**Take Home Exam** **Due: Dec 11** **CAS705 Fall 2013**

(*revised Nov 29, 2013*)

1. Let $\alpha, \beta$ be two Boolean formulas (over the set of connectives $\{\wedge, \vee, \neg\}$) such that $\alpha \to \beta$ is a tautology. Let $\mathrm{Var}(\phi)$ be the set of variables in $\phi$; for example, if $\phi$ is $x_1 \vee (\neg x_3 \wedge x_5)$, then $\mathrm{Var}(\phi) = \{x_1, x_3, x_5\}$.

   Show that there always is a formula $\gamma$ such that $\mathrm{Var}(\gamma) \subseteq \mathrm{Var}(\alpha) \cap \mathrm{Var}(\beta)$, and such that $\alpha \to \gamma$ and $\gamma \to \beta$ are both tautologies.

2. Given Boolean a Boolean formula $\alpha$:

   - let $|\alpha|$ be the *length* of $\alpha$, that is, $|\alpha|$ counts the number of symbols in $\alpha$. Note that each connective and each parenthesis count as 1, but variables count as more than 1: a variable is always of the form $p1101$, i.e., they are indexed in binary.
   - let $\mathrm{size}(\alpha)$ be the *size* (in terms of number of gates) of the smallest Boolean *circuit* (over $\{\wedge, \vee\neg\}$) that computes $\alpha$.

   Finally, let

   $$\min\{\alpha, \beta\} = \min\{\mathrm{size}(\gamma) : \alpha \to \gamma \text{ and } \gamma \to \beta\},$$

   and let

   $$\delta(n) = \max\{\min\{\alpha, \beta\} : |\alpha| = |\beta| = n\},$$

   where we are of course interested in the case where $\alpha \to \beta$ is a tautology.

   Show that $\delta(n)$ is bounded above by $O(2^n)$, assuming that a formula of length $n$ cannot have more than $O(n/\log n)$ variables — why is this assumption reasonable?

3. Use Cook's Theorem to argue that if $L$ is in **NP**, then there exists a polynomial $p(n)$ and a family of Boolean formulas $\{\alpha_n\}$, which can be generated in polynomial time in $1^n$, such that:

   $$x \in L \cap \{0,1\}^n \iff \exists y \alpha_n(x, y) \text{ is true}$$

   where $x = x_1, x_2, \ldots, x_n$ and $y = y_1, y_2, \ldots, y_{p(n)}$.

4. Suppose now that $L \in \mathbf{NP} \cap \mathbf{co\text{-}NP}$. Then, we can repeat what we did in the previous question for both $L$ and $L^c$. Let $\{\alpha_n\}$ and $\{\beta_n\}$ be the families corresponding to $L, L^c$, respectively. Show that $\alpha_n \to \neg\beta_n$ are tautologies for all $n$.

5. Let $C_n$ be the smallest Boolean circuit that computes $\gamma_n$ for $\alpha_n \to \neg\beta_n$. Observe that if $\delta(n)$ were polynomially bounded, then $|C_n| \leq q(n)$, for some fixed polynomial $q(n)$.

6. Show that if $\delta(n)$ were polynomially bounded, then any pair of disjoint languages $L_1, L_2$ in **NP** is, what we call, PC-separable, meaning that there exists a language $C$ in $\mathbf{P}/\mathrm{poly}$ such that $L_1 \subseteq C$ and $C \subseteq L_2^c$.

7. Conclude from the previous problem that if $\delta(n)$ were polynomially bounded, then all languages in $\mathbf{NP} \cap \mathbf{co\text{-}NP}$ are in $\mathbf{P}/\mathrm{poly}$.

8. Conclude that if $\delta(n)$ is not polynomially bounded, then $\mathbf{P} \neq \mathbf{NP}$.