Lecture 9: Oct 6

Lecturer: Mohammad R. Salavatipour *Scribe: Joshua Gane*

9.1 Expanding Graphs and Probability Amplification

Roughly speaking an expanding graph is a graph in which every not too large subset of vertices has relatively large number of neighbours (and so the graph is highly connected). There are tons of applications for expanding graphs. Here we will see on application in amplifying success probability of or randomized algorithms. There are several classes of expanding graphs. One of which is defined below.

Definition 9.1 *An (n, d, α, c) OR_concentrator is a bipartite graph $G(A \cup B, E)$, with $|A| = |B| = n$ such that:*
1. $\forall v \in A\colon d(v) \le d$.
2. $\forall S \subset A$ such that $|S| \le \alpha n$ then it has at least $c\,|S|$ neighbors in B.

Our main goal is to show that such graphs exist for constant d, α, c and any value of n.

Theorem 9.2 *For all large enough n, there is an $(n, 18, \frac{1}{3}, 2)$ OR_concentrator.*

Proof: Consider a bipartite graph $G(A \cup B, E)$ with $|A| = |B| = n$. For every $v \in A$ pick d vertices (with replacement) uniformly randomly from B and connect v to them, i.e. they are going to be neighbors of v. Note that degree of every vertex in A is at most d. We compute the probability that this graph satisfies the two conditions stated above. For each set S, let $\mathcal{E}_s$ be the event that set S of size s has less than cs neighbors in B. Then for a subset $T \subseteq B$: $\Pr[S$ going only to $T] \le (\frac{cs}{n})^{ds}$. Since we have $\binom{n}{s}$ choices to select S from A, and at most $\binom{n}{cs}$ choices for T then:

$$\begin{aligned}
\Pr[\mathcal{E}_s] &\le \binom{n}{s}\binom{n}{cs}(\frac{cs}{n})^{ds} \\
&\le (\frac{en}{s})^s(\frac{en}{cs})^{cs}(\frac{cs}{n})^{ds} \\
&\le [(\frac{s}{n})^{d-c-1}e^{1+c}c^{d-c}]^s \\
&\le [(\frac{1}{3})^{d-c-1}e^{c+1}c^{d-c}]^s \qquad \text{with } \ \alpha = \frac{1}{3} \\
&\le [(\frac{c}{3})^d(3e)^{c+1}]^s \qquad \text{if } \ \mathrm{c} = 2, \mathrm{d} = 18 \\
&= [(\frac{2}{3})^{18}(3e)^3]^s \\
&< 2^{-s}
\end{aligned}$$

Thus summing over all values of s:

$$\sum_{s \ge 1} \Pr[\mathcal{E}_s] < 1.$$

This implies that With positive probability an OR_concentrator of $(n, 18, \frac{1}{3}, 2)$ exists ■
We don't know how to construct such an expanding graphs in polynomial time. We don't even know how to verify a proposed graph (this problem is NP-hard). But there are some constructive proofs for expanding graphs that are nearly as good as the one proved above.

Theorem 9.3 *For large enough n, there is a bipartite graph $G(A \cup B, E)$ such that $|A| = n$, $|B| = 2^{\log^2 n}$ and:*
1. $\forall v \in B : d(v) \leq 12\log^2 n$.
2. $\forall S \subset A$ with $|S| = \frac{n}{2}$ has $\geq 2^{\log^2 n} - n$ neighbors in B.

Proof: Consider a bipartite graph with that many vertices. For each vertex of A we choose $d = \frac{2^{\log^2 n}(4\log^2 n)}{n}$ vertices of B u.r with replacement. For each $v \in B$: $\mathrm{E}[d(v)] = 4\log^2 n = \mu$. Now, using Chernoff bound:

$$\Pr[|d(v) - \mu| > 8\log^2 n] \leq e^{-(\frac{\delta^2 \mu}{3})} = e^{-(\frac{4\log^2 n}{3})}.$$

Using union bound:

$$\Pr[\text{Some } v \in B \text{ has degree } > 12\log^2 n] \leq 2^{\log^2 n} \cdot (e)^{-4\log^2 n} \ll \frac{1}{2}.$$

Now we bound the probability that condition 2 is violated. The probabilith that there is a set S with $|S| = \frac{n}{2}$ and $|N(S)| < 2^{\log^2 n} - n]$ is at most $\binom{n}{\frac{n}{2}}\binom{2^{\log^2 n}}{n}(1 - \frac{n}{2^{\log^2 n}})^{\frac{dn}{2}}$ where the first term is for choosing S, the second term for choosing those missed by S, and the last term for probability that all are non-edges. This is at most

$$\begin{aligned}
\left(\frac{en}{n/2}\right)^{n/2}\left(\frac{e2^{\log^2 n}}{n}\right)^{n} e^{-n/2^{\log^2 n}.dn/2} \quad &\leq \quad (2e)^{n/2}(e2^{\log^2 n}/n)^n e^{-n2\log^2 n} \\
&= \quad \left(\frac{(2e)^{\frac{1}{2}}e2^{\log^2 n}e^{-2\log^2 n}}{n}\right)^n \\
&<< \tfrac{1}{2}.
\end{aligned}$$

Therefore the probability that either 1) or 2) is violated is $< \frac{1}{2} + \frac{1}{2} = 1$. Thus with positive probability they are not violated. ■

There are ways to construct an expanding graph like the one in the previous theorem. The problem may seem to be that the size of the graph is not polynomial ($O(2^{\log^2 n})$). Fortunately, we don't need an explicit representation of the whole graph. We only need to be able to find neighbours of a given vertex in polynomial time. There are implicit representation of such graphs that support the neighbourhood queries in polynomial time. We show how we can use these graphs to amplify probability.

Recall the definition of RP. A language $L \in RP$ if there is an algorithm $\mathcal{A}$ s.t. it picks a random number from $1...n$ (i.e. $\log n$ random bits) and:

1. if $x \in L$: $\mathcal{A}(x, r) = 1$ with probability $\frac{1}{2}$ (or $A(x, r) = 1$ for at least half the choices of r).
2. if $x \notin L$: $\mathcal{A}(x, r) = 0$ always.

To boost the success probability we can repeat the algorithm t times. This will bring down the error probability to at most 2^{-t}. If $t = \log n$ then we have used $\log^2 n$ random bits and error probability is $\leq \frac{1}{n}$.

Consider an expanding graph as in Theorem 9.3. Given $\log^2 n$ random bits, use them to choose a random vertex $v \in B$. Then find the neighbours v, say $N(v) = A' \subseteq A$ where $A' = \{a_1, \ldots, a_k\}$. Compute $A(x, a_i)$ for each $1 \le i \le k$ and accept iff at least one of these calls accepts. Note that $k \le 12\log^2 n$ so there are only a polynomial number of calls. Clearly if $x \notin L$ the algorithm rejects. If $x \in L$, then for at least $\frac{n}{2}$ vertices of A the algorithm accepts (not that A has n vertices). So there are at most $\frac{n}{2}$ vertices of A for which algorithm $\mathcal{A}$ fails to give the right answer, call those vertices A^*. So we fail to accept if all the neighbours of B, i.e. $a_1, \ldots, a_k$ are from A^*. But there are at most n vertices of B that are not connected to anything from $A - A^*$. So the probability that neighbours of $v \in B$ are not from $A - A^*$ is at most $\frac{n}{2^{\log^2 n}}$. Thus the probability of failuer is at most $n/2^{\log^n} = 1/n^{\log n - 1}$ using only $\log^2 n$ random bits.

9.2 Lovász Local Lemma

First, let's start with an example. Suppose we are given a k-uniform hypergraph H with less than 2^{k-1} edges. We claim that there is a 2-coloring of H s.t. no edge is monochromatic. If we color every vertex with one of two colors u.r. then, for every edge e: $\Pr[e \text{ is monochromatic}] = 2^{-(k-1)}$. Since there are stritctly less than 2^{k-1} edges, $\Pr[\exists \text{ some monochromatic edge}] < 2^{(k-1)} \cdot 2^{-(k-1)} = 1$. So with positive probability H is properly 2-colored. What if the number of edges is larger than 2^{k-1}? We might be able to get a 2-coloring in that case if the dependencies between the edges is not too big.

In many examples of the probabilistic method, we have a set of "bad" events $A_1, \ldots, A_n$, each occuring with a probability, say p, and we want to prove that with positive probability none of these events happen. The Local Lemma is a powerful tool in such cases. Before stating the lemma, we need some definitions. Two (random) events A and B are called *independent* if $Pr(A|B) = Pr(A)$. An event A is *mutually independent* of a set $\{A_1, \ldots, A_n\}$ of events if $Pr(A|A_{i_1} \wedge \ldots \wedge A_{i_k}) = Pr(A)$, for all distinct indices $i_1, \ldots, i_k$. Note that the events might be pairwise independent but not mutually independent.

Lemma 9.4 ((Simple) Lovász Local Lemma) *Let $\mathcal{E}$ be a set of bad events such that for each $A \in \mathcal{E}$:*

1. $\Pr(A) \le p < 1$ *and*
2. *A is mutually independent of all but at most d other events in $\mathcal{E}$.*

If $4pd \le 1$ then $\Pr(\bigcap_{A_i \in \mathcal{E}} \bar{A}_i) > 0$.

Example 1: Suppose that H is a k-uniform and every edge interesects at most 2^{k-3} other edges. Then H is 2-colorable.
Proof: Color every vertex u.r. with one of two colors. For every edge e, let the bad event A_e be the event that e is monochromatic. Note That $\Pr[A_e] \le 2^{k-1}$. What is the degree of dependencty? The following priciple is very useful in computing the degree of dependency in may situations like this.

Mutual Independence Principle: Suppose that $X = x_1, \ldots, x_n$ is a sequence of independent random trials. Suppose further that $A_1, \ldots, A_m$ is a set of events where each A_i is determined by a set $F_i \subseteq X$. If $F_i \cap (F_{i_1}, \ldots, F_{i_k}) = \emptyset$ then A_i is mutually independent of $\{A_{i_1}, \ldots, A_{i_k}\}$.

In our situation, we can say that A_e is mutually independent of all those events $A_{e'}$ where $e \cap e' = \emptyset$. Thus $d \le 2^{k-3}$. Since $4Pd \le 4 \cdot 2^{k-3} \cdot 2^{-(k-1)} = 1$ with positive probability no bad event A_e happens, i.e. no edge is monochromatic. ■

Example 2: Consider a k-SAT formula Φ over variables $x_1, \ldots, x_n$ with clauses $C_1, \ldots, C_m$. Suppose that no variable appears in more than $\frac{2^{k-2}}{k}$ clauses. Prove that Φ is satisfiable

Proof: Assign T/F with to each variable u.r. and independently. Define the bad event A_i if C_i is not satisfied. To prove that the formula is satisfiable we have to show that no bad even A_i ($1 \leq i \leq m$) happens with positive probability. We have $\Pr[A_i] = 2^{-k}$. Also, using mutual independenc principle, event A_i is only dependent on those A_j's s.t. C_i and C_j have at least a variable in common. Thus $d \leq k \cdot \frac{2^{k-2}}{k} = 2^{k-2}$. Since $4Pd = 2^{-k} \cdot 2^{k-2} \cdot 4 \leq 1$, by LLL, with positive probability no bad event happens. ■