CS 599: The Meta-Complexity Frontier, Fall 2023
Problem Set #1

Due: 5:00PM, Friday, October 6, 2023.

Homework Policies

- Submit your completed assignment by email to `marco[at]ntime[dot]org` . Please include the string "CS599PS1" somewhere in your subject line.
- Solutions must be typeset, e.g., using LaTeX or Microsoft Word.
- You are encouraged to collaborate on the homework problems with each other in small groups (2 - 3 people). Collaboration may include brainstorming or exploring possible solutions together on a whiteboard, but should not include one person telling the others how to solve a problem. You **must write up the solutions independently** (in your own words) and **acknowledge your collaborators** at the beginning of the first page.
- You may read papers and other outside sources to help you solve these problems. If you do so, you **must cite and acknowledge any sources and write the solutions in your own words.**
- You may freely use without proof any results proved in class, in lecture notes posted on the class webpage, or in the main body of the texts assigned as reading. Note that this excludes results that appear in the texts as problems and exercises. You may, of course, use such results but you have to prove them first.
- To help your instructor calibrate the length and difficulty of future assignments, please include with each problem an estimate of how long it took you to solve it.
- Please start early! The problems are presented roughly in the order of the course content they correspond to, so you may get started on the first few problems as soon as the assignment is released. Late assignments will receive credit only with prior permission of the instructor.

Part of this and subsequent assignments will be to familiarize yourself with definitions of complexity classes and concepts that did not come up in class. These items will always be defined in our "local" complexity zoo, linked from the `Resources` section of our course webpage.

1 Informal Logic & Nondeterminism

We can reason about mathematics using the first-order logic of *Peano Arithmetic* (PA), which has a finite description and efficient "parse" and "proves" languages, as described in class. Argue at a high level that the following language is NP-complete.

$$\{\langle \varphi, 1^n \rangle : \text{statement } \varphi \text{ has a proof of length } n \text{ in the PA system}\}$$

What properties of PA did your proof actually use? You don't need to know anything about PA; the intended argument will work for many reasonable first-order theories. This is Question 2.11 of [AB09] — see their Hints, page 532, for help with the proof idea.

2 Improved Deterministic Time Hierarchy Theorem

Prove an almost-everywhere deterministic time hierarchy theorem against advice with a refuter. That is, first identify a super-constant advice bound $\alpha(n) : \mathbb{N} \to \mathbb{N}$ and prove:

$$\forall b > 7 \;\; \mathsf{DTIME}[n^{5b}] \not\subseteq \text{i.o.}\mathsf{DTIME}[n^b]/\alpha(n).$$

Your solution should state and use (but need not prove) an efficient UTM theorem for machines that take advice. Then use your proof to answer these questions:

1. How big can α be, given your proof technique? Hint: try for at least $\sqrt{n}$. Can you do better? Why or why not?
2. Construct a refuter against $\mathsf{DTIME}[n^b]$ based on your proof of this hierarchy theorem. What does the time complexity of your refuter depend on?
3. ***BONUS:*** Construct a refuter against $\mathsf{DTIME}[n^b]/\alpha(n)$ based on your proof of this hierarchy theorem. What does the time complexity of your refuter depend on?

3 Circuit Lower Bounds "From the Top"

Prove that $\mathsf{ZPEXP}^{\mathsf{MCSP}}$ is not contained in $\mathsf{P/poly}$, explicitly citing the diagonalization-based circuit lower bound you use from [Kan82]. Be careful and explicit about any padding argument(s) that may arise, and use the following Karp-Lipton theorem.

$$\mathsf{PSPACE} \subset \mathsf{P/poly} \implies \mathsf{PSPACE} \subseteq \mathsf{ZPP}^{\mathsf{MCSP}}$$

The idea is very similar to $\mathsf{MA\text{-}EXP} \not\subset \mathsf{P/poly}$ — combine the Karp-Lipton style theorem above with a previously known circuit lower bound proved via diagonalization. Part of this exercise is to extract and cite the appropriate circuit lower bound from [Kan82]. Use your proof to answer these questions:

1. What properties of $\mathsf{ZPP}^{\mathsf{MCSP}}$ did you use?
2. What properties of PSPACE did you use?
3. Using your observations above, state a Karp-Lipton style theorem that would suffice to separate NEXP from $\mathsf{P/poly}$. Try to justify this answer with a "generic" proof of $\mathsf{NEXP} \not\subset \mathsf{P/poly}$ given your proposed KL-style theorem.

4 Improving The Nondeterministic Hierarchy Theorems Seems Hard

Finally, you will apply the (bounded) relativization barrier to a concrete open problem by constructing and interpreting an appropriate oracle. First, construct an oracle A such that $\mathsf{NEXP}^A \subseteq \text{i.o.}\mathsf{NP}^A$. Using your oracle, answer the following questions:

1. What does the existence of A imply about an almost-everywhere nondeterministic time hierarchy?
2. What is the time complexity of deciding A ?
3. What does the time complexity of A imply about almost-everywhere nondeterministic time hierarchy theorems?

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009. ISBN: 978-0-521-42426-4. URL: http://www.cambridge.org/catalogue/catalogue.asp?isbn=9780521424264.

[Kan82] Ravi Kannan. "Circuit-Size Lower Bounds and Non-Reducibility to Sparse Sets". In: *Inf. Control.* 55.1-3 (1982), pp. 40–56. DOI: 10.1016/S0019-9958(82)90382-5. URL: https://doi.org/10.1016/S0019-9958(82)90382-5.