Lecture 09

Note Title

Today

- More Alternation
- Polynomial Hierarchy
- The "Infinite Hierarchy" Assumption
- Karp Lipton

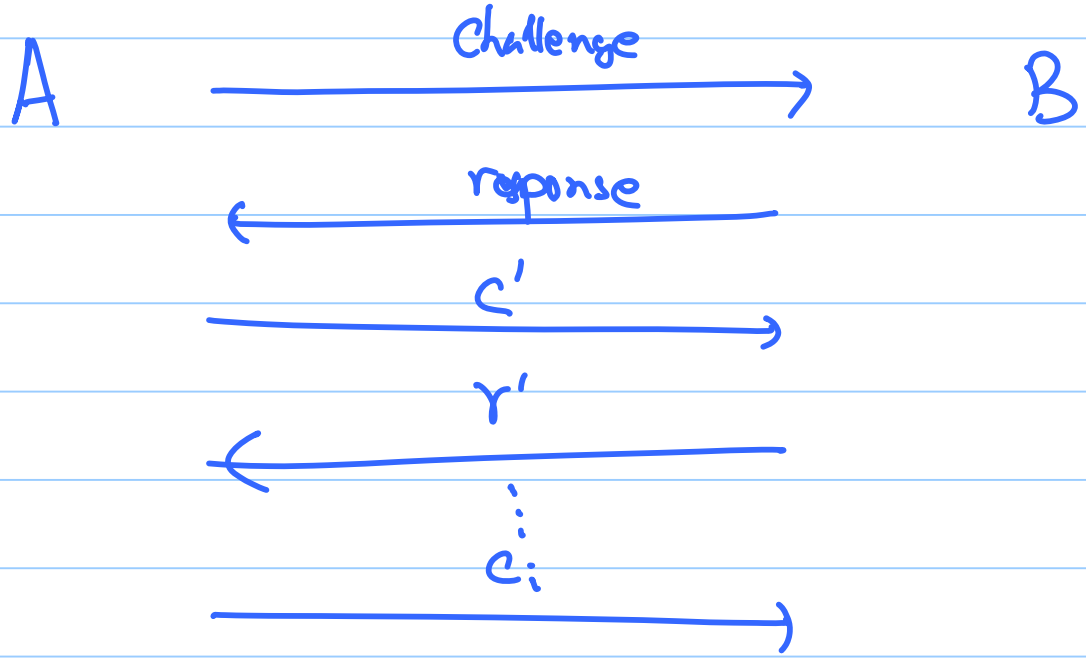
I.H.A. $\Rightarrow$ NP $\not\subseteq$ $P/_{poly}$.

Yesterday: Alternation Gives New Insights On Time + Space.

Today: Alternation Interesting In Itself.

DEBATES & ALTERNATION

Imagine setting up a debate between two players:



A claims X is true

B " " " not true

Question: Why does the listener want to hear this debate?

- Presumably to learn whether X is true or not.

But why does the listener not decide this on his/her own?

- Presumably he lacks computational power to decide; while debaters know more, at least in reference to X.

- But why an exchange? Why not have A, B send their statements to you?

- Presumably, makes a difference

- How to decide # rounds? Should we stop after 2? Who should go first?

- Believe These make differences too!

How to study formally?

- Create Model of computation

Verifier / Referee: polynomial time alg.

V

$L = \{X \mid X \text{ is "true"}\}$

Completeness: X is true $\Rightarrow \exists a_1 \forall a_2 \ldots Q_k a_k$

$V(X, a_1 \ldots a_k) = \text{true}$

Soundness: X not true $\Rightarrow \forall a_1 \ldots \overline{Q_k} a_k$

$V(X, a_1 \ldots a_k) = \text{false}.$

Question: How complex an assertion X can be debated like this?

Maybe needs 4 rounds

("Is Lewis Libby Guilty"

0 rounds ("Does raising taxes improve quality of life"

6 rounds ("Who'll make a better president"

———x———

- Does increasing # rounds help?
- Does it matter who speaks first?

———x———

- $\Sigma_i^P = \{ L \mid$ ("$x \in L$" prosecution speaks first & i rounds of debate $\}$
- $\Pi_i^P = \{ L \mid$ ("$x \notin L$") defense speaks first & i rounds of debate $\}$

Equivalently

- $\Sigma_i^P = \{ L \mid$ L decided by ATM in polytime with i alternations starting with $\exists$-quantifier $\}$
- $\Pi_i^P = \{ L \mid$ L decided by ATM in polytime with i alternations starting with $\forall$-quantifier $\}$

(Only subtlety $\supseteq$ work postponed to end).

Belief So Far

- $\forall i \; \Sigma_i^P \neq \Sigma_{i+1}^P$ ← IHA

Facts

- Defn:

$$i\text{-}\exists\text{-TQBF} = \{ 3\text{CNF } \phi \mid \exists x_1 \in \{0,1\}^n, \; \forall x_2 \in \{0,1\}^n, \; \vdots \; Q_i x_i \in \{0,1\}^n \; \phi(x_1 \ldots x_i) = \text{true} \}$$

- $i\text{-}\exists\text{-TQBF}$ is Σ_i^P- Complete
- $\Sigma_i^P = \{ L \mid \bar{L} \in \Pi_i^P \}$
- $\Sigma_i^P = NP^{(i-1)\text{-}\forall\text{-TQBF}}$ [remember relativization]

- $\Sigma_i^P = \Sigma_{i+1}^P \overset{①}{\iff} \Sigma_i^P = \Pi_i^P$

$\overset{②}{\Rightarrow} \Sigma_j^P = \Pi_j^P = \Sigma_i^P \quad \forall\, j \geq i$

Proof:

$\overset{①}{\Rightarrow} \Pi_i^P \subseteq \Sigma_{i+1}^P = \Sigma_i^P$ ✓

$\overset{①}{\Leftarrow}$ Consider $L \in \Sigma_{i+1}^P$ given by

refere V.

Consider question $x \in L$?

i.e. $\exists\, y_1\, \forall y_2 \ldots\ Q_i\, y_i \quad V(x, y_1 \ldots y_i)$?

Consider $L' = \{ (x, y_1) \mid \forall y_2 \ldots\ Q_i\, y_i$

$V(x, y_1, \ldots y_i)\ ? \}$

$L' \in \Pi_i^P = \Sigma_i^P \Rightarrow \exists\, V'$ s.t.

$L' = \{ (x, y_1) \mid \exists z_2, \bar{Q} z_i \quad V'(x, y_1, z_2 \ldots z_i)? \}$

$$\Rightarrow L = \{ x \mid \exists (y, z_2), \forall z_3 \dots \bar{Q}_i z_i \; V'(x, y, z_2 \dots z_i) \}$$

$L \in \Sigma_i^P$ ☒

(2) $\Longrightarrow$. By induction on $(j-i)$.

. Base case already proven.

. $\Sigma_i^P = \Sigma_{i+1}^P \Rightarrow$

$$\Sigma_{i+2}^P = NP^{\Sigma_{i+1}^P} = NP^{\Sigma_i^P} = \Sigma_{i+1}^P = \Sigma_i^P$$

$$\vdots$$

$$\Sigma_j^P = \Sigma_i^P$$

$$\vdots$$

☒

" First collapse $\Rightarrow$ total collapse .... "

- Polynomial Hierarchy = $PH = \bigcup_{i \geq 0} \Sigma_i^P$

$= \bigcup_{i \geq 0} \Pi_i^P$

- IHA $\Rightarrow$ $P \neq NP$

Infinite Hierarchy Assumption

$\Sigma_0^P \uparrow \quad \uparrow \Sigma_1^P$

But not $\Leftarrow$.

IHA:
- Strongest of many assumptions we make;
- But not refuted (so far)
- Might as well try to refute this first....

[Karp-Lipton] Theorem :

$$\text{1tA} \Rightarrow \text{NP} \not\subseteq \text{P/poly}$$

Motivation: • We tried proving $NP \not\subseteq P/poly$, as a route to proving $NP \neq P$.

• But maybe $NP \neq P$ but $NP \subseteq P/poly$;

• after all $P/poly$ has undecidable problems

• [KL] true, but non-uniformity is not so powerful on its own; unless we really know how to deal with quantif

Proof :: [of KL Theorem]:

Recall: Wish to show

$$NP \subseteq P/_{poly} \Rightarrow \Sigma_3^P = \Pi_3^P$$

Idea: • Will try to guess small circuit that solves NP;

• Can verify if C computes SAT in the hierarchy!

• How? $C \equiv SAT$

$\Leftrightarrow \forall \phi,$

$C(\phi)=1 \Rightarrow \exists y$ s.t. $\phi(y)=1$

$C(\phi)=0 \Rightarrow \forall z \quad \phi(z)=0$

- More crisply:

$C \in SAT \Leftrightarrow$

$\forall \phi, z \; \exists y$ s.t.

$\left((C(\phi) = 1) \text{ and } (\phi(y) = 1) \right)$

OR $\left((C(\phi) = 0) \text{ and } (\phi(z) = 0) \right)$

- $NP \subseteq P/_{poly}$ yields following alg. for satisfiability

$\psi \in SAT \Leftrightarrow \exists C \; \forall \phi, z \; \exists y$ s.t.

$C(\psi) = 1$ and $\Big(\left((C(\phi) = 1) \cdot (\phi(y) = 1) \right)$ OR $\left((C(\phi) = 0) \cdot (\phi(z) = 0) \right) \Big)$

- Did we just prove $SAT \in \Sigma_3^P$?

- Additional ideas: • Can use this idea for bottom level of any Σ_i^P / Π_i^P computation;

• Can guess C & verify its correctness in parallel to real computation.

Proof: Fix $L \in \Pi_3^P$

$$= \{ \psi \mid \forall x_1 \exists x_2 \forall x_3 \; \psi(x_1, x_2, x_3) = \text{true} \}$$

Let $L' = \{ (\psi, x_1, x_2) \mid \forall x_3 \; \psi(x_1 x_2 x_3) \}$

$L' \in$ co-NP $\subseteq P/_{poly}$

So there exist circuit C deciding L'

$L = \exists C$ (parallel)

$\forall \phi, z$,, x_1

$\exists y$,, x_2

$$C(\psi, x_1, x_2) = 1$$

and $\Big[$ $(C(\phi)=1)$ and $(\phi(y)=1)$

or $(C(\phi)=0)$ and $(\phi(z)=0)\Big]$

Clearly $L \in \Sigma_3^P \Rightarrow \Sigma_3^P = \Pi_3^P$

$\Rightarrow \neg(IHA)$