Michael Forbes
mforbes@illinois.edu
2018-02-07.4 → 2018-02-12.1
2018-02-12.e ← CS 579

CS 579: Computational Complexity Lecture 8

admin: PS 1 back Mean = 31.

today: alternation

NP vs P/poly

last time: defn alternating Turing machines - ∃ states, - ∀ states

$\Sigma^k P$: q_start is ∃, ≤ k-1 alternations eg $\Sigma^1 = NP$

Π^k " ∀ $\Pi^1 = coNP$

$PH = \bigcup_k \Sigma^k P$ [[polynomial hierarchy]]

Conj: $PH \neq \Sigma_k P$, all k [[PH is infinite]]

Q: ↳ ? [[what explanatory power does this have?]]

proof systems:

$L \in NP$: $L = \{x \mid \exists y \in \{0,1\}^{p(|x|)} \; M(x,y) = 1\}$

y ≈ witness

Prover: [[all power to! wants to prove $x \in L$]]

Verifier: [[computationally bounded, wants to know $x \in L$ or $x \notin L$]]

y →

check $M(x,y) = 1$

completeness: $x \in L \Rightarrow \exists y$ = V acc [[proof is complete]]

soundness: $x \notin L \Rightarrow \nexists y$ = V rej [[proof is sound]]

[[coNP is swapped, now $x \notin L$]]

MIN-CKT = $\{C : C$ is min size ckt computing $f_C : \{0,1\}^n \to \{0,1\}\}$

$= \forall D \; \exists x \; |D| > |C|$ or $D(x) \neq C(x)$

Prover_Y Verifier Prover_N

D ←

x →

[[P is public]]

$|D| > |C|$ or $D(x) \neq C(x)$

C minimal: Prover_Y wins = V acc

not Prover_N = V rej

⇒ PH ≅ constant round debates

Prop: 3SAT is NP complete ∃/∀

Prop: $k\text{-}\exists\text{-}TQBF = \{\varphi : \exists x_1 \forall x_2 \cdots \overline{Q_k} \; \varphi(x_1, \ldots, x_k), \varphi \text{ 3CNF}\}$ is Σ^k-complete.

Pf:

Michael Farber
mifarber@illinois.edu
2018-02-12.2 ← 2018-02-12.1 → 2018-02-12.3
CS579

Pf: $\in \Sigma^k$: easy

Σ^k-hard: do Cook Levin

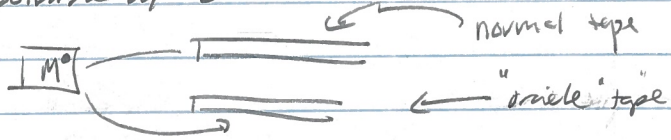
oracle machines

Recall: if $L \in NP \Rightarrow L \le 3SAT$ [one call of 3SAT]

$P = NP \Rightarrow$ can find 3SAT assignments [called 3SAT many times]

want: general notion "A solvable w/ B"

def: an oracle TM:



$Q \ni q_{oracle}, q_{acc}, q_{rej}$

...

$A \subseteq \{0,1\}^*$

M^A accepts an input x if
- compute normally
- write on oracle tape
- each q_{oracle}: oracle tape contents y; $y \in A \Rightarrow$ oracle tape replaced by 1, $y \notin A \Rightarrow$ oracle tape replaced by 0

runs in $t(n)$ steps if acc/rej in $\le t(|x|)$ steps on any x

↳ oracle work is free

$TIME^A(t(n)) = \{L : L = L(M^A)$ some M^A runs in $t(n)$ steps$\}$

$P^A = \bigcup_k TIME^A(n^k)$

NP^A $\quad NTIME^A$

Complexity class: $P^C = \bigcup_{A \in C} P^A$

eg: $NP \subseteq P^{NP} = P^{coNP} = P^{SAT}$, $P^P = P$

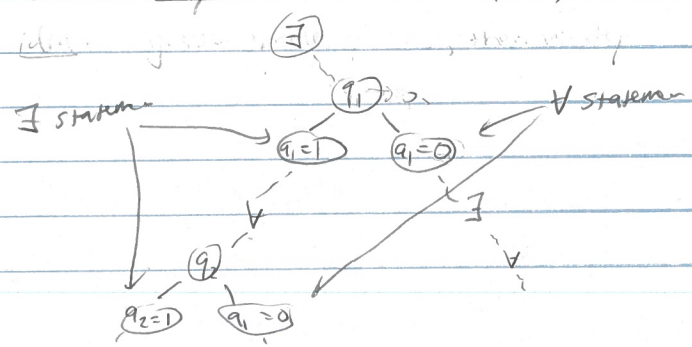
Prop: $\Sigma_{k+1}P = NP^{\Sigma_k P} = NP^{\Pi_k P}$ [intuitive]

Pf: do $k=1$: $\Sigma^2 = NP^{NP}$

$\subseteq$: $L \in \Sigma^2$ if $L = \{x : \exists y \forall z \underbrace{M(x,y,z)=1}_{\in coNP}\}$

$\in NP^{coNP} = NP^{NP}$ [used one oracle call]

$\supseteq$: issue: Many oracle calls could happen, interleaving
- NP call
- coNP call
- existential choice



Michael Forbes
mforbes@illinois.edu
2018-02-11.2 → 2018-02-11.4
2018-02-11.5
CS579

idea: at beginning: - guess questions $q_1, \dots, q_k \in \{0,1\}^*$ $k \le \text{poly}(n)$
- guess answers $a_1, \dots, a_k \in \{0,1\}^k$

$x \in L$ iff $\exists y \in \{0,1\}^{p(|x|)}$ $M^A(x,y) = 1$

iff exists $(q_1, a_1), \dots, (q_k, a_k)$

$\exists y$

$M^A(x,y)$ — $= 1$

- asks $q_1, \dots, q_k$

- gets answers $a_1, \dots, a_k$: $A = \{z : \exists w \; P(z,w) = 1\}$

if $\exists (q_i, a_i)\ \exists y$: $\{\exists w_i \; P(q_i, w_i) = 1\}_{a_i = 1}$
$\{\forall w_i \; P(q_i, w_i) = 0\}_{a_i = 0}$
$M^{(q_i = a_i)}(x,y) = 1$] P

$\Sigma^2 P$

Cor: $P = NP \Rightarrow PH = P$ [PH infinite is über $P \neq NP$]

Pf. ↳ $NP^{NP} = NP^P = NP = P$

$NP^{NP^{NP}} = NP^P = NP = P$

...

Cor: $\Sigma^k P = \Pi^k P \Rightarrow PH = \Sigma^k P$ [PH infinite is über $NP \neq coNP$]

Pf: ↳ $\Sigma^{k+1} P \subseteq \Sigma^k P$ for $k \ge k$

$L^\Psi = \{x : \exists x_{k+1}, \forall x_k \dots Q_{k+1} x_{k+1} \; Q_k x_k \dots Q_1 x_1 \; P(x, x_1, \dots, x_{k+1}) = 1\}$

eg $\exists$ $\forall$ ...

$= \exists$ —

one less alternation

$\Pi^k P = \exists^k P$

Question

Q: $NP \subseteq P/\text{poly}$?

Cor: $NP \subseteq P/\text{poly} \Rightarrow$ poly size circuit C for $\{x : \exists y \; M(x,y) = 1\}$ $\exists y \; M(x,y) = 1$ ⇒ $C(x)$ gives y s.t. $M(x,y) = 1$; $\exists y \; M(x,y) = 1$ ⇒ $C(x) = \perp$ [search to decision reduction from last time]

Thm [Karp Lipton]. $NP \subseteq P/\text{poly} \Rightarrow \Sigma^2 P = \Pi^2 P$ [$\Rightarrow PH = \Sigma^2 P$]

Pf. idea: guess $\exists$ verify $\varphi(x) = 1$ $\forall$ suffices

$L = \{x \mid \underbrace{\forall y \exists z \; P(x,y,z) = 1}_{\in NP} \} \in \Pi^2 P$

$\subseteq P/\text{poly} \Rightarrow$ poly size circuit C $\exists z \; P(x,y,z) = 1 \Rightarrow P(x,y,C(x,y)) = 1$ ∄

$x \in L$ iff $\forall y \exists z \; P(x,y,z) = 1$

iff $\exists C \; \forall y \; P(x,y,C(x,y)) = 1$ ← need to find C

iff $\exists C \; \forall y \; P(x,y,C(x,y)) = 1$ ← verified as asking $\exists z$

Michael Forbes
miforbes@illinois.edu
2018-02-14.4 ← 2018-02-14.3
→ 2018-02-13.1
CS579

Remks: - P/poly, P/1 contain uncomputable langs
- Karp Lipton ≡ PH infinite ⇒ circuits ≤ TM for natural problems

Thm [Meyer] EXP ∈ P/poly ⇒ Σ_2 = PH = PSPACE = EXP
"TIME($2^{poly(n)}$)"

Many other "Karp Lipton"-type collapses

---

next time: randomized computation