

$\text{State}(q, t)$: state at time t is q

$\text{Head}(j, t)$: head at time t is at j^{th} cell

$\text{Tape}(j, s, t)$: j^{th} cell at time t has symbol s

For $t = 1$:

$\text{size} = p(n) + 2$ [$\text{State}(q_0, 0) \wedge \text{Head}(1, 0) \wedge \overline{\text{Tape}}(1, x[1], 0) \wedge$
 $\dots \wedge \overline{\text{Tape}}(n, x[n], 0) \wedge \overline{\text{Tape}}(n+1, B, 0) \wedge$
 $\dots \wedge \overline{\text{Tape}}(p(n), B, 0)$]

- For t $\neg \text{Stat}(q, t) \vee \neg \text{Stat}(q', t)$
- $H_q: \text{Stat}(q, t) \stackrel{\equiv}{\Rightarrow} \neg \text{Stat}(q', t) \quad \text{for } q' \neq q$
- $H_j: \text{Head}(j, t) \Rightarrow \neg \text{Head}(j', t) \quad \text{for } j' \neq j$
- $H_j H_s: \text{Tape}(j, s, t) \Rightarrow \neg \text{Tape}(j, s', t) \quad \text{for } s' \neq s$
- C ____

$$\begin{aligned}
 \text{Size} &= p(n) * \left(|Q|^2 + p^2(n) + p(n) * |\Sigma|^2 \right) \\
 &= O(p^3(n))
 \end{aligned}$$

For $t \geq 1$

$$\forall j \forall s \left[\text{Stat}(q, t) \wedge \text{Head}(j, t) \wedge \text{Tape}(j, s, t) \right]$$
$$\Rightarrow \left[\text{State}(q_1, t+1) \wedge \text{Head}(j_1, t+1) \wedge \overline{\text{Tape}}(j, s_1, t+1) \right]$$
$$\vee \left[\text{State}(q_2, t+1) \wedge \text{Head}(j_2, t+1) \wedge \overline{\text{Tape}}(j, s_2, t+1) \right]$$
$$\vee \dots$$

Size $\leq \tilde{p}(n) * |Q| * |\Sigma| * |Q|^2 = O(p^3(n))$

$\left[\forall j \forall j' \neq j \forall s : \text{Head}(j, t) \Rightarrow \begin{bmatrix} \text{Tape}(j', s, t+1) \Leftrightarrow \\ \text{Tape}(j', s, t) \end{bmatrix} \right]$
 size = $O(p^3(n))$

$\bigvee_{q \in F} \text{State}(q, p(n)) \quad] \quad \text{size} = 1$

Theorem: TM M accepts x , $|x|=n$, in $p(n)$ steps
 iff formula $\neg F$ is satisfiable.
 $|F| = O(p^3(n))$

Therefore, if $SAT \in P$ then $NP = P$.



SAT is NP-hard.

Def : Set A is NP-complete if
 A is NP-hard and $A \in NP$.

Theorem : VC in NP-complet.

prof: Reduce SAT to VC.

Given formula $F = C_1 \wedge C_2 \wedge \dots \wedge C_m$
over n variables x_1, x_2, \dots, x_n .

x_1

$\neg x_1$

x_2

$\neg x_2$

:

|

x_n

$\neg x_n$

C_1

C_2

:

|

|

:

|

C_m