Lectures on Expanders	Course Instructor: V. Arvind
Lecture 1	
Lecturer: V. Arvind	*Scribe: Ramprasad Saptharishi*

1 Introduction

1.1 Motivation

We would like to build a family of graphs that are "sparse" but "highly" connected. Some conditions that we would want our graphs have are

1. The graph should be computable in time polynomial in the number of vertices
2. The graph should be edge-checkable in time poly logarithmic in the number of vertices.
3. In the context of $d-$regular graphs, $A(x, i) = y$ if y is the i^{th} neighbour of x, and this A should be polynomial time in its input length.

1.2 Graph Parameters

Sparseness:
As for the graphs being sparse, the graphs we are looking for shall be d regular, for "small" d, and thus property 3 would be applicable.

Connectivity:
A possible connectivity measure is the measure how much the graph "expands".

Definition 1. *A graph G_n is said be a (k, α) vertex expander if for all subsets S of vertices such that $|S| \leq k$, the neighbourhood of S, denotes by $\Gamma(S) \geq \alpha|S|$.*

This is a natural notion of connectivity or expansion that we would want (α "large" *implies* "expands well"), but unfortunately, checking if a graph is a (k, α) is $coNP$ complete! Hence we need a different notion of expansion.

2 Spectral Expansion

2.1 Associated Eigenvalues

Let $G(V, E)$ be a d-regular multigraph, where there could be more than 1 edge between vertices. This could be thought of as a graph with non-negative integral weights, where the weight of edge ij denotes the number of edges between i, j.

Let A be the *normalised adjacency matrix* of G

$$A_{ij} = \frac{\text{number of edges between } i, j}{d}$$

A is a real, symmetric, doubly stochastic matrix[1]. And by the spectral theorem, the eigenvalues of this matrix are real, and there exists an eigenbasis. Let the eigenvalues be $\lambda_1, \lambda_2, \cdots, \lambda_n$ such that $|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_n|$

Suppose λ is any eigenvalue of A and v an associated eigenvector.

Let $|v_i| = \max_{1 \leq j \leq n} |v_j|$

$$\begin{aligned}
|\sum_{j=1}^{n} A_{ij} v_j| &= |\lambda||v_i| \\
&\leq \sum_{j=1}^{n} |A_{ij}||v_j| \\
&\leq |v_i| \sum_{j=1}^{n} |A_{ij}| \\
&= |v_i|
\end{aligned}$$

Hence $|\lambda| \leq 1$

And since A is a stochastic matrix, clearly $(1, 1, \cdots, 1)$ is an eigenvector whose eigenvalue is 1. Speaking in terms of probability distributions, it makes more sense to say that the uniform distribution $u = \left(\frac{1}{n}, \frac{1}{n}, \cdots, \frac{1}{n}\right)$ is an eigenvector with eigenvalue 1.

Thus $\lambda_1 = 1$.

2.2 Other Eigenvalues

$\lambda_1 = 1$ for all graphs, we have to inspect the other eigenvalues to see if they tell us anything about the graph's expansion properties. Firstly, we need to see if any other $|\lambda_i| = 1$.

[1]rows and columns entries are non-negative and add up to 1

First let's examine if any $\lambda_i = 1$.

Lemma 2. *The dimension of the eigenspace of* $1 =$ *number of connected components of* G

Proof. Let $x \perp u$ and $Ax = x$. Let $x_i = \max x_j$, $X = \{k | x_k = x_i\}$.

$$\sum_{j=1}^{n} A_{ij} x_j = x_i = \sum_{j, A_{ij} \neq 0} A_{ij} x_j$$

which is a convex combination of x_j's. Thus $A_{ij} \neq 0 \implies x_i = x_j$, which implies no edges go out of the set X. Thus X is a component of G.

And if there are k connected components, dimension of eigenspace of 1 is atleast k (uniform distribution over that component is an eigenvector). And since every connected component has only u as its eigenvector, the dimension of the eigenspace of 1 is exactly k. □

Now for the case when $\lambda_i = -1$

Lemma 3. *For a connected* $d-$*regular graph* G*,*

$$G \text{ is bipartite } \iff -1 \text{ is an eigenvalue}$$

Proof. Look at the graph G^2, whose edge relation correspond to paths of length 2 in G. Note that the adjacency matrix of this graph has to be A^2 and hence the eigenvalues of G^2 has to be $\{\lambda_i^2\}_{i=1}^n$

If G is connected and bipartite, G^2 has 2 component, and thus G^2 has an eigenvalue 1 with multiplicity 2. And since G is connected, the eigenvalue 1 of G has multiplicity 1, which implies -1 is an eigenvalue of G.

Conversely. let -1 be an eigenvalue of G and x the eigenvector chosen such that $\max x_j = \max |x_j| = x_i$(say).

And repeating the argument in the earlier lemma,

$$\sum_{j=1}^{n} A_{ij} x_j = -x_i = \sum_{j, A_{ij} \neq 0} A_{ij} x_j$$

which is a convex combination of x_j. And hence, $A_{ij} \neq 0 \implies x_j = -x_i$.

Now let $X = \{k | x_k = x_i\}$. Since $x_j = x_i \implies A_{ij} = 0$, the induced subgraph on X is empty.

Since the graph is connected, let x_l be a vertex in V
X that is connected to some x_m in X. And since it is connected to some vertex in X, $A_{ml} \neq 0 \implies x_m = -x_i$

$$\sum_j A_{lj} x_j = -x_l = x_i$$

And this is possible only when $x_j = x_i$ wherever $A_{lj} \neq 0$, which means all the neighbours of x_m are in X - the graph is bipartite.

□

Hence, if G is connected, and not bipartite, $|\lambda_2| < 1$. This $|\lambda_2|$ is called the spectral expansion of G.

Definition 4. *For G, a connected $d-$regular non-bipartite graph, the spectral expansion of G is $|\lambda_2| = \lambda_2(G)$*

We shall soon see that $1 - \lambda_2(G)$ is large $\implies$ good vertex expansion.

Theorem 5.

$$\lambda_2(G) = \max_{x \perp u} \frac{\|Ax\|_2}{\|x\|_2} = \max_{x \perp u} \frac{|\langle Ax, x\rangle|}{|\langle x, x\rangle|}$$

Proof. Let $u = v_1, v_2, \cdots, v_n$ be an eigenbasis. For any $x \perp u$,

$$\begin{aligned} x &= \alpha_2 v_2 + \alpha_3 v_3 + \cdots \alpha_n v_n \\ \langle Ax, Ax\rangle &= \sum_{i=2}^{n} \alpha_i^2 \lambda_i^2 \leq \alpha_2^2 \|x\|_2 \end{aligned}$$

and the equality is attained when x is the eigenvector of λ_2

The proof of the other equality is exactly the same.

□

Fact 6. $|v|_\infty \leq \|v\|_2 \leq |v|_1 \leq \sqrt{n}\,\|v\|_2$

3 Random Walks on Expanders

3.1 Mixing Time and Spectral Expansion

Let π be a probability distribution over the vertices. Since A is a stochastic matrix, $A\pi$ is also a probabilistic distribution[2].

Definition 7. *G has mixing time $t(n)$ if for all probability distributions π*

$$\left|A^{t(n)}\pi - u\right|_\infty \leq \frac{1}{2n}$$

[2]this is the probabilistic distribution over the vertices after 1 step is taken according to π

Theorem 8. *"Good Expanders have small mixing time"*

Proof. Let $\lambda_2(G) = \lambda$ and π be any probability distribution.

$$\pi = \alpha_1 u + \alpha_2 v_2 + \cdots \alpha_n v_n$$

Note that $\langle \pi, u \rangle = \frac{1}{n}$ and hence $\alpha_1 = 1$. Hence

$$\begin{aligned} A^l \pi - u &= \alpha_2 \lambda_2^l v_2 + \cdots + \alpha_n \lambda_n^l v_n \\ \therefore \left\| A^l \pi - u \right\|_2^2 &= \alpha_2^2 \lambda_2^{2l} + \cdots + \alpha_n^2 \lambda_n^{2l} \\ &\leq \lambda_2^{2l} \left(\alpha_2^2 + \cdots + \alpha_n^2 \right) \\ &\leq \lambda_2^{2l} \left\| \pi - u \right\|_2^2 \end{aligned}$$

And since $\|pi\|_2^2 = \|u\|_2^2 + \left\| u^\perp \right\|_2^2$, we have $\|pi\|_2^2 \geq \|\pi - u\|_2^2$.
Hence we now have,

$$\left| A^l \pi - u \right|_\infty \leq \left\| A^l \pi - u \right\|_2 \leq \lambda_2^l \left\| \pi \right\|_2 \leq \lambda_2^l \leq \frac{1}{2n}$$

Hence $l = \log_{\frac{1}{\lambda_2}} 2n$
Thus for small λ_2, mixing time is small. □

4 Undirected Graph Connectivity is in RL

$$UGAP = \{(G, s, t) | \exists s - t \text{ path in } G\}$$

Definition 9. *RL is the class of languages L that are accepted by a polytime randomized logspace turing machine with onesided error.*

Note that the polynomial running time requirement is critical, since we have a stream of random bits, the machine could run for much longer. Randomized logspace machines running for more than polynomial time arguably have more computational power than RL machines.

Theorem 10. *$UGAP \in RL$*

We need some bounds before we get into the proof.

4.1 Bounds on $\lambda_2(G)$

Let G be any arbitrary connected, non-bipartite regular graph. Assuming that there are self loops on all the nodes of G, G^2 will now be a regular, non-bipartite connected graph with all its eigenvalues non-negative. Let the normalized adjacency matrix of G^2 be A and let E be the multiset of edges.

$$\begin{aligned}
\lambda_2(G^2) &= \max_{x\perp u, \|x\|=1} |\langle Ax, x\rangle| \\
&= \max_{x\perp u, \|x\|=1} \left|\sum_{i,j} A_{ij}x_i x_j\right| \\
&= \max_{x\perp u, \|x\|=1} \left|\sum_{(i,j)\in E} \frac{2}{d}x_i x_j\right| \\
&= \max_{x\perp u, \|x\|=1} \left|\frac{1}{d}\sum(x_i^2 + x_j^2) - \frac{1}{d}\sum(x_i - x_j)^2\right| \\
&= \max_{x\perp u, \|x\|=1} \left|\frac{1}{d}d\,\|x\|^2 - \frac{1}{d}\sum(x_i - x_j)^2\right| \\
\therefore 1 - \lambda_2 &= \min_{x\perp u, \|x\|=1} \left|\frac{1}{d}\sum_{(i,j)\in E}(x_i - x_j)^2\right|
\end{aligned}$$

Let x be the optimal vector for the above equation. Since $x \perp u$, let $0 < x_a = maxx_i, x_b = minx_i < 0$. Since $\|x\| = 1$, either $x_a \geq \frac{1}{\sqrt{n}}$ or $x_b \leq \frac{-1}{\sqrt{n}}$. Let P be the shortest path from a to b in G^2.

$$\therefore (x_a - x_b) = \sum_{(i,j)\in P}(x_i - x_j) \geq \frac{1}{\sqrt{n}}$$

$$\begin{aligned}
1 - \lambda_2(G^2) &\geq \sum_{(i,j)\in P}(x_i - x_j)^2 \\
&\geq \frac{1}{d|P|}\left(\sum_{(i,j)\in P}|x_i - x_j|\right)^2 \\
&\geq \frac{1}{dn}|x_a - x_b|^2 \geq \frac{1}{dn^2}
\end{aligned}$$

$$\begin{aligned} \therefore \lambda_2(G^2) &\leq 1 - \frac{1}{dn^2} \\ \implies \lambda_2(G) &\leq 1 - \frac{1}{2dn^2} \end{aligned}$$

where d is the degree of G^2, the square of the degree of G.

Thus, $\lambda_2(G) \leq 1 - \frac{1}{poly(n)}$.

4.2 Proof of Theorem 10

Replace every node of degree k by a k cycle, and add self loops to make it a regular graph, and add self loops on all the nodes.

We know that $\lambda_2(G) \leq 1 - \frac{1}{n^4}$. Suppose A is the normalized adjacency matrix. Then,

$$\left| A^{n^5}\pi - u \right|_\infty \leq \lambda_2^{n^5} \leq \left(1 - \frac{1}{n^4}\right)^{n^5} \leq \frac{1}{2n}$$

Looking at the t-th index,

$$\begin{aligned} \left| (A^{n^5}\pi)_t - \frac{1}{n} \right| &\leq \frac{1}{2n} \\ \implies (A^{n^5}\pi)_t \geq \frac{1}{2n} \end{aligned}$$

Which means,

$$\Pr[\text{on a random walk, you don't hit } t \text{ in } n^5 \text{ steps}] \leq 1 - \frac{1}{2n}$$

This error can be pushed down to the desired limit in logspace. □

Lectures on Expanders	Course Instructor: V. Arvind
Lecture 2	
Lecturer: V. Arvind	*Scribe: Ramprasad Saptharishi*

5 Amplification of success in RP

Let $L \in RP$, accepted by a randomized algorithm A with one-sided error bounded by $\frac{1}{2}$. We shall use an expander graph to boost the error probability by using fewer random bits compared to the majority vote which uses mk random bits to push the error down to 2^{-k}.

Assume that for inputs of length n, the machine takes $m = n^{O(1)}$ random bits. Consider $G(V, E)$, a $(2^m, d, \lambda)$ expander, explicitly given[3].

For $x \in L$, define $B = \{r \in \Sigma^m | A(x, r) = 0\}$. And by the error bound of A, we know that $|B| \leq 2^{m-1}$

Our algorithm is going to be the following:

1. Pick a vertex r_0 at random
2. Take a random walk for t steps starting at r_0. Let the visited nodes be $r_0, r_1, \cdots r_t$.
3. Use these r_i's as random strings to A and output "YES" if and only if atleast one of them say "YES".

Now the question boils down to asking "What is the probability that after t steps, we are confined to B?"

Theorem 11. *If G is a $(2^m, d, \lambda)$ expander, and $B \subseteq V$ such that $|B| \leq \mu|V|$, then*

$$\Pr[r_0, r_1, \cdots, r_t \in B] \leq \left(\mu + (1-\mu)\lambda^2\right)^{\frac{t}{2}}$$

And with the theorem, if $\mu = \frac{1}{2}$, we have the probability to be bounded by $\left(\frac{1+\lambda^2}{2}\right)^{\frac{t}{2}}$, which is 2^{-ct} for a constant c.

Hence, in order to push the down to 2^{-k}, you want t to be $O(k)$. And for a random walk for k steps, you only need $m + O(k)\log d$ random bits!

Now, the proof of the theorem is all that's left to justify the amplification.

[3]given x and i outputs y which is the i-th neighbour of x and runs in time $poly(m)$

5.1 Proof of Theorem 11

Let $N = 2^m$ and P be the projector on B, that is

$$\left[\begin{array}{c|c} I_{BxB} & 0 \\ \hline 0 & 0 \end{array}\right]_{N\times N}$$

Note that $|Pu|_1 = \Pr[r_0 \in B]$. Infact one can extend this to higher powers by the following claim.

Claim 12. $\left|P(AP)^i u\right|_1 = \Pr[r_0, r_1, \cdots, r_i \in B]$

Proof. The proof is just simple induction. We just saw the base case when $i = 0$. Assume that for some i

$$\left|P(AP)^i u\right|_1 = \Pr[r_0, r_1, \cdots, r_i \in B]$$

Now $A(P(AP)^i u)_j = \Pr[\text{the first } i \text{ steps are confined in } B \text{ and the last step takes it to } j]$. And by just summing over all j in B, we have

$$\left|P(AP)^{i+1} u\right|_1 = \Pr[r_0, r_1, \cdots, r_{i+1} \in B]$$

which proves the inductive step. □

Now we would like to bound $\left|P(AP)^t u\right|_1$ for the proof.

Claim 13. *Let x be any vector in,*

$$\|APx\|_2 \leq \sqrt{\mu + (1-\mu)\lambda^2} \cdot \|x\|_2$$

And once we have this, we can just take $x = u$ and we would have

$$\left|P(AP)^t u\right|_1 \leq \left|(AP)^t u\right|_1 \leq \sqrt{N}\left(\mu + (1-\mu)\lambda^2\right)^{\frac{t}{2}} \sqrt{N} = \left(\mu + (1-\mu)\lambda^2\right)^{\frac{t}{2}}$$

which proves theorem 11.

Proof. Let $y = Px$, and $y = y^{\|} + y^{\perp} = \alpha u + y^{\perp}$; note that $\alpha = \sum y_i$

$$\begin{aligned} \|Ay\|_2^2 &= \left\|Ay^{\|}\right\|_2^2 + \left\|Ay^{\perp}\right\|_2^2 \\ &= \left\|y^{\|}\right\|_2^2 + \left\|Ay^{\perp}\right\|_2^2 \\ &\leq \left\|y^{\|}\right\|_2^2 + \lambda^2 \left\|y^{\perp}\right\|_2^2 \\ &= \left\|y^{\|}\right\|_2^2 + \lambda^2 \left(\|y\|_2^2 - \left\|y^{\|}\right\|_2^2\right) \end{aligned}$$

Now

$$\begin{aligned}\frac{\alpha^2}{n} = \left\|y^{\parallel}\right\|_2^2 &= \frac{\left(\sum_{i\in B} y_i\right)^2}{n} \\ &\le \frac{\left(\sum_{i\in B} y_i^2\right)|B|}{n} \\ &= \|y\|_2 \,\mu\end{aligned}$$

Hence,

$$\|Ay\|_2^2 \le \left(\mu + \lambda^2(1-\mu)\right)\|y\|_2^2 \le \left(\mu + \lambda^2(1-\mu)\right)\|x\|_2^2$$

and that completes the proof of the claim □

... and also the proof of theorem 11 □

6 Spectral Expander $\implies$ Vertex Expander

Recall definition 1 of a (k, α) expander:
For all subsets of vertices S such that $|S| \le k$, $\Gamma(S) \ge \alpha|S|$.

Now we shall show that a "good" spectral expander is also a "good" vertex expander.

Theorem 14. *If $G(V,E)$ is a (n,d,λ) spectral expander, then for every $\alpha > 0$, G is an $\left(\alpha n, \frac{1}{(1-\alpha)\lambda^2+\alpha}\right)$ vertex expander.*

Proof. Let $S \subseteq V$ such that $|S| \le \alpha n$. Suppose π is any distribution over the vertices, it can be written as $u + u^{\perp}$.

$$\langle \pi, \pi\rangle = \frac{1}{n} + \|\pi - u\|_2^2$$

Also,

$$\begin{aligned}\langle \pi, \pi\rangle &= \sum_{i\in supp(\pi)} \pi_i^2 \\ &\ge \frac{\left(\sum \pi\right)^2}{|supp(\pi)|} \qquad \text{(Cauchy Schwarz)} \\ &= \frac{1}{|supp(\pi)|}\end{aligned}$$

Suppose π was the uniform distribution on S, then note that $\langle \pi, \pi \rangle = \frac{1}{|S|}$. Hence,

$$\|\pi - u\|_2^2 = \frac{1}{|S|} - \frac{1}{n}$$

Since $supp(A\pi) = \Gamma(S)$,

$$\begin{aligned}
\frac{1}{|\Gamma(S)|} &\leq \langle A\pi, A\pi \rangle = \frac{1}{n} + \|A\pi - u\|_2^2 \\
&\leq \frac{1}{n} + \lambda^2 \|\pi - u\|_2^2 \\
&= \frac{1}{n} + \lambda^2 \left(\frac{1}{|S|} - \frac{1}{n} \right) \\
\implies \frac{|S|}{|\Gamma(S)|} &\leq \frac{|S|}{n} + \lambda^2 \left(1 - \frac{|S|}{n} \right) \\
&= \frac{|S|}{n} \left(1 - \lambda^2 \right) + \lambda^2 \\
&\leq \alpha \left(1 - \lambda^2 \right) + \lambda^2
\end{aligned}$$

Therefore,

$$\frac{|\Gamma(S)|}{|S|} \geq \frac{1}{\alpha (1 - \lambda^2) + \lambda^2} = \frac{1}{\lambda^2 (1 - \alpha) + \alpha}$$

□

6.1 Lower Bounds on λ

Theorem 14 tells much more than an implication.

For any d regular graph, the vertex expansion of this graph is atmost d.

$$\begin{aligned}
\implies \frac{1}{\alpha + (1 - \alpha) \lambda^2} &\leq d \\
\implies \lambda^2 (1 - \alpha) &\geq \frac{1}{d} - \alpha
\end{aligned}$$

Taking α close to 0, we see that $\lambda = \Omega(\frac{1}{\sqrt{d}})$.

Infact there are better bounds known, Alon and Bopanna show that

$$\lambda \geq \frac{2\sqrt{d-1}}{d} - o(1)$$

Ramanujam graphs get very close to this optimal[4].

[4]they have $\lambda = \frac{2}{\sqrt{d-1}} - o(1)$

7 Random Graphs as Expanders

Instead of looking at general random graphs, we shall restrict ourselves to bipartite graphs and show that a random bipartite graph is a "good" *left expander.*

Definition 15. *A bipartite multigraph $G(L \cup R, E)$ is a (d, k, α) left expander if every vertex on L has degree d, and for all subsets S of vertices in L such that $|S| \leq k$, $|\Gamma(S)| \geq \alpha|S|$*

Random bipartite graphs are chosen in the following sense, for every vertex $v \in L$ randomly pick d vertices from R with repitition. For simplicity of notation, let us call the set of possible multigraphs $\mathcal{G}_{n,d}$.

Theorem 16. *For every n and $d \leq n$, there exists an $\alpha > 0$ such that random $G \in \mathcal{G}_{n,d}$ is a $(d, \alpha n, d-2)$ left expander with probability greater than $\frac{1}{2}$*

Proof. Let $S \subseteq L$, such that $|S| = k < \alpha n$, we shall estimate the $\Pr_G[|\Gamma(S)| < (d-2)|S|]$.

For every vertex $v \in L$, we chose d neighbours, which is kd elements picked from L. Thus, we want to estimate the probability that there are atleast $2k$ repititions. There are $\binom{kd}{2k}$ places where the collisions can occur and each collision with probability $\frac{kd}{n}$.

$$\therefore Pr_G[|\Gamma(S)| < (d-2)|S|] \leq \binom{kd}{2k}\left(\frac{kd}{n}\right)^{2k}$$

Summing over all S,

$$\begin{aligned}
\sum_{k=1}^{\alpha n} \binom{n}{k}\binom{kd}{2k}\left(\frac{kd}{n}\right)^2 k &\leq \sum_{k=1}^{\alpha n}\left(\frac{ne}{k}\right)^k\left(\frac{kde}{2k}\right)^{2k}\left(\frac{kd}{n}\right)^{2k} \\
&= \sum_{k=1}^{\alpha n}\left(\frac{kd^2e^3}{4n}\right)^k \\
&\leq \sum_{k=1}^{\alpha n}\left(\frac{\alpha d^2 e^3}{4}\right)^k
\end{aligned}$$

And clearly for $\alpha < \frac{1}{d^2e^3}$ this probability can be bounded by half. $\square$

8 Explicit Constructions

The earliest explicit constructions of expander graphs were given by [Margulis,Gabber-Galil], [Lubotzky,Sarnak] but the contructions are fairly complex, looks at certain subsets of matrix groups.

[Reingold,Vadhan,Wigderson] used "zig-zag products" to construct expanders, we shall be looking at them in the next lecture. Gramov had used this zig-zag products earlier, though the novelty is attibuted to [RVW]. Zig-zag products seem to mimic the semi-definite over groups.

Alon et al gave another "not-so-difficult" construction for expanders, infact he said something more.

Theorem 17 (Alon/Roichman)**.** *There exists a constant c such that for every finite group G, a random set of $c \log n$ elements define a "good" expander in the Cayley graph on the vertices.*

Lectures on Expanders	Course Instructor: V. Arvind
Lecture 3	
Lecturer: V. Arvind	*Scribe: Ramprasad Saptharishi*

In this lecture we shall be discussing the paper "'Entropy Waves', the zig-zag produt and new constant degree expanders" by Reingold, Vadhan and Wigderson, which appeared in the Annals of Mathematics $'02$.

9 The Rotation Map

Let G be an N vertex D regular graph. The rotation map is a map $Rot_G : [N] \times [D] \to [N] \times [D]$, defined as follows.

If i^{th} edge of vertex v is w, as a j^{th} neighbour, then

$$Rot_G(v, i) = (w, j)$$

Note that this map is also an involution. This map defines the graph, and we would want this to be efficient ($poly(\log N, \log D)$ computable, in this lecture).

10 Graph Products

We shall now inspect various graphs products possible and the parameters of the graph.

10.1 Powering

Let G be a (N, D, λ) expander, given by the rotation map Rot_G. Then its i^{th} power, G^t is given by the following rotation map:

$$Rot_{G^t}(v_0, (k_1, k_2, \cdots, k_t)) = (v_t, (l_t, \cdots, l_1))$$

if and only if there exists $v_1, \ldots, v_{t-1}$ such that

$$\begin{aligned} Rot_G(v_0, k_1) &= (v_1, l_1) \\ Rot_G(v_1, k_2) &= (v_2, l_2) \\ &\vdots \\ Rot_G(v_{t-1}, k_t) &= (v_t, l_t) \end{aligned}$$

And easy to see that Rot_{G^t} is efficiently computable, and infact the adjacency matrix of G^t is A^t. Hence, G^t is a (N, D^t, λ^t) expander.

10.2 Tensoring

G_1 is a (N_1, D_1, λ_1) expander, and G_2 is a (N_2, D_2, λ_2) expander and let Rot_{G_1} and Rot_{G_2} be the corresponding rotation maps.

The rotation map of $G_1 \otimes G_2$ is defined by moving parallel on G_1 and G_2.

$$Rot_{G_1 \otimes G_2}((v, w), (i, j)) = \big((v', w'), (i', j')\big)$$

if and only if $Rot_{G_1}(v, i) = (v', i')$ and $Rot_{G_2}(w, j) = (w', j')$.

Now, it is easy to see that the normalized adjacency matrix of this graph, $A_{G_1 \otimes G_2} = A_{G_1} \otimes A_{G_2}$, the tensor product of the corresponding matrices[5]

The eigenbasis will also be the tensor products of the eigenbases of the two matrices, and hence the eigenvalues will be the products of the eigen values. And since 1 is an eigen value for both A_1 and A_2, the second largest eigenvalues is $\max(\lambda_1, \lambda_2)$.

Thus, $G_1 \otimes G_2$ is a $(N_1 N_2, D_1 D_2, \max(\lambda_1, \lambda_2))$ expander.

Both the products blows up the degree of the final graph, which is not desired. We want a family of graphs with constant degree and good spectral gap[6].

11 The Zig-Zag Product

Let G_1 be a (N, D, λ_1) expander and G_2 be a (D, d, λ_2) expander, with rotation maps Rot_{G_1} and Rot_{G_2}

Define the the graph $G_1 ⓩ G_2$ as follows:

- $V(G_1 ⓩ G_2) = [N] \times [D]$, replace every vertex in G_1 by a cloud of vertices in G_2, since the degree of G_1 matches with vertex size of G_2, this can be done.

- An edge in $G_1 ⓩ G_2$ is defined by a three step walk, 1 move in the G_2 cloud, take and edge of G_1 and move to another cloud, 1 move in the new cloud. More formally,

[5] each i, j-th entry of A_1 is replaced by the block $(A_1)_{i,j} \cdot A_2$

[6] $1 - \lambda(G)$

$$((v,k),(w,l)) \in E[(G_1 ⓩ G_2)]$$

if, there exists numbers k', l' such that

$$\begin{aligned} (k,k') &\in E(G_2) \\ (l,l') &\in E(G_2) \\ Rot_{G_1}(v,k') &= (w,l') \end{aligned}$$

So $G_1 ⓩ G_2$ is a $\left(ND, d^2, \lambda_3\right)$ expander.

Theorem 18 (Zig-Zag Theorem)**.** *For G_1 and G_2 considered above, $G_1 ⓩ G_2$ is a $\left(ND, d^2, \lambda_3\right)$ expander where,*

1. $\lambda_3 \leq \lambda_1 + \lambda_2 + \lambda_2^2$
2. *If $\lambda_1 < 1$ and $\lambda < 1$, then $\lambda_3 < 1$*

We shall prove this later.

11.1 Intuition Behind this

To be filled up soon

12 A Constant Degree Expander Family

Our base graph H would be a $\left(D^8, D, \lambda\right)$ expander for a constant D, which we shall explicitly construct later.

The family $\{G_t\}$ is defined as follows:

$$\begin{aligned} G_1 &= H^2 \\ G_2 &= H \otimes H \\ \forall t > 2, \quad G_t &= \left(G_{\lceil \frac{t-1}{2} \rceil} \otimes G_{\lfloor \frac{t-1}{2} \rfloor}\right)^2 ⓩ H \end{aligned}$$

Claim 19. *G_t is a $\left(D^{8t}, D, \lambda_t\right)$ expander, where $\lambda_t = \lambda + O(\lambda^2)$, and whose rotation map is computable in time polynomial in $(t, \log N, \log D)$ with $poly(t)$ queries to the rotation maps in the recursion.*

Proof. The ambiguity is only in λ of G_2, it's clear that the vertex size of G^t is D^{8t} and that the parameters match for zig-zag.

$\lambda_1 = \lambda^2 \leq \lambda + c\lambda^2$, and $\lambda_2 = \lambda \leq \lambda + c\lambda^2$, we shall now proceed by induction.

Let $\mu_t = \max_i \lambda_i = \max(\lambda_t, \mu_{t-1})$. We know that μ_1 and μ_2 are upper bounded by $\lambda + c\lambda^2$. Assume by induction that $\mu_{t-1} \leq \lambda + c\lambda^2$.

Now, $G_t = K \textcircled{z} H$, where K is the chunk in the definition. Note that $\lambda_k \leq \mu_{t-1}^2$. Hence by the Zig-Zag theorem, we know that

$$\begin{aligned} \lambda_t &\leq \mu_{t-1}^2 + \lambda + \lambda^2 \\ &\leq (\lambda + c\lambda^2)^2 + \lambda + \lambda^2 \end{aligned}$$

We want this to be less than $\lambda + c\lambda^2$ for some c. It's easy to see that if $\lambda \leq \frac{1}{5}$, then $c = 5$ is good enough.

Thus we have a uniform family of constant degree expanders, with good spectral gap. $\square$

Also note that in the earlier lecture we showd that $\lambda \leq \frac{2}{\sqrt{D}}$, and hence

$$\lambda_t \leq \lambda + c\lambda^2 \leq \frac{2}{\sqrt{D}} + \frac{4c}{D} \leq \frac{c}{\sqrt{D}}$$

And thus $\lambda_t = O\left(\frac{1}{(deg(G))^{1/4}}\right)$.

12.1 An explicit construction for H

Let $q = p^t$, some prime power, and $\mathbb{F}_q$ be the associated field. Our graph AP_q is going to have the vertex set $V = \mathbb{F}_q \times \mathbb{F}_q$.

As for the edge set of the graph, for every vertex $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$, define the set of vertices adjacent to (a, b) as $L_{a,b}$ where

$$L_{a,b} = \{(x, y) | y = ax - b\}$$

And since $|L_{a,b}| = q$, we have a q regular graph.

Claim 20. *AP_q is a $\left(q^2, q, \frac{1}{\sqrt{q}}\right)$ expander.*

Proof. Let M eb the normalized adjacency matrix of AP_q. M^2 is a $q^2 \times q^2$ matrix. And note that

$$M^2_{(a,b),(c,d)} = \frac{1}{q^2} \left| L_{a,b} \bigcap L_{c,d} \right| \tag{1}$$

If (x, y) is a common point, then

$$\begin{pmatrix} a & -1 \\ c & -1 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

When $a \neq c$, the matrix is of rank 1 and hence by equation 1

$$M^2_{(a,b),(c,d)} = \frac{1}{q^2}$$

.
Suppose $a = c$, if $b \neq d$, there are no solutions and hence $M^2_{(a,b),(c,d)} = 0$.
If $a = c$ and $b = d$, there are q points in common and hence $M^2_{(a,b),(c,d)} = \frac{1}{q}$

Thus the $M' = q^2 M^2$ has the following form

$$M' = \begin{pmatrix} qI_q & J_q & \cdots & J_q \\ J_q & qI_q & \cdots & J_q \\ \vdots & & \ddots & \\ J_q & \cdots & J_q & q_I q \end{pmatrix}$$

or in other words,

$$M' = (I_q \otimes qI_q + (J_q - I_q) \otimes J_q)$$

where J_q is the $q \times q$ matrix with every entry being a 1.

The only eigenvalue of $I_q \otimes qI_q$ is q.

As for the other sum, $J_q - I_q$ has eigenvalue $q - 1$ with multiplicity 1 and -1 with multiplicity $q - 1$.

And J_q has eigenvalue q with multiplicity 1 and -1 with multiplicity $q - 1$. Hence $(J_q - I_q) \otimes J_q$ has eigen value $q(q - 1)$ with multiplicity 1, 0 with multiplicity $q(q - 1)$ and $-q$ with multiplicity $q - 1$.

Hence M' has eigenvalue q^2 with multiplicity 1, q with multiplicity $q(q - 1)$ and 0 with multiplicity $q - 1$.

Hence, clearly, the second largest eigenvalue of M' is atmost q, and hence the second largest eigenvalue of M is atmost $\frac{1}{\sqrt{q}}$ □

Now let $AP^1_q = AP_q \otimes AP_q$, which gives a $\left(q^4, q^2, \frac{1}{\sqrt{q}}\right)$ expander.

Define

$$AP^i_q = AP^{i-1}_q ⓩ AP_q$$

And then we have the following claim, which is easy to prove.

Claim 21. *AP^i_q is a $\left(q^{2(i+1)}, q^2, \frac{2i}{\sqrt{q}}\right)$ expander.*

And with this, if we were to choose $i = 7$, and $q > 70^2$, we have a $H = AP^7_{5000}$ as our $(D^8, D, \frac{1}{5})$ expander.

Lectures on Expanders	Course Instructor: V. Arvind

Lecture 4

Lecturer: V. Arvind — *Scribe: Ramprasad Saptharishi*

13 Overview

We saw that the zig-zag product gave us a uniform family of expanders. In the next two lectures we shall prove Reingold's Theorem.

First let us look at the rotation map of the zig-zag product as an algorithm.

$Rot_{G_1 ⓩ G_2}$:

Input: $((v,k),(i,j))$

$$\begin{aligned} (k',i') &:= Rot_{G_2}(k,i) \\ (w,l') &:= Rot_{G_1}(v,k') \\ (l,j') &:= Rot_{G_2}(l',j) \end{aligned}$$

Output: $((w,l),(j',i'))$

Notice that this is a logspace algorithm and requires just $O(1)$ extra space apart from storing the 4 vertices in consideration; this would crucial in Reingold's proof.

14 Proof of the Zig-Zag Theorem (18)

We shall prove only one of the results stated in the previous lecture.

We have to study the second largest eigenvalue of $G_1 ⓩ G_2 = G$, for which we need to look at the normalized adjacency matrix of G. Let the normalised adjacency matrix of G_2 be A, and let P be a permutation matrix defining the rotation map of G_1.

Every edge of G consists of a three step walk, the first one being a walk in one of the v clouds that are expanded to a G_2. Thus that step can be represented by the matrix $B = I_N \otimes A$.

Thus the transition matrix of G is simply $Z = BPB$.

In order to analyse the spectral gap of Z, let $f \in \mathbb{R}^{ND}, \|f\|_2 = 1, f \perp 1_{ND}$. We want to show that

$$|\langle f, Zf\rangle| \leq \lambda_1 + \lambda_2 + \lambda_2^2$$

Let $f = f^{\|} + f^{\perp}$, where $f^{\|}$ is a vector such that

$$f^{\|}_{(v,i)} = \frac{1}{D}\sum_{j=1}^{D} f(v,j) = \alpha_v$$

which makes it locally uniform in each cloud G_2, hence $Bf^{\|} = f^{\|}$. And, it also ensures that

$$\sum_{v,i} f^{\|}_{(v,i)} = \sum_{v,j} f_{(v,i)} = 0$$

and hence $f^{\|}$ and $f^{\perp}$ are orthogonal to 1_{ND}.

Note that since BPB is symmetric, $\langle f^{\perp}, BPBf^{\|}\rangle = \langle f^{\|}, BPBf^{\perp}\rangle$. We then have,

$$\begin{aligned}
|\langle f, BPBf\rangle| &= \left|\langle f^{\|}, BPBf^{\|}\rangle + 2\langle f^{\|}, BPBf^{\perp}\rangle + \langle f^{\perp}, BPBf^{\perp}\rangle\right| \\
&\leq \left|\langle f^{\|}, BPBf^{\|}\rangle\right| + 2\left|\langle f^{\|}, BPBf^{\perp}\rangle\right| + \left|\langle f^{\perp}, BPBf^{\perp}\rangle\right| \\
&= (1) + (2) + (3)
\end{aligned}$$

where $(1) = \left|\langle f^{\|}, BPBf^{\perp}\rangle\right|, (2) = 2\left|\langle f^{\|}, BPBf^{\perp}\rangle\right|, (3) = \left|\langle f^{\perp}, BPBf^{\perp}\rangle\right|$

Bounding (1)

$$\begin{aligned}
(1) &= \left|\langle f^{\|}, BPBf^{\|}\rangle\right| \\
&= \left|\langle Bf^{\|}, PBf^{\|}\rangle\right| \\
&= \left|\langle f^{\|}, Pf^{\|}\rangle\right|
\end{aligned}$$

Now

$$\begin{aligned}
\langle f^{\|}, Pf^{\|}\rangle &= \sum_{(v,i)}\sum_{(w,j)} P_{(v,i),(w,j)} f^{\|}_{(v,i)} f^{\perp}_{(w,j)} \\
&= \sum_{(v,i)}\sum_{(w,j)} P_{(v,i),(w,j)} \alpha_v \alpha_w \\
&= \sum_{(v,w)\in E} D\alpha_v\alpha_w
\end{aligned}$$

And if we were to choose $g = \left(\sqrt{D}\alpha_{v_1}, \sqrt{D}\alpha_2, \cdots, \sqrt{D}\alpha_{v_N}\right)$, the above sum is just $\langle g, Ag\rangle$. Now $g \perp 1_N$ and $\|g\|_2 = \left\|f^{\|}\right\|_2$. Hence

$$(1) = |\langle g, Ag\rangle| \leq \lambda_1 \|g\|_2 = \lambda_1 \left\|f^{\|}\right\|_2 \leq \lambda_1$$

Bounding (2)

Since $\sum_i f^{\|}_{(v,i)} = \sum_i f_{(v,i)}$ for all v, it forces that $\sum_i f^{\perp}_{(v,i)} = 0$, or $f^{\perp}_v \perp 1_D$, the projection of $f^{\perp}$ on v.

And hence

$$\begin{aligned} \left\|Af^{\perp}_v\right\|_2 &\leq \lambda_2 \left\|f^{\perp}_v\right\|_2 \\ \implies \left\|Bf^{\perp}\right\|_2 &\leq \lambda_2 \left\|f^{\perp}\right\|_2 \end{aligned}$$

Thus,

$$\begin{aligned} (2) &= 2\left|\langle f^{\|}, BPBf^{\perp}\rangle\right| \\ &= 2\left|\langle Bf^{\|}, PBf^{\perp}\rangle\right| \\ &= 2\left|\langle f^{\|}, PBf^{\perp}\rangle\right| \\ &\leq 2\left\|f^{\|}\right\|_2 \left\|PBf^{\perp}\right\|_2 \\ &= 2\left\|f^{\|}\right\|_2 \left\|Bf^{\perp}\right\|_2 \\ &\leq 2\lambda_2 \left\|f^{\|}\right\|_2 \left\|f^{\perp}\right\|_2 \end{aligned}$$

[7]By the AM-GM inequality, $2\left\|f^{\|}\right\|_2 \left\|f^{\perp}\right\|_2 \leq \left\|f^{\|}\right\|_2^2 + \left\|f^{\perp}\right\|_2^2 = \|f\|_2^2$
And hence,

$$(2) \leq \lambda_2 \|f\|_2 \leq \lambda_2$$

[7]we used some other method in class first, but this seemed to be an easier proof

Bounding (3)

$$
\begin{aligned}
(3) &= \left|\langle f^{\perp}, BPBf^{\perp}\rangle\right| \\
&= \left|\langle Bf^{\perp}, PBf^{\perp}\rangle\right| \\
&\leq \left\|Bf^{\perp}\right\|_2 \cdot \left\|PBf^{\perp}\right\|_2 \\
&= \left\|Bf^{\perp}\right\|_2^2 \\
&\leq \lambda_2^2 \left\|f\right\|_2^2 \\
&\leq \lambda_2^2
\end{aligned}
$$

Thus, $\lambda(G_1 ⓩ G_2) \leq \lambda_1 + \lambda_2 + \lambda_2^2$ □

15 Towards Reingold's Theorem

Theorem 22 (Reingold)**.** *$UGAP \in L$*

Instead of looking at $s - t$ connectivity over general graphs, we shall see that if the connected component containing s was a λ-spectral expander for some constant $\lambda < 1$, then we can check connectivity in L

First, we shall expand every vertex to a cycle, so that we get a D regular graph.

Let A be the adjacency matrix of G. We know that the mixing time of $l = O(\log_{\frac{1}{\lambda}} N) = O(\log N)$. Thus for any distribution over the connected component of s,

$$\left|A^l e_s - u_s\right|_\infty \leq \frac{1}{2N}$$

and in particular, $(A^l e_s)_t \geq 12N$ if it is inside the connected component. Hence, if there exists a path from s to t, the path is of length atmost $O(\log N)$.

But how does one enumerate all paths of length $O(\log N)$? The naive method of remembering all vertices in the path would cost you $O(\log^2 N)$ space. But since the graph is D regular for some constant D, it suffices to remember the out-edge number! Thus, the space you need to try out all paths of length $O(\log N)$ would be $O(\log D, \log N) = O(\log N)$, and this gives us the logspace algorithm.

Reingold's theorem basically forces every graph G to be transformed of one of the above category.

For any $G = (N, D, \_)$ graph,

1. Pick H, a small $\left(D^{16}, D, \frac{1}{2}\right)$ expander.
2. $G_0 = G, G_i = (G_{i-1} \textcircled{z} H)^8$
3. Thus, G_i is a $\left(ND^{16i}, D^{16}, \_\right)$ graph.

Looking at the connected component containing s, turns out that

$$\lambda(G_i) \leq \max[\lambda(G_{i-1})^2, \frac{1}{2}]$$

And now, choosing $i = l = 5 \log N$ or so, we have

$$\lambda \leq \left(1 - \frac{1}{N^4}\right)^{2^l} \leq \frac{1}{2}$$

and this reduces to the earlier case which is solvable in logspace.

The heart of the proof is to show that the rotation maps of G_i's can be computed in logspace.[8]

[8] though it seems like we need to make $O(\log N)$ recursive calls, the amortized cost of computing the rotation map is still $O(\log N)$

Lectures on Expanders	Course Instructor: V. Arvind
Lecture 5	
Lecturer: V. Arvind	*Scribe: Ramprasad Saptharishi*

16 Overview

We are on our way to showing that $UGAP$ or undirected graph connectivity can be computed in logspace. Last class we saw that if the connected component containing s was an expander with some constant positive spectral gap, then we can check connectivity it in logspace.

We shall now see how we can "expanderize" graphs in logspace, and thus solve $UGAP$ in logspace.

17 Reingold's Algorithm

1. Choose a graph H that's a $\left(D^{16}, D, \frac{1}{2}\right)$ expander for some constant D.
2. Convert G into a D^{16} regular graph G' with $N' = N^2$ many vertices. We shall elaborate on how to do this shortly.
3. Let $G_0 = G'$, and for all $i \geq 1$,

$$G_i = \left(G_{i-1} \textcircled{z} H\right)^8 = T_i(G', H)$$

Thus, G_i would be a $\left(N^2 D^{16i}, D^{16}, \_\right)$ expander.

Now we have the following claims

Claim 23. *If S is a connected component of G,*

$$T_i(G'|_S, H) = T_i(G', H)|_{S \times [D^{16}]^i}$$

This basically tells us that the products respect connected components, and hence connectivity.

Claim 24. *For all $i \geq 1$, if λ_i is the second largest eigenvalue of the connected component of G_i containing s, then*

$$\lambda_i \leq \max\left(\lambda_{i-1}^2, \frac{1}{2}\right)$$

With this claim, if we choose $i = O(\log N) = l$, we have

$$\lambda_i = \left(1 - \frac{1}{poly(N)}\right)^{2^i} < \frac{1}{2}$$

And then our problem would reduce to the case we discussed last lecture.

But we need one more crucial claim, that allow us to take the products.

Claim 25. *Rot_{G_l} can be computed in logspace from $Rot_{G'}$ and Rot_H*

So with the three claims, the algorithm is complete and we are done by just applying the algorithm discussed last class for constant spectral gap!

17.1 Converting G to a D^{16}-regular graph G'

Let the vertex set of G' be $[N] \times [N]$.

$$Rot_{G'} : ([N] \times [N]) \times [D^{16}] \to ([N] \times [N]) \times [D^{16}]$$

is defined as follows

- For all $(v, w) \in [N] \times [N]$,

  $$((v, w), 1) \mapsto ((v, w'), 2)$$

  where $w' = w + 1$ if $w < N$ and $w' = 1$ when $w = N$,

- For all $(v, w) \in [N] \times [N]$,

  $$((v, w), 2) \mapsto ((v, w'), 1)$$

  where $w' = w - 1$ if $w > 1$ and $w' = N$ when $w = 1$,

- If $(v, w) \in E$, then

  $$((v, w), 3) \mapsto ((w, v), 3)$$

  else

  $$((v, w), 3) \mapsto ((v, w), 3)$$

- For all $3 < i \leq D^{16}$

  $$((v, w), i) \mapsto ((v, w), i)$$

This clearly gives us a D^{16} regular graph which doesn't alter connected components of the G.

17.2 Proof of Claim 23

Since this is a property that we would expect graph products to preserve, let us examine all graph products.

Suppose G_1 and G_2 are two disjoint components of a graph, and for any G_3 chosen appropriately for the products to be well defined,

- $(G_1 \sqcup G_2)^t = G_1^t \sqcup G_2^t$

  This is clear since powering cannot add cross edges between components

- $(G_1 \sqcup G_2) \otimes G_3 = (G_1 \otimes G_3) \sqcup (G_2 \otimes G_3)$

  This again is clear since parallel edges can't create crosses between components.

- $(G_1 \sqcup G_2) \text{ⓩ} G_3 = (G_1 \text{ⓩ} G_3) \sqcup (G_2 \text{ⓩ} G_3)$ The step on the clouds doesn't allow you to move across vertices of the bigger graph. And one can move across vertices of the bigger graphs only using the edges of the bigger graph. Hence this is also clear.

In the zig-zag product case, through the eigenvalues of the product graph, we know that the resulting graph is connected if the components of the product are connected.

And with this, the proof of the claim is just a simple inductive argument on i where the products preserve the components and the powering gives the extra $[D^{16}]$ to the LHS. $\square$

17.3 Proof of Claim 24

For this we need a stronger bound on the eigenvalue of the zig-zag product, the proof of this shall not be done here but can be found in [ReingoldVadhanWigderson] where they discuss the zig-zag product.

Theorem 26. *If $\lambda_1, \lambda_2, \lambda_3$ are the spectral expansions of G_1, G_2 and $G_1 \text{ⓩ} G_2$ respectively, then*

$$\lambda_3 \leq 1 - \frac{1}{2}(1 - \lambda_2^2)(1 - \lambda_1)$$

Now for our case, $\lambda_2 \leq \frac{1}{2}$ and hence

$$\lambda_3 \leq 1 - \frac{1}{2}\left(1 - \frac{1}{4}\right)(1 - \lambda_1) \leq 1 - \frac{3}{8}(1 - \lambda_i)$$

Now $G_i = (G_{i-1} ⓩ H)^8$ and hence

$$\lambda_i \leq \left(1 - \frac{3}{8}(1 - \lambda_{i-1})\right)^8 \leq \left(1 - \frac{1}{3}(1 - \lambda_{i-1})\right)^8$$

If $\lambda_{i-1} \geq \frac{1}{2}$, $\lambda_i \leq \left(\frac{5}{6}\right)^8 < \frac{1}{2}$.
Otherwise if $\lambda_{i-1} < \frac{1}{2}$, with some little bit of calculus one can show that

$$\left(1 - \frac{1}{3}(1 - \lambda_{i-1})\right)^4 \leq \lambda_{i-1}$$

and we are done. □

17.4 Proof of Claim 25

Now we shall give a logspace algorithm to compute Rot_l given $Rot_{G'}$ and Rot_H. This algorithm shall use one global variable and all compuation shall be done overwriting values on it. Recursive calls shall have only constant memory overhead and hence this algorithm will run in logspace.

For each step in G_i, we need to do 16 steps in H and 8 in G_{i-1}.

The input for Rot_{G_i} is $(\bar{v}, \bar{a})$. Let us intepret $\bar{v}$ as an element of $[N^2] \times [D^{16}]^i$,

$$\bar{v} = (v, a_0, a_1, \ldots, a_{i-1})$$

Similarly, let us interpret $\bar{a} = a_i$ as an element of $[D^{16}]$,

$$\bar{a} = (k_{i,1}, k_{i,2}, \cdots, k_{i,16})$$

for $k_{i,j} \in [D]$.

These are written on the input tape as

v	a_0	a_1	$\cdots$	a_{i-1}	a_i

which consists of $O(\log N)$ bits.
The algorithm for computing Rot_{G_i} is the following:

1. **for** $j = 1$ to 16 **do**
    - **overwrite** $(a_{i-1}, k_{i,j}) := Rot_H(a_{i-1}, k_{i,j})$;
    - **If** j is odd
        - **then overwrite** $(v, a_0, \cdots, a_{i-1}) := Rot_{G_i}(v, a_0, \cdots, a_{i-1})$;

- **If** $j = 16$
  - **then overwrite** $(k_{i,1}, \cdots, k_{i,16}) :=$ **reverse**$(k_{i,1}, \cdots, k_{i,16})$

2. **done**

The overhead in the recursion is just j since everything else is maintained in the global worktape. Thus in logspace we can compute the rotation map of G_l. $\square$

This concludes Reingold's algorithm and we have proved theorem 22

Lectures on Expanders		Course Instructor: V. Arvind
	Lecture 6	
Lecturer: V. Arvind		*Scribe: Ramprasad Saptharishi*

18 Overview

In the next two lectures we shall discuss a result of Babai and Szemeridi on random sampling from finite groups.

There needs to be more introduction, shall be expanded

19 The Black-Box Group Model

You are given a group $G \subseteq \Sigma^m$, considered as strings over Σ and generated by a finite set of generator S. You are also provided an oracle that gives you the necessary group operations, i.e you can multiply, invert etc but you are not given access to the actual structure of the operations.

One could consider the group G to be embedded in a larger group, and the oracle does the operations on the larger group. Of course with Cayley's theorem $G \leq S_n$, the permutation group over n elements, but this is too large a group. So usually it's assumed to be a subset of some matrix group $GL_n(\mathbb{F}_q)$ or something.

There are quite a few of problems unlikely to be in P, here is an example.
Problem: Given $G = \langle A \rangle, H = \langle B \rangle$, compute $G \bigcap H$.

This is known to be harder than graph isomorphism, and there's strong evidence that this is not $NP-$complete and it is also not known to be in P.

Babai and Szemeridi looked at the complexity of *Membership Testing*, we shall be studying this problem over the next two lectures.

20 Membership Testing

20.1 The Problem Statement

$G = \langle S \rangle$ and is a subgroup of a matrix group $H = GL_n(\mathbb{F}_q)$ and you are provided with a black-box for H. Given x, check if $x \in G$.

We shall that this problem is in $NP \bigcap coAM$.

20.2 $MembershipTest \in NP$

The naive approach is to look at x as a string over S and guess this string. But one should note that strings could be very large since the group could be non-commutative.

However, there should be lots of blocks of repetition insead the string representing x, and hence rather than asking for the string one could ask for the *circuit* computing x over S. Our circuit would have all nodes to be multiplication gates, with the elements of S in the leaves and x being the output of the circuit. Now the question is, if $x \in G$, does there exists a small circuit for x over S?

20.3 Small Circuits for elements of G

Lemma 27 (Reachability Lemma). *For every $g \in G = \langle S \rangle$, there exists a circuit of size $(1 + \log |G|)^2$ that computes g from S.*

Proof. Let $x_1, x_2, \cdots, x_i$ be a sequence of group elements. The cube defined by $\{x_1, \cdots, x_i\}$ is defined as follows.

$$C\left(x_1, \cdots, x_i\right) = \{x_1^{e_1} x_2^{e_2} \cdots x_i^{e_i} | e_j \in \{0, 1\}\}$$

Let $C_0 = C(S) = C(S_0)$. We shall see how we can "expand" the cube to swallow G. Let $C_i = C(S_i)$. If $G \subseteq C_i^{-1} C_i$, then stop; we already have G.

Otherwise, $G \nsubseteq C_i^{-1} C_i$. This means that there exists a g_j such that $C_i^{-1} C_i g_j \nsubseteq C_i^{-1} C_i$. Hence let $h_{i+1} \in C_i^{-1} C_i g_j \backslash C_i^{-1} C_i$. Define $S_{i+1} = S_i \cup h_{i+1}$ and $C_{i+1} = C(S_{i+1})$.

Now $C_{i+1} = C_i \sqcup C_i \cdot h_{i+1}$ and hence $|C_{i+1}| = 2|C_i|$, and hence in $\log |G|$ steps, we can get $G \in C_i$. Thus G is a product of $2 \log |G|$ elements. What is left to argue is that the h_{i+1} we've been introducing all the while also has small circuits. And since we are building on the previous cubes, each h_i needs a circuit of size $2i - 1$.

Hence, for all the h_i's we need a circuit of size

$$\sum_{i=1}^{1+\log |G|} 2i - 1 = (1 + \log |G|)^2$$

as required

□

And now if $x \in G$, the NP machine can guess this circuit for x and check if it infact computes x in polynomial time. Thus $MembershipTest \in NP$.

Showing that this is infact in $coAM$ requires a lot more work, we first need to be able to sample from the group.

20.4 The Erdös and Rényi Result

Here is an informal sketch of the result:
Theorem:[informal]*For any group G, "most" $O(\log |G|)$ size sets define cubes that equal G. And for $k = c \log |G|$, the distribution*

$$x = x_1^{e_1} x_2^{e_2} \cdots x_k^{e_k}, e_i \in_R \{0, 1\}$$

is "almost" uniform, i.e,

$$\frac{1-\epsilon}{|G|} \leq \Pr_{e_1, \cdots, e_k}[x = g] \leq \frac{1+\epsilon}{|G|}$$

The formal version is the following:

Theorem 28 (Erdös and Rényi)**.** *Let G be a finite group and $x = (x_1, \cdots, x_k), x_i \in G$. And for all $g \in G$, define*

$$Q_x(g) = \Pr_{\bar{e}}[x_1^{e_1} \cdots x_k^{e_k} = g]$$

Then for all $\epsilon, \delta > 0$, if $k \geq 2 \log |G| + 2 \log\left(\frac{1}{\epsilon}\right) + \log\left(\frac{1}{\delta}\right)$,

$$\Pr_x\left[|Q_x - U|_\infty > \frac{\epsilon}{|G|}\right] \leq \delta$$

Proof. As usual, we shall work with the L_2 norm instead of the L_∞ norm.

$$\begin{aligned}
|Q_x - U|_\infty^2 &\leq \|Q_x - U\|_2^2 \\
&= \sum_g \left(Q_x(g) - \frac{1}{|G|}\right)^2 \\
\therefore E_x |Q_x - U|_\infty^2 &\leq E_x \|Q_x - U\|_2^2 \\
&= \sum_g E_x \left(Q_x(g)^2 + \frac{1}{|G|^2} - 2Q_x(g)\frac{1}{|G|}\right) \\
&= E_x\left(\sum_g Q_x(g)^2\right) - \frac{1}{|G|}
\end{aligned}$$

Note that the first term in the last line is the collision probability. Hence, define $\chi_x(\bar{e}, \bar{e'})$ as the indicator random variable to check for collision, i.e,

$$\chi_x(\bar{e}, \bar{e'}) = \begin{cases} 1 & \text{if } x_1^{e_1} \cdots x_k^{e_k} = x_1^{e'_1} \cdots x_k^{e'_k} \\ 0 & \text{otherwise} \end{cases}$$

Hence,

$$\begin{aligned} E_x\left(\sum_g Q_x(g)^2\right) &= E_x \frac{1}{2^{2k}} \sum_{e,e'} \chi(e, e') \\ &= \frac{1}{2^{2k}} \sum_{e,e'} E_x[\chi_x(e, e')] \\ &= \frac{1}{2^{2k}} \sum_{e,e'} \Pr_x[\chi_x(e, e') = 1] \end{aligned}$$

Now, when $e = e'$, then $\Pr_x[\chi_x(e, e') = 1] = 1$. As for the other case when $e \neq e'$, taking all the e_i to one side we have $\Pr_x[\chi_x(e, e') = 1] = \frac{1}{|G|}$. And hence,

$$\begin{aligned} E_x\left(\sum_g Q_x(g)^2\right) &= \frac{1}{2^{2k}}\left(\sum_{e=e'} 1\right) + \frac{1}{2^{2k}}\left(\sum_{e\neq e'} \frac{1}{|G|}\right) \\ &= \frac{1}{2^k} + \frac{2^{2k} - 2^k}{2^{2k}} \frac{1}{|G|} \\ &= \frac{1}{|G|} + \frac{1}{2^k}\left(1 - \frac{1}{|G|}\right) \\ \therefore E_x\left(|Q_x - U|_\infty^2\right) &\leq \frac{1}{2^k}\left(1 - \frac{1}{|G|}\right) \end{aligned}$$

And now to estimate $\Pr_x[|Q_x - U|_\infty > \frac{\epsilon}{|G|}]$, we can use Markov's inequality and the result follows. □

20.5 Towards Babai's Sampling Algorithm: The Cayley Graph

Let $G = \langle S \rangle$. The cayley graph $X(G, T)$ where $T = S \cup S^{-1} \cup \{1\}$ has the vertex set as G. And (x, y) is an edge in the $X(G, T)$ if there exists a $g \in T$ such that $xg = y$.

Earlier we say the following eigenvalue bound

$$\lambda_2 \leq 1 - \frac{1}{O(diam^2|G|^2)}$$

In arbitrary graphs, one could have a very small diameter but the size of the graph could be large (two complete graphs connected by a cut edge, diameter is 3 but size is large). But for Cayley graphs, the additional structure ensure the following eigenvalue bound.

$$\lambda_2 \leq 1 - \frac{1}{O(diam^2)}$$

Babai achieves the random sampling by looking at the Cayley Graph as an expander and taking a random walk on it. Cayley graphs aren't really expander but they have a property that Babai called the *Local Expansion Property.*

Lemma 29 (Local Expansion Lemma). *Define T^t to be the $t-$neighbourhood of T, the set of all vertices reachable from T by a path of length atmost t. Let $0 < \alpha < \frac{1}{2t+1}$, and $D \subseteq T^t$ such that $|D| \leq (1 - 2t\alpha)|G|$. Then there exists a $g \in S$ such that $|D \backslash Dg| \geq \alpha|D|$*

Note that if t was the diameter of $X(G, T)$, then $T^t = G$. Taking $\alpha = \frac{1}{4t}$, we then have for all $D \subseteq G, |D| \leq \frac{|G|}{2}$, $|\Gamma(D)| \geq \left(1 + \frac{1}{4t}\right)|D|$, and this actually gives us that $\lambda_2 \leq 1 - \frac{1}{diam^2}$.

We shall see the proof of this lemma and the sampling algorithm in the next lecture.

Lectures on Expanders	Course Instructor: V. Arvind
Lecture 7	
Lecturer: V. Arvind	*Scribe: Ramprasad Saptharishi*

21 Recap

Last class we wanted to show that the membership testing problem in the blackbox group model is in $NP \cap coAM$, and showing it was in NP was done by construction of small circuits (by expanding "cubes") acting as a witness. To show that it is in $coAM$, we needed to sample from the group; that was the focus of Babai's paper.

The result of Erdös and Rényi tells us that given a random set of size $O(\log|G|)$ can be used to sample almost uniformly at random from the group G. But this would first require to pick the set of $O(\log|G|)$ elements, which is too costly.

When we noted that Babai then describes the Cayley graph and Lemma 29 tells us that the Cayley Graph has decent expansion properties, and we shall be exploiting this. As seen in some of our earlier lecture, we shall analyse random walks on these Cayley Graphs to help us achieve almost uniform sampling from G.

22 Proof of Lemma 29

Suppose the lemma is not true, then for all $g \in S$, $|D \backslash Dg| < \alpha|D|$.
Now for $x, y \in G$,

$$\begin{aligned} D \setminus D_{xy} &\subseteq (D \setminus D_y) \cup (D_y \setminus D_{xy}) \\ &= (D \setminus D_y) \cup (D \setminus D_x) \cdot y \\ \therefore |D \setminus D_{xy}| &\leq |D \setminus D_x| + |D \setminus D_y| \end{aligned}$$

Hence, for all k, $u \in T^k$,

$$|D \setminus D_u| < k\alpha|D|$$

Thus for $k = 2t+1$,

$$|D \setminus D_u| < |D|$$

but this is possible only when D_u contains some elements of D, i.e $D \cap D_u \neq \phi \implies u \in D^{-1}D \subseteq T^{2t}$ for all u, and hence $G = T^{2t}$.

Now lets count the number of pairs (x, u) such that $x \in D, u \in G, xu \in D$. For every $u \in G$, there exists an x such that $xu \in D$ since $D \cap D_u \neq \phi$. Hence for $k = 2t$,

$$\begin{aligned} |D \setminus D_u| &< 2\alpha t|D| \\ \implies |D \cap D_u| &> (1 - 2\alpha t)|D| \end{aligned}$$

And since $|D \cap D_u|$ many x's are possible for each u, the total number of pairs is atleast $(1 - 2\alpha t)|D| \cdot |G|$.

And also clearly the number of pairs is less than $|D|^2$, which then forces the contradiction on the size of D. □

23 Local Expanders

In order to study more on the "local expanders" we have the following definition.

Definition 30. *Let $X = (V, E)$ any undirected graph and let Y be a vertex induced subgraph of X. We say Y is ϵ expanding subgraph of X if for all $W \subseteq V(Y)$, $|\Gamma_X(W)| \geq (1 + \epsilon)|W|$*

Theorem 31. *If $G = \langle S \rangle$ and $X = X(G, T), T = S \cup S^{-1} \cup \{1\}$ then if $|T^t| \leq \frac{|G|}{2} \implies T^t$ is a $\frac{1}{4t}$ expanding subgraph of X, i.e*

$$\forall D \subseteq T^t, |\Gamma(D)| \geq \left(1 + \frac{1}{4t}\right)|D|$$

Proof. Put $\alpha = \frac{1}{4t}$ in the earlier lemma and the theorem is done. □

Earlier we had shown that spectral expansion implied vertex expansion. Here is a result in the other direction, we won't prove it though.

Theorem 32 (Alon's Eigenvalue Bound)**.** *Let G be a $d-$regular connected non-bipartite undirected graph such that for all $U \subseteq V, |U| \leq \frac{|V|}{2}$, $|\Gamma(U)| \geq (1 + \epsilon)|U|$. Then*

$$\lambda_2(G) \leq \left(d - \frac{\epsilon^2}{4 + 2\epsilon^2}\right)\frac{1}{d}$$

And in the context of locally expanding subgraphs:

Theorem 33 (Babai's Eigenvalue Bound). *If Y is an $\epsilon-$expanding subgraph of X, then we have the following bound for the largest eigenvalue of the adjacency matrix (the non-normalized adjacency matrix) of Y*

$$\lambda_1(Y) \leq d - \frac{\epsilon^2}{4+2\epsilon^2}$$

Now for random walks on these local expanders.

Theorem 34. *Suppose we start at a random walk on X from any vertex $v_0 \in Y$, then*

$$\Pr[\textit{the random walk is confined to } Y \textit{ for } l \textit{ steps}] \leq |V(Y)| e^{-\frac{\epsilon^2 l}{4+2\epsilon^2}\frac{1}{d}}$$

Proof. Let A be the adjacency matrix of Y, and $e_0 \in \mathbb{R}^{|V(Y)|}$, the standard basis vector with 1 at v_0 and 0 everywhere else. Assuming that the walk is completely confined in Y, the transition matrix of the walk is $\frac{1}{d}A$.

Now, the probability that you are confined in Y for l steps is precisely

$$(1, 1, \cdots, 1)^T \left(\frac{1}{d}A\right)^l e_0$$

Since A is a real symmetric matrix, we know by the spectral theorem that there exists a real eigenbasis. Hence $A = C^T DC$ where C is an orthogonal matrix and D is the diagonal matrix of eigenvalues. Hence the probability of staying inside Y for l steps (let me call that value as $P(l)$)

$$\begin{aligned} P(l) &= \frac{1}{d^l}(CJ)^T \cdot D^l \cdot (Ce_0) \\ &\leq \|CJ\|_2 \cdot \lambda_1^l \|J\|_2 \\ &= \left(\frac{\lambda_1}{d}\right)^l |V(Y)| \end{aligned}$$

And now using Babai's eigenvalue bound, the theorem follows. $\square$

The only other property we need the Cayley graph to satisfy is the small diameter criteria. Then our random walk would sample almost uniformly from G.

Claim 35. *If $diam(G) > 2t$, then $|T^t| \leq \frac{|G|}{2}$*

Proof. If $diam(G) > 2t$, then we know that

$$\begin{aligned} G &\nsubseteq \left(T^t\right)^{-1} T^t \\ \implies \exists g &: T^t g \cap T^t = \phi \\ \implies |T^t| &\leq \frac{|G|}{2} \end{aligned}$$

□

Now, suppose $diam(G) > 2t$, we know that $|T^t| \leq \frac{|G|}{2}$ and then, by our earlier theorem, T^t is a $\frac{1}{4t}$ expanding subgraph of $X(G,T)$. And then, the probability of the random walk being confined to T^t is upper bounded as follows

$$P(l) \leq |G| e^{\frac{l}{(64t^2+2)|T|}}$$

And when $l = (64t^2+2)|T| \left(\log |G|\right)^2$, then $P(l) \frac{1}{|G|}$ and this l is polynomially bounded in $\log |G|$, so we are in good shape to emulate the reachability lemma.

Define $R_1 = T$ and for inductive procedures, $C_i = R_1 \cdots R_i$. Suppose $G \subseteq T^{4i}$, we already have small diameter and hence we are done.

Suppose $G \nsubseteq T^{4i}$, then $T^{2i} \leq \frac{|G|}{2}$. Do a random walk for l steps (for the suitable l for $2i$) and add all the elements visited to R_{i+1}.

With good probability, we have an $x \notin C_i^{-1} C_i$ and hence $|C_{i+1}| \geq 2|C_i|$, the size doubles with each time. Hence with little error, we would be reaching small diameter in $\log |G|$ steps.

The accumulated error, by the union bound, is upper bounded by $\frac{poly(\log |G|)}{|G|}$ and we are in good shape. We can now use Erdös and Rényi and we would be able to sample almost uniformly from G.

24 $MembershipTest \in coAM$

Needs to be filled out, not sure of it myself.