CS 5/7350 – Test 3
April 26, 2023

Name: _____

- This exam is **closed book** and **closed notes**.
- You MAY have the approved TI-30Xa calculator
- No cell phones, or other electronics except as required for zoom and only used for zoom or other proctoring.
- Pencil and/or pen are permitted.
- It is **3 hours** in duration plus time for scanning and uploading, etc.
- You should have xx problems. Pay attention to the point value of each problem and dedicate time as appropriate.

*On my honor, I have* neither given nor received unauthorized aid on this exam.

SIGNED:_____

DATE:_____

CS 5/7350 – Test #3
April 26, 2023

Name: _____

ID:_____
[+ 7 pts for max quiz score for 5350 students]

1. [6 pts] You want to prove that some problem $P_A$ is NP-Complete. You know that problem $P_H$ is NP-Hard. Mark the following statements as **True** or **False**.

   (i) _____ You need to prove that $P_A$ can be verified in polynomial time.

   (ii) _____ You need to prove that $P_H$ can be verified in polynomial time.

   (iii) _____ You need to prove that a solver for $P_A$ can also solve $P_H$.

   (iv) _____ You need to prove that a solver for $P_H$ can also solve $P_A$.

   Other questions to answer mark the following statements as **True** or **False**.

   (i) _____ The difference between NP-Complete problems and NP-Hard problems is that NP-Complete problems can also be verified in polynomial time.

   (ii) _____ Some Problems in NP can be solved in Polynomial Time

2. [6 pts] We have Big-Oh, Little-Oh, Big-Omega, Little-Omega and Big-Theta for asymptotic bounding functions. Why is there no Little-Theta ?

3. [6 pts] You have the following table computing the Longest Increasing Subsequence (Treat the 99s as if they are infinity and not a part of the sequence) .

| Index | Value | 99 | 99 | 99 | 99 | 99 | 99 | 99 | 99 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | 5 | 99 | 99 | 99 | 99 | 99 | 99 | 99 |
| 2 | | 5 | 8 | 99 | 99 | 99 | 99 | 99 | 99 |
| 3 | | 5 | 8 | 9 | 99 | 99 | 99 | 99 | 99 |
| 4 | | 5 | 7 | 9 | 99 | 99 | 99 | 99 | 99 |
| 5 | | 5 | 7 | 9 | 13 | 99 | 99 | 99 | 99 |
| 6 | | 5 | 7 | 9 | 13 | 15 | 99 | 99 | 99 |
| 7 | | 5 | 7 | 9 | 13 | 14 | 99 | 99 | 99 |
| 8 | | 5 | 7 | 9 | 10 | 14 | 99 | 99 | 99 |
| 9 | | 5 | 7 | 8 | 10 | 14 | 99 | 99 | 99 |
| 10 | | 5 | 7 | 8 | 10 | 12 | 99 | 99 | 99 |
| 11 | | 4 | 7 | 8 | 10 | 12 | 99 | 99 | 99 |
| 12 | | 3 | 7 | 8 | 10 | 12 | 99 | 99 | 99 |
| 13 | | 3 | 7 | 8 | 9 | 12 | 99 | 99 | 99 |
| 14 | | 3 | 5 | 8 | 9 | 12 | 99 | 99 | 99 |
| 15 | | 3 | 5 | 6 | 9 | 12 | 99 | 99 | 99 |
| 16 | | 3 | 5 | 6 | 7 | 12 | 99 | 99 | 99 |
| 17 | | 3 | 5 | 6 | 7 | 12 | 13 | 99 | 99 |
| 18 | | 3 | 5 | 6 | 7 | 11 | 13 | 99 | 99 |
| 19 | | 3 | 5 | 6 | 7 | 11 | 13 | 15 | 99 |
| 20 | | 3 | 5 | 6 | 7 | 9 | 13 | 15 | 99 |
| 21 | | 3 | 5 | 6 | 7 | 9 | 12 | 15 | 99 |

(i) What is the Longest Increasing Subsequence?

(ii) How Long is the Longest Increasing Subsequence?

(iii) What does the value 6 mean in row 21

4. [6 pts] You are filling in the table for the Longest Common Subsequence between two strings. One string ends in "TCC" and the other ends with GTC. Parts of the table which have been previously filled out are either shown or greyed out.

   (i) Fill in the remaining 9 cells at the bottom right.
   (ii) What is the length of the Longest Common Subsequence?

| LCS | | | | | | G | T | C |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | 1 | 2 | 2 | 2 |
| T | | | | | 2 | | | |
| C | | | | | 3 | | | |
| C | | | | | 3 | | | |

5. [6 pts] You are filling in the table for the Levenshtein Edit Distance between two strings. One string ends in "TCC" and the other ends with GTC. Parts of the table which have been previously filled out are either shown or greyed out.

   (i) Fill in the remaining 9 cells at the bottom right.
   (ii) What is the length of the Levenshtein Edit Distance Subsequence?

| LED | | | | | | T | T | C |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | 2 | 3 | 4 | 5 |
| T | | | | | 3 | | | |
| C | | | | | 4 | | | |
| C | | | | | 5 | | | |

6. [6 pts] Argue that the problem F of finding the maximum flow from a single source in a graph to a single sink in a graph is just as hard or possibly harder ( within a factor of $\Theta(|V|)$ ) than the problem M of finding the maximum flow from a set of multiple sources to a set of multiple sinks in a graph.

7. [8 pts] Consider an RSA encryption system that has a public key of 68719 for the value e and 482431 for the value of the modulus N. You also saw a message that had been encrypted by the public key. The value of this encrypted message was 8.

   (i) You are able to factor N=482431 into the product of two prime numbers 613 * 787. What is the value of the private key? Show your work including the table for computing the Extended Euclidean Algorithm.

   (ii) What was the message before it was encrypted (Give a formula and an integer)

8. [8 pts] Answer the following graph related questions. When necessary, use vertex "S" as the starting vertex:

   (i) Create a graph that contains a cycle and the weight of the third edge chosen with Prims Minimum Spanning Tree Algorithm is less than the weight of the third edge chosen with Kruskal's Minimum Spanning Tree Algorithm. Mark the third edge chosen by prim's algorithm with a "P" and the third edge chosen by Kruskal's algorithm with a "K".

   (ii) Create a graph that is not a tree and the weight of the third edge chosen with Kruskal's Minimum Spanning Tree Algorithm is less than the weight of the third edge chosen with Prims Minimum Spanning Tree Algorithm. Mark the third edge chosen by prim's algorithm with a "P" and the third edge chosen by Kruskal's algorithm with a "K".

   (iii) Create a graph that has a Hamiltonian Cycle, but not an Euler Tour

   (iv) Create a graph where the sum of the degrees of the vertices is odd or explain why one can't exist.

9. [6 pts] Answer the following questions:

   (i) A program requires 5 days to brute force attack an encryption key of 64 bits. If the running time is $\Theta(2^n)$ about how many bits could you brute-force attack in 4 years.

   (ii) A program requires 5 days to brute force attack an encryption key of 64 bits. If you have access to an algorithm and computer where the running time is $\Theta(n^2)$ about how many bits could you brute-force attack in 4 years.

10. [6 pts] Implementation Ix solves Problem Px and Implementation Ix is $\Theta(n!)$:

   (i) Problem Px is O(n!) Circle one: (yes, no, maybe)

   (ii) Problem Px is O(n) Circle one: (yes, no, maybe)

   (iii) Problem Px is O(1) Circle one: (yes, no, maybe)

11. [8 pts] Use the DGT algorithm discussed in class to determine how to represent the value 393 using the number system $\beta=5$, D = { -7, -3, 0, 1 }. Show your work.

12. [8 pts] A message contains the following number of each symbol:

20 A’s, 14 B’s, 12 C's, 8 D's, 6 E's, 6 F's, 4 G's, 2 H and 2 K.

Create a Huffman coding for each symbol:

How many bits are in the entire Huffman coded message?

How much entropy does each “C” have?

13. [6 pts] You are guessing an integer, N, between 1 and almost infinity. You may ask true/false questions to determine the number. Give a procedure you can follow to guess the number with $\Theta$ (lg (N)) guesses. (Hint, this may be 2*lg(N) or 3*lg(N), etc.)

14. [8 pts] You run different programs for various values of "n" and create 4 tables of the runtimes. Give the asymptotic bounds that each table supports.

a.

| n | time (ms) |
|---|---|
| 20 | 423 |
| 30 | 923 |
| 40 | 1623 |
| 50 | 2523 |
| 60 | 3623 |
| 70 | 4923 |
| 80 | 6423 |
| 90 | 8123 |
| 100 | 10023 |

b.

| n | time (ms) |
|---|---|
| 10 | 11153 |
| 20 | 161153 |
| 30 | 811153 |
| 40 | 2561153 |
| 50 | 6251153 |
| 60 | 12961153 |
| 70 | 24011153 |
| 80 | 40961153 |
| 90 | 65611153 |

c.

| n | time (ms) |
|---|---|
| 10 | 3.321928 |
| 20 | 4.321928 |
| 30 | 4.906891 |
| 40 | 5.321928 |
| 50 | 5.643856 |
| 60 | 5.906891 |
| 70 | 6.129283 |
| 80 | 6.321928 |
| 90 | 6.491853 |

d.

| n | time (ms) |
|---|---|
| 10 | 1396 |
| 20 | 1048948 |
| 30 | 1.07E+09 |
| 40 | 1.1E+12 |
| 50 | 1.13E+15 |
| 60 | 1.15E+18 |
| 70 | 1.18E+21 |
| 80 | 1.21E+24 |
| 90 | 1.24E+27 |

15. [6 pts] Two people need to establish a secret key for encrypting communications. They agree to use a Diffie-Hellman key exchange with a modulus of 13 and decide on 2 as the base. Person A chooses a random value of 4 and person B chooses a random value of 9.

    a. What is the value Person A sends to Person B

    b. What is the value Person B sends to Person A

    c. What is the shared secret key between Person A and Person B

16. [4 pts Extra Credit] Answer the following questions:

(i) What is the length of the Longest Common Subsequence of the following (Note, you do not have to show any work)?

String A = ZYXWVUTSRQ and String B = 1234567890

(ii) What is the Levensthein Edit Distance of the following two strings (Note, you do not have to show any work)

String A = ABC and String B = ABC

(iii) You have 4 sixteen-sided die. Each dice has sides of all ones:

{1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1}.
How many ways can you roll a 0 with these die
(you do not have to set up the table):

(iv) How many swaps are required to create a min-heap from an array that is already sorted in ascending order?

(v) How many cycles does a tree with 4 vertices have?

(vi) How many edges does a tree with 1 vertex have?

(vii) How would you represent the value 0 in the number system
$\beta = 7$, D = {-2, -1, 0, 1, 2, 3, 4 }

(viii) How much entropy is in the following message: A A A A A A A A A