EECS 376 Final Exam, Winter 2022

Instructions:

This exam is closed book, closed notebook. You may not provide your own scratch paper. No electronic devices are allowed. You may use one 8.5 × 11-inch study sheet (both sides). Make sure you are taking the exam at the time slot and the classroom you were assigned by the staff.

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

The exam consists of 12 multiple choice questions, 4 short-answer questions, and 3 longer proofs. *You only need to answer two of the longer proof questions.* ***You are to cross out the one proof question you don't want graded.*** For the multiple choice questions, please fill-in the circle you select completely and clearly. ***Please print your UNIQNAME at the top of each page.***

For the short-answer and proof sections, please write your answers clearly in the spaces provided. If you run out of room or need to start over, you can use the blank pages at the end but you **MUST** make that clear in the space provided for the answer. The exam has 14 pages printed on both sides, including this page and two blank pages at the end.

You must leave all pages stapled together in their original order.

Sign the honor pledge 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 before exam grades are released.
I attest that I am taking the exam at the time slot and the classroom I was assigned by the staff.

Signature: ______________________________

Name: ______________________________

Uniqname: ____________________

[**Markov's Inequality**] If Z is a non-negative random variable and $a > 0$, then

$$\Pr[Z \geq a] \leq \frac{\mathbb{E}[Z]}{a}.$$

[**Chernoff-Hoeffding**] If $X_1, X_2, ...X_n$ are are independent, identically distributed RVs w/ expectation μ, and range in [0,1] then, for any $k > 0$, the following holds for their sum:

$$\Pr\left[\sum_{i=1}^{n} X_i \geq \mu n + k\right] \leq e^{-2k^2/n}$$

Version C

UNIQNAME (print): ______________________________

Multiple Choice – 36 points

1. Let language $L = \{(A, x) \mid x \text{ is the minimum element of array } A\}$. Let L_2 be an NP-Hard language. The statement $L_2 \leq_T L$ is (always/sometimes/never) true.

   ○ Always

   ○ Sometimes

   ○ Never

2. Using Markov's inequality, what is the upper bound on the probability that tossing a biased coin 40 times results in at least 33 tails if Pr(Heads) = 0.7?

   ○ 20/33

   ○ 28/33

   ○ 23/40

   ○ 12/33

   ○ 33/28

   ○ 28/40

3. ~~Which of the following languages are recognizable?~~

   i $L_{\text{GREATER}} = \{M : \ |L(M)| > 1\}$

   ii $L_{\text{SMALL}} = \{M : \ (|L(M)| == 1) \text{ or } (|L(M)| == 0) \ \}$

   iii $L_{\text{APPLE}} = \{M : M \text{ is a TM that accepts the input string "apple"}\}$.

   ○ i and ii

   ○ i, ii and iii

   ○ ii and iii

   ○ i and iii

   ○ only iii

4. There is a row of apple trees where each tree i has A$[i]$ apples. If you pick up apples from a given tree then you can't pick up apples from any of its adjacent trees. For instance, If you pick up the apples from tree number 6 you can't pick apples from tree number 5 or tree number 7.
   The function $T(n)$ returns the maximum number of apples you can pick up from n trees.
   The base cases are $T(1) = \text{A}[1]$ as we only have one tree and $T(0) = 0$.
   What is the recurrence relation for $T(n)$?

   ○ $T(n) = \max(T(n-1), \text{A}[n])$

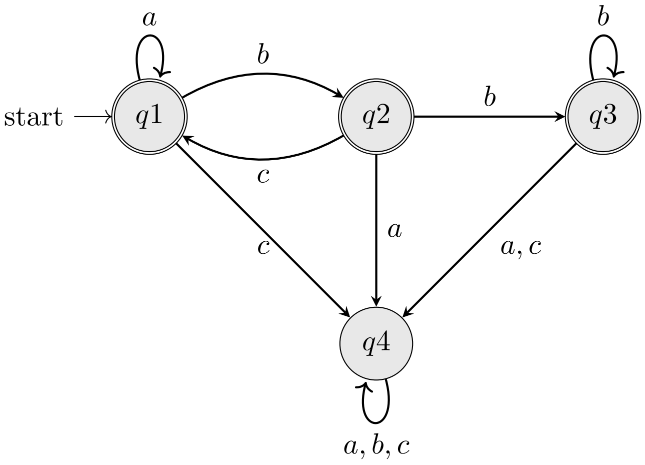
   ○ $T(n) = \max(T(n-1), T(n-2))$

   ○ $T(n) = \max(\text{A}[n] + T(n-1), \text{A}[n] + T(n-2))$

   ○ $T(n) = \max(T(n-1), \text{A}[n] + T(n-2))$

   ○ $T(n) = \max(\text{A}[n], \text{A}[n+1] + \text{A}[n-1])$

5. Consider the following DFA, what language does it decide?



○ $(a^*|bc)^+a^*b^*$

○ $(a^+|bc)^+a^+b^+$

○ $(a^*|b^*c^*)^+a^*b^*$

○ $(a^+|bc)^*a^+b^+$

○ $(a^*|bc)^*(a^+|b^+)$

6. Given RSA public key (e=7, n=33), what should be the *signature* for message m=4?

○ 31

○ 23

○ 19

○ 25

○ 11

7. What is 5^{146} (mod 13)?

○ 8

○ 3

○ 12

○ 5

○ 4

8. Let B-3N be a divide-and-conquer algorithm. On an input of size n, B-3N splits the input into 5 subproblems of size $\frac{n}{3}$. Splitting the input and recombining the results takes $O(3n+1)$ time. Using the Master Theorem, what is the tightest time complexity of B-3N?

   ○ $O(n^{\log_3 5})$

   ○ $O(n)$

   ○ $O(n \log n)$

   ○ $O(n^5)$

   ○ The Master Theorem cannot be used to find the time complexity of B-3N.

9. ~~Let L_1 and L_2 be recognizable languages. Then $L_1 \setminus \overline{L_2}$ is (always/sometimes/never) recognizable.~~

   ~~*Recall:* "\" denotes set difference. $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$.~~

   ○ Always

   ○ Sometimes

   ○ Never

10. Consider a language A that is NP-Complete. For some arbitrary language L, if A $\leq_p$ L then L is (always/sometimes/never) NP-Complete.

    ○ Always

    ○ Sometimes

    ○ Never

11. ~~Which of the following languages can be shown to be undecidable by a direct application of Rice's Theorem? (Select all that apply)~~

    ○ $L = \{(\langle M \rangle, x) \mid M(x) \text{ halts on the } 376^{th} \text{ step}\}$

    ○ $L = \{\langle M \rangle \mid L(M) \subseteq \sum^*\}$

    ○ $L = \{x \mid x \text{ is a prime number}\}$

    ○ $L = \{\langle M \rangle \mid M \text{ accepts an even number of inputs}\}$

    ○ $L = \{\langle M \rangle \mid M \text{ accepts the input '376' in 101 steps}\}$

12. Which of the following statements is **false**?

    ○ Vertex-Cover is efficiently reducible to the Knapsack problem.

    ○ All languages that can be efficiently verified are decidable.

    ○ If P = NP, then all NP-complete problems are in coNP.

    ○ If NP $\neq$ coNP, there is at least one NP-hard language that is in coNP.

UNIQNAME (print): ____________________

Shorter Answer – 34 points

1. **Encryption**

   (10 points) Sarah and Matt wish to communicate securely and so they need to obtain a shared secret key k, but they can only communicate over an *nonsecure* channel! So, they turn to the Diffie-Hellman protocol to establish their secret key. They pick their favorite prime $p = 19$ and a generator $g = 4$ (wait a second, 4 is not a generator for $\mathbb{Z}_{19}$! 4 does not generate 18 mod 19, for example) Sarah then picks the private key $a = 5$ and Matt picks the private key $b = 16$.

   (a) Compute Sarah's and Matt's public keys A and B as well as their shared secret key, k.

   (b) Their arch nemesis, Eve, has been eavesdropping the whole time! What are **all** the parameters that Eve is able to extract *without performing any computation*?

   (c) Notice that a generator was not used here at all, but this procedure worked fine. Using a generator is not necessary for the correctness of Diffie-Hellman. Why is it that we *prefer* to use generators (or elements that can generate close to the entirety of $\mathbb{Z}_p^*$ - *"almost generators"*)? Your justification does not need to be lengthy, 2-3 sentences suffices.

2. (10 points) Suppose you have $n \geq 2$ bins. You independently toss n^2 balls at the bins, uniformly at random. You may find formulas on the first page to be helpful.

   (a) For each $i \in \{1, \ldots, n\}$, what is the expected number of balls in bin i?

   (b) Use Markov's inequality to bound the probability that bin i has at least $2n$ balls.

   (c) Use Chernoff-Hoeffding to bound the probability that bin i has at least $2n$ balls.

3. (4 points)

   Prove or disprove the following statement *assuming* $\mathsf{P} \neq \mathsf{NP}$

   Suppose $L \in \mathsf{NP}$, and $L \leq_p$ SAT, then $L \in \mathsf{NP}$-complete.

4. (10) Exactly two of the following statements are known to be true. Fill in the circle next to the true statements and then briefly show why each of the those two statements are true. For the statements you think are false, you do not need to prove anything. **You are to assume $\mathsf{P} \neq \mathsf{NP}$.**

   ○ $A \leq_p A$ for any language $A \in$ NP.

   ○ (L is undecidable) $\implies$ ($L \in$ NP)

   ○ $(L \in P) \implies (\overline{L} \in P)$.

   ○ (($A \leq_p B$) and ($B \in$ NP-hard)) $\implies$ ($A \in$ NP-hard)

Proofs and longer questions – 30 points

Answer two of the following three questions. **Clearly cross out the question you do not want graded.** If it isn't clear what problem you don't want graded, we will grade the first two. Each of the two questions are worth 15 points.

1. Let A be a array of n items each with a weight of A[i]. Given a integer size B, and a capacity, K, we say that the array is "packable" if we can split it up into K partitions such that the sum of each partition is less than or equal to B. Formally we define:

   $$\textsc{Packable} = \{\langle A, B, K\rangle \mid \text{An array } A \text{ with } n \text{ elements, with each element a rational number, can be partitioned into } K \text{ subarrays such that the sum of each subarray is less than or equal to an integer B.}\}$$

   (a) Show that Packable $\in$ NP

   (b) Show that Packable $\in$ NP-Hard. HINT: You may use the fact that that

   $$\text{PARTITION} = \{\langle A\rangle : \text{A is a set of } 2m \text{ numbers which can be partitioned into 2 non-intersecting subsets with equal sums}\}$$

   is NP-Complete.

   The next page has been left blank, please keep your answer on this page and the next.

This page left blank, please use only for proof problem 1

UNIQNAME (print): ______________________________

2. Bob is sending a message to Alice using the RSA algorithm as taught in class. Say that Bob wishes to communicate message m and thus sends $m' = m^e \bmod n$ as normal, where e is Alice's public key. Eve knows e, the RSA modulus n, and the encoded message m'. In this problem, we consider the classic model of computation. (In particular, we exclude quantum algorithms.) Hence, you may assume that there is no (publicly) known efficient way to find m given only e, n, and m'.

   (a) If Eve knows the factors of n, is there a (publicly) known efficient algorithm for Eve to find m? If so, provide that algorithm, an argument as to why that algorithm works, and an explanation as to why that algorithm is efficient. If not, explain how you know that.

   (b) Suppose Bob's friend Carl spills the beans to Eve and tells her the correct value of m which encrypts to m'. Now Eve has access to m in addition to all the public information she already had. Is there any (publicly) known efficient algorithm that she could use to factor n given this information, i.e., message m, its ciphertext m', RSA modulus n, and public key e? If so, provide that algorithm, an argument as to why that algorithm works, and an explanation as to why that algorithm is efficient. If not, explain how you know that.

3. In the original 3SAT problem, a clause is satisfied if at least one of its literals is true. Suppose we modify the 3SAT problem such that a clause is satisfied only if at least one of its literals is true and at least one of its literals is false. We name this problem 3SATFT. Given an arbitrary **exact** 3CNF formula ϕ (i.e. within any given clause, there are 3 distinct variables), prove that there exists an assignment that satisfies 3/4 of the clauses for 3SATFT.

This page intentionally left blank.

If you have answers on this page be certain you write “answer continues on page 13” under the actual question.

This page intentionally left blank.

If you have answers on this page be certain you write “answer continues on page 14” under the actual question.