Computational Complexity

Mohammad Mahmoody

Session 9

11 Feb 2014

Last time

- Diagonalization as in the proof of Halting Theorem

- Time Hierarchy Theorem Using “Diagonalization Technique”

Today

- A comment about the proof of Time-Hierarchy theorem

- Limits of Diagonalization Technique:

  A "similar proof" to "time hierarchy theorem" cannot prove $\mathbf{P} \neq \mathbf{NP}$

Ptime $(n^2) \not\supseteq$ Dtime$(10n)$

Proving $\mathbf{Dtime}(n^{k+1}) \neq \mathbf{Dtime}(n^k)$

$c \cdot T \cdot \log T$

- Recall Universal TM:
UTM gets (M, x) as input, simulates T steps of $M(x)$ in time $O(T \log T)$

Construct language $L \in$ Dtime(n^2) but $L \notin$ Dtime$(10n)$

def of L: given x : if run x over x for time $n^{1.5}$ t

$\begin{cases} \text{if } x \text{ accepts } x \Longrightarrow \text{reject} : x \notin L \\ \text{oth.} \Longrightarrow x \in L \end{cases}$

claim 1

$L \in$ Dtime$(t \log t) \simeq$ Dtime$(c \cdot n^{1.5} \cdot \underbrace{\log(n^{1.5})}_{=\log(n)}) \subseteq$ Dtime(n^2) ? $< n^2$

claim 2: $L \notin$ Dtime$(10n)$; $\exists M$ solves L in $10n$

Run M over M $\begin{cases} \text{accep} \to \text{reject} \\ \text{rej.} \end{cases}$

Can a "similar proof" show $\mathbf{P} \neq \mathbf{NP}$?

Thm 1

$P^O \overset{?}{=} \bigcup_k \mathrm{Dtime}^O(n^k)$

- Recall how we showed $\mathbf{Dtime}(n^{k+1}) \neq \mathbf{Dtime}(n^k)$

$\bigcap \quad \supseteq \quad \bigcap$

$NP^O \overset{?}{=} \bigcup_k \mathrm{NDtime}^O(n^k)$

- Claim:
  Same proof shows that $\mathbf{Dtime}^{\mathbf{O}}(n^{k+1}) \neq \mathbf{Dtime}^{\mathbf{O}}(n^k)$ for any oracle **O**
  $\mathbf{Dtime}^{\mathbf{O}}(n^k)$: languages decidable in time n^k given oracle access to **O**

~~Proof of~~ Thm 1 relativizes : (Thm 1 holds relative to any oracle O)

Only needs $\left(\begin{array}{c}\text{UTM}\\ \text{Simulation}\end{array}\right)$ holds relative to any oracle.

Can a "similar proof" show $\mathbf{P} \neq \mathbf{NP}$?

- Same proof shows that $\mathbf{Dtime}^{\mathbf{O}}(n^{k+1}) \neq \mathbf{Dtime}^{\mathbf{O}}(n^k)$ for any oracle $\mathbf{O}$

$\mathbf{Dtime}^{\mathbf{O}}(n^k)$: languages decidable in time n^k given oracle access to $\mathbf{O}$

recall proof without O:

$k=1$

Defined L: given x $\boxed{\text{run } x \text{ over } x \text{ for } n^{1.5} \text{ steps}}$ with help of O

and flip answer

* $L \in \cancel{O(n^2)}$: $\text{Dtime}^{O}(n^2)$

$L \notin \cancel{O(n)}$: $\text{Dtime}^{O}(10n)$

$M \in L \to M \notin L$

$M \notin L \to M \in L$

$\mathrm{Dtime}(n^k) \neq \mathrm{Dtime}(n^{k+1})$ $\mathrm{Ntime}(n^k) \neq \mathrm{Ntime}(n^{k+1})$

There exists oracle $\mathbf{O}$ such that $\mathbf{P^O} = \mathbf{NP^O}$

$\Rightarrow$ There exist no "relativizing" proof for $P \neq NP$

if proof of $P \neq NP$ relativize $\Rightarrow$ $P^O \neq NP^O$ for any O

$\underbrace{P^{SAT}}_{\text{includes } NP,\ coNP} \overset{?}{=} NP^{SAT}$ $= NP$

O = Exptime oracle: $\begin{cases} \text{query: } (M, x, 1^t) \\ \text{answer: } M(x) \text{ after } 2^t \text{ steps. Yes/No} \end{cases}$

① P^O = Exptime.

② NP^O = Exptime

$O =$ query : $(M, x, 1^t)$

answer : $M(x)$ accepts / reject in 2^t

P^O = Exptime $\qquad NP^O$ = Exptime

$\underline{Exp \subseteq P^O} \subseteq NP^O \subseteq Exp$

$L \in EXP$: $\exists M$ solves $x \overset{?}{\in} L$ in 2^{n^c} ($t = n^c$)

given x : ask O query $(M, x, 1^{n^c})$: answer = $x \overset{?}{\in} L$

$NP^O \subseteq EXP$: given x : question does NTM M^O accep x (in any branches) : $\boxed{\text{enumerate all branches of } M \text{ and solve all } O \text{ queries}}$