Complexity - Exercise 3

Oren Roth - 200701068

January 6, 2018

Question 1

Assume by contradiction:

$$DSPACE(n^3) = NP \tag{1}$$

Let $S \in DSPACE(n^9) \setminus DSPACE(n^3)$, we assure it exists by space hierarchy theorem, let M_S be the TM that determine S in n^9 time, denote a new language:

$$S' = \{1^{|x|^3}0x : \forall x \in S\}$$

Now we can have new TM, $M_{S'}$, which given input w will:

1. Count in i and delete the leading 1's until the first zero, delete the first zero as well - denote by x the word that left on the tape
2. Assure $|x|^3 = i$, if not reject
3. run M_S on the x and return as M_S

$M_{S'}$ will determine S':

$$w \in S' \iff w = 1^{|x|^3}0x \wedge x \in S \iff M_{S'} \text{ on } w \text{ will pass step 2 without rejects and will accept in step 3}$$
$$\iff M_{S'} \; accepts \; w$$

The time $M_{S'}$ runs steps 1,2 in linear time with respect to the input size, we pass step 2 only if we run $M_{S'}$ on input from the form $w = 1^{|x|^3}0x$. Step 3 run M_S on x which takes $|x|^9$ time, which is smaller than $|w|^3$ time (As $|w| \geq |x|^3$). Concluding $M_{S'}$ runs in n^3 time.

$$S' \in DSPACE(n^3)$$

By (1) we know $S' \in NP$, and hence there is M', TM for which

$$x \in S' \iff \exists y \; s.t. \; M;(x, y) \; accepts$$

Given M', we can show that $S \in NP$ by showing the following TM M. On input (x, y), M add leading $|x|^3$ 1's to x and runs and return as $M'(1^{|x|^3}0x, y)$, clearly M runs in polynomial time, now we have:

$$x \in S \iff 1^{|x|^3}0x \in S' \iff \exists y \; s.t. \; M'(1^{|x|^3}0x, y) \; accepts \iff \exists y \; s.t. \; M(x, y) \; accepts$$

So we conclude $S \in NP$ and by (1) we know $S \in DSPACE(n^3)$ which is contradiction to the definition of S.

Question 2

a.

Let $A \in PP$ and let M be the probabilistic TM that determine it as promise by the definition of PP. M is polynomial, and let $p(n)$ be the upper bound of steps M takes for input of size n. W.L.O.G assume M runs exactly $p(n)$ steps for each input and for each random calculation route. (If M is not like that we can look at another TM which acts like M and for each calculation route if it's not exceed $p(n)$ steps than it does dummy steps until it reaches and rejects/accepts).

Let us define M', deterministic TM which will determine A in polynomial space. M' will hold two counters, one for counting all the accepting paths of M on given input x. The second counter will count all the rejecting paths of M on x. Given x, M' will simulate M on x but instead of using a random bit to decide whereas using δ_1 or δ_2 it will go over all possible $2^{p(|x|)}$ options (We assume each calculation route has exactly $p(n)$ steps and hence $2^{p(|x|)}$ calculation routes). Namely, M' will go over all $r \in \{0,1\}^{p(|x|)}$, for each r, it will simulate M where in each step i, M will take $\delta_{r[i]}$. In the end of each simulation M' will add 1 to the corresponding counter (depends if it accepts or rejects in the end). M' accepts if and only if the first counter is strictly bigger than the second counter.

We notice that number of accepting routes of M is corresponding exactly with the probability that M accepts x. So we have:

$$\begin{aligned} M' \textit{ accepts } x \iff M \text{ has more accepting routes which accepts } x \iff \Pr[M \textit{ accpets } x] > \frac{1}{2} \\ \iff x \in A \end{aligned}$$

M' use two counters of size $\log(2^{p(|x|)}) = p(|x|)$ and tape to go over all the possible r's which also needs $p(|x|)$ bits. To simulate M we need another tape with maximum $p(|x|)$ space as M runs at most $p(|x|)$ steps. In total M' use at most $4 \cdot p(|x|)$ space, so we conclude $A \in PSPACE$.

b.

Given x, N in the first step will use a coin r, identical distribute over $\{0,1\}$. If $r = 0$, N will run M on x and return as M, otherwise N accepts.

$$\Pr[N \textit{ accepts } x] = \frac{1}{2} + \frac{1}{2} \cdot \Pr[M \textit{ accepts } x]$$

c.

Given $A \in NP$ let M be non deterministic TM for which:

$$x \in A \iff \text{there is accepting route in the run of } M \text{ on } x$$

Let N be the corresponding TM for M as described in the previous clause (2b.). We claim for N:

$$\begin{aligned} x \in A \quad & \Pr[N \textit{ accepts } x] > \frac{1}{2} \\ x \notin A \quad & \Pr[N \textit{ accepts } x] \leq \frac{1}{2} \end{aligned}$$

By question (2b.) we knoe:

$$\Pr[N \textit{ accepts } x] = \frac{1}{2} + \frac{1}{2} \cdot \Pr[M \textit{ accepts } x]$$

Well if $x \in A$ there is accepting route of M so

$$\Pr[M \ accepts \ x] > 0$$

So we get:

$$\Pr[N \ accepts \ x] = \frac{1}{2} + \frac{1}{2} \cdot \Pr[M \ accepts \ x] > \frac{1}{2}$$

Otherwise if $x \notin A$ there is no accepting route of M so

$$\Pr[M \ accepts \ x] = 0$$

And we get:

$$\Pr[N \ accepts \ x] = \frac{1}{2} + \frac{1}{2} \cdot \Pr[M \ accepts \ x] = \frac{1}{2}$$

And we proof our claim, concluding $A \in PP$. And hence:

$$NP \subseteq PP$$

Question 3

a.

Let $U \sim^U V$, denote:

$$U = \{u_1, u_2, \ldots, u_{2\log n}\}$$

Let I^* be the IS of size k in G. We denote $2\log n$ random variables Y_i, for each $1 \leq i \leq 2\log n$:

$$Y_i = \begin{cases} 1 & \text{if } u_i \in I^* \\ 0 & \text{otherwise} \end{cases}$$

Denote new random variable

$$Y = \sum_{i=1}^{2\log n} Y_i$$

Denote by $\mathbb{E}[*]$ the expected maximal size IS in $G|_U$, when U is uniformly drawn from V. So we having:

$$\mathbb{E}[*] \geq \mathbb{E}[Y]$$

Due to the fact than any choice for u_i's get the LHS bigger than the RHS (as on the RHS a choice for u_i with value $Y = r$ says that there is at least IS of size r in $G|_U$) We need to show:

$$\mathbb{E}[*] \geq k \cdot (\frac{2\log n}{n})$$

We will show

$$\mathbb{E}[Y] \geq k \cdot (\frac{2\log n}{n})$$

And from transitivity we will gain our goal.

$$\mathbb{E}[Y_i] = \frac{k}{n}$$

As for each node $u \in V$ there is k over n options to be in I^*.

$$\mathbb{E}[Y] = \mathbb{E}[\sum_{i=1}^{2\log n} Y_i] = \sum_{i=1}^{2\log n} \mathbb{E}[Y_i] = 2\log n \cdot \frac{k}{n}$$

And we conclude:

$$\mathbb{E}[*] \geq k \cdot (\frac{2\log n}{n})$$

Denote by A all the sub graphs $G|_U$:

$$A = \{G|_U : |U| = 2\log n\}$$

Now we will show that at least α of the graphs in A have IS in size $\frac{k\log n}{n}$, where $\alpha = \frac{n-2\log n}{n-\log n}$. If by contradiction this is not true, we will have less than α of the graphs in A having maximal IS of size smaller than $\frac{k\log n}{n}$ and for the rest of the graphs have IS of size at most k, so we conclude:

$$\mathbb{E}[*] < \alpha \cdot \frac{k\log n}{n} + (1-\alpha)\cdot k = k \cdot (\frac{2\log n}{n})$$

But this is contradiction to what we showed before. So we conclude at least α of the graphs in A have IS in size $\frac{k\log n}{n}$.

$$\Pr[\text{maximal IS size in } G|_U < \frac{k\log n}{n}] \leq 1-\alpha = \frac{\log n}{n-\log n}$$

b.

Question 4

We will show $coNP \subseteq IP'$ and $IP' \subseteq coNP$.

<u>$IP' \subseteq coNP$</u>: Let $A \in coNP$ so we know there is a TM M s.t.

$$x \in A \iff \forall y: \ M(x,y) \ accepts$$

Let us show $A \in IP'$ by describing protocol of a prover P and Verifier V.
Given x, P will send to the V, y. V will run $M(x,y)$ and answer as M.

If $x \in A$, for any prover P, no matter which y it sends, V will accepts with probability 1. (As $M(x,y)$ accepts for all y).
If $x \notin A$ than by definition there exists y s.t. $M(x,y)$ rejects. So the prover that sends this y will make P accepts with probability 0, which is smaller than one half.
We conclude:

$$A \in IP'$$

$\underline{coNP \subseteq IP'}$: Let $A \in IP'$, and let be V the verifier protocol, so we define non-deterministic TM M which will show $A \in coNP$. On given input x, M will guess $y = (a, r)$ where a will be a guess of all answers of some prover for all the questions of V, and r will be a guess of the coins that V takes. As IP' define both a, r are polynomial in x. M will simulate V on answers a with the coins r and accepts iff V accepted.

If $x \in A$, for any prover P, V will accepts for all answers with probability 1 $\Rightarrow$ for any guess $y = (a, r)$, $M(x, y)$ accepts.
If $x \notin A$, there exists prover s.t $\Pr[V \textit{ accepts } x] \leq \frac{1}{2} \Rightarrow$ for this prover's answers a, not all the calculation routes of V are accepting $\Rightarrow$ there exists $y = (a, r)$ s.t. $V(x)$ with coins r and answers a rejects $\Rightarrow$ Exists y s.t. $M(x, y)$ rejects.
We conclude:

$$x \in A \iff \forall y : \; M(x, y) \textit{ accepts}$$

And hence:

$$A \in coNP$$