CS 6815: Lecture 20

Instructor: Eshan Chattopadhyay Scribe: Juan C. Martínez Mori

November 6, 2018

1 Hardness vs. Randomness

Definition 1.1 (Boolean Circuits)**.** *A Boolean circuit C with n inputs is a directed acyclic graph with the following properties: i) There are n vertices of in-degree 0; these are called the inputs to the circuit and are labeled $x_1, x_2, \cdots, x_n$. There is one vertex with out-degree 0; this is called the output of the circuit. ii) Every vertex v that is not an input or the output is labeled with one Boolean function $b(v)$ from the set $\{AND, OR, NOT\}$. A vertex labeled with NOT has in-degree 1. iii) Every input to the circuit is assigned a Boolean value. Under such an assignment of input values, each vertex v computes the Boolean function $b(v)$ of the values on the incoming edges, and assigns this value to its outgoing edges. The value of the output is thus a Boolean function of $x_1, x_2, \cdots, x_n$; the circuit is said to compute this function. iv) The size of the circuit $|C|$ is the number of vertices labeled AND or OR (note that size is more often defined as the number of vertices in C).*

Definition 1.2 (Circuit Family)**.** *Consider a Boolean function $f : \{0,1\}^* \to \{0,1\}$. We denote by f_n the function f restricted to inputs from $\{0,1\}^n$. A sequence $\mathcal{C} = C_1, C_2, \cdots$ of circuits is a circuit family for f if C_n has n inputs and computes $f_n(x_1, x_2, \cdots, x_n)$ at its output for all n-bit inputs $(x_1, \cdots, x_n)$. We may denote the family $\mathcal{C}$ by $\{C_n\}_{n \geq 1}$. We say $\{C_n\}_{n \geq 1}$ is polynomial-sized if the size of C_n is bounded above by $S(n)$ for every n, where $S(\cdot)$ is a polynomial.*

Fact 1.3. *For any $f : \{0,1\}^n \to \{0,1\}$, there exists C which computes f and satisfies $|C| = O(2^n)$.*

Proof. Write the truth table of f and express it in conjunctive normal form (CNF). □

Fact 1.4. *There exists $f : \{0,1\}^n \to \{0,1\}$ such that if C computes f, $|C| = \Omega\left(\frac{2^n}{n}\right)$.*

Proof. A non-constructive proof can be obtained by a counting argument, but explicitly showing such a function is non-trivial. □

Fact 1.5. *Suppose $\mathcal{L} \subseteq \{0,1\}^*$ is decided by a Deterministic Turing Machine (DTM) which halts after $t(n)$ steps. Then, there exists $\{C_n\}_{n \geq 1}$ satisfying $|C_n| = \tilde{O}(t(n))$ such that $\{C_n\}_{n \geq 1}$ decides $\mathcal{L}$.*

Definition 1.6 (Hard Functions)**.** *$f : \{0,1\}^n \to \{0,1\}$ is average case (S, ϵ)-hard if for all circuits C satisfying $|C| \leq S$, we have*

$$\Pr_{x \sim U_n}[f(x) = C(x)] \leq \frac{1}{2} + \epsilon.$$

Intuitively, a function is *hard on average* if it is hard to compute correctly on randomly chosen inputs. In other words, no efficient algorithm can compute f much better than random guessing.

Definition 1.7 (Pseudorandom)**.** *A random variable X on $\{0,1\}^n$ is (S,ϵ)-pseudorandom if*

$$\left|\Pr_{x\sim U_n}[C(x)=1]-\Pr_{x\sim X}[C(x)=1]\right|\leq\epsilon,$$

where C is any circuit satisfying $|C|\leq S$.

Definition 1.8 (Pseudorandom Generator)**.** *A deterministic function $G:\{0,1\}^r\to\{0,1\}^n$ is a (S,ϵ) pseudorandom generator (PRG) if $G(U_r)$ is (S,ϵ)-pseudorandom.*

Note that we will allow G to run in time $2^{O(r)}$.

2 Derandomize BPP

Our *goal* now is to derandomize BPP. Suppose there exists G with $r=O(\log n)$, $S=n^{O(1)}$, $\epsilon=1/10$. That is, suppose we have a *dream PRG*. Then, let $A_x(r)\in BPP$ be a randomized algorithm running in time n^c (for some constant c) given x. $A_x(r)$ implies a circuit C_x satisfying $|C_x|\leq n^c$ such that

$$|\Pr[C_x(U_n)=1]-Pr[C_x(G(U_r))=1]|\leq\frac{1}{10}.$$

If this were the case, we could brute force over all seeds, obtaining a deterministic algorithm that runs in $n^{O(1)}$. Thus, we would have $BPP=P$.

3 Pseudorandom Generators from Average-Case Hardness

Lemma 3.1. *Suppose $f:\{0,1\}^n\to\{0,1\}$ is (S,ϵ)-hard. Then, $(U_n,f(U_n))$ is (S,ϵ)-pseudorandom. In other words, we stretch randomness by one bit.*

Proof. Let $X\sim U_n$ and $b\sim U_1$. We want to show that

$$|\Pr[C(x,f(x))=1]-\Pr[C(x,b)=1]|\leq\epsilon,$$

where C is any circuit satisfying $|C|\leq S$. By way of contradiction, suppose there exists C that satisfies the opposite. Consider the following algorithm A on input X. First, flip bit b. Then, if $C(x,b)=1$, output b, Otherwise, output $1-b$. We have the following claim.

Claim 3.2. *Let C be as in our assumption. Then, $\Pr[A(x,b)=f(x)]>\frac{1}{2}+\epsilon$.*

Proof. Let $\xi:b\sim U_1$. Then,

$$\begin{aligned}\Pr[A(x,b)=f(x)]&=\Pr[A(x,b)=f(x)|\xi]\Pr[\xi]+\Pr[A(x,b)=f(x)|\bar{\xi}]\Pr[\bar{\xi}]\\&=\Pr[A(x,b)=f(x)|\xi]\frac{1}{2}+\Pr[A(x,b)=f(x)|\bar{\xi}]\frac{1}{2}\\&=\frac{1}{2}\left(\Pr[A(x,b)=f(x)|\xi]+\Pr[A(x,b)=f(x)|\bar{\xi}]\right)\\&=\frac{1}{2}\left(\Pr[C(x,f(x))=1|\xi]+\Pr[C(x,\bar{f(x)})=0|\bar{\xi}]\right)\\&>\frac{1}{2}+\epsilon,\end{aligned}$$

where the inequality follows from our assumption. □

Claim 3.3. $\Pr[C(x, f(x)) = 1] - \Pr[C(x, \bar{f}(x)) = 1] \geq 2\epsilon$.

Proof.

$$\Pr[C(x, f(x)) = 1] - \frac{1}{2}\big(\Pr[C(x, f(x)) = 1] + \Pr[C(x, \bar{f}(x)) = 0]\big) > \epsilon,$$

based on the previous claim. □

This is a contradiction on f being hard. □

Theorem 3.4 (Nisan and Wigderson)**.** *If $f : \{0,1\}^n \to \{0,1\} \in \mathbb{E} = \mathbb{DTIME}(2^{O(n)})$ is (S, ϵ)-hard with $S = 2^{\delta n}$, $\epsilon = 2^{-\delta n}$ for some $\delta > 0$, then there exists a dream PRG.*

Proof. We use the following definition.

Definition 3.5. *$S_1, \cdots, S_m \subset [d]$ is an (n, k)-design if*

1. *$\forall i, |T_i| = n$, and*
2. *$\forall i \neq j, |T_i \cap T_j| \leq k$.*

Let $(f(Z_{|T_1}, f(Z_{|T_2}), \cdots, f(Z_{|T_l}) \in \{0,1\}^l$, where $Z_{|T_i}$ denotes the projection of Z on T_i. Let $G : \{0,1\}^r \to \{0,1\}^l$. We will continue the proof by contradicition.

We know use the *hybrid technique.* Let $D_0 : f(Z_{|T_1}, f(Z_{|T_2}), \cdots, f(Z_{|T_l})$, $D_1 : r_1, f(Z_{|T_2}), \cdots, f(Z_{|T_l})$, $D_2 : r_1, r_2, f(Z_{|T_3}), \cdots, f(Z_{|T_l})$, $\cdots$, $D_l : r_1, r_2, f(Z_{|T_3}), \cdots, r_l$. Note that D_i and D_{i+1} differ only at the $i+1$th position. By our assumption (and the triangle inequality), $\exists i$ such that

$$\Pr[C(D^i) = 1] - \Pr[C(D^{i+1}) = 1] > \frac{\epsilon'}{l}.$$

We will continue the proof **next time**. □