CMSC 651, Automata Theory, Fall 2010

Sandipan Dey,
Homework Assignment - 11

December 18, 2010

Problem 1 Solution

We have to show that for any language L,

$$L \in Co-NE \Rightarrow L \in NE/poly$$

Proof

We have, $L \in Co-NE \Rightarrow \bar{L} \in NE$.

Also, let's assume that we have a set of NTMs M_c, each machine runs for $2^{c|x|}$ steps & accepts if $x \in \bar{L}$, $\forall c = 1, 2, \ldots$

Let's Construct a TM M s.t.

$M(x)$

1. Constructs NTMs $M_c,\ c \geq 1$.
2. Runs $M_1, M_2, \ldots$ simultaneously on x.
3. Accepts x if any of the M_cs accepts, ow rejects.

M accepts iff $x \in \bar{L} \Rightarrow L(M) = \bar{L}$.

Now we have to construct a TM M' that runs in NE with size of advice function being polynomial in input size and decides L. We have to decide the membership in L, which is same as non-membership in $\bar{L}$ and can be nondeterministically decided using census in the following manner:

$M'(x)$

1. Constructs & runs NTMs $M'_c(\langle x, c|x|\rangle)$, each machine guesses $|L(M_c)| = 2^{2^{c|x|}}$ different (e.g. lexicographically) strings in $L(M_c)$ & accepts if none equals x.
2. Accepts x if every M'_c accepts, ow rejects.

M' accepts iff $x \in L \Rightarrow L(M') = L \in$ NE/poly.

Problem 2 Solution

To prove: $\exists.BP.P \subseteq BP.\exists.P$.

Proof

Let $L \in \exists \cdot \mathrm{BP} \cdot \mathrm{P}$.

Then there exist a language L' in $\mathrm{BP} \cdot \mathrm{P}$ and a bound $p' \in \mathbf{poly}$ such that $L = \exists^{p'}(L')$

By probability amplification to obtain a language L'' in P and a bound $p'' \in \mathbf{poly}$ s. t.

$$(\langle x, w\rangle, \langle y, w\rangle) \in L' \implies \Pr_r[(\langle\langle x, w\rangle, r\rangle, \langle\langle y, w\rangle, r\rangle) \in L''] \geq 1 - 2^{-\ell'_n - 2} \text{ , and}$$

$$(\langle x, w\rangle, \langle y, w\rangle) \notin L' \implies \Pr_r[(\langle\langle x, w\rangle, r\rangle, \langle\langle y, w\rangle, r\rangle) \in L''] \leq 2^{-\ell'_n - 2}$$

for every n-bit input pair (x, y) and witness w.

Here, $\ell'_n := \lceil p'(\log n) \rceil$, and the random string r is uniformly drawn from $\mathbb{B}^{\ell''_n}$, where $\ell''_n := \lceil p''(\log n) \rceil$.

Define $L''' := \left\{(\langle\langle x, r_1\rangle, w_1\rangle, \langle\langle y, r_2\rangle, w_2\rangle) \,\middle|\, (\langle\langle x, w_1\rangle, r_1\rangle, \langle\langle y, w_2\rangle, r_2\rangle) \in L''\right\}$.

Hence, $L'''' := \exists^{p'}(L''') \in \exists{\cdot}\mathrm{P}$.

Now,

$$\begin{aligned}
(x, y) \in L &\implies \exists w\colon (\langle x, w\rangle, \langle y, w\rangle) \in L' \\
&\implies \Pr_r[\exists w\colon (\langle\langle x, w\rangle, r\rangle, \langle\langle y, w\rangle, r\rangle) \in L''] \geq \frac{3}{4} \\
&\implies \Pr_r[\exists w\colon (\langle\langle x, r\rangle, w\rangle, \langle\langle y, r\rangle, w\rangle) \in L'''] \geq \frac{3}{4} \\
&\implies \Pr_r[(\langle x, r\rangle, \langle y, r\rangle) \in L''''] \geq \frac{3}{4} \text{ ,}
\end{aligned}$$

$$\begin{aligned}
(x, y) \notin L &\implies \forall w\colon (\langle x, w\rangle, \langle y, w\rangle) \notin L' \\
&\implies \Pr_r[\exists w\colon (\langle\langle x, w\rangle, r\rangle, \langle\langle y, w\rangle, r\rangle) \in L''] \leq 2^{\ell'_n} \cdot 2^{-\ell'_n - 2} \\
&\implies \Pr_r[(\langle x, r\rangle, \langle y, r\rangle) \in L''''] \leq \frac{1}{4} \text{ .}
\end{aligned}$$

$\implies L \in \mathrm{BP} \cdot \exists \cdot \mathrm{P}$.

Hence, $L \in \exists \cdot \mathrm{BP} \cdot \mathrm{P}. \implies L \in \mathrm{BP} \cdot \exists \cdot \mathrm{P}$. $\quad \therefore\ \exists{\cdot}\mathrm{BP}{\cdot}\mathrm{P} \subseteq \mathrm{BP}{\cdot}\exists{\cdot}\mathrm{P}$.

It works for $BP.\exists.P \subseteq \exists.BP.P$ as well.

Problem 3 Solution

The reduction in Cook's theorem is parsimonious.

Proof

We need to show that $\#acc_N(x) = \#SAT(\Phi)$, where the formula
$\Phi = \Phi_{cell} \bigwedge \Phi_{start} \bigwedge \Phi_{move} \bigwedge \Phi_{acccept}$. It's enough to show that there is a one-to-one correspondence between the # of distinct satisfying assignments of Φ and the # accepting configurations of N, as per the construction of Cook's reduction.

From theorem 3.37, it's easy to see that an accepting configuration of N on input x (s.t. $q_0 x\$ \overset{n^k}{\vdash} y q_{acc}\$$) corresponds to a satisfying assignment of the formula Φ, since $\Phi_{start} \bigwedge \Phi_{acccept} = True$ ensures that the satisfying assignment must satisfied the starting and accepting configuration of N, while $\Phi_{cell} \bigwedge \Phi_{move} = True$ ensures that every cell contains exactly one symbol and every move of N is a legal move. Also, for a any two distinct satisfying assignments must have two different configurations in N, since they must be different in Φ_{move} and/or Φ_{accept}, there must be different configurations in N.

Hence, $\#acc_N(x) = \#SAT(\Phi)$.