CSE696, Spring 2019 **Problem Set 2** **Due Thu. 4/11**

Reading:

We are into Chapter 8 of the Arora-Barak text on Interactive Proofs. There will then be selections from chapters 9–11 (including quantum) and 20 (on de-randomization).

(1) Given $0 < a < b < 1$, define $\mathsf{BPP}_{a,b}$ to be the class of languages L such that for some polynomial $p(n)$ and predicate $R(x, y)$ decidable in $p(|x|)$ time, and all x:

$$x \in L \implies \Pr_y[R(x, y)] \geq b;$$
$$x \notin L \implies \Pr_y[R(x, y)] \leq a.$$

(Here I've left tacit that y ranges over $\{0, 1\}^{p(|x|)}$.) Show that $\mathsf{BPP}_{a,b} = \mathsf{BPP}$. But now for the real question: Suppose a and b depend on n. Most in particular, suppose $q(n)$ and $q'(n)$ are polynomials such that $a(n) = 1/q(n)$ and $b(n) = a(n) + 1/q'(n)$. Then when you do some number $t(n)$ of trials to amplify the success probability, do you get a higher power of $q(n)$ versus $q'(n)$, or are they about the same? (21 pts. total)

(2) Show that for any two functions $f, g \in \#\mathsf{P}$—using the same bounding polynomial $p(n)$ but different relations $R_f(x, y)$ and $R_g(x, y)$—the functions $h(x) = f(x) + g(x)$, $h'(x) = f(x) * g(x)$, and $h_k(x) = \binom{h(x)}{k}$ for any fixed k are also in $\#\mathsf{P}$. In each case, what is the new bounding polynomial $p'(n)$ that you get? Then given any $f \in \#\mathsf{P}$ with bounding polynomial q, define:

$$h''(x) = \begin{cases} 2^{q(|x|)} & \text{if } f(x) = 0 \\ f(x) - 1 & \text{if } f(x) \neq 0. \end{cases}$$

Can you show that h'' belongs to $\#\mathsf{P}$? If not, what fails? Show that if h'' always belongs to $\#\mathsf{P}$, then the class US equals $\mathsf{co\text{-}NP}$. (A language L belongs to US iff for some $f \in \#\mathsf{P}$, $L = \{x : f(x) = 1\}$. 6+6+6+12 = 30 pts.)

(3) Now define $\mathcal{G}$ to be the class of functions h such that for some $f, g \in \#\mathsf{P}$, and all x, $h(x) = f(x) - g(x)$. We will see later that BQP reduces to one call to a a function in $\mathcal{G}$. Show that $\mathcal{G}$ is closed under all the operations in problem (2), indeed under simple difference $h''(x) = h(x) - h'(x)$. (24 pts. total)

(4) Show that if $\mathsf{US} \subseteq \mathsf{BPP}$, then $\mathsf{NP} = \mathsf{RP}$. (21 pts. total)

(5) (An alternate proof of the first part of Toda's Theorem): Let $K = 2^{q(n)}$ and $N = 2^{r(n)}$ where $r(n)$ is the number of random bits the $\mathrm{BP} \cdot \oplus\mathsf{P}$ machines we are building will be allowed. Say that a $K \times N$ matrix G with 0-1 entries is *good* if:

- Any given entry $G[i, j]$ can be computed in time polynomial in $q(n) + r(n)$—note that this is the length of i as a $q(n)$-bit number plus that of j as an $r(n)$-bit number.
- For every i, $1 \leq i \leq K$, row i has at least $N/8$ 1's. Moreover, so does every N-vector obtained by XOR-ing any subset S of the rows of G.

Take for granted that there exist families $[G_n]$ of good matrices for any polynomials $q(n)$ and $r(n)$, which by the first condition gives polynomial time in n overall. Indeed, they can be built with $G_n[i, j]$ computable in time $(q(n) + r(n))$ times a polynomial in $\log n$. Use this to show $\mathsf{NP} \subseteq \mathsf{RP}[\oplus\mathsf{P}]$. Compare the efficiency of the reduction in terms of $q(n)$ and $r(n)$ with the reductions given in the text and/or in lecture. (30 pts., for 126 total on the set)