The University of North Carolina at Greensboro
CSC 653: Advanced Theory of Computation
Prof. Stephen R. Tate

Handout 12
December 2, 2008

Practice Problems 3

These problems are "practice problems" to prepare for the final exam. There are more problems here than will be on the exam, but they are approximately the same difficulty and depth of the problems that will be on the exam — as a result they are easier than many of the homework problems (where you have time to think about them), but they are also not just "memorize some facts to repeat" questions! Also note that these questions cover just the material since the last exam, but the final will contain some questions over earlier material as well.

Students will work out and present solutions to as many of these problems as we can get to in class on Thursday, December 4, and we will discuss the solutions. Be prepared for that!

1. (Textbook Exercise 8.11) Show that, if every NP-hard language is also PSPACE-hard, then PSPACE = NP.

2. (Textbook Exercise 8.22a) Let $ADD = \{\langle x, y, z\rangle \mid x, y, z > 0$ are binary integers and $x + y = z\}$. Show $ADD \in L$.

3. The simple algorithm for TQBF uses $O(n^2)$ space, meaning that TQBF $\in$ SPACE(n^2). Since TQBF is PSPACE-complete, does this mean that PSPACE $\subseteq$ SPACE(n^2)? Explain your answer.

4. State and prove Savitch's Theorem.

5. (Textbook Exercise 10.5) Show that the majority function with n inputs can be computed by a branching program that has $O(n^2)$ nodes.

6. (Textbook Exercise 10.18) Prove that, if A is a regular language, a family of branching programs $(B_1, B_2, \ldots)$ exists wherein each B_n accepts exactly the strings in A of length n and is bounded in size by a polynomial in n.

7. The class PP is defined as the class of all languages A that have a corresponding probabilistic Turing machine such that

   1. $w \in A$ implies $Pr[M \text{ accepts } w] > \frac{1}{2}$
   2. $w \notin A$ implies $Pr[M \text{ accepts } w] < \frac{1}{2}$

   Show that $NP \subseteq PP$.

8. Define classes RP and BPP and prove that $RP \subseteq NP$ and $RP \subseteq BPP$.

9. Consider a class of languages defined as follows: language A is in this class if there exists a probabilistic Turing machine M such that

   1. $w \in A$ implies $Pr[M \text{ accepts } w] = 1$
   2. $w \notin A$ implies $Pr[M \text{ accepts } w] \leq \frac{1}{2}$

   We haven't studied exactly this class, studied we have studied a related class. What can you say about this new class in terms of languages that we studied? Justify your answer.

10. Give the definition for an interactive proof system. Then describe an interactive proof system for graph non-isomorphism and show that it meets the required properties.

11. Consider an interactive proof system for a language A in which the error probabilities are as high as 0.35, exceeding the maximum $1/3$ allowed in the definition of an interactive proof system (Definition 10.28 on page 389). Show how to convert this interactive proof system into a new system in which the $1/3$ error bound is achieved, showing that $A \in IP$.

12. In homework you showed that randomization was important for the verifier in an interactive proof. For this problem, prove that randomization doesn't make any difference for the prover — specifically, show that the class of languages with interactive proofs using a probabilistic prover is the same as the class of languages with interactive proofs using a deterministic prover.

13. The following 4-by-4 matrix shows a potential operation for a quantum gate — we're trying to make an "AND gate", so have taken two inputs and replaced the second input by the AND of the two inputs, giving the following matrix:

	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$\|00\rangle$	1	1	0	0
$\|01\rangle$	0	0	0	0
$\|10\rangle$	0	0	1	0
$\|11\rangle$	0	0	0	1

   Unfortunately, this is not a valid transition matrix for a quantum gate. Why not? Give both a mathematical reason (what mathematical property does the matrix not satisfy?) and a fundamental physical reason (what physical property do all quantum gates have to satisfy?).

14. Give a valid transition matrix for a quantum gate that takes 3 inputs, $|x\rangle$, $|y\rangle$, and $|z\rangle$, and produces three outputs: $|x\rangle$, $|y\rangle$, and $|z \oplus (x \text{ OR } y)\rangle$

15. Describe Deutsch's Algorithm for determining if a two-input function is constant or balanced. What is the benefit of using quantum gates for this problem?