

Problem Set #4

Prof. Michael A. Forbes

Due: Sun., 2026-11-01 12:00pm

All problems are of equal value.

1. Show that if  $\text{NP} \subseteq \text{BPP}$  then  $\text{NP} = \text{RP}$ .
2. (Multiplicative Chernoff Bound). Let  $X_1, \dots, X_n$  be independent random variables taking values over  $[0, 1]$ . Let  $X = \sum_i X_i$ . Show that
  - (a) For  $r \in (-\infty, \ln 2]$ , prove that  $\mathbb{E}[e^{rX}] \leq e^{r\mathbb{E}[X] + r^2\mathbb{E}[X]}$ . You may use without proof that  $1 + z \leq e^z$  for all  $z \in \mathbb{R}$ , and that  $e^z \leq 1 + z + z^2$  for  $z \leq \ln 2$ .
  - (b) Explain how the above used the independence of the  $X_i$ .
  - (c) Apply Markov's inequality ( $\Pr[Y \geq a] \leq \mathbb{E}[Y]/a$ ) to  $e^{rX}$ , and optimize over  $r$ , to conclude that
    - i. For  $0 \leq \epsilon \leq \ln 4$ ,  $\Pr[X \geq (1 + \epsilon)\mathbb{E}[X]] \leq e^{-\epsilon^2\mathbb{E}[X]/4}$
    - ii. For  $\epsilon \geq \ln 4$ ,  $\Pr[X \geq (1 + \epsilon)\mathbb{E}[X]] \leq 2^{-\epsilon\mathbb{E}[X]/2}$
    - iii. For  $0 \leq \epsilon \leq 1$ ,  $\Pr[X \leq (1 - \epsilon)\mathbb{E}[X]] \leq e^{-\epsilon^2\mathbb{E}[X]/4}$
    - iv. (Additive Chernoff Bound) For  $\epsilon \geq 0$ ,  $\Pr[|X - \mathbb{E}[X]| \geq \epsilon \cdot n] \leq 2e^{-\epsilon^2 n/4}$

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

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

$$x \in L \implies \exists y \in \{0, 1\}^{\text{poly}(n)} \Pr[M(x, y) = 1] = 1,$$

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

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  $\text{coNP} \subseteq \text{MA}$  then the polynomial hierarchy collapses.

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