18.404/6.840 Fall 2006 Michael Sipser
Theory of Computation

FINAL EXAM SAMPLE PROBLEMS and SOLUTIONS

1. For each of the following statements, answer `True`, `False` or `Open question` according to our current state of knowledge of complexity theory, as described in class. Give *brief* reasons for your answers.

   (a) $\text{P} \subseteq \text{TIME}(n^5)$?

   (b) $\text{NSPACE}(n^5) \subseteq \text{PSPACE}$?

   (c) $\text{coNP} \subseteq \text{PSPACE}$?

   (d) $\text{NP} \subseteq \text{BPP}$?

   (e) $\text{P} \subseteq (\text{NP} \cap \text{coNP})$?

   (f) $\text{P}^{SAT} \subseteq (\text{NP} \cup \text{coNP})$?

   (g) *CLIQUE* is coNP-hard ?

   (h) *ISO* is NP-hard ?

   (i) *TQBF* is EXPSPACE-complete ?

   (j) For any languages A, B and C, if $A \leq_{\text{L}} B$ and $B \leq_{\text{L}} C$ then $A \leq_{\text{L}} C$?

   (k) $SAT \leq_{\text{P}} \overline{SAT}$?

   (l) $SAT \leq_{\text{m}} \overline{SAT}$?

   (m) $TQBF \leq_{\text{L}} PATH$?

   (n) $HAMPATH \leq_{\text{P}} PATH$?

   (o) $PATH \leq_{\text{P}} \overline{PATH}$?

   (p) $PATH \leq_{\text{L}} \overline{PATH}$?

2. In this problem we let M denote a deterministic Turing machine, w a string, i and j binary integers, and α a member of $Q \cup \Gamma$ where Q is the set of states of M and Γ is its tape alphabet.

   Let $C = \{\langle M, w, i, j, \alpha\rangle |\ \alpha$ is the ith symbol of the configuration after the jth step of the computation of M on input $w\}$.

   Show that C is EXPTIME-complete.

3. Consider the following solitaire game. You are given an $m \times m$ board where each one of the m^2 positions may be empty or occupied by either a red stone or a blue stone. Initially, some configuration of stones is placed on the board. Then, for each column you must remove either all of the red stones in that column or all of the blue stones in that column. (If a column already has only red stones or only blue stones in it then you do not have to remove any further stones from that column.) The objective is to leave at least one stone in each row. Finding a solution that achieves this objective may or may not be possible depending upon the initial configuration. Let

   $$SOLITAIRE = \{\langle G\rangle |\ G \text{ is a game configuration with a solution}\}.$$

   Prove that *SOLITAIRE* is NP-complete.

4. Let $INP = \{\langle M\rangle |\ M$ is a deterministic TM where $L(M) \in \text{P}\}$. In other words, $\langle M\rangle \in INP$ if the language recognized by M is decidable (perhaps by some other TM) in polynomial time. Prove that INP is undecidable.

5. Let $ODD\text{-}PARITY = \{w|\ w \in \{0,1\}^*$ and w contains an odd number of 1s$\}$. Recall that $PATH = \{\langle G, a, b\rangle |$ there is a path from a to b in directed graph $G\}$.

   (a) Prove that there is a log space reduction from $ODD\text{-}PARITY$ to $PATH$, i.e., $ODD\text{-}PARITY \leq_{\text{L}} PATH$.
   (You may use any theorem we have proved in this course)

   (b) No log space reduction from $PATH$ to $ODD\text{-}PARITY$ is known. State what surprising consequence would follow if such a reduction were discovered, and why.

6. Recall the complexity class BPP, containing the languages that can be decided by probabilistic polynomial time Turing machines with error probability $\frac{1}{3}$. In lecture we observed that BPP $\subseteq$ IP and stated that IP = PSPACE. Hence we can conclude that BPP $\subseteq$ PSPACE.

   Here, give a direct proof that BPP $\subseteq$ PSPACE, without using interactive proof systems.

7. In the standard interactive proof system model, the Prover has unlimited computational ability. Define a ***weak Prover*** to be a polynomial-time bounded Turing machine. A weak Prover has access to the input and to the messages that the Verifier sends, but must compute its responses within deterministic polynomial time. Define a ***weak interactive proof system*** to be an interactive proof system where a weak Prover attempts to convince the Verifier to accept. Let ***weak-IP*** be the associated class of languages.

   More precisely, $A \in$ weak-IP if there is a probabilistic polynomial-time Verifier and a weak Prover P such that for any Prover $\widetilde{P}$ (weak or otherwise):
   If $w \in A$ then P causes the Verifier to accept with probability at least $\frac{2}{3}$.
   If $w \notin A$ then $\widetilde{P}$ causes the Verifier to accept with probability at most $\frac{1}{3}$.

   (a) Recall the interactive proof system we gave to show that $\#SAT \in$ IP.
   Is the Prover which follows that protocol a weak Prover? Why or why not?

   (b) The class weak-IP is equal to another class that we have previously defined.
   What is that class? Prove your answer.