Complexity Theory 236313 - Homework Assignment #3

Due January 10, 2023. Submit a single PDF file to the course site

December 27, 2022

Question 1. Denote $\mathsf{NL}^k \triangleq \mathsf{NSPACE}\left(\log^k n\right)$ and $\mathsf{DL}^k \triangleq \mathsf{DSPACE}\left(\log^k n\right)$. Let NC^k denote the class of decision problems decidable by poly-size and log-space *uniform* Boolean circuits of depth $O\left(\log^k n\right)$.

1. Prove that $\mathsf{NC}^k \subseteq \mathsf{DL}^k$ for all k.
2. Prove that for all k and for all $L \in \mathsf{NL}^k$, there exists a family of circuits of depth $O\left(\log^{2k} n\right)$ and fan-in 2 that decides L. Note that the circuits might not be poly-size or uniform.
3. Show that proving that $\mathsf{NL}^k \subseteq \mathsf{NC}^{2k}$ for all k settles an important open problem in complexity theory. State the open problem and prove your answer.

Question 2. In this question, we will prove that $\mathsf{CON} \notin \mathsf{AC}^0$ using the fact that $\mathsf{PARITY} \notin \mathsf{AC}^0$. Given an assignment to $x_1, \ldots, x_n$, let us define a graph G_1 as follows:

- G_1 will have $n+2$ vertices, named $s, v_1, \ldots, v_n, t$.
- We add an edge (s, v_i) iff i is the minimal index for which $x_i = 1$.
- We add an edge (v_j, t) iff j is the maximal index for which $x_j = 1$.
- We add an edge (v_i, v_j) iff: (i) $i < j$, (ii) $x_i = x_j = 1$, and (iii) $x_\ell = 0$ for all $i < \ell < j$.

1. Describe an AC^0 circuit that computes the adjacency matrix $M_1 \in \{0,1\}^{(n+2)\times(n+2)}$ of G_1 given the variables $x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n$.
2. Describe an AC^0 circuit that computes the adjacency matrix of a graph G_2 that has the same vertices as G_1, and has an edge between two vertices (u, w) iff there exists a path of length exactly 2 edges between u and w in G_1.
3. Use the aforementioned circuits to prove that $\mathsf{PARITY} \leq_{\mathsf{AC}^0} \mathsf{CON}$.

Question 3. Let us define the following operator @ on classes of languages: given a class C, we say that $L \in @\mathsf{C}$ if there exists some $L' \in \mathsf{C}$ such that:

- If $w \in L$ then $\exists_p x \forall_p y : (w, x, y) \in L'$.
- If $w \notin L$ then $\forall_p x \exists_p y : (w, x, y) \notin L'$.

1. Prove that $@\mathsf{P} \subseteq \Sigma_2^p \cap \Pi_2^p$.
2. Prove that $\mathsf{P}^{@\mathsf{P}} \subseteq @\mathsf{P}$.
3. Prove that $\mathsf{BPP} \subseteq @\mathsf{P}$. (**Hint**: recall the proof that $\mathsf{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$.)

Question 4. Let us define a *random oracle* A as follows: for every $x \in \Sigma^*$, $x \in A$ with probability $\frac{1}{2}$ (independently of other words). Prove that for all $\varepsilon > 0$, $\mathsf{BPP} \subseteq \mathsf{P}^A$ with probability $1-\varepsilon$ taken over all random oracles A.

Hint: Number the languages in BPP and take a probabilistic Turing machine with small enough error probability for each one.

Question 5. Prove the following claims:

1. $\mathsf{BPP}^{\mathsf{BPP}} \subseteq \mathsf{BPP}$.
2. $\mathsf{NP}^{\mathsf{BPP}} \subseteq \mathsf{BPP}^{\mathsf{NP}}$.
3. If $\mathsf{NP} \subseteq \mathsf{BPP}$ then $\mathsf{NP} = \mathsf{RP}$.
4. If $\mathsf{NP} \subseteq \mathsf{BPP}$ then the Polynomial Hierarchy collapses.

Question 6.

1. Let RL' be the complexity class we get when take RL and remove the requirement for polynomial time from its definition. Prove that $\mathsf{RL}' = \mathsf{NP}$.
2. Let RSPACE be the complexity class we get when take RP and convert the requirement for polynomial time with a requirement for polynomial space. Prove that $\mathsf{RSPACE} = \mathsf{PSPACE}$.
3. Given a complexity class C that is defined using probabilistic poly-time Turing machines, let us define C^* to be the same class only that we allow poly-time *in expectation.* Prove or disprove the following claims:
   (a) $\mathsf{BPP} = \mathsf{BPP}^*$.
   (b) $\mathsf{PP} = \mathsf{PP}^*$.