CS221 LECTURE 7

2/13/2018

TODAY

MORE ALTERNATION

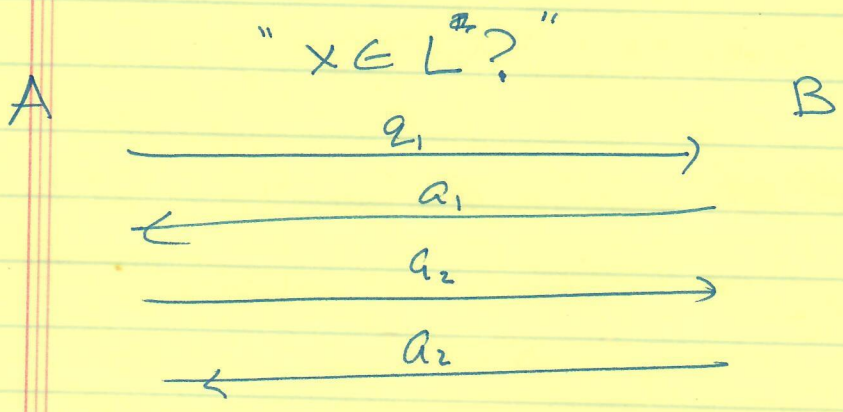
- POLYNOMIAL HIERARCHY
- IHA : Infinite Hierarchy Assumption
- Karp-Lipton : IHA $\Rightarrow$ NP $\not\subseteq$ $P/poly$.

Last lecture: Alternation vs. Time vs. Space :

$$SAT \in L \Rightarrow SAT \notin TIME(n^{1+o(1)}).$$

Today : Focus on $O(1)$ - alternations.

Debates (vs. Games)



$$V(q_1, a_1, q_2, a_2, x) = 0/1$$

- How complex can L be if $\exists$ polytime verifier V & (unboundedly powerful) A, B s.t. V accepts iff $x \in L$? [with 4 rounds of comm., Alice speaks first]

- $L \in \Sigma_p^i$ if (1) Alice speaks first
  (2) i rounds of comm.
  (3) $V(x, y_1, y_2, \ldots y_i) = 1 \iff x \in L$.

" $\exists y_1 \forall y_2 \exists y_3 \ldots Q_i y_i \quad V(x, y_1 \ldots y_i) = 1 \iff x \in L$.

$L \in \Pi_p^i$ if (1) Bob speaks first

⋮

" $\forall y_1 \exists y_2 \ldots Q_i y_i \quad V(x, y_1, \ldots y_i) = 1 \iff x \in L$.

Three Views

(1) Debates (2) Quantifiers (3) "Oracles"

Oracle - Computation

C^O : Given oracle for language $O \in \{0,1\}^*$

↳ resources corresponding to C,

how much computation can we do?
(what problems can we solve).

WARNING: Smoking Oracles is Injurious to Health.

- C^O is not well-defined as a concept.
- But well-defined for some C, [$C \in \{P, NP, coNP, PSPACE, \ldots\}$]
- First Use of Oracles.

[Baker-Gill-Solovay] :: Diagonalization proofs "relativize"
∴ "$P \neq NP$" does not.

Definition: Proof that $C_1 \neq C_2$ relativizes if it shows

$\forall O$, $C_1^O \neq C_2^O$.

Example: $\text{Time}(n) \neq \text{Time}(n^2)$, but proof shows

$\text{Time}(n)^{\text{CHESS}} \neq \text{Time}(n^2)^{\text{CHESS}}$ ...

But with NP & P

① $\exists O$ s.t. $P^O \neq NP^O$ [Good Exercise]

② $\exists O$ (QBF) s.t. $P^O = NP^O$ [O = QBF, $P^O = NP^O = PSPACE$]

⇒ $NP \neq P$ ~~&~~ can not have relativizing proof.

Warning: Proof that SAT is NP-Complete does not relativize.

So if your proof is diagonalization for SAT... then it could work!

Back To Alternation

What is P^{NP} ? [formally P^{SAT}]

or NP^{NP} ?

or $coNP^{NP}$?

(i) $coNP \subseteq P^{NP}$ so $NP \neq P^{NP}$

(ii) $NP^{NP} = NP^{coNP}$

(iii) $NP^{coNP} \supseteq \Sigma_2^P$; $NP^{coNP} \subseteq \Sigma_2^P$.

Oracle View: $\Sigma_i^P = NP^{\Sigma_{i-1}^P} = NP^{\Pi_{i-1}^P}$

$\Pi_i^P = coNP^{\Sigma_{i-1}^P} = coNP^{\Pi_{i-1}^P}$

$$PH = \bigcup_{i>0} \Sigma_i^P = \bigcup_{i>0} \Pi_i^P$$

[convention $P = \Sigma_0^P = \Pi_0^P$]

Example Problems:

- $NP \ni$ ⊙ $coNP$ [No sat. assignment, or $\chi(G) > k$ or $TSP(G) > L$ ..]

① MINDNF [Σ_2^P complete [Umans]]

① VC Dim [Σ_3^P complete].

Given $C: \{0,1\}^N \times \{0,1\}^n \to \{0,1\}$, D is the VC-dimension of the class $\mathcal{C} \subseteq \{f: \{0,1\}^n \to \{0,1\}\}$

$\mathcal{C} \{C(h, \cdot) \mid h \in \{0,1\}^N\}$

$\leq D$?

IHA: $\forall i \quad \Sigma_i^P \neq \Pi_i^P$

① IHA $\Rightarrow$ $P \neq NP$

② IHA $\Rightarrow$ $NP \neq coNP$

③ IHA $\Rightarrow$ $\forall i \neq j$ $\quad \Sigma_i^P \neq \Pi_j^P$

$\Sigma_i^P \neq \Sigma_j^P$

$\Pi_i^P \neq \Pi_j^P$

w.l.o.g. Assume $\Sigma_i^P = \Sigma_{i+1}^P$.

- Then suppose $L \in \Sigma_{i+1}^P$ given by V s.t.

$$L = \{x \mid \exists y_1 \forall y_2 \ldots Q_{i+1} y_{i+1} \; V(x; y_1 \ldots y_{i+1})\}$$

Let $L' =$

Then $\Pi_i^P \subseteq \Sigma_{i+1}^P = \Sigma_i^P$; $\Sigma_i^P \subseteq \Pi_j^P$

$\Rightarrow co\Sigma_i^P \subseteq co\Pi_j^P$.

$\Rightarrow \Sigma_i^P \subseteq \Pi_i^P$.

$\Sigma_i^P = \Pi_i^P \Rightarrow \forall j \geq i \quad \Sigma_j^P = \Sigma_i^P$.

Proof: WLOG $j = i+1$

$L \in \Sigma_{i+1}^P : \quad L = \{x \mid \exists y_1 \ldots Q_{i+1} y_{i+1} \; V(x; y_1 .. y_{i+1})\}$

Let $L' = \{(x, y_1) \mid \forall y_2 \ldots Q_{i+1} y_{i+1} \; V(x; y_1 \ldots y_{i+1})\}$

$L' \in \Pi_i^P \Rightarrow L' \in \Sigma_i^P$ so $\exists V'$

$\Rightarrow L' = \{(x, y) \mid \exists z_1 \ldots Q_i z_i \; V'(x; y, z_1, .. z_i)\}$

But now

$L = \{x \mid \exists y, z_1 \; \forall z_2 .. Q_i z_i \; V'(x; y, z_1 .. z_i)\}$

$\Downarrow$

$L \in \Sigma_i^P$

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

Karp-Lipton: $\text{HTA} \Rightarrow NP \subseteq P/_{poly}$.

Intuition: $P/_{poly}$ closed under complement.

$NP \subseteq P/_{poly} \Rightarrow coNP \subseteq P/_{poly}$

$\Downarrow$

Can prove $\phi \notin SAT$?

Converting Intuition

Idea 1:

A: "$\phi \notin SAT$"

C: "s.t. $\forall \psi$, $C(\psi)=1 \leftrightarrow \psi \in SAT$" → B

Not a "proof" since Alice may lie. How do we know C is correct?

Idea 2:

A → C

C → A: ψ, a s.t. $C(\psi)=0$; $\psi(a)=1$

or ψ, x_i s.t. $C(\psi)=1$, $C(\psi|_{x_i=0})=0$, $C(\psi|_{x_i=1})=0$.

Unfortunately only proves $coNP \subseteq \Sigma_2^P$ ("trivial").

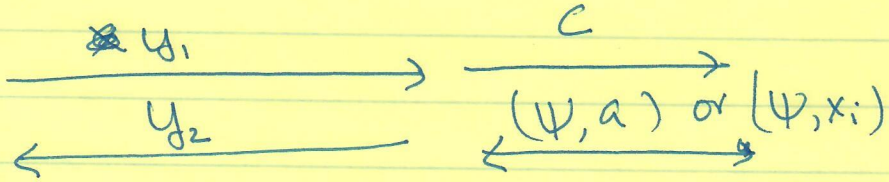
Clinching Idea: Will prove Σ_3^P statements.

$$L = \{x \mid \exists y_1 \forall y_2 \exists y_3 \text{ s.t. } V(x, y_1, y_2, y_3)\}$$

$$L' = \{(x, y_1, y_2) \mid \exists y_3 \text{ s.t. } V(x, y_1, y_2, y_3)\}$$

$\Rightarrow$ $\exists$ tranformation $(x, y_1, y_2) \to \phi_{x,y_1,y_2}$ s.t. $\phi \in$ SAT $\Leftrightarrow \ldots$

$L' \in NP \Rightarrow \exists$ Circuit C solving $\phi_{L'}$ SAT



Accept if $C(\phi_{x,y_1,y_2}) = 1$

and ($C(\psi) = 1$ if $\psi(a) = 1$

or $C(\psi) = 0$ or $C(\psi|_{x_i=0}) = 1$

or $C(\psi|_{x_i=1}) = 1$)

Proves $\Sigma_3^P \subseteq \Sigma_2^P \Rightarrow \Sigma_2^P = \Pi_2^P$

"PH collapses to second level"

$\boxtimes$