CSC 2401F 2008, Assignment 3
Due: December 9

1. Show that the LP decision problem is hard for $\mathcal{P}$ (with respect to some efficient reduction such as $\leq_{log}$.) That is, show that for every $L \in$P, $L \leq_{log} LP$.
   Hint: Use the fact that $CIRCUIT - VALUE$ is hard for $\mathcal{P}$.

2. Prove that there exists a language $L \in EXPSPACE$ such that $L \notin SIZE(2^{o(n)})$.
   Hint: It is more interesting to note and probably easier to prove that there is such an $L \in EXPSPACE$ which cannot be computed in $SIZE(M(n)-1)$ where $M(n)$ is defined to be the maximum size needed to compute all n variable Boolean functions.

3. Our definition of a probabilistic Turing machine (PTM) and the resulting randomized complexity classes assumed that there are (at most) two possible transitions $\delta(q, \sigma, \gamma_1, \ldots, \gamma_k)$ for any setting of the state and symbols on the input and work tapes. Suppose now that a k-tape PTM has at most 3 (uniformly chosen) possible transitions for any setting of the state and symbols on the input and work tapes. Show that the classes BPP, RP and ZPP remain the same.

4. Consider the proof that EQ_{ROBP} is in BPP as presented in Sipser (Theorem 10.13). Explain why this proof fails for arbitrary branching programs. Be as specific as possible as to where in the proof something does not hold when considering arbitrary (not read once) branching programs.

5. This problem is optional and mainly for those who want an opportunity to raise their grade.
   Consider the Hamiltonian cycle (HC) problem. That is, Given $G = (V, E)$ determine if G has a Hamiltonian cycle. Give a ZKIP for HC and informally argue that the proof is indeed zero knowledge.
   Hint: Consider a random isomorphism $\phi(G) = (V, \phi(E))$ where $\phi(E) = \{(\phi(u), \phi(v))|(u, v) \in E\}$. What can be said about a Hamiltonian cycle in $\phi(G)$?