# Lecture 17 10/22/2025

## Expanders and Random Walks

Expander graphs are almost magical graphs that have many applications in mathematics and Computer Science.

Defn: A multigraph $G = (V, E)$ is an $\alpha$-edge-expander if $|\delta(S)| \geq \alpha |S|$ for all $S \subseteq V$ with $|S| \leq \frac{|V|}{2}$.

$$\alpha(G) = \min_{S : |S| \leq \frac{|V|}{2}} \frac{|\delta(S)|}{|S|}.$$

The surprising fact is that a random 3 regular graph has expansion 0.18 with high probability.

Theorem [Bollobas] Let $d \geq 3$ be an integer and $\eta \in (0,1)$.

If $2^{4/d} < (1-\eta)^{1-\eta}(1+\eta)^{1+\eta}$

then a random $d$-regular graph has expansion $(1-\eta)\frac{d}{2}$.

Corollary: As $n \to \infty$ a random $n$ vertex $d$-regular graph has expansion $(1-\eta)\frac{d}{2}$ with high probability.

In particular for $d=3$ we can obtain expansion $0.18$.

The proof is via the probabilistic

method and not very difficult. Nevertheless it is somewhat technical.

Simpler proofs give weaker expansion property.

Although random regular graphs are expanders and one can generate them relatively easily, it is hard to compute the expansion. Therefore there have several works that construct expanders explicitly. Many of these are based on group theoretic constructions.

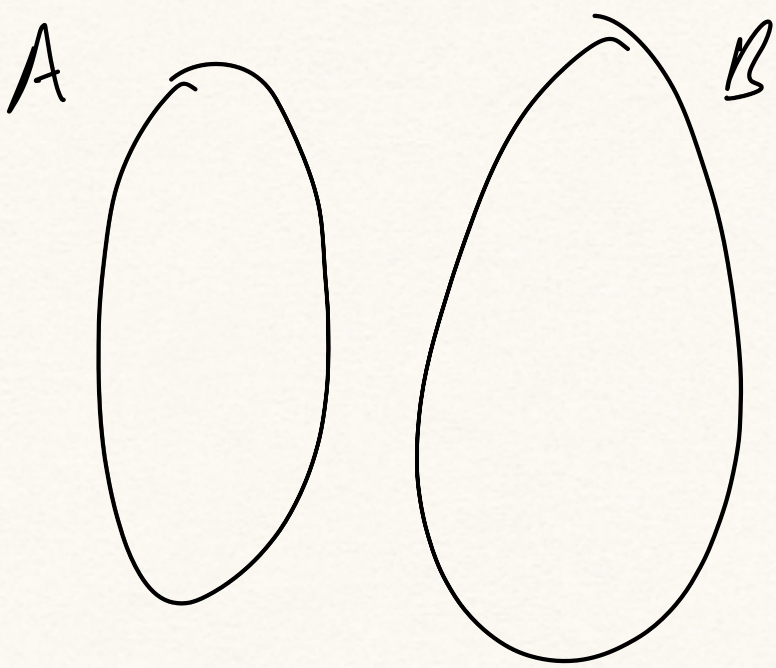
One of the early explicit constructions is given by Margulis and analyzed by Gabber and Galil.

Fix integer $m$ and let $n = 2m^2$.

We construct a graph on $n$ vertices. It is a bipartite graph with $A$ and $B$ with $|A| = |B| = m^2$.

$A = \{ u_{(r,s)} \mid r, s \in \mathbb{Z}_m \}$,

$B = \{ v_{(r,s)} \mid r, s \in \mathbb{Z}_m \}$.



For each vertex $u_{(x,y)}$ in $A$

we add 5 edges to vertices

$v_{(x,y)}$, $v_{(x,x+y)}$, $v_{(x,x+y+1)}$, $v_{(x+y,y)}$, $v_{(x+y+1,y)}$

Here addition is done mod $m$.

It can be shown that expansion

is $\frac{2-\sqrt{3}}{4}$.

A notion related to expansion is

<u>conductance</u>.

<u>Defn:</u> The conductance $\phi(G)$ of a

graph is

$$\min_{S : \mathrm{Vol}(S) \le \frac{\mathrm{Vol}(G)}{2}} \frac{|\delta(S)|}{\mathrm{Vol}(S)}$$

where $\mathrm{Vol}(S) = \sum_{u \in S} \deg(u)$.

Note that $G$ is $d$-regular then $\mathrm{Vol}(S) = d|S|$ and hence for those graphs $\alpha(G) = d\,\phi(G)$.

## Cheeger's Inequality

Recall that we did a spectral analysis of the convergence of random walks in undirected graphs.

Let $A_G$ be the adjacency matrix of $G$. Then the random walk matrix

$W = A_G D_G^{-1}$ where $D_G$ is the diagonal matrix with $D_{ii} = \deg(i)$.

The lazy walk matrix is

$$\frac{1}{2}(I + AD^{-1}).$$

If $G$ is $d$-regular then $W$ is symmetric. Otherwise we considered the normalized adjacency matrix

$$\mathcal{A}_G = D^{-\frac{1}{2}} A D^{-\frac{1}{2}}$$ and noted that

$$W = D^{\frac{1}{2}} \mathcal{A}_G D^{-\frac{1}{2}}$$ which implies

that $W$ is similar to the symmetric matrix $\mathcal{A}_G$. Note that $\mathcal{A}_G = A_G D^{-1}$ if $G$ is $d$- .

Let $\alpha_1 \geq \alpha_2 \ldots \geq \alpha_n$ be the real eigen values of $A_G$. Then

$1 = \alpha_1 > \alpha_2 \ldots \geq \alpha_n \geq -1$ if $G$ is connected (we assume wlog).

We saw that the random walk on $G$ converges in $O\left(\frac{\log \frac{n}{\varepsilon}}{\beta}\right)$ steps to a distribution that has $\varepsilon$ - total variation distance from the stationary distribution where

$\beta = \min(1 - \alpha_2, 1 - |\alpha_n|)$ is the spectral gap. For the lazy random walk $\beta = \frac{1-\alpha_2}{2}$.

How do we know when $\beta$ is not too small?

Cheeger's inequality allows us to bound conductance via another important matrix of graphs called the Laplacian.

$$L_G = D - A_G$$

The normalized Laplacian is

$\mathcal{L} = I - \mathcal{A}_G$ where $\mathcal{A}_G$ is the normalized adjacency matrix.

$\mathcal{L}_G$ and $\mathcal{L}$ are positive semi-definite matrices.

<u>Observation</u> Let $0 = \lambda_1 < \lambda_2 \cdots \leq \lambda_n$ be the eigen values of $\mathcal{L}$.

Then $\lambda_i = 1 - \alpha_i$ where $\alpha_1, \ldots, \alpha_n$ are the eigenvalues of $A_G$.

Thus $1 - \alpha_2 = \lambda_2$.

<u>Theorem [Cheeger]</u> For any graph

$$\frac{\lambda_2}{2} \leq \phi(G) \leq \sqrt{2\lambda_2}.$$

Corollary: Suppose $G$ is $d$-regular.
Let $1 = \alpha_1 > \alpha_2 \dots \geq \alpha_n$ be eigenvalues of $A_G D^{-1}$. Then

$$d \cdot \frac{1-\alpha_2}{2} \leq \alpha(G) \leq d\sqrt{2(1-\alpha_2)}.$$

Proof: For $d$-regular graphs
$\Phi(G) = d\,\alpha(G)$ and also
we have $1-\alpha_2 = \lambda_2$. $\square$

Thus if we have a constant degree expander $1-\alpha_2 \geq \left(\frac{\alpha(G)}{d}\right)^2$.
$\Rightarrow$ random walk mixes in $O(\log n)$ steps.

# Randomized Complexity Classes

Recall P is the set of decision problems that have a deterministic poly-time algorithm.

RP stands for randomized poly-time.

$L \in RP \iff \exists$ a poly-time randomized algorithm A such that $\forall$ inputs $x \in \Sigma^*$

(i) if $x \notin L$ $A(x)$ says NO

(ii) if $x \in L$ $A(x)$ says YES with probability $\geq \frac{1}{2}$.

One sided error.

co-RP is one sided error for $x \notin L$.

$L \in$ co-RP iff $\bar{L} \in$ RP.

BPP is the set of languages that admit poly-time randomized algorithms that can make 2-sided errors.

$L \in BPP \Rightarrow \exists$ a randomized polytime algorithm $A$ s.t.

$\forall x \in \Sigma^*$

(i) if $x \in L$ $A(x)$ outputs YES with prob $\geq \frac{3}{4}$

(ii) if $x \notin L$ $A(x)$ outputs YES with prob $\leq \frac{1}{4}$.

RP and BPP algorithms are called Monte Carlo algorithms. They seem in polytime but can make a mistake

Clear that

$$P \subseteq RP \subseteq BPP$$

ZPP is the set of problems for which there is a randomized algorithm A such that $\forall x \in \Sigma^*$

(i) if $x \in L$ $A(x)$ returns YES

(ii) if $x \notin L$ $A(x)$ returns NO

(iii) The expected run time of A on $x$ is $\leq p(|x|)$ for some fixed polynomial $p$.

<u>Claim:</u> ZPP = RP $\cap$ co-RP.

<u>Proof:</u> Exercise.

Las Vegas algorithms.

# Error reduction in randomized algorithms

Easy lemma based on repetition

**Lemma:** Suppose $L \in RP$ and $A$ is a randomized poly time algorithm for $L$. Suppose on input $x$, $A$ takes $n$ random bits and is correct with prob $\frac{1}{2}$. Then by running $A$ $k$ times we can reduce error to $\frac{1}{2^k}$.

Now suppose we have $L \in BPP$. How do we reduce error?

We run A $k$ times independently and take majority vote of the outputs.

<u>Lemma</u>: Error is $\leq \frac{1}{c^k}$ for some fixed $c$.

Use Chernoff bounds..

Repeating $k$ times independently requires $kn$ random bits where $n$ is the number of random bits for each run. Is this optimal? Can we do better?

Turns out that one can reduce

error to $\frac{1}{2^k}$ by using only $O(n + k)$ bits!

How? By random walks on expanders..

Let $N = 2^n$. We will assume that we can construct implicitly a constant degree expander on $N$ vertices. Typically we will not be able to construct expanders for all $N$ but we will not worry about that technicality for now.

Let $G = (V, E)$ be the expander with expansion $\alpha$ and degree $d$. We assume $d = O(1)$ and $\alpha = \Omega(1)$.

Each vertex $v \in V$ corresponds to a $n$-bit binary string.

We will assume that given $v$ we can find the $d$-neighbors of $v$ in $poly(n)$ time. For example in the explicit Margulis/Gabber-Galil expander we can do this. Thus we can implement a random walk on $G$ for $t$ steps in $poly(t, n)$ time and the number of random bits required to implement $t$-step walk is $O(t)$ since each step requires only $O(1)$ bits to pick a random neighbor. We will assume walk in $G$ is ergodic, otherwise we can do the lazy random walk.

For both RP and BPP amplification we do the following.

1. Pick a uniformly random $v_1 \in V$
2. Do a random walk for $t$ steps and let $v_1, v_1, v_2, \ldots, v_t$ be the vertices.

3. Let $r_1, r_1, \ldots, r_t$ be the $n$-bits random strings associated with $v_1, \ldots, v_t$ be $r_1, r_2, \ldots, r_t$

4. Let $b_i = A(x, r_i)$ be the output of $A$ on input $x$ with random string $r_i$

<u>Lemma:</u> Let $G = (V, E)$ be an undirected graph whose random walk matrix has spectral gap $\gamma$. Consider a $t$-step random walk $v_1, v_2, \ldots, v_t \in V$ where $v_1 \in V$ is chosen uniformly at random. For any set $B \subset V$.

$$\Pr\left[\{v_1, v_2, \ldots, v_t\} \subseteq B\right] \leq \left(\mu + (1-\beta)\right)^t .$$

where $\mu = \dfrac{|B|}{|V|}$.

Assume lemma is true. Now consider the algorithm we had using random walks on expanders with each vertex being a $n$-bit random string.

Suppose we have $L \in RP$ and $A$ on input $x$ outputs No if $x \notin L$ and outputs YES with prob $\geq 1-\mu$ for $x \in L$.

Let $b_1, b_2, \ldots, b_t$ be the outputs of $A(x, r_1) \ldots, A(x, r_t)$.

The algorithm outputs Yes if any of the outputs is Yes. Otherwise it outputs No.

Suppose $x \notin L$ then it is clear that $A$ will output No.

Suppose $x \in L$. What is the prob it will output No.

$$\leq (\mu + (1-\beta))^t.$$

Expander gives us $\beta$ is a fixed constant. By basic repetition we can ensure that $\mu \leq \frac{\beta}{2}$.

$\Rightarrow \quad \mu + 1 - \beta \leq 1 - \frac{\beta}{2}$

If we choose $t$ s.t.

$\left(1 - \frac{\beta}{2}\right)^t \leq \frac{1}{2^k}$ we will

have failure probability $\leq \frac{1}{2^k}$.

$\Rightarrow \quad t = O(k)$ suffices

the $O(\ )$ notation hides

a $\frac{1}{\beta}$ dependence which we

assume is a fixed constant.

$\square$.

## Proof of the Lemma

Let $W$ be the random walk matrix. $W = AD^{-1}$ and since $G$ is $d$-regular $W$ is symmetric.

Let $1 = \alpha_1 > \alpha_2 \cdots \cdots >, \alpha_n > -1$ be the eigen values of $W$.

$B \subset V$ and $\mu = \dfrac{|B|}{|V|}$.

Let $P$ be a $|V| \times |V|$ diagonal matrix with $P_{vv} = 1$ iff $v \in B$

So for any vector $\bar{x} \in R^{|V|}$

$$P\bar{x} = \sum_{i \in B} x_i .$$

$P$ is like the identity matrix.

What is the probability that $v_1, v_2, \ldots, v_t \in B$:

We claim it is $\|(PWP)^t p^{(0)}\|_1$.

Here since $v_1$ is chosen uniformly at random $p^{(0)} = \frac{\bar{1}}{n}$ where $n = |V|$.

$PWP$ is also a symmetric matrix.

Recall $W$ can be written as

$\sum_{i=1}^{n} \alpha_i \, z_i^T \oplus \bar{z}_i$ where $\bar{z}_1, \bar{z}_2, \ldots, \bar{z}_n$ are the orthonormal eigen vectors

$\alpha_1 = 1$ and $\bar{z}_1 = \frac{\bar{1}}{\sqrt{n}}$ since we normalize to unit vectors.

<u>Lemma:</u> For any vector $\bar{y}$

$$\| P W P \bar{y} \|_2 \leq (\mu + (1-\beta)) \| \bar{y} \|_2 .$$

<u>Proof:</u> We can assume that $y_i = 0$ if $i \notin B$ because it can only help the inequality. We can also assume $\bar{y} \geq 0$. We can then assume that $\sum_{i=1}^{n} y_i = 1$ by scaling $\bar{y}$ since it doesn't change inequality..

Thus $\bar{y}$ can be written as

$\bar{y} = \bar{u} + \bar{z}$ where $\bar{u} = \frac{\bar{1}}{n}$ is the uniform distribution and $\bar{z}$ is orthogonal to $\bar{u}$.

$$PWP\bar{y} = PW\bar{y} = PW(\bar{u}+\bar{z})$$

(because $\bar{y}$ is in support of $B$)

$$= PW\bar{u} + PW\bar{z}$$

$$= P\bar{u} + PW\bar{z}$$

By $\Delta$le inequality

$$\|PWP\bar{y}\|_2 \le \|P\bar{u}\|_2 + \|PW\bar{z}\|_2$$

First we show

$$\|P\bar{u}\|_2 \le \mu \|\bar{y}\|$$

$$\frac{1}{n^2}+\frac{1}{n^2}\cdots\frac{1}{n^2}$$

$$\|P\bar{u}\|_2 \le \left(\mu n \cdot \frac{1}{n^2}\right)^{\frac{1}{2}}$$

$\beta n$

$$\le \left(\frac{\mu}{n}\right)^{\frac{1}{2}}.$$

Since $P$ has at most $\mu n$ 1's on diagonal.

By Cauchy-Schwartz and the fact that $\bar{y}$ has support at most $\mu n$.

$$1 = \sum_{i=1}^{n} y_i \leq \sqrt{\mu n}\ \|y\|_2$$

$$\Rightarrow \|P\bar{u}\|_2 \leq \sqrt{\frac{\mu}{n}} \leq \mu \cdot \|\bar{y}\|_2 . \quad (1)$$

Now consider

$$\|PW\bar{z}\|_2 \leq \|W\bar{z}\|_2 \text{ since}$$

$P$ is a contraction in $l_2$.

Since $\bar{z}$ is orthogonal to $\bar{u}$ the fixed eigen vector of $W$ and

$$|\alpha_2|, \ldots, |\alpha_n| \leq 1-\beta .$$

$$\|W\bar{z}\|_2 \leq (1-\beta)\|\bar{z}\|_2 .$$

Thus $\|PAP\bar{y}\|_2 \leq (\mu + (1-\beta))\|\bar{y}\|_2$.

$\Rightarrow$ max eigen value of $PWP$

$$\leq \mu + (1-\beta).$$

Now we prove the lemma.

We have $\|(PAP)^{t}\bar{u}\|_1 \leq \sqrt{n}\,\|PAP\bar{u}\|_2$

$$\leq \sqrt{n}\,(\mu+(1-\beta))^{t}\|u\|_2$$

$$\leq \sqrt{n}\,(\mu+(1-\beta))^{t}\frac{1}{\sqrt{n}}$$

$$\leq (\mu+(1-\beta))^{t}.$$

$\square$

BPP derandomization is a bit more technical to prove.

We state a Chernoff bound for walks in expanders.

Theorem

Let $G=(V,E)$ be a regular graph.
Let $v_1, v_2, \ldots, v_t$ be vertices of a random walk on $G$ where $v_1$ is chosen uniformly at random from $V$.
Let $f: V \to [0,1]$ be any bounded function. Then

$$\Pr\left[\frac{1}{t}\sum_{i=1}^{t} f(v_i) \geq E[f] + \varepsilon + (1-\beta)\right] \leq e^{-\Omega(\varepsilon^2 t)}.$$

Here $E[f] = E[f(v)]$ where $v$ is chosen uniformly at random. A $\beta$ is the spectral gap. Note $\beta = 1-\alpha_2$ if $G$ is ergodic.

Using the above powerful theorem one can generalize the majority vote algorithm for BPP to obtain error reduction to $\frac{1}{2^k}$ using $O(n+k)$ random bits.