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 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:

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

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

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

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

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

Pf:

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

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

• 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)

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

$\square$ (Thm)

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

__Corollary:__ For $I \subseteq [0..k]$,

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

- 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.