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 $\chi_{SAT}^5$ as follows:

$\chi_{SAT}^5(\phi_1, \phi_2, \phi_3, \phi_4, \phi_5) = d_1d_2d_3d_4d_5$

where each $d_i \in \{0, 1\}$ and $d_i = 1 \iff \phi_i \in SAT$. Note that $\chi_{SAT}^5$ is trivially 32-enumerable.

Show that if $\chi_{SAT}^5$ is 5-enumerable, then $P = NP$ 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 $\phi \in SAT$.

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

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

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

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

$x \in L \implies \text{Prob}_{y}[(x, y) \in A] \geq 2/3$

$x \notin L \implies \text{Prob}_{y}[(x, y) \in A] \leq 1/3$

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

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

Prove that $\exists \cdot BP \cdot P \subseteq BP \cdot \exists \cdot P$.

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

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