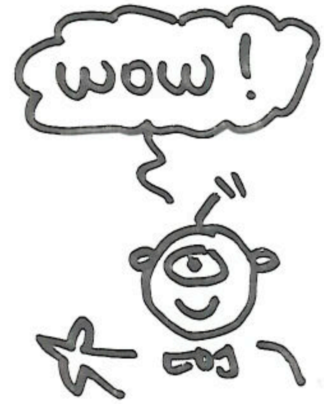
The AMAZING Cook-Levin Theorem!

[1971] [1973]



Theorem: 3SAT is $\mathcal{NP}$-complete

Just About as Good Theorem: SAT is $\mathcal{NP}$-complete

SAT: $(x_1 \vee x_2 \vee \overline{x_3} \vee x_4) \wedge (x_1 \vee \overline{x_4}) \wedge \cdots \wedge (x_2 \vee \overline{x_3} \vee x_4)$

Goal: $L \le_p SAT$

absolutely any $L \in \mathcal{NP}$!

- $L \in \mathcal{NP} \Rightarrow \exists$ TM (nondeterministic TM !) M that accepts L in time $p(n)$. (some polynomial)

- $M = (\underbrace{Q}_{\{q_0, \dots, q_r\}}, \Sigma, \underbrace{\Gamma}_{\{\sigma_0, \sigma_1, \dots, \sigma_g\}}, \delta, q_0, \underbrace{q_{yes}}_{q_1}, \underbrace{q_{no}}_{q_2})$

accept, reject

blank: σ_0

- Now, construct $f : L \longrightarrow SAT$

Variable Name	Range	Meaning
$Q_{i,k}$ "state"	$0 \le i \le p(n)$ $0 \le k \le r$	At time i, M is in state q_k
$H_{i,j}$ "head"	$0 \le i \le p(n)$ $0 \le j \le p(n)$	At time i, tape head on cell j.
$S_{i,j,k}$ "symbol"	$0 \le i \le p(n)$ $0 \le j \le p(n)$ $0 \le k \le g$	At time i, contents of tape cell j is σ_k

The Six Clause Groups

Group	Role
G_1	At time 0, the machine is in its original configuration
G_2	At each time i, M is in exactly one state.
G_3	At each time i, the tape head is scanning exactly one cell.
G_4	At each time i, each tape cell contain exactly one symbol from Γ'.
G_5	For each time i, the configuration at time $i+1$ follows by a δ-rule.
G_6	By time $p(n)$, M is in state q_Y.

"At time 0, machine is in its original configuration"

G_1 :

Let $w = \underbrace{\sigma_{i_0} \sigma_{i_1} \cdots \sigma_{i_{n-1}}}_{\text{input has length } n}$

$$(Q_{0,0}) \wedge (H_{0,0}) \wedge$$

at time 0 ... ... in state 0 ... at time 0 ... ... head at position

$$(S_{0,0,i_0}) \wedge (S_{0,1,i_1}) \wedge \ldots$$

at time 0 ... ...cell 0... ...contain σ_{i_0}

$$\ldots \wedge (S_{0,n-1,i_{n-1}}) \wedge (S_{0,n,0}) \wedge$$

$$\ldots \wedge (S_{0,p(n),0})$$

"At each time i, M is in exactly one state"

G_2 :

$$\underbrace{(Q_{i,0} \vee Q_{i,1} \vee \ldots \vee Q_{i,r})}_{\text{"at time } i\text{, } M \text{ is in at least one state"}}$$

$$\wedge \; (\underbrace{\overline{Q_{i,j}} \vee \overline{Q_{i,k}}}_{\text{"at time } i \text{ } M \text{ is not in state } j \text{ AND in state } k\text{"}})$$

$$0 \le i \le p(n)$$

$$0 \le j < k \le r$$

G_3: "At each time i, M is scanning exactly one tape cell"

$$\overbrace{\left(H_{i,0} \vee H_{i,1} \vee \dots \vee H_{i,p(n)} \right)}^{\text{at time } i\text{, head is in \underline{at least} one position}}$$

$$\wedge \left(\underbrace{\overline{H_{i,j}} \vee \overline{H_{i,k}}}_{\text{at time } i\text{, head is not in position } j \text{ \underline{AND} position } k} \right)$$

$$0 \le i \le p(n)$$

$$0 \le j < k \le p(n)$$

G_4: "At each time i, each tape cell contains exactly one symbol from Γ"

$$\overbrace{\left(S_{i,j,0} \vee S_{i,j,1} \vee \dots \vee S_{i,j,g} \right)}^{\text{at time } i\text{, cell } j \text{ contains symbol } \sigma_0 \text{ or } \sigma_1 \text{ or } \dots \text{ or } \sigma_g}$$

$$\wedge \left(\overbrace{\overline{S_{i,j,k}} \vee \overline{S_{i,j,\ell}}}^{\text{at time } i\text{, cell } j \text{ does not contain \underline{both} } \sigma_k \text{ \underline{AND} } \sigma_\ell} \right)$$

$$0 \le i \le p(n)$$

$$0 \le j \le p(n)$$

$$0 \le k < \ell \le g$$

G_5: "For each time i, the configuration at time $i+1$ follows by a δ-rule."

For i, j, k, ℓ

$0 \le i \le p(n)$ ← range of time

$0 \le j \le p(n)$ ← range on head position

$0 \le k \le r$ ← range of states

$0 \le \ell \le g$ ← range of symbols

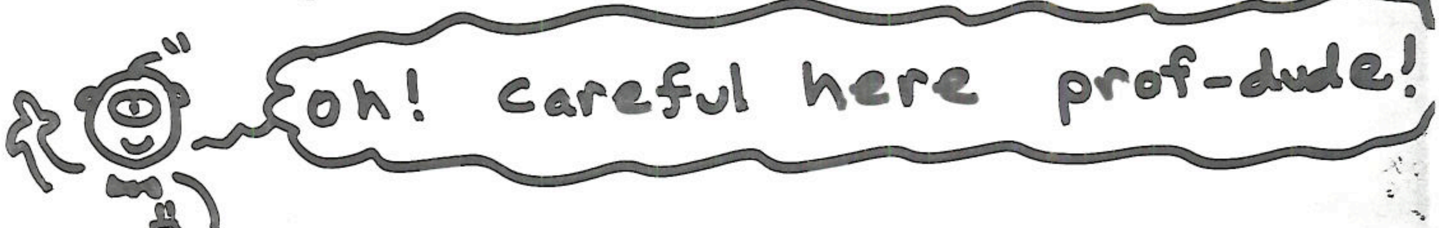
$$\delta(q_k, \sigma_\ell) = (q_{k'}, \sigma_{\ell'}, \Delta)$$

Δ: +1 or −1 for "right" and "left"

$$(\overline{H_{\underset{\text{time}}{i},\underset{\text{head position}}{j}}} \vee \overline{Q_{\underset{\text{time}}{i},\underset{\text{state}}{k}}} \vee \overline{S_{\underset{\text{time}}{i},\underset{\text{pos}}{j},\underset{\text{symbol}}{\ell}}} \vee H_{i+1,j+\Delta})$$

$$\wedge\ (\overline{H_{i,j}} \vee \overline{Q_{i,k}} \vee \overline{S_{i,j,\ell}} \vee Q_{i+1,k'})$$

$$\wedge\ (\overline{H_{i,j}} \vee \overline{Q_{i,k}} \vee \overline{S_{i,j,\ell}} \vee S_{i+1,j,\ell'})$$



$$\delta(q_k, \sigma_\ell) = \{ (q_{k'}, \sigma_{\ell'}, \overbrace{+1}^{\text{"move right"}}), \\ (q_{k''}, \sigma_{\ell''}, -1) \}$$

$$(\overline{H_{i,j}} \vee \overline{Q_{i,k}} \vee \overline{S_{i,j,\ell}} \vee H_{i+1,j+1} \\ \vee H_{i+1,j-1})$$

$$\wedge (\overline{H_{i,j}} \vee \overline{Q_{i,k}} \vee \overline{S_{i,j,\ell}} \vee Q_{i+1,k'} \\ \vee Q_{i+1,k''})$$

$$\wedge (\overline{H_{i,j}} \vee \overline{Q_{i,k}} \vee \overline{S_{i,j,\ell}} \vee S_{i+1,j,\ell'} \\ \vee S_{i+1,j,\ell''})$$

G_6 : "At time $p(n)$, M is in the accepting state q_1"

$$(Q_{p(n),1})$$

- $G_1 \wedge G_2 \wedge G_3 \wedge G_4 \wedge G_5 \wedge G_6$ is satisfiable iff M accepts w ($w \in L$).

- Did the reduction really take polynomial time?

How many variables?

$Q_{i,k}$ $\quad 0 \le i \le p(n)$ ← time
$\quad 0 \le k \le r$ ← max state

$H_{i,j}$ $\quad 0 \le i \le p(n)$ ← time
$\quad 0 \le j \le p(n)$ ← location

$S_{i,j,k}$ $\quad 0 \le i \le p(n)$ ← time
$\quad 0 \le j \le p(n)$ ← location
$\quad 0 \le k \le g$ ← symbol

How many clauses? $\quad 6\,[p(n)]^2 \cdot (r+1)(g+1)$

And finally...

Corollary:

3SAT is $\mathcal{NP}$-complete

Pf:

1. $3SAT \in \mathcal{NP}$

2. $SAT \leq_p 3SAT$

$$(x_1) \wedge (\overline{x_2} \vee x_3) \wedge (x_1 \vee x_2 \vee \overline{x_3})$$
$$\wedge (x_1 \vee \overline{x_2} \vee x_3 \vee x_4 \vee \dots \vee x_k)$$

$$(x_1) \longrightarrow (x_1 \vee a \vee b) \wedge (x_1 \vee a \vee \overline{b}) \wedge (x_1 \vee \overline{a} \vee b) \wedge (x_1 \vee \overline{a} \vee \overline{b})$$

$$(\overline{x_2} \vee x_3) \longrightarrow (\overline{x_2} \vee x_3 \vee c) \wedge (\overline{x_2} \vee x_3 \vee \overline{c})$$

$$(x_1 \vee \overline{x_2} \vee x_3 \vee x_4 \vee \dots \vee x_k) \longrightarrow$$