Lecture 8

$$DTIME(f) \subsetneq DTIME(g)$$

$$f = o\left(g/\log g\right)$$

$$NTIME(f) \subsetneq NTIME(g)$$

$$f(n+1) = o(g(n))$$

NP-Intermediate Languages

Q: are all NP langs NP complete?

- Thm: If $P \neq NP$ then $\exists\, L \in NP \setminus P$ s.t. L is not NP-complete

I.e., If all $\forall L \in NP \setminus P$

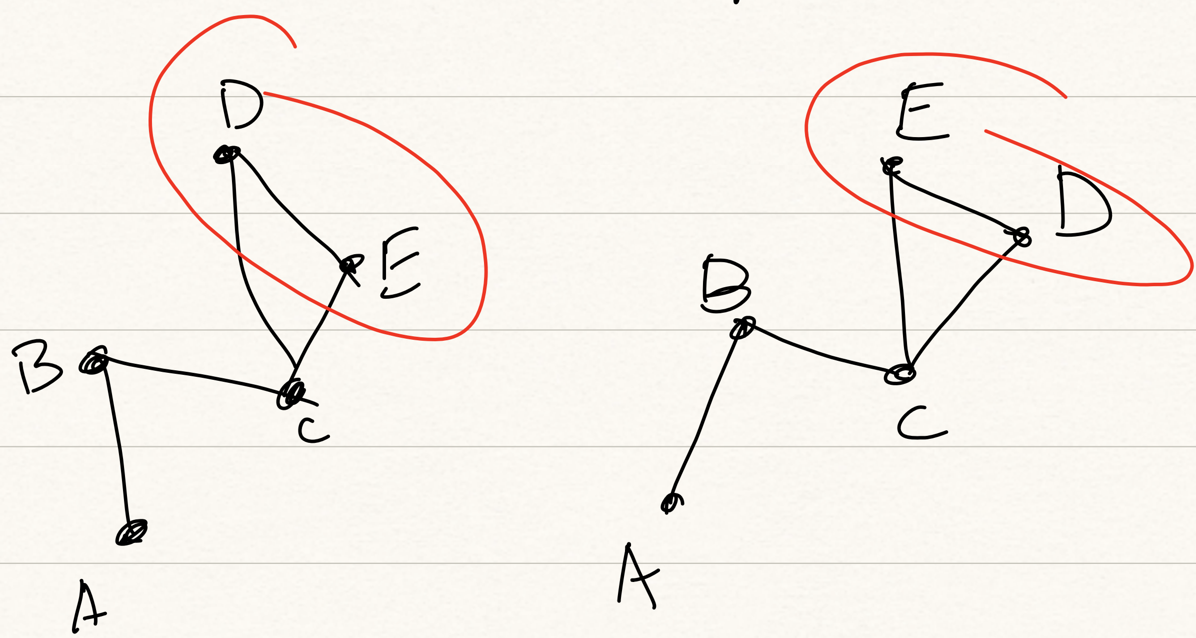
s.t. L is NP-complete,

then $P = NP$.

- 2 example

① Factoring

② Graph isomorphism



Oracle Machines

- When we showed

$$\mathrm{DTIME}(f) \subsetneq \mathrm{DTIME}(g)$$

M s.t. D decides here

$$L(M) = L(D)$$

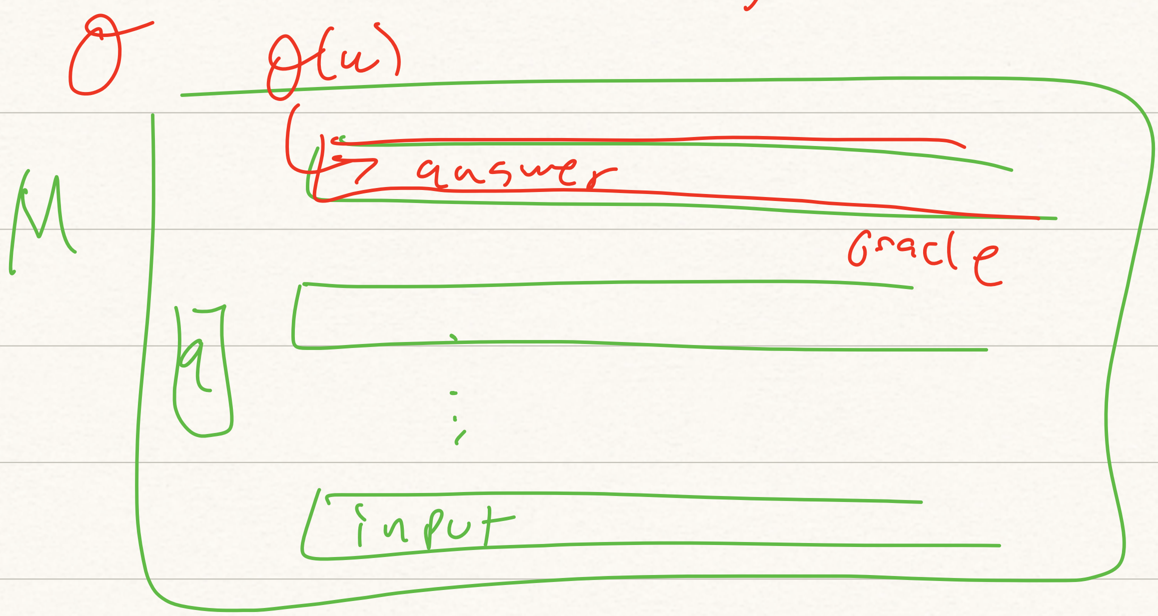
① I can always eff. represent M as $\langle M \rangle_2$

② D simulated M given $\langle M \rangle_2$ in time $T \log T$ where T is time of M

* D doesn't know anything about the internals of M.

Oracle TM

- TM's with an extra oracle tape, and an oracle $\mathcal{O}$
  - $M^{\mathcal{O}}$ can query $\mathcal{O}(u)$ in 1 time step and get answer



- If M is a TM and L is a language, then

  M^L is given oracle to a decider for L.

P^L = all poly-time decidable languages relative to oracle L.

NP^L = same thing but with NTM

$P^{SAT} = \{$ langs L decidable by a poly-time det. oracle TM w/ oracle SAT $\}$

$\hookrightarrow SAT(\phi) = 1$ iff ϕ is SAT

<u>Ex</u>: $\overline{SAT} = \{\phi : \phi$ is unsat. $\}$

$\overline{SAT} \in P^{SAT}$

- Given $M^{SAT}(\phi)$
  - Output opposite of $SAT(\phi)$

$\overline{SAT} \in P^{INDSET}$

- For any $L \in P$

  $P^L = P$

  - $P \subseteq P^L$
  - $P^L \subseteq P$

- $\overset{E}{\overset{\shortparallel}{EXPCOM}} =$

  $\{ (M, x, 1^n) : M(x) = 1 \text{ within } 2^n \text{ steps} \}$

$P^E = NP^E = EXP$

① $EXP \subseteq P^E$

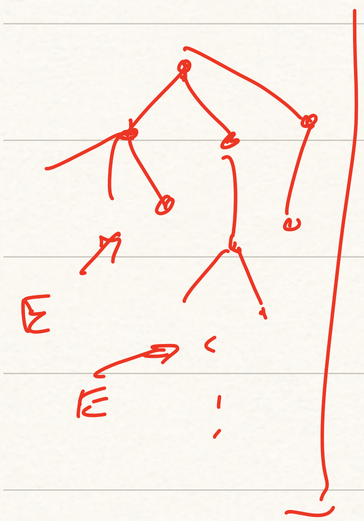
can do a single exponential-time computation with one oracle call

(2) $P^E \subseteq NP^E$ → trivially

(3) $NP^E \subseteq EXP$

→ simulate E in exp time ✓

runtime $= n$



n is length of ... path

→ Run all computation paths of NTM in $O(2^n)$ time

→ EXP time

longer ...

Limits of Diagonalization

① I can always eff. represent M as $\langle M \rangle_2$

② D simulated M given $\langle M \rangle_2$ in time $T \log T$ where T is time of M

Theorem: There exists oracles A, B such that

① $P^A = NP^A$

② $P^B \neq NP^B$

Proof

① $A = EXPCOM$ □

② we use diagonalization.

We're going to construct B.

First, for any $L \subseteq \{0,1\}^*$
Let

$$U_L = \{ 1^n \mid \exists x \in L : |x| = n \}$$

Notice: $U_L \in NP^L$ $\forall L$

How?

- $\tilde{M}^L(1^n)$:
  - guess $x \in \{0,1\}^n$
  - check $L(x)$
  - output accordingly

Constructing B so $\underline{U_B}$ & P^B

① • Set $B = \emptyset$
• Let $Q = \emptyset$
• Let $B' = \emptyset$

② $\underline{\text{Step 1}}$:

- Let M_1 be the deterministic oracle TM represented by $\langle 1 \rangle_2$
- For simplicity, assume $M_1(|x|)$ runs in time $O(|x|)$
- Choose n s.t. $2^n > n$
- Run $M_1^B(1^n)$: oracle machine

- $M_1^B(1^n)$ will make some

oracle queries

$q_1, \dots, q_k$ (is $q_i \in B$?)

- Reply NO/Reject/0 for all of these queries.
- Add $q_1, \dots, q_a$ to Q

11011

- If $M_i^B(1^n) = 1$ $\quad 1^n \in U_B \Leftrightarrow \exists x \in \{0,1\}^n$, $x \in B$
  - Add $\{0,1\}^n$ to B

Things Not in B

$\forall x \in \{0,1\}^n$, $x \notin B$

- Else $M_i^B(1^n) = 0$ $\quad 1^n \notin U_B \Leftrightarrow \nexists x \in \{0,1\}^n$ s.t. $x \in B$
  - Find $x^* \in \{0,1\}^n$ s.t. $x^* \notin Q$

- Add all $\{0,1\}^n \setminus \{x^*\}$ to B'
- Add x^* to B

(3) For $i = 2, 3, \ldots$

- Assume M_i runs in time n^i for length n inputs
- Choose n s.t. $2^n > n^i$
- Run $M_i^B(1^n)$
  - $M_i^B(1^n)$ make queries $q_1, \ldots, q_k \rightarrow$ add to Q
  - For each $j \in [k]$:
    - If $q_j \in B'$ reply NO
    - If $q_j \in B$

reply YES

- If $M_i^B(1^n) = 1$
  - Put all $\{0,1\}^n$ in B'
  - Declare $\forall x \in \{0,1\}^n$ $x \notin B$
- If $M_i^B(1^n) = 0$
  - Find $x^* \in \{0,1\}^n$ $x^* \notin Q$
  - ~~Add x^* to B~~
  - Add $\{0,1\}^n \setminus \{x^*\}$ to B'
- ⋮

- For each M_i, there are infinite # of equivalent poly-time oracle machines

$\Rightarrow U_B \in P^B$ $\square$

Lecture 8