cs579 Computational Complexity

Problem Set #4

Prof. Michael A. Forbes — Due: *Thu., 2023-10-26 12:00*

All problems are of equal value.

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 $\mathbb{E}[\mathrm{e}^{r\mathsf{X}}] \le \mathrm{e}^{r\mathbb{E}[\mathsf{X}] + r^2\mathbb{E}[\mathsf{X}]}$. You may use without proof that $1 + x \le \mathrm{e}^x$ for all $x \in \mathbb{R}$, and that $\mathrm{e}^x \le 1 + x + x^2$ for $x \le \ln 2$.

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

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

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

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

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

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

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

3. There are various ways to define a *randomized* version of NP. One definition is that of *Merlin-Arthur* proofs, where Merlin is a powerful (but untrusted) wizard who needs to convince a skeptical mortal (Arthur) that a statement is true. The complexity class MA is defined by a randomized polynomial-time TM M, such that

$$x \in L \implies \exists y \in \{0,1\}^{\mathsf{poly}(n)} \Pr[M(x,y) = 1] = 1,$$
$$x \notin L \implies \forall y \in \{0,1\}^{\mathsf{poly}(n)} \Pr[M(x,y) = 1] \le \frac{1}{2}.$$

   That is, true statements have proofs that make Arthur always accept, while any "proof" of a false statement is rejected with constant probability. If we changed $\frac{1}{2}$ to 0 then this would just be NP.

   Show that if $\mathsf{coNP} \subseteq \mathsf{MA}$ then the polynomial hierarchy collapses.

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