CS 4814: Homework 8

due Friday 11/6, 11:59pm
(late submission until **Monday 11/9 11:59pm**)

Each question is worth 30 points.

Question 1

So far we have seen definitions of NP in terms of polynomial-time verifiers and in terms of non-deterministic polynomial-time Turing machines.

In this exercise, we will see a definition of NP in terms of polynomial-time probabilistic Turing machines.

Let $L \subseteq \{0,1\}^*$ be some decision problem. Show that $L \in$ NP if and only if there exists a polynomial-time probabilistic Turing machine M such that

$$\forall x \in \{0,1\}^*. \quad x \notin L \Leftrightarrow \Pr\left\{M(x) \neq 1\right\} = 1.$$

In words, M rejects every NO instance of L with probability 1 and M accepts every YES instance of L with positive probability.

Question 2

So far our discussion of randomized computation has focused on polynomial-time algorithms that are allowed to err on inputs with some probability.

In this exercise, we will see that sometimes it is possible to obtain randomized algorithms that always output the correct answer but their running time is polynomial only in expectation.

Let $L \subseteq \{0,1\}^*$ be some decision problem. Suppose there exist polynomial-time probabilistic Turing machines M_0 and M_1 with the following properties:

$$\forall x \in L. \quad \Pr\left\{M_1(x) = 1\right\} = 1 \quad \text{and} \quad \Pr\left\{M_0(x) = 1\right\} \geq 2/3$$
$$\forall x \notin L. \quad \Pr\left\{M_1(x) = 0\right\} \geq 2/3 \quad \text{and} \quad \Pr\left\{M_0(x) = 0\right\} = 1.$$

In words, M_1 has success probability 1 for YES instances of L and it has success probability at least 2/3 for NO instances of L. Symmetrically, M_0 has success probability 1 for NO instances of L and it has success probability at least 2/3 for YES instances of L.

Show that there exists a probabilistic Turing machine M and a polynomial $p\colon \mathbb{N} \to \mathbb{N}$ such that for every $x \in \{0,1\}^*$, M on input x correctly solves problem L with probability 1 and the expected running time of M on input x is bounded by $p(|x|)$.

Hint: You may use the following fact without proof: For every $k \in \mathbb{N}$ and $p < 1$, the following infinite series converges,

$$\sum_{i=1}^{\infty} p^i \cdot i < \infty.$$