Today
- Derandomization implies Circuit Lower Bounds
- Easy Witness Method

Lecture 32
Computational Complexity
(16 Jun, 2020)
Instructor: Prahladh Harsha

Recall some of the derandomization results

[NW] : $f \in E$ that is strongly average-case hard for $2^{\delta n}$-sized ckts
(ie, all ckts C of size $2^{\delta n}$ satisfy
$$\Pr[f(x) = C(x)] \leq \frac{1}{2} + \frac{1}{2^{\delta n}} \quad)$$
then $BPP = P$.

[IW] If $f \in E$ st f is worst-case hard for $2^{\delta n}$-sized ckts, then $BPP = P$

[In lecture, proof due to Sudan-Trevisan-Vadhan]

These proofs are stronger that they give some derandomization even on weaker hypotheses.

[IW'] : $f \in E$ st f is worst-case hard for 2^{n^ϵ}-sized ckts for all $\epsilon \in (0,1)$
$$\Downarrow$$
$$BPP \subseteq DTIME(2^{\text{polylog} n})$$

[IW'] $f \in E$ s.t. f is worst-case hard for n^c-sized ckts for all $c \geq 1$

$\Downarrow$

$$BPP \subseteq \bigcap_{\forall \varepsilon > 0} DTIME(2^{n^\varepsilon})$$

All these results are of the form

some ckt lower bd $\Rightarrow$ some derandomization of BPP

$\Downarrow$

a better upper bound for BPP than EXP.

Qn: Do we really need ckt lower bounds to prove these results?

Won't be able to show for BPP

But work w/ MA instead.

We can prove similar derandomization results for MA.

$f \in E$ s.t. f is worst-case hard against $2^{\delta n}$-sized ckts, then $MA = NP$

Today, these derandomization results of MA require circuit lower bounds

In fact derandomizing PIT requires circuit lower bounds.

Karp-Lipton Theorem: $NP \subseteq P/poly \Rightarrow NP \subseteq \Sigma_2^P$

Meyer's Theorem: $EXP \subseteq P/poly \Rightarrow EXP = \Sigma_2^P$

Strengthening of Meyer's Theorem due to Interactive Proofs.

Thm: $EXP \subseteq P/poly \Rightarrow EXP \subseteq MA$. ... (*)

Pf: Assume $EXP \subseteq P/poly$

Meyer's thm $EXP = PSPACE = \Sigma_2^P$

$PSPACE = IP$ and furthermore the prover in IP for PSPACE requires only poly space.

$PSPACE \subseteq P/poly$. (due to the hypothesis)

Hence, the IP-prover can be described by a poly-sized ckt

Consider the following MA-protocol for any $L \in PSPACE$

On input x

Merlin		Arthur
	$\xrightarrow{\text{poly-sized}}$ ckt that describes the prover	Arthur does the entire IP-protocol, using poly-sized ckt.

Hence $L \in MA$

ie, $PSPACE \subseteq MA$. Hence, $EXP \subseteq MA$. $\boxtimes$

This thm shows

any separation of MA from EXP implies a circuit lower bound.

Suppose, we had the following theorem

[IKW] $NEXP \subseteq P/poly \Rightarrow NEXP \subseteq MA$

This would imply any derandomization of MA implies a ckt lower bound.

Impagliazzo-Kabanets-Wigderson proved this using the easy-witness method

---

Polynomial-Identity Testing:

Theorem [Kabanets-Impagliazzo]

Suppose $PIT \in P$ (ie, PIT can be derandomized completely).

&

perm has poly-sized algebraic circuit.

$\Downarrow$

$P^{\#P} \subseteq NP$

Pf: Natural NP-alg for $P^{\#P}$ is as follows

① Guess the poly-sized alg ckt for permanent

② Use circuit to answer the oracle calls to perm.

Problem: How does one know that the guessed circuit is correct?

Use the fact that perm is downward self reducible.

$$\mathrm{Perm}_n(M_{n\times n}) = \sum_{i=1}^{n} M(1,i)\, \mathrm{Perm}_{n-1}(M^{(1,i)}) \quad \ldots (*)$$

Replace Step ①.

- (1a) Guess poly sized ckts $C_1 \ldots C_n$ for perm of matrix $1, 2, \ldots n$.

(1b) Check that C_i is correct if C_{i-1} is correct using the identity (*) (PIT ∈ P)

(1c) C_1 is obly correct

Hence, C_n is correct

☒

A combination of this & IKW thm implies any derandomization of PIT implies ckt lower bounds.

Theorem [Kabanets-Impagliazzo]. If PIT $\in P$ then one of the following must be true.

(a) $NEXP \not\subseteq P/poly$

(b) perm $\notin$ Alg P/poly.

Pf: For contradiction.

(1) PIT $\in P$

(2) perm $\in$ Alg P/poly

(3) $NEXP \subseteq P/poly$

(1) & (2) $\Rightarrow P^{\#P} \subseteq NP$

(3) $\Rightarrow NEXP \subseteq MA$

$NEXP \supseteq P^{\#P} \supseteq MA \supseteq NP$

$NEXP = NP$ – contradiction ✗

Hence, at least one of (1), (2) & (3) must be false ☒

A derandomization of PIT implies a ckt lower bd

(Proof can be strengthened to show any weak derandomization of PIT also implies circuit lower bds).

Easy-Witness Method

[IKW] NEXP $\not\subseteq$ EXP $\Rightarrow$ NEXP $\not\subseteq$ P/poly

$L \in \text{NEXP} \setminus \text{EXP}$.

$L \in \text{NEXP}$

$\Downarrow$

$\exists$ a relation $R(x,y)$ computable in time 2^{n^a} $n = |x|$

$x \in L \iff \exists y \in \{0,1\}^{2^{|x|^b}}$ s.t. $R(x,y)$ is true.

By padding, let's assume $a = b = 1$

$x \in L \iff \exists y \in \{0,1\}^{2^{|x|}}$ s.t. $R(x,y) = 1$

& R is computable in time $2^{|x|}$.

Can $y \in \{0,1\}^{2^{|x|}}$ - y can be thought of as a truth table of a fn. $f : \{0,1\}^n \to \{0,1\}$.

$x \in L \iff \exists f : \{0,1\}^n \to \{0,1\}$, $R(x, TT(f)) = 1$

f is easy if it can be computed by a poly-sized circuit (say n^c)

Suppose this were the case
that is for every $x \in L$, there is
a witness $y = TT(f)$ that is
n^c-easy (ie, f is computable by
a ckt of size n^c).

then the following exp-time alg
solves L.

(1) Go over all possible ckts of size n^c
(2) Check if the $TT(C)$ is a witness
& accept

Running time $= \#\text{ckts} \cdot 2^n = \exp(n)$.

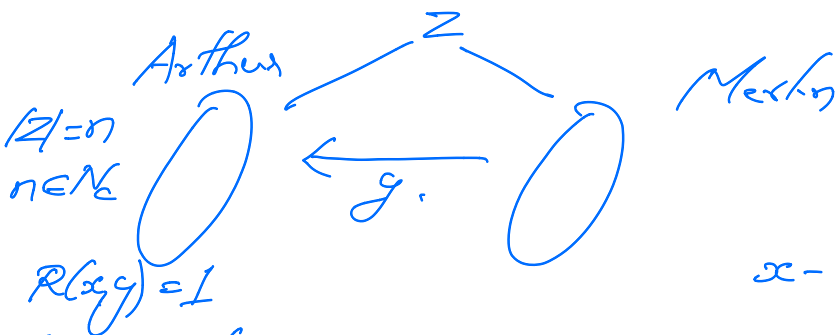
If $NEXP \neq EXP$, then there is
a $L \in NEXP \setminus EXP$ such that

for every $c \in \mathbb{N}$, there is an
infinite subset $N_c \subseteq \mathbb{N}$ s.t $\forall$
$n \in N_c$, there exists an $x \in L$.

- $|x| = n$
- $x \in L$.
- every witness for x is <u>not</u>
easy.

$NEXP \neq EXP \Rightarrow MA \subseteq co\text{-}NTIME(2^{n^a})/n$
for some a

Use above to derandomize MA



$L \in MA$

$z \overset{?}{\in} MA$

x - advice string

Use y to as the basis for PRG & derandomize his random steps.

$MA \subseteq \text{co-}NTIME(2^{n^a})/n$. if $NEXP \neq EXP$.

—

Completing: IKW proof:

Thm: $NEXP \subseteq P/poly \Rightarrow NEXP \subseteq MA$

Pf: $NEXP \subseteq P/poly \Rightarrow EXP \subseteq P/poly$

$\Rightarrow EXP = MA$.

Cases

(i) $NEXP = EXP$: $NEXP = MA$ ✓

(ii) $NEXP \neq EXP$: $MA \subseteq \text{co-}NTIME(2^{n^a})/n$

$EXP \subseteq \text{co-}NTIME(2^{n^a})/n$

↪ diagonalization is false.

This case cannot arise ⊠