Undergraduate Complexity Theory **CMU 15-455, Spring 2017**

HOMEWORK 11

Due: 5:00pm, Thursday May 4

Feature: As before, if your homework is typeset (as opposed to handwritten), you will receive 1 bonus point.

1. **(Two-sided error doesn't help for NP.)** (10 points.) Prove $\mathsf{NP} \subseteq \mathsf{BPP} \implies \mathsf{NP} \subseteq \mathsf{RP}$. (Hint: you will probably need the error-reduction fact mentioned in Problem 4.)

2. **(Lex-first assignment, with a SAT oracle.)** (10 points.) Prove that there exists a polynomial-time SAT-oracle algorithm with the following property: On input a Boolean formula ϕ on variables $x_1, \dots, x_n$, the machine (correctly) outputs either: (i) "ϕ is unsatisfiable"; or (ii) the lexicographically first satisfying assignment. (This refers to the ordering $x = (0, \dots, 0, 0), (0, \dots, 0, 1), (0, \dots, 1, 0), \dots, (1, \dots, 1, 1)$.)

   Remark: We can't literally say this problem is in P^{NP} because it's a function problem, not a decision problem. It's possible to artificially convert it to a decision problem; e.g., "accept if and only if ϕ is satisfiable and the last bit of its lexicographically first satisfying assignment is a 1". In such a decision form, this problem is known to be *complete* for P^{NP}!

3. **(This problem has nothing to do with computational complexity.)** Given $S \subseteq \{0,1\}^m$ and $u \in \{0,1\}^m$, we define the *shift of S by u* to be the set

   $$u \oplus S = \{u \oplus x : x \in S\},$$

   where $\oplus$ denotes bitwise-XOR. Reminder: $\oplus$ has the property that $u \oplus x = z$ if and only if $u = x \oplus z$, and hence doing "$u\oplus$" gives a permutation on all strings in $\{0,1\}^m$.

   Fix a parameter $2 \le n \le m$. In the remainder of the problem, we will only consider sets S of one of two kinds: We say S is *tiny* if $|S| \le 2^{-n} \cdot 2^m$, and *huge* if $|S| \ge (1 - 2^{-n}) \cdot 2^m$.

   We are interested in the following question: Do there exist m strings $u_1, \dots, u_m \in \{0,1\}^m$ such that the associated shifts of S *cover* $\{0,1\}^m$? By this we mean:

   $$\forall z \in \{0,1\}^m \quad \exists 1 \le i \le m \quad \text{such that } z \in u_i \oplus S. \qquad (*)$$

   (a) (2 points.) Assuming $n > \log_2 m$, show that when S is tiny, there do *not* exist $u_1, \dots, u_m$ such that $(*)$ holds.

   (b) (8 points.) Show that when S is huge, there *do* exist $u_1, \dots, u_m$ such that $(*)$ holds. In fact, show that if $u_1, \dots, u_m$ are chosen at random, the probability that $(*)$ fails is very small. (Hint: union bound.)

4. **(BPP in the hierarchy.)**

   (a) (8 points.) Let $L \in \mathsf{BPP}$. As described in Lecture 22, there is a simple error reduction strategy (repeat-many-times-and-take-majority-answer) that lets us conclude the following: There is a polynomial-time randomized Turing Machine A with the following properties:

   $$x \in L \implies \mathbf{Pr}[A \text{ accepts } x] \ge 1 - 2^{-n}, \qquad x \notin L \implies \mathbf{Pr}[A \text{ accepts } x] \le 2^{-n},$$

   where $n = |x|$. Using this fact, and also Problem 3, show that $L \in \mathsf{PH}$. At the very least you should get $L \in \Sigma_3\mathsf{P}$; for full credit, you should get $L \in \Sigma_2\mathsf{P} \cap \Pi_2\mathsf{P}$.

   (b) (2 points.) Show that $\mathsf{BPP} \ne \mathsf{P} \implies \mathsf{NP} \ne \mathsf{P}$ (as stated in Lecture 22).