CS 505 Spring 2025 — Homework 5

YOUR NAME HERE (FIRST AND LAST) (UID: YOUR UID HERE)

Due Date: May 06, 2025, no later than 2:00pm Central Time.

Collaboration Policy

Collaboration between students is encouraged. However, **all collaborations** need to be acknowledged (whether they are in this class or not in this class). You **MUST** list all collaborators for homework assignments. Moreover, collaborating **does not mean** you can copy-paste work from each other. Each submission needs to be in the students own words, otherwise it will be considered plagiarism.

Moreover, you are allowed to look to other resources for help with the homework. Please correctly cite such resources by using the `\cite` command, and including the correct citations in `local.bib`.

Finally, please acknowledge any other discussions that helped you complete this assignment. This can include "office hours," "Piazza," or other discussions where a direct collaboration did not happen.

Collaborator and Discussion Acknowledgements

Please list your collaborators below. Include their First and Last names, along with their UID if they are a UIC student. If you did not collaborate with others for this assignment, please copy-paste the following line into the first item of the `itemize` below.

I worked on this assignment individually and did not collaborate with others.

- Collaborator 1...

1 PCP Theorem (25 Points)

1.1 Part 1 (5 Points)

Prove that for every two functions $r, q \colon \mathbb{N} \to \mathbb{N}$ and constants $s < 1$, if $\mathbf{PCP}_s(r, q)$ is identical to the class $\mathbf{PCP}(r, q)$ except with the soundness error replaced with s instead of $1/2$, then $\mathbf{PCP}_s(r, q) = \mathbf{PCP}(r, q)$.

Proof of Problem 1 Part 1. Your answer here... □

1.2 Part 2 (10 Points)

Prove that $\mathbf{PCP}(0, \log(n)) = \mathbf{P}$ and $\mathbf{PCP}(0, \text{poly}(n)) = \mathbf{NP}$.

Proof of Problem 1 Part 2. Your answer here... □

1.3 Part 3 (10 Points)

Let ϕ be any $3CNF$ on n variables and m clauses such that each clause of ϕ has exactly 3 distinct variables in each clause (i.e., you cannot repeat variables in each clause). Give a probabilistic polynomial-time algorithm which, on input any such ϕ above, outputs some assignment of ϕ which satisfies at least 7/8 of the clauses.

Hint: Show that the expected number of satisfied clauses from a random assignment is at least $(7/8) \cdot m$*, then use Markov's inequality to show that the probability of satisfying at least* $(7/8 - 1/(2m)) \cdot m$ *clauses is at least* $1/\text{poly}(m)$*.*

Proof of Problem 1 Part 3. Your answer here... □

2 Crypto and Complexity (25 points)

2.1 Part 1 (5 Points)

Show that if **P** = **NP**, then one-way functions do not exist.

Proof of Problem 2 Part 1. Your answer here... □

2.2 Part 2 (10 Points)

Prove that if f is a one-way function, then g defined as $g(x, y) = (f(x), y)$, where $|x| = |y|$, is also a one-way function.

Proof of Problem 2 Part 2. Your answer here... □

2.3 Part 3 (10 Points)

Show that if one-way functions exist, then $\mathbf{distNP} \not\subseteq \mathbf{distP}$.

Proof of Problem 2 Part 3. Your answer here... □