CS 278: Computational Complexity Theory
Homework 2

Due: **October 24th, 2025**

Fall 2025

Instructions:

- Collaboration is allowed but solutions must be written independently. List collaborators and external resources.
- Write your solutions in LaTeX and submit a single PDF by email to `lijiechen@berkeley.edu` with subject "CS 278 - Homework 2 – [Your Name]".
- Name your file `CS278-HW2-[YourName].pdf`. **Deadline:** 11:59pm Pacific Time October 24th, 2025.
- Late submissions lose **10%** per day (e.g., three days late $\rightarrow 0.9^3$ of your score).
- This homework has 4 problems, each with multiple parts, totaling **160 points**. As in HW1, our course policy on homework aggregation applies unchanged.

1 Problem 1 (40 pts): A circuit lower bound for quadratic space

Show that languages decidable in quadratic space do not admit linear-size circuits.

Statement. Prove that $\mathrm{SPACE}[n^2] \not\subseteq \mathrm{SIZE}(O(n))$. In other words, there is a language $L \in \mathrm{SPACE}[n^2]$ such that every Boolean circuit family computing L on inputs of length n has size $\omega(n)$ for all sufficiently large n.

2 Problem 2 (40 pts): NEXP $\subseteq$ coNEXP$/_{n+1}$

Statement. Prove that NEXP $\subseteq$ coNEXP$/_{n+1}$. In other words, for every language $L \in$ NEXP, prove that there exists an advice function $a(n) \in \{0,1\}^{n+1}$ such that there exists a coNEXP machine M that, for every $n \in \mathbb{N}$, given the correct advice $a(n)$, M computes L on all n-bit inputs.

3 Problem 3 (40 pts): Prove CL $\subseteq$ ZPP

The class CL (catalytic logspace) allows an algorithm logarithmic *clean* space and polynomially many *dirty* bits that must be restored at the end. Show that every $L \in \mathrm{CL}$ has a zero-error expected-polynomial-time algorithm.

Definition of ZPP. The complexity class ZPP (Zero-error Probabilistic Polynomial time) consists of all languages L for which there exists a probabilistic polynomial-time Turing machine M such that:

1. For every input x, $M(x)$ outputs either 0, 1, or $\perp$ ("don't know").
2. If $x \in L$, then $\Pr[M(x) = 1] \geq \frac{1}{2}$ and $\Pr[M(x) = 0] = 0$.
3. If $x \notin L$, then $\Pr[M(x) = 0] \geq \frac{1}{2}$ and $\Pr[M(x) = 1] = 0$.
4. The expected running time of M on any input is polynomial.

Equivalently, ZPP is the class of languages that can be decided by Las Vegas algorithms: randomized algorithms that always give the correct answer when they terminate, and have polynomial expected running time.

Statement. Prove that CL $\subseteq$ ZPP.

4 Problem 4 (40 pts): Prove that $\mathbf{TC}^1 \subseteq \mathrm{CL}$

In the class we sketch the high-level idea of the proof that $\mathrm{TC}^1 \subseteq \mathrm{CL}$. In this problem, you will complete the proof.

Statement. Prove that $\mathrm{TC}^1 \subseteq \mathrm{CL}$. You should give a complete register program for the TC^1 circuit and prove it's correctness.

Optional references and context

For accessible background on catalytic logspace and the toggling construction, see:

- Nathan Sheffield, *A quick-and-dirty intro to CL.*
- Ian Mertz, *Reusing Space: Techniques and Open Problems.*

(Optional) Solution placeholders
You may use the following headings for your writeup; remove them if not needed.

Solution to Problem 1

Solution to Problem 2

Solution to Problem 3

Solution to Problem 4