Hardness of problems

To prove problem Y is hard

1. Find a known hard problem X

2. Prove $X \leq_p Y$

X can be solved in polytime given a magic box that solves Y in polytime.

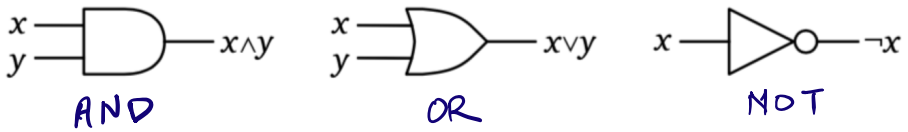
So If Y were easy, X would be easy

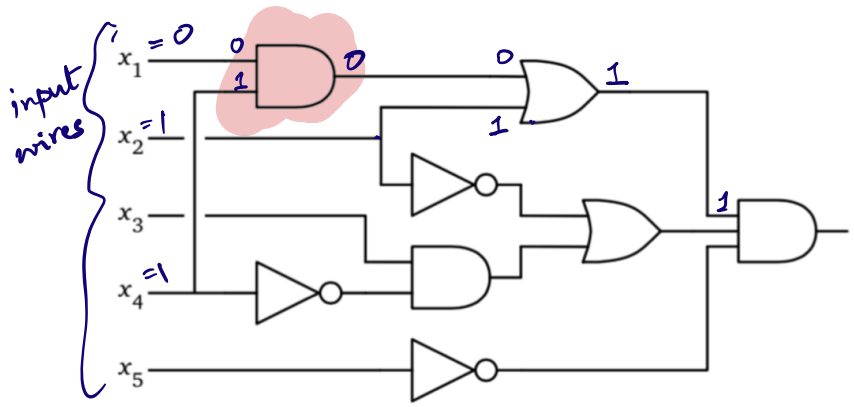
But by 1, X is hard. So Y must be hard.

Example of a known hard problem:

Circuit satisfiability

GATES.





BOOLEAN CIRCUIT

Circuit Satisfiability Problem :

Given boolean circuit C, is there any assignment to its input wires for which the circuit outputs 1 ?

Given an assignment to input wires, there is a linear time algorithm that computes the output.

$O(2^n \cdot \text{ckt size})$ = exponential in n.

$\times 1.9999^n$ Believe: no polynomial-time algorithm

P : set of languages where $x \in L$ can be decided by a TM in time $\text{poly}(|x|)$

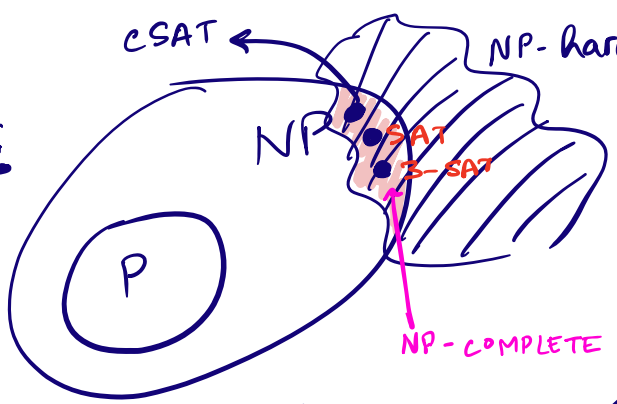
NP : set of languages where membership of any $x \in L$ can be verified in time $\text{poly}(|x|)$.

$\exists$ Turing Machine M that is polynomial-time s.t. for every $x \in L$, $\exists$ certificate w s.t. $M(x, w) = 1$

for every $x \notin L$ $\forall$ certificates w, $M(x, w) = 0$.

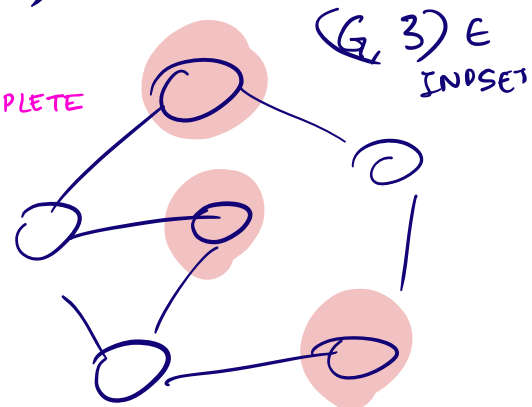
$P \overset{?}{=} NP$. $P \neq NP$.

Belief:



INDEPENDENT SET:

(G, k).



COOK-LEVIN THEOREM.

Ver1: Assuming $P \neq NP$,
there is no polynomial-time algorithm
for circuit SAT.

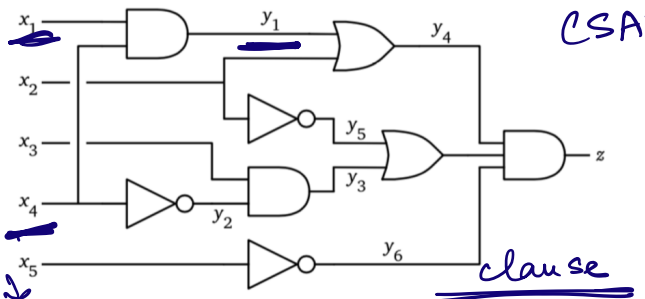
Ver2: Circuit-SAT is NP-hard.

Formula-satisfiability
(SAT for short).

Given a boolean formula:

$$(y_1 = x_1 \wedge x_2) \wedge (y_2 = \bar{x}_2) \wedge$$
$$(y_3 = x_3 \wedge y_2) \wedge (\ \ldots\ )$$

SAT is also hard.
(Assuming $P \neq NP$, no polynomial-time
algorithm for SAT).

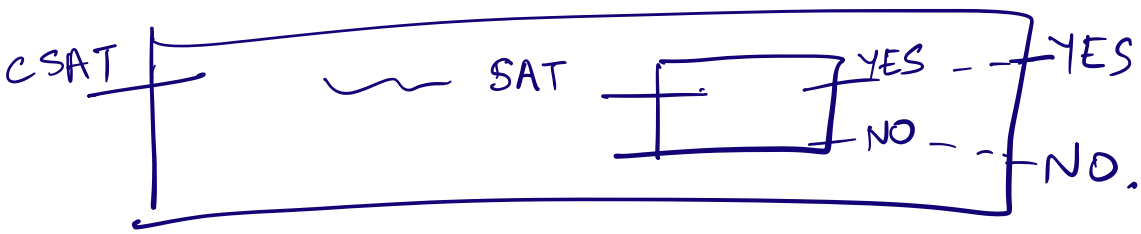


CSAT

CSAT $\leq$ SAT.

clause

$$(y_1 = x_1 \wedge \overline{x_4}) \wedge (y_2 = \overline{x_4}) \wedge (y_3 = x_3 \wedge y_2) \wedge (y_4 = y_1 \vee x_2) \wedge$$
$$(y_5 = \overline{x_2}) \wedge (y_6 = \overline{x_5}) \wedge (y_7 = y_3 \vee y_5) \wedge (z = y_4 \wedge y_7 \wedge y_6) \wedge z$$



---

exactly 3 literals

$$(a \vee b \vee c) \wedge (b \vee \bar{c} \vee \bar{d}) \wedge (\bar{a} \vee c \vee d) \wedge (a \vee \bar{b} \vee \bar{d})$$

OR literal AND

3-CNF problem.

Conjunctive normal form.

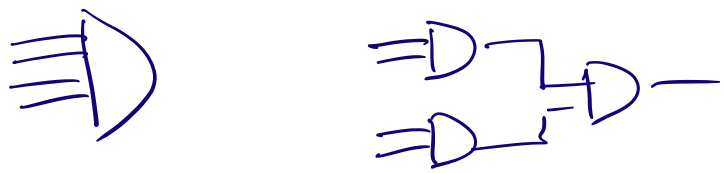
3-SAT
3-CNF SAT.

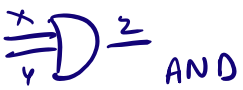
Given a 3-CNF formula, is there an assignment to variables that makes the formula true?

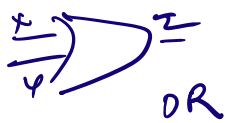
CSAT $\leq$ 3CNF-SAT.

Given an **arbitrary** boolean circuit.

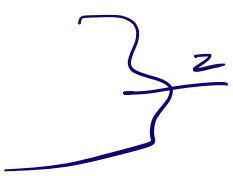
① Make all gates binary.



②  AND $(z = x \wedge y) \wedge$

 OR $(z = x \vee y) \wedge$

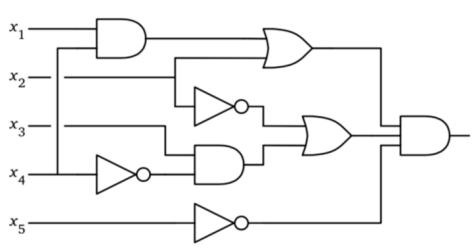
 $(z = \overline{x}) \wedge$

 $\ldots \wedge z$

③ $(a = b \wedge c) \rightsquigarrow$ **CNF** $(a \vee \overline{b} \vee \overline{c}) \wedge (\overline{a} \vee b) \wedge (\overline{a} \vee c)$ ← 2 literals

④ $(a \vee b) \rightarrow (a \vee b \vee p) \wedge (a \vee b \vee \overline{p})$

$z \rightarrow (z \vee p \vee q) \wedge (z \vee \overline{p} \vee q) \wedge (z \vee p \vee \overline{q}) \wedge (z \vee \overline{p} \vee \overline{q})$



$(y_1 \vee \overline{x_1} \vee \overline{x_4}) \wedge (\overline{y_1} \vee x_1 \vee z_1) \wedge (\overline{y_1} \vee x_1 \vee \overline{z_1}) \wedge (\overline{y_1} \vee x_4 \vee z_2) \wedge (\overline{y_1} \vee x_4 \vee \overline{z_2})$
$\wedge (y_2 \vee x_4 \vee z_3) \wedge (y_2 \vee x_4 \vee \overline{z_3}) \wedge (\overline{y_2} \vee \overline{x_4} \vee z_4) \wedge (\overline{y_2} \vee \overline{x_4} \vee \overline{z_4})$
$\wedge (y_3 \vee \overline{x_3} \vee \overline{y_2}) \wedge (\overline{y_3} \vee x_3 \vee z_5) \wedge (\overline{y_3} \vee x_3 \vee \overline{z_5}) \wedge (\overline{y_3} \vee y_2 \vee z_6) \wedge (\overline{y_3} \vee y_2 \vee \overline{z_6})$
$\wedge (\overline{y_4} \vee y_1 \vee x_2) \wedge (y_4 \vee \overline{x_2} \vee z_7) \wedge (y_4 \vee \overline{x_2} \vee \overline{z_7}) \wedge (y_4 \vee \overline{y_1} \vee z_8) \wedge (y_4 \vee \overline{y_1} \vee \overline{z_8})$
$\wedge (y_5 \vee x_2 \vee z_9) \wedge (y_5 \vee x_2 \vee \overline{z_9}) \wedge (\overline{y_5} \vee \overline{x_2} \vee z_{10}) \wedge (\overline{y_5} \vee \overline{x_2} \vee \overline{z_{10}})$
$\wedge (y_6 \vee x_5 \vee z_{11}) \wedge (y_6 \vee x_5 \vee \overline{z_{11}}) \wedge (\overline{y_6} \vee \overline{x_5} \vee z_{12}) \wedge (\overline{y_6} \vee \overline{x_5} \vee \overline{z_{12}})$
$\wedge (\overline{y_7} \vee y_3 \vee y_5) \wedge (y_7 \vee \overline{y_3} \vee z_{13}) \wedge (y_7 \vee \overline{y_3} \vee \overline{z_{13}}) \wedge (y_7 \vee \overline{y_5} \vee z_{14}) \wedge (y_7 \vee \overline{y_5} \vee \overline{z_{14}})$
$\wedge (y_8 \vee \overline{y_4} \vee \overline{y_7}) \wedge (\overline{y_8} \vee y_4 \vee z_{15}) \wedge (\overline{y_8} \vee y_4 \vee \overline{z_{15}}) \wedge (\overline{y_8} \vee y_7 \vee z_{16}) \wedge (\overline{y_8} \vee y_7 \vee \overline{z_{16}})$
$\wedge (y_9 \vee \overline{y_8} \vee \overline{y_6}) \wedge (\overline{y_9} \vee y_8 \vee z_{17}) \wedge (\overline{y_9} \vee y_6 \vee z_{18}) \wedge (\overline{y_9} \vee y_6 \vee \overline{z_{18}}) \wedge (\overline{y_9} \vee y_8 \vee \overline{z_{17}})$
$\wedge (y_9 \vee z_{19} \vee z_{20}) \wedge (y_9 \vee \overline{z_{19}} \vee z_{20}) \wedge (y_9 \vee z_{19} \vee \overline{z_{20}}) \wedge (y_9 \vee \overline{z_{19}} \vee \overline{z_{20}})$

To Prove Y is NP-hard.

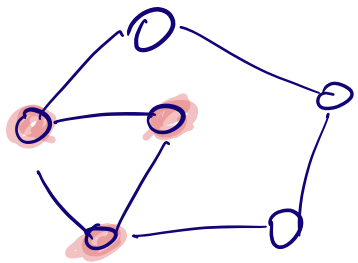
- Find a known NP-hard problem X
  (CSAT, SAT, 3-SAT)
- Show $X \leq_p Y$.

$(G, k) \in L_{CLIQUE}$ iff

G has a CLIQUE of size $\geq k$.

Q: Show that CLIQUE is NP-complete.

A: 1) First, show CLIQUE is in NP.



2) CLIQUE is NP-hard.

$3SAT \leq_p$ CLIQUE.

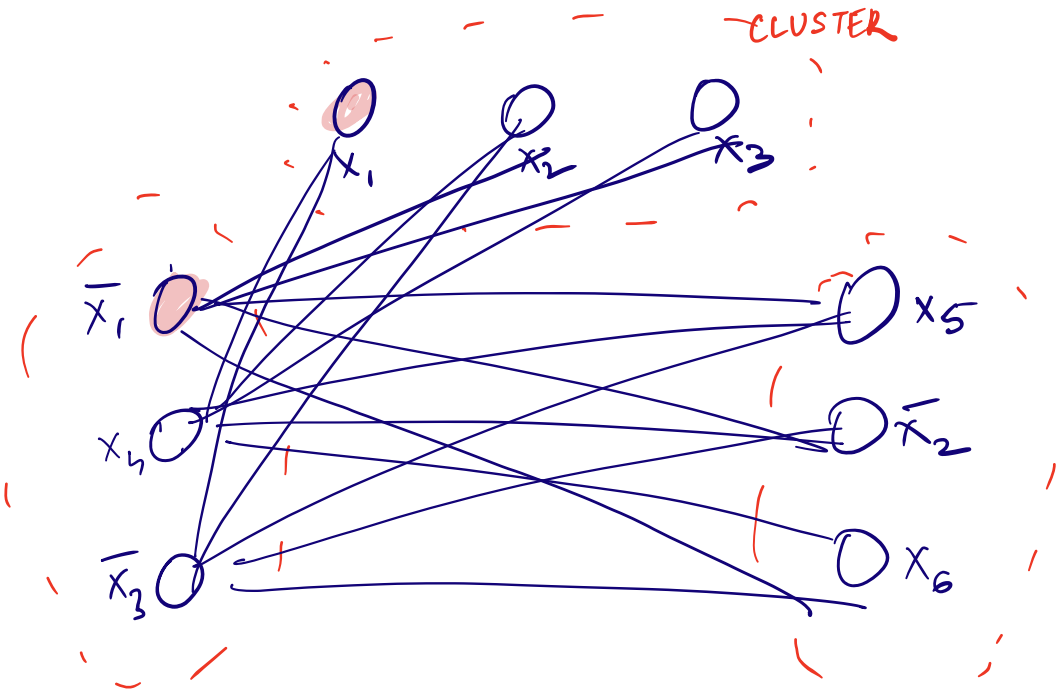
Get an ARBITRARY 3SAT instance.

$f = (x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_4 \vee \bar{x}_3) \wedge (x_5 \vee \bar{x}_2 \vee x_6)$

$\wedge$ - - - - - k clauses.

Suppose there are k clauses.

Build a graph G, find an integer (k ?) such that $(G, k) \in$ CLIQUE iff $f \in$ 3SAT.



$k = 3$

1) If 2 nodes are connected, both variables can be assigned true at the same time.

2) If 2 literals not from the same clause can be assigned true simultaneously, then they share an edge in the graph.

Suppose G has a clique of size $\geq k$

$\Rightarrow$ this clique must have 1 node from each cluster

$\Rightarrow$ there is 1 variable in every cluster that can be True simultaneously.

$\Rightarrow$ 3-CNF is satisfiable.

Suppose 3-CNF is satisfiable

$\Rightarrow$ $\exists$ at least 1 variable in each clause that can be TRUE/1 simultaneously.

$\Rightarrow$ corresponding vertices in G are all pairwise connected to each other (by circled observ.)

$\Rightarrow$ G has a clique of size $\geq k$.

Reduction is polynomial time.

$3SAT \leq_p$ CLIQUE

$\Rightarrow$ CLIQUE is NP-hard.

NP-hard Problems

3SAT

SAT

CSAT ~ Cook-Levin

CLIQUE

INDSET

VERTEX COVER

(are all NP-Complete)

HAMILTONIAN CYCLE (NP hard).