CS 262: Computational Complexity *Instructor: Sandy Irani*

Homework 5

Due: May 23, 2018

1. Let f be a family of one-way permutations, and let $b = \{b_n\}$ be a hard bit for f^{-1}. Assume that both f and b are computable in polynomial time. Use f and b to describe a language L for which $L \in (\mathbf{NP} \cap \mathbf{coNP}) - \mathbf{BPP}$.

   (This shows that the assumption we used to construct the BMY pseudo-random generator placed *a priori* bounds on the power of **BPP** – it presumed that **BPP** was not powerful enough to simulate $\mathbf{NP} \cap \mathbf{coNP}$.)

2. Consider the following problem. An instance of the problem is a pair $(\Phi, 1^B)$, where Φ is a Boolean expression in disjunctive normal form and B is an integer. $(\Phi, 1^B)$ is in the language if there is a Boolean expression that is equivalent to Φ that is in conjunctive normal form and has at most B clauses.

   Recall that a Boolean expression is in disjunctive normal form, if it is the disjunction of a set of terms, where each term is a conjunction of literals. A Boolean expression is in conjunctive normal form, if it is the conjunction of a set of clauses, where each clause is a disjunction of literals.

   Show that the language described in in Σ_2.

3. Show that if $\mathbf{NP} \subseteq \mathbf{TIME}(n^{\log n})$, then $\mathbf{PH} \subseteq \cup_{k \geq 1} \mathbf{TIME}(n^{\log^k n})$.

4. Recall the definition of QSAT:

$$\text{QSAT } = \{\Phi(x_1, \ldots, x_n) \mid \exists x_1 \forall x_2 \ldots \forall x_n \Phi(x_1, \ldots, x_n) = 1\},$$

   where Φ is a 3-CNF formula. Show that $P^{QSAT} = NP^{QSAT}$.