Complexity - Exercise 2

Oren Roth

December 12, 2017

Question 1

Let M be the TM which decide A and $p(n)$ a polynomial, which for any input with size n, M runs at most $p(n)$ steps with oracle access to inputs with length at most $n-1$. We will describe M' that will use only $n * p(n)$ space for any input of size n and decide A. This will show $A \in PSPACE$. Given $x \in \Sigma^*$, M' will save n slots with size $p(n)$ each. M' runs as follows:

- Copy x to the first slot
- run M on the input in slot 1. When oracle request is asked copy the input for the oracle to the next slot and runs M on it.
- Continue the same process when oracle request is asked copy the input for the oracle to the next slot and runs M on it and so on.
- When M answer on input of slot $i > 1$, clear slot i and return the answer to M on slot $i-1$ that asked the question to the oracle and continue the run of M on slot $i-1$.
- When answer of M appears on slot 1, M' return the same.

First notice that any calls for oracle is shrink the input by one, so we will use at most n slots, because each slot is with size $p(n)$, M' uses $poly(n)$ space. Moreover as M need $p(n)$ time for an input in size n, it for sure use at most $p(n)$ space for inputs in size $\leq n$, in each slot we run on inputs with size $\leq$ to n and hence each slot as sufficient space for running M.
If all the calls for the oracle are correct M' is just simulating M on slot 1 and hence $L(M') = L(M)$. Assume that all the calls for the oracle in input y with $|y| < k$ are simulating correctly by M' and let y be input for the oracle with $|y| = k$, for this we will open new slot and run M on y, with every oracle call on inputs in size at most $k-1$ which by the induction assumption we know M' simulate correctly and hence, M' on y will answer exactly as M on y.

Question 2

We will assume $CO-NP \subseteq NP$, and derive $PH \subseteq NP$ and hence $PH = NP$.

$$PH = \bigcup_{i=0}^{\infty} \Sigma_i^p$$

We will show by induction on i that $\Sigma_i^p \subseteq NP$.
$i = 0$, $\Sigma_0^p = P \subseteq NP$.

$i = 1$, $\Sigma_1^p = NP \subseteq NP$.
Assume that for i, $2 \leq i < k$:

$$\Sigma_i^p \subseteq NP$$

We know $NP \subseteq \Sigma_i^p$ and hence $NP = \Sigma_i^p$.
This makes $\Pi_i^p = CO - NP$, and because we know $CO - NP \subseteq NP$ we get $\Pi_i^p \subseteq \Sigma_i^p$.
Let us show $\Sigma_k^p \subseteq NP$:

$$L \in \Sigma_k^p \iff \exists M \; polynomial \; TM \; s.t:$$
$$x \in L \iff \exists y_1 \forall y_2 \dots Q_k y_k \; M(x, y_1, y_2, \dots, y_k) = 1$$

Let us define L':

$$L' = \{(x, y_1) : \forall y_2 \exists y_3 \dots Q_k y_k \; M(x, y_1, y_2, \dots, y_k) = 1\}$$

So we have:

$$x \in L \iff \exists y_1 \forall y_2 \dots Q_k y_k \; M(x, y_1, y_2, \dots, y_k) = 1 \iff \tag{1}$$
$$\forall y_2 \exists y_3 \dots Q_k y_k \; M(x, y_1, y_2, \dots, y_k) = 1 \iff (x, y_1) \in L' \tag{2}$$

By definition $L' \in \Pi_{k-1}^p$ but we showed for all indexes $i < k$ that $\Pi_i^p \subseteq \Sigma_i^p$, and so we conclude $\Pi_{k-1}^p \subseteq \Sigma_{k-1}^p$, and:

$$L' \in \Sigma_{k-1}^p$$

and hence there exists polynomial M' s.t.

$$(x, y_1) \in L' \iff \exists y_2 \forall y_3 \dots Q_k y_k \; M'(x, y_1, y_2, \dots, y_k) = 1$$

And moreover:

$$(x, y_1) \in L' \iff \exists y_2 \forall y_3 \dots Q_k y_k \; M'(x, y_1, y_2, \dots, y_k) = 1 \iff$$
$$\exists y_1, y_2 \forall y_3 \dots Q_k y_k \; M'(x, y_1, y_2, \dots, y_k) = 1$$

Adding with the inequality in (1) we conclude:

$$x \in L \iff \exists y_1 \; s.t. \; (x, y_1) \in L' \iff$$
$$\exists y_1, y_2 \forall y_3 \dots Q_k y_k \; M'(x, y_1, y_2, \dots, y_k) = 1$$

And we got that $L \in \Sigma_{k-1}^p$, which by IA we know $\Sigma_{k-1}^p \subseteq NP$, and we derive our desire conclusion:

$$L \in NP$$

And thus,

$$\Sigma_k^p \subseteq NP$$

By induction we showed that for any $i \in \mathbb{N}$, $\Sigma_i^p \subseteq NP$ and thus $PH \subseteq NP$, we know $NP \subseteq PH$, so we conclude: $PH = NP$.

Question 3

a.

Assume $DP \subseteq NP$, for any $L \in CO-NP$, if we will look at:

$$L \cap \Sigma^* = L$$

Because $\Sigma^* \in P \subseteq NP$ we got $L \in DP$. So we showed that also:

$$CO-NP \subseteq DP$$

Together with our assumption we got:

$$CO-NP \subseteq DP \subseteq NP$$

And we already showed in Q.2 that $CO-NP \subseteq NP$ is concluding to $PH = NP$.

b.

Question 4

a.

b.

SAT is a special case of boolean formula, so as we showed in 1, iff $x \in SAT$ there is a witness for it, a interpretation for it a with:

$$(x, a) \in FVAL$$

Because the witness tape is just like a normal tape we can run the algorithm from section a, and determine $x \in SAT$ iff $\exists a$ s.t. $(x, a) \in FVAL$.

c.

Claim 0.1 *G is not bipartite graph $\iff$ there is a cycle of odd length in G*

We will show that $BIPARTITE \in CO-NL$ and by theorem we showed in class ($NL = CO-NL$) we will conclude $BIPARTITE \in NL$. Let us show $\overline{BIPARTITE} \in NL$ by describe M non deterministic TM which decide $\overline{BIPARTITE}$.
M will receive as an witness the odd cycle in G (by our claim we know there exist iff $G \in \overline{BIPARTITE}$) and just check that this cycle exists in G.
M will accept $\iff$ there is such witness $\iff$ $G \in \overline{BIPARTITE}$.

Proof of claim *($\Leftarrow$) Let $C = \{v_1, v_2, \ldots, v_{2n+1}\}$ be a cycle of odd length, by contradiction assume $G = (V \cup E)$ is bipartite with $V = L \cup R$ division of V to two disjoint sets as promised. WLOG assume $v_1 \in L$ so $v_2 \in R$, $v_3 \in L$ and so on (there is edge between those vertices so they have to be in different sets), we conclude all the odd vertices are in L but there is edge between v_{2n+1} to v_1 and we arrive to contradiction.*
($\Rightarrow$) Let be ■

Question 5

a.

Let be f a one-directional function, and we will show $P = NP$.
Let M_f be the polynomial TM which compute f.
Let us define TM $M(y, x)$,

- given (y, x)
- M runs $M_f(x)$ and get y'
- M accepts iff $y' = y$

So M is polynomial. We will define now L':

$$L' = \{(y, x, 1^n) : \exists z \ s.t \quad M(y, x \cdot z) = 1 \wedge |x \cdot z| = n\}$$

We will show $L' \in NP \setminus P$:

- $L' \in NP$: We will show a non deterministic TM M' which will decide L'. Given $(y, x, 1^n)$, M' will will guess $z \in \{0,1\}^{n-|x|}$ and run $M(y, x \cdot z)$ and answer the same. We will have:

$$(y, x, 1^n) \in L' \iff \exists z \ s.t \quad M(y, x \cdot z) = 1 \wedge |x \cdot z| = n \iff$$
$$\textit{there exists accepting computation for } M'$$

- $L' \notin P$: Otherwise by contradiction $L' \in P$, there exists TM M_p s.t

$$(y, x, 1^n) \in L' \iff M_p(y, x, 1^n) = 1 \iff \exists z \ s.t \quad M(y, x \cdot z) = 1 \wedge |x \cdot z| = n$$

  So we can build the following algorithm $\mathcal{A}$ which reverse f, like that, given y and $1^{|x|}$, $\mathcal{A}$ will set the first bit of x to 1 if the run of $M_p(y, 1, 1^{|x|})$ accepts, and 0 otherwise. Continue by running $M_p(y, x_1 1, 1^{|x|})$ to determine the second bit of x and after total $|x|$ runs of M_p we will find x, and hence $\mathcal{A}$ is polynomial in $(y, 1^{|x|})$. We got:

$$\Pr_{x^R \in \{0,1\}^*, f(x) = y}[\mathcal{A}(y) = x' \quad s.t. \quad f(x') = y] = 1 > \frac{1}{n}$$

  for all $n > 1$, and contradiction that f is one-directional function.

b.