Q: ETH vs P ≠ NP (Oleg)

2019-02-26.4 ⇌ 2019-02-26.2

Michael Forbes
miforbes@illinois.edu

2019-02-25.1
CS 579

CS 579: Computational Complexity: Lecture 14 — 10/15/2019

admin: - ps 3 due today
- ps 4 out tonight

last time: circuits - existence of hard functions
- ckt size hierarchy
- NP vs P/poly

today: - alternation - examples
- def
- completeness
- polynomial hierarchy

~~NP vs P/poly~~

ex: MIN-CKT = { C : C ckt on n vars [real life] w minimum size }

any ckt D on n vars w $D(\bar{x}) = C(x)\ \forall x \in \{0,1\}^n \Rightarrow |D| \geq |C|$

$C \in$ ∈ P? ∈ NP? [small ckts on n inputs]

iff $\forall D\ \exists x$ { $|D| \geq |C|$ or $C(\bar{x}) \neq D(x)$ }

coNP, NP

as only poly |C| bits to describe D

$\Rightarrow$ MIN-CKT $\in$ coNP^{NP} [alternation]

def: alternating TM has
- states $Q \ni q_{acc}, q_{rej}$
- tape alphabet Γ
- transition $\delta: Q \times \Gamma \to 2^{Q \times \Gamma \times \{L,S,R\}}$
- each state labelled w $\forall$ or $\exists$

ATM A runs in time $t(n)$: all inputs length n, all possible transitions → halting ≤ t(n) steps

a configuration of A on input x is accepting if [defined inductively]
- at q_{acc}
- at $\exists$-state, some transition to accepting configs
- at $\forall$-state, all "

A accepts input x if starting config is accepting

$ATIME(t(n)) = \{ L : L = L(A)$ for ATM A running in time $t(n) \}$

$AP = ATIME(poly(n))$

lem: - P, NP, coNP ⊆ AP
- MIN-CKT ∈ AP [first do ∀, then ∃]

Prop: AP = PSPACE

Sketch: $SPACE(f) \subseteq ATIME(f^2)$

$\subseteq$ TQBF $\subseteq \exists\forall\exists\forall\cdots \in$ [same as before, like switching thm]

Michael Forbes
2019-02-28.2 ← 2019-02-28.1 → 2019-02-28.3
miforbes@illinois.edu
CS579

$ATIME(f) \subseteq SPACE(f)$ [same as before]

$\exists \forall \exists \forall \cdots = TQBF_\epsilon$ ↑

[unbounded alternation is very strong, bounded alternation?]

def. ATM state is $\exists$ state if $\forall$ state; $\forall$ state if $\exists$ state

ATM uses $\le k$ alternations if on all inputs and all branches, at most $k-1$ transitions from { $\exists$ state to $\forall$ state, $\forall$ " " $\exists$ "

$\Sigma^k P = \{L : L = L(A),\ A\ TM$ - starts in $\exists$-state - uses $\le k$ alternations $\}$

$\Pi^k P = \{L : L = L(A),\ A\ TM$ - starts in $\forall$-state - uses $\le k$ alternations $\}$

eg: $\Sigma^1 P = NP$, $\Pi^1 P = coNP$

$PH := \bigcup_k \Sigma^k P = \bigcup_k \Pi^k P$

↳ polynomial hierarchy

$\Sigma^k P \subseteq \Pi^{k+1} P$

eg: $MIN\text{-}CKT \in \Pi^2 P$

$\forall D \exists x \cdots$

Conj: $\forall k\ PH \neq \Sigma^k P$ [no "collapse" of polynomial hierarchy]

Q: $L \Rightarrow ???$ [use $P \neq NP$ conj] [explanatory power?]

= Questions

proof systems [witness]

$L \in NP$ $\quad L = \{x : \exists y \in \{0,1\}^{poly(|x|)}\ V(x,y) = 1\}$

[computer] Prover [all powerful] [unrestricted] $\xrightarrow{\ y\ }$ Verifier [computationally bounded] [wants to decide "$x \in L$"?]

checks $V(x,y) = 1$

completeness: $x \in L \Rightarrow \exists y$ Vacc [can prove any correct statement]

soundness: $x \notin L \Rightarrow \forall y$ Vacc [can only prove correct statements]

[coNP is swapped]

$MIN\text{-}CKT = \{C : C$ is min ckt$\}$

$= \forall D \exists x$ $\quad |D| \ge |C|$ or $D(x) \neq C(x)$

↑ on $|C|$ many bits

[$\subseteq$ public]

Prover$_{YES}$ $\xleftarrow{\ D\ }$ Verifier $\xrightarrow{\ x\ }$ Prover$_{NO}$

$|D| \ge |C|$ or $P(x) \neq C(x)$

C minimal: Prover$_{YES}$ wins $\equiv V_{acc}$

not " " NO " $\equiv V_{rej}$

intuition: PH is $O(1)$ round debate between Prover$_{YES}$, Prover$_{NO}$, referee is verifier

Michael Forbes
mforbes@illinois.edu

2019-02-28.2 → 2019-02-28.3
2019-02-28.4 ←
CS579

Thm [Cook Levin]: 3SAT is NP complete

Prop: $k\text{-}\exists\text{-TQBF} = \{\varphi : \varphi = \exists x_1 \forall x_2 \cdots Q_k \underbrace{\phi(x_1,\dots,x_k)}_{\hookrightarrow 3CNF}\}$
φ is true

is $\Sigma^k P$-complete ↳ wrt $\le_p$ reductions

Sketch: $\in \Sigma^k P$: easy

$\Sigma^k P$-hard: generalize Cook Levin.

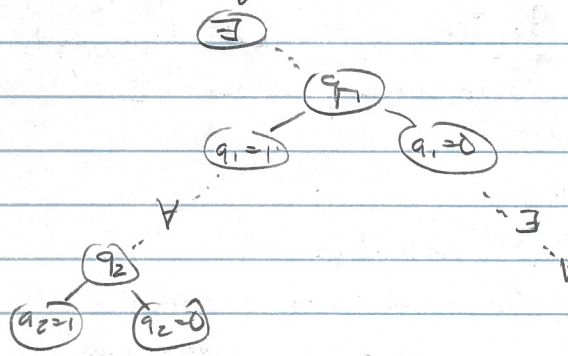
Thm: $\Sigma^{k+1} P = NP^{\Sigma^k P} = NP^{\Pi^k P}$ [recall oracles]

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

$\subseteq$: $L \in \Sigma^2$ iff $L = \{x : \exists y \underbrace{\forall z\ V(x,y,z)=1}_{\in coNP \leftarrow \text{consolve w/ NP oracle}}\}$

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

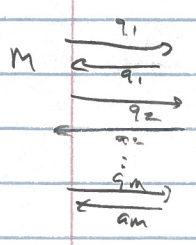
$\supseteq$: issue: Many oracle calls interleaving
- NP call
- coNP call
- existential choice
- universal choice



idea: - guess questions $q_1,\dots,q_m \in \{0,1\}^{poly(n)}$, $m \in poly(n)$
- guess answers $a_1,\dots,a_m \in \{0,1\}$

$x \in L$ iff $\exists y \in \{0,1\}^{poly(n)}$ $M^A(x,y)=1$ $A \in NP$

iff $\exists y\ \exists (q_1,a_1),\dots,(q_m,a_m)$ s.t.



$M^{\bar q=\bar a}(x,y)$ is consistent

- q_1 is first oracle call of $M^{\circ}(x,y)$
- when q_1 returned to ↗, q_2 is second oracle call
- when a_2 returned to ↗, q_3 is third oracle call
- ...
- $M^{\bar q=\bar a}(x,y)=1$
- a_i is correct answer to q_i wrt $A=\{z : \exists w\ V(z,w)=1\}$

iff $\exists y\ \exists \bar q,\bar a\ [\exists w_i : V(q_i,w_i)=1]_{a_i=1}$
$[\forall w_i\ V(q_i,w_i)=1]_{a_i=0}$
$M^{\bar q=\bar a}(x,y)=1$ consistently

$\in \Sigma^2 P$ ∎

Michael Forbes
miforbes@illinois.edu
2019-02-28.4 ← 2019-02-28.3
→ 2019-03-05.1
CS579

Cor: $P = NP \Rightarrow PH = P$

Pf: $\hookrightarrow NP^{NP} = NP^P = NP = P$

$\Sigma^3 P = NP^{(NP^{NP})} = NP^P = P$

...

Cor: $\Sigma^k P = \Sigma^{k+1} P \Rightarrow PH = \Sigma^k P$ [similar]

Pf: $NP^{\Sigma^k P} = \Sigma^{k+1} P$

$\Sigma^{k+2} P = NP^{\Sigma^{k+1} P} = NP^{\Sigma^k P} = \Sigma^{k+1} P$

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

Pf: warm-up $\hookrightarrow \Sigma^{k+1} P = \Sigma^k P$ ⇧

$L = \{x : \exists y_1 \forall y_2 \cdots Q_k y_k Q_{k+1} y_{k+1} P(x, y_1, \ldots, y_k, y_{k+1}) = 1\}$

$\downarrow \Pi^k P = \Sigma^k P$

$\exists y_1 \exists z_1 \cdots Q_k z_k P'(x, y_1, z_1, \ldots, z_k) = 1\}$

no alternation ⇒ $\hookrightarrow$ is $\Sigma^k P$!

today: - alternation - as resource
- MIN-CKT^{NP}
- PH - as $O(1)$ debate
- PH infinite ⇒ $P \neq NP$
$NP \neq coNP$
$NP^{NP} \neq coNP^{NP}$

next time: - $NP \subseteq P/poly \Rightarrow PH = \Sigma^2 P$ [collapse]
- randomness