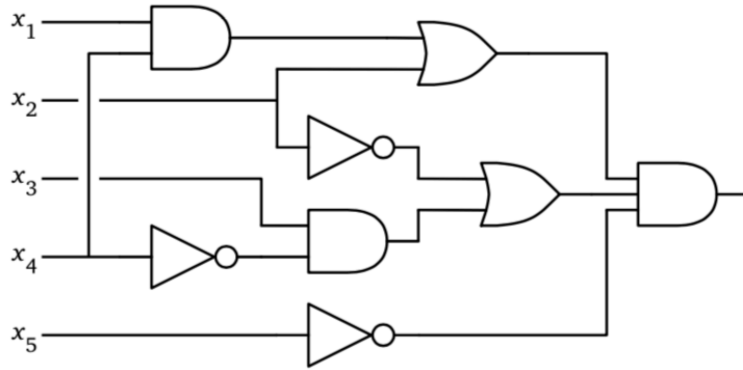


CircuitSAT: Given a boolean circuit is there a set of inputs that make output = 1?



P — Set of languages where membership of  $x \in \Sigma^*$  can be decided in time  $O(|x|^c)$  for some  $c$ .  
 by a TM  
 Problems with poly-time algorithms.

NP — set of languages where membership can be verified in poly time.

Input:  $x + y$   
           string      certificate

If there is a poly-time algo for CircuitSAT then  $P = NP$

1973  
 Levin: perebor  
 Cook:

2000: Clay \$1M

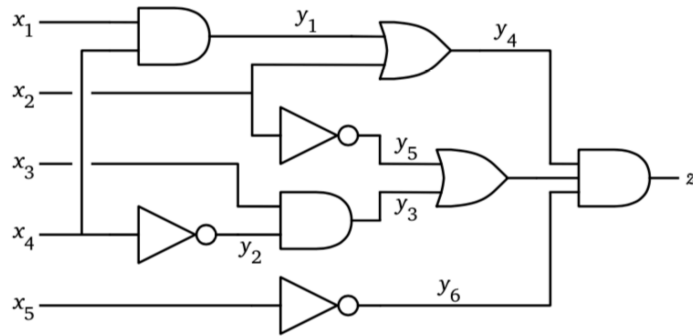
CircuitSAT is NP-hard

LAW OF NATURE: There is no poly time algo  
for CIRCUIT SAT

To prove  $X$  is NP-hard

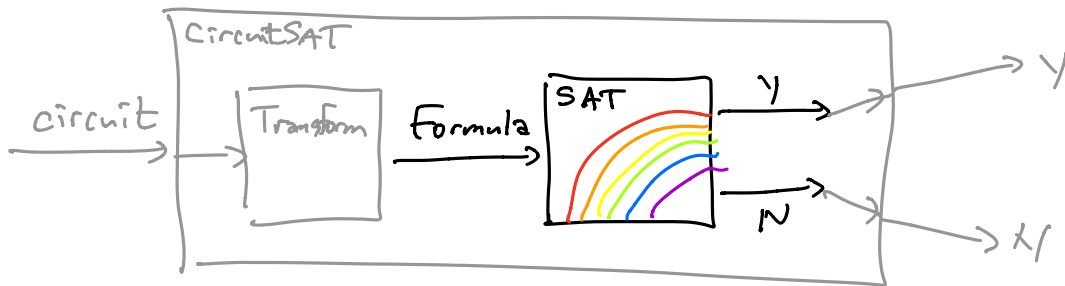
- Be Cook/Levin

- Reduce CIRCUIT SAT  
or 3SAT to  $X$  in poly time



$$(y_1 = x_1 \wedge x_4) \wedge (y_2 = \bar{x}_4) \wedge (y_3 = x_3 \wedge y_2) \wedge (y_4 = y_1 \vee x_2) \wedge$$

$$(y_5 = \bar{x}_2) \wedge (y_6 = \bar{x}_5) \wedge (y_7 = y_3 \vee y_5) \wedge (z = y_4 \wedge y_7 \wedge y_6) \wedge z$$



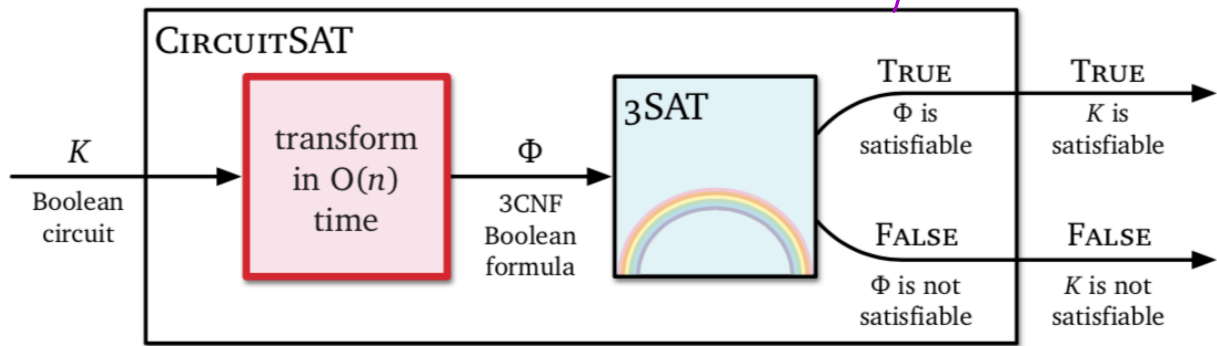
$$(a \vee b \vee c) \wedge (b \vee \bar{c} \vee \bar{d}) \wedge (\bar{a} \vee c \vee d) \wedge (a \vee \bar{b} \vee \bar{d})$$

literals  
↓ ↓ ↓  
Clauses

Conjunctive Normal Form  
 3 literals per clause  
 $\Rightarrow$  3CNF

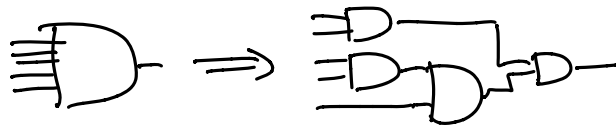
3SAT: Given a 3CNF formula,  
 Is it satisfiable?

# Reduce CIRCUITSAT to 3SAT in poly time.

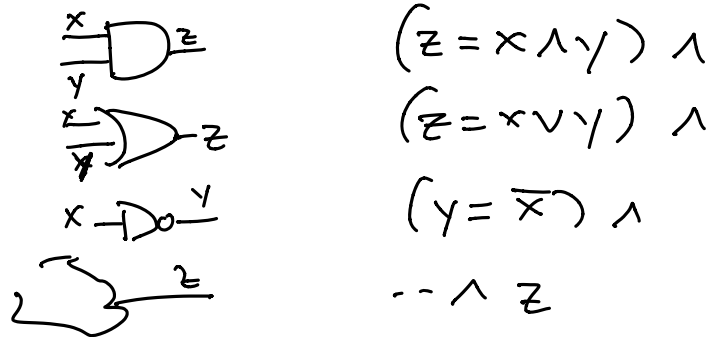


Let  $K$  be an arbitrary boolean circuit.

① Make every AND + OR gate binary



② Write circuit as a formula



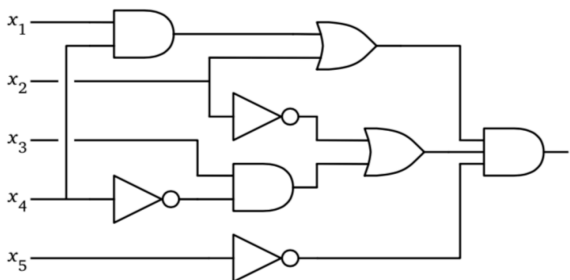
③  $\rightarrow$  CNF

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

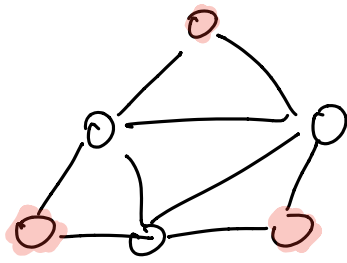
④  $\rightarrow$  3CNF

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

$$z \rightarrow (z \vee x \vee y) \wedge (z \vee \bar{x} \vee y) \wedge (z \vee x \vee \bar{y}) \wedge (z \vee \bar{x} \vee \bar{y})$$



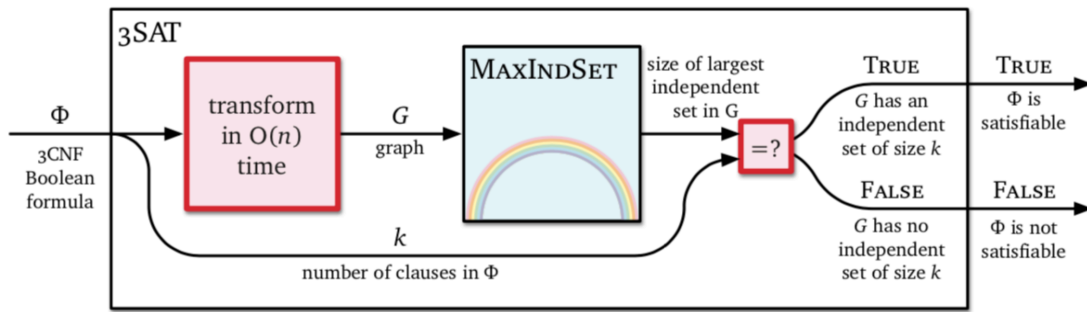
$$(y_1 \vee \bar{x}_1 \vee \bar{x}_4) \wedge (\bar{y}_1 \vee x_1 \vee z_1) \wedge (\bar{y}_1 \vee x_1 \vee \bar{z}_1) \wedge (\bar{y}_1 \vee x_4 \vee z_2) \wedge (\bar{y}_1 \vee x_4 \vee \bar{z}_2) \wedge (y_2 \vee x_4 \vee z_3) \wedge (y_2 \vee x_4 \vee \bar{z}_3) \wedge (\bar{y}_2 \vee \bar{x}_4 \vee z_4) \wedge (\bar{y}_2 \vee \bar{x}_4 \vee \bar{z}_4) \wedge (y_3 \vee \bar{x}_3 \vee \bar{y}_2) \wedge (\bar{y}_3 \vee x_3 \vee z_5) \wedge (\bar{y}_3 \vee x_3 \vee \bar{z}_5) \wedge (\bar{y}_3 \vee y_2 \vee z_6) \wedge (\bar{y}_3 \vee y_2 \vee \bar{z}_6) \wedge (\bar{y}_4 \vee y_1 \vee x_2) \wedge (y_4 \vee \bar{x}_2 \vee z_7) \wedge (y_4 \vee \bar{x}_2 \vee \bar{z}_7) \wedge (y_4 \vee \bar{y}_1 \vee z_8) \wedge (y_4 \vee \bar{y}_1 \vee \bar{z}_8) \wedge (y_5 \vee x_2 \vee z_9) \wedge (y_5 \vee x_2 \vee \bar{z}_9) \wedge (\bar{y}_5 \vee \bar{x}_2 \vee z_{10}) \wedge (\bar{y}_5 \vee \bar{x}_2 \vee \bar{z}_{10}) \wedge (y_6 \vee x_5 \vee z_{11}) \wedge (y_6 \vee x_5 \vee \bar{z}_{11}) \wedge (\bar{y}_6 \vee \bar{x}_5 \vee z_{12}) \wedge (\bar{y}_6 \vee \bar{x}_5 \vee \bar{z}_{12}) \wedge (\bar{y}_7 \vee y_3 \vee y_5) \wedge (y_7 \vee \bar{y}_3 \vee z_{13}) \wedge (y_7 \vee \bar{y}_3 \vee \bar{z}_{13}) \wedge (y_7 \vee \bar{y}_5 \vee z_{14}) \wedge (y_7 \vee \bar{y}_5 \vee \bar{z}_{14}) \wedge (y_8 \vee \bar{y}_4 \vee \bar{y}_7) \wedge (\bar{y}_8 \vee y_4 \vee z_{15}) \wedge (\bar{y}_8 \vee y_4 \vee \bar{z}_{15}) \wedge (\bar{y}_8 \vee y_7 \vee z_{16}) \wedge (\bar{y}_8 \vee y_7 \vee \bar{z}_{16}) \wedge (y_9 \vee \bar{y}_8 \vee \bar{y}_6) \wedge (\bar{y}_9 \vee y_8 \vee z_{17}) \wedge (\bar{y}_9 \vee y_8 \vee \bar{z}_{17}) \wedge (\bar{y}_9 \vee y_6 \vee z_{18}) \wedge (\bar{y}_9 \vee y_6 \vee \bar{z}_{18}) \wedge (\bar{y}_9 \vee y_8 \vee z_{19}) \wedge (\bar{y}_9 \vee y_8 \vee \bar{z}_{19}) \wedge (y_9 \vee \bar{z}_{19} \vee z_{20}) \wedge (y_9 \vee \bar{z}_{19} \vee \bar{z}_{20}) \wedge (y_9 \vee z_{19} \vee z_{20}) \wedge (y_9 \vee z_{19} \vee \bar{z}_{20})$$



# Max Ind Set

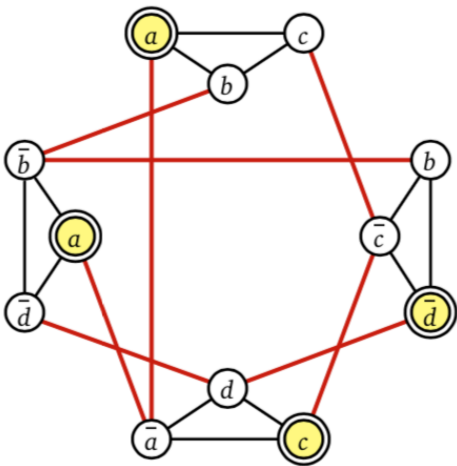
Given graph  $G$   
Find # vertices in  
largest indep set

Prove NP-hard by reducing from 3SAT



Given arbitrary 3CNF formula  $\Phi$ :

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



Build a graph  $G=(V,E)$ :

- $V$  - 3 per clause, 1 per literal.
- $E$  - two types  
clause - connect literals in same clause

consistency - connect opposite literals in diff clauses

