upper bound on p_m for a fixed m:-

$S \subseteq L \qquad |S| = m$

let $v_1, v_2, \dots v_{mD} \rightarrow$ be the nbrs of $S \rightarrow \underline{\underline{N(S)}}$ — there could be repetitions in these

We say; v_i : is a repeat if $v_i \in \{v_1, \dots v_{i-1}\}$

$\Pr[v_i \text{ is a repeat}] \leq \left(\frac{i-1}{N}\right) \rightarrow$ as we ~~get max~~ can choose among at max $(i-1)$ previously occurred vertices out of N if we want v_i to be a repeat

$\leq \frac{mD}{N}$ $\rightarrow$ $\forall\, i$ this holds (Although very loose bound)

$\Pr[\, |N(S)| \leq (D-2)m \,]$

$= \Pr[\, \exists \text{ atleast } 2m \text{ repeats among } v_1, v_2, \dots v_{mD} \,]$

$\leq \underbrace{\binom{mD}{2m}}_{\text{prob of selecting } 2m \text{ repeats}} \left(\frac{mD}{N}\right)^{2m}$

$p_m \leq \binom{N}{m} \binom{mD}{2m} \left(\frac{mD}{N}\right)^{2m}$

$\binom{N}{m}$ → No of ways to choose a set of size m

$\leq \left(\frac{Ne}{m}\right)^m \left(\frac{mDe}{2m}\right)^{2m} \left(\frac{mD}{N}\right)^{2m}$

$= \left(\frac{e^3 D^4 m}{4N}\right)^m \qquad$ Set $\alpha = \frac{1}{e^3 D^4}$

Now $m \leq \alpha N$

$p_m \leq \left(\frac{e^3 D^4 \times 1}{4 \times e^3 D^4}\right)^m = 4^{-m}$

$$\Pr[G \text{ is not an } (\alpha N, D\cdot 2)\text{-expander}] = \sum_{m=1}^{|\alpha N|} P_m$$

$$= \sum_{m=1}^{|\alpha N|} 4^{-m} \leq \sum_{m=1}^{\infty} 4^{-m}$$

$$= \frac{1}{4(1-1/4)}$$

$$= \frac{1}{3} < \frac{1}{2}$$

M: Random walk transition matrix $(n \times n)$ for a graph G
↳ Probability Transition Matrix

M_{ij} = Prob of going from vertex i to vertex j in one step.

π: Prob Dis^n of vertices

$$(\pi M)_j = \sum_i \pi_i M_{ij}$$

$\pi M^t \Rightarrow$ Dis^n on vertices after t steps of the Random Walk

$u = \left(\frac{1}{n}, \frac{1}{n}, \ldots \frac{1}{n}\right)$
↳ uniform distribution

* If G is d-regular, then $\boxed{uM = u}$

Mixing Time:-
How large should t be so that $\|\pi M^t - u\|$ is small?

$$\Pr[G \text{ is not an } (\alpha N, D-2)\text{-expander}] = \sum_{m=1}^{|\alpha N|} P_m$$

$$= \sum_{m=1}^{|\alpha N|} 4^{-m} \leq \sum_{m=1}^{\infty} 4^{-m}$$

$$= \frac{1}{4(1-1/4)}$$

$$= \frac{1}{3} < \frac{1}{2}$$

M: Random walk transition matrix $(n \times n)$ for a graph G
↳ Probability Transition Matrix

M_{ij} = Prob of going from vertex i to vertex j in one step :

π: Prob Dis^n of vertices

$$(\pi M)_j = \sum_i \pi_i M_{ij}$$

$\pi M^t \Rightarrow$ Dis^n on vertices after t steps of the Random Walk

$u = \left(\frac{1}{n}, \frac{1}{n}, \ldots \frac{1}{n}\right)$
↳ uniform distribution

* If G is d-regular, then $\boxed{uM = u}$

Mixing Time:-
How large should t be so that $\|\pi M^t - u\|$ is small ?

Here we will consider L_2 norm b/w $\|\pi M^t - u\|$

Defⁿ:- For a ~~r~~ regular ~~graph~~ digraph G with random walk matrix M, we define

$$\lambda(G) = \max_{\pi} \frac{\|\pi M - u\|}{\|\pi - u\|} = \max_{x \perp u} \frac{\|xM\|}{\|x\|}$$

$\lambda(G) \in [0,1]$; L_2-norm

~~Proof~~: If $\lambda(G)$ is very small, then for any starting distribution π, the random walk ~~do~~ quickly converges to the uniform distⁿ (Rapidly Mixing)

Proof: $uM = u$ → we know this for ~~a reg~~ a regular di-graph

now ~~f~~ for any $\pi \Rightarrow (\pi - u) \perp u$ as $\langle \pi - u, u \rangle = \frac{1}{n} - \frac{1}{n} = 0$

$$\therefore \frac{\|\pi M - u\|}{\|\pi - u\|} = \frac{\|(\pi - u)M\|}{\|\pi - u\|} \quad \text{for } (\pi - u) \perp u$$

Let $\pi - u = x$

$$\therefore \max_{(\pi - u) \perp u} \frac{\|(\pi - u)M\|}{\|\pi - u\|} \equiv \max_{x \perp u} \frac{\|xM\|}{\|x\|}$$

Show the opp - dirⁿ as follows :-

Let $\pi = u + \alpha x$ for any $x \perp u$.

$$\frac{1}{n}\sqrt{n-1\left(\frac{1}{n^2}\right)+\left(1-\frac{1}{n}\right)^2}$$

$$\sqrt{\frac{n-1}{n^2}+\frac{(n-1)^2}{n^2}} \Rightarrow \frac{1}{n}\sqrt{(n-1)+(n-1)^2}$$

Lemma:- For every initial distribution π on the vertices of G and any $t \in Z^+$, we have

$$\|\pi M^t - u\| \le (\lambda(G))^t \|\pi - u\|$$
$$\le (\lambda(G))^t$$

Proof:- By induction on $t \Rightarrow$

For $t=1$,
$$\frac{\|\pi M - u\|}{\|\pi - u\|} \le \max_{\pi} \frac{\|\pi M - u\|}{\|\pi - u\|} = \lambda(G)$$

$$\therefore \boxed{\|\pi(M) - u\| \le \lambda(G)\|\pi - u\|}$$

For $t+1 \Rightarrow$

Let $\pi' = \pi M^t$

$$\|\pi' M - u\| \le \lambda(G)\|\pi' - u\|$$
$$= \lambda(G)\|\pi M^t - u\|$$

By induction, holds for t

$$\le \lambda(G)\left[(\lambda(G))^t \|\pi - u\|\right]$$

$$\|\pi' M - u\| \le (\lambda(G))^{t+1}\|\pi - u\| \Rightarrow \|\pi M^{t+1} - u\| \le (\lambda(G))^{t+1}\|\pi - u\|$$

$\therefore$ we have proved $\|\pi M^t - \mu\| \le (\lambda(G))^t \|\pi - \mu\|$

$$\|\pi - \mu\|^2 = \|\pi\|^2 + \|\mu\|^2 - 2\langle \pi, \mu \rangle$$

$$= \sum_{i=1}^{n} (\pi_i)^2 + \frac{1}{n} - 2\left(\frac{1}{n}\right)$$

$$= \sum_{i=1}^{n} (\pi_i)^2 - \frac{1}{n} \le \sum_{i=1}^{n} (\pi_i) - \frac{1}{n}$$

$$\le 1 - \frac{1}{n}$$

$$\therefore \boxed{\|\pi - \mu\| \le 1 - \frac{1}{n} \quad \forall \pi}$$

$\therefore$ 2nd inequality $\Rightarrow$ $\|\pi M^t - \mu\| \le (\lambda(G))^t \|\pi - \mu\|$

$$\le (\lambda(G))^t$$

$\therefore$ Smaller value of $(\lambda(G))$ $\Rightarrow$ implies faster mixing ($\because$ smaller mixing time) for a random walk on graphs.

Eigenvalues :-

$v \in \mathbb{R}^n \setminus \{0\}$ is an eigenvector of $n \times n$ matrix M
if $vM = \lambda v$ for some $\lambda \in \mathbb{R}$

λ is the corresponding eigenvalue.

Spectral Theorem for Symmetric Matrices:-

M: symmetric $n \times n$ real matrix with distinct eigenvalues $\mu_1, \mu_2, \ldots, \mu_k$

$W_i = \{ v \in \mathbb{R}^n \mid vM = \mu_i v \}$

$\uparrow$
eigenspaces
of M

For symmetric matrices, all W_i's are orthogonal & span whole of $\mathbb{R}^n$.

i.e. $W_1 + W_2 \ldots + W_k = \mathbb{R}^n$ ✱

$\mathrm{Dim}(W_i)$ = Multiplicity of μ_i $\rightarrow$

✱ $\mathbb{R}^n$ has a basis consisting of orthogonal eigenvectors $v_1, v_2, \ldots v_n$ having resp. eigenvalues $\lambda_1, \lambda_2, \ldots \lambda_n$

✱ Let G: undirected regular graph with random walk matrix M

$\therefore$ M: symmetric & it is a prob transition matrix

Now $uM = u$ (as G $\rightarrow$ regular graph)

$\therefore$ u = an eigenvector of M with eigenvalue = 1

Let $v_2, v_3, \ldots v_n$ & $\lambda_2, \ldots \lambda_n$ be the remaining eigenvector & eigenvalues of M.

π: prob disn

$\pi = u + c_2 v_2 + c_3 v_3 + \ldots c_n v_n$ for some $c_2, \ldots c_n$

$\pi M^t = uM^t + c_2 v_2 M^t + \ldots c_n v_n M^t$

$\pi M^t = u + \lambda_2^t c_2 v_2 + \ldots \lambda_n^t c_n v_n$

Lemma:- Let G be a regular undirect graph whose ~~transition~~ matrix random walk matrix = M. Let the eigenvalues be $\lambda_1, \lambda_2, - \lambda_n$

s.t $1 = \lambda_1 \geq |\lambda_2| \geq |\lambda_3| - - \geq |\lambda_n|$.

Then, $\underline{\underline{\lambda(G) = |\lambda_2|}}$.

Proof: $x \perp u \rightarrow$ ~~dx for an~~ Take any $x \perp u$

$x = c_2 v_2 + - - c_n v_n$

$$\|(xM)\|_2^2 = \| \lambda_2 c_2 v_2 + - \lambda_n c_n v_n \|^2$$

$$= \lambda_2^2 c_2^2 \|v_2\|^2 + - - \lambda_n^2 c_n^2 \|v_n\|^2$$

$$\cancel{= \lambda_2^2 c_2^2 + \lambda_n^2 c_n^2}$$

$$\leq |\lambda_2|^2 \left(c_2^2 \|v_2\|^2 + - c_n^2 \|v_n\|^2 \right)$$

$$\|xM\|_2^2 \leq |\lambda_2|^2 \|x\|_2^2$$

$$\therefore \frac{\|xM\|_2}{\|x\|_2} \leq |\lambda_2| \quad \text{for any } x \in \mathbb{R}^n$$

$$\therefore \max \frac{\|xM\|_2}{\|x\|_2} \leq |\lambda_2|$$

$\hookrightarrow$ we defined this $= \lambda(G)$

$$\therefore \lambda(G) \leq |\lambda_2|$$

max occurs for $x = v_2 \rightarrow$

and for that case the max value $= |\lambda_2|$

$$\therefore \lambda(G) = |\lambda_2|$$

1/11/23

Expanders:-

G: undirected regular graph with random walk matrix M.

We showed $\lambda(G) = |\lambda_2| \rightarrow$ second largest eigenvalue of M.

G: N-vertex regular ~~graph~~ digraph with random walk matrix M

$$\lambda(G) = \max_{\pi} \frac{\|\pi M - u\|}{\|\pi - u\|} = \max_{x \perp u} \frac{\|xM\|}{\|x\|}$$

where $u = \left(\frac{1}{N}, \frac{1}{N}, \text{———} \frac{1}{N}\right)$

$\lambda(G) = |\lambda_2| \longrightarrow$ also holds for it (Proofs: Check out yourself)

* Spectral Gap of G:- $\gamma(G) = 1 - \lambda(G)$

larger value of $\gamma \Rightarrow$ higher expansion [as per definition of Spectral Expansion]

means smaller $\lambda(G) \rightarrow$ implies faster mixing for RWs on graphs

Spectral Expansion:-

* A regular digraph G has spectral expansion γ ($\gamma \in [0,1]$) if $\gamma(G) \geq \gamma$ (equivalently, $\lambda(G) \leq 1-\gamma$).

SPECTRAL EXPANSION $\Rightarrow$ VERTEX EXPANSION

Theorem:- If G is a ~~d~~regular digraph with spectral expansion $\gamma = 1 - \lambda$ ($\lambda \in [0,1]$) then for every $\alpha \in [0,1]$, G is an $\left(\alpha N, \frac{1}{\lambda^2(1-\alpha)+\alpha}\right)$ - vertex expansion.

Def:- For a probability distribution π, define collision probability of π as the probability that two independent samples of π are equal $\Rightarrow$

$$\therefore \boxed{CP(\pi) = \sum_x \pi_x^2}$$

support of π, $Supp(\pi) = \{x \mid \pi_x > 0\}$

Lemma: For any distribution, $\pi \in [0,1]^N$, we have

① $CP[\pi] = \|\pi\|^2 = \|\pi - \mu\|^2 + 1/N$
$\hookrightarrow$ uniform dis^n

$\cancel{\|\pi\|^2 + \frac{1}{N} - 2\left(\frac{1}{N}\right) - 1/N}$

As $\|\pi - \mu\|^2 = \sum_x \left(\pi_x - \frac{1}{N}\right)^2$

$$= \sum_x (\pi_x)^2 - \frac{2}{N}\sum \pi_x + \sum_x \frac{1}{N^2}$$

$$= \|\pi\|^2 - \frac{1}{N}$$

$$\therefore \boxed{\|\pi - \mu\|^2 + \frac{1}{N} = \|\pi\|^2}$$

$\therefore$ From ① $\Rightarrow$ $CP(\pi) = \|\pi\|^2 = \|\pi - \mu\|^2 + 1/N$

② $CP(\pi) \geq \dfrac{1}{|Supp(\pi)|}$

let $y \in \mathbb{R}^n$ st $y_i = \begin{cases} 1 & \text{if } i \in Supp(\pi) \\ 0 & \text{o.w.} \end{cases}$

$$\langle y, \pi\rangle = \sum_{x \in Supp(\pi)} \pi_x = 1$$

$\langle y, \pi \rangle = 1$

Applying Cauchy's Schwarz $\Rightarrow$

$$\langle y, \pi \rangle \leq \|y\| \cdot \|\pi\|$$

Now $\|y\| = \sqrt{\sum_{i=1}^{N}(y_i^2)}$

$= \sqrt{|supp(\pi)|}$

$\therefore \langle y, \pi\rangle \le \|y\| \cdot \|\pi\|$

$= 1' \le \sqrt{|supp(\pi)|} \cdot \sqrt{CP(\pi)}$

$$\therefore \boxed{CP(\pi) \ge \frac{1}{|supp(\pi)|}}$$

Equality holds for uniform distribution over supp (π)

Proof of Theorem :- Spectral expansion $\gamma = 1-\lambda$ implies

$\Rightarrow G$ is $\left(\alpha N, \frac{1}{(1-\alpha)\lambda^2+\alpha}\right)$ - vertex expansion

Proof :- $CP(\pi M) - \frac{1}{N} = \|\pi M - u\|^2$ (from above lemma)

$\le \|\pi - u\|^2 \lambda(G)^2$ (from previous classes)

$\le (\lambda(G))^2 \left[CP(\pi) - 1/N\right]$

$\le \lambda^2 \left(CP(\pi) - 1/N\right)$

This result holds for all π

as $\gamma = 1-\lambda$

and $\gamma(G) \ge 1-\lambda$

$\therefore \lambda(G) \le 1-\gamma$

$\le \lambda$

~~For~~

VERTEX-EXPANSION $\Rightarrow$ SPECTRAL EXPANSION:-

For every $\delta > 0$, $D > 0$, $\exists \gamma > 0$ s.t. if G is a D-regular $(\frac{N}{2}, 1+\delta)$ vertex expander, then it has spectral expansion γ where

$$\gamma \sim \Omega\left(\left(\frac{\delta}{D}\right)^2\right)$$

Larger values of δ (vertex expansion) $\rightarrow$ imply larger values of γ

Randomness - Efficient Error Reduction:- (for class RP)

for randomized algo with one-sided error.

A: randomized algorithm with one-sided error using m-random bits running in time T deciding membership in L.

$x \in L$ $\Pr[A(x) = 1] \geq \frac{1}{2}$ OR $= 1$

$x \notin L$ $\Pr[A(x) = 1] = 0$ OR $\leq \frac{1}{2}$

Task: reduce error probability to $\frac{1}{2^t}$

Method	~~Time~~ No of Repetitions	# Random bits
Independent repetitions	t	tm
Pairwise independence	2^t	$2 \cdot O(\max\{t, m\})$ (much less compared to case 1)

S: subset of vertices with $|S| \le \alpha N$

π: uniform dis^n on S.

$$CP(\pi) = \frac{1}{|\text{supp}(\pi)|} = \frac{1}{|S|}$$ (as we have uniform dis^n over supp(π))

$$CP(\pi M) \ge \frac{1}{|\text{Supp}(\pi M)|} = \frac{1}{|\text{Neigh}(S)|}$$

$\downarrow$
all vertices in neighbourhood of S come in supp (πM) as πM denotes taking one step of the Random Walk

$$\left(\frac{1}{N(S)} - \frac{1}{N}\right) \le CP(\pi M) - \frac{1}{N} \le \lambda^2 \left(CP(\pi) - \frac{1}{N}\right)$$
$$= \lambda^2 \left(\frac{1}{|S|} - \frac{1}{N}\right)$$

$$\frac{1}{N(S)} - \frac{1}{N} \le \lambda^2 \left(\frac{1}{|S|} - \frac{1}{N}\right)$$

Also, $\underline{\underline{|S| \le \alpha N}}$

$\therefore N \ge \frac{|S|}{\alpha}$

$$\boxed{\frac{1}{N} \le \frac{\alpha}{|S|}}$$

$$\frac{1}{N(S)} \le \lambda^2 \left(\frac{1}{|S|}\right) + \frac{1}{N}(1-\lambda^2)$$

$$\frac{1}{N(S)} \le \lambda^2 \left(\frac{1}{|S|}\right) + \frac{\alpha}{|S|}(1-\lambda^2)$$

$$\frac{1}{N(S)} \le \frac{1}{|S|}\left[\lambda^2 + \alpha - \alpha\lambda^2\right]$$

$$\frac{1}{N(S)} \le \frac{1}{|S|}\left[\alpha + \lambda^2(1-\alpha)\right]$$

$$N(S) \ge \cancel{\frac{|S|}{\lambda^2 + (1-\lambda^2)\alpha}} \quad \frac{|S|}{\alpha + \lambda^2(1-\alpha)}$$

$\therefore G$ is $\left(\alpha N, \frac{1}{(1-\alpha)\lambda^2 + \alpha}\right)$ vertex expander

$\therefore$ Spectral Expansion implies vertex expansion

$x_i = ai + b \pmod p$

$x_1, x_2, \ldots x_t \qquad \frac{1}{t}$

Also $\log p \simeq O(m)$

Also $2^t \leq p \rightarrow t \simeq O(\log p)$

Method	No of Reps.	# Random bits
with expanders	t repetitions	$O(m+t)$

__How?__

Let G be an expander graph on 2^m vertices with vertex set $\{0,1\}^m$. Also G is a __D-regular__ expander graph

D ⇒ is a constant

⇒ Choose a vertex $v_1 \in \{0,1\}^m$ uniformly at random ⇒ __Requires m ~~$O(m)$ bits~~ bits__

⇒ Do a random walk starting from v_1 of length $t-1$.

Let $v_1, v_2, v_3, \ldots v_t$ be the path.] ⇒ At each vertex we have D-choices for choosing next vertex ∴ Total $O(t \log D)$ bits for random walk.

⇒ Run $A(x; v_i)$ for $i = 1, 2, \ldots t$

and return 1 if $A(x; v_i) = 1$ for some i and

~~0 otherwise~~

return 0 otherwise

∴ # of Random bits required $= O(t \log D) + O(m)$

(If we treat $\log D$ to be constant,) then, # of random bits $= \underline{\underline{O(m+t)}}$

Analysis :-

Let B : be a set of "bad" vertices , i.e. non-witnesses for the membership of x in L

G is a good expander $\Rightarrow$ $Pr[\bigwedge_{i=1}^{t} v_i \in B]$ vanishes exponentially in t.

i.e. $\boxed{Pr[\bigcap_{i=1}^{t} v_i \in B] \leq \frac{1}{2^t}}$

$|B| \leq \frac{2^m}{2}$ $\rightarrow$ or $\frac{|B|}{2^m} \leq \frac{1}{2}$ $\Rightarrow$ Density of B $\Rightarrow$ $\frac{|B|}{2^m}$

$\downarrow$

As the failure probability for membership is $\leq \frac{1}{2}$

(we need all this analysis only for case of non-zero membership → there with error probability)

Hitting Property of Expanders:-

If G is a regular digraph with spectral expansion $1-\lambda$, then for any $B \subset V(G)$ of density μ, the prob that a random walk $v_1, v_2, v_3, \ldots v_t$ starting in a uniformly random vertex V_1 always remains in B is

$V_1 \downarrow B$

$$\boxed{Pr[\bigwedge_{i=1}^{t} v_i \in B] \leq (\mu + (1-\mu)\lambda)^t}$$

$\downarrow$

Prob that a random walk starting in a vertex $\in B$ always lands up in a vertex $v_i \in B$ for the t steps

$\Rightarrow$ In this case, our algo (with t steps) will give ~~error~~ wrong

Def^n :- $\text{Bipartite}_{N,D}$: set of bipartite digraphs with N vertices on each side ($|L| = |R| = n$) and ~~are d-left~~ D-left Regular
(ie all vertices in L have degree D)

<u>Existence of Bipartite Vertex Expanders</u> :: (using Probabilistic Method)

<u>**Theorem**</u>: For any constant D, $\exists\, \alpha > 0$, s.t $\forall N$, a uniformly chosen graph from $B_{N,D}$ is an $(\alpha N, D-2)$ with prob $> \frac{1}{2}$.

<u>Proof</u> $\quad G \xleftarrow[\text{at random}]{\text{unif at random}} Bip_{N,D}$

Fix $N \Rightarrow \therefore L, R \to$ sets of size N

For every vertex v in L, choose D vertices from R uniformly with replacement (as we have a multigraph family)

$\{u_1, u_2, \ldots u_D\}$ $\quad (v, u_i) \in E$ for $\forall\, i \in \{1, 2 \ldots D\}$

Take any set $S \subseteq L$ s.t. $|S| \le \alpha N$ $\quad$ we want to show $|N(S)| \geq (D-2)|S|$ $\forall\, S \subseteq L$ s.t. $|S| \le \alpha N$

Let $m \le \alpha N$

<u>P_m</u>: prob that $\exists\, S \subseteq L$ with $|S| = m$, that does not expand by a factor $\ge$ <u>$D-2$</u>