CS 880: Pseudorandomness and Derandomization 4/24/2013

Lecture 16: Shrinkage

Instructors: Holger Dell and Dieter van Melkebeek Scribe: Lubos Krcal

DRAFT

This lecture is about the concept of shrinkage - a technique that is used to prove circuit lower bounds and construct pseudorandom generators. These techniques are very new - 2012.

1 Random Resctrictions

Definition 1 (Active variables). *These are partial assigments to the variables $\rho \in \{0,1,\star\}^n$. We call a variable active, it is was not assigned a value, $\rho_i = \star$. The set of active variables A of ρ is then $A(\rho) = \{i|\rho_i = \star\}$.*

Let's consider boolean function (circuit) f that takes n variables: $f : \{0,1\}^n \to \{0,1\}$.

Definition 2 (Restricted circuit). *A boolean function $f|_\rho : \{0,1\}^{A(n)} \to \{0,1\}$ that takes as an input only the active variables from ρ defined as:*

$$f|_\rho(y) = f(x), \text{ where } x_i \begin{cases} \rho_i & \text{if } i \notin A(\rho) \\ y_i & \text{if } i \in A(\rho) \end{cases}$$

Definition 3. *Let R_P be a distribution on $\{0,1,\star\}$, with proability p that it will be left active.*

$$\Pr[\rho_i = \star] = p$$

2 Warmup excercise

Before we start talking about shrinkage, let's look to a warmup excercise.

For this example, we will assume that when a variable is assigned a value, there is an equal probability it will be 0 or 1. Formally

$$\forall i : \Pr_{\rho\ R_P}[\rho_i = 0] = \Pr_{\rho\ R_P}[\rho_i = 1] = \frac{1-p}{2}$$

Let F be a k-CNF formula with m clauses. $F = (x_1 \vee \ldots \vee x_k) \wedge (\ldots) \wedge \ldots$. What is the effect of random restriction? With probability p, a variable will be set, and with probability, it will be set to $\frac{1-p}{2}$. So the probability $(1 - \frac{1-p}{2})^k$ corresponds to the probability, that a single clause will not have any variable assigned to 1 and thus remain in the formula.

Assuming the occurences of variables in the clauses are independent, then the expected value of remaining / usnatisfied clauses is:

$$\mathrm{E}_{\rho\ R_P}[\#\text{ unsatisfied clauses of } F|_\rho] \leq m\left(1 - \frac{1-p}{2}\right)^k$$

3 Branching program

Let's now have an extension of branching programs, that can read multiple variables in any order – these are not layered branching programs.

Definition 4 (Generalized branching program). *Directed graph with outdegree 2 and an arbitrary indegree. Each node has a label x_i that sais, which variable are we going to read at that node. We can read any variable arbitraty number of times. The general branching program will end either in accept or reject state.*

Definition 5 (Size of branching program). *The size S of the branching program B is the total number of states. It can be written based on the total number of occurences of all labels.*

$$S(B) = \#\ of\ states\ in\ B\ = \sum_i n_i\ ,\ where\ n_i = \#\ of\ occurences\ of\ label\ x_i$$

Now we look at what happens to branching programs under random restriction.

For a function $f : \{0,1\}^n \to \{0,1\}$, we let the $S(f)$ be the minimal size of a branching program B / circuit that computes f.

$$S(f) = \min_{B \equiv f} S(B)$$

Lemma 1. *If H is a subset of variables: $H \subseteq \{x_1, \ldots, x_n\}$. For $h \in \{0,1\}^H$, we let*

$$(\rho_h)_i = \begin{cases} h_i & if\ f_{x_i} \in H \\ \star & otherwise \end{cases}$$

In other words, h is a partial assigment / restriction h of $x_1 \ldots x_n$.

It would be very convenient to us, if we set the variables that occur very often. We will be able to show that most of the variables that occur often will be set with high probability.

We can then expres the size of the branching program with this restriction. For each assignment f, the size of the coresponding f is:

$$\forall f : S(f) \leq 2^{|H|} \left(\max_h S(f|_{rho_h}) \right) + 2^{|H|}$$

Proof. We can compute f with the following branching program: from the starting node, we create a branching program over h (the set part of the variables x). This is exactly $2^{|H|}$ branches. Then we append branching programs for only the unset variables (with variables from h already set) – $f|_{rho_h}$, with size of $S(f|_{rho_h})$. □

4 Shrinkage

Let $S = S(f)$ is the size of unrestricted branching program. The variable x_i is indicator random variable, so that $x_i = 0$, when $i \in A(\rho)$ and that occurs with probability p. Also note that $\sum n_i = S$b.

Lemma 2. *The expected value of restricted branching program is then:*

$$E_\rho[S(f|_\rho)] \leq E_\rho[\sum n_i x_i] = Sp$$

Lemma 3.

$$\Pr_{\rho \sim R_P}[S(f|_\rho) \geq 8^{\sqrt{clog(S)}} Sp] \leq S^{-c}$$

Proof. TODO □

References