Assignment 3 **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. Let L, L' be languages. We say that L' is polytime reducible to L, write $L' \leq_p L$, if there exists a polytime function f such that $x \in L' \iff f(x) \in L$.

   A language L is NP-complete if it is in NP, and for all $L' \in \text{NP}$, $L' \leq_p L$.

   Cook's Theorem: SAT is an NP-complete language.

   Define BOOL to be the language of satisfiable boolean formulas. Using Cook's Theorem, show that BOOL is also an NP-complete language.

2. Let co-NP $= \{\overline{L} | L \in \text{NP}\}$. Show that TAUT $= \{\tau | \tau \text{ is a tautology}\}$ is co-NP-complete; that is, show that TAUT is in co-NP, and every co-NP language is polytime reducible to TAUT.

3. Show that $L \in \text{NP}$ iff there exists a polytime predicate R and a polynomial p, such that $x \in L \iff \exists y(|y| \leq p(|x|) \wedge R(x,y))$. That is, $x \in L$ iff there exists a *certificate* y, of length bounded by a fixed polynomial in $|x|$, such that $R(x,y)$ holds. (Note that "$R(x,y)$ is a polytime predicate" means that there exists a polytime TM M_R such that $M_R(x,y)$ accepts iff $R(x,y)$ holds.)

4. We say that the polytime predicate V is a propositional proof system for TAUT, if the following holds: $\tau \in \text{TAUT} \iff \exists p V(p,\tau)$. That is, p is the *proof* of τ.

   We say that V is polybounded, if there exists a fixed polynomial r, such that $\tau \in \text{TAUT} \iff \exists p(|p| \leq r(|\tau|) \wedge V(p,\tau))$; that is, τ has a proof in the system V of length at most $r(|\tau|)$. Show that a polybounded propositional proof system exists iff NP=co-NP.

5. Show that NP $\neq$ co-NP implies that P $\neq$ NP. Thus, if one could show that no polybounded proof system exists, it would follow that P $\neq$ NP.