Lecture 4

Last time

NP-completeness (finally!)

co-NP

EXP and NEXP

If EXP ≠ NEXP, then P ≠ NP

Proof used padding

Problem set 1

Should be out on Tuesday

Lecture rooms

Are we fine in 1537?

(Apparently yes.)

Today

Circuits

TODAY

- Boolean circuits
- Studied since 1940s
- Shannon: Circuit minimization (Σ_2^P - problem)
- Connection to P vs NP soon made in 1970s
- Circuits explicit combinatorial objects — simpler to reason about?

BOOLEAN CIRCUIT

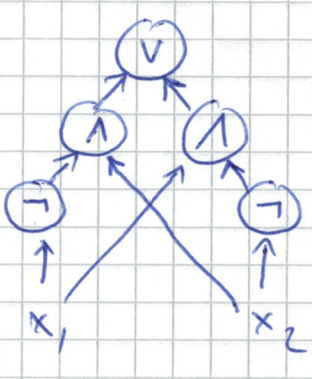
- Directed acyclic graph (DAG) ← NOT TRUE FOR REAL-WORLD CIRCUITS
- n inputs/sources labelled by variables
- one sink
- Internal (non source) vertices labelled

$\wedge$	AND	fan-in 2
$\vee$	OR	fan-in 2
$\neg$	NOT	fan-in 1

- size = # vertices
- depth = length of longest path

Value computed by circuit on $x \in \{0,1\}^n$ defined bottom-up in natural way

EXAMPLE 3 x_1 XOR x_2:



Easy to generalize to multiple outputs:
one output bit per sink

How do we decide problems — inputs of growing size?

DEF 4 $T : \mathbb{N} \to \mathbb{N}$ function

A $T(n)$-size circuit family is a sequence $\{C_n\}_{n \in \mathbb{N}}$ of Boolean circuits where $\forall n$ C_n has n inputs, one output, and size $|C_n| \leq T(n)$ (for some constant k: $\leq n^k$)

$L \in SIZE(T(n))$ if $\exists$ $T(n)$-size $\{C_n\}_{n \in \mathbb{N}}$ s.t. $L = \{x \mid C_n(x) = 1 \text{ for } n = |x|\}$

EX 5 $\{1^n : n \in \mathbb{N}\} \in SIZE(n)$

Build tree of AND-gates

Proved in lec 2: any $f : \{0,1\}^n \to \{0,1\}$ computed by CNF of size $n 2^n$.

In fact, can do $O(2^n/n)$.

More interesting: poly-size circuits

DEF 6 $P/poly = \bigcup_{c \in \mathbb{N}^+} SIZE(n^c)$ "P slash poly"

Why this name? Will get back to it later today.

THM 7 $P \subseteq P/poly$

BTW Arora-Barak $P_{/poly}$ subscript
Also common $P/poly$

Proof sketch Similar to Cook-Levin.

Given poly-time TM M

Make oblivious TM $\tilde{M}$ with quadratic time blow-up

Given oblivious $T(n)$-time $\tilde{M}$, construct $\{C_n\}_{n \in \mathbb{N}}$

s.t. $C_n(x) = M(x)$ $\forall x \in \{0,1\}^n$

Transcript of M on x

Sequence of snapshots $z_1, z_2, \ldots, z_{T(n)}$

- machine state
- symbols read

Snapshot z_i constant # bits

depends on constant # bits

- previous snapshot z_{i-1}
- last times current tape position visited $z_{i_1}, \ldots, z_{i_k}$

$\Rightarrow \exists$ constant-size circuit computing

z_i from $z_{i-1}, z_{i_1}, \ldots, z_{i_k}$

Glue such circuits together and check

$z_{T(n)}$ accepting. □

LEMMA 8 $P \neq P_{/poly}$

Any unary language $L \subseteq \{1^n : n \in \mathbb{N}\}$ is in $P_{/poly}$ (use idea from Ex 5)

Let

UHALT $= \{1^n \mid$ binary expansion of n encodes $\langle M, x \rangle$ such that M halts on input $x\}$

Boolean circuits can be used to prove Cook-Levin

DEF 9

CIRCUIT SAT $= \{x \mid x$ describes a circuit C and $\exists u$ s.t. $C(u) = 1\}$

LEMMA 10 CIRCUIT SAT is NP-complete

Prof Clearly in NP.

$L \in NP \Rightarrow \exists M$ s.t. $x \in L$ iff $\exists u \in \{0,1\}^{p(|x|)}$ $M(x,u) = 1$

Run proof of Thm 7 to get C s.t. $M(x,u) = C(u)$ (Hard-wire value x)

LEMMA 11 CIRCUITSAT $\leq_p$ 3-SAT

Proof idea For every circuit gate/node v_i:

Introduce variable z_i

Write clauses enforcing that z_i is correctly computed given inputs

Say $v_i = v_j$ AND v_k. Get clauses:

$$(\bar{z}_j \vee \bar{z}_k \vee z_i) \wedge (z_j \vee \bar{z}_i) \wedge (z_k \vee \bar{z}_i)$$

Finally add unit clause z_i for output node v_i. ☑

~~~

VITALT $\in P_{/poly}$ is a bit weird. We have no way of constructing these circuits. Would be reasonable to require as well?

DEF 12 $\{C_n\}_{n \in \mathbb{N}}$ is P-uniform if $\exists$ poly-time TM M that on input 1^n outputs (description of) C_n.

More reasonable — but not so fun. Collapses $P_{/poly}$ to P

LEM 13 L is computable by P-uniform circuit family iff $L \in P$

Proof sketch

($\Rightarrow$) Given x, run M on $1^{|x|}$ to obtain $C_{|x|}$ and then evaluate $C_{|x|}$ on x.

($\Leftarrow$) Go over proof of Thm 7 carefully to check that construction is P-uniform.
~~~

Turing machines that take advice

Given x, look at $n = |x|$

Get advice string α_n which depends on n

(but is common for all x with $|x| = n$)

DEF 14 $T: \mathbb{N} \to \mathbb{N}$ $a: \mathbb{N} \to \mathbb{N}$ functions

$DTIME(T(n))/a(n)$ contains every L s.t.

$\exists \{\alpha_n\}_{n \in \mathbb{N}^+}$, $\alpha_n \in \{0,1\}^{a(n)}$,

$\exists$ TM M

s.t. $x \in L$ iff $M(x, \alpha_n) = 1$

and M runs in time $O(T(n))$.

THM 15 $P_{/poly} = \bigcup_{c,d} DTIME(n^c)/n^d$

($\Rightarrow$) Suppose $L \in P_{/poly}$

Let advice string be description of $C_{|x|}$

($\Leftarrow$) Use proof of Thm 7 to construct

poly-sized circuit D_n s.t. $D_n(x, \alpha) = M(x, \alpha)$

Let $C_n = D_n$ with α_n hardwired as 2nd input.

Could it be that CNFSAT $\notin P$ but for all formulas φ of size s there is some really useful advice α_s so that we can solve φ given α_s ?!

That is, can it be that $NP \subseteq P_{/poly}$?

Want to argue this is "unlikely".
How to do that?
Study hierarchy of problems above NP and co-NP

MINIMUM SIZE CIRCUIT PROBLEM

Given Boolean circuit C, find equivalent circuit C^* that has minimal size

a) $\forall x \quad C(x) = C^*(x)$

b) C^* smallest circuit with this property

Decision version

Input: Circuit C, number k

Question: Does there exist circuit C' with $\leq k$ gates that is equivalent to C?

Complexity of this problem?

Equivalence problem probably not in P

i.e. $C \equiv C'$?

Let C be 3-CNF formula

Let C' be trivial circuit that outputs false

Question $C \equiv C'$? $\Leftrightarrow$ Is C satisfiable

But equivalence problem $C \equiv C'$?
is in coNP

For no instances, can find easily verifiable witness.

Can solve MIN-SIZE-CIRCUIT decision problem by

(a) Guessing circuit C' NP problem
(b) check if $C \equiv C'$ co-NP problem

DEF Σ_2^P Set of all languages L for which exists poly-time TM and polynomial q such that

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{q(|x|)} \forall v \in \{0,1\}^{q(|x|)} M(x,u,v) = 1$$

Σ_2^P contains both NP (use u, ignore v)
and coNP (use v, ignore u)

MIN-SIZE-CIRCUIT

There exists circuit u such that for all inputs v circuit is correct

DEF (POLYNOMIAL HIERARCHY)

For $i \geq 1$, $L \in \Sigma_i^P$ if

$\exists$ poly-time TM M

$\exists$ polynomial q

such that

$$x \in L \Leftrightarrow \exists u_1 \in \{0,1\}^{q(|x|)} \forall u_2 \in \{0,1\}^{q(|x|)} \exists u_3 \in \{0,1\}^{q(|x|)} \dots Q_i u_i \in \{0,1\}^{q(|x|)}$$
$$M(x, u_1, u_2, \dots, u_i) = 1$$

Polynomial hierarchy $PH = \bigcup_{i=1}^{\infty} \Sigma_i^P$

$\Pi_i^P = co\Sigma_i^P = \{ \overline{L} : L \in \Sigma_i^P \}$

$\Sigma_1^P = NP \qquad \Pi_1^P = coNP$

$\Sigma_i^P \subseteq \Pi_{i+1}^P \subseteq \Sigma_{i+1}^P \subseteq \dots$

Hence $PH = \bigcup_{i=1}^{\infty} \Pi_i^P$

---

u_i vectors of variables
φ Boolean formula (say CNF)

Complete problems Σ_i-SAT

$$\exists u_1 \forall u_2 \exists u_3 \dots Q_i u_i \; \varphi(u_1, u_2, \dots, u_i)$$

Π_i-SAT $\forall u_1 \exists u_2 \dots Q_i u_i \; \varphi(u_1, u_2, \dots, u_i)$

Common belief (and kind of assumption for this course)

$P \neq NP$ $\quad$ $NP \neq coNP$

Generalization

$$\Sigma_i^P \subsetneq \Sigma_{i+1}^P \quad \text{for all } i$$

"The polynomial hierarchy does not collapse"

Argue that some claim $\mathcal{C}$ is unlikely:

If $\mathcal{C}$ holds, then the polynomial hierarchy collapses to the ith level

$$PH = \Sigma_i^P$$

THEOREM 5 (exercise)

If $\Sigma_i^P = \Pi_i^P$, then $PH = \Sigma_i^P$, i.e. the polynomial hierarchy collapses to the ith level

---

If $NP \subseteq P_{/poly}$ then PH would collapse to the second level

THEOREM [Karp-Lipton '80]
If $NP \subseteq P/poly$, then $PH = \Sigma_2^P$

How to prove this?

By Thm E, sufficient to show

$$\Sigma_2^P = \Pi_2^P$$

In fact, suffices to show $\Pi_2^P \subseteq \Sigma_2^P$ (why?)

Take Π_2^P-complete language L
Show that $L \in \Sigma_2^P$

Π_2SAT = All true formulas of form

$$\psi = \forall u \in \{0,1\}^n \exists v \in \{0,1\}^n \varphi(u,v) = 1$$

Π_2SAT is in Σ_2^P if there is a poly-time TM M s.t.

$$\psi \in \Pi_2\text{SAT} \iff \exists u^* \in \{0,1\}^{q(|\psi|)} \forall v^* \in \{0,1\}^{q(|\psi|)} M(\psi, u^*, v^*) = 1$$

i.e., flip $\forall$- and $\exists$- quantifier
How?!

Have to use assumption

$$NP \subseteq P/poly$$

But proof will have to wait...

Next two lectures:

Boolean circuit complexity continued with JOHAN HÅSTAD

SUMMING UP TODAY'S LECTURE

- Def of Boolean circuits
- P/poly - polynomial-size circuits
- $P \subseteq P/poly$
- But circuits NON-UNIFORM model of computation - can solve uncomputable problems.
- Circuits = Turing machines with ADVICE
- Crash course on the POLYNOMIAL HIERARCHY
- Generalization of P≠NP hypothesis: "The polynomial hierarchy doesn't collapse"
- If we believe this, then poly-size Boolean circuits cannot decide NP. (But proof of this will be given later)