Today: Cook-Levin Theorem:

If $L \in NP$ (non-deterministic poly time), then you can solve L in poly time if you have a "button" that solves SAT or 3SAT.

Recall: $SAT = \{ \langle f \rangle \mid$ f is a Boolean formula that is satisfiable $\}$

e.g.

Boolean formula: e.g. $f = ((x_1 \text{ and } \neg x_2) \text{ or } x_3) \text{ and } (\neg x_1 \text{ or} \ldots$

$\langle f \rangle \in \Sigma^*$, $\Sigma = \{ (,), x, 0, \ldots, 9, \neg, \text{and}, \text{or} \}$

$\neg \Leftrightarrow$ not, and $\Leftrightarrow \wedge$, or $\Leftrightarrow \vee$

e.g. $f = x_{171} \text{ OR } (\neg x_{133})$

$\langle f \rangle = \underbrace{x\,171 \text{ OR } (\neg x\,133)}_{\text{length } 12} \in \Sigma^*$

=

f is satisfiable if $f = f(x_1, \ldots, x_n)$ and there is an assignment $x_1 \to T/F$, $x_2 \to T/F$, $\ldots$, $x_n \to T/F$ that makes f true.

=

For reasons to be made clear:

f is 3CNF (3 conjuctive normal form) if

$f = \text{blah}_1 \text{ and } \text{blah}_2 \text{ and } \text{blah}_3 \text{ and } \ldots \text{ and } \text{blah}_e$

where each $\text{blah}_i = (\text{z} \text{ OR } \text{z} \text{ OR } \text{z})$ each z is a variable $x_1, \dots, x_n$ or $\neg x_1, \dots, \neg x_n$.

Idea: SAT, 3SAT $\in$ NP. I.e. if f is a Boolean formula, you can "guess" T/F values for its variables ("write down non-derministically") and you can verify whether f holds or not.

Also 3COLOR $\in$ NP,

We claim: SAT, 3SAT is as difficult a question as there is in NP

P vs. NP? $\Longleftrightarrow$ Is SAT in P?

For this reason we say that SAT is NP-complete.

1SAT, 2SAT | 3SAT, 4SAT

1COLOR, 2COLOR | 3COLOR, 4COLOR

in P | NP-complete

Given a non-det Turing machine M, input w, let's simulate if w is accepted (non-det) by M:

T.M. computation:

Initial Config — state q_0 — $w_1 \mid w_2 \mid \cdots \mid w_n \mid \sqcup \mid \sqcup \mid \sqcup \mid \cdots$

step 1

non-deterministic

Step 2 — other state — $\gamma \mid w_2 \mid \cdots \mid w_n \mid \sqcup \mid \sqcup \mid \sqcup \mid \cdots$

step 3

step 4

etc.

step n^5 — q_{acc}

Say tape symbols Γ ← fixed, constant

states Q

Boolean

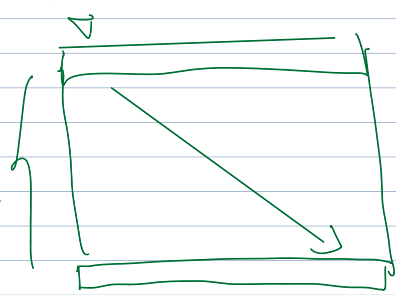
$$X_{ijr} = \begin{cases} T & \text{if at time } i\text{, cell } j\text{, we have symbol } r \\ F & \text{otherwise} \end{cases}$$

When is the computation possible

$$Y_{ij} = \begin{cases} T & \text{if tape head at time } i \text{ is on cell } j \\ F & \text{otherwise} \end{cases}$$

$$Z_{iq} = \begin{cases} T & \text{if at time } i \text{ we are in state } q \\ F & \text{otherwise} \end{cases}$$

Time $n^5 \longleftrightarrow n^5$ steps



n^5 steps

cell number $\leq n^5$

X_{ijr} : i – cell number $\leq n^5$, $r \in$ finite set

j time/step $\leq n^5$,

x variables $\leq n^5 \cdot n^5 \cdot |\Gamma| \leq c\, n^{10}$

y vars, # z vars $\leq$ polynomial in n

Can you reach q_{acc} in n^5 time/steps ?

Yes, if at step 1 ...... formula that express that you see on tape what you should

from (step 1 $\rightarrow$ step 2 everything is valid)

AND (step 2 $\rightarrow$ step 3 " " ")

AND (step 3 $\rightarrow$ step 4 " " ")

AND ⋮

AND (step n^5-1 $\rightarrow$ step n^5 " " ")

AND (step n^5 we are in state q_{acc})

3 CNF

$$Z_{n^5\, q_{acc}} = T$$

$$(Z_{n^5\, q_{acc}})$$