CS58400 - Theory of Computation and Computational Complexity Spring 2026

Assignment 4 *Due: Apr 23*

Note: Use LaTeX to typeset your solutions. You can use the source code of this file as a template or reference. Bonus questions are still capped by the total assignment grades, so only work on them if you want a challenge.

Problem 1 (Error reductions of AM). Let $\mathsf{AM}_{c,s}$ be the class of languages that can be proved with two-round Arthur-Merlin protocols with completeness c and soundness s (for instance, $\mathsf{AM}_{2/3,1/3}$ is just AM that we defined in class). For every $p(n) \leq \text{poly}(n)$, prove the following equivalences:

1. **(5 pts)**. $\mathsf{AM}_{1,1/2} = \mathsf{AM}_{1,2^{-p(n)}}$.
2. **(5 pts)**. $\mathsf{AM} = \mathsf{AM}_{1-2^{-p(n)},2^{-p(n)}}$.
3. **(Bonus, 5 pts)**. $\mathsf{AM} = \mathsf{AM}_{1,2^{-p(n)}}$.

   Hint. Try the argument used for $\mathsf{BPP} \subseteq \Sigma_2^{\mathrm{p}}$. *You will need several rounds of error reduction.*

Problem 2 (Improving Meyer's theorem). In class we proved that if $\mathsf{EXP} \subseteq \mathsf{P/poly}$ then $\mathsf{EXP} = \Sigma_2^{\mathrm{p}}$. In fact we can prove a slightly stronger result:

1. **(5 pts)**. Prove that if $\mathsf{PSPACE} \subseteq \mathsf{P/poly}$ then $\mathsf{PSPACE} = \mathsf{MA}$.

   Hint. The prover in the interactive proof protocol of TQBF *runs in polynomial space.*
2. **(5 pts)**. Use the above to conclude that if $\mathsf{EXP} \subseteq \mathsf{P/poly}$ then $\mathsf{EXP} = \mathsf{MA}$.

Problem 3 (Advices vs. oracles).

1. **(5 pts)**. Prove that $\mathsf{P}^{\mathsf{P/poly}} = \mathsf{P/poly}$.

   Hint. Use the advice formulation of $\mathsf{P/poly}$.
2. **(Bonus, 5 pts)**. Prove that if $\mathsf{NP} \subseteq \mathsf{P/poly}$, then $\mathsf{PH} \subseteq \mathsf{P/poly}$.

   Hint. Prove that if $\mathsf{NP} \subseteq \mathsf{P/poly}$ *then* $\mathsf{NP/poly} = \mathsf{P/poly}$.

Problem 4 (Monotone circuit complexity). For $x, y \in \{0,1\}^n$, we use $x \leq y$ to denote coordinate-wise comparison, that is $x_i \leq y_i$ for every coordinate $i \in [n]$. We write $x < y$ if $x \leq y$ and $x \neq y$.

A Boolean function $f : \{0,1\}^n \to \{0,1\}$ is monotone if $f(x) \leq f(y)$ for every $x \leq y \in \{0,1\}^n$. A Boolean circuit is monotone if it does not contain the NOT gate, so that it must compute a monotone function. For a monotone Boolean function f, let $\mathrm{Size}_{\mathrm{m}}(f)$ be the minimum size of a monotone Boolean circuit that computes f.

1. **(5 pts)**. Prove that for every n, there exists a monotone Boolean function $f : \{0,1\}^n \to \{0,1\}$ such that $\mathrm{Size}_{\mathrm{m}}(f) \geq 2^n/\mathrm{poly}(n)$.

   Hint. Use a counting argument.

2. **(10 pts)**. For $x \in \{0,1\}^n$, let $\overline{x} \in \{0,1\}^n$ be the coordinate-wise negation of x. Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, let $g : \{0,1\}^{2n} \to \{0,1\}$ as

$$g(x,y) = \begin{cases} f(x) & \text{if } \overline{x} = y; \\ 1 & \text{if } \overline{x} < y; \\ 0 & \text{otherwise.} \end{cases}$$

   Prove that g is monotone, and $|\mathrm{Size}_{\mathrm{m}}(g) - \mathrm{Size}(f)| \leq O(n)$.