Problem Set 6

Read Sections 9.1, 9.2, 10.2, 10.4 through Theorem 10.33. Skip the section on Primality (Theorem 10.6 thru Theorem 10.9) and the proof of Lemma 10.30.

1. For any positive integer \( x \), let \( x^R \) be the integer whose binary representation is the reverse of the binary representation of \( x \). (Assume no leading 0s in the binary representation of \( x \).)
   Define the function \( R^+ : N \to N \) where \( R^+(x) = x + x^R \).

   (a) Let \( A_2 = \{ \langle x, y \rangle | R^+(x) = y \} \). Show \( A_2 \in L \).
   (b) Let \( A_3 = \{ \langle x, y \rangle | R^+(R^+(x)) = y \} \). Show \( A_3 \in L \).

2. Describe a deterministic, polynomial-time SAT-oracle Turing machine \( M_{SAT} \) that takes as input a directed graph \( G \) and nodes \( s \) and \( t \), and outputs a Hamiltonian path from \( s \) to \( t \) if one exists. If none exist, then \( M_{SAT} \) outputs No Hamiltonian path.

3. For branching program \( B \) and \( w = w_1 \ldots w_m \), where each \( w_i \in \{0, 1\} \), let \( B(w) \) be the output of \( B \) when its input variables \( x_1, \ldots, x_m \) are set \( x_i = w_i \) for each \( i \).
   (a) Let \( ALL_{ROBP} = \{ \langle B \rangle | B \) is a read-once branching program and \( B(w) = 1 \) on all \( w \} \). Show that \( ALL_{ROBP} \in P \).
   (b) Let \( ALL_{BP} = \{ \langle B \rangle | B \) is a branching program and \( B(w) = 1 \) on all \( w \} \). Show that \( ALL_{BP} \) is coNP-complete.

4. Prove that if \( A \subseteq \{0, 1\}^* \) is a regular language, a family of branching programs \((B_1, B_2, \ldots)\) exists where each \( B_n \) accepts exactly the strings in \( A \) of length \( n \) and is bounded in size by a constant times \( n \).

5. Let \( ICFL \) be the class of languages that can be expressed as the intersection of two context free languages. In other words \( ICFL = \{ A | A = B \cap C \text{ for some CFLs } B \text{ and } C \} \).
   (a) Prove \( ICFL \subseteq P \).
   (b) Prove that \( P \) contains some language which is not in \( ICFL \).
      (Hint: a theorem we proved in lecture is useful here.)

6. Say that a probabilistic algorithm uses randomness \( r(n) \) if it uses at most \( r(n) \) coin tosses on each computation thread.
   (a) Recall the probabilistic algorithm for \( EQ_{ROBP} \) we presented. How much randomness does it use when it is run on two branching programs that have \( m \) input variables? Give your answer as a function of \( m \) using big-O notation. Explain your reasoning.
   (b) Let \( BPP[f(n)] = \{ A | A \) is decided by a probabilistic, polynomial time TM that uses at most \( O(f(n)) \) randomness on all inputs of length \( n \} \). Show that \( BPP[\log(n)] \subseteq P \).

7. (Optional) The class RP is a subset of BPP, where the probabilistic polynomial time decider never accepts for inputs outside the language, thereby exhibiting one-sided error. More formally, RP is the collection of languages \( A \) for which a probabilistic polynomial time decider, accepts with probability at least \( \frac{2}{3} \) (or equivalently \( \frac{1}{2} \)) for inputs in \( A \) and accepts with probability 0 for inputs not in \( A \). Show that if \( NP \subseteq BPP \) then \( NP = RP \).

The Final Exam will be held Monday, December 17, 2018, 1:30–4:30, duPont Gym.
Covers Chapters 1, 2 (except 2.4), 3, 4, 5, 6.1, 7, 8, 9.1, 9.2, 10.2 (except the part on Primality), and 10.4 through Theorem 10.33.