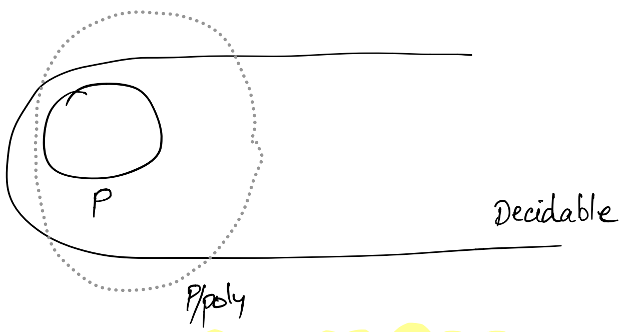
Computational Complexity - Lecture 12.

Recap: - Polynomial hierarchy

Thm: $\Sigma_i = \Pi_i \Rightarrow PH = \Sigma_i$.

- Circuit families: $C = \{C_i\}_{i=1...}$ with C_i "handling" length i strings
- $SIZE(f(n)) = \{L : L$ is decided by a circuit family of size $s(n)\}$.
- $P/poly = \bigcup_{c \geq 0} SIZE(n^c)$

Agenda: - Karp-Lipton(-Sipser) Theorem
- More on circuits & advice.



Where is NP here?

Thm: [Karp-Lipton] If $NP \subseteq P/poly$, then $PH = \Sigma_2$.

Pf: We'll show that $NP \subseteq P/poly$ then $\Sigma_2 = \Pi_2$.

$L \in \Pi_2$ $\quad x \in L \iff \forall y\, \exists z.\ M(x,y,z) = 1$ $\quad \varphi'$

$L' = \{(x,y) : \exists z.\ M(x,y,z) = 1\} \in NP$

$\Rightarrow$ By the hyp. there is a circuit family $\{C_i\}$ deciding L'.

No clue of what $\{C_i\}$ is ... but we can guess!

We can use this $\{C_i\}$ to find a z. if one exists.

$$\varphi : \quad \exists C_1, \ldots, C_m \quad \forall y \quad M(x, y, \text{Get Witness}(C_1, \ldots, C_m, x, y)) = 1$$

Claim: φ is true iff φ' is true

Pf: $\varphi' = \text{true} \Rightarrow \varphi$ is true.

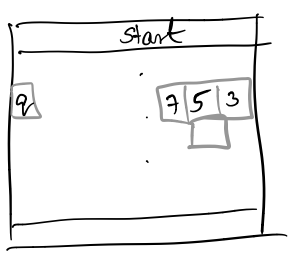
$\varphi = \text{true} \Rightarrow \varphi'$ is true

$\therefore \Pi_2 \subseteq \Sigma_2 \Rightarrow PH = \Sigma_2 \cap \Pi_2$. $\square$.

An extension of this theorem

Thm [Meyer] If $EXP \subseteq P/poly$ then $EXP = \Sigma_2$

Pf: M - TM that runs in exp. time. (2^{n^c})



$L_M = \{(x, t, s) :$ s^{th} symbol in the t^{th} row, when M starts on x is 1. $\}$

$L_M \in EXP. \subseteq P/poly$

$\Rightarrow$ There is some circuit family.

$|x| = n$

$\exists C \quad \forall t, s.$ Local Check (C, x, t, s)

$\wedge$ StartState $(\ )$

$\wedge$ Final state (accept) $\square$.

$\Rightarrow EXP = \Sigma_2$.

Hierarchy theorems?

Is $SIZE(f(n)) \subsetneq SIZE(g(n))$ if $f(n) \ll g(n)$.?

Usual diagonalisation doesn't quite work. (why?).

Thm: For any f, g with $n < 10 f(n) < g(n) < 2^n/n$, we have $SIZE(f(n)) \subsetneq SIZE(g(n))$.

Revisiting the quiz:

- ▷ How many fns $F : \{0,1\}^\ell \to \{0,1\}$ are there?

  2^ℓ

  2^{2^ℓ}

- ▷ How many circuits are there of size s?

  gates $1, 2, \ldots, s$

  For each gate:

  - ▷ type $\wedge, \vee, \neg$ — $O(1)$
  - ▷ Left child — $\log s$
    Right child. — $\log s$

Description : $\leq 3 s \log s \Rightarrow \#$ circuits $= 2^{3 s \log s}$

Corollary: There are fns $F : \{0,1\}^\ell \to \{0,1\}$ that cannot be computed by $s = 2^\ell / 10\ell$ size.

Pf: $3 s \log s \leq 3 \cdot 2^\ell / 10\ell \cdot \ell \leq 2^\ell / 3 \Rightarrow \#$ circuits $\leq 2^{2^\ell / 3}$

But there are 2^{2^ℓ} functions! HPP $\Rightarrow$ Done! $\square$

Note: A "random" function is probably very hard.
"Pseudorandom property"

Thm: For any f, g with $n < 10 f(n) < g(n) < 2^n/n$, we have $SIZE(f(n)) \subsetneq SIZE(g(n))$.

Pf: Choose an ℓ carefully

Claim 1: There are functions $F: \{0,1\}^\ell \to \{0,1\}$ that cannot be comp by size $2^\ell/10\ell$.

Claim 2: Every function $F: \{0,1\}^\ell \to \{0,1\}$ can be comp by circuits of size $2^\ell/\ell$.

Set ℓ : $f(n) \lesssim 2^\ell/10\ell$

$F': \{0,1\}^n \to \{0,1\}$ defined by $F'(x) = F(\text{first } \ell \text{ bits of } x)$

$\square$.

About the power of P/poly.

$L \in$ P/poly if there exists $\{C_i\}_{i=1\ldots}$

that accepts L.

Varun: But we aren't saying anything about how hard it is to construct C_n given n.

↳ Non-uniform model

Crypto!

Uniform Circuit families: $\{C_i\}_{i=1\ldots}$ is a $*$-uniform circuit family if the function $1^i \mapsto C_i$ can be computed in $*$.

Replace $*$ by your favourite class.

Go back and check: $P \subseteq$ L-uniform P/poly.

Why P/poly? Is there a P/logn?

TMs with advice.

DTIME$(t(n))/a(n)$

Languages accepted by a DTIME$(t(n))$ machine when given an advice.

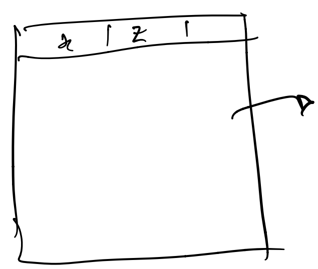
$$\left\{ L : \exists\, M \in \mathrm{DTIME}(t(n)),\ \exists\, \{z_i\}_{i=1\ldots} \text{ such that } |z_i| \le a(i) \text{ and } x \in L \text{ iff } M(x, z_{|x|}) = 1. \right\}$$

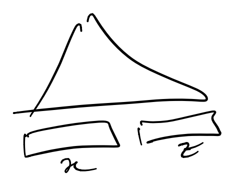
Eg: UHALT = $\{ 1^n :$ The n^{th} machine halts on a blank tape$\}$.
$\in P/1$.

Thm: $P/poly = \bigcup_{c,d} DTIME(n^c)/n^d$

Pf: $\subseteq$: The advice strings $\{z_i\}$ is just the desc. of the circuit family.
& M is Ckt Eval

$\supseteq$:





$\square$

Some important circuit classes:

poly size.

fan-in 2	fan in unbounded.
depth $O((\log n)^i)$	depth $O((\log n)^i)$
NC^i	AC^i
Nick' Class (by Steve Cook)	(Alt. TMs)

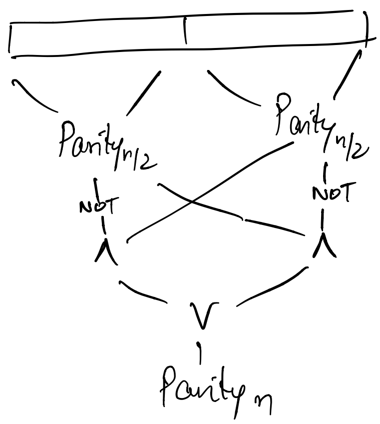
AC^0: constant depth circuits, unbounded fan in, poly size.

NC^0: constant depth circuits, bounded fan-in
depends only on $O(1)$ bits! Boring.

NC^1: bounded fan-in log-depth, poly size.

Obs: PARITY $\in NC^1$.

Pf:



size = poly(n)
Depth = $O(\log n)$
fan-in = 2.

□.

□.

Thm: [Furst-Saxe-Sipser, Håstad, Razborov, Smolensky]
PARITY $\notin AC^0$.

$$
\begin{tikzcd}
NC^0 \arrow[r] \arrow[d] & NC^1 \arrow[r] \arrow[d] & NC^2 \arrow[d] & \cdots \\
AC^0 \arrow[r] \arrow[ur] & AC^1 \arrow[r] \arrow[ur] & AC^2 & \cdots
\end{tikzcd}
$$

ACC: AC class with $\wedge, \vee, \neg$, Mod_6 gates

Does it make sense to study large circuits?

say exponential size? $S = 2^{n^c}$. $i = 2^{n^c}$

Defn: (Direct connection uniformity).

$\{C_n\}$ is a DC-uniform family if there is a poly-time algorithm to do the following tasks:

Type (i, "g") : What is the type of gate 'g'.

Child (i, "g_1", "g_2") : Is g_1 a child of g_2?

Size (i) : What is the size of C_i?

Makes sense even for exponential size circuits.

Thm: $L \in PH$ iff L is computed by a DC-uniform circuit family $\{C_i\}$ with

- Size $(C) \leq 2^{\text{poly}(n)}$
- $\{C_i\}$ is a constant depth family with unbounded fan-in.
- All NOT gates pushed to the inputs.

(Hence the name AC).

Also, if we remove the const. depth requirement, we get EXP.

Next class: Randomised computation