Complexity Theory II Course Instructor: V. Arvind

Lecture 4,5 : Aug 11, 2006

Lecturer: V. Arvind *Scribe: Ramprasad Saptharishi*

1 Overview

Hardness	PRG	Derandomization
$E \nsubseteq P/poly$	$n^\epsilon \rightarrow n$	$BPP \subseteq SUBEXP$
$E \nsubseteq SIZE(2^{\epsilon n})$	$\log n \rightarrow n$	$BPP = P$

In the first few lectures, we say that hardness → PRG, and then we saw that hardness → derandomization.

In this lecture we shall look at other implications between hardness, PRGs and derandomization

2 Hardness ↔ PRG

Theorem 1. *Suppose $G : \log n \rightarrow n$ be a quick PRG which is secure against circuits of size n, i.e*

$$\forall |C| \leq n, \left| \Pr_{y \in_R \Sigma^n}[C(y) = 1] - \Pr_{x \in_R \Sigma^{\log n}}[C(G(x)) = 1] \right| < \frac{1}{n}$$

then, there $\exists f, f \in E, f \notin SIZE(2^{\epsilon n})$.

Proof. Let $\log n = l$. $G' : l \rightarrow l + 1$ be the truncated version of G. Hence clearly

$$\forall |C| \leq n, \left| \Pr_{y \in_R \Sigma^{l+l}}[C(y) = 1] - \Pr_{x \in_R \Sigma^l}[C(G'(x)) = 1] \right| < \frac{1}{n}$$

$Range(G') = \{y | y = G'(x)\}$ and clearly $Range(G')$ is computable in E since given a y we can run through all $|x| = |y| - 1$ and check if $G'(x) = y$.

Claim: $Range(G') \notin SIZE(2^{\epsilon n})$

For if it were in $SIZE(2^{\epsilon n})$, it would mean that you can next bit predict G using a this circuit which will be of size $2^{\epsilon \log n} = n^\epsilon < n$, contradicting the hardness of G.

Thus we now have a language ($Range(G')$) which is computable in E but is not in $SIZE(2^{\epsilon n})$. □

And together with what we have done earlier, we have Hardness ↔ PRG.

3 Derandomizing Identity Testing

Impagliazzo and Kabanets then showed that derandomization has implications of lower bounds on arithmetic circuits. In this section we shall look at the main result of the paper "Derandomization identity testing means proving circuit lower bounds - Impagliazzo,Kabanets".

We would need to use the result from a paper by Impagliazzo, Kabanets and Wigderson in their paper "In search of an easy witness".

Theorem 2 (Impagliazzo,Kabanets,Wigderson)**.** *If $NEXP \subseteq P/poly$ then $NEXP = EXP$.*

We know from the [BFNW] result discussed in the earlier lecure, $EXP \subseteq P/poly$ implies $EXP = MA = AM$. And hence $NEXP \subseteq P/poly \Rightarrow NEXP = MA = AM$.

We shall give the proof this in section 4

3.1 The Permanent

$Perm_{\mathbb{Z}}(A)$: a degree n polynomial over n^2 variables.

$$Perm_{\mathbb{Z}}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)}$$

Let P_n be the function evaluating the permanent for an $n \times n$ matrix. And the permanent satisfies the following conditions:

$$\begin{aligned} P_1(x) &= x \\ P_i(x) &= \sum_{j=1}^{i} X_{1j} P_{i-1}(X_j) \end{aligned}$$

And more, any functions that satisfies the above properties has to be the permanent.

Summing up a few results we know already:

[Valiant79]: $Perm$ is $\#P$ complete

[Toda89]: $PH \subseteq P^{Perm}$

[BFNW + IKW]: $NEXP \subseteq P/poly \Rightarrow NEXP = EXP = MA = PH = P^{Perm}$

3.2 *ACIT*: Arithmetic Circuits for Identity Testing

$ACIT = \{C | C \text{ defines a polynomial} p, p = 0\}$.
Obviously, $\deg p \leq 2^{SIZE(C)}$. And we also know the Schwarz-Zippel lemma

Lemma 3 (Schwarz-Zippel)**.** *If $p : F^n \to F, p \neq 0$ of degree d, then for any subset $S \subseteq F$*

$$\Pr_{a \in S^n}[p(a) = 0] < \frac{d}{|S|}$$

Claim 4. *$ACIT \in coRP$*

Proof. We shall appeal to Shwarz-Zippel by choosing our $S = \{1, 2, 3, \ldots, 2^{s^2}\}$ for a size s circuit. Then the Schwarz-Zippel lemma would have bounded the error probability to $\frac{2^s}{2^{s^2}} \leq 2^{-s}$, but the value of $p_C(a)$ could be huge, as large as $2^{2^s s^2}$. Thus we need to do *chinese remindering*

Assume that $p_C \neq 0$. We would now evaluate C modulo a random $m \in \{2^{s^2}, \ldots, 2^{s^3}\}$. By the prime number theorem, atleast $\frac{1}{s^4}$ fraction of them would be primes.

Our bad case happens when either m is composite or m divides $p_C(a)$. Case 1 can happen with probability atmost $\left(1 - \frac{1}{s^4}\right)$. Now if $p_C \neq 0$, atmost 2^s primes in the range can divide it, and thus the probability that a random prime divides p_C is $\leq \frac{1}{s^4 2^s} < 2^{-s^2}$.

Hence, if $p_C \neq 0$

$$\Pr_{a,m}[p_C(a) \equiv 0 \mod m] \leq 2^{-s} + 2^{-s^2} + \left(1 - s^{-4}\right) \leq \left(1 - s^{-5}\right)$$

Repeating this over s^6 independantly chosen m from the range, we can get the error probability less than half, and thus $ACIT \in coRP$. □

3.3 Circuits for Permanent and Identity Testing

Define $ACP = \{(C, n) : C \text{ evaluates } Perm_{\mathbb{Z}}^{n \times n}\}$.

Claim 5. *$ACP \leq_m^P ACIT$*

Proof. Let C be a circuit evaluating a polynomial p over n^2 variables. Interpretting p_n to be a function of a matrix $\{x_{ij}\}_{i,j}^n$. Let p_i be the restriction of p_n to $\{i \times i\}$ matrices of variables. Thus if p_n evaluates the permanent, so will p_i on the restricted matrix.

Now define

$$\begin{aligned} h_1(x) &= p_i(x) - x \\ h_i(X) &= p_i(X) - \sum_{j=1}^{i} X_{1j} p_{i-1}(X_j) \end{aligned}$$

Now clearly if p_n evaluates the permanent, then each of the h_i has to be identically zero. And hence look at

$$h(x) = \sum_{i=1}^{n} h_i(X)^2$$

and C evaluates permanent *if and only if* $h = 0$. □

3.4 The Impagliazzo-Kabanets Theorem

Theorem 6 (Impagliazzo-Kabanets)**.** *If $ACIT \in SUBEXP$, either $NEXP \not\subseteq P/poly$ or $Perm_{\mathbb{Z}}$ does not have polysized arithmetic circuits.*

Also not that if $BPP = P$, then $NP = MA$. And we then can't have $NEXP \subseteq P/poly$ since it would then absurdly give $NP = NEXP$.

Proof. If $NEXP \subseteq P/poly$, $NEXP = P^{Perm} = NP^{Perm}$.

Claim: $NEXP \subseteq P/poly$, $Perm$ has poly sized circuits $\Rightarrow$ $NEXP \subseteq NP^{ACIT}$

Pf: Let $L \in NEXP$, and x an instance of L. Now by our assumption, $L \in NP^{Perm}$ and hence $L = \mathfrak{L}(M^{Perm})$ for some n^k time machine M.

This forces the largest permanent queries to be those of $n^k \times n^k$ matrices. Guess the permanent cirucit, can be done since the size of the circuit is polynomially bounded! In order to verify, we know that $ACP \leq_m^P ACIT$, so use that as a query for the oracle. And thus $NEXP \subseteq NP^{ACIT}$.

Now with this claim, if you further have that $ACIT \in SUBEXP$, we can then would be able to simulate $NEXP$ in NE thus giving an absurd implication that $NE = NEXP$. Hence the main theorem is proved. □

4 Proof of Theorem 2

Just like we have $P/poly$, and we shall use a similar notation $\mathcal{C}/f$.

Definition 7. *For any complexity $\mathcal{C}$ and function $f : \mathbb{N} \rightarrow \mathbb{N}$, $L \in \mathcal{C}/f$ if there exists a sequence of strings $\{y_i\}_{i \geq 0}$ with $|y_n| = f(n)$ and $L' \in \mathcal{C}$ such that for all $x \in \Sigma^*, x \in L \Leftrightarrow (x, y_{|x|}) \in L'$*

The proof of this theorem shall be broken down into the following steps:

1. $EXP \nsubseteq \text{i.o} - SIZE(n^c)$ for each c
2. $EXP \nsubseteq \text{i.o} - \left[DTIME(2^{n^c})\right]/n^c$ for each c.
3. $NEXP = EXP \Rightarrow EXP \nsubseteq \text{i.o} - \left[NTIME(2^n)\right]/n$
4. $NEXP \subseteq P/poly \Rightarrow EXP \nsubseteq \text{i.o} - \left[NTIME(2^n)\right]/n$
5. **Theorem:** If $NEXP \neq EXP$, then $AM \subseteq \text{i.o} - \left[NTIME(2^{n^\epsilon})\right]/n^\epsilon$ for every $\epsilon > 0$

4.1 Proof of Step 1

The number of boolean functions on length n inputs is 2^{2^n} and we saw earlier that the number of boolean functions that have size $\leq n^c$ is atmost $2^{n^{c'}}$ for some c'(depending on c)

Now the inputs are $x_1, x_2, \cdots, x_{n^c+2}, \cdots, x_{2^n}$. Define a function f as follows:

$$\begin{aligned} \forall i \leq n^c + 2 \quad &, \quad f(x_i) = b_i \\ \forall i > n^c + 2 \quad &, \quad f(x_i) = 0 \end{aligned}$$

where $b_i = \mathrm{m}aj(C(x_i))$ over all circuits $C \in SIZE(n^c)$.

Clearly this is in $DTIME(2^{n^{c+1}}) \subseteq EXP$ but not in $SIZE(n^c)$ at any length. □

4.2 Proof of Step 2

The number of boolean functions over n inputs is 2^{2^n}. Consider turing machine descriptions M of size $leqn$ with advice of size n^c, running for atmost 2^{n^c} steps. Let $\mathfrak{F}$ = All boolean functions from $\Sigma^n \rightarrow \Sigma$ computed by such turing machines. As earlier $|\mathfrak{F}| \leq 2^{n^{c'}}$.

And hence we can find a assignment of truth values to the first $n^{c'} + 2$ strings that diagonalises against $\mathfrak{F}$. The lexigraphically least of such assignments is our language in EXP, but not in i.o$-\left[DTIME(2^{n^c})\right]/n^c$. □

4.3 Proof of Step 3

We shall show that if $NEXP = EXP$, then $[NTIME(2^n)]/n \subseteq$ i.o $- \left[DTIME(2^{n^c})\right]/n$ for some fixed c. And then, using step 2 we would be done.

Let U be a universal non-deterministic turing machine that takes a pair (i, x) as input and simulates the ith non-deterministic machine M_i on x for $2^{|x|}$ steps and accepts iff M_i accepts x within that many steps. Hence

$$\mathfrak{L}(U) \in NTIME(2^{|x|+|i|})$$

Now for every language $L \in NTIME(2^n)$ can be decided in $NTIME(2^{|x|+|i|})$ where $|i|$ is the constant sized description of the machine accepting L. And by our assumption this can be simulated in $DTIME(2^{n^c})$ for some fixed c. Consequently, every language in $[NTIME(2^n)]/n$ can be simulated in $\left[DTIME(2^{n^c})\right]/n$, and the proof is done. □

4.4 Proof of Step 4

Just similar to the earlier proof, every language in $[NTIME(2^n)]/n$ can be simulated in $SIZE(n^d)$ for some fixed d and we would hence obtain a similar contradiction to 1 if 4 is false. □

4.5 Proof of Step 5

By the [BFNW] theorem we have that $EXP \nsubseteq P/poly$ would imply that $BPP \subseteq$ i.o $- SUBEXP$. The point to note here is that the proof of the theorem relativises!

For every oracle A,

$$EXP^A \nsubseteq P^A/poly \Rightarrow BPP^A \subset \text{i.o} - SUBEXP^{\text{``}A''}$$

where $SUBEXP^{\text{``}A''}$ is the class of $SUBEXP$ turing machines with oracle A but is allowed only small (polynomial sized) queries to the oracle.

In particular, when $A = SAT$,

$$EXP \nsubseteq P^{SAT}/poly \Rightarrow BP.NP = AM \subseteq BP.P^{NP} \subseteq \text{i.o} - NSUBEXP$$

Like in the BFNW case, if we can get hold of a "suitably hard" function, then we can derandomize AM into $SUBEXP$ non-uniformly.

Assume $NEXP \neq EXP$, let $\mathfrak{L}(M) = L \in NE, L \notin EXP$. Since L is a language in $NTIME(2^n)$, accepting paths of M are of size 2^n, one can interpret them as functions from Σ^n to Σ.

The number of oracle circuits of size n^c is atmost $2^{n^{c'}}$ for some c', and hence they can all be enumerated in EXP. Since $L \notin EXP$, there must exist infinitely many n such that there is an x_n of length n such that the accepting paths of M on x_n do not have polynomial sized circuits.

Pick an x_1 that fails for $c = 1$, and a larger string x_2 that fails for $c = 2$ and so on. Hence, this gives you an infinite sequence $\{x_n\}$ such that for every polynomial n^c, all but finitely many x_n's are such that $M(x_n)$'s accepting paths are not in $SIZE^{SAT}(|x_n|^c)$.

This basically shows that the computations paths are not in *P/poly* almost everywhere.

Consider advice strings of this form $z_n = 1 \cdot x_n$ if such an x_n exists at that length, and 0^{n+1} otherwise. Now with this advice, in $NTIME(2^{|z_n|})$ one can guess the computational path of $M(x_n)$, and we would get the hard function.

And now, with our Nisan-Wigderson design as in [BFNW] we can simulate $BP.NP = AM$ in $NSUBEXP$ with the advice z_n.

Hence $NEXP \neq EXP \Rightarrow AM \subseteq \text{i.o} - [NTIME(2^{n^\epsilon})]/n^\epsilon$ for every $\epsilon > 0$ □

4.6 Proof of Theorem 2

We have remarked earlier that if $NEXP \subseteq P/poly$, then $EXP = MA = AM$. And further, with step 5, $NEXP \subseteq P/poly$ and $NEXP \neq EXP$ would imply that $EXP = AM \subseteq \text{i.o} - [NTIME(2^n)]/n$.

Now, if $NEXP \neq EXP$ with the assumption that $NEXP \subseteq P/poly$, by 4 we have $EXP \nsubseteq \text{i.o} - [NTIME(2^n)]/n$, contradicting the above implication.

Hence $NEXP \subseteq P/poly \Rightarrow NEXP = EXP$ □

5 One more theorem

Definition 8. *$L \in MA \cdot EXP$ if there exists a polynomial time predicate $R(x, y, z)$ and a polynomial n^c such that if $x \in L$, there exists a $y \in \Sigma^{2^{n^c}}$ such that*

$$\Pr_z[R(x, y, z) = 1] \geq \frac{2}{3}$$

And if $x \notin L$,

$$\Pr_z[R(x, y, z) = 1] \leq \frac{1}{3}$$

Theorem 9. *$MA \cdot EXP \nsubseteq P/poly$, $ZEXP^{NP} \nsubseteq P/poly$*

Proof. If $EXP \nsubseteq P/poly$, then we are done. Otherwise, we know that $EXP = MA$. And just as $P = NP \Rightarrow EXP = NEXP$, we can extend $EXP = MA$ to $EEXP = MA \cdot EXP$.

But $EEXP \nsubseteq P/poly$, infact $DTIME(2^{n^{f(n)}}) \nsubseteq P/poly$ for any f that grows!

And $MA \subseteq ZPP^{NP}$ and hence again we have $ZEXP^{NP} \subseteq P/poly$ $\square$