CPSC 421/501 Nov 20, 2023

Thm (Cook-Levin): Let L be decidable by a non-det. T.m. M in time $\leq Cn^k$ on an input of length n. Then there is a polynomial time algorithm that given $\sigma_1 \ldots \sigma_n \in \Sigma^n$ (where $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$) produces a 3CNF Boolean formula $f(x_1, \ldots, x_N)$ such that

① f is of size polynomial in n

② $\sigma_1 \ldots \sigma_n \in L \iff f$ is satisfiable

Strategy:

Step 1 $\quad q_0 \quad |\,\sigma_1\,|\,\sigma_2\,|\,\cdots\,|\,\sigma_n\,|\,\sqcup\,|\,\sqcup\,|\,\cdots$

step 2

$\vdots$

Step T $\quad q_{acc} \quad |\quad|\quad|\;\cdots$

$T = Cn^k$

can we get to q_{acc}

$X_{ij\gamma}$ is $T \iff$ cell $[i,j]$ has γ

Y_{ij} is $T \iff$ tape head at step i is over cell j

Z_{iq} is $T \iff$ at step i we are in state q

$$f = \tilde{f}_{\text{uniqueness}} \qquad (T = Cn^k)$$

AND

$$\tilde{f}_{\text{initial}} \wedge \tilde{f}_{\substack{\text{final} \\ \text{is acc}}}$$

$$\wedge \bigwedge_{i=1}^{T-1} \tilde{f}_{\substack{\text{from } i \text{ to} \\ i+1 \text{ is} \\ \text{permitted} \\ \text{transition}}}$$

$\tilde{f}_{\text{uniqueness}}$: $\forall i,j,$ exactly one of $\{x_{ij\gamma}\}_{\gamma\in\Gamma}$ is T, $\forall i$ exactly one of $\{y_{ij}\}_{j\in T}$, $\forall i \ldots$ $\{z_{iq}\}_{q\in Q}$

One method:

$$a_1 \text{ or } a_2 \text{ or } \ldots \text{ or } a_N = T$$

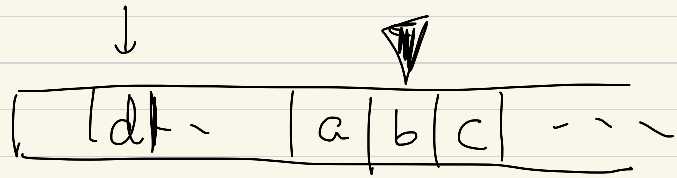
$$\Longleftrightarrow$$

$$\left.\begin{array}{l} (a_1 \text{ or } a_2 \text{ or } z_1) \text{ AND} \\ (\neg z_1 \text{ or } a_3 \text{ or } z_2) \text{ AND} \\ \vdots \end{array}\right\} \text{3CNF}$$

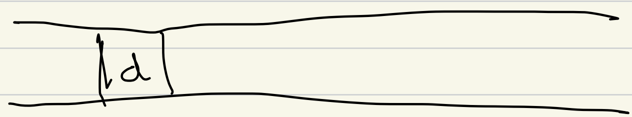
is satisfiable

if tape head not here

step i $\quad q$



step $i+1$: some permitted transition



$$\bigwedge_{i=1}^{T-1}\bigwedge_{j=1}^{T-1}\left[\left(\text{if } (Y_{ij}=F) \text{ AND } (X_{ijr}=T)\right) \text{ then } X_{i+1\,j\,r}=T\right]$$

$$\Updownarrow$$

$$\left(\text{if } \left[(p_1=F) \text{ and } (p_2=T)\right]\right)$$

$$\text{then } (p_3=T)$$

if $(\neg p_1$ and $p_2)$ then p_3

$(\neg p_1$ and $p_2) \Rightarrow p_3$

(if r_1 then r_2)

equiv to $\neg r_1$ or r_2

" " $\underbrace{\neg r_1 \text{ OR } r_2 \text{ or } r_2}_{\text{part of a 3CNF}}$

$\neg(\neg p_1 \wedge p_2)$ OR p_3

$(\neg(\neg p_1)$ OR $\neg p_2)$ OR p_3

p_1 OR $\neg p_2$ OR p_3

$$\bigwedge_{\substack{i=1,\dots,T-1 \\ j=1,\dots,T-1 \\ \gamma \in \Gamma}} \left[\begin{array}{l} \left(\text{if } (Y_{ij} = F) \text{ AND } (X_{ij\gamma} = T)\right) \\ \quad \text{then } X_{i+1\, j\, \gamma} = T \end{array} \right]$$

$=$

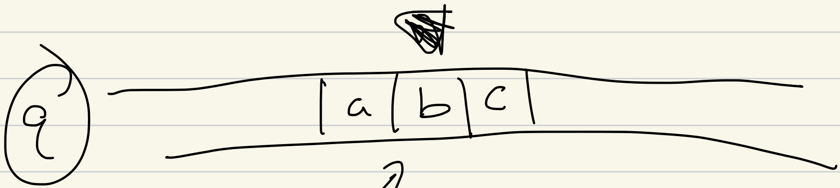
$$\bigwedge_{i,j,\gamma} \left(Y_{ij} \text{ OR } \neg X_{ij\gamma} \text{ OR } X_{i+1,j,\gamma} \right)$$

Rem:

$\#(i,j,\gamma)$ is $\quad Cn^k \, Cn^k \, |\Gamma|$

$= \text{const } n^{2k}$

Say $Y_{ij} = T$ ...



cell[i,j]

want to enforce

at step i+1

$$\delta(q, b) = \{ (q_5, d, R), (q_6, e, L) \}$$

---

if $(Y_{ij}$ and X_{ijb} and $Z_{iq})$ then

$$\Big((Z_{i+1,q_5} \text{ and } Y_{i+1,j+1} \text{ and } X_{i+1,j,d}) \text{ OR } (Z_{i+1,q_6} \wedge Y_{i+1,j-1} \wedge X_{i+1,j,e}) \Big)$$

if $(p_1 \wedge p_2 \wedge p_3)$ then Messy

Equiv

$(\neg p_1 \text{ OR } \neg p_2 \text{ OR } \neg p_3 \text{ OR Messy})$

} 3CNF

Remark: the parts in RED above are corrections to the class notes.

Recall:

$(X_1 \wedge X_2) \text{ OR } X_3$

$\iff (X_1 \text{ OR } X_3) \wedge (X_2 \text{ OR } X_3)$

$(X_1 \text{ OR } X_2) \wedge X_3$

$\iff (X_1 \wedge X_3) \text{ OR } (X_2 \wedge X_3)$

$(p_1 \wedge p_2 \wedge p_3)$ or $(p_4 \wedge p_5 \wedge p_6)$

$\equiv$

$($ or $) \wedge ($ or $) \wedge$ _ _ _

$= (p_1 \wedge p_4)$ or $(p_1 \wedge p_5)$ or $(p_1 \wedge p_6)$

or

p_2 p_2 p_2

p_3 p_3 p_3