Computational Complexity

Mohammad Mahmoody

Session 17
20 March 2014

Last Time

$f:\{0,1\}^* \rightarrow \{0,1\}$

- $f = \{f_n\} \in \text{Size}(s(n))$ if f_n can be computed by circuit of size $s(n)$
- Every f is in $\text{Size}(2^n \cdot 3n)$
- $\mathbf{P}/poly = \bigcup_c \text{Size}(n^c)$
- $\mathbf{P} \subset \mathbf{P}/poly$ because of Cook-Levin reduction:
  any $L \in \text{Dtime}(t)$ also belongs to $\text{Size}(t^2)$
- $\mathbf{P} \neq \mathbf{P}/poly$ because even $\text{Size}(n)$ contains incomputable languages

$g < s$

Limits of $\mathbf{P}/poly$

$g+n = s$

$f \in Size(2^n \cdot 10n)$
$\subseteq Size(1000\, 2^n/n)$

Theorem 6.21 *(Existence of hard functions* [Sha49a]*)*
For every $n > 1$, there exists a function $f : \{0, 1\}^n \to \{0, 1\}$ that cannot be computed by a circuit C of size $2^n/(10n)$.

let $s = 2^n/10n$

how many functions $f: \{0,1\}^n \to \{0,1\}$ exist? 2^{2^n}

upper-bound # of circuits of size s:

$g+n=s$

$\leq$

total # functions computable by a circuit of size $\leq s$

α_i : total numbers to add gate i

$3s^2 \geq \alpha_i =$ 3 : types of gates.
ways to choose input wires $\leq (n+i-1)^2 \leq s^2$

$$\prod \alpha_i \leq (3s^2)^s \leq \boxed{s^{3s}} = \left(\frac{2^n}{10n}\right)^{3(2^n/10n)} < 2^{n \cdot 3\left(\frac{2^n}{10n}\right)} = 2^{3 2^n/10 \ldots}$$

Hierarchy Theorem for Circuits

Theorem 6.22 *(Nonuniform Hierarchy Theorem)*
For every functions $T, T' : \mathbb{N} \to \mathbb{N}$ *with* $2^n/n > T'(n) \geq \overset{1000000}{\cancel{10}}\, T(n) > n$,

$$\mathbf{SIZE}(T(n)) \subsetneq \mathbf{SIZE}(T'(n))$$

ℓ bits.

(Size by which we can compute all functions over ℓ bits.) $\dfrac{2^\ell \times 1000}{\ell} = T'(n)$

(Size that is Not enough for all function of ℓ bit input) $\dfrac{2^\ell}{10\ell} = T(n)$

Why calling it $\mathbf{P}/poly$?

Let M be: input $x \in \{0,1\}^n$, C_n
output $C_n(x)$

- $f \in \mathbf{P}/poly \;\Rightarrow f_n$ can be computed efficiently give C_n as "advice"

$L \in$ iff $\exists\, a_1, a_2 \cdots a_n \cdots$ $|a_n| \le t(n)$ $\exists$ efficient M
$M(a_n, x) =$ correct answer

- Let $\mathbf{P}/\mathrm{t(n)}$ be set of functions efficiently computable with help of a **single** "advice" of length $t(n)$ for **all inputs** of length n

Thm Def$_1$(P/poly) $\subseteq$ ✓
Def$_2$(P/poly) $\supseteq$?

- Let $\mathbf{P}/poly = \mathrm{U}_c \mathbf{P}/\mathrm{n^c}$

$\boxed{\text{Def 2}}$

because $C_n = a_n$ is the advice we need.

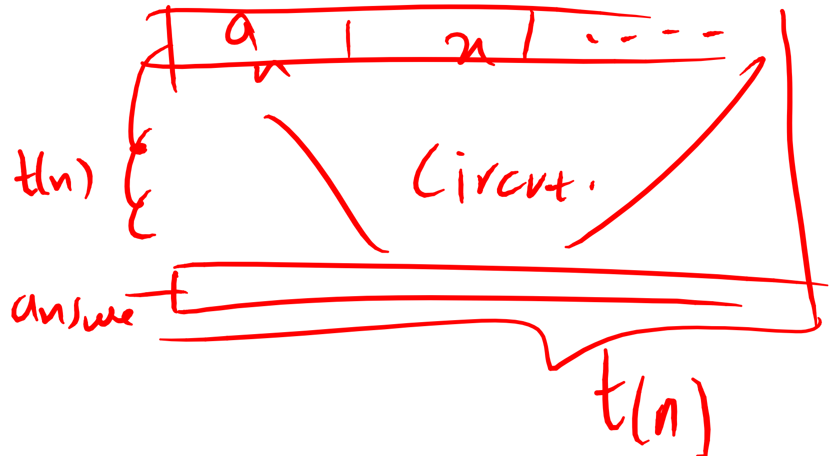
$Def_2 \subseteq Def_1$

Two definitions are equivalent

$L \in$ Def$_2$ of P/poly $\left\{ \begin{array}{l} \text{if } \exists M, \; a_1, a_2 \ldots a_n \ldots \; : \text{sequence of advice} \\ M \text{: poly-time machine} \\ M(a_n, x) = \text{correct answer} \quad (x \overset{?}{\in} L) \\ |x| = n \end{array} \right.$

$\Leftrightarrow$ $\exists$ sequence $C_1\, C_2 \ldots C_n$ of $|C_n| \leq poly(n)$

such that $C_n(x) = \text{correct answer} \; (x \overset{?}{\in} L)$



C_n : Circuit coming from Cook-Levin reduction by hardwiring advice a_n into the circuit.

Is $\mathbf{NP} \subseteq \mathbf{P}/poly$?

Theorem 6.19 *(Karp-Lipton Theorem [KL80])*
If $\mathbf{NP} \subseteq \mathbf{P}_{/\mathbf{poly}}$, *then* $\mathbf{PH} = \mathbf{\Sigma}_2^p$.