cs579: Computational Complexity	Assigned: *Mon., Feb. 19, 2018*
Problem Set #3	
Prof. Michael A. Forbes	Due: *Mon., Mar. 5, 2018 (3:30pm)*

1. Define $\mathsf{FACTORING} = \{\langle a, b, n\rangle : n \text{ has a prime factor in the interval } [a, b]\}$. For this problem you may assume that there is a deterministic polynomial time primality test, that is, $\mathsf{PRIMES} \in \mathsf{P}$, so that primality of a number n can be decided in $\mathsf{poly}(\lg n)$ time as a number n is represented by $O(\lg n)$ bits. Show that

   (a) If you can factor integers deterministically in polynomial time, then $\mathsf{FACTORING} \in \mathsf{P}$.

   (b) If $\mathsf{FACTORING} \in \mathsf{P}$, then you can factor numbers deterministically in polynomial time.

   (c) Show that $\mathsf{FACTORING} \in \mathsf{NP} \cap \mathsf{coNP}$.

   (d) Show that if $\mathsf{FACTORING}$ is NP-hard then $\mathsf{NP} = \mathsf{coNP}$ and hence the polynomial hierarchy collapses to $\mathsf{PH} = \mathsf{NP}$.

   Thus, the above suggests that even though factoring integers is not known to be in P, it is also not expected to be NP-hard. As such, $\mathsf{FACTORING}$ is a candidate NP-intermediate problem (which unconditionally (under $\mathsf{P} \neq \mathsf{NP}$) exist due to Ladner's Theorem).

2. Show that if $\mathsf{NP} \subseteq \mathsf{BPP}$ then $\mathsf{NP} = \mathsf{RP}$.

3. (Multiplicative Chernoff Bound). Let $\mathsf{X}_1, \ldots, \mathsf{X}_n$ be independent random variables taking values over $[0, 1]$. Let $\mathsf{X} = \sum_i \mathsf{X}_i$. Show that

   (a) For $r \in (-\infty, \ln 2]$, prove that $\mathbb{E}[e^{r\mathsf{X}}] \leq e^{r\mathbb{E}[\mathsf{X}]+r^2\mathbb{E}[\mathsf{X}]}$, where you may use-without-proof that $1 + x \leq e^x \leq 1 + x + x^2$ for such r.

   (b) Explain how the above used the independence of the X_i.

   (c) Apply Markov's inequality ($\Pr[\mathsf{Y} \geq a] \leq \mathbb{E}[\mathsf{Y}]/a$) to $e^{r\mathsf{X}}$, and optimize over r, to conclude that

      i. For $0 \leq \epsilon \leq \ln 4$, $\Pr[\mathsf{X} \geq (1+\epsilon)\mathbb{E}[\mathsf{X}]] \leq e^{-\epsilon^2\mathbb{E}[\mathsf{X}]/4}$

      ii. For $\epsilon \geq \ln 4$, $\Pr[\mathsf{X} \geq (1+\epsilon)\mathbb{E}[\mathsf{X}]] \leq 2^{-\epsilon\mathbb{E}[\mathsf{X}]/2}$

      iii. For $0 \leq \epsilon \leq 1$, $\Pr[\mathsf{X} \leq (1-\epsilon)\mathbb{E}[\mathsf{X}]] \leq e^{-\epsilon^2\mathbb{E}[\mathsf{X}]/4}$

      iv. (Additive Chernoff Bound) For $\epsilon \geq 0$, $\Pr[|\mathsf{X} - \mathbb{E}[\mathsf{X}]| \geq \epsilon \cdot n] \leq 2e^{-\epsilon^2 n/4}$

   Note that the additive Chernoff bound suffices for BPP amplification, but the multiplicative bound is in general stronger and sometimes needed (e.g. consider $\mathbb{E}[\mathsf{X}] = \lg n$ and the resulting bound for $\Pr[\mathsf{X} \geq 2\mathbb{E}[\mathsf{X}]]$).

4. (Arora-Barak Problem 6.5) Show that for every constant $c \geq 1$ there is a language in PH that requires circuits of size $\Omega(n^c)$.

Some hints.

4. Where have we seen languages that require large circuits? How can I debate you to prove I am computing such a language? What if there are multiple such languages? Obtain such a language in $\Sigma^4\mathsf{P}$.