CSE 200
Computability and Complexity
Homework 4
Space Complexity and Probabilistic Time Complexity Due June 6

June 4, 2007

Give proofs for each problem. Proofs can be high-level, but be precise. You may use without giving a proof any result proved in class or in the textbook.

Indirect arguments: It is an open problem whether $P \subseteq DSPACE(n)$ and it is also open whether $DSPACE(n) \subseteq P$. Nevertheless, prove that $P \neq DSPACE(n)$. (Hint: show that $DSPACE(n)$ is not closed under polynomial-time reducibility using the Space Hierarchy Theorem, Theorem 9.3, page 337).

2-SAT: The 2-SAT problem is to decide Satisfiability for CNF formulas with at most 2 literals per clause. Prove that $2-SAT$ is $co-NL$-complete (under deterministic logspace many-one reductions). You can use without proof that $PATH$ is NL-complete.

Counting classes Consider the problem of *counting* the number of accepting runs of a non-deterministic Turing machine N on input x. Show that if N uses $O(\log n)$ space, then the associated counting problem is in FP.

Probabilistic complexity : Remember that for complexity class C, P^C is the class of all decision problems poly-time Turing reducible to L for some $L \in C$.

a. Prove that $P^{BPP} = BPP$.

b. Prove that $P^{ZPP} = ZPP$.

c. Prove that $RP = ZPP$ if and only if $P^{RP} = RP$.

Cryptography : A function f is a *one-way permutation* if

1. $|f(x)| = |x|$
2. f is 1-1, $f(x) = f(y) \rightarrow x = y$.
3. $f \in P$
4. For every polynomial-time algorithm A, and every polynomial p, the probability that, for $x \in \{0,1\}^n$ chosen at random, $A(f(x)) = x$, is at most $1/p(n)$ for all sufficiently large n.

Prove that, if $P = NP \cap Co-NP$, then there are no one-way permutations.