P — Solvable in polynomial time

NP — Checkable in polynomial time

X is NP-hard — If poly time algo for X, then P=NP

↗ Heresy!

Cook-Levin Theorem: CircuitSAT is NP-hard!

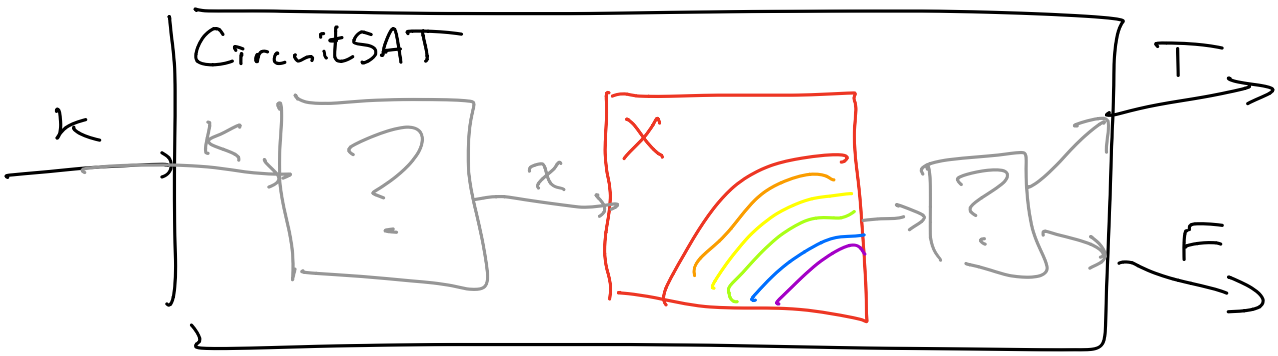
To prove X is NP-hard

Reduce CircuitSAT to X in poly time.

or 3SAT

or MaxIndSet/MaxClique/MinVertexCover

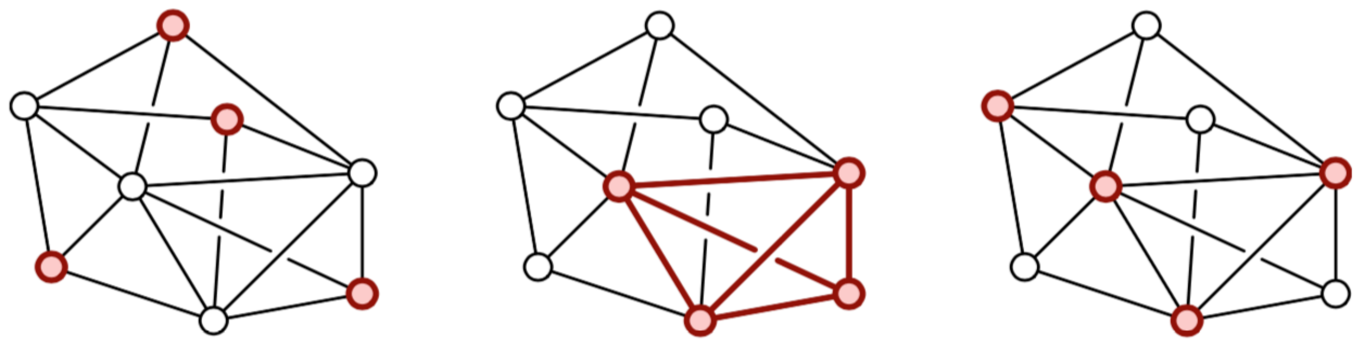
or 3Color/4Color/MinColor/.....



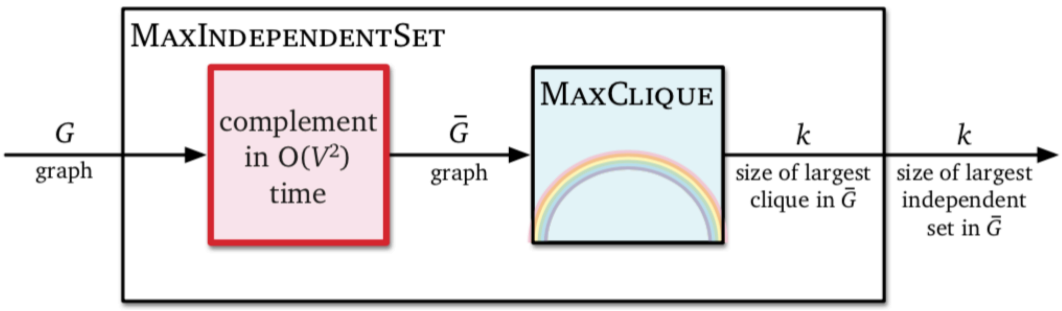
Transform arb. input K to CIRCUITSAT

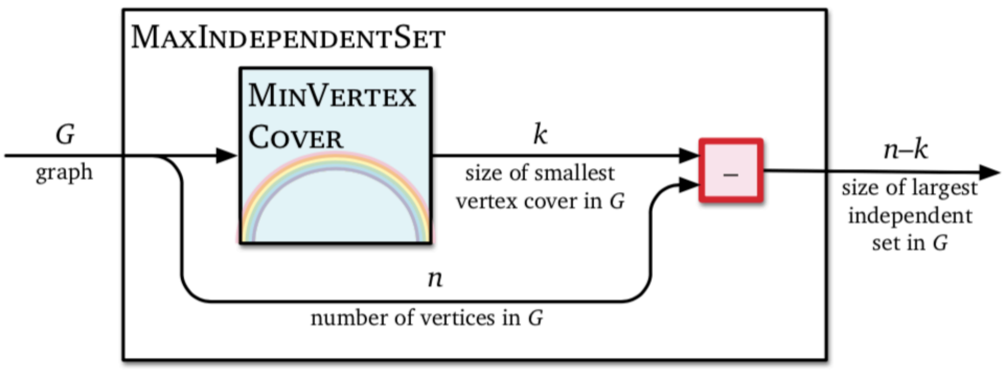
into an input x for X

- TRUE outputs are correct
- FALSE outputs are correct

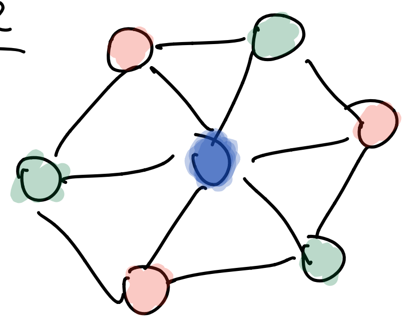


Max Independent Set MaxClique Min Vertex Cover
NP-hard



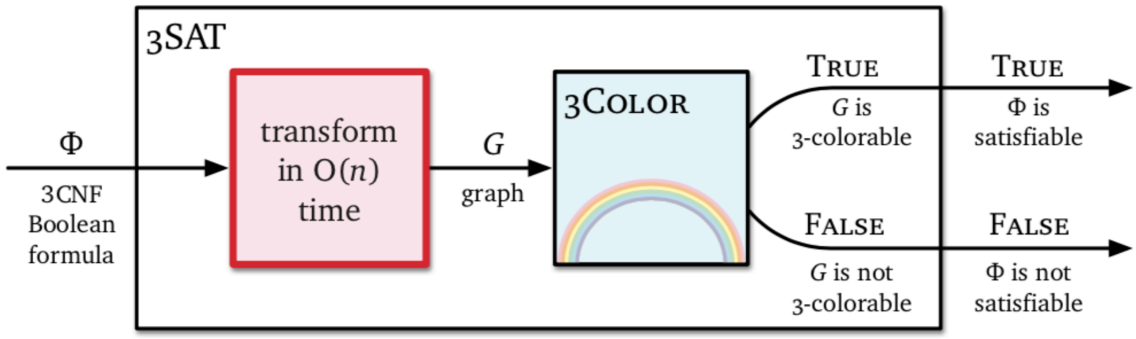


3Color

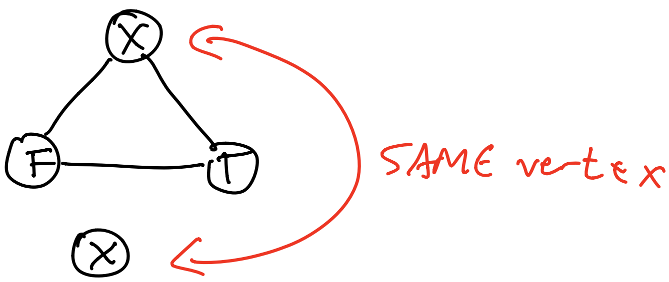


Input: G=(V,E)

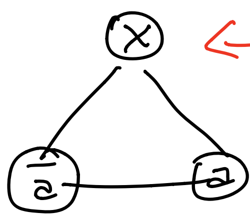
Can we color vertices red, green, blue so that every edge touches two colors?



Truth gadget:



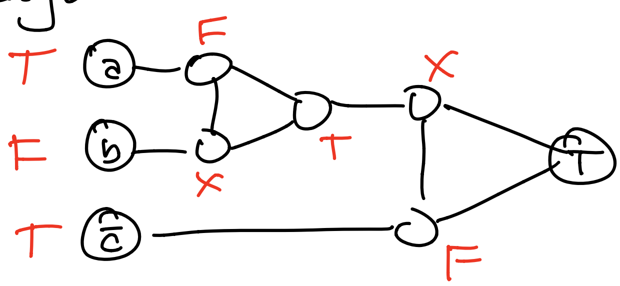
Variable gadget:

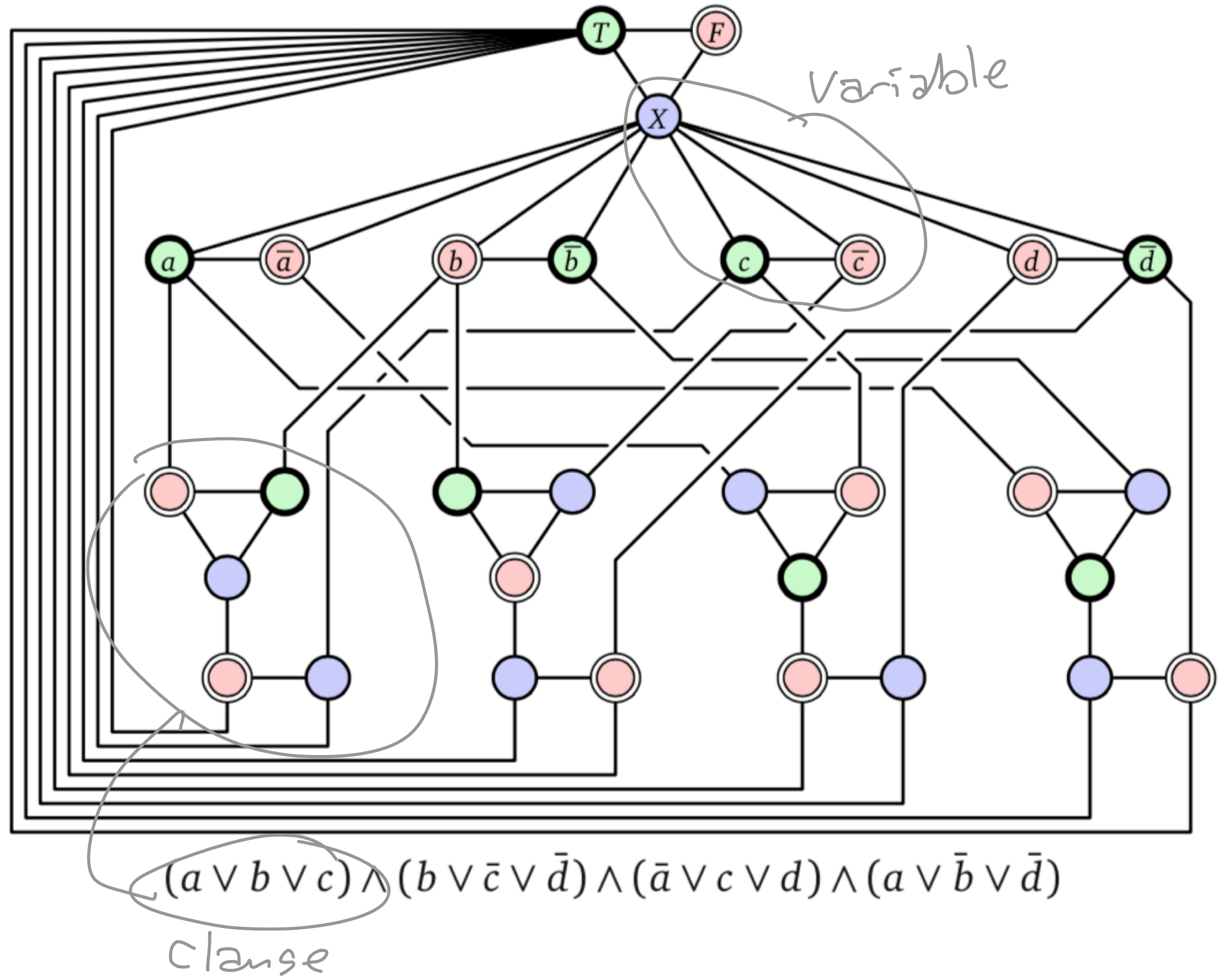


for each variable a

Clause gadget:

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

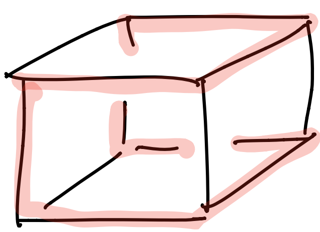




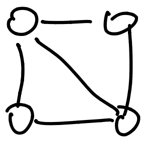
Hamiltonian Cycle

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

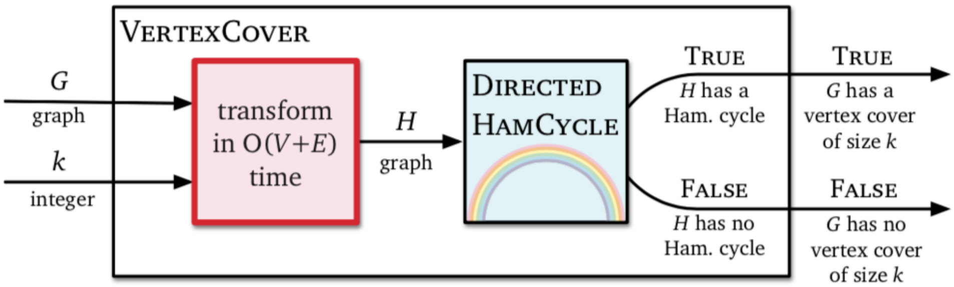
Is there a simple cycle in G through every vertex



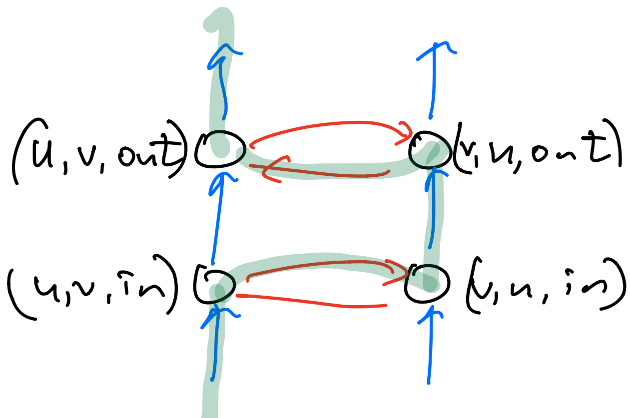
Reduce From Vertex Cover

G = 

k=2

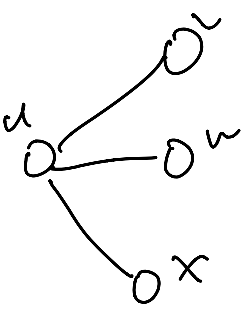


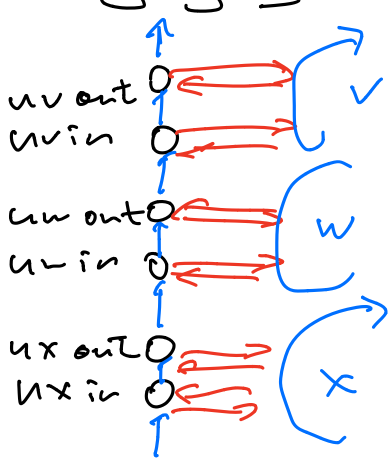
Edge gadgets



Vertex Gadgets

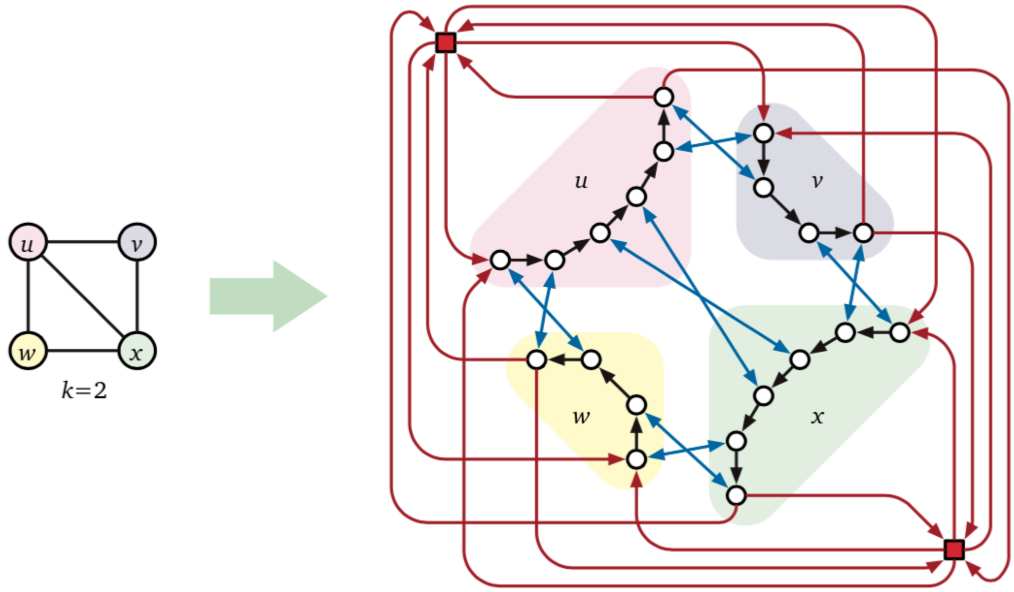
connect all incident edge gadget

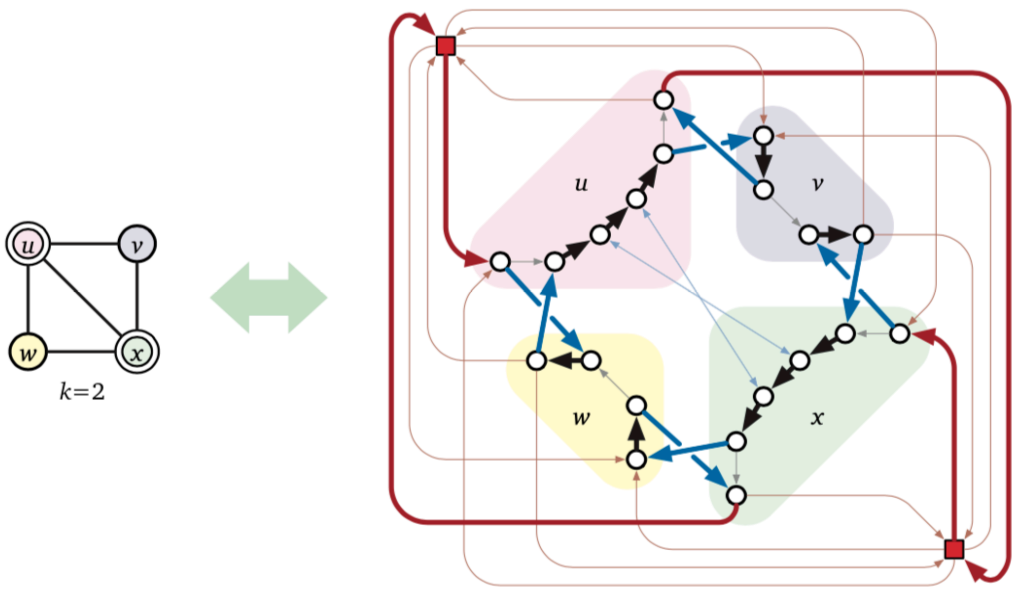




Cover gadget

k vertices connected to vertex chains


u
v
w
x
k=2
u
v
w
x


u
v
w
x
k=2
u
v
w
x