Michael Forbes
mforbes@illinois.edu

2018-02-05.4 → 2018-02-07.1
2018-02-07.2

cs579

cs 579: Computational Complexity : Lecture 7 6/9

today: Cook Levin
alternation

=

$\exists \tilde{x}\ \varphi(\tilde{x}) = 1$

Thm [Cook Levin]: 3SAT = { $\langle \varphi \rangle$: φ satisfiable 3CNF formula }

CKT-SAT = " circuit

$NP \overset{(a)}{\leq_p} CKT\text{-}SAT \overset{(b)}{\leq_p} 3SAT$

Cor ↳ NP-complete ∎ guess × ∀

Pf: (a) $L \in NP$ $L = L(N)$ N nondet TM runs in poly(n) time

$= \{ x : \exists y \in \{0,1\}^{p(|x|)}\ M(\langle x, y \rangle) = 1 \}$

last time: $TIME(t(n)) \subseteq SIZE(t(n)^2)$ and ckt can be computed in poly(t) time

M: poly(n)-time TM, $|\langle x,y \rangle| \leq q(|x|)$

⇒ in poly(|x|) time construct ckt $C_{M,q(|x|)}$ s.t. $M(\langle x,y \rangle) = 1$ iff $C_{M,q(|x|)}(\langle x,y \rangle) = 1$

on $q(|x|)$ size inputs $|C_{M,q(|x|)}| \leq poly(|x|)$

⇒

$C_{x,p(|x|)}(y) := C_{M,q(|x|)}(\langle x,y \rangle)$

↑ $p(|x|)$-size inputs

s.t. $x \in L$ iff $\exists y \in \{0,1\}^{p(|x|)}\ M(\langle x,y \rangle) = 1$

iff $\exists y\ C_{M,q(|x|)}(\langle x,y \rangle) = 1$

iff $\exists y\ C_{x,p(|x|)}(y) = 1$

iff $C_{x,p(|x|)} \in CKT\text{-}SAT$

$x \mapsto C_x$ in poly(|x|) time

⇒ $L \leq_p CKT\text{-}SAT$

= Questions.

(b) want: $CKT\text{-}SAT \leq_p 3SAT$

idea: introduce new variable per gate
enforce correctness gate by gate

eg: $C =$ ∧ = z (x, y) $C(x,y) = 1$ iff $z = 1$ and $z = x \wedge y$

last time: any $f: \{0,1\}^n \to \{0,1\}$ has DNF size $O(n \cdot 2^n)$

$\vee_i \wedge_j \ell_{ij}$

=> CNF "

Pf: $\neg f = \vee_i \wedge_j \ell_{ij}$

$f = \neg \vee_i \wedge_j \ell_{ij}$

$= \wedge_i \neg \wedge_j \ell_{ij} = \wedge_i \vee_j \neg \ell_{ij}$] CNF

Michael Forbes
mforbes@cs.illinois.edu

AND
- $z = 1 \Rightarrow$ CNF on 1 var $=$ 3CNF
- $z = x \wedge y \Rightarrow$ CNF on 3 vars $=$ 3CNF

$\Rightarrow$ 3CNF

ex: $z = 1 \Rightarrow (z)$

$z = x \wedge y \Rightarrow (x \vee \neg z) \wedge (y \vee \neg z) \wedge (\neg x \vee \neg y \vee z)$

$\equiv \neg x \Rightarrow \neg z$ $\quad \neg y \Rightarrow \neg z$ $\quad x \wedge y \Rightarrow z$

$\Big\}$ 3CNF

in general: C circuit - fan-in 2
- AND, OR, NOT gates
- vars $x_1, \dots, x_n$
- size s

$\mapsto$ 3CNF φ - variables $x_1, \dots, x_n, g_1, \dots, g_s$ (partial results at each gate)
- $\varphi = (g_s) \wedge \bigwedge_{i=1}^{s} c_i$

(g_s): output gate $= 1$; c_i: 3CNF asserting g_i correct

$C \mapsto \varphi$ poly time

$\exists x\ C(x) = 1 \Rightarrow \exists x$ partial computations $g_1, \dots, g_s$ - $g_s = 1$
- g_i computed from children

$\Rightarrow \exists x, g\ \varphi(x, g) = 1$

$C \in$ CKT-SAT; $\varphi \in$ 3SAT

$\Rightarrow$ CKT-SAT $\leq_p$ 3SAT

why: 3SAT useful starting point for reductions

Rmk: gives formula for TQBF transition function

2SAT $\in P$

= Questions

alternation:

ex: CLIQUE $= \{\langle G, k\rangle \mid G$ has k-clique$\} \in NP$ // NP-complete //

MAX-CLIQUE $=$ (k NP) $\wedge$ (no $k+1$ clique ? coNP)

Q: in NP?

Q: how to merge together?

ex: SAT $= \{\langle \varphi \rangle \mid \exists x\ \varphi(x) = 1\} \in NP$

$P = NP \Rightarrow$ SAT $\in P$

Q: find x?

Prop: $P = NP \Rightarrow$ can find sat. assign in poly time

Pf: idea: search to decision reduction

eg: binary search // guess my number //

Michael Forbes
miforbes@illinois.edu
2018-02-07.2 →
2018-02-07.4 ←
2018-02-07.3
CS 579

$\varphi(x_1,\dots,x_n)$ is satisfiable $\Rightarrow \exists\, b_1,\dots b_n \in \{0,1\}$ $\varphi(b_1,\dots b_n)=1$

$\Rightarrow \exists\, b_1 \in \{0,1\}$ $\varphi(b_1, x_2,\dots x_n)$ satisfiable

$\Rightarrow$ iff $\varphi(0,\bar{x}_{>1})$ or $\varphi(1,\bar{x}_{>1})$ is satisfiable

$\Rightarrow P=NP \Rightarrow$ can find which one w/ one NP decision.

$\varphi(\bar{x})$ sat $\Rightarrow b_1$ w/ $\varphi(b_1,\bar{x}_{>1})$ sat

$\Rightarrow b_1, b_2$ w/ $\varphi(b_1,b_2,\bar{x}_{>2})$ sat

...

$\Rightarrow b_1,\dots b_n$ w/ $\varphi(b_1,\dots b_n)$ sat $\Rightarrow \varphi(\bar{b})=1$ ∎

[[used NP repeatedly]]

eg: MIN-CKT $= \{ C : C$ acts on n variables w/ min size $\}$

$\equiv$ any D s.t. $C(\bar{x}) = D(\bar{x})$ $\forall x \in \{0,1\}^n$

$\Rightarrow |D| \geq |C|$ [[real life]]

$\equiv \underbrace{\forall D}_{coNP}\ \underbrace{\exists x}_{NP}$ s.t. $|D| \geq |C|$ or $C(\bar{x}) \neq D(\bar{x})$

Q: how to model these?

def: an alternating TM has
- tape alphabet Γ
- state space $Q \ni q_{acc}, q_{rej}$
- σ_0, σ_1 transition functions
- labelled w/ $\exists$ or $\forall$

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

a configuration of A accepts if
- at q_{acc}
- [[defined inductively]] is at $\exists$-state, either σ_0 or σ_1 leads to accepting config
- is at $\forall$-state, both "

ATM A accepts x if starting config is accepting

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

$AP = ATIME(poly(n))$

lem: $P, NP, coNP \subseteq AP$

lem: MAX-CLIQUE, MIN-CKT $\in AP$

Prop: $AP = PSPACE$

lem: $SPACE(s(n)) \overset{(a)}{\subseteq} ATIME(poly(s)) \overset{(b)}{\subseteq} SPACE(poly(s))$, $s(n)$ space constructible

Sketch: $\hookrightarrow \leq$ TQBF $= \{ \exists\forall\exists\forall\cdots\varphi \} \in ATIME(poly(s))$

$\hookrightarrow \subseteq \underbrace{\exists\forall\cdots\exists\forall}_{poly(s)}$ (time $poly(s)$) $\in SPACE(poly(s))$

[[like TQBF $\in$ PSPACE]]

Michael Forbes
MForbes@illinois.edu
2018-02-07.4 ← 2018-02-07.3
→ 2018-02-12.1
CS 579

∃ ∀ ∃∀∃∀...

$P \subseteq NP, coNP \subseteq PSPACE$

Q: alternation as a resource?

def: $\Sigma^k P$ / $\Pi^k P$ = { languages of ATMs that alternate $k-1$ times starting in $\exists$ / $\forall$ }

eg $\Sigma^1 P = NP$, $\Pi^1 P = NP$ $\Sigma^0 P = \Pi^0 P = P$

$PH = \bigcup_k \Sigma^k P = \bigcup_k \Pi^k P$ polynomial hierarchy

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

lem: MAX-CLIQUE, MINCKT $\in \Pi^2 P$

↳ also in $\Sigma^2 P$

Q: $\exists k$ s.t. $PH = \Sigma^k P$?

↑ "collapse"

next time: no collapse = über $P \neq NP$

↳ $NP \not\subseteq P/poly$