

CPSC 468/568 Exam
April 26, 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 468/568, and today's date on the covers of all blue books you submit.

Question 1

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) $P^{\#P} = PSPACE$
- (b) (5 points) $BPP \subseteq NP \cup coNP$
- (c) (5 points) $coNP \subseteq IP$
- (d) (5 points) There is a three-round Arthur-Merlin (aka "public-coin") proof system for Graph Non-Isomorphism. (Here, a "round" is a move by Arthur followed by a move by Merlin.)

Question 2

- (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 probabilistic, polynomial-time (ppt) oracle Turing Machines. State precisely the [FRS] definition of "L is accepted by a ppt oracle Turing Machine M."
- (b) (5 points) In MIP, an "oracle" convinces a ppt verifier that a string is in a language. In IP, a "prover" convinces a ppt verifier that a string is in a language. Briefly explain the essential difference between an oracle and a prover.
- (c) (10 points) Recall that Graph Non-Isomorphism is in IP; *a fortiori*, it is in MIP. Prove that Graph Non-Isomorphism is in MIP by giving a ppt oracle Turing Machine that accepts it.

Question 3

- (a) (9 points) For three points each, define the complexity classes RP, coRP, and BPP.
- (b) (11 points) Recall that L is in the class ZTIME(T(n)) if there is a probabilistic Turing Machine M that has expected running time $O(T(n))$ and never errs. That is, for all x in L, M accepts x with probability 1; for all x not in L, M halts with probability 1 without accepting x; and, for all x, the expected running time (where expectation is computed over the coin tosses of M on input x) is $O(T(|x|))$. ZPP is the union, over all polynomials p, of ZTIME(p(n)).
Prove that $ZPP = RP \cap coRP$.

Question 4

Recall that the permanent of an n -by- n , integer-valued matrix A is defined by the formula

$$\text{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^n A_{i, \sigma(i)} \quad (*)$$

- (a) (5 points) For general integer matrices, give an alternative definition of the permanent in terms of cycle covers, and prove that this definition is equivalent to (*).
- (b) (5 points) For 0-1 matrices, give an alternative definition of the permanent in terms of perfect matchings, and prove that this definition is equivalent to (*).
- (c) (10 points) Let “K-permanent” be the restriction of the general integer-permanent problem to instances in which all of the integer entries of the matrix have absolute value at most K . Show that, for any fixed constant K , there is a deterministic, polynomial-time reduction from K-permanent to 0-1 permanent.

Question 5

- (a) (8 points) Define the term *collection of pairwise-independent hash functions that map $\{0, 1\}^n$ to $\{0, 1\}^k$* and give an example of such a collection.
- (b) (6 points) State the Valiant-Vazirani Theorem about randomized reductions of SAT. (Two statements of this theorem were discussed in class; you will get full credit for a correct rendition of either of them.)
- (c) (6 points) Let f be a CNF formula on n boolean variables and w be a vector in $\{0, 1\}^n$. Construct formulas g and h such that (1) g is a formula on n boolean variables whose solutions v are also solutions of the formula f and of the equation $v \cdot w = 0$ (where \cdot is the inner product over the $\text{GF}[2]$) and (2) h is a boolean formula on $x_1, \dots, x_n, y_1, \dots, y_m$ such that there is a bijection between solutions of g and those of h given by equality on the values of x_1, \dots, x_n . (Hint: This construction is a key step in the proof of the Valiant-Vazirani Theorem.)

Question 6

- (a) (10 points) Define the arithmetization over $\text{GF}[p]$ of a 3CNF formula on n boolean variables. How big (as a function of n) does the prime p have to be for this arithmetization to be used in an interactive proof system for the unsatisfiability of 3CNF formulae on n variables?
- (b) (10 points) Define “downward self-reducibility,” and show that the permanent function is downward self-reducible.