April 18, 2019 10:59 AM

Last Time:

P = all decision problems solvable in polytime

$L_1 \leq_p L_2$ polytime reduction

NP = all decis. problems solvable in <u>nondet.</u> polytime

= all problems of the form

Input: x

Output: yes iff $\exists y$ s.t. $C(x,y)$ is true

poly size certificate

poly-time certifier

Fact $\underbrace{P \subseteq NP} \subseteq EXP$

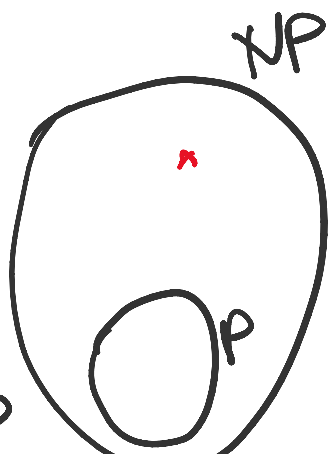
EXP: all problems solvable in $2^{p(n)}$ time for some poly

Pf: ($P \subseteq NP$) certifier ignores certificate

($NP \subseteq EXP$) try all certificates by brute force.

"Million-Dollar" Conjecture:

$$P \neq NP.$$



idea - to find a hard problem in NP, take the <u>hardest</u> problem in NP.

Def L is <u>NP-complete</u> iff

① $L \in NP$, and

② $\underline{\forall} L' \in NP$, $L' \le_p L$. ← NP-hard

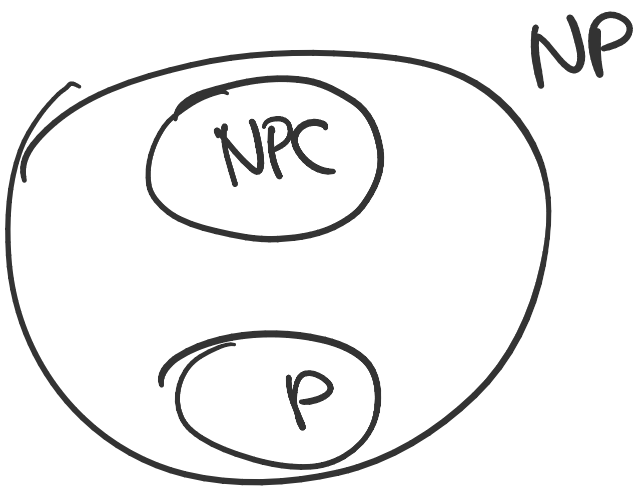
Fact 3 Let L be NP-complete.
Then $L \notin P \iff P \neq NP$.

Pf: ($\Rightarrow$) Suppose $L \notin P$.
Then $L \in NP - P$. Then $P \neq NP$.

($\Leftarrow$) Suppose $L \in P$.
Then $\forall L' \in NP$, $L' \le_p L$
$L \in P$
$\overset{\text{Fact 1}}{\Longrightarrow}$ $L' \in P$.

$\therefore P = NP$. □

World assuming $P \neq NP$:



<u>"First" NP-Complete Problem: Satisfiability (SAT)</u>

Input: Boolean formula in n vars
$F(x_1, \dots, x_n)$

$F(x_1, \ldots, x_n)$

Formula-SAT $\left\{ \text{Output: yes iff } \exists \text{ assignment of Boolean values to vars s.t. } F \text{ evaluates to true} \right.$

e.g. $F(x_1,x_2,x_3) = \left(\overline{x}_1 \vee \overline{x_2 \wedge \overline{x}_3}\right) \wedge (x_1 \vee x_2)$

yes $(x_1 = 1,\ x_2 = 0,\ x_3 = 0 \text{ or } 1)$

brute force $\tilde{O}(2^n)$

faster?

Cook-Levin Thm (1971) SAT is NP-complete.

Pf Sketch: ① SAT $\in$ NP:

certificate: assignment ← poly size

certifier: check F evaluates to true on A ← poly time

② Need to give a polytime reduction from every $L \in NP$ to SAT:

Say L is: Input: z

Output: yes iff $\exists y$ s.t. $C(z,y)$ is true

checkable by a polytime algm/TM M

idea: simulate M by Boolean formula F

create vars $x[i,j]$ = content of tape cell i at step j

⋮

□

Can prove other problems NP-complete by reduction ...

Recipe to NPC:

Fact 4 If ① $L \in NP$ and

② $L_0 \leq_p L$ for a known NP-complete prob. L_0,

then L is NP-complete.

Pf: $\forall L' \in NP$, $L' \leq_p L_0$ since L_0 is NPC

$L_0 \leq_p L$

$\overset{\text{Fact 2}}{\Rightarrow} L' \leq_p L$. $\square$

Ex: 3SAT

Input: Boolean formula of the form

$$F = \bigwedge_{i=1}^{m} \underbrace{(\alpha_{i1} \vee \alpha_{i2} \vee \alpha_{i3})}_{\text{clauses}}$$

3CNF formula

where each α_{ij} is either a var or its complement

literal

Output: yes iff $\exists$ assignment that makes F true

e.g. $F = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_2 \vee x_4)$
$\wedge (x_2 \vee x_3 \vee \bar{x}_4) \wedge (\bar{x}_1 \vee x_3 \vee \bar{x}_4)$

yes $(x_1 = 0 \text{ or } 1,\ x_2 = 1,\ x_3 = 0 \text{ or } 1,\ x_4 = 0)$

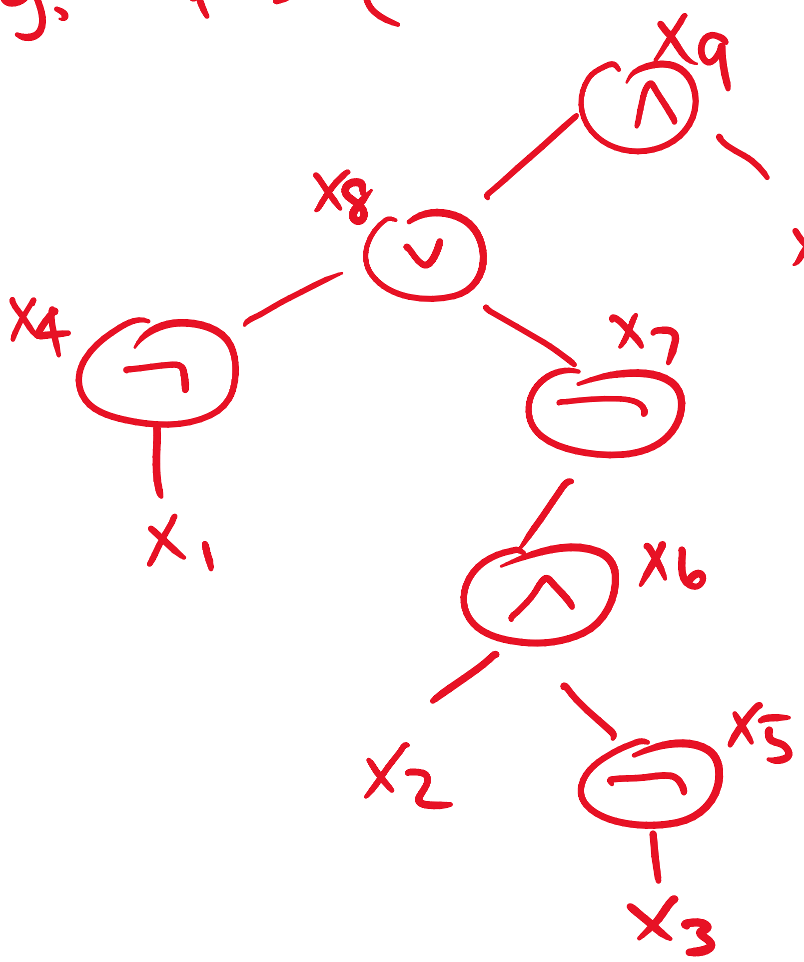
Claim 3SAT is NP-complete.

Pf: (sketch)

1. 3SAT $\in$ NP ✓
2. $\underline{\text{SAT}} \le_p \underline{\text{3SAT}}$:

Given arbitrary Boolean formula F, construct a 3CNF formula F' as follows:

e.g. $F = (\bar{x}_1 \vee \overline{x_2 \wedge \bar{x}_3}) \wedge x_1$



$$
\begin{aligned}
F' = & (x_4 \equiv \bar{x}_1) \\
\wedge & (x_5 \equiv \bar{x}_3) \\
\wedge & (x_6 \equiv x_2 \wedge x_5) \\
\wedge & (x_7 \equiv \bar{x}_6) \\
\wedge & (x_8 \equiv x_4 \vee x_7) \\
\wedge & (x_9 \equiv x_8 \vee x_1) \\
\wedge & \ x_9
\end{aligned}
$$

each can be converted to 3CNF

Construction $F \to F'$ takes polytime.

Correctness: $\exists$ assignment that makes F true

$\iff \exists$ " - - - F' true.

$\square$