HW 9 out later today
due next Tue

HW 10 out next week
due after break

HW 11 out after break
prob. not graded

① Simple computers (DFAs)
   What they can and can't do

② Algorithms - What general
   purpose computers can do

③ What computers can't
do (well)
CIRCUIT SAT

$P$ - polynomial time  \( O(n^{173}) \)

$NP$ - nondeterministic poly time

For any instance where answer is YES, there is a proof verifiable in poly time.

Glass box

Can we set inputs so that output = T?

Only algo known: BRUTE FORCE \( \Theta(2^n) \)
To prove that \( X \) is NP-hard:
Prove that if \( X \) can be solved in poly time, then so can CIRCUIT SAT.

"Reduce CIRCUIT SAT to \( X \) in poly time"
Solve CIRCUIT SAT in poly time using subroutine for \( X \).

NP-hardness

black box
Only way to see if it works is brute force
$P = NP$?

Let's just assume not.

$NP \subseteq P$

Circuit SAT

$NP$-hard

If this problem can be solved in poly time, $P = NP$.

Cook-Levin:

Circuit SAT is NP-hard.
Let's just assume not Circuit SAT \( \Phi \) 3SAT

Yes

No
To prove that \( X \) is NP-hard:

Prove that if \( X \) can be solved in poly time, then so can \( \text{CIRCUIT SAT} \).

"Reduce \( \text{CIRCUIT SAT} \) to \( X \) in poly time."

Solve \( \text{CIRCUIT SAT} \) in poly time using subroutine for \( X \).

\[
(\text{Formula SAT}) \quad (a \wedge (b \Rightarrow c)) \vee (\overline{5} \Rightarrow (\overline{c} \wedge \overline{d}) \wedge b))
\]

Can we assign values to \( \text{vars} \) to make given formula \( T \)?
BSAT — Conjunctive Normal Form with 3 literals per clause

\[(\overline{a} \lor b \lor c) \land (\overline{b} \lor \overline{c} \lor d) \land (\overline{c} \lor \overline{v} \lor c \land d) \land (\overline{c} \lor \overline{v} \lor d)\]

Clause

Given an arbitrary circuit \( K \)

1. \( \overline{a} \lor b \lor c \Rightarrow \overline{D} \lor D \)

2. Transcribe the circuit

   \[(c=ab) \land (c=ab) \land (b=\overline{a}) \Rightarrow \]

3. Convert to 3CNF

   \[(c=ab) \Rightarrow (c \lor \overline{a} \lor b) \land (c \lor \overline{v} \lor a \lor x) \land (\overline{c} \lor \overline{v} \lor a \lor x) \land (\overline{c} \lor v \lor b \lor x) \land (\overline{c} \lor v \lor a \lor x)\]