NP-hardness and Cook-Levin theorem

Friday, May 2, 2025 11:33 AM

Administrivia.

- HW4 due May 9 (next Friday)

Last time in complexity land: P = NP ?

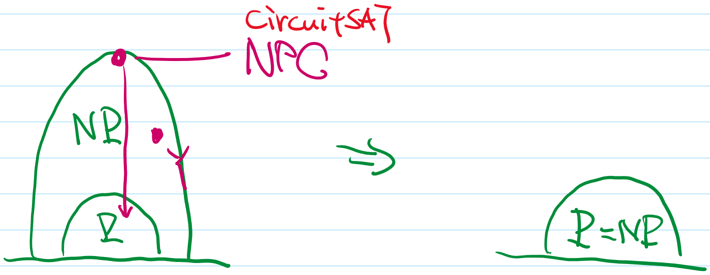
- An unnatural next Q:
  Could it be that there's a hardest problem in NP ?

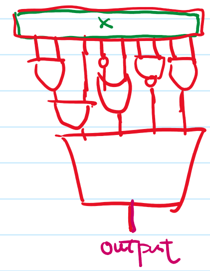
NP-hard: If you can solve problem X ~~fast~~ in poly time,
then you can solve all problems in NP fast
(i.e. NP = P).

NP-complete: NP-hard + in NP.

CircuitSAT

NP-complete : NP-hard + in NP.





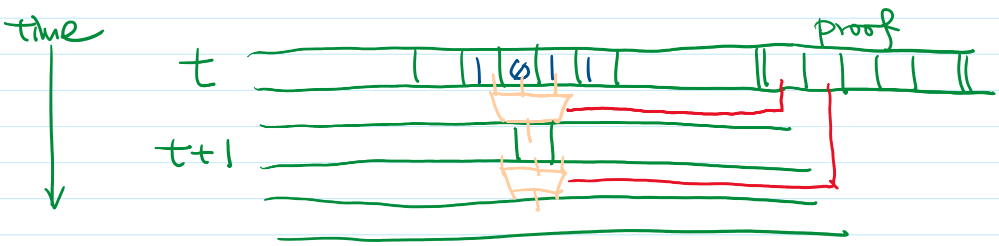
CircuitSat

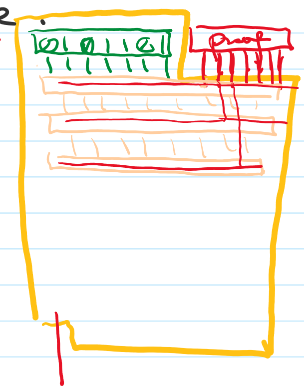
input: A circuit consists of AND, OR, NOT gates,
some input wires, one output wire

output: Is there an input to the circuit such that
the output wire is 1?

NP-hard + NP.

Cook-Levin Thm. CircuitSat is NP-complete



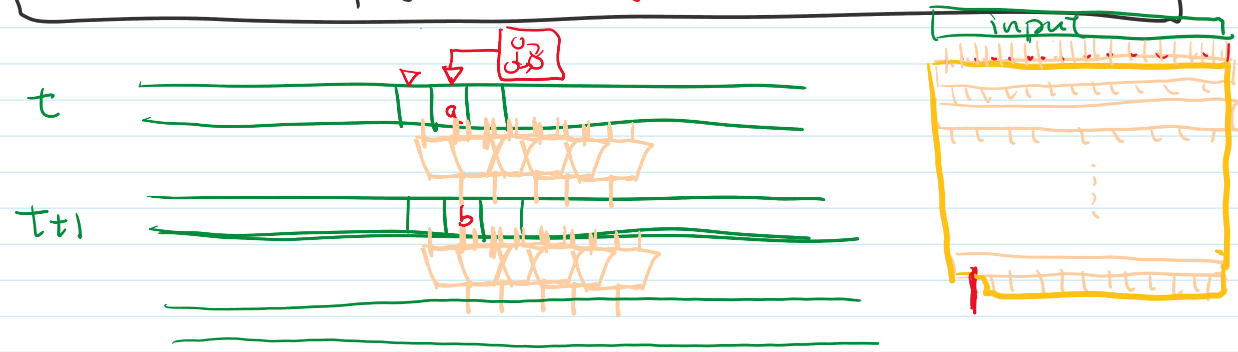


Circuit Value

input: A circuit consists of AND, OR, NOT gates,
some input wires, one output wire, input bits

output: ~~Is there an input to the circuit such that~~
Is the output wire ~~is~~ 1?

is the output wire ~~x~~ 1?



<u>Thm</u>. CIRCUITVALUE is in P. (actually P-complete)

Another triumph of the simplicity of TM model.

<u>Question</u>. Now what?

- more NPC problems?
- simpler SAT structures?

<u>Reductions</u>. subroutine / library

Problem A <u>reduces</u> to B

if solving B $\underset{\text{poly.}}{\Rightarrow}$ solving A.

$A \le B$

$(A \leftarrow B)$

Q. Is A or B harder?

<u>example</u>. sorting $\gtrless$ searching.

P finding triangle $\le$ finding biggest clique, NP

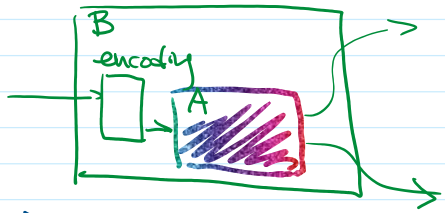
every NP problem $\le$ CIRCUITSAT.

every P problem $\le$ CIRCUITVALUE

To prove Problem A is NP-hard, reduce known NP-hard problem to A

NP-hard

$B \le A$ thus A is NP-hard.



If you solve A fast, you also solve X fast; but by def. of NP-hard, you solve all NP-problems fast
$\Rightarrow$ A is NP-hard as well.

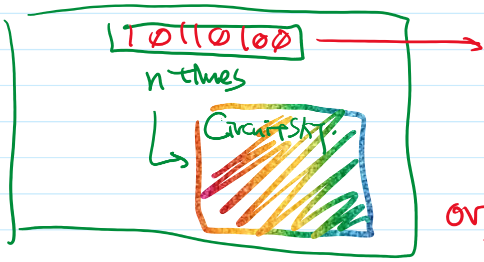
The reduction has to run in poly. time.

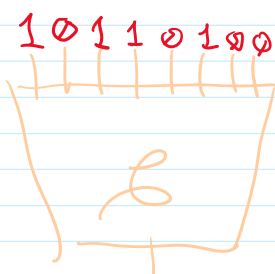
example.

ComputeSAT
input: a circuit C
output: an input satisfying the circuit

NP-hard.

CircuitSAT $\le$ ComputeSAT.





oracle reduction

example

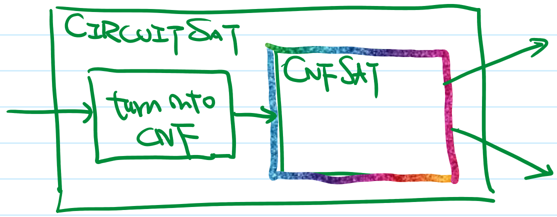
CNFSAT
input: a CNF formula
output: is the formula satisfiable?

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

CIRCUITSAT $\le$ CNFSAT:

turn a circuit into a CNF form.

s.t. yes-inst. / no- $\Rightarrow$ yes-inst. / no-



mapping reduction

Pf. (sketch) apply distr. rule

$$(x_1 \wedge \cdots \wedge x_k) \vee (y_1 \wedge \cdots \wedge y_\ell)$$
$$= (x_1 \vee y_1) \wedge \cdots \wedge (x_k \vee y_\ell)$$

& $$\overline{(x_1 \wedge \cdots \wedge x_k)} = \overline{x_1} \vee \cdots \vee \overline{x_k}$$
$$\overline{(x_1 \vee \cdots \vee x_k)} = \overline{x_1} \wedge \cdots \wedge \overline{x_k}$$

the Boolean fcn. computed does not change $\square$.

example.

3SAT

input: an 3CNF formula

output: is the formula satisfiable?

SAT $\le$ 3SAT:

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

$$(a \vee x_1) \wedge (\bar{x}_1 \vee b \vee x_2) \wedge (\bar{x}_2 \vee c \vee x_3) \wedge (\bar{x}_3 \vee d)$$

Thm. 3SAT is NP-hard