Computational Complexity : Lecture 6.

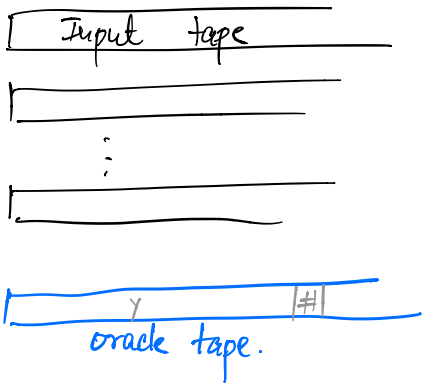
Recap:
- Det. & non-det. time hierarchy theorems.
  "with more time comes more responsibility"
- Ladner's Thm: If $P \neq NP$, then there are languages that are of "intermediate" complexity.
- Diagonalisation:
  - Systematically enumerate TM source code.
  - Simulate them for some bounded amount of time.
  - Do something with their output.

Main Qn for today: What are some limits to such techniques?

Oracle TMs:

TM has access to a God that speaks one language.

$A \subseteq \{0,1\}^*$ A- oracle TMs.



query resp. y
resp no.

You instantaneously know if $y \in A$ or not.

What can we compute now?

$DTIME^A(n)$

$P^A = \{ L(M^A) : M \text{ is an oracle TM that always runs in poly time} \}$

$NP^A = \{ L(M^A) : \text{" .. an oracle NTM ... } \}$.

Qn: Are these languages in P^{SAT} ? Cook-Levin ⇒ any $L \in NP$ reduces to CNF-SAT.

- SAT — Yes.
- Smallest vertex cover.
- TAUT — Yes.

Qn: If $A \in P$, what can you say about P^A ? P

Qn: What about NP^{SAT} ? PH will tell you more...

▷ TAUT

▷ (φ, k) is there a $\psi \equiv \varphi$ s.t $|\psi| \leq k$?

Guess ψ Ask: $\psi(x) \equiv \varphi(x)$ satisfiable ?

Qn: Is $DTIME^A(n^2) \subsetneq DTIME^A(n^3)$?

Or $NTIME^A(n^2) \subsetneq NTIME^A(n^3)$.

Yes! Exactly the same proof.

That proof was "insensitive" to the inner workings of M. In part, if M had oracle tapes.

This can also be a limitation.

Thm: [Baker-Gill-Solovay]. There is an oracle $A \subseteq \Sigma^*$ such that $P^A = NP^A$.
And there is an oracle $B \subseteq \Sigma^*$ s.t $P^B \neq NP^B$.

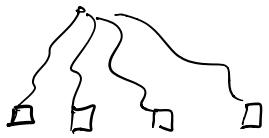
∴ Oracle insensitive arguments <u>cannot</u> hope to resolve P vs NP.

Pf: Want to find $A \subseteq \Sigma^*$ s.t the "non-determinism" of TM is irrelevant.

A be any EXP-complete language.

Claim: $P^A = NP^A = EXP$.

$P^A \subseteq NP^A \subseteq EXP \subseteq P^A$



Run through all guesses made by machine.
Solve queries as it comes.

The fun direction is to show there is a $B \subseteq \Sigma^*$ s.t $P^B \neq NP^B$ provably!

$L_B = \{ 1^m : \exists x \in B \quad |x| = m \}$.

Obs: For <u>any</u> B, $L_B \in NP^B$

Pf: Guess x of length m (inp)
Query B to check if $x \in B$. □

Idea: Design B s.t $L_B \notin P^B$
by diagonalisation!

Defining B in stages:
$M_1, M_2, \ldots$ oracle TMs.

Stage i: (diag against M_i)

Choose a length n not considered so far.
Run M_i by plugging in B as oracle.
When M_i queries y

Run for $2^{n/100}$ steps.
- if already committed to y, answer accordingly.
- Else, answer "No".

If M_i accepts 1^n, put <u>no</u> string of this length in B.

If M_i rejects 1^n, add some string of length n to B.

Details under the rug:

If M_i runs in n^{c_i} time, want to make sure that $2^{n/100} > n^{c_i}$

every machine shows up inf. often in the listing.

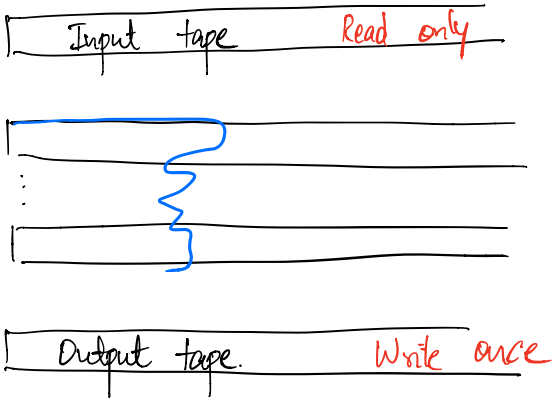
Remarks:
- Most techniques we have for separations "relativises".
  - There are a few that don't relativise! (IP = PSPACE, the PCP theorem)
  - NOT the same as "what if $A \in P$" !

Space Complexity:

What can (& can't) you do with space as the resource?

Meaningful to talk about "sublinear space" too. (Streaming applications etc.)

Space bounded TMs.



$L \in SPACE(S(n))$ if there is a det. TM M that decides L s.t on any input x accesses $\leq c \cdot S(|x|)$ work space cells.

"" for $NSPACE(S(n))$ - there is an NTM deciding L that, on every non-det computation, accesses $\leq c \cdot S(|x|)$ cells.

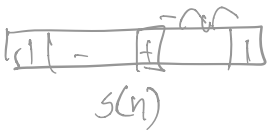
Convention: $S(n) \geq \log n$

Defn: $S: \mathbb{N} \to \mathbb{N}$ is space constructible if $S(|x|)$ can be computed in $SPACE(S(n))$

Obs: $DTIME(S(n)) \subseteq SPACE(S(n))$

Pf: Duh!

Qn: $DSPACE(S(n)) \subseteq DTIME(?)$



$S(n)^2$?

$2^{O(S(n))}$

Thm: $DTIME(S(n)) \subseteq SPACE(S(n)) \subseteq NSPACE(S(n))$

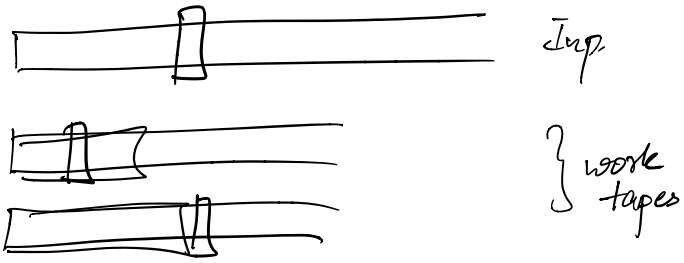
$\subseteq$

$DTIME(2^{O(S(n))})$

Any ideas?

Configurations.

(q, head positions, content of workspace)



How many configurations are there? (on an input x)

$$|Q| \cdot n \cdot S(n)^2 \cdot |\Sigma|^{2 \cdot S(n)} = 2^{O(S(n))}.$$

So what? What does this have to do with computation?

Configuration graphs

– Next time.