Expanders

- We now start the first topic in our list of pseudorandom constructions.

- Motivation: Solving the problem of undirected connectivity in logspace ($\mathbb{L}$ or RL).

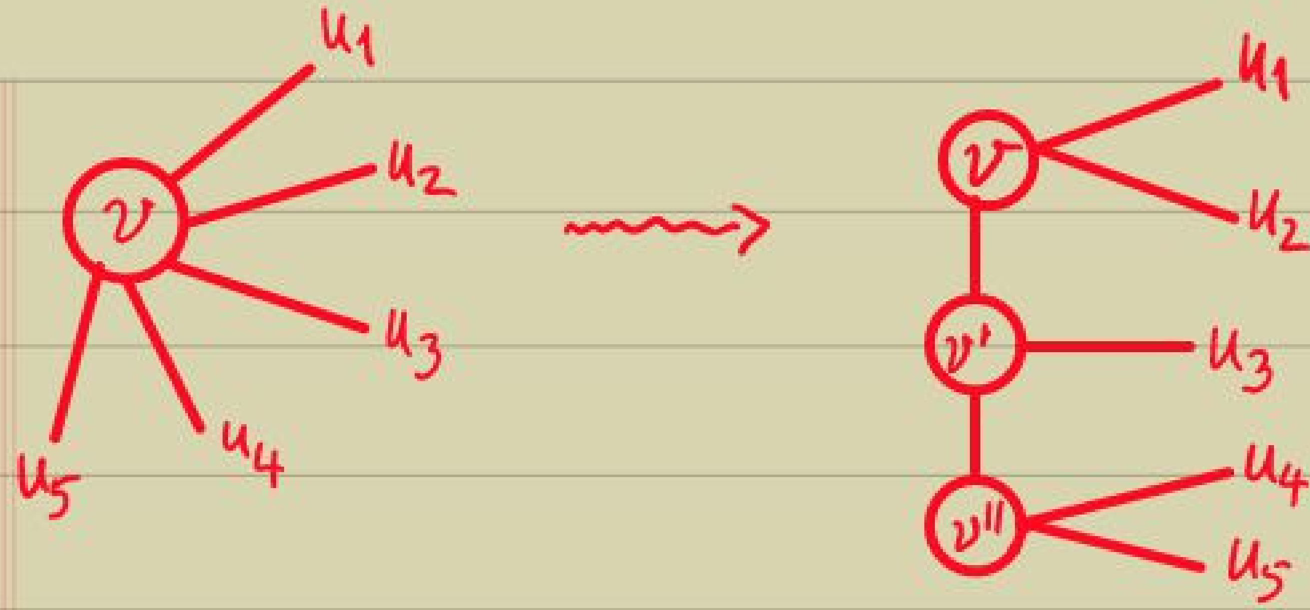
Defn: Upath $:= \{(G,s,t) \mid \exists$ path $s \rightsquigarrow t$ in the undirected graph $G\}$.

Theorem (Aleliunas, Karp, Lipton, Lovász, Rackoff 1979): Upath $\in$ RL.

Pf:

- Suppose G is the given undirected graph with n vertices.
- Wlog we can assume G to be d-regular.

Eg. the following gadget achieves 3-regularity (in logspace):



- Now the algorithm is to do a <u>random walk</u>, starting from v, of length $300 n^4 \lg n$.

Helps in remembering the history of the walk

- Assume that each vertex in G has a <u>self-loop</u>.

- Let A be the <u>normalized</u> adjacency matrix of G. I.e. $A_{ij} := \#\text{edges}(i,j)/d$.

▷ A is symmetric with entries in $[0,1]$.
▷ The row-sum, resp. col-sum, is $\underline{1}$.
(A is <u>symmetric stochastic</u>.)

- At any stage of the walk, $\bar{p} = (p_1, \dots, p_n)^T$ collects the probability p_i of being at the vertex i.

▷ In one step of the random walk the probability changes as $\bar{p}$ to $\bar{q} = A \cdot \bar{p}$.

<u>Pf</u>:

- $q_i := \Pr[\text{walk is at } i]$

$$= \sum_{j \in [n]} \Pr[\text{walk was at } j] \cdot \Pr[\text{walk is at } i \mid \text{was at } j]$$

$$= \sum_j p_j \cdot A_{ji} = (A \cdot \bar{p})_i .$$ □

- Let $\bar{e}^s$ be the elementary vector that is 1 at the s-th coordinate.

▷ After l steps of the random walk, the probability vector is $A^l \cdot \bar{e}^s$.

- Now we study the action of A, by using its eigenvalues as the main tool.

<u>Exercise</u>: A has real eigenvalues $\lambda_1, \ldots, \lambda_n$ with $|\lambda_n| \leq |\lambda_{n-1}| \leq \cdots \leq |\lambda_1| = 1$.

- Denote the uniform probability vector $(1/n, \dots, 1/n)^T$ by $\bar{1}$.

Since $A \cdot \bar{1} = \bar{1}$ we have $\bar{1}$ as an eigenvector. Consider $\bar{1}^\perp := \{v \in \mathbb{R}^n \mid \langle v, \bar{1} \rangle = 0\}$.
(vectors orthogonal to $\bar{1}$)

▷ $\lambda(A) := \max\{\|Av\| \mid v \in \bar{1}^\perp \ \& \ \|v\| = 1\}$ is the second largest eigenvalue of A.

Pf:

- Since A is symmetric we can find an orthonormal basis $\{b_1, \dots, b_n\}$ of $\mathbb{R}^n$ s.t. b_i is an eigenvector of λ_i and $b_1 = \bar{1}$.

$\Rightarrow \quad \bar{1}^\perp = sp_{\mathbb{R}}\{b_2, \dots, b_n\}$

$\Rightarrow$ for a $v = \sum_{i>1} \alpha_i b_i \in \bar{1}^\perp$,

$$Av = \sum_{i>1} \alpha_i \lambda_i b_i$$

$$\Rightarrow \frac{\|Av\|^2}{\|v\|^2} = \frac{\|\sum \alpha_i \lambda_i b_i\|^2}{\|\sum_{i>1} \alpha_i b_i\|^2} = \frac{\sum \alpha_i^2 \lambda_i^2}{\sum_{i>1} \alpha_i^2} \leq \lambda_2^2 .$$

$\Rightarrow$ max $\|Av\|$ over unit vectors in $\bar{1}^\perp$ is exactly λ_2. $\square$

▷ $\lambda(A^\ell) \leq \lambda(A)^\ell$.

Pf:

- By the definition of $\lambda(\cdot)$,
  $\|Av\| \leq \lambda(A)\cdot\|v\|$, for $v \in \bar{1}^\perp$.
- Also, $\langle Av, \bar{1}\rangle = \langle v, A\cdot\bar{1}\rangle = \langle v, \bar{1}\rangle = 0$,
  for $v \in \bar{1}^\perp$.

$\Rightarrow$ A maps $\bar{1}^\perp$ to itself, shrinking each vector by a factor of $(\leq)$ $\lambda(A)$.

$\Rightarrow \|A^\ell v\| \leq \lambda(A)^\ell\cdot\|v\|$, for $v \in \bar{1}^\perp$

$\Rightarrow \lambda(A^\ell) \leq \lambda(A)^\ell$. $\square$

Exercise: $\lambda(A^\ell) = \lambda(A)^\ell$.

Lemma 1: $\forall$ probability vector $\bar{p}$, $\|A^\ell\cdot\bar{p} - \bar{1}\| < \lambda(A)^\ell$.

Pf:

- $\|A^\ell\bar{p} - \bar{1}\| = \|A^\ell\cdot(\bar{p}-\bar{1})\|$
  $\leq \lambda(A^\ell)\cdot\|\bar{p}-\bar{1}\|$ $\quad (\because \langle \bar{p}-\bar{1}, \bar{1}\rangle = 0)$
  $< \lambda(A)^\ell\cdot\|\bar{p}-\bar{1}\|$

- Define $\bar{p}' := \bar{p} - \bar{1}$

$\Rightarrow \bar{p}' \in \bar{1}^{\perp}$.

$\Rightarrow$

$$\|\bar{p}\|^2 = \|\bar{1}\|^2 + \|\bar{p}'\|^2$$

$$\Rightarrow \|\bar{p}'\| < \|\bar{p}\| \leq \left(\sum_{i=1}^{n} p_i\right)^2 = 1.$$

$$\Rightarrow \|A^{\ell} \cdot \bar{p} - \bar{1}\| < \lambda(A)^{\ell}. \qquad \square$$

▷ Thus, the <u>further</u> $\lambda(A)$ is from 1, the <u>faster</u> is the convergence of $A^{\ell} \cdot \bar{p}$ to $\bar{1}$!

- $1 - \lambda(A)$, or $1 - \lambda(G)$, is called the <u>spectral gap</u> of the graph G.

We wish it large.

<u>Lemma 2:</u> $\forall$ d-regular, connected G (with self-loops),

$$1 - \lambda(G) \geq 1/8dn^3.$$

Pf: • Let $u \in \bar{1}^{\perp}$ be a unit vector & $v := Au$.

• We will show $1 - \|v\|^2 \geq 1/4dn^3$.

$$\text{Thus, } \|v\|^2 \leq 1 - \frac{1}{4dn^3}$$

$$\Rightarrow \|v\| \leq 1 - 1/8dn^3 .$$

▷ $1 - \|v\|^2 = \sum_{i,j \in [n]} A_{ij} \cdot (u_i - v_j)^2$.

• Also quad. form in the Laplacian of G.

Pf:

• $\sum A_{ij} \cdot (u_i - v_j)^2 = \sum A_{ij} u_i^2 - 2 \sum A_{ij} u_i v_j + \sum A_{ij} v_j^2$

$$= \sum_i (\sum_j A_{ij}) \cdot u_i^2 - 2 \cdot \langle Au, v \rangle + \sum_j (\sum_i A_{ij}) \cdot v_j^2$$

$$= \|u\|^2 - 2 \cdot \|v\|^2 + \|v\|^2$$

$$= 1 - \|v\|^2 . \qquad \square$$

• Thus, it suffices to show that $\exists i, j$ st.

$$A_{ij} \cdot (u_i - v_j)^2 \geq 1/4dn^3 .$$

• If $\exists i$, $(u_i - v_i)^2 \geq 1/4n^3$ then we are done (as $A_{ii} = 1/d$).

• So, assume that $\forall i$, $|u_i - v_i| < 1/2n^{1.5}$.

- Sort the coordinates of $\bar{u}$; wlog $u_1 \geq \cdots \geq u_n$.
- $\sum u_i = 0$ & $\sum u_i^2 = 1 \Rightarrow$ either $u_1 \geq 1/\sqrt{n}$ or $u_n \leq -1/\sqrt{n}$.

  $\Rightarrow u_1 - u_n \geq 1/\sqrt{n}$

  $\Rightarrow \exists i_0, \quad u_{i_0} - u_{i_0+1} > 1/n^{1.5}$

  $\Rightarrow \forall i \in [i_0], j \in [i_0+1 \ldots n], \ u_i - u_j > 1/n^{1.5}$.

- Since G is connected we can pick such an edge, say (i,j).

$$\Rightarrow A_{i,j} \cdot (u_i - v_j)^2 \geq \frac{1}{d} \cdot (|u_i - u_j| - |u_j - v_j|)^2$$

$$> \frac{1}{d}\left(\frac{1}{n^{1.5}} - \frac{1}{2n^{1.5}}\right)^2 = \frac{1}{4dn^3}.$$

$\Rightarrow 1 - \|Au\|^2 \geq 1/4dn^3$

$\Rightarrow 1 - \lambda(A) \geq 1/8dn^3$. $\square$

<u>Lemma 3:</u> Let $l := 10dn^3 \lg n$. If s,t are connected in G then $\Pr[$random walk reaches t at the l-th step $] > 1/2n$.

Pf: • Let $\bar{p}$ be the probability vector at the ℓ-th step.

• Lemma 2 & 1 $\Rightarrow \|A^{\ell}\cdot\bar{e}^{s}-\bar{1}\| \leq \left(1-\frac{1}{8dn^3}\right)^{\ell}$

$$\leq \left(1-\frac{1}{8dn^3}\right)^{10dn^3\lg n} < \frac{1}{2n^{1.5}} \cdot \left(e^{-1.25\lg n}\right)$$

• By Cauchy-Schwarz inequality:

$$\|A^{\ell}\cdot\bar{e}^{s}-\bar{1}\|_1 \leq \|A^{\ell}\cdot\bar{e}^{s}-\bar{1}\|_2 \cdot \sqrt{n} < 1/2n.$$

$$\Rightarrow |(A^{\ell}\cdot\bar{e}^{s}-\bar{1})_t| < 1/2n$$

$$\Rightarrow \Pr[\text{reaching } t \text{ at } \ell] > \frac{1}{n}-\frac{1}{2n}=\frac{1}{2n}. \quad \square$$

- Thus, by continuing this walk for a longer amount we can bring the probability above 3/4.

  eg. $\left(1-\frac{1}{2n}\right)^{4n} \leq \frac{1}{e^2} < \frac{1}{4}$

  $\Rightarrow \ell = 40dn^4\log n$ suffices.

- This random walk is in logspace, as we only need to store the current vertex label (of bit-size $O(\lg n)$), proving the theorem. $\square$

- Can it be derandomized?

  This was an intriguing question for three decades, and several tools were developed.

- The basic idea is to convert the input G to G' – a graph with constant spectral gap, so that $\ell = O(\lg n)$ suffices to reach any vertex from s.

  Now one can exhaustively look for all $O(\lg n)$-length paths from s, in $\mathbb{L}$.

- This relation between spectral gap & connectivity motivates the following two definitions of expanders.

Definition (Algebraic): • We call a graph G an (n, d, λ)-expander if G is n-vertex, d-regular & $\lambda(G) \leq \lambda$.

- A (d,λ)-expander family $\{G_n\}_n$ is s.t. $\forall n$, G_n is an (n,d,λ)-expander.

Show $\lambda(G) > 1/\sqrt{d}$ by using $tr(A^2)$.

- Alon-Boppana (1986) showed that $\lambda(G)$ is at least $2\sqrt{d-1}/d$.

assuming a sufficiently large diameter

The graphs meeting this bound are called Ramanujan graphs. for $d = p^k+1$

Their explicit constructions are due to Lubotzky-Phillips-Sarnak (1988).

Definition (Combinatorial): We call G an (n,d,ρ)-edge expander if G is an n-vertex d-regular graph s.t. $\forall S \subseteq V(G)$ with $|S| \leq n/2$, $|E(S,\bar{S})| \geq \rho \cdot d \cdot |S|$.

edges going out of S

- Note: In the algebraic definition we desire λ to be small ($\approx 2/\sqrt{d}$), while in the combinatorial definition we want ρ to be large ($\approx 1/2$).

- We will now show the equivalence of the two definitions. (G is regular, has self-loops)

<u>Theorem 1</u>: G is an (n,d,λ)-expander $\Rightarrow$
" " " $(n,d,\frac{1-\lambda}{2})$-edge expander.

<u>Theorem 2</u>: G is an (n,d,ρ)-edge expander $\Rightarrow$
" " " $(n,d,1-\rho^2/8)$-expander.

▷ <u>Cheeger's inequality</u>: $\frac{1-\lambda(G)}{2} \leq \rho(G) \leq \sqrt{2(1-\lambda(G))}$.
(Measures <u>bottlenecks</u> in graph)

<u>Pf of Thm 1</u>:

- The number of edges going out of S are estimated by considering $Z := \sum_{i,j\in[n]} A_{ij}\cdot(x_i - x_j)^2$.

- Define $\bar{x} \in \mathbb{R}^n$ as $x_i := \begin{cases} |\bar{S}| & \text{if } i \in S \\ -|S| & \text{if } i \notin S. \end{cases}$

$$\Rightarrow Z = \sum_{(i,j)\in S^2} + \sum_{(i,j)\in \bar{S}^2} + \sum_{(i,j)\in S\times\bar{S} \cup \bar{S}\times S}$$

$$= 0 + 0 + 2\cdot n^2 \cdot \sum_{(i,j)\in S\times\bar{S}} A_{ij} = 2n^2 \cdot \frac{\#E(S,\bar{S})}{d}.$$

- On the other hand,

$$Z = \sum_{i,j} A_{i,j} x_i^2 - 2 \cdot \sum_{i,j} A_{i,j} x_i x_j + \sum_{i,j} A_{ij} x_j^2$$

$$= \sum_i \left(\sum_j A_{ij}\right) \cdot x_i^2 - 2 \langle A\bar{x}, \bar{x} \rangle + \sum_j \left(\sum_i A_{ij}\right) x_j^2$$

$$= 2 \cdot \|\bar{x}\|^2 - 2 \cdot \langle A\bar{x}, \bar{x} \rangle$$

$$\geqslant 2 \cdot \|\bar{x}\|^2 - 2 \cdot \lambda \|x\|^2$$

$\left(\because \bar{x} \in \bar{1}^{\perp} \Rightarrow \|A\bar{x}\| \leq \lambda \|\bar{x}\| \right.$

$\left. \text{\& Cauchy-Schwarz} : |\langle \bar{x}, \bar{y} \rangle| \leq \|\bar{x}\| \cdot \|\bar{y}\| \right)$

$$\Rightarrow \#E(S, \bar{S}) \cdot \frac{2n^2}{d} = Z \geqslant 2 \cdot \|x\|^2 \cdot (1-\lambda)$$

$$= 2 \cdot (1-\lambda) \cdot \left(|S| \cdot |\bar{S}|^2 + |\bar{S}| \cdot |S|^2 \right)$$

$$\Rightarrow \#E(S, \bar{S}) \geqslant \frac{(1-\lambda) d}{n} \cdot |S| \cdot |\bar{S}|$$

$$\geqslant (1-\lambda) \cdot \frac{d}{n} \cdot |S| \cdot \frac{n}{2} = \left(\frac{1-\lambda}{2}\right) \cdot d \cdot |S| .$$

$\Rightarrow G$ is an $\left(n, d, \frac{1-\lambda}{2}\right)$-edge expander. $\square$

<u>Pf of Thm 2</u>: Now we assume G to be an (n,d,ρ)-edge expander.

- The idea again is to estimate Z, but now using an eigenvector corresponding to λ_2 as $\bar{x}$.

Recall that $1=\lambda_1 \geq |\lambda_2| \geq \dots \geq |\lambda_n|$ are the eigenvalues of A.

- Let $\bar{u} \neq 0$ be an eigenvector s.t.

$$A\bar{u} = \lambda_2 \cdot \bar{u} \quad \& \quad \bar{u} \in \bar{1}^{\perp}.$$

- Since $\bar{u}$ has positive & negative coordinates, let us collect them in $\bar{v}$ & $\bar{w}$ respectively.

$$\Rightarrow \quad \bar{u} = \bar{v} + \bar{w} \ ; \ \bar{v}, -\bar{w} \in (\mathbb{R}_{\geq 0})^n.$$

- Wlog $\bar{v}$ has $\leq \frac{n}{2}$ nonzero entries (else we take $-\bar{u}$).

Assuming $v_1 \geq v_2 \geq \dots \geq v_n \geq 0$

- Consider $Z := \sum_{i<j \in [n]} A_{ij} \cdot (v_i^2 - v_j^2)$.

- We will show that:

<u>Claim 1</u>: $Z \geqslant \rho \cdot \|\bar{v}\|^2$ (uses edge expansion)

<u>Claim 2</u>: $Z \leq \sqrt{8(1-\lambda_2)} \cdot \|\bar{v}\|^2$ (general graph property)

▷ Clearly, the above two claims prove Thm 2.

<u>Pf of Claim 1</u>:

- Sort the coordinates of $\bar{v}$: $v_1 \geqslant \dots \geqslant v_n \geqslant 0$ with $v_i = 0$ for $i > n/2$.
- $Z = \sum_{i<j\in[n]} A_{ij} (v_i^2 - v_j^2)$

$$= \sum_{i<j\in[n]} A_{ij} \sum_{i\leq k<j} (v_k^2 - v_{k+1}^2)$$

(flip the sums)

$$= (1/d) \cdot \sum_{k=1}^{n/2} \#E([k], [k+1\dots n]) \cdot (v_k^2 - v_{k+1}^2)$$

(Using the fact that $v_i = 0$, $i > n/2$)

$$\geqslant (1/d) \cdot \sum_{1\leq k\leq n/2} \rho d k \cdot (v_k^2 - v_{k+1}^2) = \rho \cdot \sum_{1\leq k\leq \frac{n}{2}} (k v_k^2 - k v_{k+1}^2)$$

$$= \rho \cdot \sum_{1\leq k\leq \lfloor n/2 \rfloor} (k v_k^2 - (k-1) v_k^2) = \rho \cdot \|v\|^2. \quad \square$$

Pf of Claim 2:

- Z & λ_2 are fundamentally related:

- $\langle A\bar{u}, \bar{v}\rangle = \langle \lambda_2 \bar{u}, \bar{v}\rangle = \langle \lambda_2 \bar{v} + \lambda_2 \bar{w}, \bar{v}\rangle = \lambda_2 \cdot \|\bar{v}\|^2$.
- Also, $\langle A\bar{u}, \bar{v}\rangle = \langle A\bar{v}, \bar{v}\rangle + \langle A\bar{w}, \bar{v}\rangle \leq \langle A\bar{v}, \bar{v}\rangle$.

$$\Rightarrow \quad \lambda_2 \leq \frac{\langle A\bar{v}, \bar{v}\rangle}{\|\bar{v}\|^2}$$

$$\Rightarrow 1-\lambda_2 \geq \frac{\|\bar{v}\|^2 - \langle A\bar{v}, \bar{v}\rangle}{\|\bar{v}\|^2}$$

$$= \frac{2\cdot\sum_i v_i^2 - \sum_{i,j} 2\cdot A_{ij}\cdot v_i \cdot v_j}{2\cdot\|\bar{v}\|^2}$$

$$= \frac{\sum_{i,j} A_{ij} v_i^2 + \sum_{i,j} A_{ij} v_j^2 - \sum_{i,j} 2A_{ij}\cdot v_i v_j}{2\cdot\|\bar{v}\|^2}$$

$$= \sum_{i<j\in[n]} A_{ij}\cdot(v_i - v_j)^2 \Big/ 2\cdot\|\bar{v}\|^2$$

$$= \frac{\left\{\sum_{i<j} A_{ij}\cdot(v_i - v_j)^2\right\}\cdot\left\{\sum_{i<j} A_{ij}\cdot(v_i + v_j)^2\right\}}{2\cdot\|\bar{v}\|^2 \cdot \left\{ \quad '' \quad \right\}}$$

- Let us estimate the two expressions:

- Numerator — Cauchy-Schwarz inequality gives: $\geq \left(\sum_{i<j} A_{ij}\cdot(v_i^2-v_j^2)\right)^2 = Z^2$.

- Denominator —

$$\frac{1}{2}\cdot\sum_{i,j\in[n]} A_{ij}\cdot(v_i+v_j)^2 = \frac{1}{2}\sum A_{ij}\cdot(v_i^2+v_j^2) + \sum A_{ij}v_iv_j$$

$$= \|\bar{v}\|^2 + \sum A_{ij}v_iv_j$$

$$\leq \|\bar{v}\|^2 + \sum A_{ij}\left(\frac{v_i^2+v_j^2}{2}\right) = 2\cdot\|\bar{v}\|^2$$

$$\Rightarrow 1-\lambda_2 \geq Z^2 / 8\cdot\|\bar{v}\|^4$$

$$\Rightarrow Z \leq \sqrt{8(1-\lambda_2)}\cdot\|\bar{v}\|^2$$

□

- The polynomial $Z(G) = \sum_{i,j\in[n]} A_{ij}\cdot(x_i-x_j)^2$ is called Laplacian quadratic form of G. It carries useful information about expansion & sparsest cut in G.

Applications – Error-reduction using Expanders

- Recall that a problem $L \in BPP$ with an algorithm $M(x)$ of error $\leq 1/3$ (using r random bits) can also be solved in error $\leq 2^{-k}$.
  The naive way of repeating $M(x)$ k times requires rk random bits. Can this be improved?

- We will show that expander walk reduces the random bits to $r + O(k)$!

Idea:
- Suppose we have a $(2^r, d, 1/10)$-expander G for a constant d, where the neighbours of any vertex are listable in $poly(r)$ time.
- Choose a vertex $v_0 \in V(G)$ at random & do a random-walk for k steps; going to vertices $v_1, v_2, \ldots, v_k$.
- Use these vertex labels as random bits

to run $M(x)$ $(k+1)$-times.

Clearly, we needed $\leq r + k\lg d$ random bits. We will show that the probability of the majority-vote being wrong is $< 2^{-k}$.

- First, we bound the probability of the walk being confined to bad vertices.

Theorem (Ajtai, Komlós, Szemerédi, 1987): Let G be an (n,d,λ)-expander & $B \subseteq V(G)$, $|B| = \beta n$.

Then, $\Pr_{\text{walk in } G}[\forall i \in [0..k], v_i \in B] \leq (\beta+\lambda)^k$.

Proof:

- Let A be the normalized adjacency matrix of G.
- The idea is to express the intersection probability as a matrix product & then analyze using the spectral norm.

- Let $P = P_B$ be the $n \times n$ identity matrix with the rows corresponding to $[n] \setminus B$ set to zero.

$\|\bar{u}\|_1 := \sum_i |u_i|$

$\triangleright \Pr_{\text{walk in } G}[\forall i,\ v_i \in B] = \|(PA)^k \cdot P\bar{1}\|_1$.

Pf:

- Clearly, the prob. of $v_0 \in B$ is $\|P\bar{1}\|_1$.
- Prob. of being <u>in B</u> after one step is $\|PA \cdot P\bar{1}\|_1$.
- This easily generalizes to k steps $\square$

- Now we will study the <u>spectral norm</u> of PAP, i.e. the factor by which it shrinks a vector.

<u>Claim:</u> $\forall \bar{v} \in \mathbb{R}^n$, $\|PAP\bar{v}\| < (\beta+\lambda) \cdot \|\bar{v}\|$.

Pf:

- We could assume that $\bar{v}$ is <u>supported</u> <u>on B</u>. (Otherwise, we replace $\bar{v}$ by

$B \neq \phi$

$P\bar{v}$. This only changes the RHS but cannot increase it, i.e. $\|P\bar{v}\| \leq \|\bar{v}\|$.)

- Similarly, we assume $\bar{v}$ to be nonnegative & $\|\bar{v}\|_1 = 1$.

- Express $P\bar{v} = \bar{v} = \alpha \cdot \bar{1} + \bar{z}$, where $\bar{z} \in \bar{1}^{\perp}$.

  Since $\langle n\bar{1}, \bar{v} \rangle = 1$, we get $1 = \alpha \cdot \langle n\bar{1}, \bar{1} \rangle$. Thus, $\bar{v} = \bar{1} + \bar{z}$.

$\Rightarrow PAP\bar{v} = PA \cdot \bar{1} + PA \cdot \bar{z} = P \cdot \bar{1} + PA\bar{z}$

$\Rightarrow \|PAP\bar{v}\| \leq \|P\bar{1}\| + \|PA\bar{z}\|$.

- We now bound these by $\beta\|\bar{v}\|$ resp. $\lambda\|\bar{v}\|$, which together prove the claim.

▷ $\|P\bar{1}\| \leq \beta\|\bar{v}\|$.

Pf:

- By Cauchy-Schwarz we deduce:

$\langle e_B, \bar{v} \rangle \leqslant \|e_B\| \cdot \|\bar{v}\|$, where e_B is zero at $[n] \setminus B$ & one at B positions.

$\Rightarrow \quad 1 \leqslant \sqrt{\beta n} \cdot \|\bar{v}\|$

• Also, $\|P\bar{1}\| = \sqrt{\beta n \cdot \frac{1}{n^2}} = \sqrt{\beta/n}$.

$\Rightarrow \quad \|P\bar{1}\| = \beta \cdot \frac{1}{\sqrt{\beta n}} \leqslant \beta \cdot \|\bar{v}\|$. $\square$

$\triangleright$ $\|PA\bar{z}\| < \lambda \cdot \|\bar{v}\|$.

Pf:

• Since $\bar{z} \in \bar{1}^{\perp}$, we have $\|A\bar{z}\| \leqslant \lambda \cdot \|\bar{z}\|$.

$\Rightarrow \quad \|PA\bar{z}\| \leqslant \|A\bar{z}\| \leqslant \lambda \cdot \|\bar{z}\|$.

• We know that $\bar{v} = \bar{1} + \bar{z}$ is an orthogonal decomposition.

$\Rightarrow \|\bar{v}\|^2 = \|\bar{1}\|^2 + \|\bar{z}\|^2$

$\Rightarrow \quad \|\bar{z}\| < \|\bar{v}\|$

$\Rightarrow \|PA\bar{z}\| < \lambda \|\bar{v}\|$. $\square$

$\square$ (Claim)

- Once we know that the spectral norm of PAP is at most $(\beta+\lambda)$, we can estimate the matrix product:

(Cauchy-Schwarz)

$$\|(PA)^k P\bar{1}\|_1 \leq \sqrt{n} \cdot \|(PA)^k \cdot P\bar{1}\|$$
$$= \sqrt{n} \cdot \|(PAP)^k \cdot \bar{1}\|$$
$$< \sqrt{n} \cdot (\beta+\lambda)^k \cdot \|\bar{1}\|$$
$$= (\beta+\lambda)^k .$$

$\square$ (Thm)

- The above technique is strong enough to estimate the probability of being in B at specified steps:

<u>Corollary</u>: For $I \subseteq [0..k]$,

$$\Pr_{\text{walk in } G} [\, \forall i \in I,\ v_i \in B\,] < (\beta+\lambda)^{|I|-1} .$$

- Say, algorithm $M(x)$ uses r random bits and has error $\leq \beta$.

- We intend to employ an $(N=2^r, d, \lambda)$-expander G to walk.

  Let $B \subseteq \{0,1\}^r = V(G)$ be the bad vertices for $M(x)$, $|B| \leq \beta N$.

  Let $v_0, v_1, \ldots, v_k$ be the walk.

$\Rightarrow$ majority-vote of $\{M(x, v_i) \mid i\}$ is wrong iff $\exists I \subseteq [0 \ldots k]$, $|I| \geq \frac{k+1}{2}$ s.t. $\forall i \in I$, $v_i \in B$.

- By the union-bound & the Corollary, the latter event has Prob. $< 2^k \cdot (\beta+\lambda)^{\frac{k-1}{2}}$.

- Assuming $\beta + \lambda \leq 1/8$, we get the error-prob. $O(2^{-k/2})$ using only $(r + k \cdot \lg d)$ random bits.