EECS 376 Final Exam

The multiple-choice portion of the exam consists of the 8 questions in the "Multiple Choice" section below. The written portion of the exam consists of the 4 questions in the "Written Answer" section below. These two portions are released as a single Canvas quiz. You are to submit the answers to the multiple-choice portion on Canvas. Submit your written solutions to Gradescope as you would for a homework assignment. **You will not submit anything on Canvas for the written part.**

Both portions are to be submitted before 9pm Eastern Time, but the written part will have a 15-minute grace period until 9:15pm.

Logistics:

- The exam will take place on Wednesday, December 14, 7pm - 9pm Eastern Time.
- You must **submit your multiple-choice answers on Canvas prior to 9pm Eastern Time**. There is no grace period for the multiple-choice questions.
- The deadline to **submit your written answers to Gradescope is 9pm Eastern Time. There will be a grace period until 9:15pm.** However, you must start the process of preparing your submission by 8:45pm.
- You may use any **course** resources for the exam, including the textbooks, lecture slides, online notes, discussion materials, etc.
  You may **not** use any **non-course** resources, such as search engines (e.g. Google) or calculators (e.g. a physical calculator, WolframAlpha, etc.).
- You are prohibited from searching for answers to any of the exam questions online.
- You are prohibited from soliciting help from anyone, whether in person, over text/chat, on StackOverflow, making public Piazza posts, or any other means.
- Your solutions must be entirely your own work.
- If you have clarification questions, make a private post on Piazza, and a staff member will respond as soon as possible.
- If you run into technical issues or have an emergency, contact the staff (eecs376f22@umich.edu) right away. Do **not** contact a fellow student for help.
- Each multiple-choice question has only a single correct answer.

Any deviation from these rules will constitute an Honor Code violation. In addition, the staff reserves the right **not** to grade any exam taken in violation of this policy.

Attest to the following honor pledge by signing your name below.

Honor pledge:

I have neither given nor received aid on this exam, nor have I concealed any violations of the Honor Code.
I will not discuss the exam with anyone who has not already taken it.
I am taking the exam at the time I was assigned by the staff.

Signature: _____

Recall the following languages (unless otherwise specified, all graphs are simple and undirected):

- $L_{\text{ACC}} = \{\langle M, x\rangle : M \text{ is a Turing machine that accepts the input } x\}$
- $L_{\text{HALT}} = \{\langle M, x\rangle : M \text{ is a Turing machine that halts on input } x\}$
- $\overline{L} = \{x \in \Sigma^* : x \notin L\}$
- $\text{SAT} = \{\phi : \phi \text{ is a satisfiable Boolean formula}\}$
- $\text{3SAT} = \{\phi : \phi \text{ is a satisfiable 3CNF formula}\}$
- $\textsc{Clique} = \{(G, k) : G \text{ is a graph with a clique of size (at least) } k\}$
- $\textsc{Vertex-Cover} = \{(G, k) : G \text{ is a graph with a vertex cover of size (at most) } k\}$
- $\textsc{Independent-Set} = \{(G, k) : G \text{ is a graph with an independent set of size (at least) } k\}$
- $\textsc{Hamiltonian-Cycle} = \{G : G \text{ is a graph with a Hamiltonian cycle}\}$
- $\textsc{Hamiltonian-Path} = \{(G, s, t) : G \text{ is a graph with a Hamiltonian path from } s \text{ to } t\}$
- $\text{TSP} = \{(G, k) : G \text{ is a weighted graph with a tour of weight at most } k\}$
- $\textsc{Max-Cut} = \{(G, k) : G \text{ is a graph with a cut of size at least } k\}$

Multiple Choice (5 points each)

1. Suppose that a language B is NP-Complete, and we demonstrate that $B \leq_p A$ for some language A. Which of the following can we **always** conclude about the language A?
   - ◯ A is NP-Hard
   - ◯ A is NP-Complete
   - ◯ A is in NP
   - ◯ None of the other choices are valid facts we can conclude.

2. Suppose that a language A is in P and a language B is NP-Complete. Then it must be the case that $A \leq_p B$.
   - ◯ True
   - ◯ False
   - ◯ Unknown

3. Suppose a language L is **not** in the class P. Then L must be undecidable.
   - ◯ True
   - ◯ False
   - ◯ Unknown

4. Which of the following is an **invalid** public key (n, e) for the RSA encryption scheme?
   - ◯ (55, 40)
   - ◯ (65, 13)
   - ◯ (77, 13)
   - ◯ (85, 27)
   - ◯ All of the other choices are valid public keys.

5. Suppose that we have $(n, e) = (51, 11)$ as an RSA public key, and we wish to sign the message $m = 5$ using the RSA **signature** scheme. What is the correct value for the signed message s?

- ◯ 11
- ◯ 13
- ◯ 14
- ◯ 23
- ◯ 49

6. Suppose that X is a non-negative random variable with an expectation equal to 1. Which of the following is **always** a correct upper bound on $\Pr[X \geq 3/4]$?

- ◯ 0.001
- ◯ $e^{-3/4}$
- ◯ 3/4
- ◯ 1

7. Assuming P $\neq$ NP, the CLIQUE language is **not** NP-Complete.

- ◯ True
- ◯ False
- ◯ Unknown

8. Define #SAT to be the problem of determining how many satisfying assignments a Boolean formula ϕ has. Define the decision version as follows:

$$L_{\#\text{SAT}} = \{(\phi, k) : \phi \text{ is a Boolean formula with} \geq k \text{ satisfying assignments}\}$$

Suppose we have an efficient decider D for the decision problem $L_{\#\text{SAT}}$. Then the following algorithm would *efficiently* solve the #SAT problem:

$A =$ "On input ϕ:
1. $k \leftarrow 0$
2. While $D(\phi, k+1)$:
3. $\quad k \leftarrow k+1$
4. Return k"

- ◯ True
- ◯ False
- ◯ Unknown

Written Answer (15 points each)

9. A blood test for a rare disorder is being performed on n people. Each person can be tested individually, but this is expensive. To decrease the cost, the n people are divided into n/k groups, $G_1, G_2, \ldots, G_{n/k}$, of k people each (assume that k divides n); the blood samples of the people in a group are then pooled and tested together, so that only n/k tests are used initially. If the test for group G_i is negative, none of the members of G_i have the disorder, so they don't need to be tested individually. On the other hand, if the test for group G_i is positive, at least one person in the group has the disorder, and the entire group must be retested individually.

   Suppose each person independently has a probability p of having the disorder. Compute each of the following quantities as a simplified expression in terms of n, k, and p. Justify your answers.

   (a) The probability that a specific group G_i needs individual testing for its members.

   (b) The expected number of groups that need individual testing.

   (c) The expected number of total tests required over all groups, including both group and individual tests.

10. We define the following language:

$$\text{BIG-CLIQUE} = \{G = (V, E) : G \text{ is an undirected graph with a clique of size } |V| - 1\}$$

Prove that BIG-CLIQUE is in P.

11. You are planning to drive from Michigan to Southern California for the CFP National Championship game, and there are a number of sights you'd like to see along the way (e.g. Yellowstone, The Grand Canyon, Death Valley). You'd like to see as many of these places as possible, without having to backtrack (traverse a cycle) during your trip.

    Formally, we define the following language:

$$\textsc{Road-Trip} = \left\{ (G = (V, E), s, t, S, k) : \begin{array}{r} G \text{ has a simple path from } s \text{ to } t \text{ that} \\ \text{visits at least } k \text{ of the vertices in } S \end{array} \right\}$$

    (A *simple path* is a path without a cycle.)

    Given an efficient decider D for Road-Trip, design and analyze (both correctness and runtime) an efficient algorithm that given $(G = (V, E), s, t, S)$, finds an actual simple path (i.e. a path without a cycle) from s to t that goes through as many vertices of S as possible. The path should be returned as a set of edges (the edges do **not** have to be ordered). You may assume that $\{s, t\} \subseteq V$ and $S \subseteq V$.

12. *Note: The language here is the same as the one defined in the previous question.*

You are planning to drive from Michigan to Southern California for the CFP National Championship game, and there are a number of sights you'd like to see along the way (e.g. Yellowstone, The Grand Canyon, Death Valley). You'd like to see as many of these places as possible, without having to backtrack (traverse a cycle) during your trip.

Formally, we define the following language:

$$\textsc{Road-Trip} = \left\{ (G = (V, E), s, t, S, k) : \begin{array}{r} G \text{ has a simple path from } s \text{ to } t \text{ that} \\ \text{visits at least } k \text{ of the vertices in } S \end{array} \right\}$$

(A *simple path* is a path without a cycle.)

(a) Provide an efficient verifier for Road-Trip. You do **not** need to provide analysis for this part.

(b) Prove that Road-Trip is NP-Hard.