COMP 330
DEC 3, 2010
(NOT Hamed Hatami)

PAUL HUSSMAN

last Class.

SAT vs NP complete

Recall: A language $L \in NP \iff \exists$ polynomial P, verifier V s.t.

SAT

literal B is either a variable x or its negation $\bar{x}$

Formula φ is an expression of literals joined with logic operators $\wedge, \vee, \neg$, and we can use brackets ( ).

$|\varphi|$ = # literals in it

Problem: given φ, $\exists$ some assignment true/false st φ is true?

Claim: $SAT \in NP$

φ $(A \wedge \neg B) \wedge (\neg A \vee B)$

y: $\{A=T, B=F\}$

$\forall L \in NP$, $L \leq_P SAT$

let V be the verifier of $L \in NP$.

let $x \in L$ $n = |x|$

let y be a certificate for x

let Q be the states of V

let Γ be the tape alphabet

let δ be the transition function

Assume V always starts with the following tape configuration

$[Y_m, Y_{m-1}, \dots, Y_1 \# x_1, x_2, \dots, x_n]$

$m, \dots, \quad 0, 1, 2, \dots n$

Assume V always halts at position 0 with $a_{Accept} \in \Gamma \iff y$ is a true certificate for x.

Note: $|y| = m \leq P(n)$ and the head of the machine can move at most $P(n)$ positions to the right or left.

$STEPS = \{1, 2, \dots, P(n)\}$

$POSITIONS = \{-P(n), \dots, P(n)\}$

want: $(V, x, *) \Rightarrow \varphi_x$

Literals

I. $\forall i \in STEPS$, $\forall q \in Q$, R_{iq} means that after i steps, V is in state q.

II. $\forall i \in STEPS$, $\forall j \in POSITIONS$, $\forall a \in \Gamma$, S_{ija} means that after i steps, a is at position j.

III. $\forall i \in STEPS$, $\forall j \in POSITIONS$, T_{ij} means that after i steps, it's at position j.

1. At each step, V is in at least 1 state.

$\forall i \in STEPS, \left(\bigvee_{q \in Q} R_{iq}\right) \equiv (R_{iq_0} \vee R_{iq_1} \vee \dots \vee R_{iq_{|Q|}})$

$P(n)|Q| = O(P(n))$

2) At each step, V is at most 1 state

$\forall i \in STEPS$, $\forall q_k, q_l \in Q$ such that $q_k \neq q_l$ $\neg(R_{iq_k} \wedge R_{iq_l})$

$P(n)|Q|(|Q|-1) = O(P(n)^2)$

3) At each step, each tape position contains at least one symbol

$\forall i \in STEPS, \forall j \in POSITIONS,$

$$\left(\bigvee_{a \in \Gamma} S_{ija} \right)$$

$P(n)(2P(n)+1)|\Gamma| = O(P(n)^2)$

4) At each step, each tape position contains at most one symbol

$\forall i \in Steps, \forall j \in POSITIONS, \forall a_k, a_\ell \in \Gamma$ st $a_k \neq a_\ell$,

$$\neg \left(S_{ija_k} \wedge S_{ija_\ell} \right)$$

$P(n)(2P(n)+1)|\Gamma|(\Gamma - 1) = O(P(n)^2)$

5) At each step, the head is in at least 1 position

$\forall i \in STEPS$

$$\left(\bigvee_{j \in POS} T_{ij} \right)$$

$P(n)(2P(n)+1) = O(P(n)^2)$

6) At each step, the head is in at most 1 position

$\forall i \in STEPS, \forall p_k, p_\ell \in POSITIONS$ st $p_k \neq p_\ell$

$$\neg (T_{ip_k} \wedge T_{ip_\ell})$$

$P(n)(2P(n)+1)(2P(n)) = O(P(n)^3)$ (still polynomial)

... now comes the tricky part: (TRANSITION FUNCTION).

7) The configuration of V after the first step depends only on δ.

$\delta(j, q, a) \rightarrow (j', q', a' \text{ at } j)$

[Note: $A \rightarrow B \equiv (\neg A \vee B)$]

$\forall i \in STEPS$, $\forall j \in POS$, $\forall q \in Q$, $\forall a \in \Gamma$

$(T_{ij} \wedge R_{iq} \wedge S_{ija}) \rightarrow R_{(i+1)q'}$

$(T_{ij} \wedge R_{iq} \wedge S_{ija}) \rightarrow T_{(i+1)j'}$

$(T_{ij} \wedge R_{iq} \wedge S_{ija}) \rightarrow S_{(i+1)ja'}$

$(S_{ija} \wedge \neg T_{ij}) \rightarrow S_{(i+1)ja}$

$(12 \cdot |Q| + 3)(P(n)(2P(n))|T|) = O(P(n)^2)$

8) Initially, V starts at position 0 in q_{start}

$$\left(R_{0q_{start}} \wedge T_{00} \right)$$

9) $P(n)^{th}$ step: V halted at position 0, a_{accept}

$$R_{P(n)q_{halt}} \wedge T_{P(n)0} \wedge S_{P(n)0a_{accept}}$$

10) X is written on the tape as $x = x_1 x_2 \dots x_n$ 3

$(S_{01a} \wedge S_{02x_2} \wedge \dots \wedge S_{0nx_n})$ n literals

PAUL HUSMAN

$x \in L \Rightarrow \varphi_x \in SAT$

$x \in L \Rightarrow \exists$ certificate y for x such that $V(x,y)$ accepts
(ie; halts, at pos 0 w/ q_{accept}).

$[y \quad\quad y \ \# \ x]$ means that $\varphi_x \in SAT$.

$x \notin L \Rightarrow \varphi \notin SAT$.

$x \notin L \Rightarrow \nexists y$ such that $V(x,y)$ accepted $\Rightarrow$ halts, is at pos 0 but not w/ q accept.

so $x \in L \Leftrightarrow \varphi_x \in SAT$.

$O(P(n)^3)$ $\square$ $\boxed{\Rightarrow \forall L \in NP, L \leq_p SAT}$