Igor Pak

# Erdős-Rényi Theorem

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

$\Gamma_k = \Gamma(g_1 \dots g_k) \leftarrow$ 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 $\Rightarrow$ $k = (\log_2 |G|) + O\left(\log \frac{1}{\varepsilon}\right)$

$\Leftrightarrow$ Random Cayley graphs $\Gamma_k$ 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 $\Gamma_k$ have diam $\leq k$ w/ Prob $> 1-\varepsilon$

---

Note: Harder E-R Thm $2 \to 1$.

We prove original version which implies more.

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

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

/distribution of random subproducts/

---

**Th** [E-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:

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

---

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

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

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

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

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

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

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

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

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

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

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

<u>Note</u> **L1 + L2 $\Rightarrow$ ML**

---

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

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

---

<u>Indeed</u> $$\left.\begin{aligned} Q_{\bar g}(h) &= \frac{1}{2^k}\sum_{\bar\varepsilon:\,\bar g^{\bar\varepsilon}=h} 1 \\ \Rightarrow \sum_{h\in G} Q_{\bar g}(h)^2 &= \frac{1}{2^{2k}}\sum_{\bar\varepsilon,\,\bar\varepsilon':\,\bar g^{\bar\varepsilon}=\bar g^{\bar\varepsilon'}=h} 1\end{aligned}\right\}\ \forall \bar g$$

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

---

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

$(g_1\, g_3\, g_4\, g_7 \cdots)$
<u>vs</u> $(g_1\, g_3\, g_7 \cdots)$

(Proof of L2 cont'd)

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

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

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

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

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

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

$\blacksquare$

$\Rightarrow$ **ML**

# Proof of E-R Thm

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

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

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

---

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

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

---

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

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

$\square$

# Future directions

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

2. $\Gamma_k$ are *expanders*, $k = \Omega(\log|G|)$

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