CS 5/7350 – Test 3
April 26, 2023

Name: Bingying Liang

- 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: Bingying Liang

DATE: Apr 27, 2023

CS 5/7350 – Test #3
April 26, 2023

Name: Bingying Liang

ID: 48999397

[+ 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) True You need to prove that P_A can be verified in polynomial time.

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

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

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

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

2. [6 pts] We have Big-Oh (O), Little-Oh (o), Big-Omega (Ω), Little-Omega (ω) and Big-Theta (Θ) for asymptotic bounding functions. Why is there no Little-Theta ?

   Because there is not notion of strict equality versus unstrict equality. If little Theta exist it will redundant the existing asymptotic notations Big-Theta: Provides both an upper and lower bound on the growth rate of a function, stating that the function's growth rate is asymptotically equal to other function.
   It doesn't need to have 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?

5, 8, 9, 10, 12, 13, 15

(ii) How Long is the Longest Increasing Subsequence?

7

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

6 is the smallest ending value of a subsequence of length 6.

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	2	3	3
C					3	3	3	4
C					3	3	3	4

(ii) 4

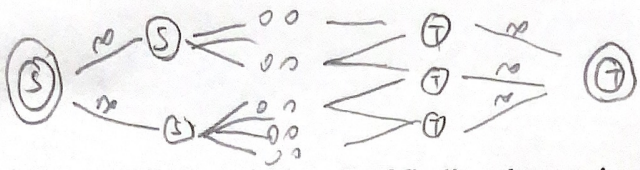
5. [6 pts] You are filling in the table for the Levenshtein Edit Distance between two strings. One string ends in "TCC" and the other ends with GTC. Parts of the table which have been previously filled out are either shown or greyed out.

   (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	2	3	4
C					4	3	3	3
C					5	4	4	3

(ii) 3

Example:



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.

sol: The problem F of finding the maximum flow from a single source in a graph to a single sink in agraph is just as hard or possibly harder (within a factor of $\Theta(|V|)$) than the problem M. since a solver for the problem F can solve the problem M. This is done by treat a set of multiple sources as a single super source. Then we can use the solver of problem F to solve the M problem. I draw a simple graph as the example.

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.

sol: public key: $(e,n) = (68719, 482431)$

private key: (d,n)

$d = \frac{1}{e} \bmod \Phi(n) = \frac{1}{68719} \bmod \Phi(482431)$

$\Phi(482431) = \Phi(613 \times 787) = (613-1)\times(787-1)$

$= 612 \times 786 = 481032$

$\therefore d = \frac{1}{68719} \bmod 481032$

	r	B	Q	R	α	β
-1					1	0
	481032	68719	6	68718	0	1
	68719	68718	1	1	1	-6
	68718	1	68718	0	-1	7
	1	0	-	-	68719	-481032

$7 \times 68719 = 481033 \quad 1 \times 481032 = 481032$

$\therefore -1 \times 481032 + 7 \times 68719 = 1$

$0 + (7 \times 68719) \bmod 482432 = 1$

$\therefore d = 7$

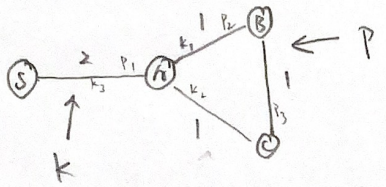
$\therefore$ private key: $(7, 482431)$

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

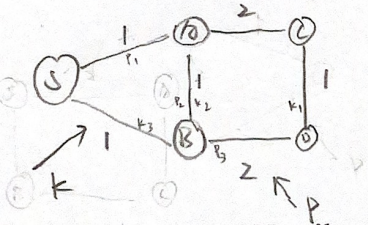
$8^7 \bmod 482431 = 2097152 \bmod 482431 = 167428$

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

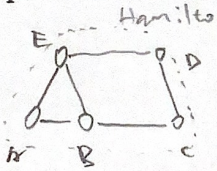
(i) Create a graph that contains a cycle and the weight of the third edge chosen with Prims Minimum Spanning Tree Algorithm is less than the weight of the third edge chosen with Kruskal's Minimum Spanning Tree Algorithm. Mark the third edge chosen by prim's algorithm with a "P" and the third edge chosen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



like B. it is degree of 3.
For Euler Tour, it will no way our.
Therefore, it is 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.

The graph can't exist.

Because each edge ends at two vertices. If there is no edge, just a single vertice (A) its degree is 0, which is even. When you want an edge, it will connect two vertices. which means it will create two degrees.

Sum = 2E

∴ Sum must be even.

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.

4 years = 4×365 = 1460 days

suppose x bits.

$\frac{2^x}{2^{64}} \times 5 = 1460 \Rightarrow 2^x = \frac{1460}{5} \times 2^{64}$

$2^x = 292 \times 2^{64}$

$x = \log_2(292 \times 2^{64})$

$x = \log_2(73 \times 2^{66})$

$x = \log_2 73 + \log_2 2^{66}$

$= 66 + \log_2 73$

≈ 72.196 bits

(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.

4 years = 1460 days

suppose x bits

$\frac{x^2}{64^2} \times 5 = 1460$ $\left(\frac{x}{64}\right)^2 = 292$ $\therefore x = \sqrt{292} \times 64 \approx 1093.63$ bits.

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.

Sol. $-7 \bmod 5 = 3$

$-3 \bmod 5 = 2$

$393 \bmod 5 = 3 \Rightarrow (-7)$

$393 - (-7) = 400$

$400 \div 5 = 80$

$80 \bmod 5 = (0)$

$80 - 0 = 80$

$80 \div 5 = 16$

$16 \bmod 5 = (1)$

$16 - 1 = 15$

$15 \div 5 = 3$

$3 \bmod 5 = 3 \Rightarrow (-7)$

$3 - (-7) = 10$

$10 \div 5 = 2$

$2 \bmod 5 = 2 \Rightarrow (-3)$

$2 - (-3) = 5$

$5 \div 5 = 1$

$1 \bmod 5 = (1)$

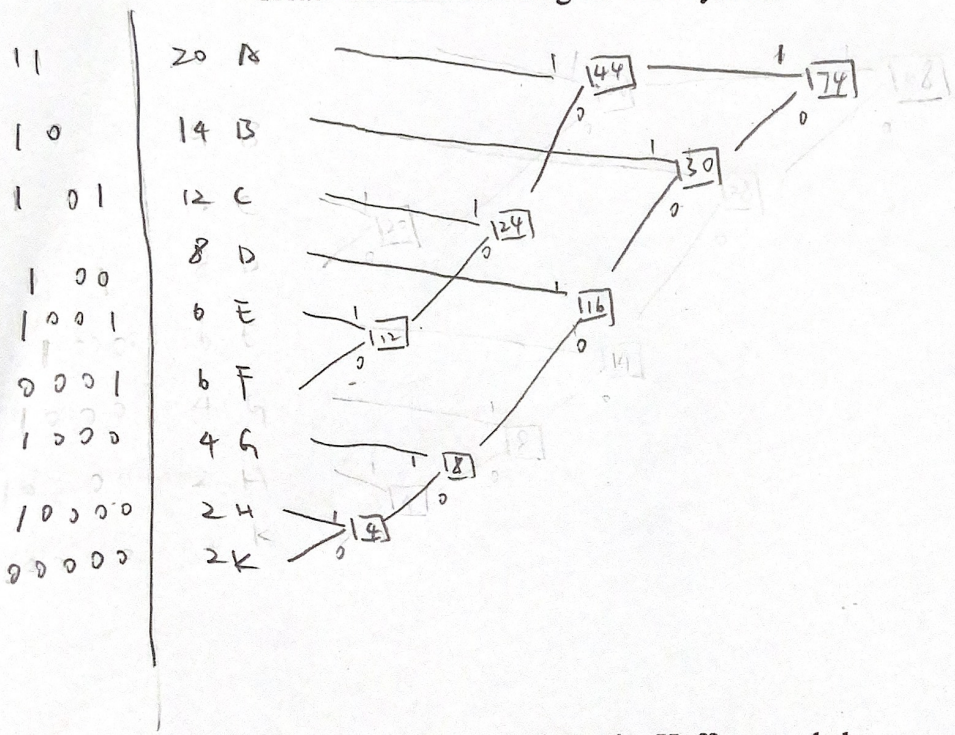
$1 - 1 = 0$

$\therefore \quad 1\ 3\ 7\ 10\ 7$

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?

$20\times2 + 14\times2 + 12\times3 + 8\times3 + 6\times4 + 6\times4 + 4\times4 + 2\times5 + 2\times5 = 40 + 28 + 36 + 24 + 24 + 24 + 16 + 10 + 10 = 212$ bits

How much entropy does each "C" have?

$$P_C = \frac{12}{20+14+12+8+6+6+4+2+2} = \frac{12}{74} = \frac{6}{37}$$

$$\log_2 \frac{1}{P_C} = \log_2 \frac{1}{\frac{6}{37}} = \log_2 \frac{37}{6} \approx 2.62 \text{ bits}$$

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 Θ (lg (N)) guesses. (Hint, this may be 2*lg(N) or 3*lg(N), etc.)

We can use binary search to solve this problem.

sol:

```
public boolean search (int[] nums, int target){
    if (nums == null || num length = 0){
        return false;
    }

    left = 0;
    right = num.length - 1;
    while (left <= right){
        int mid = left + right - 1;
        if (guess == target){ return true;}
        else if (guess < target){ left = mid + 1;}
        else { right = mid - 1;}
    }
    return false;
}
```

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

$\Theta(n^2)$

b.

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

$\Theta(n^4)$

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

$\Theta(\sqrt[3]{n})$

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

$\Theta(2^n)$

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

$2^4 \bmod 13 = 16 \bmod 13 = 3$

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

$2^9 \bmod 13 = 512 \bmod 13 = 5$

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

$3^9 \bmod 13 = 19683 \bmod 13 = 1$

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

0

(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

0

(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):

0

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

0

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

0

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

0

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

0

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

0