CS 535: Complexity Theory, Fall 2020

Homework 7

Due: 2:00AM, Saturday, November 7, 2020.

Reminder. Homework must be typeset with LaTeX preferred. Make sure you understand the course collaboration and honesty policy before beginning this assignment. Collaboration is permitted, but you must write the solutions *by yourself without assistance.* You must also identify your collaborators. Assignments missing a collaboration statement will not be accepted. Getting solutions from outside sources such as the Web or students not enrolled in the class is strictly forbidden.

Problem 0 (Term Paper)**.** Your term paper topic and partner (if applicable) are due on Gradescope at the same time this homework assignment is. Instructions for the term paper are here: `https://cs-people.bu.edu/mbun/courses/535_F20/handouts/term_paper.pdf` and a list of suggested topics is here: `https://piazza.com/class/keda2wyieyz10e?cid=277`.

Problem 1 (Circuit Lower Bounds for **PH**)**.** In this problem, you will prove that **PH** can compute languages with high circuit complexity. Specifically, you will show that for every integer $k \geq 1$, there is a language in $\mathbf{\Sigma}_2^p$ that cannot be computed by circuits of size at most n^k.

(a) Show that for every input length n, there exists a function $f : \{0,1\}^n \to \{0,1\}$ that is computed by a circuit of size at most $20n^k$, but not computed by any circuit of size at most n^k. Hint: Use the nonuniform hierarchy theorem (Theorem 6.22 in Arora-Barak). (2 points)

(b) Let C, C' be circuits, both on n-bit inputs. Say that C' comes lexicographically before C, written $C' <_{\text{lex}} C$, if the string encoding C' precedes the string encoding C in the lexicographic ordering. Define the language L to consist of all strings x such that $C(x) = 1$, where C is the lexicographically first circuit of size at most $20|x|^k$ that is not computed by any circuit of size at most $|x|^k$. Show that $L \notin \mathbf{SIZE}(n^k)$. (1 point)

(c) Show that the language $L \in \mathbf{\Sigma}_4^p$. Conclude that $\mathbf{\Sigma}_4^p \not\subseteq \mathbf{SIZE}(n^k)$. (6 points)

Hint: C is the lexicographically first circuit of size at most $20n^k$ that is not computed by any circuit of size at most n^k if: $|C| \leq 20n^k$ and for all $C' <_{\text{lex}} C$ where $|C'| \leq 20n^k$, there exists a smaller circuit C'' of size $\leq n^k$ such that $C'' \equiv C'$.

(d) Combine part (c) with the Karp-Lipton Theorem ($\mathbf{NP} \subseteq \mathbf{P_{/poly}} \implies \mathbf{PH} = \mathbf{\Sigma}_2^p$) to show that $\mathbf{\Sigma}_2^p \not\subseteq \mathbf{SIZE}(n^k)$. (3 points)

(e) Does part (d) imply $\mathbf{\Sigma}_2^p \not\subseteq \mathbf{P_{/poly}}$? Explain your answer. (3 points)

Problem 2 (**ZPP** vs. **RP** $\cap$ **coRP**)**.** Let $L \in \mathbf{RP} \cap \mathbf{coRP}$ be decided by an **RP** algorithm M_0 and a **coRP** algorithm M_1, each running in time $p(n)$ for some polynomial p. Show that the following is a zero-error randomized algorithm deciding L in expected polynomial time, and thus $\mathbf{RP} \cap \mathbf{coRP} \subseteq \mathbf{ZPP}$:

On input x:
Repeat the following indefinitely:

1. Run M_0 on input x. If it accepts, accept; else, continue.
2. Run M_1 on input x. If it rejects, reject; else, continue.

We already showed in class that $\mathbf{ZPP} \subseteq \mathbf{RP} \cap \mathbf{coRP}$, so this completes the proof that $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$. (5 points)