Complexity Theory 236313 - Homework Assignment #4

Due January 26, 2023. Submit a single PDF file to the course site

January 10, 2023

Question 1. Let AO be the *And-Or* function defined on inputs x of length $n = 2^k$:

$$\mathsf{AO}(x) = \begin{cases} \mathsf{AO}\left(x_1 \dots x_{\frac{n}{2}}\right) \wedge \mathsf{AO}\left(x_{\frac{n}{2}+1} \dots x_n\right) & k \text{ is even} \\ \mathsf{AO}\left(x_1 \dots x_{\frac{n}{2}}\right) \vee \mathsf{AO}\left(x_{\frac{n}{2}+1} \dots x_n\right) & k \text{ is odd} \end{cases}.$$

Prove that $\mathcal{D}(\mathsf{AO}) = n$, where $\mathcal{D}$ denotes decision tree complexity.

Question 2. Let $\mathsf{BP} \cdot \mathsf{NP} = \left\{L \mid L \leq_r^{\mathsf{BPP}} \mathsf{3SAT}\right\}$. Let MA be the class of all languages for which there exists an interactive proof system (V, P) that satisfies the following properties:

- V is a polytime probabilistic verifier, P is an unbounded prover.
- Given input x, P sends a single message to V, who then does some computation and decides whether to accept of reject x. Neither V nor P sends additional messages.
- If $x \in L$, V accepts with probability $\geq \frac{2}{3}$.
- If $x \notin L$, V accepts with probability $\leq \frac{1}{3}$.

1. Prove that $\mathsf{AM}[2] = \mathsf{BP} \cdot \mathsf{NP}$.
2. Prove that $\mathsf{MA} \subseteq \Sigma_2^p$.

Question 3. Let $\mathsf{IP}(a, b)$ be the class of languages for which there exists an interactive proof system (V, P) that satisfies:

- If $x \in L$, V accepts with probability $> a$.
- If $x \notin L$, V accepts with probability $\leq b$.

Prove that $\mathsf{IP}\left(\frac{1}{2}, \frac{1}{2}\right) = \mathsf{IP}$.
Remark: we claimed in the lectures that $\mathsf{IP}\left(\frac{2}{3}, 0\right) = \mathsf{NP}$.

Question 4. A *multiprover proof system* for a language L is defined in a similar fashion to the standard single-prover interactive proof systems we defined in class: the verifier V is a probabilistic Turing machine, and there are k deterministic computationally unbounded Turing machines for the provers ($k \geq 2$ is fixed). Each prover has a separate communication channel with the verifier, and the provers cannot send each other messages. When the protocol begins, all parties receive the input x. In each step, the verifier can choose to send a message to some prover, and when he does only that prover receives the message. When the prover responds, only the veriefier receives the response. The proof system should satisfiy the following requirements:

- Completeness: for all $x \in L$, if the verifier interacts with the "right" provers, V always accepts.
- Soundness: for all $x \notin L$ and for any k provers, the verifier accepts with probability at most $1 - \frac{3}{4p(|x|)}$ for some polynomial $p(\cdot)$.

Let MIP denote the class of languages for which there exists a multiprover proof system.

A *probabilistic oracle protocol* for a language L is an oracle Turing machine M that satisfies the following requirements:

- Completeness: for all $x \in L$, there exists an oracle A_x for which $\Pr_r\left[M^{A_x}(x, r) = \text{acc}\right] = 1$.
- Soundness: for all $x \notin L$ and for any oracle A, $\Pr_r\left[M^{A}(x, r) = \text{acc}\right] < \frac{1}{4}$.

Let POP denote the class of languages for which there exists a probabilistic oracle protocol.

In this question, we shall prove one side of the equality $\mathsf{MIP} = \mathsf{NEXP}$, where $\mathsf{NEXP} = \bigcup_{c>0} \mathsf{NTIME}\left(2^{n^c}\right)$. This is another important theorem similar to $\mathsf{IP} = \mathsf{PSPACE}$.

1. Prove that $\mathsf{MIP} \subseteq \mathsf{POP}$.
2. We shall now prove that $\mathsf{POP} \subseteq \mathsf{MIP}$. Given a probabilistic oracle protocol M for a language L, we suggest the following (single-prover) proof system: the verifier simulates $M^A(x)$, and on every oracle question the verifier queries the prover for the answer.
   (a) Explain why this proof system fails (shortly).
   (b) Add another prover to the suggested proof system to satisfy the completeness and soundness criteria. Prove your answer.
3. Prove that $\mathsf{MIP} \subseteq \mathsf{NEXP}$.

Question 5. Let $\mathsf{MAX\text{-}3SAT}_3$ be a variant of $\mathsf{MAX\text{-}3SAT}$ where each variable appears in the formula at most 3 times. It can be shown that there exists a *gap-preserving reduction* from $\mathsf{MAX\text{-}3SAT}$ to $\mathsf{MAX\text{-}3SAT}_3$; i.e., there exists some $\varepsilon' > 0$ such that given a $\mathsf{3CNF}$ formula φ we can construct a $\mathsf{3CNF}_3$ formula φ' such that:

$$\mathsf{MAX\text{-}3SAT}(\varphi) = 1 \Longrightarrow \mathsf{MAX\text{-}3SAT}_3\left(\varphi'\right) = 1,$$
$$\mathsf{MAX\text{-}3SAT}(\varphi) < \frac{1}{1+\varepsilon} \Longrightarrow \mathsf{MAX\text{-}3SAT}_3\left(\varphi'\right) < \frac{1}{1+\varepsilon'}.$$

Let IS_4 be a variant of the independent set problem where all vertex degrees are at most 4.

1. Show a gap-preserving reduction from $\mathsf{MAX\text{-}3SAT}_3$ to IS_4, i.e., prove that if IS_4 has an r-approximation there there exists some r' such that $\mathsf{MAX\text{-}3SAT}_3$ has an r'-approximation (where r' depends only on r).
2. Conclude that there exists some constant r_1 such that IS_4 does not have an r_1-approximation.
3. Show that IS_4 has an r_2-approximation for some constant r_2.