**Due: Thursday October 20, 2005**

1. A function $f$ is $m$-enumerable if there exists a polynomial-time computable function $g$ such that for all $x$, $g(x) = \langle y_1, \ldots, y_m \rangle$ and $f(x) \in \{y_1, \ldots, y_m\}$. I.e., $g$ generates $m$ possible outputs and one of them is $f(x)$.

   Now, define $\chi_5^{\mathrm{SAT}}$ as follows:

   $$\chi_5^{\mathrm{SAT}}(\phi_1, \phi_2, \phi_3, \phi_4, \phi_5) = d_1 d_2 d_3 d_4 d_5$$

   where each $d_i \in \{0, 1\}$ and $d_i = 1 \iff \phi_i \in \mathrm{SAT}$. Note that $\chi_5^{\mathrm{SAT}}$ is trivially 32-enumerable. Show that if $\chi_5^{\mathrm{SAT}}$ is 5-enumerable, then $\mathrm{P} = \mathrm{NP}$ using tree pruning, the self-reducibility of SAT and the following combinatorial lemma:

   **Lemma:** Given $\ell$ distinct bit vectors $b_1, \ldots, b_\ell$ each with $j$ bits, where $\ell \leq j$, there exists a coordinate $k$ such that the bit vectors can be distinguished without using the $k$-th coordinate.

   *Hint:* During the tree-pruning of the self-reduction tree of a formula $\phi$, if $g(\phi_1, \phi_2, \phi_3, \phi_4, \phi_5)$ does not contain the bit vector 00000, where the $\phi_i$'s are descendants of $\phi$ in the self-reduction tree for $\phi$, then you already know that $\phi \in \mathrm{SAT}$.

2. For a class of languages $\mathcal{C}$, we define $\exists\cdot\mathcal{C}$ and $\mathrm{BP}\cdot\mathcal{C}$ as follows:

   **Defn:** $L \in \exists\cdot\mathcal{C}$ if there exists a language $A \in \mathcal{C}$ and a polynomial $p()$ such that

   $$x \in L \iff \exists y,\ |y| = p(|x|) \text{ and } \langle x, y \rangle \in A.$$

   **Defn:** $L \in \mathrm{BP}\cdot\mathcal{C}$ if there exists a language $A \in \mathcal{C}$ and a polynomial $p()$ such that

   $$x \in L \Longrightarrow \mathrm{Prob}_y[\langle x, y \rangle \in A] \geq 2/3$$

   $$x \notin L \Longrightarrow \mathrm{Prob}_y[\langle x, y \rangle \in A] \leq 1/3$$

   where $y$ is chosen uniformly at random from strings with length $p(|x|)$.

   Observe that if $\mathcal{C} = \mathrm{P}$ then $\exists\cdot\mathrm{P} = \mathrm{NP}$ and $\mathrm{BP}\cdot\mathcal{C} = \mathrm{BPP}$.

   Prove that $\exists\cdot\mathrm{BP}\cdot\mathrm{P} \subseteq \mathrm{BP}\cdot\exists\cdot\mathrm{P}$.

   Justify any amplification claims you make (but you do not have to reprove the Chernoff bounds). Also, when you claim that you have a $\mathrm{BP}\cdot\exists\cdot\mathrm{P}$ machine $M$ for some language $L \in \exists\cdot\mathrm{BP}\cdot\mathrm{P}$, make sure you prove both directions of $L \subseteq L(M)$ and $L(M) \subseteq L$.

   Does your proof work for $\mathrm{BP}\cdot\exists\cdot\mathrm{P} \subseteq \exists\cdot\mathrm{BP}\cdot\mathrm{P}$? Why or why not?