Theory Qual
Spring 2016

Directions. You have four hours. There are 4 problems. Please do them all. If you cannot completely solve a problem, we will award partial credit for work that is correct and relevant to the question.

1. Let $\mathbf{Z}_3 = \{0, 1, 2\}$ denote the integers mod 3. An *arithmetic circuit* is just like a Boolean circuit, except that it uses values from $\mathbf{Z}_3$, and the nodes can do addition, subtraction, or multiplication in $\mathbf{Z}_3$. We also allow nodes with constant values.

   Show that the following problem is NP-complete:

   Instance: An arithmetic circuit C, and a "target" value t.

   Question: Can the input variables be set so as to make C evaluate to t?

2. This problem is concerned with Boolean functions, that is, functions from $\{0,1\}^n$ to $\{0,1\}$. A *certificate* is a partial assignment that is sufficient to determine the value of the function. For example, the certificates for x OR y are:

$$\begin{array}{cccccccc} x & = & 0 & 0 & 1 & 1 & 1 & - \\ y & = & 0 & 1 & 0 & 1 & - & 1 \end{array}$$

   a) Let $N(f)$ be the minimum number of certificates necessary to completely specify the Boolean function f. Determine $\max_f\{N(f)\}$, where the max is taken over all n-variable Boolean functions.

   b) Suppose you have an oracle that, when presented with a partial assignment, tells you whether that partial assignment is a certificate for f or not. You have no other access to f. In particular, the oracle does not tell you the value taken by f.

      The oracle allows one to determine f up to some symmetry. What is that symmetry?

   c) Give an algorithm to determine f up to that symmetry using as few oracle queries as possible in the worst case. You do not need to argue the optimality of your algorithm.

3. You are given a tree with a root that is colored red or blue with equal probability. Consider the following random process for coloring the remaining nodes of the tree red or blue. At step $i \geq 1$ all nodes at distance i from the root are assigned colors; the color of each node is chosen independently to be the same color as its parent with probability $1 - \delta$ and the opposite color with probability δ.

   a) Determine the probability that a given vertex in the tree is colored red conditioned on the root being colored red.

   b) Suppose that you are given the coloring assigned to all of the leaves in the tree at the end of the above process. Give an efficient algorithm to compute the conditional probability that the root is colored red. You may assume that the degree of every node is bounded by a constant, b.

4. Recall that a strong hierarchy theorem for randomized computations with bounded error is open. In this problem you'll show that such a theorem holds under the hypothesis that NP is in BPP.

   Let BPTime(t) represent the class of languages that can be decided by randomized machines with bounded two-sided error that run in time $O(t)$.

   a) Show that if NP $\subseteq$ BPP then

   $$\text{For every real } c \geq 1, \text{ BPTime}(n^c) \subset \text{BPP}. \qquad (*)$$

   (We write $A \subset B$ for strict containment.)

   b) Show that (*) implies that for all reals c and d with $1 \leq c < d$, BPTime(n^c) $\subset$ BPTime (n^d).