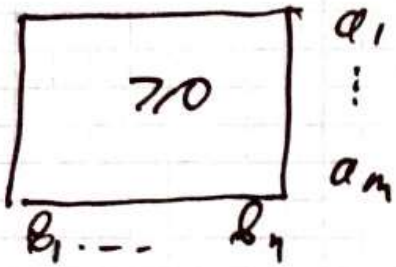


$$CT(\bar{a}, \bar{b}) = \{(x_{ij}),\ x_{ij} \geq 0 \text{ s.t. } \sum_j x_{ij} = a_i,\ \sum_i x_{ij} = b_j\}$$

Q: Compute / estimate / sample from $CT(\bar{a}, \bar{b})$

4

CT's are orbits



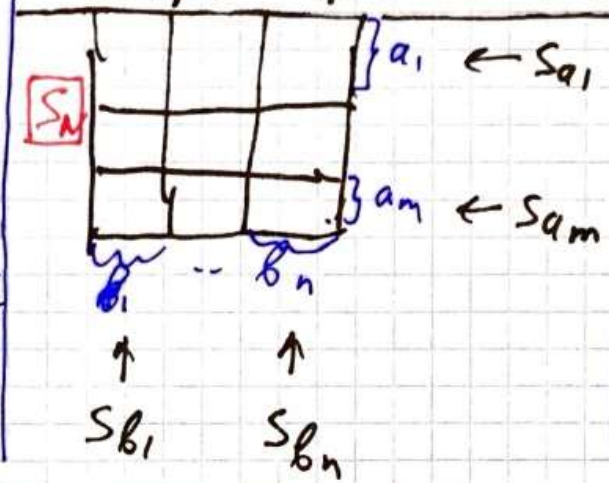
$N = a_1 + \dots + a_m$
$= b_1 + \dots + b_n$

Diaconis - Gangolli MC

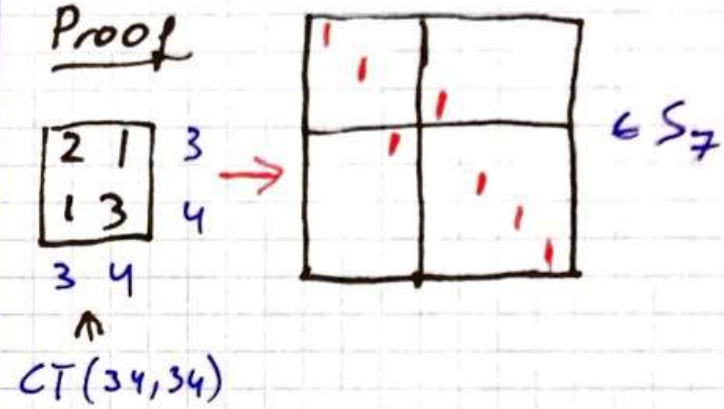
$\begin{pmatrix} \pm 1 & \mp 1 \\ \mp 1 & \pm 1 \end{pmatrix}$ if possible

Let $\Sigma := S_{a_1} \times \dots \times S_{a_m} \times S_{b_1} \times \dots \times S_{b_n}$

Prop $\#CT(\bar{a}, \bar{b}) = \#$ orbits of Σ on S_N



Proof



Theorems

1) $m, n = O(1)$ $\#CT(a,b) \leftarrow$ Barvinok '93
2) $m = \Theta(n)$, $a_{max}/a_{min}, b_{max}/b_{min} < 1.6$ [Barvinok et al '10]
3) $\min\{m,n\} = O(1)$ [Chyan-Dyer '03]
4) $a_{min}, b_{min} = \Omega(n^{2.5} \log n)$ [Dyer-Kannan-Mount '97] [Morris '02]
   $m = n$

New thm [Dittmer - P. '19]

$a_i, b_j = O(n^{1/4 - \varepsilon})$ $\#CT$ can be approx in poly time using BP
$m = \Theta(n)$

5

Final Thoughts, Results, Conjectures

1) PRA ← rw on $\Gamma_k(G)$, $mix = O(k^3 \log |G|)$

Q: lower bounds? $mix = \Omega(k \log k \log |G|)$

Can 3 be improved?

---

2) Q: Is there cutoff as $|G| \to \infty$?

Th [Peres-Tanaka-Zhai '20] yes, in TV, $k \to \infty$ $\forall G$.

/formerly Diaconis - Saloff-Coste conj '96/

---

3) Th [Lubetzky-Sly '10, '11]

1) random 3-regular graphs have cutoff

2) $\exists$ explicit construction of expanders w/ no cutoff and those w/ cutoff

---

Open Problem: Do MGG expanders have cutoff?

4) Th [Alon-Roichman 1994] $\forall$ finite G $\exists/R$ S, $\langle S\rangle = G$

$|S| = O(\log|G|)$ s.t. $1-\lambda_1 > \frac{1}{10}$, $\lambda_1 \leftarrow \mathrm{Cayley}(G,S)$

Th [P, 1999] —//— $\min \mathrm{Cayley}(G,S) = O(\log|G|)$

Th [Arvind, 2014] can be done in poly time.

---

5) Th [Radoicic-P.] $\forall G$ $\exists S$, $\langle S\rangle = G$, $|S| \le \log_2|G|$

s.t. $\mathrm{Cayley}(G,S) \leftarrow$ Hamiltonian.

Th [Lubotzky '02] $k = d(G) + O(\log\log|G|) \Rightarrow \varphi_k(G) > 1-\varepsilon$

Open $S \subset G$ random, $|S| =$ —//—//— $\Rightarrow \mathrm{Cayley}(G,S)$

is Hamiltonian w/ $P > 1-\varepsilon$

---

6) Th $\forall$ G - solvable, $k > 3.75\, d(G) \Rightarrow \varphi_k(G) > \frac{1}{4}$

[Mann '96, Lucchini-Menegazzo-Morigi '06]

Th $\exists$ G - ~~nilpotent~~ solvable which exhibits bias

[Crestani-Lucchini '15] / start w/ $G = S_4 \wr S_4 \wr S_4 \cdots \wr S_4$ / 7

Exc $d(G) = ??$

7) $G = SL(k, \mathbb{F}_p)$, $R = \{E_{ij}\}$, k - fixed

<u>Q:</u> $\exists$ explicit word proving $\mathrm{dist}(1, g) \le c \log p$

<u>Th</u> [Riley, 2005] yes, $k \geq 3$

<u>Th</u> [Larsen, 2003] almost, $k \geq 2$, $\mathrm{dist} = O(\log p \log\log p)$

<u>Th</u> [Bramberg-Shpilrain-Vdovina] #17 for of, $k = 2$

$G = SL(2, \mathbb{F}_p)$, $R = \left\{ \begin{pmatrix} 1 & \pm 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 2 & 1 \end{pmatrix} \right\}$

---

8) <u>Conj</u> BP for CT w/ $a_i, b_i = \mathrm{poly}(n)$, $m = \Theta(n)$ mixes in poly time. /extending Diffmar P/

8