cs579 Computational Complexity Assigned: *2021-10-07 (Thu.) 12:00pm*

Problem Set #4

Prof. Michael A. Forbes Due: *2021-10-21 (Thu.) 12:00pm*

All problems are of equal value.
Note: there are hints on the last page, for those who want them.

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

2. (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 $\Pr[\mathsf{X} \geq 2\mathbb{E}[\mathsf{X}]]$).

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

4. Show that $\mathsf{TIME}\left(2^{n^{O(\lg n)}}\right) \not\subseteq \mathsf{P/poly}$.

Some hints.

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

4. Use the proof of the circuit size hierarchy theorem, and ideas similar to those arising in problem 3. When does asymptotic behavior kick in?