18.405J/6.841J Advanced Complexity Theory	March 30

Lecture 13

Lecturer: Dan Spielman — *Scribe: Rudi Seitz*

Let M be a BPP algorithm with error probability $1/100$ (the choice of this constant is arbitrary). By running the algorithm $O(k(n))$ times and taking the majority vote, we can reduce the error probability to $2^{-k(n)}$. If the original algorithm M uses $f(n)$ random bits then the new algorithm uses $O(f(n)k(n))$ random bits. In this lecture we will see how to achieve error probability $2^{-k(n)}$ while using only $f(n) + O(k(n))$ random bits.

For the purposes of this lecture we will take d to be some constant. We will say that a d-regular graph G is a good expander if $\lambda/d \leq 1/10$, where λ is an upper bound on the absolute value of all eigenvalues of the adjacency matrix of G besides d. It is possible to construct infinite families of good expanders, but we will not specify a construction here.

Our probability amplification procedure will use a good expander G with $N = 2^{f(n)}$ nodes. We will start by choosing a random node of G, and then we will take a random walk of $7k$ steps. For each vertex encountered, we will treat its label as a sequence of "random" bits, and we will run the algorithm A using these bits. At the end of the walk, we will output the majority vote of A's decisions.

We spend $f(n)$ random bits to choose the first node. Since the degree of G is constant, each step of the random walk requires only a constant number of random bits. Therefore the total number of random bits used is $f(n) + O(k(n))$ as promised.

We will use some basic techniques from spectral graph theory to prove that the procedure works. Let p be a probability vector on G (i.e. p has length n, all its entries are non-negative, and $\sum_i p_i = 1$.) Let $\hat{A} = 1/d \cdot A$ be the transition probability matrix of a random walk on G. All rows in $\hat{A}$ sum to 1, and $\hat{A}p$ is the probability distribution on nodes induced by choosing a random node according to p and then choosing a random neighbor of that node.

Let B denote the set of "bad" vertices in G (i.e. those vertices whose labels, when used as random bits for the algorithm A, cause it to give the wrong answer). We will abuse notation and let B also denote the diagonal matrix such that $B_{ij} = 1$ iff $i = j \in B$. Let $\bar{B}$ denote the set of "good" vertices and also the corresponding diagonal matrix. Then $B + \bar{B} = I$.

Given a probability vector p, $|Bp|$ is the probability that a node drawn according to p is in the set B, where $|(x_1, x_2, \ldots, x_n)| = \sum_i |x_i|$. For example, $|\bar{B}\hat{A}B\hat{A}Bp|$ is the probability that when drawing a random node according to p, the node is in B, a random neighbor is in B, and a random neighbor of that neighbor is in $\bar{B}$.

Let $p_0 = (1/N, 1/N, \ldots, 1/N)$ denote the uniform distribution on nodes. Then $||p_0|| = N^{-1/2}$. The Cauchy-Scharz inequality gives $|p| \leq N^{1/2} \cdot ||p||$ for any vector p of length N.

Theorem 1 *Let p be a positive vector. Then $||B\hat{A}p|| \leq ||p||/5$ where A is the adjacency matrix of a good expander.*

Proof Express p as $\alpha 1 + v$, where $v \perp 1$. We have $B\hat{A}p = B\hat{A}(\alpha 1 + v) = B\hat{A}(\alpha 1) + B\hat{A}v$. Now, $B\hat{A}(\alpha 1) = \alpha B 1$, so $||B\hat{A}(\alpha 1)|| \leq ||\alpha 1||/10$ (using the fact that the set B contains at most $1/100$ of the vertices). Furthermore, $||B\hat{A}v|| \leq ||\hat{A}v|| \leq \frac{\lambda}{d}||v|| \leq ||v||/10$ (using the fact that $v \perp 1$). Therefore we may conclude $||B\hat{A}p|| \leq ||\alpha 1||/10 + ||v||/10 \leq ||p||/5$. ■

Theorem 2 *If we choose a node of a good expander at random, and walk randomly for $7k$ steps, the probability that the majority of vertices encountered fall in B ($\mu(B) \leq 1/100$) is at most 2^{-k}.*

Proof Let p_0 represent the uniform distribution on nodes. If $M_i \in \{B, \bar{B}\}$ for $i = 1, 2, \ldots, 7k$ then $|M_{7k}\hat{A}M_{7k-1}\hat{A}\cdots M_2\hat{A}M_1p_0|$ expresses the probability that for all i, the walk is in set M_i on the i-th step. Assuming that $M_i = B$ for the majority of i's, we can upper bound this probability as follows:

$$
\begin{aligned}
|M_{7k}\hat{A}M_{7k-1}\hat{A}\cdots M_2\hat{A}M_1p_0| &\leq N^{1/2} \cdot ||M_{7k}\hat{A}M_{7k-1}\hat{A}\cdots M_2\hat{A}M_1p_0|| \\
&\leq N^{1/2} \cdot ||p_0|| \cdot 5^{-|\{i \mid M_i = B\}|} \\
&\leq 5^{-7k/2}.
\end{aligned}
$$

Now, the number of ways of choosing the M_i's such that the majority equal B is less than 2^{7k}. So the probability that the majority of steps in the walk land in B is at most $2^{7k} \cdot 5^{7k/2} \leq 2^{-k}$.
■

It should be clear that this theorem implies the correctness of our procedure.