University of California, Los Angeles
CS 281 Computability and Complexity
Instructor: Alexander Sherstov

March 13, 2024

Instructions

- Your solutions are due March 23, 2024 at 5 p.m. Please typeset your work using the provided LaTeX template and submit the resulting PDF document on Gradescope. Late work will not be accepted or graded, resulting in zero credit for this assignment.

- You cannot collaborate with other students on this assignment. The work that you submit must be your own.

- This exam can be solved in its entirety using the course material taught so far, without consulting any additional sources. However, you are welcome to use any scholarly sources, including your textbook and the Internet. If you do, please write the solution in your own words and acknowledge the sources that you have consulted.

- If you are using a fact that we have not covered in class, please provide a proof for it. This applies even to facts that are published and well-known.

- If you are not able to solve a problem in full, make a simplifying assumption. Start early, do your best, and take pride in your discoveries. Most importantly, have fun!

Final Exam

1 Let D denote the set of all decidable languages. Either construct a D-complete language, or prove that it does not exist.

2 Prove that $\mathsf{EXP} \neq \mathsf{NEXP}$ implies $\mathsf{P} \neq \mathsf{NP}$.

3 Suppose that the polynomial hierarchy does not collapse. Prove that then, PH is a proper subset of EXP.

4 Construct an oracle O such that $\mathsf{P}^O \neq \mathsf{BPP}^O$.

5 Let L be any NP-complete language. Prove that $L \in \mathsf{BPP}$ if and only if $L \in \mathsf{RP}$.

6 Prove that there is a real number $0 < p < 1$ with the following property: given access to a coin with bias p, a randomized Turing machine can decide an undecidable language in *polynomial time.* "Access to the coin" means the ability to receive any desired number of random bits $X_1, X_2, X_3, \ldots \in \{0, 1\}$, each an independent random variable with expectation p.

7 Alice and Bob each have an n-bit string. They would like to determine, with correctness probability 99%, whether their strings are equal. Show that $O(\log n)$ bits of communication suffice.

8 Construct a circuit of $\wedge, \vee, \neg$ gates that computes the majority function on n bits. Your circuit should have depth $O(\log n)$ and polynomial size.

9 Prove that with Hadamard coding, it is in general impossible to recover the original codeword if the received transmission is corrupted in 25% or more of the coordinates.

10 Suppose that SAT has a PCP verifier with $o(\log n)$ random bits and $O(1)$ queries. Prove that then $\mathsf{P} = \mathsf{NP}$.

11 Prove that increasing the completeness parameter in the definition of IP from $2/3$ to 1 does not change this complexity class. What class do we get if we keep the completeness unchanged but increase the soundness from $2/3$ to 1?

12 Give a randomized algorithm that takes as input a pair of binary strings and determines in time $O(n \log n)$ whether one of them is a substring of the other.