Assignment 1

Due February 3 in lecture

The work you submit must be your own. You may discuss problems with each others; however, you should prepare written solutions alone. Copying assignments is a serious academic offense, and will be dealt with accordingly.

(It is helpful to give a high level description of a proof or an algorithm before giving the details.)

Question 1 (Exercise 2.6 (b) in the text) In this question we view each string $\alpha \in \{0,1\}^*$ as the encoding of a nondeterministic Turing machine M_α.

Show that there is an universal nondeterministic Turing machine U such that U accepts input (α, x), if and only if M_α accepts x. Moreover, the machine U must run in time $cT(|x|)$ for some constant c that depends only on M_α, where $T(|x|)$ is the running time of M_α on x.

Question 2 Assume that $DTIME(n) = NTIME(n)$. Show that $\mathbf{P} = \mathbf{NP}$.

Question 3 (Exercise 2.5 in the text) Let PRIME be the language of all prime numbers. This question is to show directly that PRIME is in $\mathbf{NP} \cap co\text{-}\mathbf{NP}$ without using the fact that PRIME is in $\mathbf{P}$.

a) Show that PRIME is in co-$\mathbf{NP}$.

b) Show that PRIME is in $\mathbf{NP}$ using the following theorem:

Lucas test: An integer $n > 2$ is prime if and only if there is an integer $1 < r < n$ such that $r^{n-1} \equiv 1 \mod n$ and for all prime divisor q of $n-1$, $r^{\frac{n-1}{q}} \not\equiv 1 \mod n$.

Question 4 (Exercises 2.10 and 2.29 in the text) (a) Let L_1, L_2 be two languages in $\mathbf{NP}$. Show that $L_1 \cap L_2$ and $L_1 \cup L_2$ are both in $\mathbf{NP}$.

(b) Let L_1, L_2 be two languages in $\mathbf{NP} \cap co\text{-}\mathbf{NP}$. Show that $L_1 \oplus L_2$ is also in $\mathbf{NP} \cap co\text{-}\mathbf{NP}$, where

$$L_1 \oplus L_2 = \{x \ : \ x \text{ is in exactly one of } \ L_1, L_2\}$$

Question 5 None of the two inclusions is known: $\mathbf{P} \subset DSPACE(n)$ and $DSPACE(n) \subset \mathbf{P}$, but using padding and the Space Hierarchy Theorem we can show that $\mathbf{P} \neq DSPACE(n)$. Complete the following steps:

(a) For every language L, let $L^* = \{x01^{|x|^2} \ : \ x \in L\}$. Show that if L^* is in $\mathbf{P}$, then so is L.

(b) Show that there is a language $L \notin DSPACE(n)$ but $L^* \in DSPACE(n)$. Conclude that $\mathbf{P} \neq DSPACE(n)$.