Expanders (or Expansion)

- We now start the first topic in our list of pseudorandom constructions.
  - We want to construct a graph family that is very well-connected. (eg. distance $O(\log|V|)$).

- Application 1: Solve the problem of undirected graph connectivity in logspace (L or RL).
  - derandomize?

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

- Upath $\in P$.

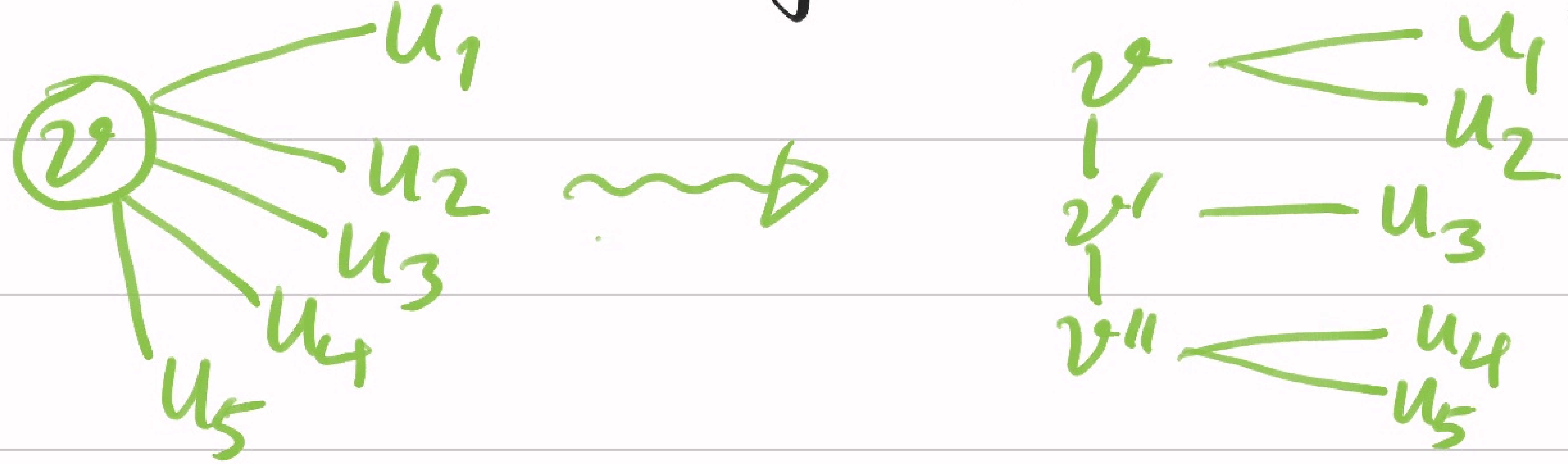
Theorem (Aleliunas, Karp, Lipton, Lovász, Rackoff '79):

$$\text{Upath} \in RL$$ (randomized-logspace-algo)

Proof: Idea- Consider adjacency matrix A & simulate a random walk on graph G as matrix powering.

- Suppose G is the given undirected graph with n vertices.
- We need G to be d-regular (i.e. $\forall v \in V(G)$, $deg(v)=d$).
- Eg. we can transform G to get $d=3$:

e.g.



▷ Apply this gadget on all the vertices, in logspace: $O(\lg n)$.

- Now on, assume G to be $d(=3)$-regular.
- On this we do a random walk, starting from s, of length $300 \cdot n^4 \lg n$.

▷ Random walk is implementable in $O(\lg n)$-space.

- Assume G to have self-loops: $(v,v) \in E(G)$, $\forall v \in V$.
- Defn: Let $A_{n\times n}$ be the normalized adjacency matrix of G, i.e. $A_{ij} := \#\text{edges}(i,j)/d$. A is symmetric stochastic matrix.

▷ $\forall i \in [n]$, $A_{ii} = 1/d$.

▷ A is symmetric, with entries in $\{0, 1/d\}$.

▷ A's row-sum, & column-sum, is 1.

- Idea: A transforms the probability vector $\bar{p} := (p_1, \dots, p_n)^T$, where $p_i :=$ probability of being at vertex i.

▷ At any stage of the walk: $\sum_{i=1}^{n} p_i = 1$.
(Initially, $p_i = 1$ for $i = s$ & 0 otherwise.)

▷ In one-step of the random-walk the prob. vector changes as: $\bar{p} \mapsto \bar{q} := A \cdot \bar{p}$.

Pf: • By definition, $q_i := Pr[\text{walk is at vertex } i]$

$$= \sum_{j=1}^{n} Pr[\text{walk at } i \mid \text{previous was } j] \times Pr[\text{prev} = j]$$

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

$$\Rightarrow \quad \bar{q} = A \cdot \bar{p}. \qquad \square$$

- Let $\bar{e}^s$ be the elementary vector with 1 at the s-th coordinate (& others 0).

▷ After ℓ steps of the random-walk, the prob. vector is $(A^\ell \cdot \bar{e}^s)$.

- Next qn: How large is $(A^\ell \cdot \bar{e}^s)_t = \Pr[\text{reaching } t \text{ in } \ell \text{ rnd. steps}]$?

- Idea: Study the magnitude by using the eigenvalues λ of A, as the main technical tool.
(i.e. $A \cdot v = \lambda v$)
eigenvectors v

Exercise: Symmetric stochastic $A \implies$ eigenvalues $\lambda_1, \ldots, \lambda_n$ are real & $|\lambda_n| \le |\lambda_{n-1}| \le \cdots \le |\lambda_1| = 1$.

- Denote the uniform-prob. vector $(1/n, \ldots, 1/n)^T =: \bar{1}$

▷ $A.\bar{1} = \bar{1}$. [Thus, 1 is an eigenval & $\bar{1}$ is eigenvec. of A.]

- Denote $\bar{1}^\perp := \{v \in \mathbb{R}^n \mid \langle v, \bar{1} \rangle = 0\}$ is a subspace.

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: • Pick an orthonormal basis $\{b_1 = \bar{1}, b_2, \ldots, b_n\}$ of $\mathbb{R}^n$ s.t. b_i is an eigenvector corresponding to λ_i, $\forall i \in [n]$.

$\Rightarrow \quad T^{\perp} = Sp_{\mathbb{R}}\{b_2, \dots, b_n\}$.

$\alpha_i \in \mathbb{R}$

$\Rightarrow$ Any vector $v \in T^{\perp}$ can be written as: $v = \sum_{i \geq 2} \alpha_i b_i$

$$\Rightarrow \quad Av = \sum_{i \geq 2} \alpha_i (A b_i) = \sum_{i \geq 2} (\alpha_i \lambda_i) b_i$$

$$\Rightarrow \quad \|Av\|^2 = \sum_{i \geq 2} (\alpha_i \lambda_i)^2 \Rightarrow \frac{\|Av\|^2}{\|v\|^2} = \frac{\sum \alpha_i^2 \cdot \lambda_i^2}{\sum \alpha_i^2} \leq \lambda_2^2$$

- Also, $A b_2 = \lambda_2 b_2 \Rightarrow \|A b_2\| / \|b_2\| = \lambda_2$.

$\Rightarrow \lambda(A) := \max \|Av\|$, over unit vectors in $T^{\perp}$, is exactly λ_2. $\square$

$\triangleright \quad \lambda(A^\ell) \leq \lambda(A)^\ell$.

Pf: • By defn of $\lambda(\cdot)$: $\|Av\| \leq \lambda(A)\cdot\|v\|$, $\forall v \in \bar{1}^\perp$.

• Also, $\langle Av, \bar{1}\rangle = \langle v, A\bar{1}\rangle = \langle v, \bar{1}\rangle = 0$, $\Rightarrow Av \in \bar{1}^\perp$.

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

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

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

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

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

Pf: • $A^\ell \bar{p} - \bar{1} = A^\ell \cdot (\bar{p} - \bar{1})$ & $\langle \bar{p}-\bar{1}, \bar{1}\rangle = \langle \bar{p}, \bar{1}\rangle - \langle \bar{1}, \bar{1}\rangle$
$= 1/n - 1/n = 0$.

$$\Rightarrow \|A^{\ell}\cdot(\bar{p}-\bar{1})\| \leq \lambda(A^{\ell})\cdot\|\bar{p}-\bar{1}\| \leq \lambda(A)^{\ell}\cdot\|\bar{p}-\bar{1}\|$$

- Define $p' := \bar{p}-\bar{1}$. $\Rightarrow \|\bar{p}\|^2 = \|p'\|^2 + \|\bar{1}\|^2$

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

$$\Rightarrow \|p'\| < 1.$$

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

▷ The further $\lambda(A)$ is from 1, the faster is the convergence of $A^{\ell}\bar{p}$ to $\bar{1}$.

Defn: $1-\lambda(A)$, or $1-\lambda(G)$, is called the spectral gap of graph G.

▷ We wish it large for expansion!

Lemma 2: $\forall$ d-regular, connected, n-vertex graph (with self-loops) : $1-\lambda(G) \geq 1/8dn^3$. ← inverse-poly in input size!

Proof: Idea – Use the norm interpretation of $\lambda(G)$: where A acts on $\mathbb{1}^\perp$.

- Let $u \in \mathbb{1}^\perp$ be a unit vector & $v := Au$.
  - We'll show: $1-\|v\|^2 \geq 1/4dn^3$.

    Thus, $\|v\|^2 \leq 1 - 1/4dn^3$.

    $\Rightarrow \|v\| \leq (1-1/4dn^3)^{1/2} < 1 - 1/8dn^3$.

▷ $1-\|v\|^2 = \sum_{i,j\in[n]} A_{ij}\cdot(u_i - v_j)^2$ [Quadratic form in the Laplacian of G]

Pf: $RHS = \sum A_{ij}\cdot u_i^2 - 2\sum A_{ij}u_i v_j + \sum A_{ij}\cdot v_j^2$

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

$$= \sum u_i^2 - 2\langle Au, v\rangle + \sum v_j^2 = \|u\|^2 - 2\langle v, v\rangle + \|v\|^2$$

$$= 1 - \|v\|^2 = LHS. \quad \square$$

- Thus, it suffices to show: $\exists i, j$, $A_{ij} \cdot (u_i - v_j)^2 \geq 1/4dn^3$.
- If $\exists i$, $(u_i - v_i)^2 \geq 1/4n^3$ then we are done.
  - So, assume: $\forall i$, $|u_i - v_i| < 1/2n^{1.5}$.
- Sort the coordinates of u: $\underset{\geq 0}{u_1} \geq u_2 \geq \dots \geq \overset{\leq 0}{u_n}$.

▷ $\sum u_i = 0$ & $\sum u_i^2 = 1$.

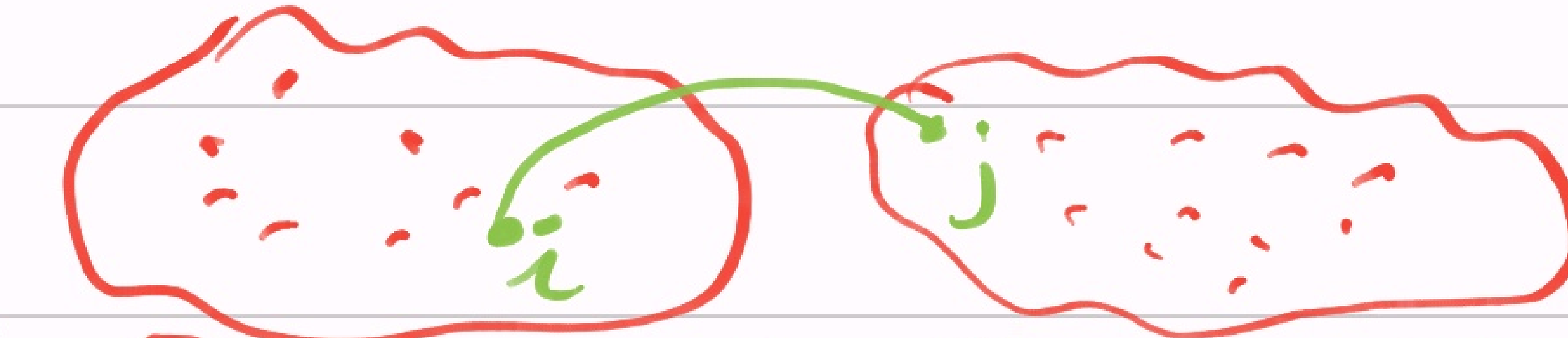
$\Rightarrow$ either $u_1 \geq 1/\sqrt{n}$ or $u_n \leq -1/\sqrt{n}$.

▷ $u_1 - u_n \geq 1/\sqrt{n}$.

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

$\Rightarrow \exists$ edge $(i,j) \in E(G)$ s.t.

$i \in [i_0]$ & $j \in [i_0]^c$.



$V(G) = [i_0] \sqcup [i_0+1 \dots n]$

$\triangleright \quad u_i - u_j > 1/n^{1.5}$ & $(i,j) \in E$.

$$\Rightarrow \quad A_{ij} \cdot (u_i - v_j)^2 \geq \frac{1}{d} \cdot \left(|u_i - u_j| - |u_j - v_j| \right)^2$$

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

$\Rightarrow \quad 1 - \|v\|^2 > 1/4dn^3$

$\Rightarrow \quad 1 - \lambda(G) > 1/8dn^3$. $\square$

Lemma 3: Let $\ell := 10dn^3 \lg n = 30n^3 \lg n$. If s,t are connected in G, then $\Pr[\text{rnd. walk reaches } t \text{ at the } \ell\text{-th step}] > 1/2n$.

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

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

$$\leq (1 - 1/8dn^3)^{10dn^3 \lg n} < e^{-5 \lg n/4} < 1/2n^{1.5}.$$

• By Cauchy-Schwarz inequality:

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

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

$\Rightarrow \Pr[\text{reaching } t \text{ at } \ell\text{-th step}] > 1/2n.$ $\square$

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

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

▷ $\ell := 40\,d n^4 \lg n = 120 n^4 \lg n$ makes error $< 1/4$.

- This rnd. walk is in logspace (rnd.), as we need to store the current vertex label; which has only $O(\lg n)$-bits.

$\Rightarrow$ Upath $\in$ RL.

(also outputs a path!)

$\square$

- Qn: Can it be derandomized?

This was an intriguing question for three decades; to solve it several tools were developed.

- Idea: Convert G to G' — a graph with constant spectral gap, so that $\ell = O(\lg n)$ suffices to reach t from s.

Then, one can exhaustively look for all $O(\lg n)$-length options from s, in $\mathbb{L}$. [$\because d=3$]

- G' motivates Expanders: 'highly'-connected graphs. We'll see two definitions.

Defn (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 $\{G_n\}_{n\geq 1}$ is s.t. $\forall n$, G_n is (n,d,λ)-expander.

– Alon-Boppana '86 showed that $\lambda(G) \geq 2\sqrt{d-1}/d$.

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

▷ Graphs with $\lambda = 2\sqrt{d-1}/d$ are called Ramanujan Graphs. Their explicit constructions are known due to (Lubotzky-Phillips-Sarnak '88).

$d = p^k + 1$, prime p.

Defn (Combinatorial): We call G an (n,d,ρ)-edge-expander if G is n-vertex, d-regular s.t.

$$\forall\, S \subseteq V(G) \text{ of } |S| \leq n/2,\ |E(S,\bar{S})| \geq \rho \cdot \underbrace{d \cdot |S|}_{\max}$$

edges $S \times \bar{S} \cap E(G)$

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

- Next, we show the equivalence of these two defns.

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

Theorem 2: G is an (n,d,ρ)-edge expander $\Longrightarrow$
" " " $(n,d,1-\rho^2/2)$-expander.

Cheeger's Inequality: $\frac{1-\lambda(G)}{2} \leq \rho(G) \leq \sqrt{2(1-\lambda(G))}$.
ρ (measures bottlenecks in a graph)

Pf. of Thm 1: • The #edges out of S are estimated by considering $Z := \sum_{i,j\in[n]} A_{ij} \cdot (x_i - x_j)^2$. ← Laplacian quadratic form

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

$\triangleright$ $\bar{x} \in T^{\perp}$.

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

$$= 0 + 0 + 2 \cdot \sum_{(i,j)\in S\times\bar{S}} A_{ij} \cdot (x_i - x_j)^2$$

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

- On the other hand, $Z = \sum A_{ij} x_i^2 - 2\sum A_{ij} x_i x_j + \sum A_{ij} x_j^2$

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

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

$[\, \|A\bar{x}\| \leq \lambda \cdot \|\bar{x}\|$ & $|\langle \bar{y}, \bar{x}\rangle| \leq \|\bar{y}\| \cdot \|\bar{x}\|. \,]$

$$\Rightarrow \quad \#E(S,\bar{S})\cdot(2n^2/d) = Z \geq 2\cdot\|\bar{x}\|^2\cdot(1-\lambda)$$
$$= 2(1-\lambda)\cdot\left(|S|\cdot|\bar{S}|^2+|\bar{S}|\cdot|S|^2\right)$$

$$\Rightarrow \quad \#E(S,\bar{S}) \geq \left(\frac{d}{2n^2}\right)\cdot 2(1-\lambda)\cdot |S|\cdot|\bar{S}|\cdot n = \frac{(1-\lambda)d}{n}\cdot|S|\cdot|\bar{S}|$$
$$\geq \frac{(1-\lambda)d}{n}\cdot\frac{n}{2}\cdot|S| = \left(\frac{1-\lambda}{2}\right)\cdot d\cdot|S|$$

$\Rightarrow \quad \rho(G) \geq (1-\lambda)/2$ &

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

Pf. of Thm2: • Assume G to be an (n,d,ρ)-edge-expander.

• We again estimate Z; use $\bar{x}$ = eigenvector of $\lambda_2(A)$.

- Pick $\bar{u}$: $A \cdot \bar{u} = \lambda_2 \cdot \bar{u}$ & $\bar{u} \in \mathbb{1}^\perp$ & $\bar{u} \neq \bar{0}$.

  $\Rightarrow$ $\bar{u}$ has +ve & −ve coordinates; let us collect them in $\bar{v}$ & $\bar{w}$ resp.

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

- Wlog $\bar{v}$ has $\leq n/2$ nonzero entries (else we use $-\bar{u}$).
- Consider $Z := \sum_{i<j\in[n]} A_{ij} \cdot \underbrace{(v_i^2 - v_j^2)}_{\geq 0}$. ← assume $v_1 \geq v_2 \geq \cdots \geq v_n \geq 0$.
- We'll show: Claim 1: $Z \geq \rho \cdot \|\bar{v}\|^2$ (use edge-expansion)

  Claim 2: $Z \leq \sqrt{2(1-\lambda_2)} \cdot \|\bar{v}\|^2$ (matrix analysis)

▷ The two claims will prove Theorem 2.

Pf. of Claim 1: • Recall in $\bar{v}$: $v_1 \geqslant v_2 \geqslant \cdots \geqslant v_n \geqslant 0$ &

$$v_i = 0, \quad \forall\, i > n/2.$$

• $Z = \sum_{i<j} A_{ij} \cdot (v_i^2 - v_j^2)$ [Idea: Relate to $E([k],[k+1..n])$]

$$= \sum_{i<j} A_{ij} \cdot \sum_{i \le k < j} (v_k^2 - v_{k+1}^2)$$

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

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

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

Pf. of Claim 2: • Z & λ_2 are fundamentally related.

Idea: Use $\langle A\bar{u}, \bar{v}\rangle$ & recalculate Z.

• $\langle A\bar{u}, \bar{v}\rangle = \langle \lambda_2 \bar{u}, \bar{v}\rangle = \langle \lambda_2 \bar{v} + \lambda_2 \bar{w}, \bar{v}\rangle = \lambda_2 \|\bar{v}\|^2$

• $\quad$ " $\quad = \langle A\bar{v}, \bar{v}\rangle + \langle A\bar{w}, \bar{v}\rangle \leq \langle A\bar{v}, \bar{v}\rangle$.

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

$$\Rightarrow \quad 1-\lambda_2 \geq \left(\|\bar{v}\|^2 - \langle A\bar{v}, \bar{v}\rangle\right) / \|\bar{v}\|^2$$

[$\rightarrow$ We want to "reach" Z.]

$\triangleright$ $2\left(\|\bar{v}\|^2 - \langle A\bar{v}, \bar{v}\rangle\right) = 2\|\bar{v}\|^2 - 2\sum A_{ij} v_i v_j$

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

$$= \sum_{i,j} A_{ij} \cdot (v_i - v_j)^2$$

$$\Rightarrow \quad 1-\lambda_2 \geq \left[\frac{\sum_{i,j} A_{ij}\cdot(v_i-v_j)^2}{2\cdot\|\bar{v}\|^2} \cdot \frac{\sum_{i,j} A_{ij}(v_i+v_j)^2}{\left[\sum_{i,j} A_{ij}\cdot(v_i+v_j)^2\right]} \right]$$

- Numerator estimate: $\geq \left(\sum_{i,j} A_{ij}\cdot|v_i^2-v_j^2|\right)^2$ [by Cauchy-Schwarz inequality]

$$= (2Z)^2 = 4Z^2.$$

- Denominator estimate:

$$D\,\frac{1}{2}\cdot\sum_{i,j} A_{ij}\cdot(v_i+v_j)^2 = \frac{1}{2}\sum A_{ij}\cdot(v_i^2+v_j^2) + \sum A_{ij}\cdot v_i v_j$$

$$= \|\bar{v}\|^2 + \sum_{i,j} A_{ij} v_i v_j \leq \|\bar{v}\|^2 + \frac{1}{2}\cdot\sum A_{ij}(v_i^2+v_j^2)$$

$$= 2\cdot\|\bar{v}\|^2.$$

$$\Rightarrow \quad \sum_{i,j} A_{ij} \cdot (v_i + v_j)^2 \leq 4 \cdot \|\bar{v}\|^2 .$$

Combining all inequalities: $1 - \lambda_2 \geqslant \dfrac{4 Z^2}{2\|\bar{v}\|^2 \cdot 4\|\bar{v}\|^2}$

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

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

$\Rightarrow$ Thus, Theorem 2 is proved.

$\square$

$\rightarrow$ Laplacian quadratic form $Z(G) := \sum_{i,j} A_{ij} \cdot (x_i - x_j)^2$.
It carries information about expansion & sparsest-cut!

Application — Error-reduction using (explicit) expanders.

- Recall that a problem $L \in BPP$ with an algorithm $M(x)$ of error-probability $\leq 1/3$, using r random bits, can also be solved with a much smaller error $= 2^{-k}$.

The naive way is to repeat $M(x)$, k-times using (rk) random bits. Qn: Can you do better?

→ We'll show that by "walking in an expander" we can reduce rnd. bits to $r + O(k)$.

additive!

Idea: • Start with an $(2^r, d, 0.1)$-expander graph G, for constant d. Assume that the neighbors of any vertex in G 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 $v_1, \ldots, v_k \in V(G)$.

• Use strings $v_0, v_1, \ldots, v_k \in \{0,1\}^r$ as "random" strings to run $M(x)$ $(k+1)$-times! ← pseudorandom?

• Finally, output the majority vote of the $(k+1)$ outputs.

• We'll show that error-prob $\leq 2^{-k}$, & we used only $(r + k \cdot \lg d) = r + O(k)$ random bits! $\ll (r \cdot k)$

- First, we bound the prob. of the rnd. walk, being confined to bad vertices B (eg. v_i's on which $M(x)$ is wrong).

Theorem (Ajtai, Komlós, Szemerédi, '87): Let G be an (n,d,λ)-expander & $B \subseteq V(G)$, $|B| = \beta \cdot n$. Then,

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

exp. small!

- Once we've this, we'll upper-bound the prob. of $(\geq 1/2)$ of $\{v_0, \ldots, v_k\}$ being in B.

Proof of Thm: • Let A be the normalized adjacency matrix of G.

- <u>Idea:</u> Express the probability as a <u>matrix product</u> (using the <u>submatrix</u> $A_{B\times B}$) & then analyze using <u>spectral-norm</u> of A & $|B|$.

- Let $\underline{P} := P_B$ be the $n\times n$ identity matrix with the rows corresponding to $[n]\setminus B$ set to 0.

  $\triangleright$ $P^2 = P$ & $P\cdot AP = A_{B\times B}$.

<u>Claim 1:</u> $\Pr_{\text{walk in } G}[\forall i, v_i \in B] = \|(PA)^k \cdot P\bar{\pi}\|_1$

<u>Pf:</u>

- The prob. of $v_0 \in B$ is $\|P\cdot\bar{\pi}\|_1$.
- Prob. of being <u>in B</u> after 1-step is $\|PA\cdot P\bar{\pi}\|_1$.
- Induct to k. $\square$

$\triangleright$ $(PA)^2 \cdot P \cdot \bar{1} = PA \cdot \underbrace{P}A \cdot P\bar{1} = PA\underbrace{P \cdot P}AP \cdot \bar{1} = (PAP)^2 \cdot \bar{1}$

$\triangleright$ $(PA)^k \cdot P\bar{1} = (PAP)^k \cdot \bar{1}$

- Now, we'll study the spectral norm of PAP, i.e. the factor by which it shrinks a vector.

Claim 2: $\forall \bar{v} \in \mathbb{R}^n$, $\|PAP \cdot \underbrace{\bar{v}}\| < (\beta + \lambda) \cdot \|\bar{v}\|$

Pf: • Assume that $\bar{v}$ is supported on B. (else, replace $\bar{v}$ by $P\bar{v}$ in the inequality. This cannot increase RHS.)

• Similarly, assume $\bar{v}$ to be non-negative & $\|\bar{v}\|_1 = 1$.

- Write $P\bar{v} = \bar{v} =: \alpha \cdot \bar{1} + \bar{z}$, for $\bar{z} \in \bar{1}^{\perp}$.
- Since $\langle n\bar{1}, \bar{v}\rangle = \langle (1,\dots,1)^T, \bar{v}\rangle = \sum v_i = 1$,

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

$\Rightarrow \bar{v} = \bar{1} + \bar{z}$.

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

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

— We bound these resp. by $\beta\|\bar{v}\|$ & $\lambda\|\bar{v}\|$, proving the claim.

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

Pf: • $\|P \cdot \bar{1}\| = \sqrt{\beta n \cdot \frac{1}{n^2}} = \sqrt{\beta/n}$. 1 in B-positions only

• On the other hand, $1 = \sum_{i \in B} v_i = \langle \bar{e}_B, \bar{v}\rangle \leq \|\bar{e}_B\| \cdot \|\bar{v}\|$

$\Rightarrow 1 \leq \sqrt{\beta n} \cdot \|\bar{v}\| \Rightarrow \|P \cdot \bar{1}\| \leq \beta \cdot \|\bar{v}\|$. $\square$

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

Pf: • Since $\bar{z} \in \bar{1}^{\perp}$, we have $\|A\bar{z}\| \leq \lambda \cdot \|\bar{z}\|$

$\Rightarrow \|PA\bar{z}\| \leq \|A\bar{z}\| \leq \lambda \cdot \|\bar{z}\|$

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

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

$\Rightarrow \|PAP \cdot \bar{v}\| < (\beta + \lambda) \cdot \|\bar{v}\|$. $\square$ (Claim 2)

• Since we now know that the spectral norm of PAP is $< (\beta+\lambda)$, we can estimate the matrix-product:

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

· The above technique is strong enough to estimate the prob. of being at B at specified steps (in the random walk).

e.g. $I = \{0, 2, 4\}$-th step you want to be in B,

the $\Pr_{\text{walk}}[\forall i \in I, v_i \in B] = \|PA \cdot A \cdot PA \cdot A \cdot P \cdot \mathbb{1}\|_1$.

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

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

(Exercise)

- Say, algorithm $M(x)$ uses r random bits & has error $\leq \beta$. $N := 2^r$.
  Define $B \subseteq \{0,1\}^r$ be the bad strings. $\triangleright$ $|B| \leq \beta \cdot N$

- Employ an (N, d, λ)-expander G to walk.
  $V(G) = \{0,1\}^r$; $B \subseteq V(G)$ are bad vertices.
- Let $v_0, v_1, \ldots, v_k$ be the walk.
- The majority-vote $\{M(x, v_i) \mid i \in [0..k]\}$ is wrong iff $[\exists I \subseteq [0...k], |I| \geq \frac{k+1}{2}$ s.t. $\forall i \in I, v_i \in B]$

$\triangleright$ $\Pr_{walk}[\text{—}] < 2^k \cdot (\beta+\lambda)^{(k+1)/2}$. Assuming $\beta+\lambda \leq 1/8$ we get error-prob $< 2^{-k/2}$; rnd-bits $\leq (r + k \lg d)$.