Assignment 3 SOLUTIONS **CAS776 Fall 2002** **due on November 14**

In this assignment we show that there exists a proof system for propositional tautologies, where each tautology has a "short" proof, iff NP is closed under complementation. This result was first shown in the seminal paper of Cook and Reckhow, "The relative efficiency of propositional proof system," Journal of Symbolic Logic, Vol 44, Number 1, March 1979.

1. Just note that instances of SAT (formulas in CNF) are a subclass of instances of BOOL (formulas in general form). BOOL is in NP by the same argument that shows that SAT is in NP: there is a nondeterministic TM that that "guesses" a truth assignment to the variables of a formula, and checks in polytime that this truth assignment satisfies it. BOOL is NP-complete, because the same reduction that reduces every NP problem to SAT, reduces every problem to BOOL.

2. Note that $\overline{\text{TAUT}}$ is the set of formulas which are not tautologies, i.e., the set of formulas ϕ such that for some T, $T \nvDash \phi$, or put another way, $\phi \in \overline{\text{TAUT}} \iff \neg\phi \in \text{BOOL}$. From this we see that $\overline{\text{TAUT}}$ is NP-complete. Thus TAUT is co-NP, furthermore, the same reduction f that reduces every L in NP to $\overline{\text{TAUT}}$, reduces every L in co-NP to TAUT.

3. Let L be any language in NP. Let f be the polytime reduction that reduces L to SAT, i.e., $x \in L \iff f(x) \in \text{SAT}$. Define R as follows: given x, y, $R(x, y)$ is true iff y is a truth assignment to $f(x)$ that satisfies $f(x)$. Note that $f(x)$ can be computed in polytime in $|x|$ (so $|f(x)| \leq p(|x|)$ for some polynomial p), and y is just a string of 0s and 1s encoding the truth assignment (e.g., if a_1, a_2, a_3 are the variables of $f(x)$, then $y = 001$ sets a_1, a_2 to 0 and a_3 to 1), so $|y| \leq |f(x)| \leq p(|x|)$.

4. Suppose that NP=co-NP. Then, by the previous question, there exists a polytime predicate R and a polynomial p such that $x \in \text{TAUT} \iff \exists y(|y| \leq p(|x|) \wedge R(x, y))$. Just let $V = R$, and we have our polybounded proof system.

   Conversely, suppose that we have a polybounded proof system V. Then let $R = V$, and we are also done.

5. If P=NP, then NP=co-NP (since P is closed under complementation). Taking the contrapositive, we have that if NP$\neq$co-NP, then P$\neq$NP. But, if there is no polybounded propositional proof system, then NP$\neq$co-NP.