Today
- Random Walk
- Hitting Set Lemma.
- Explicit Constructions

CSS. 413.1
Pseudorandomness
Lecture 10 (2021-9-23)
Instructor: Prahladh Harsha.

---

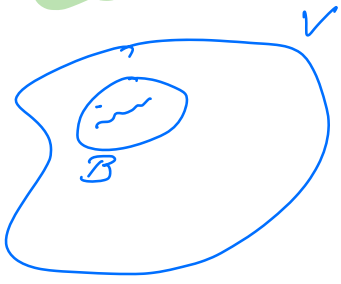
Today - Random Walk on expanders

## Hitting Set for Random walks on expanders

$G$ - expander on $N$ vertices w/ spectral gap $1-\lambda$ w/ $\lambda < 1$
where $\lambda = \max\{\lambda_2, |\lambda_n|\}$.

$M$ - corresponding RW Matrix.

$B \subseteq V$ $\quad \pi(B) = \mu$




$X_1 \ldots X_t$ - random walk of length $t$ starting from an initial vertex $X_1 \sim \pi$

Then

(*) $\ldots$ $\Pr_{X_1 \ldots X_t}\left[\bigwedge_{i \in [t]} (X_i \in B)\right] \leq \mu\left(\mu + \lambda(1-\mu)\right)^{t-1}$

Remarks:

(1) $G$ - complete graph w/ self loops

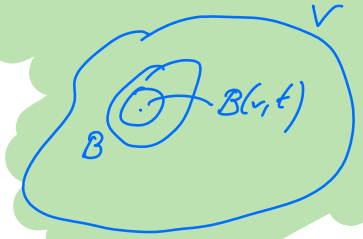
$M_{ind}$ : $\lambda = 0$ ✓

(*) $\leq \mu^t$

(2) Application to Derandomization

**Thm [Karp-Pippenger-Sipser]**

$G$ is an $N$-vertex $D$-regular $(\frac{N}{2}, A)$-vertex expander for some $A > 1$,




$B \subseteq V$, $|B| \leq |V|/2$

$\Downarrow$

$\Pr_{v \leftarrow \pi}[B(v,t) \subseteq B] \leq \frac{\mu}{A^t}$

RPS $\rightarrow$ RP error reduction

$\frac{1}{2} \rightarrow \delta$

(a). $\mu = \frac{1}{2}$ .. $\frac{\mu}{A^t} \leq \delta$ ; $t = O\left(\frac{\log(\frac{1}{\delta})}{\log A}\right)$

(b). # repetitions: $|B(v,t)| \leq (D+1)^t$

$= \text{poly}(n)$

provided $t = O(\log n)$

Concl: Reduce error $1/2 \to \frac{1}{poly(n)}$

w/o paying any additional randomness.

Qn: Can we reduce error further than say to inverse exponential (or possibly paying a few extra random bits)

YES. By Hitting Set Lemma.

RP error reduction

error : $\delta \to 1/2$

$\pi(B) = 1/2$.

$$Pr[\text{walk} \in B] \le \mu(\mu + \lambda(1-\mu))^{t-1}$$

$$= \frac{1}{2}\left(\frac{1+\lambda}{2}\right)^{t-1}$$

$$\le \left(\frac{1+\lambda}{2}\right)^{t} = c^t$$

for some $c < 1$

$t$-step.

error : $1/2 \to \exp(-t)$

# random coins $= \log N + (t-1)\log D$

$= n + O(t)$.

# iterations $= t$.

Rewriting in terms of $\delta$

error: $\frac{1}{2} \to \delta$ $\quad (\delta = \exp(-t))$

AKS: $\begin{cases} \#\text{ random coins} = n + O(\log \frac{1}{\delta}) \\ \#\text{ iterations} = O(\log \frac{1}{\delta}). \end{cases}$

kPS: $\begin{cases} \#\text{ random coins} = n \\ \#\text{ iterations} = \text{poly}(\frac{1}{\delta}) \end{cases}$

Ind. $\begin{cases} \#\text{ random coins} = O((\log \frac{1}{\delta}) \cdot n) \\ \#\text{ iterations} = O(\log(\frac{1}{\delta})). \end{cases}$

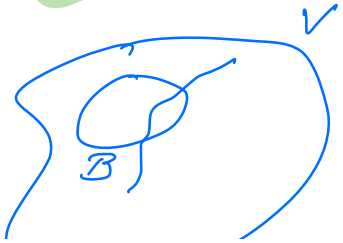
What about BPP error reduction.

Chernoff Bound for RW on expanders

$G$ - expander on $N$ - vertices w/ spectral gap $1-\lambda$ w/ $\lambda < 1$ where $\lambda = \max\{\lambda_2, |\lambda_n|\}$.

$M$ - corresponding RW Matrix.

$B \subseteq V$ $\quad \pi(B) = \mu$




$X_1 \ldots X_t$ - random walk of length $t$ starting from an initial vertex $X \sim \pi$

Then

$$\Pr_{X_1 \ldots X_t}\left[\left|\frac{\#\{i \in [t] \mid X_i \in B\}}{t} - \mu\right| > \varepsilon\right] \leq 2\exp\left(-(1-\lambda)\varepsilon^2 t\right)$$

Problem Set 2: Weaker version of Chernoff bd (using the hitting set lemma)

Proof of hitting set lemma:

$$(*) = \Pr_{X_1 \ldots X_t}\left[\bigwedge_{i \in [t]} (X_i \in B)\right]$$

$$= \sum_{v_1 \ldots v_t \in B} \Pr\left[X_1 = v_1, X_2 = v_2 \ldots X_t = v_t\right]$$

$$= \sum_{v_1 \ldots v_t \in B} \pi(v_1) M(v_1, v_2) M(v_2, v_3) \ldots M(v_{t-1}, v_t).$$

$$\mathbb{1}_B = \mathbb{1}[v \in B] \qquad B \quad V \setminus B$$

$$P = \mathrm{Diag}(\mathbb{1}_B) = \begin{array}{c} B \\ V \setminus B \end{array} \left[\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right]$$

$$(\star) = \sum_{v_1 \dots v_\ell \in V} \pi(v_1)\, P(v_1, v_1)\, M(v_1, v_2)\, P(v_2, v_2) \cdot M(v_2, v_3)\, P(v_3, v_3) \dots P(v_{\ell-1}, v_{\ell-1})\, M(v_{\ell-1}, v_\ell)\, P(v_\ell, v_\ell)$$

$$= \sum_{v \in V} \pi(v) \left(P(MP)^{\ell-1} \mathbb{1}\right)(v) \quad \text{(Moving to } \pi\text{-inner product)}$$

$$(\star) = \left\langle P(MP)^{\ell-1} \mathbb{1}, \mathbb{1} \right\rangle_\pi$$

$$= \left\langle P(MP)^{\ell-1} \mathbb{1}, \mathbb{1}_B \right\rangle_\pi \quad \text{(since } \operatorname{supp}(P(MP)^{\ell-1}\mathbb{1}) \subseteq B\text{)}$$

$$= \left\langle P(MP)^{\ell-1} \mathbb{1}_B, \mathbb{1}_B \right\rangle_\pi \quad \text{(since } P\mathbb{1} = P\mathbb{1}_B\text{)}$$

$$\leq \left\| P(MP)^{\ell-1} \mathbb{1}_B \right\|_{2,\pi} \cdot \left\| \mathbb{1}_B \right\|_{2,\pi} \quad \text{(Applying Cauchy Schwarz)}$$

$$= \left\| P(MP)^{\ell-1} \mathbb{1}_B \right\|_{2,\pi} \cdot \sqrt{\mu}.$$

$$= \left\| (PMP)^{\ell-1} \mathbb{1}_B \right\|_{2,\pi} \cdot \sqrt{\mu} \quad \text{(since } P^2 = P\text{)}$$

What is the 2-norm of $(PMP)^{\ell-1}\mathbb{1}_B$?

For a general operator $M: \mathbb{R}^v \to \mathbb{R}^v$

$$\|M\|_{2,\pi} = \max \frac{\|Mx\|_{2,\pi}}{\|x\|_{2,\pi}}$$

- largest eigenvalue of $M$.
(if one exists)

Obs: (1) $\|M_1 + M_2\| \le \|M_1\| + \|M_2\|$

(2) $\|M_1 \cdot M_2\| \le \|M_1\| \cdot \|M_2\|$

Going back to the proof

$$\|(PMP)^{t-1} x_B\|_{2,\pi} \le \|(PMP)^{t-1}\|_{2,\pi} \cdot \|x_B\|_{2,\pi}$$

(defn of $\|M\|$)

$$= \|(PMP)^{t-1}\|_{2,\pi} \cdot \sqrt{\mu}$$

$$\le \|PMP\|_{2,\pi}^{t-1} \cdot \sqrt{\mu}.$$

$$(A) \le \|PMP\|_{2,\pi}^{t-1} \cdot \mu.$$

Qn: What is $\|PMP\|_{2,\pi}$?

Suffices to show $\|PMP\|_{2,\pi}$

$\le \mu + \lambda(1-\mu)$

$= (1-\lambda)\mu + \lambda$

Warmup Case: $M$ - independent random coin.

$G$ - complete graph w/ self loops

$$M_{ind} = \begin{bmatrix} \pi \\ \pi \\ \pi \\ \pi \end{bmatrix} \qquad (pM_{ind} = \pi)$$

since $p$ - prob dist

$$= J\Pi \qquad (J \text{ is all 1's matrix})$$

$$\Pi = Diag(\pi)$$

$$PM_{ind}P = \begin{bmatrix} I & 0 \\ \hline 0 & 0 \end{bmatrix}_{B} \begin{bmatrix} \pi \\ \pi \\ \pi \\ \pi \end{bmatrix} = \begin{bmatrix} I & 0 \\ \hline 0 & 0 \end{bmatrix}_{B}$$

$$= \begin{bmatrix} \pi_B & 0 \\ \pi_B & \\ \pi_B & \\ \hline 0 & 0 \end{bmatrix}_{B}$$

Rank 1 matrix $\quad PM_{ind}P \cdot \mathbb{1}_B = \pi(B) \cdot \mathbb{1}_B$

$\mathbb{1}_B$ is the e-vector for $PM_{ind}P$ w/ evalue $\pi(B) = \mu$.

$$\| PM_{ind}P \|_{2,\pi} = \mu.$$

What we want is $\|PMP\|_{2,\pi}$

Const $\|PM_{ind}P\|_{2,\pi}$

Idea: Write $M$ as a combination of $M_{ind}$ & error matrix

$M$: $v_1 = \mathbb{1} \longrightarrow \mathbb{1}$

$v_2 \longrightarrow \lambda_2 v_2$

$v_3 \longrightarrow \lambda_3 v_3$

$\vdots$

$v_n \longrightarrow \lambda_n v_n.$

$M_{ind}$: $v_1 \longrightarrow v_1$

$v_2 \longrightarrow 0$

$\vdots$

$v_n \longrightarrow 0$

$M_E$: $v_1 \longrightarrow \lambda v_1$

$v_2 \longrightarrow \lambda_2 v_2$

$v_3 \longrightarrow \lambda_3 v_3$

$v_n \longrightarrow \lambda_n v_n.$

$$M = (1-\lambda) M_{ind} + M_E$$

Matrix Decomposition of RV matrix

$\|M_E\|_{2,\pi}$: $x \longmapsto M_E x.$

$x = \sum \alpha_i v_i$ $\qquad \|x\|_{2,\pi}^2 = \sum \alpha_i^2.$

$$M_E x = \alpha_1 \lambda v_1 + \sum_{i=2}^{n} \alpha_i \lambda_i v_i.$$

$$\|M_E x\|_{2,\pi}^2 = \alpha_1^2 \lambda^2 + \sum_{i=2}^{n} \alpha_i \lambda_i^2 \le \lambda^2 \left(\sum \alpha_i^2\right)$$
$$= \lambda^2 \|x\|_{2,\pi}$$

Hence $\|M_E x\|_{2,\pi} \le \lambda$

Conclusion: $M$ is a s.c.w matrix w/ spectral $1-\lambda$ then

$$M = (1-\lambda) M_{ind} + M_E$$

where $\|M_E\| \le \lambda$

$$\|PMP\|_{2,\pi} = \|P((1-\lambda)M_{ind} + M_E)P\|_{2,\pi}$$
$$\le (1-\lambda)\|PM_{ind}P\|_{2,\pi} + \|PM_EP\|_{2,\pi}$$
$$= (1-\lambda)\mu + \|PM_EP\|_{2,\pi}$$
$$\le (1-\lambda)\mu + \|P\| \cdot \|M_E\| \cdot \|P\|$$
$$\le (1-\lambda)\mu + \|M_E\| \quad (\text{since } \|P\| \le 1)$$
$$\le (1-\lambda)\mu + \lambda$$

$$(*) \le \|PMP\|^{t-1} \cdot \mu$$
$$= (\lambda + (1-\lambda)\mu)^{t-1} \cdot \mu$$
$$= (\mu + \lambda(1-\mu))^{t-1} \mu .$$

∎

# Explicit Constructions of Expander Graphs

explicit : poly(N) ( mildly explicit)

super-explicit: Given $v \in [N]$, $c \in [D]$
can calculate the $i$-th nbr of $v$ in time poly(log N, log D).
(fully explicit).

Algebraic Constructions of explicit expander graphs.

(1) $m$ - +ve integer

$V = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$\left\{ (x,y) \;\middle|\; \begin{matrix} x \\ y \end{matrix} \in \{0, \ldots m-1\} \right\}$

$(x,y) \longrightarrow (x,y), (x+1,y), (x,y+1), (x, x+y), (-y,x)$

$(x-1,y), (x,y-1), (x,y-x), (y,-x)$

8- regular.

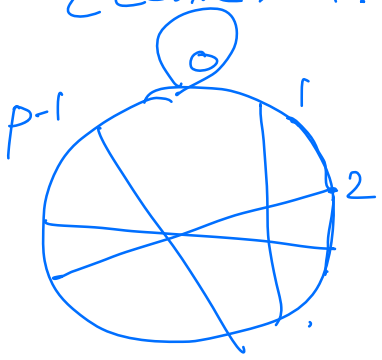
Margulis: $\exists\ \lambda < 1$, s.t. $\forall\ m$, the above graph is $(1-\lambda)$-spectral expander

(2) $V = \mathbb{F}_p$ $\quad$ $p$ - prime

3-regular graph.

$x \longrightarrow x+1,\ x-1,\ 1/x$

(Convention: $1/0 = 0$)




$\frac{3}{16}$ - Selberg Theorem:

$\exists \lambda,\ \lambda < 1$ for $p$.

this graph is a $(1-\lambda)$-spectral expander.

(3) Lubotzky - Phillips - Sarnak.

$p$ - prime $\quad p \equiv 1 \pmod 4$

$q$ - prime power $\quad q \neq p$ $\quad q$ - square $(\bmod p)$

$\exists i \in \mathbb{F}_q,\ i^2 + 1 = 0.$

$A = \{(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4 \mid a_0$ - odd positive, $a_1, a_2, a_3$ - even, $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p\}$.

$|A| = p+1 = D$ (degree)

Graph on $\mathbb{F}_q \cup \{\infty\}$ (ie $N = q+1$)
which is $(A$-regular.

$(a_0, a_1, a_2, a_3)$-th nbr of $z \in \mathbb{F}_q \cup \{\infty\}$

$$\frac{(a_0 + ia_1)z + (a_2 + ia_3)}{(-a_2 + ia_3)z + (a_0 - ia_1)}$$

**Thm [LPS]**: $\forall$ prime powers $q$.
[Margenstern] $G_q$ has spectral gap $1-\lambda$ where $\lambda = \frac{2\sqrt{p}}{p+1}$

$= \frac{2\sqrt{D-1}}{D}$

[Ramanujan Graphs]