CPSC 468 Exam
December 6, 2007

Answer five of the following six questions. If you answer all six, the first five of your answers will be graded, and the sixth will be ignored. Please remember to write your name, CPSC 468, and today's date on the covers of all blue books you submit.

Question 1 (20 points)
Recall that the Valiant-Vazirani Lemma shows that restricting the domain of the SAT problem to formulas that are guaranteed to have either 0 or 1 satisfying assignments does not make the problem appreciably easier. More precisely, let φ be a CNF formula. For any predicate Q, the function $USAT_Q(\varphi)$ is defined to be 0 if $\#SAT(\varphi) = 0$, 1 if $\#SAT(\varphi) = 1$, and $Q(\varphi)$ if $\#SAT(\varphi) > 1$. For all Q, there is a probabilistic polynomial-time (ppt) reduction from SAT to $USAT_Q$.

Does the NP-complete HAMPATH problem have the same property? Let G be a graph. For any predicate Q, the function $UHAMPATH_Q(G)$ is defined to be 0 if #HAMPATH(G) = 0 (i.e., if there are no Hamiltonian paths in G), 1 if #HAMPATH(G) = 1, and Q(G) if #HAMPATH(G) > 1. Is there a ppt reduction from HAMPATH to UHAMPATH? Briefly justify your answer.

Question 2

(a) (5 points) Prove that BPP = P if NP = P.

(b) (5 points) Define the complexity classes BPL and RL. Is UPATH in RL?

(c) (10 points) Define the complexity class PP and explain why it is essentially different from BPP.

Question 3
State whether each of the following claims is true, false, or unknown. If you answer true or false, give a very brief justification.

(a) (5 points) There is an O(1)-round interactive proof system for the PERMANENT function.

(b) (5 points) Probabilistic provers are more powerful than deterministic provers.

(c) (5 points) For every L in PH, there is a deterministic polynomial-time reduction from L to parity-SAT.

(d) (5 points) For every L in BPP, there is a deterministic polynomial-time reduction from L to #SAT.

Question 4

(a) (5 points) Recall that dIP is the class of languages recognizable by interactive proof systems with deterministic verifiers and that AM is the class of languages recognizable by public-coin interactive proof systems in which the entire interaction consists of one move by Arthur followed by one move by Merlin. Prove that dIP is contained in AM.

(b) (15 points) Let L = {(G_1, G_2, K) such that the number of isomorphisms from G_1 to G_2 is at least K}. Prove that there is an Arthur-Merlin game in which Arthur accepts (G_1, G_2, K) with high probability if it is in L and rejects (G_1, G_2, K) with high probability if the number of isomorphisms from G_1 to G_2 is at most K/2.

Question 5

(a) (5 points) Recall that Fortnow, Rompel, and Sipser [FRS] proved that MIP, the class of languages accepted by multi-prover, interactive proof systems, is equivalent to the class of languages accepted by ppt oracle Turing Machines. State precisely the [FRS] definition of "L is accepted by ppt oracle Turing Machine M."

(b) (7 points) Prove that MIP $\subseteq$ NEXP.

(c) (8 points) Recall that $\omega(G)$ is the size of the largest clique in G and that, if there is a deterministic polynomial-time algorithm that approximates $\omega(G)$ within a factor of 2, then EXP=NEXP. Give a deterministic exponential-time reduction that maps an instance (x, L) to a graph G_x such that a factor-of-2 approximation of $\omega(G_x)$ enables one to determine easily whether x is in L, where L is an arbitrary language in NEXP. (You need not complete the proof that EXP=NEXP if approximating the clique number is easy; just specify precisely how one constructs the graph G_x.)

Question 6

(a) (5 points) Define the term *parsimonious reduction*.

(b) (10 points) Explain the essential role of a parsimonious reduction in the proof of the Valiant-Vazirani Lemma.

(c) (5 points) (Here the notation "a^b" is used for exponentiation; so "2^(2^i)" denotes "2 to the (2 to the i).")
Let φ be a boolean formula and $\#(\varphi)$ denote the number of satisfying assignments of φ.
Give a boolean formula ψ that satisfies the following two conditions.
(i) If $\#(\varphi) \equiv -1$ (mod 2^(2^i)), then $\#(\psi) \equiv -1$ (mod 2^(2^(i+1))), and
(ii) If $\#(\varphi) \equiv 0$ (mod 2^(2^i)), then $\#(\psi) \equiv 0$ (mod 2^(2^(i+1))).
(You need not prove that ψ satisfies (i) and (ii); just give the formula.)