TODAY

NP - hardness

circuit - SAT (Cook - Levin)

Reductions

SAT, 3SAT, MIS

Recall

A decision problem is a function $f : D \to \{T/F\}$

A DP is equivalent to a language

$L \subset \Sigma^*$ $\quad L = \{ x \in D \mid f(x) = T \}$

A language L is in P if there is an algorithm that recognizes L in time $O(n^c)$ for some c

(so RL, CFL are all in P)

A certifier for a language L is an algorithm $C(x, w)$ that returns T/F such that

if $x \in L$ then $\exists$ some w with $C(x, w) = T$

if $x \notin L$ then for all w $C(x, w) = F$

An efficient certifier runs in time $O(|x|^c)$ for some c

A language is in NP if it has an efficient certifier

A language L is NP-hard if $L \in P \Rightarrow P = NP$

$L_{\text{Composite}} = \{ x \mid x \text{ is a composite number} \}$

$C_{\text{composite}}(x, w)$

return true if $w < x$ and $\gcd(x, w) > 1$

$L_{\text{composite}} \in NP$, $L_{MIS} \in NP$, $L_{SP} \in NP$

$L_{\text{Subsum}} \in NP$

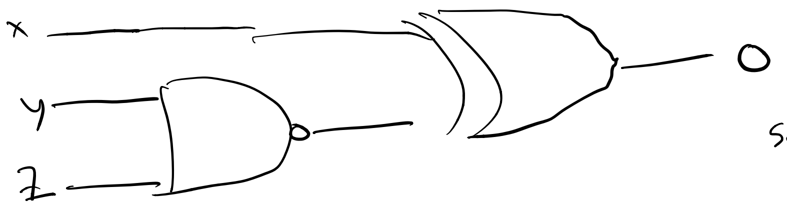
$P \subseteq NP$ if $L \in P$

then certifier (x, w)
return true if $x \in L$

$P \stackrel{?}{=} NP$

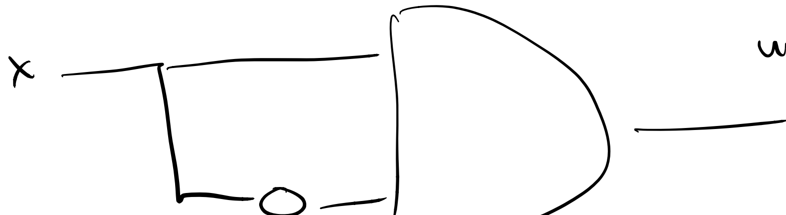
"If 374 final is on a Saturday everyone will get an A"

<u>Circuit-SAT</u> Given a circuit that uses AND, OR, and NOT gates



satisfiable

is there a setting of inputs s.t. output is <u>1</u>



unsatisfiable

<u>Theorem</u> Cook-Levin Theorem CIRCUIT-SAT is NP-hard

i.e., if Circ-SAT $\in P$ then $P = NP$

"Proof" take $x \stackrel{?}{\in} L$ and $C(\cdot,\cdot)$ for L

build Circuit simulates $C(x,\cdot)$ on input w

<u>E.g.</u> $C_{composite}(\cdot,\cdot)$

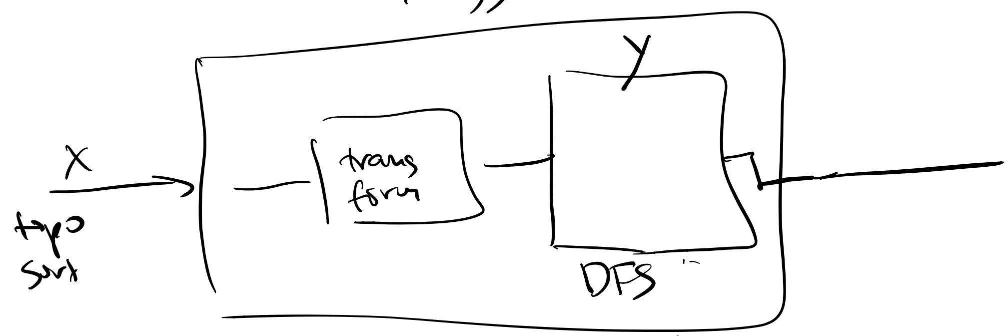
Given x, $C_{GCD(x)}$ w and outputs 1 if $GCD(x,w) > 1$

Reductions we reduce X to Y

alg (x)

create $y = f(x)$

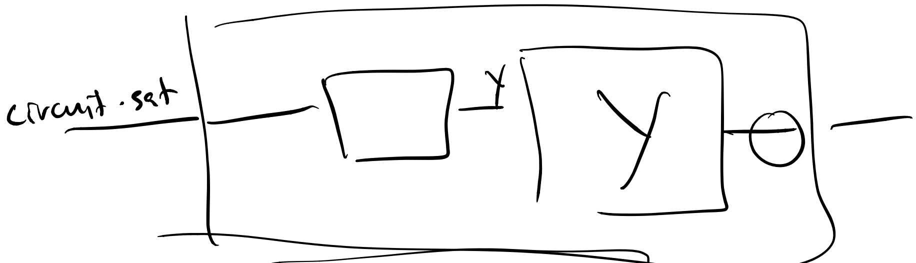
call Y (y)



Poly-time reduction → red runs in poly time in the input

A poly-time reduction of X to $Y \in P$ means that $X \in P$

If X is NP-hard and X has poly-time reduction to Y then Y is NP-hard



If $Y \in P$ $\boxed{\Rightarrow X \in P \Rightarrow}$ $P = NP$

Circuit-sat to 3SAT

3SAT → input a formula in 3-CNF

(Conjunctive Normal Form)

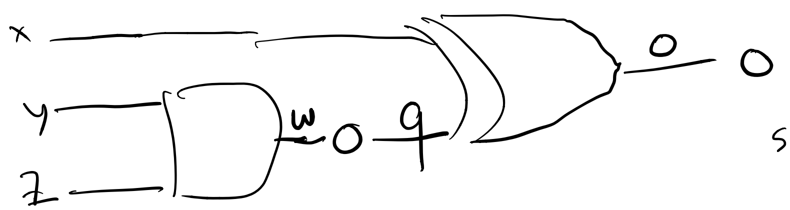
$$(x \vee y \vee z) \wedge (\overline{x} \vee \overline{y} \vee w) \wedge (x \vee \overline{z} \vee \overline{w})$$

output is the formula satisfiable

$x = T$ $y = F$, $w = T$, $z = F$

Claim 3-CNF is NP-hard

Proof reduce Circuit-SAT to 3-CNF



1 add variable for each wire

2. add clauses for each gate

AND gate $w = y \wedge z$

$$(w \wedge \overline{y} \wedge \overline{z}) \wedge (\overline{y} \vee z) \wedge (y \vee \overline{z})$$

OR gate $o = q \vee x$

$$(\overline{o} \vee q \vee x) \wedge (o \vee \overline{x}) \wedge (o \vee \overline{q})$$

NOT gate $q = \neg w$

$$(q \vee w) \wedge (\overline{q} \vee \overline{w})$$

3. add output clause (o)

Φ_1 is a CNF formula.

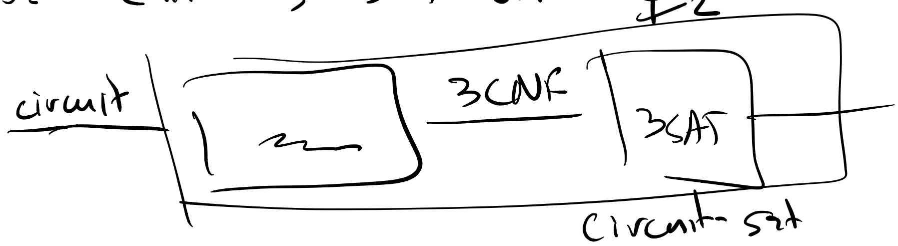
$$o \wedge (q \vee w) \wedge (\overline{q} \wedge \overline{w}) \wedge (w \wedge \overline{y} \wedge \overline{z}) \wedge \dots$$

4. transform Φ_1 into 3CNF Φ_2

$$(q \vee w) \rightarrow (q \vee w \vee x_1) \wedge (q \vee w \vee \bar{x}_1)$$

$$(o) \rightarrow (o \vee x_1 \vee x_2) \wedge (o \vee x_1 \vee \bar{x}_2) \wedge (o \vee \bar{x}_1 \vee x_2) \wedge (o \vee \bar{x}_1 \vee \bar{x}_2)$$

5. call 3-SAT on Φ_2



MIS is NP-hard

3-CNF formula

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

3-CNF $\rightarrow$ MIS