Exercise Sheet 3

This is the third of three sets of assessed exercises. It represents 20% of the continuously assessed component of the course (which in turn accounts for 25% of the overall credit for the course). The deadline for submission of solutions is 16:30, Friday 28th March. Please hand your solutions to ITO (Appleton Tower, Room 4.02).

The questions are not necessarily in increasing order of difficulty.

1. Show that if $\mathsf{NP} \subseteq \mathsf{BPP}$, then $\mathsf{NP} = \mathsf{RP}$. HINT: Use the downward self-reducibility of SAT to eliminate error on NO instances.

2. Indecisive Turing machines are Turing machines which, in addition to accepting and rejecting states, have a "don't know" state in which the computation may terminate. A language L is said to be in ZPP (zero-error probabilistic polynomial time) if there is an indecisive randomized Turing machine M halting in polynomial time such that:

   (a) If $x \in L$, M does not halt in a rejecting state on *any* computation path (it halts either in an accepting state or the "don't know" state), and it halts in an accepting state with probability at least $1/2$.

   (b) If $x \notin L$, M does not halt in an accepting state on *any* computation path (it halts either in a rejecting state or the "don't know" state), and it halts in a rejecting state with probability at least $1/2$.

   Prove that $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.

3. $\mathsf{PCP}[r(n), q(n)]$ is the class of languages accepted by probabilistically checkable proof systems where the verifier uses at most $r(|x|)$ random bits and makes at most $q(|x|)$ non-adaptive queries to the proof on any input x. Show that $\mathsf{PCP}[0, \log(n)] = \mathsf{P}$.

Rahul Santhanam, March 2014