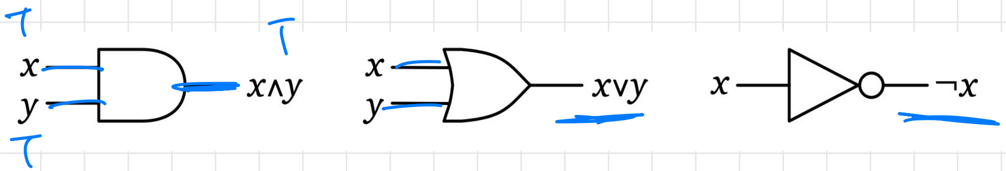
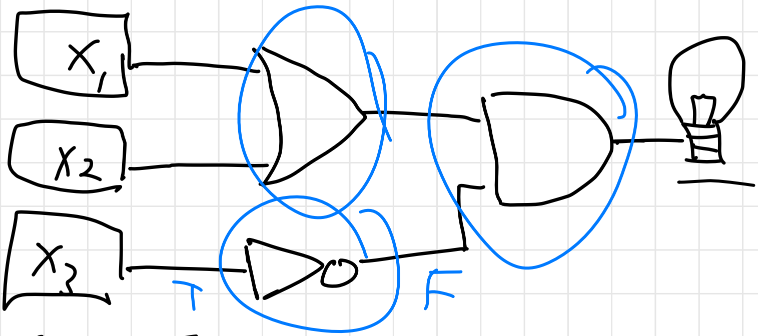
Today: define P vs. NP + NP-hardness



Boolean circuit



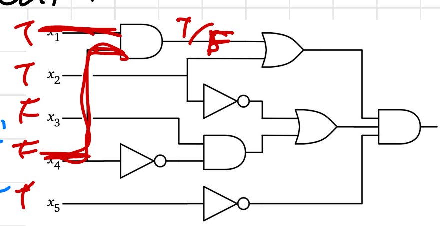
$x_1 = T$
$x_2 = T$ evaluate to T?
$x_3 = T$

is there a satisfying assignment yes

x_1	T
x_2	F
x_3	F

CIRCUITSAT: given a Boolean circuit, is there a satisfying assignment?

solving vs. verifying ⟶ certificate: information needed to prove answer is correct



A problem is in NP if a yes answer can be verified in polynomial time.

CIRCUITSAT $\in$ NP ?

(1) what is the certificate?

(2) what is the poly time alg. to verify?

which of the following is in NP? Why?

- EVEN: given integer m, is it even?

$\in$ NP. certificate is integer n. verification alg: compute $2n = m$

- KVERTEXCOVER: given an undirected graph G and an integer K, does it have a VC of size K?

certificate: proposed vc, $S \subseteq V$

alg for verifying: $|V| = K$

check that S is a VC

check that every edge has an endpoint in S

- MINVERTEXCOVER: given an undirected graph G and an set $S \subseteq V$, is S the min. VC?

$\notin$ NP.

what if I want to verify a no instance?

Co-NP: set of all problems we can verify no instances for in poly time.

P = all problems solvable in poly time.

If a problem $X \in P$, $X \in NP$?

kVC, EVEN

yes, trivially - X can be the certificate because I can just solve X

If a problem $X \in NP$, is $X \in P$? *

seems like no...

to prove no, give a prob in NP but show not in P

$P = NP$ if * true

$P \neq NP$ if * not true

Defs

Problem X is NP-hard iff a poly time alg for X implies that $P = NP$.

Cook-Levin theorem:

If CIRCUITSAT $\in P$, then $P = NP$.

by def, CIRCUITSAT is NP-hard.

SAT: given a Boolean formula, is it satisfiable?

eg $(a \vee b \vee \bar{c}) \wedge (a \Rightarrow b) \vee \overline{(a = b \vee c)}$

negation   if-then

To prove SAT is NP-hard:

Reduce CIRCUITSAT to SAT in poly time

To prove any problem NP-hard, reduce known NP-hard problem to new prob. in poly time

3SAT: given a Boolean formula in conjunctive normal form w/ 3 literals per clause, is it satisfiable?

eg $\overbrace{(a \vee b \vee c)}^{\text{clause}} \wedge (b \vee b \vee c) \wedge (\bar{c} \vee \bar{b} \vee d)$

literal   literal

book: CIRCUITSAT reduces to 3SAT in poly time

so 3SAT is NP-hard

Theorem: MAXINDSET is NP-hard.

pf: by reduction from 3SAT.

SOLVE3SAT(3CNF Formula Φ w/ k clauses)

$\vdots$

MAX IND SET

$\vdots$

return T

return F

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