Assignment 3 **CAS705 Fall 2005** **Due on October 24**

The work you submit must be your own. *You may discuss problems with each other; however, you should prepare written solutions alone. In particular, you should not leave with any written notes from such discussions. The style and clarity of your answers will be an important factor in the grade.*

Each question is worth 20%.

1. Suppose that the language L has a polybounded proof system V, and suppose that $\mathbf{P} = \mathbf{NP}$. Show then that there exists a polytime function f, such that for every $x \in L$, $V(x, f(x))$ holds, and for $x \notin L$, $f(x) =$ "I'm very sorry, no luck this time". In other words, if $x \in L$, then $f(x)$ outputs in polytime (in $|x|$) a proof of membership, and if $x \notin L$, then f says so.

2. We say that a propositional proof system V is *automatizable*, if there exists an algorithm A, such that given a ϕ in TAUT as input, A outputs a proof p of ϕ in time polynomial in the length of the shortest proof of ϕ. Show that a polybounded automatizable PPS exists iff $\mathbf{P} = \mathbf{NP}$.

3. We can go back and forth between a clausal representation of a formula and its CNF in the obvious way. Now what about:

   (a) Suppose that you are given a general boolean formula ϕ (not necessarily in CNF); show how to translate ϕ (in polynomial time) into a formula in CNF ϕ' such that ϕ is satisfiable iff ϕ' is satisfiable. What is the consequence of this little result for resolution?

   (b) Suppose that you managed to do (a) *without* introducing any new variables; what would be the consequence of that for propositional proof systems?

4. Let **BF** be the class of languages recognizable by a family of polynomial size Boolean Formulas. That is, $L \in \mathbf{BF}$ iff $\exists\, \phi_1, \phi_2, \phi_3, \ldots$, where ϕ_i has i variables, and a polynomial p such that $|\phi_i| \leq p(i)$, and

   $$w \in L \iff \phi_{|w|}(w_1, w_2, \ldots, w_n) \text{ is true}$$

   Show that $\mathbf{NC}^1 = \mathbf{BF}$.

5. Extended Resolution (ER) is define as the usual Resolution PPS, together with the extension rule which allows us to abbreviate formulas by new variable names. That is, we allow the introduction of new variables v_{new}, and a definition $v_{\text{new}} \equiv \alpha$; now we can refer to α by the new name v_{new}. Using your ideas in 3(a) give a clausal form for $v_{\text{new}} \equiv \alpha$. Show that ER proves PHP_n^{n+1} in polynomial size. (Give an outline of the method, not the details of the proof!)