P — solvable in polynomial time

NP — YES instances can be confirmed in polytime

A problem X is NP-hard

Formally: If X can be solved in poly time then P=NP

Practical: X cannot be solved in poly time

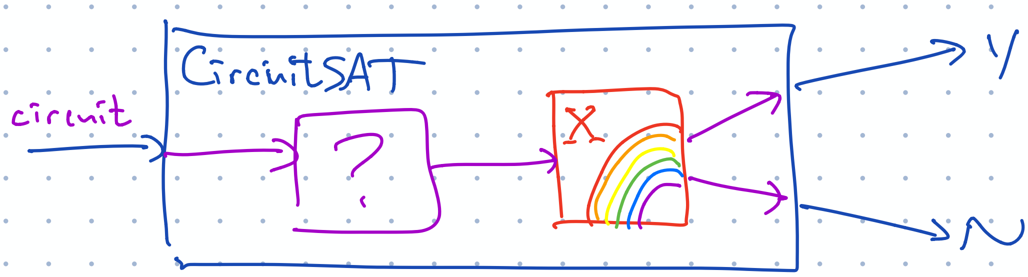
Cook-Levin: CIRCUITSAT is NP-hard

To prove X is NP-hard

Reduce a known NP-hard problem to X in poly time

CircuitSAT
SAT
3SAT

MaxIndSet




literals

3SAT input: $(a \vee b \vee c) \wedge (\bar{a} \wedge \bar{b} \wedge d) \wedge (b \vee \bar{c} \vee \bar{e}) \wedge \cdots$

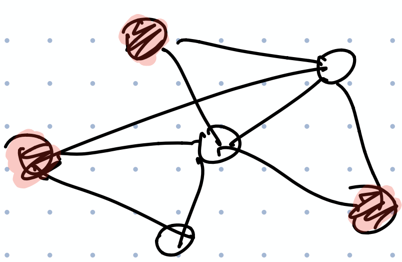
clause

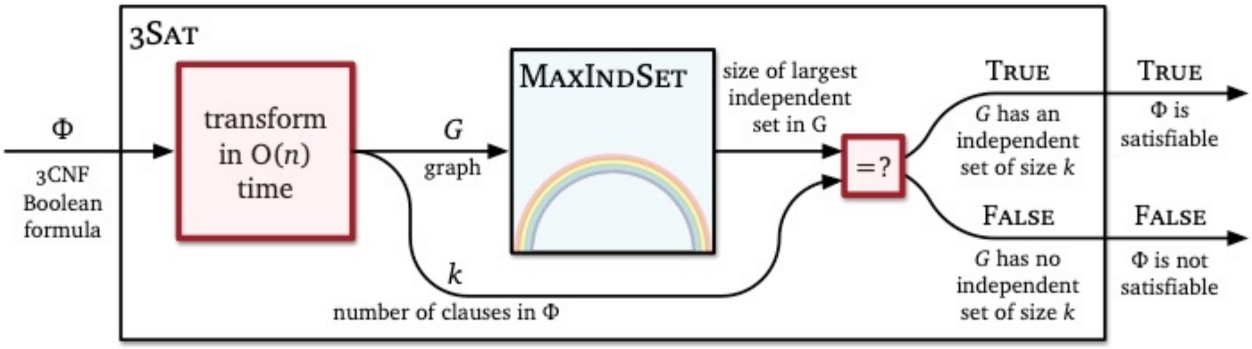
---

Max Independent Set

Input: Graph $G=(V,E)$

Question: Size of largest ind set of vertices?






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

MaxIndSet ≤ k

V = literals

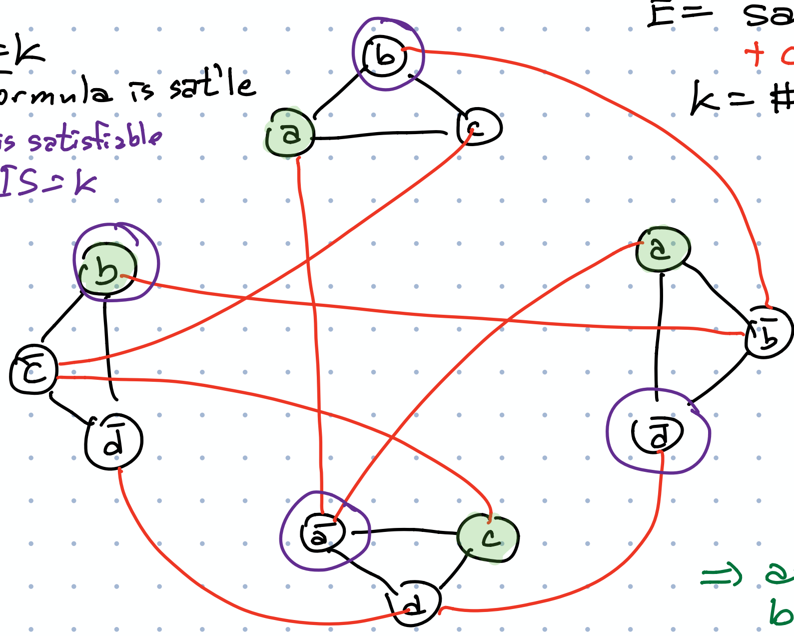
E = same clause + contradictions

k = #clauses

If MIS = k then formula is sat'le

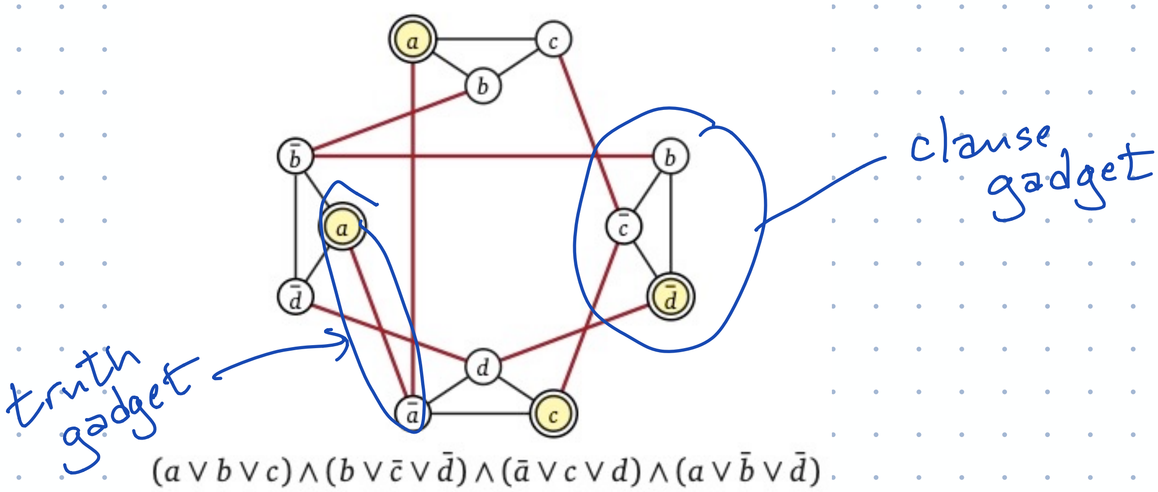
If formula is satisfiable then MIS = k

poly time ✓



a = F
b = T
c = F
d = F

⇒ a = T
b = T
c = T
d = whatever

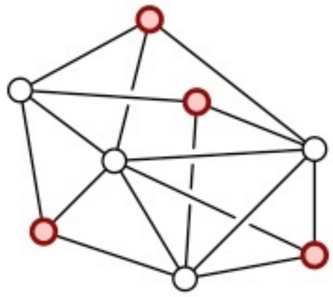



$(a \vee b \vee c) \wedge (b \vee \bar{c} \vee \bar{d}) \wedge (\bar{a} \vee c \vee d) \wedge (a \vee \bar{b} \vee \bar{d})$

## NP-hardness proof: Reduce Z to X:

1. Describe a polytime algo that transforms arbitrary input to Z into a special input to X
2. Prove: if input to Z is good then input to X is also good
3. Prove: if input to X is good then input to Z is also good.

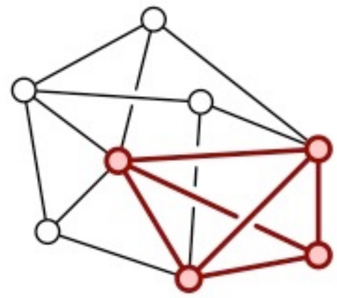
NP-hard



Max Ind Set

no pair of marked verts has an edge

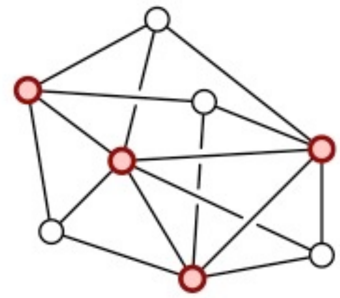
NP-hard



Max Clique

every pair of marked verts has an edge

NP-hard



Min Vertex Cover

Every edge has ≥ 1 marked end

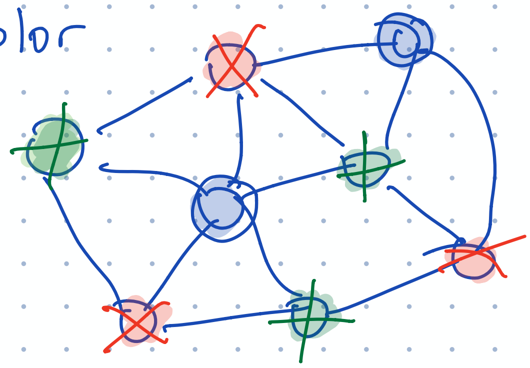
Given $G=(V,E)$

Build new graph $G'=(V,E')$

$$E' = \{uv \mid uv \notin E\}$$

---

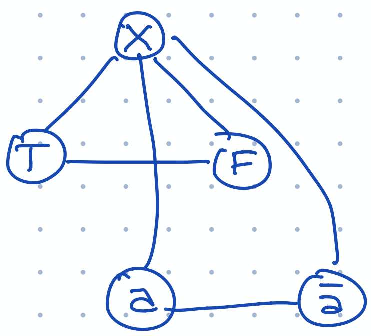
3-Color



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

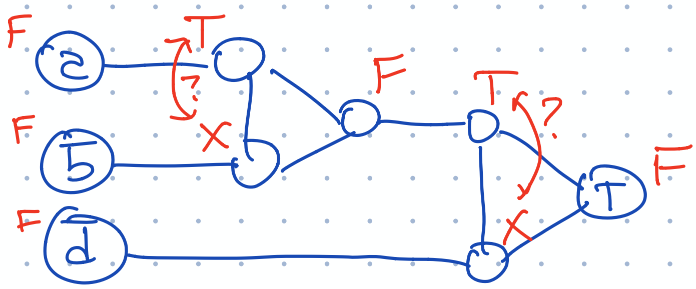
Reduction from 3SAT

(1) Truth gadget

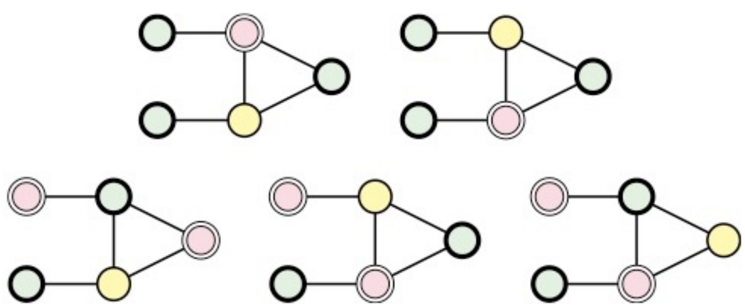


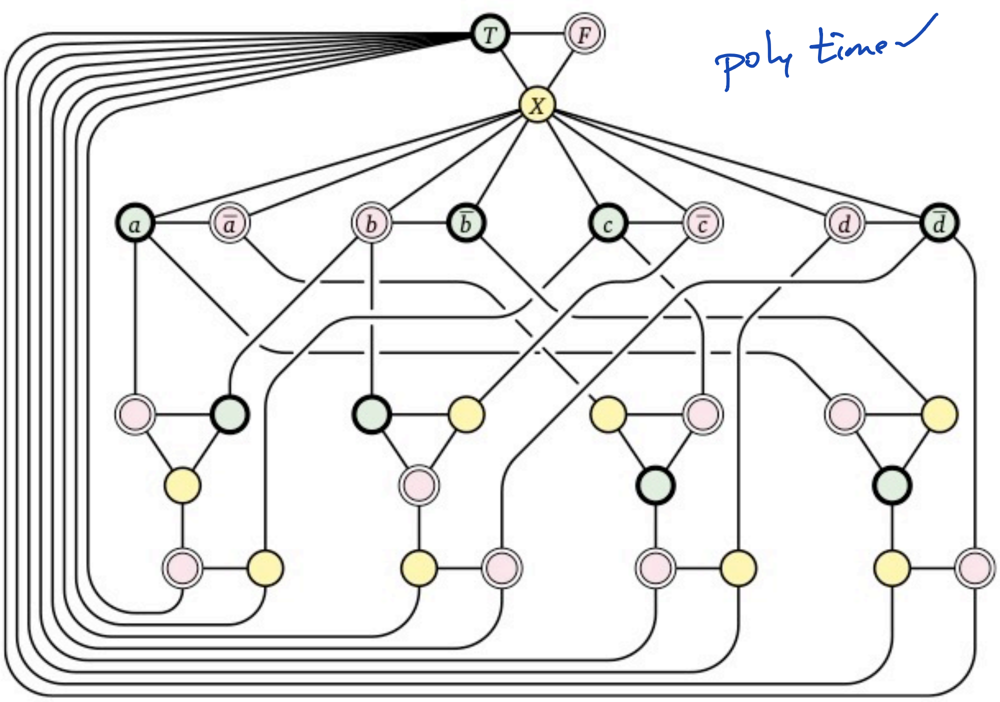

(2) Variable gadget

## ③ Clause gadget $(a \vee \bar{b} \vee \bar{d})$




≥ One of these must be T






poly time ✓

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