LECTURE 6

LAST TIME

- Sublinear space, in particular logspace
- Careful with reductions (implicitly logspace computable)
- PATH NL-complete (and in general space cplx classes closed under complement)
- coNL = NL!
- In between P and PSPACE: polynomial hierarchy PH
- L in Σ_i^P if

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

(q: poly; M: poly-time)

- $\Pi_i^P = \text{co}\Sigma_i^P$
- $PH = \bigcup_{i \in \mathbb{N}^+} \Sigma_i^P$
- $\Sigma_1^P = NP \qquad \Pi_1^P = \text{co}NP$

THEOREM 1

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

Smaller i $\Rightarrow$ stronger statement

THEOREM 2

$PH \subseteq PSPACE$ and inclusion strict unless hierarchy collapses.

Σ_i^P-complete problems and Π_i^P-complete problems

$$\Sigma_i\text{SAT} = \{ \psi \mid \psi = \exists u_1 \forall u_2 \exists u_3 \cdots Q_i u_i \; \varphi(u_1, u_2, \ldots, u_i) \}$$

(ψ one; u_j bit vectors, φ CNF formula)

$$\Pi_i\text{SAT} = \{ \psi \mid \psi = \forall u_1 \exists u_2 \forall u_3 \cdots Q_i u_i \; \varphi(u_1, \ldots, u_i) \}$$

(ψ one)

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

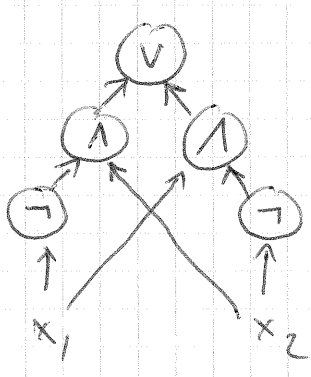
- Directed acyclic graph (DAG)
- n inputs/sources labelled by variables
- one sink
- Internal (non source) vertices labelled

$\wedge$	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

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: $\leq T(n)^k$)

$L \in SIZE(T(n))$ 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

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

LEMMA 10 CIRCUITSAT is NP-complete

Proof 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. $M(x,u) = C(u)$

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

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 $NP \subseteq P/poly$?

No... Unless the polynomial hierarchy collapses...

To the 2nd level...

THM 16 [Karp-Lipton '80]
If $NP \subseteq P/poly$, then $PH = \Sigma_2^P$.

Proof By Thm 1, sufficient to show $\Sigma_2^P = \Pi_2^P$.
In fact sufficient to show $\Pi_2^P \subseteq \Sigma_2^P$ (why?).
Consider Π_2^P-complete language $\Pi_2 SAT$ =
= all one formulas $\forall$ an form

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

Now, given φ and $u \in \{0,1\}^n$, can set u-variables in φ to their values and simplify.
So consider $\varphi(u,\cdot)$ as formula on n variables for any fixed u. Is $\varphi(u,\cdot)$ satisfiable?
That's an NP-question.
We're assuming $\boxed{NP \subseteq P/poly}$.
Hence $\exists C_n$ s.t.

$$C_n(\varphi, u) = 1 \text{ iff } \exists v \in \{0,1\}^n \text{ s.t. } \varphi(u,v) = 1.$$

Now reduce search to decision

Run C_{n-1} on $(\varphi, u, v_1 = 0)$ et ceetera
Find $v \in \{0,1\}^n$ satisfying $\varphi(u,\cdot)$
Yields (multi-output circuits) $\{C'_n\}_{n \in \mathbb{N}}$ of poly size $q(n)$ s.t.

$$\exists v \in \{0,1\}^n \varphi(u,v) = 1 \iff \varphi(u, C'(\varphi,u)) = 1$$

$\{C'_n\}_{n \in \mathbb{N}}$ exists for one ψ roughly size $q(n) \Rightarrow$ can be described with $(q(n))^2$ bits (or less)
How to find? Guess (and then verify)!

① Guess description w of C'_n

② Verify for all $u \in \{0,1\}^n$ that $\varphi(u, C'_n(\varphi,u)) = 1$

Suppose ψ false

Then $\exists u \in \{0,1\}^n$ such that no satisfying v can be computed $\Rightarrow$ guess will fail.

Hence we can reduce Π_2^P-formula ψ in (*) to

$$\psi' = \exists w \in \{0,1\}^{q(n)^2} \forall u \in \{0,1\}^n \quad (**)$$

(Σ_1^P – statement $\exists w \forall u\, M(x,w,u)$)

"w describes a circuit C' and $\varphi(u, C'(\varphi,u)) = 1$"

(verifiable in poly time)

Circuit evaluation can be done in poly time, so verification in (**) can be performed in poly time

Hence get instance of Σ_2^P-language.

Thus $\Pi_2^P \subseteq \Sigma_2^P$ and the theorem follows.

Can also prove:

<u>THM 17</u> (Meyer's theorem)

If $EXP \subseteq P/poly$ then $EXP = \Sigma_2^P$

<u>COR 18</u>

If $P = NP$ then $EXP \not\subseteq P/poly$

<u>Proof</u>

If $P = NP$ then $P = \Sigma_2^P$ by Thm 1.

If $EXP \subseteq P/poly$ then by Thm 17 $P = EXP = \Sigma_2^P$.

Violates time hierarchy theorem □

So complexity <u>upper</u> bounds can prove circuit <u>lower</u> bounds!

Can we prove any unconditional circuit lower bounds? Yes. Some functions must require very large circuits (worst-case hard)

THM 19

For every $n \in \mathbb{N}^+$ there is a function $f: \{0,1\}^n \to \{0,1\}$ that cannot be computed by any circuit of size $2^n/(10n)$

Proof By counting.

functions from $\{0,1\}^n$ to $\{0,1\}$

2^n possible inputs, 2 choices for every input

2^{2^n} functions

How many circuits of size S?

Each gate can be

- $\wedge, \vee, \neg$, input — 4 choices
- for input specify which of $n < S$ variables
- for $\neg$ (not) specify input gate $\leq S$ choices
- for $\wedge, \vee$ specify two inputs $\leq S^2$

Total # circuits sth like (don't need to count very carefully

$$(4S^2)^S = 2^{S \log(4S^2)} \overset{\text{base-2}}{\leq} 2^{9S \log S}$$

Set $S = 2^n/(10n)$. Then # circuits $\leq$

$$2^{9 \cdot \frac{2^n}{10n} \log\left(\frac{2^n}{10n}\right)} \leq 2^{\frac{9}{10} 2^n \cdot \frac{1}{n} \log 2^n} = 2^{\frac{9}{10} 2^n}$$

$< 2^{2^n}$. Hence $\exists$ function $f: \{0,1\}^n \to \{0,1\}$ not computed by circuits of size $S = 2^n/(10n)$ ∎

A different take on Shannon's theorem

Pick function $f: \{0,1\}^n \to \{0,1\}$ at random by flipping a coin for every input x

For a fixed circuit C, probability that f and C agree on x is $= \frac{1}{2}$.

$Pr[f \text{ and } C \text{ agree on every input}] = 2^{-2^n}$

$Pr[\exists\, C \text{ which agrees with } f] = ?$

Union bound

For any events $A_1, A_2, \ldots, A_m$, probability that one of A_i happens is bounded by sum of probabilities

$$Pr\left[\bigcup_{i=1}^{m} A_i\right] \leq \sum_{i=1}^{m} Pr[A_i]$$

$Pr[\exists \text{ Circuit } C \text{ agreeing with } f] \leq$

$$\sum_{\substack{\text{all circuits} \\ C_i}} Pr[C_i \text{ agrees with } f] \leq$$

$$2^{\frac{9}{10}2^n} \cdot 2^{-2^n} = 2^{-\frac{1}{10}\cdot 2^n}$$

That is, <u>vast majority</u> of functions $f: \{0,1\}^n \to \{0,1\}$ are hard

Probabilistic method Prove that object $\mathcal{O}$ with property P exists by choosing $\mathcal{O}$ randomly and showing $Pr[\mathcal{O} \text{ has property } P] > 0$

Since probability is strictly positive, such an element must exist!

In our case

$$\Pr[\text{randomly chosen } f \text{ hard}] \geq 1 - 2^{-\Omega(2^n)}$$

$\to 1$ as $n \to \infty$

Means that most random objects have property.

Counting can also be used to prove nonuniform time hierarchy theorem for circuits — see Thm 6.22 in text-book

SUMMING UP

Today we studied Boolean circuits

$P/poly$ class of languages computed by polynomial-size circuits $\{C_n\}_{n \in \mathbb{N}^+}$

Nonuniformity a bit tricky

$P/poly$ strict superset of P since it contains undecidable languages

$P = NP$ iff NP has uniform poly-size circuits

Even dropping uniformity condition, believe

$NP \not\subseteq P/poly$ (or PH collapses).

Most functions are hard (require exp size circuits)
What about lower bounds for explicit functions?
Next time ...