L14 (4/29/2020)

# Random Random Walks

Igor Pak

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

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

$\quad\quad \overset{\shortparallel}{P}(\Gamma(G,S) \text{ is connected})$

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

$h \leftarrow g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k}$ 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** ($\mathcal{E}$-R) $k > 2 \log_2 |G| + 2 \log_2 \frac{1}{\varepsilon} + \log \frac{1}{\delta}$

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

D $\varepsilon R$ 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 $g_i$

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

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

---

$$h' := g_1^{\varepsilon_1} \cdots g_i^{\varepsilon_i} \, x \, g_{i+1}^{\varepsilon_{i+1}} \cdots g_k^{\varepsilon_k}$$
$$= x \, (x^{-1} g_1^{\varepsilon_1} x)(x^{-1} g_2^{\varepsilon_2} x) \cdots (x^{-1} g_i^{\varepsilon_i} x) \, g_{i+1}^{\varepsilon_{i+1}} \cdots g_k^{\varepsilon_k}$$
$$= x \left((g_1^x)^{\varepsilon_1}\right)\left((g_2^x)^{\varepsilon_2}\right) \cdots \left((g_i^x)^{\varepsilon_i}\right) g_{i+1}^{\varepsilon_{i+1}} \cdots g_k^{\varepsilon_k}$$
$$= x \, v_1^{\varepsilon_1} v_2^{\varepsilon_2} \cdots v_k^{\varepsilon_k}$$, where $v_i = (g_i)^x$ - unif indep

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

---

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

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

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

---

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

## Lazy R-R walk

$S = \{g_1 \ldots g_k\}$ ← $\{g_i\}$ 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
$\varepsilon \in \{0,1\}$ — " —

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

---

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

---

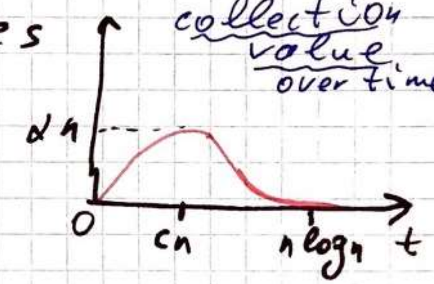
ER Thm + L ⇒ $\text{sep}(t) < \underset{\uparrow 3}{O}(\varepsilon)$ for $t = k + O(\log\frac{1}{\varepsilon})$
w/ $\Pr > 1-\varepsilon$

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

# 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. $\leftarrow \tau$

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

---

**Q2:** What's worth of your collection at time $\tau$?

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

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

/Chernoff Bound/

---

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

## Notes ~~of~~ on the result

① Th ← P. (1999)

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** $\mathrm{diam}(\Gamma) = 20$

[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]

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

**Th** [Jerrum 1984] $\quad \mathrm{diam}\ \Gamma$ = PSPACE-c

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

$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ **Th** $\mathrm{diam} = \Theta(n^2)$ [Ellenberg] 1993

Open Problem

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

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

# Two Bonus Parts

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

Th [Gates – Papadimitriu, 1979]

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

/recently improved/

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