Final Exam, Computational Complexity 2023

- Books, notes are allowed.
- Communication, calculators, cell phones, computers, etc... are not allowed.
- Your explanations and proofs should be clear enough and in sufficient detail so that they are easy to understand and have no ambiguities.
- You are allowed to refer to material covered in lectures (but not exercises) including theorems without reproving them.
- **Do not touch until the start of the exam.**

Good luck!

Name: ______________________ **N° Sciper:** ______________

Problem 1 / 15 points	Problem 2 / 15 points	Problem 3 / 20 points	Problem 4 / 20 points	Problem 5 / 20 points	Problem 6 / 20 points

Total / 110

1 *(15 pts)* **Quick-fire round.** Consider the following statements.

1. SAT $\leq_p$ Graph Isomorphism.
2. ZPP is closed under complement.
3. Graph Isomorphism $\leq_p$ DEQ (Diophantine equation).
4. If $\Sigma_2\mathsf{P} = \Pi_3\mathsf{P}$, then $\Sigma_2\mathsf{P} = \Pi_2\mathsf{P}$.
5. $\mathsf{NP} \subseteq \mathsf{SIZE}[n^2]$.
6. $\mathsf{EXP}^{\mathsf{EXP}} = \mathsf{EXP}$.
7. $\mathsf{BPL} \subseteq \mathsf{NP}$.
8. $\mathsf{P}^{\mathsf{BPP}} \subseteq \mathsf{P/poly}$.
9. If $\mathsf{L} = \mathsf{NL}$, then $\mathsf{P} = \mathsf{NP}$.
10. There is a polynomial time algorithm that takes CNF formula φ and produces DNF formula ψ such that ψ is satisfiable iff φ is satisfiable.
11. There exists an unsatisfiable CNF formula φ with n variables such that any tree-like Resolution proof for φ has superpolynomial size in terms of n, but there is a polynomial-size CP proof.
12. The decision tree complexity for every non-constant symmetric boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is exactly n.
13. There exist boolean functions f with $s(f) > \min\{C_0(f), C_1(f)\}$.
14. If CNF formula is unsatisfiable then there is a Cutting Planes proof of this fact.
15. For any boolean function, $D(f) \leq C_0(f)^2$.

For each box below, write one of the following symbols:

- **T** if the statement is known to be true.
- **F** if the statement is false *or not known to be true.* E.g., both $\mathsf{P} = \mathsf{NP}$ and $\mathsf{P} \neq \mathsf{NP}$ should be marked **F**.
- or leave the box empty.

A correct **T**/**F** answer is worth +1 point, an incorrect answer is worth −1 point, and an empty answer is worth 0 points.

1.	
2.	
3.	
4.	
5.	

6.	
7.	
8.	
9.	
10.	

11.	
12.	
13.	
14.	
15.	

2 *(15 pts)* **Problem Garden.** For each problem below, classify it into the smallest possible complexity class (as seen in lectures/exercises). You do not need to justify your answers.

1. **Input:** Graphs G_1, G_2. **Output:** YES iff G_2 is isomorphic to the subgraph of G_1.
2. **Input:** Boolean circuit C. **Output:** YES iff C has exactly two satisfying assignments.
3. **Input:** Undirected graph G. **Output:** YES iff G is a forest.
4. **Input:** Binary string x a description of a Turing machine M. **Output:** YES iff M stops on empty input after at least $|x|^2$ number of steps.
5. **Input:** A collection $S := \{\varphi_1, \ldots, \varphi_m\}$ of 3-DNF formulas on n variables, and a integer k. **Output:** Yes iff there is a subset $S' \subseteq S$ of size at most k for which $\bigvee_{\varphi \in S'} \varphi \equiv 1$.

3 *(20 pts)* **NP-completeness.** Let $G := (V, E)$ be an undirected graph and $C := \{V_i\}_{i \in [k]}$ a partition of V (i.e. $\bigcup_{i \in [k]} V_i = V$ and $V_i \cap V_j = \emptyset$ for $i \neq j$). We say that (G, C) admits an **independent set of representative** if there exists $S \subseteq V$ such that:

- S is an independent set of G and
- S contains one vertex of each part, i.e. for all $i \in [k]$, $|S \cap V_i| = 1$.

Let $L := \{\langle G, C \rangle : (G, C) \text{ has an independent set of representative}\}$. Show that L is NP-complete.

4 *(20 pts)* **Oracles.** Show that there exist two oracles:

- *(5 pts)* $A \subseteq \{0,1\}^*$ such that $\mathsf{P}^A = \mathsf{RP}^A$;
- *(15 pts)* $B \subseteq \{0,1\}^*$ such that $\mathsf{P}^B \neq \mathsf{RP}^B$;

Hint: how to modify language that separates P^B *and* NP^B *such that the result will belong to* RP^B*?*

5 *(20 pts)* **Decision Complexity.** Show the following equality for decision complexity $\mathrm{D}(\wedge_n \circ g) = n \cdot \mathrm{D}(g)$ where $g\colon \{0,1\}^m \to \{0,1\}$ is an arbitrary function and

$$(\wedge_n \circ g)(x_{1,1}, x_{1,2}, \ldots, x_{1,m}, \ldots, x_{n,1}, \ldots, x_{n,m}) \coloneqq \bigwedge_{i=1}^{n} g(x_{i,1}, x_{i,2}, \ldots, x_{i,m}).$$

6 Communication Complexity. Alice has an n-bit string x, and Bob has an n-bit string y such that y differs from x in exactly one position.

1. *(10 pts)* Design a deterministic communication protocol with complexity $O(\log n)$, which allows Bob to find out x.

2. *(10 pts)* Design a one-round deterministic communication protocol with complexity $O(\log n)$, which allows Bob to find out x. (In one-round protocol Alice sends some message to Bob, and after that Bob computes the result). *Hint: if i is the position of a difference, maybe it would be helpful to consider the binary representation of i.*