CS 880: Advanced Complexity Theory 2/15/06

Lecture 9: One-Sided Error Reduction

Instructor: Dieter van Melkebeek Scribe: Matthew Anderson, Shuaiqi Gu

1 Introduction

Recalled last time we introduced the notion of deterministic amplification. We will continue today with showing an approach for 1-sided deterministic amplification that will improve error probability to one over a polynomial without using any additional randomness. We will also discuss randomness efficient 1-sided error reduction; this will allows us to make the error exponentially small using only linearly more random bits. Next time we will discuss improving error on 2-sided algorithms.

2 1-Sided Deteministic Amplification

Recall that the behavior of Turing machines with 1-sided error can be described as follows:

$$\begin{aligned} x \notin L &\Rightarrow \Pr_{\rho}[M(x;\rho) \text{ accepts}] = 0 \\ x \in L &\Rightarrow \Pr_{\rho}[M(x;\rho) \text{ accepts}] \geq \frac{1}{2} \end{aligned} \tag{1}$$

where $|\rho| = |x|^r$ which is polynomial in the input of the x. Let $n = |x|$.

2.1 The Idea

The purpose of deterministic amplification is to produce a new machine, $M'(x;\rho')$, that has a much smaller error probability though it uses M and the same amount of randomness. Let ρ' be the set of all bitstrings ($\rho' = \{\rho_1, \rho_2, ...\}$) reachable from ρ in s step on an expander with $N = 2^{n^r}$ vertices (with each vertex corresponding to a unique bitstring).

To compute $M'(x;\rho')$ run $M(x;\rho_i)$ for each ρ_i and accept iff at least one $M(x;\rho_i)$ accepts. Intuitively, using the expander we should be able to explore a large space of bitstrings and hopefully locate a witness for $x \in L$. There are a number of parameters in this computation, we will perform the analysis first then set the parameters so that it results in a one over poly error probability.

2.2 Analysis Using Vertex Expansion

There two cases that must be considered. First, $x \notin L$, trivially M' must also reject x because each $M(x;\rho_i)$ will reject. The second case is more interesting, $x \in L$. Consider the probability that M' rejects in this case:

$$\Pr_{\rho'}[M'(x;\rho') \text{ rejects}] = \Pr_{\rho'}[\text{For all } \rho_i \text{ reachable from } \rho \text{ in } s \text{ steps, } M(x;\rho_i) \text{ rejects}]. \tag{2}$$

Define two sets B and B' as:

$$\begin{aligned} B &: \text{bad } \rho' \text{ for } M'(x;\cdot) \\ B' &: \text{bad } \rho \text{ for } M(x;\cdot) \end{aligned} \tag{3}$$

So we have $\Gamma^s(B') \subseteq B$. As long as you do not hit the limit of the expander set size the neighborhood will increase by some constant factor c in each step. Giving us $|\Gamma^s(B')| \geq c^s|B'|$ provided that B is small enough ($|B| \leq k = \frac{N}{2}$, where k is the maximum set size for our expander).

$$\begin{aligned} c^s|B'| \leq |\Gamma^s(B')| \leq |B| \leq \frac{N}{2} \\ \Pr_{\rho'}[M'(x;\rho') \text{ rejects}] = \frac{|B'|}{N} \leq \frac{1}{2c^s} \end{aligned} \tag{4}$$

So provided G is $(\frac{N}{2}, c)$-expanding, $\Pr[M' \text{ errs}] \leq \frac{1}{2c^s}$. Using this procedure, you can reduce error to $\leq \frac{1}{n^a}$ for any $a > 0$:

- Choose some constant $c > 1$ and $s = \Theta(\lg n)$ and any constant spectral gap expander graph family.
- Using Ramanujan graphs choosing $s = 1$ and $c = O(d)$, with d is some polynomial of n. Recall that Ramanujan graphs are $(\alpha N, \frac{1}{\alpha+(1-\alpha)\lambda_2^2})$-expanders, with $\lambda_2 \propto \frac{1}{\sqrt{d}}$. Varying α gives the freedom to modify the error reduction properties.

3 Randomness Efficient Error Reduction

3.1 The Idea

The algorithm for randomness efficient error reduction is similar to the algorithm for deterministic amplification. But instead of considering all bitstrings within some number of steps from the original bitstring, we will use additional random bits to construct a path through the expander and consider only bitstrings along that path. The setup for constructing M' from M is exactly the same as for deterministic amplification except for the generation of ρ'. Define $\rho' = \{\rho_0, \rho_1, ..., \rho_s\}$ where ρ_0 is the initial random seed and $\forall i, \rho_{i+1} \in \Gamma(\rho_i)$.

The total amount of randomness used in this procedure is: $|\rho'| = |\rho| + s \log_2 d$, where s is some polynomial in n and d is fixed. We can show that $\Pr[M' \text{ errs}] = 2^{\Omega(s)}$, which is to say we can make the error exponentially small with only a linear number of additional random bits.

3.2 Analysis

Theorem 1. $\Pr[M' \ errs] \leq (\epsilon + (1-\epsilon)\lambda_2)^s$ *where* $\Pr[M \ errs] \leq \epsilon$.

Proof. Consider the probability distribution after s steps on G given that each step remains in the bad set ($\forall i, \rho_i \in B$). This distribution can be described by the following expression:

$$(RA)^s Ru, \tag{5}$$

where A is still the normalized adjacency matrix of the expander, u is the uniform distribution over all vertices in the expander and R is the projection from G onto B ($R_{ii} = 1, v_i \in B$ and zero otherwise). Note, this is not a proper probability distribution because probabilities do not sum to one; mass is lost during the projections. The sum of the elements (the L_1-norm) of this distribution is the probability that M' errs because it represents the paths that never touch a witness for x even though $x \in L$:

$$\Pr[M' \text{ errs}] = \|(RA)^s Ru\|_1 \tag{6}$$

We would like to show:

$$\forall x, \|(RA)^s Ru\|_2 \leq (\epsilon + (1-\epsilon)\lambda_2)^2 \cdot \|x\|_2 \tag{7}$$

This would allow us to show (using Cauchy-Schwartz in the second step):

$$\begin{aligned} \Pr[M' \text{ errs}] &= \|(RA)^s Ru\|_1 \\ &\leq \sqrt{N}\|(RA)^s Ru\|_2 \\ &\leq \sqrt{N}(\epsilon + (1-\epsilon)\lambda_2)^s \|u\|_2 \\ &= \sqrt{N}(\epsilon + (1-\epsilon)\lambda_2)^s \frac{1}{\sqrt{N}} \\ &= (\epsilon + (1-\epsilon)\lambda_2)^s \\ \Pr[M' \text{ errs}] &\leq (\epsilon + (1-\epsilon)\lambda_2)^s \end{aligned} \tag{8}$$

$\square$

Now all we need to do is to prove that claim. The result for $(RA)^s$ can be acheived by repeatedly applying the following claim:

Claim 1. $\forall x, \|RARx\|_2 \leq (\epsilon + (1-\epsilon)\lambda_2)\|x\|_2$.

Proof. Recall the Rayleigh quotient:

$$\forall \text{ symmetric matrices } A', \max_{x \neq 0} \frac{\|A'x\|_2}{\|x\|_2} = \max_{x \neq 0} \frac{x^T A' x}{x^T x} \tag{9}$$

We can choose $A' = RAR$. Using this we can perform come manipulation on the LHS of the claim:

$$\frac{\|RARx\|_2}{\|x\|_2} = \frac{x^T RARx}{x^T x} = \frac{(Rx)^T A (Rx)}{x^T x} = \frac{y^T A y}{x^T x} \tag{10}$$

We rewrite Rx as y, note that $\|y\|_2 \leq \|x\|_2$ because R is a projection. Let,

$$y = y^{\|} + y^{\perp} \text{ s.t. } y^{\|} \parallel u, y^{\perp} \perp u. \tag{11}$$

Then we can expand the numerator of our term from the Rayleigh quotient:

$$y^T A y = (y^{\|})^T A y^{\|} + (y^{\|})^T A y^{\perp} + (y^{\perp})^T A y^{\|} + (y^{\perp})^T A y^{\perp} \tag{12}$$

u is an eigenvalue of A so that $Ay^{\|} = y^{\|}$. The cross terms disappear because $y^{\perp} \perp y^{\|}$. We are left with:

$$y^T A y = (y^{\|})^T y^{\|} + (y^{\perp})^T A y^{\perp}. \tag{13}$$

Since $y^\perp \perp u$ we know that $Ay^\perp \leq \lambda_2 y^\perp$. This allows us to rewrite the equation in terms of magnitudes:

$$|y^T Ay| \leq \|y^\|\|_2^2 + \lambda_2 \|y^\perp\|_2^2 = (1 - \lambda_2)\|y^\|\|_2^2 + \lambda_2 \|y\|_2^2 \tag{14}$$

Before we can complete the proof we need to bound $\|y^\|\|_2$:

$$\begin{aligned} y^\| &= \frac{u^T \cdot y}{u^T \cdot u} \cdot u \\ \|y^\|\|_2 &= \frac{|u^T \cdot y|}{\|u\|_2} = \frac{|\frac{1}{N}\chi_B^T y|}{\frac{1}{\sqrt{N}}} \\ &= \frac{1}{\sqrt{N}}|\chi_B^T y| \leq \frac{1}{\sqrt{N}}\|\chi_B\|_2 \cdot \|y\|_2 \\ &= \frac{\sqrt{B}}{\sqrt{N}}\|y\|_2 = \sqrt{\epsilon}\|y\|_2 \\ \|y^\|\|_2 &\leq \sqrt{\epsilon}\|y\|_2 \end{aligned} \tag{15}$$

Substituing this result back into our previous equation and using the fact that $\|y\|_2 \leq \|x\|_2$:

$$\begin{aligned} |y^T Ay| &\leq (\epsilon + (1 - \epsilon)\lambda_2)\|y\|_2^2 \\ &\leq (\epsilon + (1 - \epsilon)\lambda_2)\|x\|_2^2. \end{aligned} \tag{16}$$

Putting this back into the Rayleigh quotient we conclude the proof:

$$\|RARx\|_2 \leq (\epsilon + (1 - \epsilon)\lambda_2)\|x\|_2. \tag{17}$$

$\square$