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.
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)
  - \( F: \{0,1\}^* \rightarrow \{0,1\} \in \text{\textbackslash NP} \iff \exists V_F \text{ polytime comp. s.t. } F(x) = 1 \iff \exists w \text{ s.t. } V_F(x, w) = 1 \)

• Defined NP-Hard and NP-complete
  - \( F \text{ NP-hard} \iff \forall G \in \text{NP}, G \leq_p F \)
  - \( F \text{ NP-complete} \iff F \in \text{NP} \text{ and } F \text{ NP-complete.} \)

• Asserted: 3SAT is NP-Complete
  - \( 3SAT(C_1 \land C_2 \cdots C_m) = 1 \iff \exists x_1, \ldots, x_n \in \{0,1\} \text{ s.t. } \forall j \exists \text{ literal in } C_j \text{ that is 1.} \)
  - 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

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: $3NAND \leq_p 3SAT$
\textbf{NANDSAT}

\textbf{3NAND}

\[
(x_4 \land \text{NAND}(x_2, x_3)) \land (x_8 \land \text{NAND}(x_4, x_5)) \land \ldots
\]

\textbf{3SAT}

\[
(x_0 \lor \bar{x}_2 \lor x_7) \land (x_5 \lor x_2 \lor \bar{x}_{12}) \land (x_9 \land x_2 \land \bar{x}_0) \ldots
\]
Input: $\Psi$ 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 $\Psi$

Q: If $\Psi = (z_0 = NAND(z_2, z_3)) \land (z_3 = NAND(z_2, z_1)) \land (z_1 = NAND(z_2, z_3))$
what is 3NAND($\Psi$)?

Lemma 2: $NANDSAT \leq_p 3NAND$
Lemma 3: $3\textit{NAND} \leq_p 3\textit{SAT}$

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

$$c = \textit{NAND}(a, b)$$

$$\bar{a} \lor \bar{b} \lor \bar{c}$$

$$\land$$

$$c \lor a$$

$$\land$$

$$c \lor b$$

**Q:** Prove key claim.

**Key claim $\Rightarrow$ lemma.**
NANDSAT

3NAND

\[(x_4 = NAND(x_2, x_3)) \land (x_8 = NAND(x_4, x_5)) \land \ldots\]

3SAT

\[(x_0 \lor \bar{x}_2 \lor x_7) \land (x_5 \lor x_2 \lor \bar{x}_{12}) \land (x_9 \land x_2 \land \bar{x}_8) \ldots\]
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: $\Psi$ 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 $\Psi$

Lemma 2: $NANDSAT \leq_p 3NAND$

“Proof by example:”

$z_2 = NAND(z_0, z_1)$
$z_3 = NAND(z_0, z_2)$
$z_4 = NAND(z_1, z_2)$
$z_5 = NAND(z_3, z_4)$
$z_5 = 1$
$z_6 = NAND(z_0, z_0)$
$z_5 = NAND(z_0, z_6)$
**NANDSAT**

\[ x_4 = \text{NAND}(x_2, x_3) \land (x_8 = \text{NAND}(x_4, x_5)) \land \ldots \]

**3NAND**

\[ (x_0 \lor \bar{x}_2 \lor \bar{x}_7) \land (x_5 \lor x_2 \lor \bar{x}_{12}) \land (x_9 \land x_2 \land \bar{x}_8) \ldots \]

**3SAT**
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. $\forall x \in \{0,1\}^n$
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.

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

$\leq n^{2b}$ gates
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
\[x_1 + x_2 + x_3 = 3, x_\bar{1} + x_4 = 2, \ldots\]

ISET

LONGPATH

SUBSETSUM
112321, 5645868, 34664, 34543, \ldots

**NANDSAT**

**3NAND**
\[(x_4 = \text{NAND}(x_2, x_3)) \land (x_8 = \text{NAND}(x_4, x_5)) \land \ldots\]

**3SAT**
\[(x_0 \lor \bar{x}_2 \lor x_7) \land (x_5 \lor x_2 \lor \bar{x}_{12}) \land (x_9 \land x_2 \land \bar{x}_0) \ldots\]
Example to illustrate proof

Example: $\text{ISET} \leq_p 3\text{SAT}$

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 $\Psi$ s.t. $\exists z$ with $\Psi(z) = 1$ iff $\exists S$ s.t. $C_G(S) = 1$

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

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