CS 830: Randomness and Complexity 3/10/05

Lecture 16: The Ajtai-Komlós-Szemerédi Generator

instructor: Jin-Yi Cai Scribe: Matthew Anderson

1 Overview

We are given a regular d-degree expander on N vertices. We can think of $N = \{0,1\}^n$, with each n-bit string representing a test for some RP predicate. The measure of the witness set, W_x, is greater or equal to one half. We would like to estimate the failure probability (never hitting the witness set) in a random walk on this expander. We pick uniformly at random a point, $y_0 \epsilon \{0,1\}^n$, then take k steps on the expander away from that point: $y_1, y_2, ..., y_k$. As we argued last time if you take $O(\log N)$ steps on an expander the distribution of the final position on the expander is uniform.

Its takes n bits to describe the starting position of the random walk and $(k\lceil \log d \rceil)$ bits to describe the which edge to follow at each step in the walk through the graph. Thus, we can describe the walk in $(n + O(k))$ bits. Using this setup we will get an error probability of $2^{-O(k)}$.

This is not the best generator. It is, however, better than the ones we have seen so far, but is not as good as some generators that have appeared in recent work. We would rather have $2^{-O(n)}$ error probability, but that would require $O(n)$ time to compute.

2 Other Amplification Methods

2.1 Naive Amplification

Run m times independently, out of $2^{m \cdot n}$ strings, at most $2m \cdot n - m$ could be "bad". We can measure the strength of the amplification by comparing the log of bad strings to the total number of strings:

$$\frac{\log \ \# \text{ of bad strings}}{\log \ \# \text{ of strings}} = \frac{m(n-1)}{mn} = \frac{n-1}{n} \to 1. \tag{1}$$

As n goes to infinity, this ratio goes to one.

2.2 Amplification with Extractors

Using extractors asymptotically better amplification is possible. For all $\epsilon > 0$, one can "blackbox" amplify at a length n^k (where k depends on ϵ) such that out of all 2^{n^k} strings at most $2^{\epsilon \cdot n^k}$ strings are bad. The blackbox is a circuit that can test for membership in W_x. We can again compare the log of bad strings to good strings:

$$\frac{\log \ \# \text{ of bad strings}}{\log \ \# \text{ of strings}} = \frac{\epsilon \cdot n^k}{n^k} = \epsilon. \tag{2}$$

Notice that for this construction the ratio may be arbitrarily small.

Example: Consider BPP.

We would like to test if some string x is in the language L. Recall that if $x \epsilon L$ then $\mu(W_x) \geq 3/4$ and if $x \not\epsilon L$ then $\mu(W_x) \leq 1/4$. We can construct a circuit that takes an x and $y \epsilon (W_x \cup \bar{W}_x)$ and determines whether y is a witness for $x \epsilon L$.

We will amplify this to some length $m = n^k$ such that at most $2^{1/3 \cdot m}$ strings out of 2^m strings are bad (we choose ($\epsilon = 1/3$) in this example).

Consider all 2^m strings divided into segments as follows:

$$\text{Let } S_y = \{x \epsilon 2^m | \exists z \epsilon 2^{m/2}, y \epsilon \{0,1\}^{m/2}, x = yz\} \tag{3}$$

Notice that the number of S_y's is $2^{m/2}$ and that $|S_y|$ is $2^{m/2}$. Since only $2^{m/3}$ strings are bad, most of the segments are free of bad strings.

Claim: $BPP \subseteq \Sigma_2^p \cap \Pi_2^p$.

If $x \epsilon L$ there are not enough bad strings to put one in each S_y, so for some y all the strings in S_y must be good. The reverse is also true, if $\exists y$ such that S_y contains no bad strings, then $x \epsilon L$ because there must be at least $2^{m/2}$ good strings. Notice that this does depend on ϵ being asymptotically less than 1/2.

$\boxtimes$

Subsequent work has shown: $\forall q > 0$, you can construct a black box amplification of length $\rho(n)$, for some polynomial ρ (which may depend on ϵ), so that out of $2^{\rho(n)}$ strings at most $2^{\rho(n)^\epsilon}$ strings are bad. We apply a $\log - \log$ comparison this time:

$$\frac{\log\log \ \# \text{ of bad strings}}{\log\log \ \# \text{ of strings}} = \frac{\log\log 2^{\rho(n)^\epsilon}}{\log\log 2^{\rho(n)}} = \epsilon. \tag{4}$$

One application of this work is by Goldreich: suppose an adversary sets all but length ϵ many bit positions, then most of the strings are good. Using this idea, given a graph on n-vertices we want to check whether the graph is connected. The idea is to use the graph itself as the random input. Goldreich showed that at most 2^{n^ϵ} graphs are bad. This allows the construction of a deterministic log-space algorithm for graph connectivity.

3 Ajtai-Komlós-Szemerédi Generator

We are given a regular d-degree expander on N vertices. Let M be the eigenvalue-normalized adjacency matrix on the expander. Define a uniform distribution on N as $p_0 = \frac{1}{N}(1, ..., 1)^T$. The starting point y_0 will be drawn from this distribution. Consider the distribution for y_1: $p_1 = Mp_0 = \lambda_1 p_0 = 1p_0 = p_0$. Similarly the distributions for y_i (p_i) are also all uniform. We want to estimate the failure probability: $Pr[\{y_1, ..., y_k\} \subseteq \bar{W}_x]$.

Define $w_i = Pr[\{y_1, ..., y_i\} \subseteq \bar{W}_x]$. Let ν_i be the conditional distribution of y_i, given $\{y_1, ..., y_{i-1}\} \subseteq \bar{W}_x$. Denote $P = P_{\bar{W}_x}$ as the projection matrix from N to the set $\bar{W}_x$ (this is the matrix that has ones only in the diagonal cells corresponding to elements of $\bar{W}_x$, zeroes everywhere else).

For the second step in the walk we have the distribution:

$$\nu_2 = M \frac{PMp_0}{\|PMp_0\|_1}. \tag{5}$$

The projector P, forces the distribution, ν_1, onto the space of $\bar{W}_x$ and the term $\|PMp_0\|_1$ normalizes the new distribution. The matrix M is applied finally to walk one step further on the expander. Notice that $w_1 = \mu(\bar{W}_x)$.

Claim:

$$w_{i-1} = \|(PM)^{i-1}p_0\|_1, \tag{6}$$

$$\nu_i = \frac{M}{w_{i-1}}(PM)^{i-1}p_0. \tag{7}$$

Proof: We can show this by joint induction. The base cases were discussed previously. First consider induction on ν:

$$\nu_i = M\frac{P\nu_{i-1}}{\|P\nu_{i-1}\|_1} = M\frac{P\frac{M}{w_{i-2}}(PM)^{i-2}p_0}{P\|\frac{M}{w_{i-2}}(PM)^{i-2}p_0\|_1} = M\frac{(PM)^{i-1}p_0}{\|(PM)^{i-1}p_0\|_1} = \frac{M}{w_{i-1}}(PM)^{i-1}p_0. \tag{8}$$

Now consider induction on w_i:

$$w_i = w_{i-1}Pr[y_i\epsilon\bar{W}_x|\{y_1,...,y_{i-1}\} \subseteq \bar{W}_x] = w_{i-1}\frac{1}{w_{i-1}}\|(PM)^i p_0\|_1 = \|(PM)^i p_0\|_1. \tag{9}$$

3.1 Analysis

Given any vector v we would like to estimate PMv. Express v in the eigenbasis of M:

$$v = \sum_{i=1}\alpha_i v_i, \tag{10}$$

where $\alpha_i = \langle v, v_i\rangle$, the length of the projection of v onto the i^{th} eigenvector. Recall that for probability distributions $\lambda_1 = 1$ and that $v_1 = \frac{1}{\sqrt{N}}(1,...,1)^T$. So we have

$$Mv = \sum_{i=1}\alpha_i\lambda_i v_i = \alpha_1 v_1 + \sum_{i=2}\alpha_i\lambda_i v_i \tag{11}$$

Consider the application of P to an arbitrary vector x:

$$\|Px\|_2^2 = \sum_{i\epsilon\bar{W}_x} x_i^2 \leq \sum_i x_i^2 \leq \|x\|_2^2. \tag{12}$$

So for the eigenvectors, which have unit length, $\|Pv_i\|_2 \leq 1$. By the triangle inequality:

$$\|PMv\|_2 \leq |\alpha_1|\|Pv_1\|_2 + \|\sum_{i=2}\alpha_i\lambda_i v_i\|_2. \tag{13}$$

But $\|Pv_1\|_2^2 = \mu(\bar{W}_x) \leq \frac{1}{2}$. Also,

$$\|\sum_{i=2}\alpha_i\lambda_i v_i\|_2 = \sum_{i=2}(\alpha_i\lambda_i)^2 \leq \lambda^2\sum_{i=1}\alpha_i^2 \leq \lambda^2 \cdot \|v\|_2^2. \tag{14}$$

So we get:

$$\|PMv\|_2 \leq |\alpha_1|\frac{1}{\sqrt{2}} + \lambda\|v\|_2 \leq \left(\frac{1}{\sqrt{2}} + \lambda\right)\|v\|_2. \tag{15}$$

Combining everything we can estimate w_k (applying the Cauchy-Schwartz inequality):

$$w_k = \|(PM)^k p_0\|_1 \leq \sqrt{N}\|(PM)^k p_0\|_2 \leq \sqrt{N}\left(\frac{1}{\sqrt{2}} + \lambda\right)\|p_0\|_2 = \theta^k = 2^{-c \cdot k}. \tag{16}$$

We have achieved a $2^{-O(k)}$ bound on the failure probability, w_k, of the amplifier.

Homework: Try to generalize this to BPP predicates, as well as to look at the other generators using similar analysis.