Problem Set 4 **CAS705 Fall 2003**

1. All the exercises and problems in Chapter 7.

2. Let A be any language in NP, with verifier V, so that $w \in A$ iff there exists a c (of size polynomial in $|w|$) such that V accepts $\langle w, c\rangle$.

   Show that if P = NP, then if $w \in A$, we can actually computer a certificate c in time polynomial in $|w|$.

3. Show that if f, g are polytime functions, then so is $h = f \circ g$. Use this to show that "$\leq_p$" is transitive; i.e., if $L_1 \leq_p L_2$ and $L_2 \leq_p L_3$, then $L_1 \leq_p L_3$.

4. Suppose that we have a "black-box" algorithm for solving SAT. That is, we have an oracle which on input ϕ answers "yes" or "no," depending on whether ϕ is satisfiable or not. Show how to use this oracle to compute in polytime a satisfying assignment for ϕ (if it is indeed satisfiable).

5. Visit `www.claymath.org` and check-out the MILLENNIUM PRIZE PROBLEMS, the "P vs NP" problem in particular.