$$\text{SAT} = \{ \langle \varphi(x_1, \dots, x_n) \rangle \mid \varphi \text{ is satisfiable} \}$$

Cook-Levin's Theorem: SAT is NP-complete.

Proof:

(1) $\text{SAT} \in \text{NP}$. ✓

(2) $\forall L \in \text{NP}$, want to show

$$L \leq_p \text{SAT}.$$

By definition of NP, there is a verifier $V(x,y)$, running in deterministic time $O(|x|^c)$ (for some const $c > 0$) s.t.

$\forall x, |x| = n$

$x \in L \Rightarrow \exists y, |y| \leq O(n^c)$ $V(x,y)$ accepts

$x \notin L \Rightarrow \forall y, |y| \leq O(n^c)$ $V(x,y)$ rejects.

Idea: Simulate $V(x,y)$ by a polysize propositional formula $\varphi(x,y,z)$:

$\forall x, y$, $V(x,y)$ accepts $\Leftrightarrow \exists z \ \varphi(x,y,z) = \text{True}$

Then the reduction f from L to SAT will be:

$$\forall x, \quad f(x) = \psi(y,z) = \varphi(x,y,z).$$

<u>Check</u>: (1) $x \in L \Rightarrow \exists y \ V(x,y)$ accepts

$\Rightarrow \exists y \ \exists z \ \varphi(x,y,z) = \text{True}$

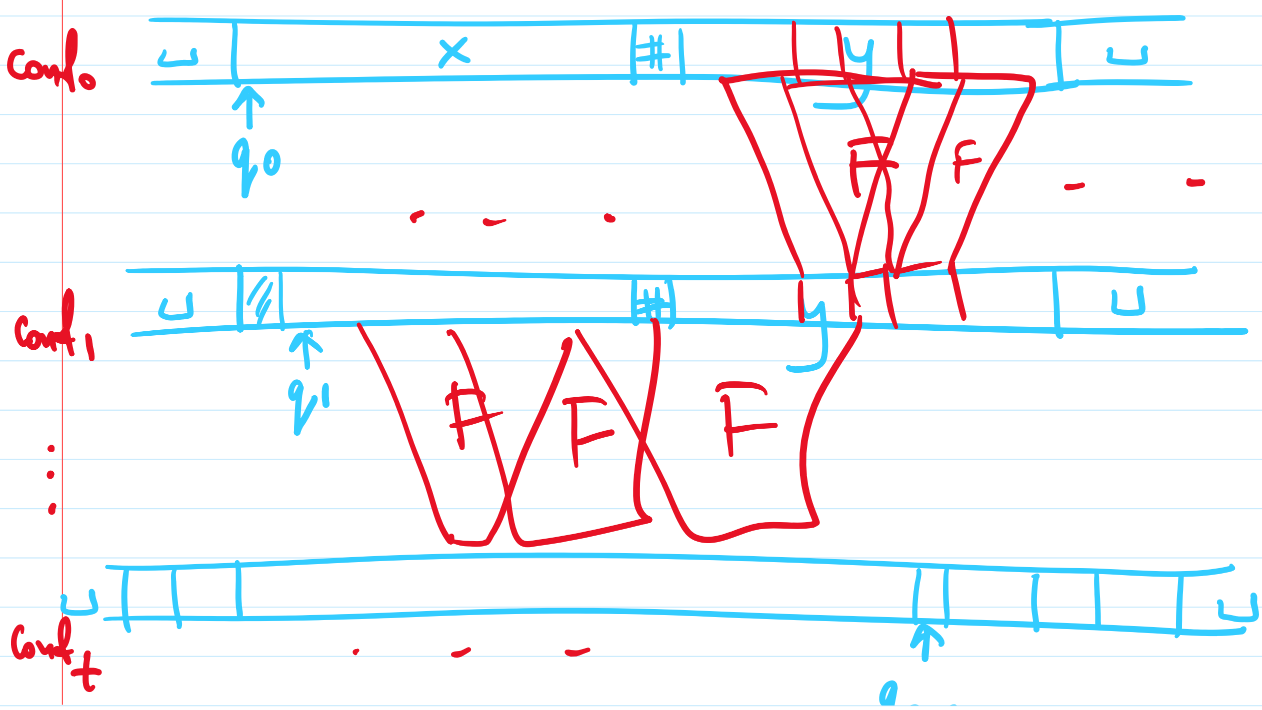
$\Rightarrow \psi(y,z) \in \text{SAT}$

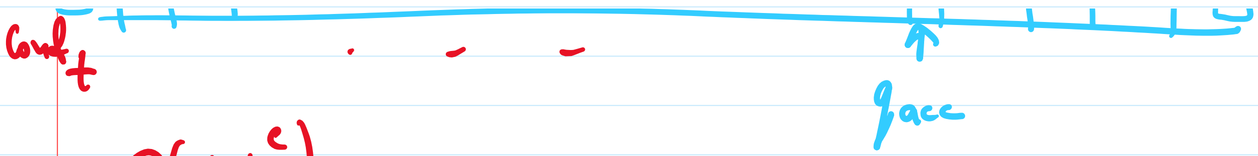
(2) $x \notin L \Rightarrow \forall y \ V(x,y)$ rejects

$\Rightarrow \forall y \ \forall z \ \varphi(x,y,z) = \text{False}$

$\Rightarrow \psi(y,z) \notin \text{SAT}$

Consider the computation of V on x, y.





$t \leq O(|x|^c)$

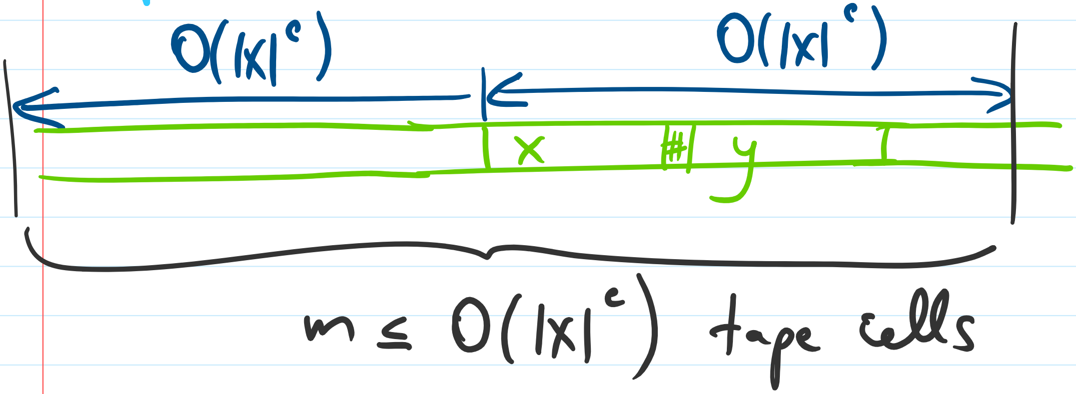
The computation $V(x,y)$ is <u>accepting</u> iff

(1) $conf_0$ is correct

(2) $conf_t$ is accepting

(3) $\forall i$, $conf_{i+1}$ correctly follows from $conf_i$, using the transition function of V.

<u>Observe:</u> $V(x,y)$ runs for $\leq O(|x|^c)$ steps. Hence, V will touch at most $O(|x|^c)$ tape cells.



So, enough to consider configurations on m tapecells only.

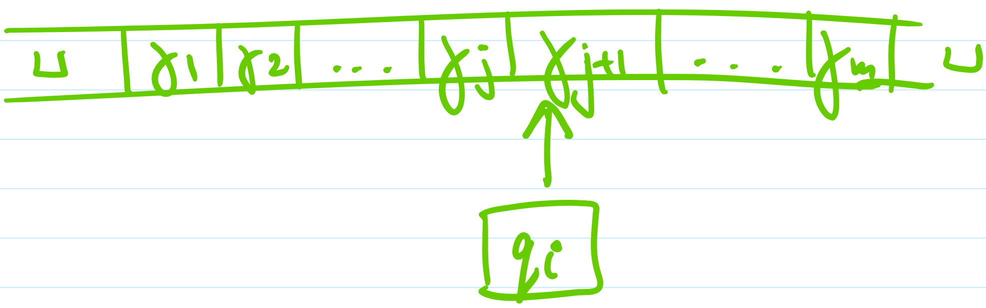
Code each configuration in binary :

Code each configuration in binary:

$$conf_i = a_1 a_2 \dots a_{m'} \quad , \quad m' \le O(m), \; a_i \in \{0,1\}$$

(code each tape symbol of V as a binary string;
code the state of V as a binary string)

$$\boxed{conf_i = \gamma_1 \gamma_2 \dots \gamma_j \, q_i \, \gamma_{j+1} \dots \gamma_m}$$



$z_{1,1} \dots z_{1,m'}$ $\underline{\text{encode}}$ $conf_0$

$z_{2,1} \dots z_{2,m'}$ —— $conf_1$

$\dots$

$z_{m,1} \dots z_{m,m'}$ —— $conf_m$

$m \cdot m'$ propositional variables z_i

(1) Formula: $init(z_{1,1}, \dots, z_{1,m'})$

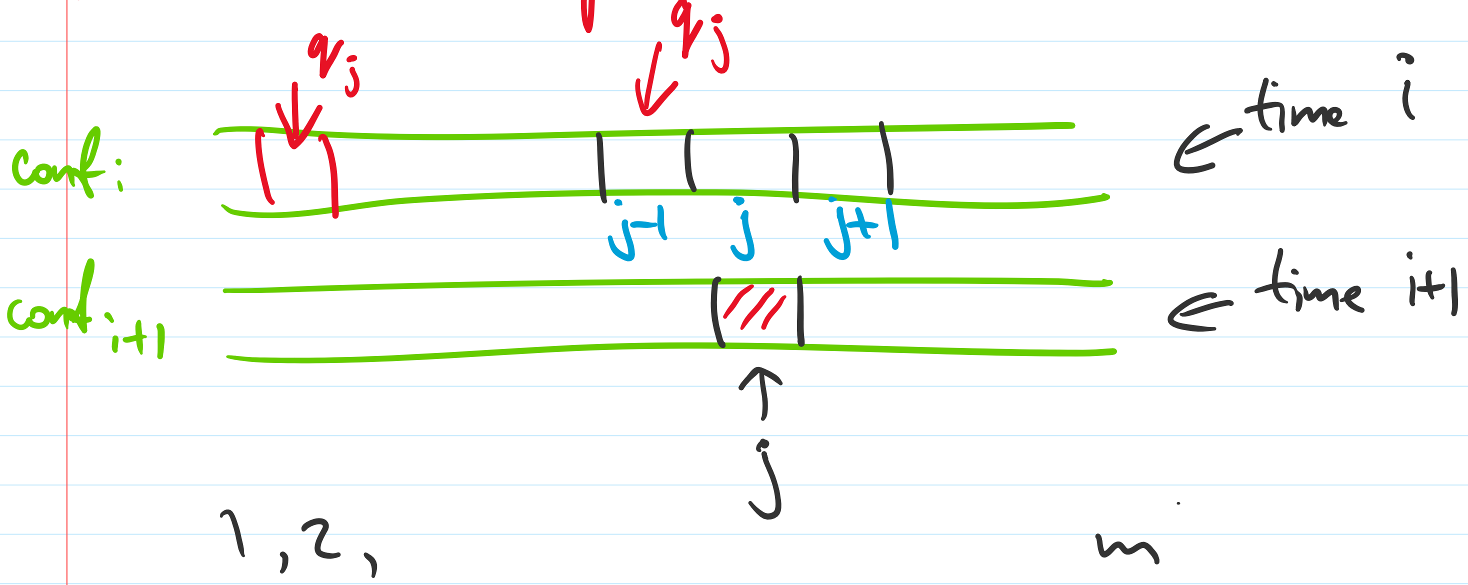
(1) Formula: $\text{init}(z_{1,1}, \ldots, z_{1,m'})$

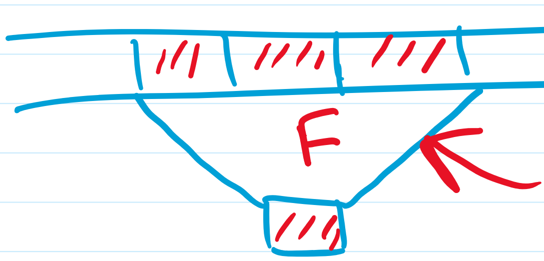
checks that $z_{1,1}, \ldots, z_{1,m'}$ is a correct encoding of $\text{conf}_0 = (q_0 \, x \# y)$

(2) Formula: $\text{final}(z_{m,1}, \ldots, z_{m,m'})$

checks that $z_{m,1}, \ldots, z_{m,m'}$ is a correct encoding of an accepting configuration (which mentions q_{acc} somewhere).

(3) Formula: Step





$\text{Step}(z_{i,j-1}, z_{i,j}, z_{i,j+1}, z_{i+1,j})$

$\mathrm{Step}(z_{i,j-1}, z_{i,j}, z_{i,j+1}, z_{i+1,j})$

$=$ True iff

time i $\quad \boxed{\overline{z_{i,j-1}}} \boxed{\overline{z_{i,j}}} \boxed{\overline{z_{i,j+1}}}$

time $i+1$ $\quad \boxed{\overline{z_{i+1,j}}}$

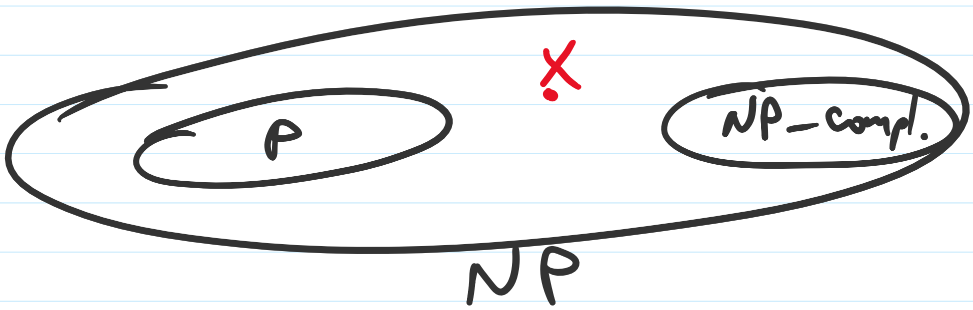
My final formula

$$\varphi(x, y, z) = \mathrm{init}(..) \wedge \mathrm{final}(..) \wedge \bigwedge_{i=1}^{m} \bigwedge_{j=1}^{m} F(\ldots)$$

$$|\varphi| \leq O(m^2)$$

Ladner's Thm

$P \neq NP \Rightarrow$



$\exists X \notin P$, & X is not NP-complete.