Computational Complexity

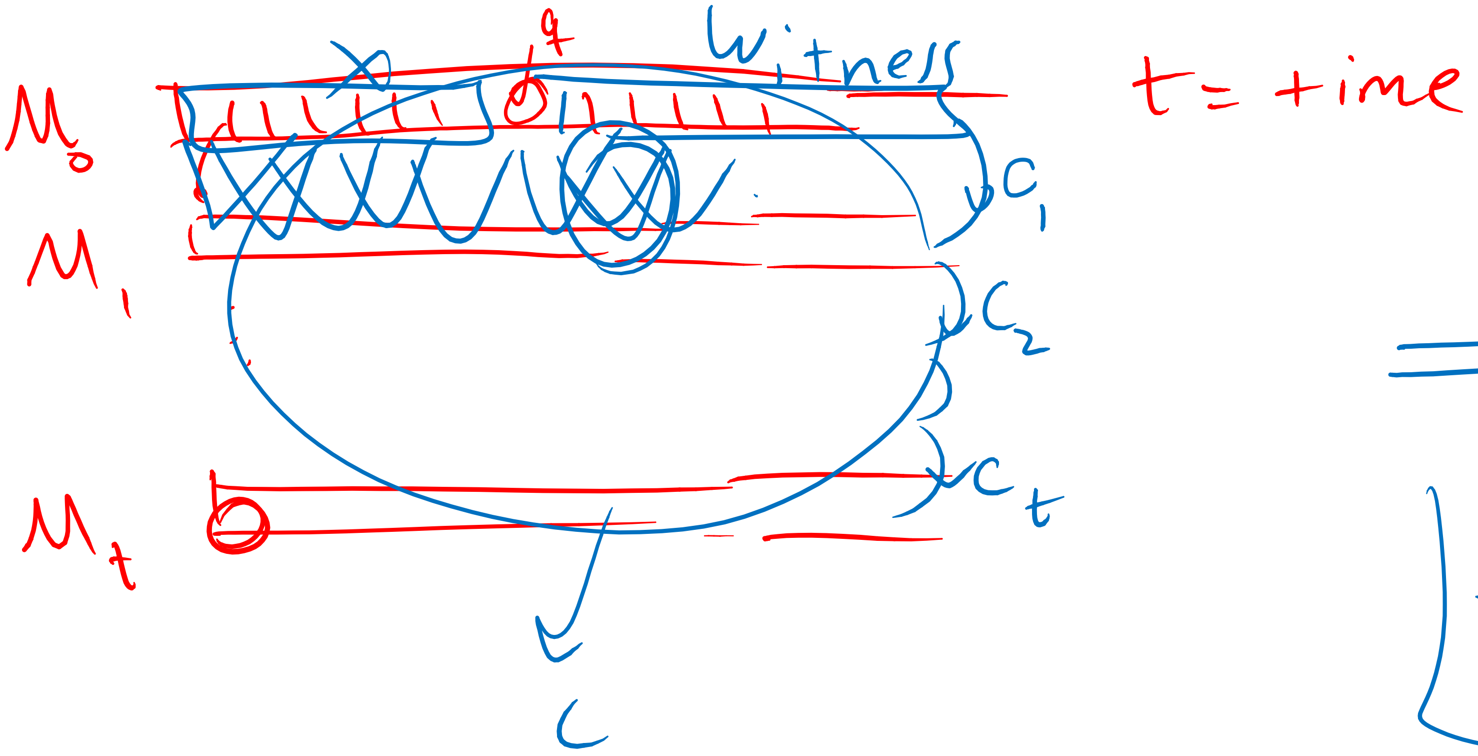
Mohammad Mahmoody

Session 16
18 March 2014

Today

- Circuit Complexity

Recal Cook-Levin Reduction



if $L \in DTime(t)$

$\Longrightarrow$ there exist a circuit C of size $O(t^2)$ that, given x, $C(x) = L(x)$

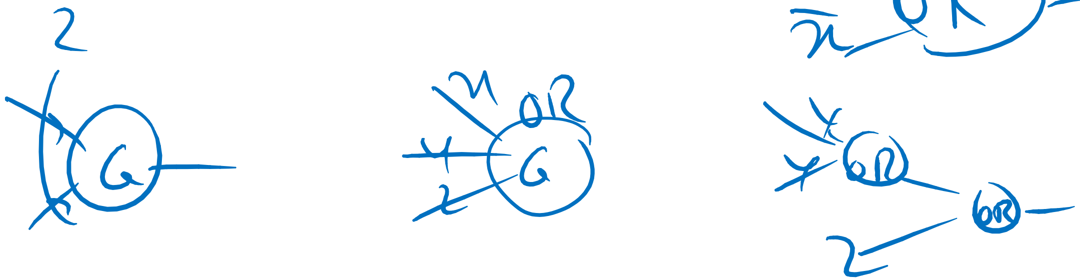
$t(\cdot)$

hope $P \neq NP$

Some Details

- Constant gates: 0 1

- Fan-in: ≤ 2



- Fan-out: not limited

- Other gates: {AND, OR, NOT}, {NAND} {~~XOR~~}

Definition of class $\mathbf{P}/poly$

C_n

$f:\{0,1\}^n \longrightarrow \{0,1\}$ can be computeb by circuit of size $2^n\cdot(3n)$

$f:\{0,1\}^* \longrightarrow \{0,1\}$ can be - - - - - by $C=\{C_1,\dots C_i,\dots C_n,\dots\}$ such that $|C_i| \leq 2^n(3\cdot n)$

$f \in \mathrm{Size}(t)$ if $\exists\ C=\{C_1,\dots C_n,\dots\}$ such that

① for $|x|=n$ $C_n(x)=f(x)$

② $|C_n| \leq t(n)$

Thm ①: $\forall f$: $f \in \mathrm{Size}(2^n\cdot 3n)$

$P/poly$: $\bigcup_{c>0} \mathrm{Size}(n^c)$

Thm ② $P \subseteq P/poly$?

$\mathrm{Dtime}(t) \subseteq \mathrm{Size}(t^2)$

Can $\mathbf{P}$ be equal to $\mathbf{P}/poly$?

Cantor's Theorem

$|\mathbb{N}| < |\mathbb{R}|$

① easy proof that $P \neq P/poly$

$r = 0.r_1 r_2 \cdots r_n \cdots$

② Halting problem $\notin P$

if $1^n \in L$ then C_n is AND of $x_1 \ldots x_n$
if $1^n \notin L$ — is always $= 0$

Proof

Unary Language $L = \{ 1^n \mid$ if turing Machine encoded by n halts $\}$

$\cap$

$\{1, 11, 111, \ldots\}$

$L \in P/poly$: any unary lang $\in P/poly$

$\boxed{L \notin P}$

Can $\mathbf{P}/poly$ contain all languages?

- Recall: any $f : \{0,1\}^n \to \{0,1\}$ is computable by a circuit of size $2^n \cdot (3n)$

Thm P/Poly does NOT include everything.

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 $2^n/(10n)$.