Chain of Reductions

To show X is NP-complete : 1) show $X \in NP$
2) show $Y \le_p X$ for some NP-complete Y

$\le_p$ INDEPENDENT SET

$\le_p$ VERTEX COVER

SAT $\le_p$ 3-SAT $\le_p$ DIRECTED HAMILTONIAN CYCLE $\le_p$ HAMILTONIAN CYCLE $\le_p$ HAMILTONIAN PATH

$\le_p$ 3-COLOR

$\le_p$ TRAVELLING SALESPERSON

Chain of Reductions

To show X is NP-complete: 1) show $X \in NP$
2) show $Y \leq_p X$ for some NP-complete Y

$\leq_p$ INDEPENDENT SET

$\leq_p$ VERTEX COVER

$Y \leq_p$ SAT $\leq_p$ 3-SAT $\leq_p$ DIRECTED HAMILTONIAN CYCLE $\leq_p$ HAMILTONIAN CYCLE $\leq_p$ HAMILTONIAN PATH

$\leq_p$ 3-COLOR

$\leq_p$ TRAVELLING SALESPERSON

Cook-Levin Theorem: SAT is NP-complete

SAT $\in$ NP

for all $Y \in NP$, $Y \leq_p$ SAT

Reducing an arbitrary Y in NP to SAT

Let $Y \in NP$. Then there is a polynomial-time verification algorithm Y-VERIFY

$p \to q \equiv \sim p \vee q$ $\qquad$ $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

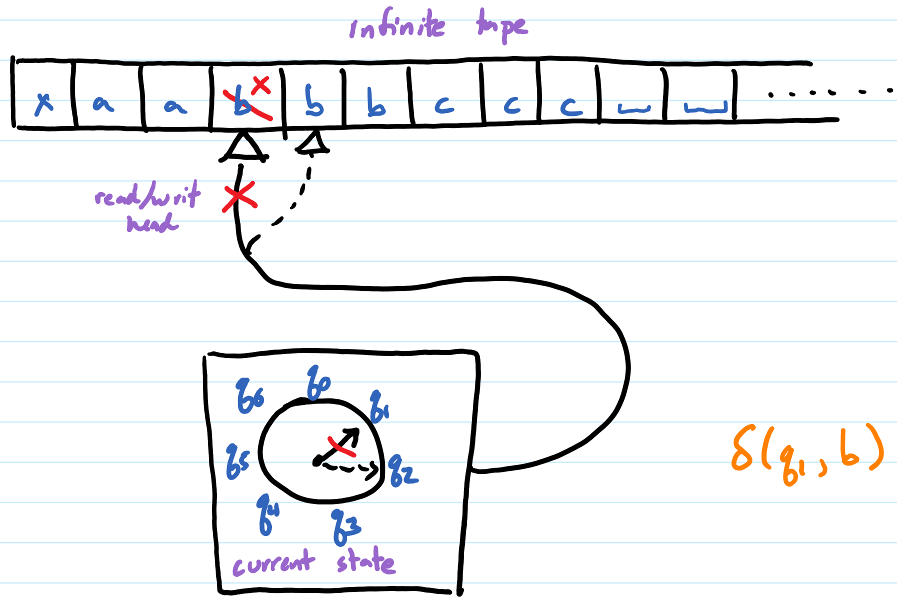
"$a_{t,i} = \sigma$" meaning "location i at time t contains σ" $\equiv \left(\bigwedge_{\sigma' \neq \sigma} \sim a_{t,i,\sigma'} \right) \wedge a_{t,i,\sigma}$

$b_t = q$ meaning "state is q at time t"

$c_t = i$ meaning "r/w head is at i at time t"

similar

Turing Machines

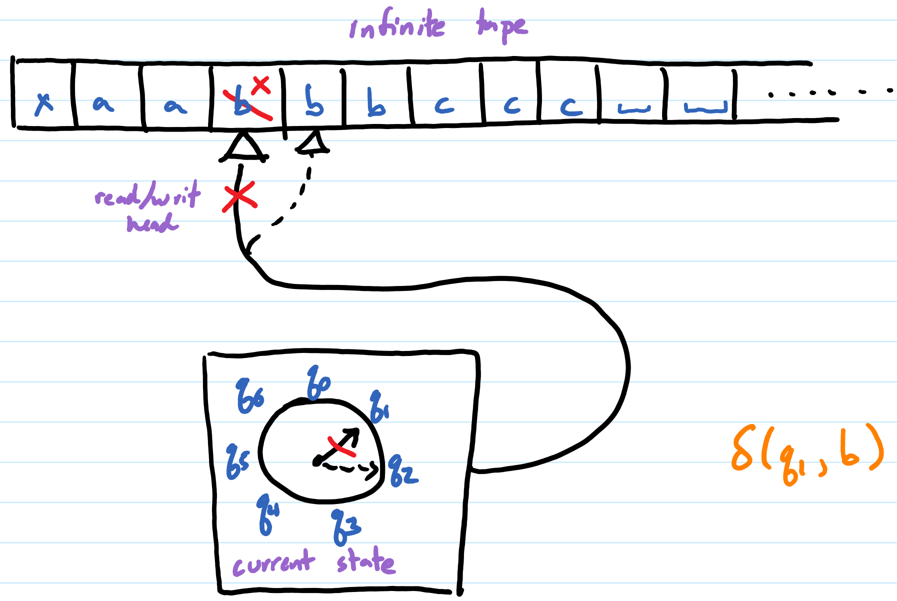


$\delta(q_1, b) = (x, q_2, R)$

Polynomial-time algorithm in your favorite language → polynomial time Turing machine

Proof: see CPSC 460

Turing Machines



$\delta(q_1, b) = (x, q_2, R)$

Polynomial-time algorithm in your favorite language → polynomial time Turing machine

Proof: see CPSC 460

Reducing an arbitrary Y in NP to SAT

Let $Y \in NP$. Then there is a polynomial-time verification algorithm Y-VERIFY

[need to, given x, create a formula φ such that $Y(x) = YES \longleftrightarrow \varphi$ is satisfiable and length of φ is polynomial in length of x]

Let $p(n)$ be such that Turing machine M for Y-VERIFY(x,y) takes $p(|x|+|y|)$ time.

polynomial

Let $q(n)$ be such that $\forall x$ s.t. $Y(x)=YES$, $\exists y$ s.t. $|y| \le q(|x|)$ and $\underbrace{\text{Y-VERIFY}(x,y)}$ = YES

total running time $= p(|x|+|y|)$
$= p(n+q(n))$
$=$ polynomial in n $= |x|$

$$p \rightarrow q \equiv \sim p \vee q \qquad\qquad p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

"$a_{t,i} = \sigma$" meaning "location i at time t contains σ" $\equiv \left(\bigwedge_{\sigma' \neq \sigma} \sim a_{t,i,\sigma'} \right) \wedge a_{t,i,\sigma}$

$b_t = q$ meaning "state is q at time t"
$c_t = i$ meaning "r/w head is at i at time t"

similar

Reducing an arbitrary Y in NP to SAT

Let $Y \in NP$. Then there is a polynomial-time verification algorithm Y-VERIFY

[need to, given x, create a formula φ such that $Y(x) = YES \leftrightarrow \varphi$ is satisfiable
and length of φ is polynomial in length of x]

Let $p(n)$ be such that Turing machine M for Y-VERIFY(x,y) takes $p(|x|+|y|)$ time.
← polynomial →
Let $q(n)$ be such that $\forall x$ s.t. $Y(x)=YES$, $\exists y$ s.t. $|y| \leq q(|x|)$ and $\underbrace{\text{Y-VERIFY}(x,y)}_{\text{total running time}} = YES$

total running time $= p(|x|+|y|)$
$= p(n+q(n))$
$=$ polynomial in n
call this $r(n)$ $\quad n = |x|$

Interpret $a_{t,i,\sigma} = T$ to mean tape location i contains symbol σ at time t

$b_{t,q} = T$ to mean M is in state q at time t

$c_{t,i} = T$ to mean the read/write head is at location i at time t

polynomial $\left[\begin{array}{l} 0 \leq t \leq r(|x|) \\ 0 \leq i \leq r(|x|) \end{array} \right.$ $\quad \left. \begin{array}{l} q \in \{0, \ldots, k-1\} \\ \sigma \in \Sigma \cup \{\sqcup, Y, N\} \end{array} \right]$ finite $\quad$ so polynomial # of variables

$$p \to q \equiv \sim p \vee q \qquad\qquad p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

"$a_{t,i} = \sigma$" meaning "location i at time t contains σ" $\equiv \left(\bigwedge_{\sigma' \neq \sigma} \sim a_{t,i,\sigma'} \right) \wedge a_{t,i,\sigma}$

$b_t = q$ meaning "state is q at time t"
$c_t = i$ meaning "r/w head is at i at time t"
similar

Huge Formula

From $x = x_0 \ldots x_{n-1}$ create φ to express

note: omitting edge cases (end of tape, M halts, ...)

each tape location contains exactly one symbol at any time

$$\bigwedge_{t=0}^{r(n)} \bigwedge_{i=0}^{r(n)} \bigvee_{\sigma \in \Sigma \cup \{\sqcup, Ⓨ, Ⓝ\}} \left(a_{t,i,\sigma} \wedge \bigwedge_{\sigma' \neq \sigma} \sim a_{t,i,\sigma'} \right)$$

M is in exactly one state and the read/write head is at exactly one location at any time

similar

1st input to M is x, the tape after the 2nd input is blank and M starts in state 0, location 0

$$\bigwedge_{i=0}^{n-1} a_{0,i,x_i} \qquad \bigwedge_{i=n+g(n)}^{r(n)} a_{0,i,\sqcup} \qquad b_{0,0} \qquad c_{0,0}$$

at all times, the tape, state, and head position reflect the operation of M

$$\bigwedge_{t=0}^{r(n)} \bigwedge_{i=0}^{r(n)} \bigwedge_{\sigma \in \Sigma \cup \{\sqcup, Ⓨ, Ⓝ\}} \left[(\sim c_{t,i} \wedge a_{t,i,\sigma}) \rightarrow a_{t+1,i,\sigma} \right]$$

(tape doesn't change where read/write head isn't)

Ex: $\delta(q, \sigma) = (q', \sigma', R)$

$$\bigwedge_{t=0}^{r(n)} \bigwedge_{i=0}^{r(n)} \left[(c_{t,i} \wedge b_{t,q} \wedge a_{t,i,\sigma}) \rightarrow (c_{t+1,i+1} \wedge b_{t+1,q'} \wedge a_{t+1,i,\sigma'}) \right]$$

the output is YES

$$\underbrace{\bigvee_{i=0}^{r(n)} \bigvee_{j=0}^{r(n)}}_{\text{polynomial \# of terms}} \underbrace{a_{i,j,Ⓨ}}_{\text{constant size per term}}$$

so conjunction of all parts is of size polynomial in size of x

$Y(x) = YES \rightarrow \exists$ some y s.t. $Y\text{-VERIFY}(x,y) = M(x,y) = YES$

setting variables in φ according to input x, y, and behavior of machine makes φ true

$Y(x) = NO \rightarrow$ no y makes $Y\text{-VERIFY}(x,y) = M(x,y) = YES \rightarrow$ all truth assignments make φ false

(either no tape location is ever Ⓨ or the variables don't reflect the operation of M)