CS 535: Complexity Theory, Fall 2023

Homework 7

Due: 11:59PM, Tuesday, November 7, 2023.

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 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. (Curiously, this is a non-constructive proof...we know the language exists, but we don't know what it is. For more context, note that the best circuit size lower bound we have for SAT is roughly $5n$.)

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

(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 (on $|x|$-bit inputs) of size at most $|x|^{k+1}$ that is not computed by any circuit of size at most $|x|^k$.

By construction, we have that $L \notin \mathbf{SIZE}(n^k)$. Show that the language $L \in \mathbf{\Sigma}_4^p$, and thereby 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 n^{k+1} that is not computed by any circuit of size at most n^k if: $|C| \leq n^{k+1}$ and *for all* $C' <_{\text{lex}} C$ where $|C'| \leq n^{k+1}$, there *exists* a smaller circuit C'' of size $\leq n^k$ such that $C'' \equiv C'$.

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

(d) Does part (c) imply $\mathbf{\Sigma}_2^p \not\subseteq \mathbf{P}_{/\mathbf{poly}}$? Explain your answer. (2 points)

Problem 2 (Characterizing **ZPP**)**.** Recall that we defined the class **ZPP** to consist of languages that are decidable by probabilistic TMs in expected polynomial time. In this problem, you will explore two different alternative characterizations of this class.

(a) First, let us complete the proof we started in class (Thursday, 11/2) that $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$. We already showed in class that $\mathbf{ZPP} \subseteq \mathbf{RP} \cap \mathbf{coRP}$. For the opposite containment, let $L \in \mathbf{RP} \cap \mathbf{coRP}$ be decided by an $\mathbf{RP}$ algorithm M_0 and a $\mathbf{coRP}$ algorithm M_1, each running in (worst-case) 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 $\mathbf{RP} \cap \mathbf{coRP} \subseteq \mathbf{ZPP}$. (4 points)

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.

(b) An *abstaining* probabilistic TM is like a normal probabilistic TM for a decision problem, except that it may output any of the answers $0, 1$, or ? (standing for "I abstain from answering"). Show that a language $L \in \mathbf{ZPP}$ if and only if there exists a abstaining probabilistic TM M running in *worst-case* polynomial time such that

- If $x \in L$, then on input x, the TM M always outputs either 1 or ?,
- If $x \notin L$, then on input x, the TM M always outputs either 0 or ?, and
- For every input x, we have $\Pr[M(x) = ?] \leq 1/3$.

That is, when M produces an answer of 0 or 1, it is always correct, and on every input it abstains from answering with probability at most $1/3$. (4 points)