Computer Algorithms **Caltech CS138b, Fall 2001**
Leonard J. Schulman **Problem Set # 11, January 25, 2001**
Due Friday February 2 at 4pm in the box in the VLSI lab

1. **(10 points)** Show that if there exists a pseudo-random generator A mapping $\{0,1\}^m \to \{0,1\}^{m+1}$ then, for all $c > 1$, there is a pseudo-random generator B mapping $\{0,1\}^m \to \{0,1\}^{m^c}$.

2. **(5 points)** Prove that if $X_1, ...X_n$ are independent random variables then they are pairwise independent.

3. **(10 points)** Let n be balls be independently and uniformly tossed into n bins. Show that the expected number of unoccupied bins approaches n/e in the limit of large n.

4. **(10 points)** Show that **NP** $\subseteq$ **BPP** implies **NP** = **RP** .

   Hint: Recall that a language in **NP** is characterized by the fact that every $x \in$ **NP** has at least one "witness" y, such that the poly-time verification procedure accepts the pair (x, y). Use the **BPP** algorithm to figure out, one-by-one (though only with high reliability), the bits of the witness.