CS 121: Lecture 20
Cook-Levin Theorem

Madhu Sudan

https://madhu.seas.Harvard.edu/courses/Fall2020

Book: https://introtcs.org

How to contact us {
- The whole staff (faster response): CS 121 Piazza
- Only the course heads (slower): cs121.fall2020.course.heads@gmail.com

Announcements:

- Advanced section Thursday: Nicole Immorlica on EconCS
- Midterm 2 in 1 week.
  - Open book (Barak only). 2 pages cheat sheet (no collaboration).
  - 90 minutes long. (70 if handwritten.)
- Homework 5 due Thursday.

Where we are:

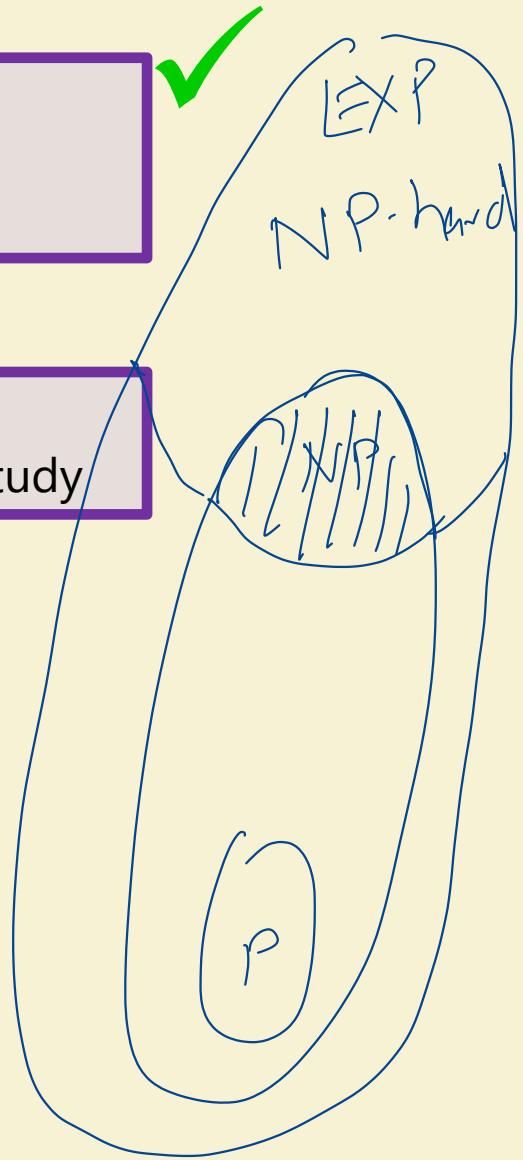
Part I: Circuits:
Finite computation,
quantitative study

Part II: Automata:
Infinite restricted computation,
quantitative study

Part III: Turing Machines:
Infinite computation, qualitative study

Part IV: Efficient Computation:
Infinite computation, quantitative study

Part V: Randomized computation:
Extending studies to non-classical algorithms



Review of last lecture

- Defined NP (solutions/witnesses/proofs polytime verifiable)
  - $F: \{0,1\}^* \to \{0,1\} \in \backslash\mathrm{NP} \Leftrightarrow \exists V_F \text{ polytime comp. } s.t. F(x) = 1 \Leftrightarrow \exists w \; s.t. V_F(x, w) = 1$
- Defined NP-Hard and NP-complete
  - F NP-hard $\Leftrightarrow \forall G \in \mathrm{NP}, G \leq_P F$
  - F NP-complete $\Leftrightarrow F \in \mathrm{NP}$ and F NP-complete.
- Asserted: 3SAT is NP-Complete
  - $3\mathrm{SAT}(C_1 \wedge C_2 \cdots C_m) = 1 \Leftrightarrow \exists x_1, \ldots, x_n \in \{0,1\} \; s.t. \forall j \; \exists$ literal in C_j that is 1.
  - Will prove today
- Proved: ISET is NP-Complete (assuming assertion)

Today

- Cook-Levin Theorem: 3SAT is NP-Complete

NP-Completeness historically

- Many mathematicians sensed NP-hardness:
  - Gauss (1800s): Can you factor integers?
  - Godel (1956): Can you automate proving of theorems?
  - Edmonds (1967): Travelling Salesperson has no polynomial time algorithm?

If [$3SAT$ has $O(n^2)$ time algorithm] then in spite of the undecidability of the Entscheidungsproblem, the mental work of a mathematician concerning Yes-or-No questions could be ***completely replaced by a machine***

Kurt Gödel to John von-Neumann, 1956

Today's Theorem

$3SAT$ is NP-hard.
NP-hard + in NP = NP complete

Cook Levin Theorem: $\forall F \in NP \; F \leq_p 3SAT$

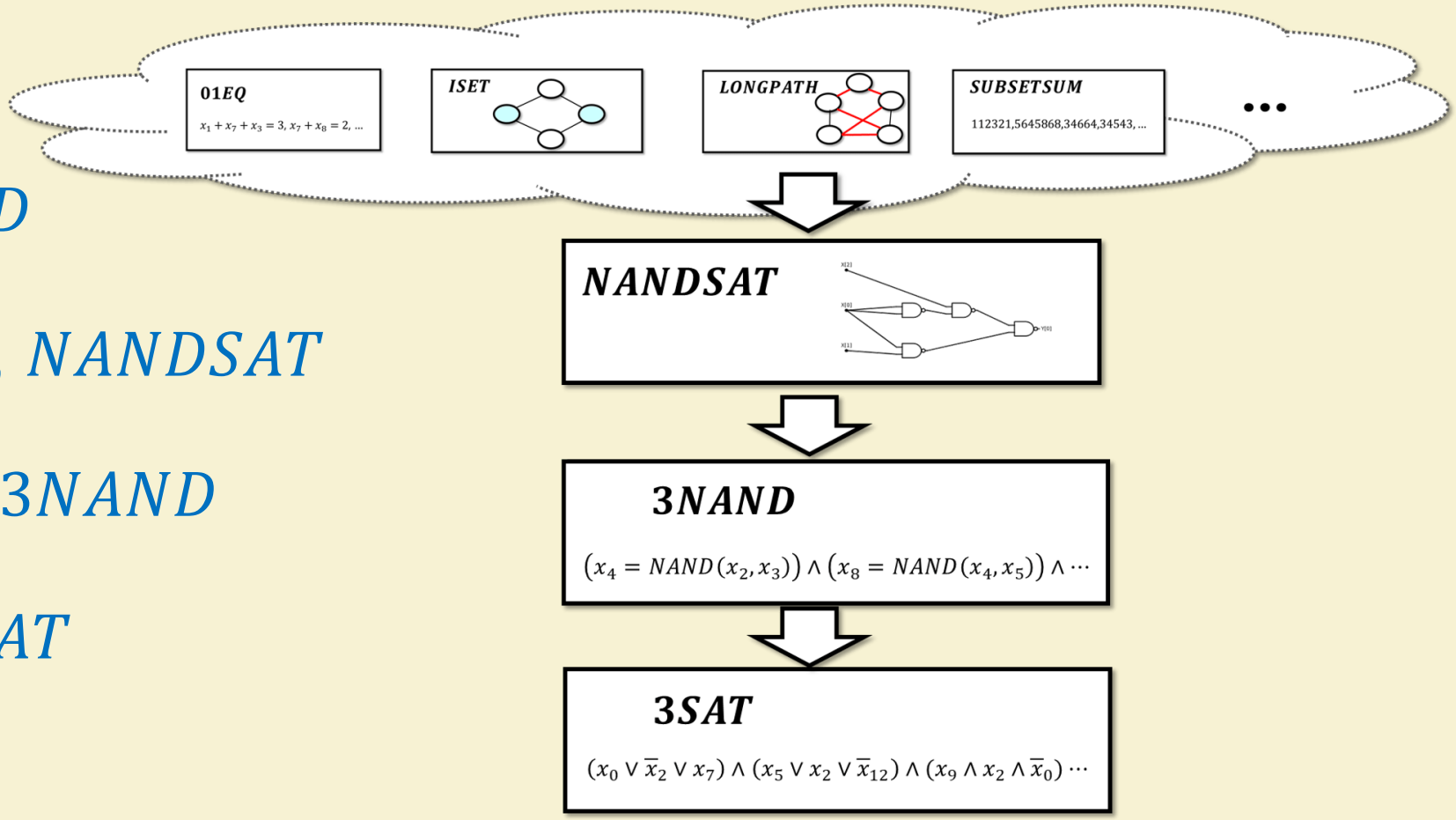
Proof:

Define $NANDSAT, 3NAND$

Lemma 1: $\forall F \in NP, F \leq_p NANDSAT$

Lemma 2: $NANDSAT \leq_p 3NAND$

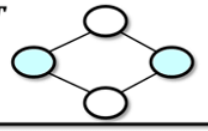
Lemma 3: $3NAND \leq_p 3SAT$



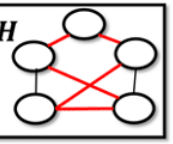
01EQ

$x_1 + x_7 + x_3 = 3,\ x_7 + x_8 = 2,\ \ldots$

ISET



LONGPATH

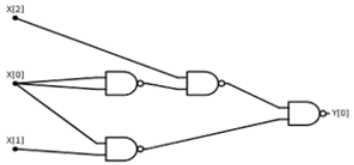


SUBSETSUM

112321,5645868,34664,34543, ...

• • •

NANDSAT



3NAND

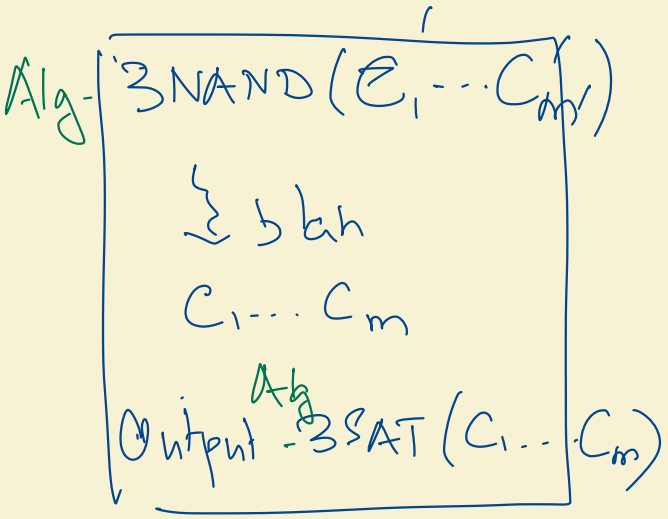
$\left(x_4 = NAND(x_2, x_3)\right) \wedge \left(x_8 = NAND(x_4, x_5)\right) \wedge \cdots$

3SAT

$(x_0 \vee \overline{x}_2 \vee x_7) \wedge (x_5 \vee x_2 \vee \overline{x}_{12}) \wedge (x_9 \wedge x_2 \wedge \overline{x}_0) \cdots$

3NAND

$C_1 \wedge C_2 \wedge C_3 \cdots C_m$



Input: Ψ is AND of constraints of form $z_i = NAND(z_j, z_k)$

Output: 1 iff there is assignment $z \in \{0,1\}^r$ satisfying Ψ

Q: If $\Psi = (z_0 = NAND(z_2, z_3)) \wedge (z_3 = NAND(z_2, z_1)) \wedge (z_1 = NAND(z_2, z_3))$

what is $3\text{NAND}(\Psi)$?

$(\bar{z}_0 \vee \bar{z}_2 \vee \bar{z}_3) \wedge (z_0 \vee z_2) \wedge (z_0 \vee z_3)$

Lemma 2: $NANDSAT \leq_p 3NAND$

In 3SAT

$C_j = (x_1 \vee \bar{x}_2 \vee x_7)$ ⟸

var: $x_1 \cdots x_n$

in 3NAND

$C_j' = (z_i \stackrel{?}{=} NAND(z_j, z_k))$

var: $z_1 \cdots z_{n'}$

Lemma 3: $3NAND \leq_p 3SAT$

Key claim: For every $a, b, c \in \{0,1\}$,

$$c = NAND(a, b) \iff$$

$$(\overline{a} \vee \overline{b} \vee \overline{c}) \wedge (c \vee a) \wedge (c \vee b)$$

if $a=b=1$ then $c=0$

if $a=0$ then $c=1$

if $b=0$ then $c=1$

Q: Prove key claim.

What you should verify

① Reduction runs in poly time

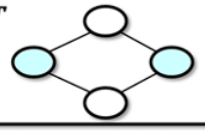
Key claim ⇒ lemma.

② 3NAND expression is SAT $\iff$ 3SAT expression is SAT.

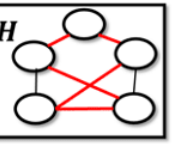
01EQ

$x_1 + x_7 + x_3 = 3,\ x_7 + x_8 = 2,\ \ldots$

ISET



LONGPATH

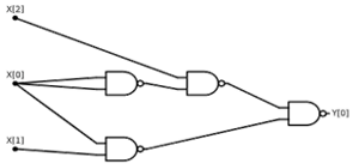


SUBSETSUM

112321,5645868,34664,34543, ...

...

NANDSAT

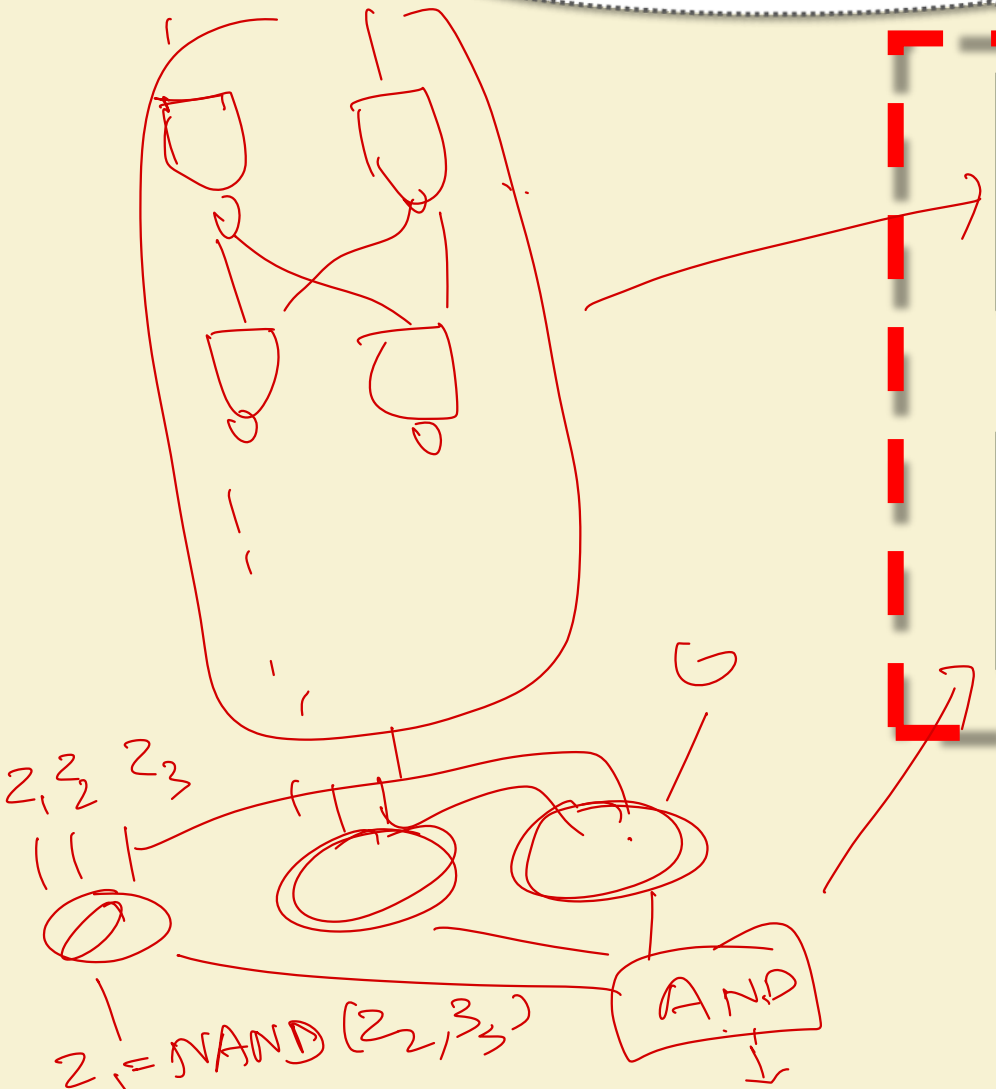


3NAND

$\left(x_4 = NAND(x_2, x_3)\right) \wedge \left(x_8 = NAND(x_4, x_5)\right) \wedge \cdots$

3SAT

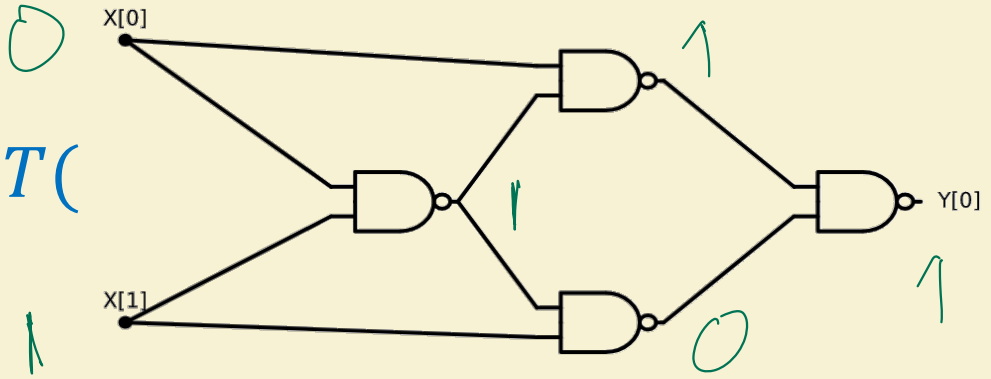
$(x_0 \vee \overline{x}_2 \vee x_7) \wedge (x_5 \vee x_2 \vee \overline{x}_{12}) \wedge (x_9 \wedge x_2 \wedge \overline{x}_0) \cdots$



NANDSAT

Input: NAND-CIRC program P (aka circuit with NAND gates)

Output: 1 iff there is $x \in \{0,1\}^n$ s.t. $P(x) = 1$

Q: What is $NANDSAT($ 

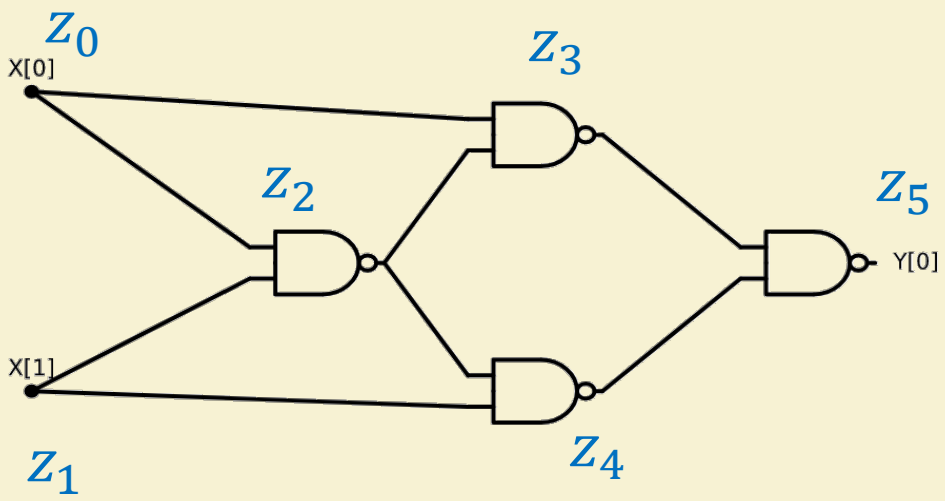
$)$?

Input: Ψ is AND of constraints of form $z_i = NAND(z_j, z_k)$

Output: 1 iff there is assignment $z \in \{0,1\}^r$ satisfying Ψ

Lemma 2: $NANDSAT \leq_p 3NAND$

"Proof by example:"



$(z_2 = NAND(z_0, z_1))$ AND $(z_3 = NAND(z_0, z_2))$ AND

$z_2 = NAND(z_0, z_1)$

$z_3 = NAND(z_0, z_2)$

$z_4 = NAND(z_1, z_2)$

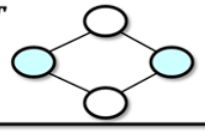
$z_5 = NAND(z_3, z_4)$

$z_5 = 1$ { $z_6 = NAND(z_0, z_0)$; $z_5 = NAND(z_0, z_6)$

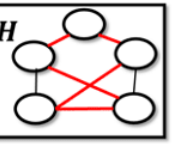
01EQ

$x_1 + x_7 + x_3 = 3,\ x_7 + x_8 = 2,\ \ldots$

ISET



LONGPATH

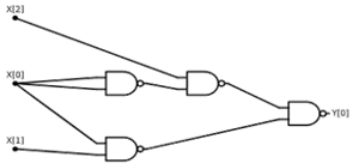


SUBSETSUM

112321,5645868,34664,34543, ...

• • •

NANDSAT



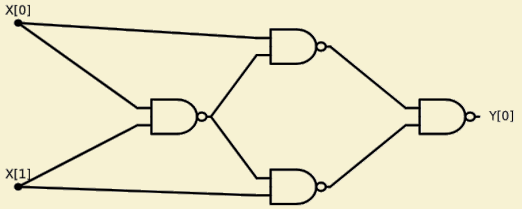
3NAND

$\left(x_4 = NAND(x_2, x_3)\right) \wedge \left(x_8 = NAND(x_4, x_5)\right) \wedge \cdots$

3SAT

$(x_0 \vee \overline{x}_2 \vee x_7) \wedge (x_5 \vee x_2 \vee \overline{x}_{12}) \wedge (x_9 \wedge x_2 \wedge \overline{x}_0) \cdots$

Input: NAND-CIRC program P (aka circuit with NAND gates)



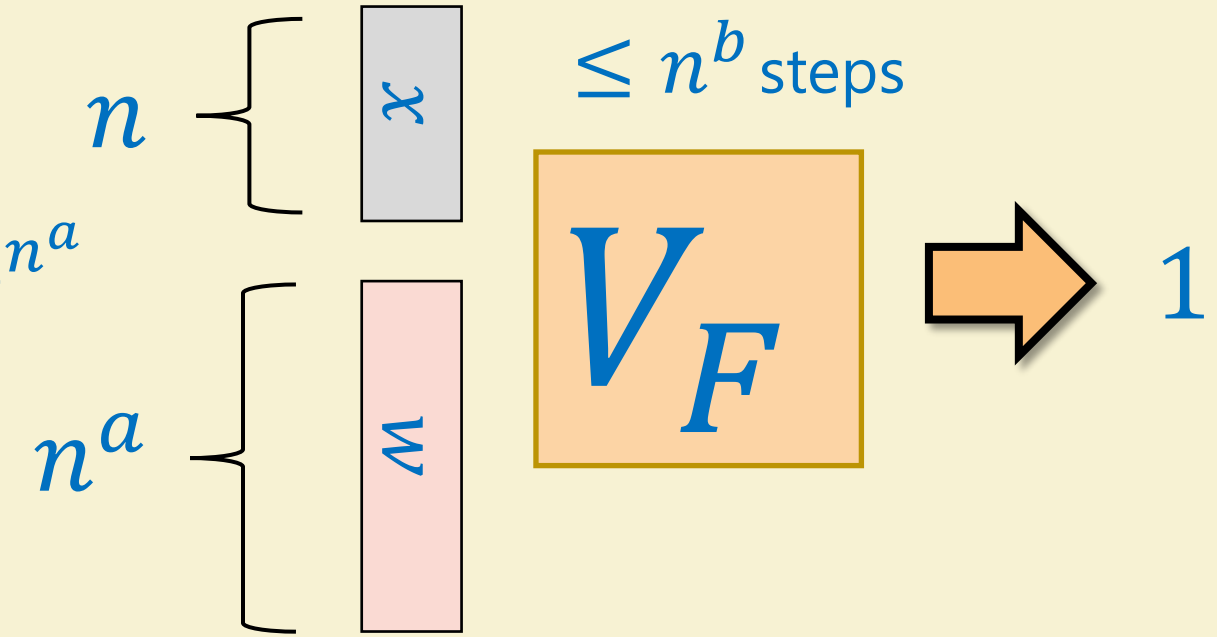
Output: 1 iff there is $x \in \{0,1\}^n$ s.t. $P(x) = 1$

$F(x)=1 \overset{?}{\iff} \exists w \; C_x(w)=1$

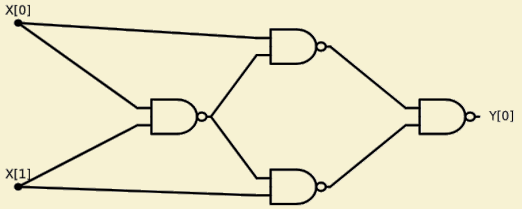
Lemma 1: For every $F \in NP$, $F \leq_p NANDSAT$

Proof: If $F \in NP$ we know $\exists$ poly-time TM V_F s.t. $\forall x \in \{0,1\}^n$

$$F(x) = 1 \iff \exists w \in \{0,1\}^{n^a}$$



Input: NAND-CIRC program P (aka circuit with NAND gates)

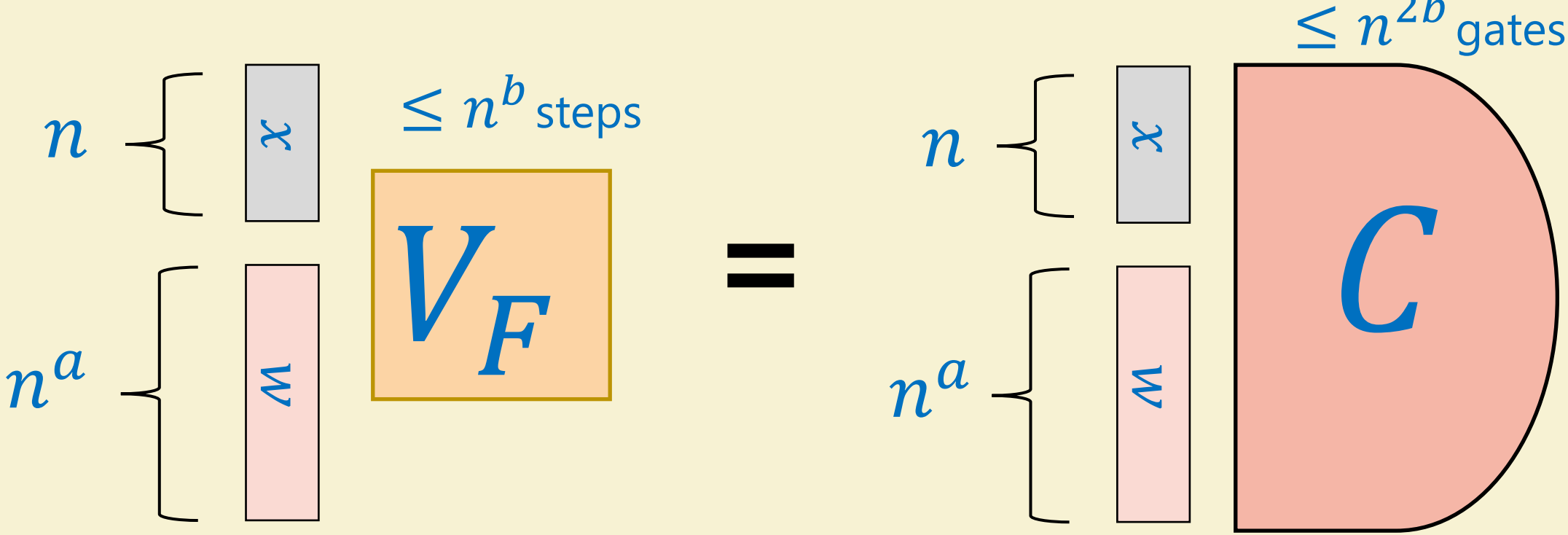


Output: 1 iff there is $x \in \{0,1\}^n$ s.t. $P(x) = 1$

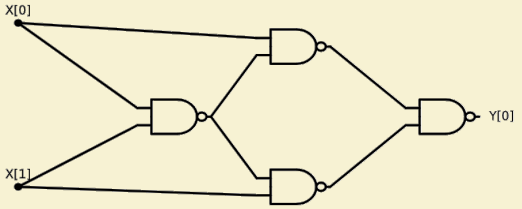
Lemma 1: For every $F \in NP$, $F \leq_p NANDSAT$

Proof: If $F \in NP$ we know $\exists$ poly-time TM M s.t. $\forall x \in \{0,1\}^n$

By proof of $P \subseteq P_{/poly}$ (Time $\leq\approx$ SIZE) can find n^{2b} sized circuit C s.t.



Input: NAND-CIRC program P (aka circuit with NAND gates)



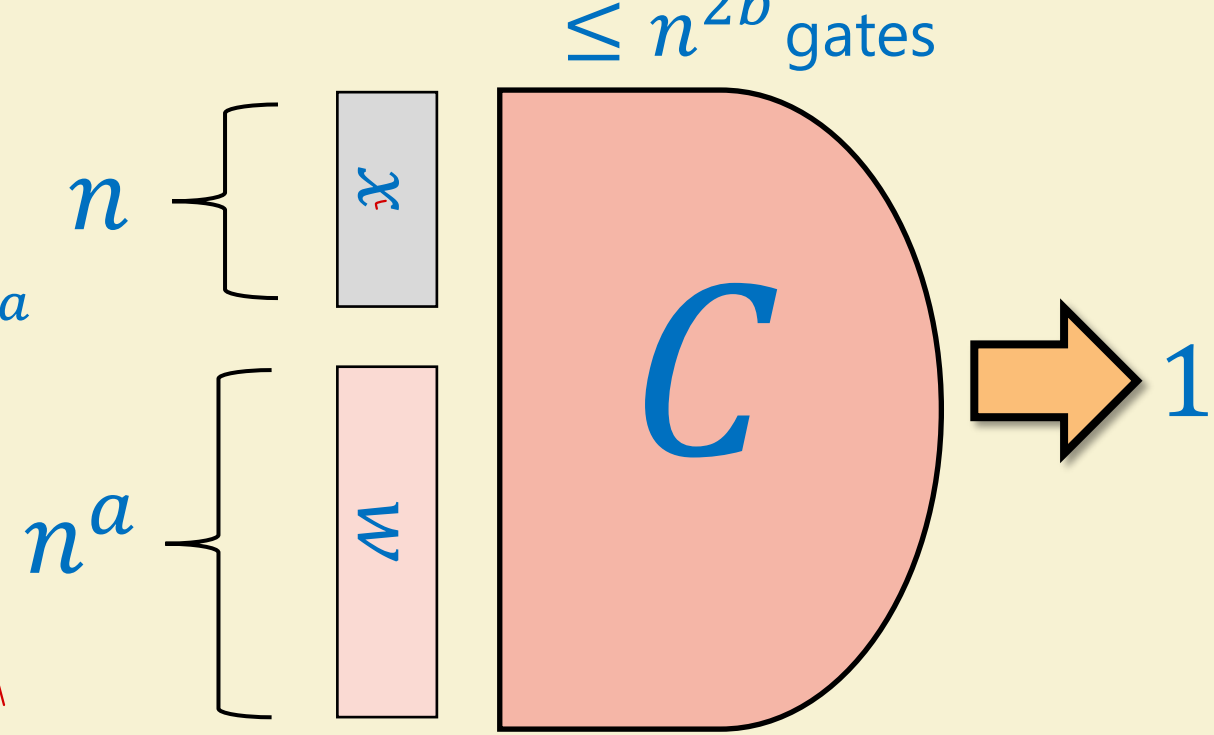
Output: 1 iff there is $x \in \{0,1\}^n$ s.t. $P(x) = 1$

Lemma 1: For every $F \in NP$, $F \leq_p NANDSAT$

Proof: If $F \in NP$ we know $\exists$ poly-time TM V_F s.t. $\forall x \in \{0,1\}^n$

By proof of $P \subseteq P_{/poly}$ can find n^{2b} sized circuit C s.t.

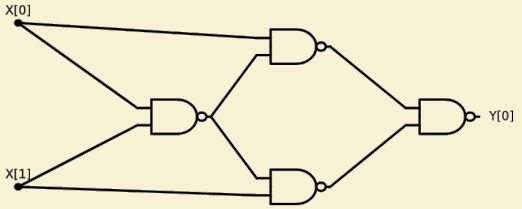
$$F(x) = 1 \iff \exists w \in \{0,1\}^{n^a}$$



Given x $\exists w$ s.t. $C(x,w)=1$

$\Rightarrow \exists w$ s.t. $C'(w)=1$

Input: NAND-CIRC program P (aka circuit with NAND gates)



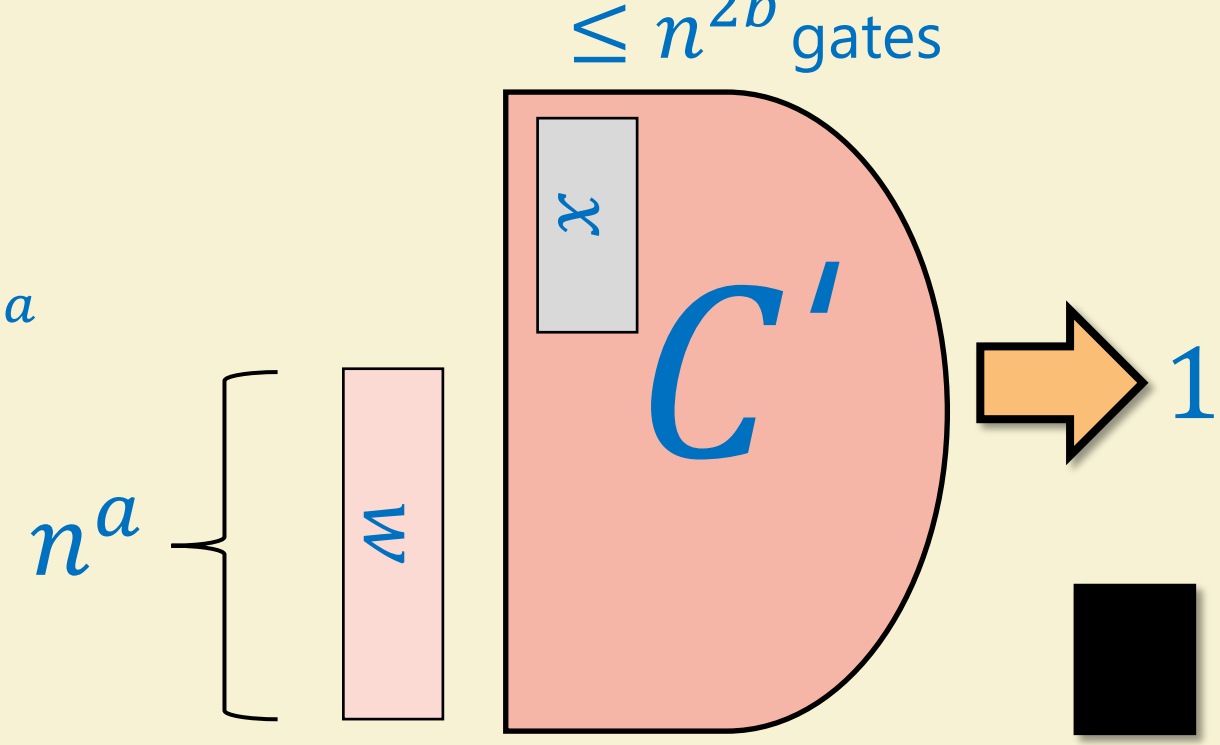
Output: 1 iff there is $x \in \{0,1\}^n$ s.t. $P(x) = 1$

Lemma 1: For every $F \in NP$, $F \leq_p NANDSAT$

Proof: If $F \in NP$ we know $\exists$ poly-time TM M s.t. $\forall x \in \{0,1\}^n$

By proof of $P \subseteq P_{/poly}$ can find n^{2b} sized circuit C s.t.

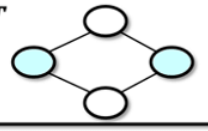
$$F(x) = 1 \iff \exists w \in \{0,1\}^{n^a}$$



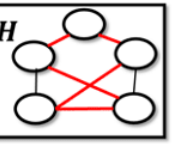
01EQ

$x_1 + x_7 + x_3 = 3,\ x_7 + x_8 = 2,\ \ldots$

ISET



LONGPATH



SUBSETSUM

112321,5645868,34664,34543, ...

• • •

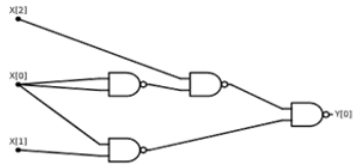
$F(x) = 1$

$\Rightarrow \exists w$ s.t.

$G_x(w) = 1$

Completeness

NANDSAT



$\exists w$ s.t. $G_x(w) = 1$

$\Rightarrow F(x) = 1$

Soundness

3NAND

$(x_4 = NAND(x_2, x_3)) \wedge (x_8 = NAND(x_4, x_5)) \wedge \cdots$

3SAT

$(x_0 \vee \overline{x}_2 \vee x_7) \wedge (x_5 \vee x_2 \vee \overline{x}_{12}) \wedge (x_9 \wedge x_2 \wedge \overline{x}_0) \cdots$

reduction $\boxed{F \leq_p \text{NANDSAT}}$

Given x output C_x s.t.

$F(x) = 1 \iff \text{NANDSAT}(C_x) = 1$

$\iff \exists\, w$ s.t. $C_x(w) = 1$

Example to illustrate proof

Example: $ISET \leq_p 3SAT$

Input: Graph G integer k

Step 1: NAND circuit C_G such that
$C_G(S) = 1$ iff $|S| \geq k$ and S independent in G

Step 2: 3NAND formula Ψ s.t. $\exists z$ with $\Psi(z) = 1$ iff $\exists S$ s.t. $C_G(S) = 1$

Step 3: 3CNF formula φ s.t. $\varphi(z) = \Psi(z)$ for every z

Next lecture

- More reductions. See more diverse NP-complete problems.