CSE 7350 – Test 2
April 12, 2023

Name: Bingying Liang

ID 48999397

95

- This exam is **closed book** and **closed notes.**
- No cell phones, or other electronics.
- Pencil and/or pen and TI-30Xa calculator only are permitted. No sharing of calculators.
- It is **3 hours** in duration.
- You should have 12 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: 04.13.2023

CSE 7350 – Exam #2
April 12, 2023

Name: Bingying Liang

ID: 48999397

[+5 pts for CS-5350 students]

10

1. [10 pts] An implementation requires 3 days to run for an input size of 64. How long would the implementation take to run for an input size of 128 if:

   (i) The implementation is $\Theta(n^3)$?

   $\frac{128^3}{64^3} \times 3 = (\frac{128}{64})^3 \times 3 = 2^3 \times 3 = 8 \times 3 = 24$ days

   (ii) The implementation is $\Theta(n)$?

   $\frac{128}{64} \times 3 = 2 \times 3 = 6$ days

   (iii) The implementation is $\Theta(n^2)$?

   $\frac{128^2}{64^2} \times 3 = 2^2 \times 3 = 4 \times 3 = 12$ days

   (iv) The implementation is $\Theta(n!)$?

   $\frac{128!}{64!} \times 3$ days

   (v) The implementation is $\Theta(2^n)$?

   $\frac{2^{128}}{2^{64}} \times 3 = 2^{64} \times 3$ days

4

2. [6 pts] Set up the table and show the Extended Euclidean Algorithm for computing 1/23 modulo 15717. Give the answer as well:

sol: $\frac{1}{23}$ mod 15717

	A	B	Q	R	α	β
-1					1	0
	15717	23	683	8	0	1
	23	8	2	7	1	-683
	8	7	1	1	-2	1367
	7	1	7	0	3	-2050
	1	0	–	–	-23	15717

$-3 \times 15717 + 2050 \times 23 = 1$

$(-3 \times 15717)\% 15717 + (2050 \times 23)\% 15717 = 1$

$0 + (2050 \times 23)\% 15717 = 1$

$\because (\frac{1}{23} \times 23)\% 15717 = 1$

$\therefore \frac{1}{23}$ mod 15717 = 2050 mod 15717

$= \cancel{2050}$

-2050

$= 13667$

3. [10 pts] Consider an RSA encryption system that has a public key of 294947 for the value e and 812909 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 is 3.

10

(i) You are able to factor N=561233 into the product of two prime numbers 853 * 953. What is the value of the private key? Show your work including the table for computing the Extended Euclidean Algorithm.

sol: public key: $(e,n) = (294947, 812909)$

private key: $(d,n) = (d, 812909)$

$d = \frac{1}{e} \bmod \Phi(n) = \frac{1}{294947} \bmod \Phi(812909)$

$\Phi(812909) = \Phi(853 \times 953) = (853-1)\times(953-1) = 852 \times 952 = 811104$

$\therefore d = \frac{1}{294947} \bmod 811104$

A	B	Q	R	α	β
-1				1	0
811104	294947	2	221210	0	1
294947	221210	1	73737	1	-2
221210	73737	2	73736	-1	3
73737	73736	1	1	3	-8
73736	1	73736	0	-4	11
1	0	–	–	294947-811104	

$-4 \times 811104 + 11 \times 294947 = 1$

$\therefore (11 \times 294947) \bmod 811104 = 1$

$\because (\frac{1}{294947} \times 294947) \bmod 811104 = 1$

$\therefore d = \frac{1}{294947} \bmod 811104 = 11$

$\therefore$ private key: $(11, 812909)$

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

$3^{11} \% 812909 = 177147 \% 812909 = 177147$

7

4. [10 pts] Set up the table to find the longest increasing sub-sequence of the following sequence: 5, 6, -3, 9, -1, 10, 4, 7, 8, -2, 6, 9, 7, 5, 2

5	5								
6	5	6							
-3	-3	6							
9	-3	6	9						
~~-1~~	-1	6	9						
10	-1	6	9	10					
~~4~~	4	6	9	10					
7	4	6	7	10					
8	4	6	7	8					
-2	-2	6	7	8					
6	-2	6	7	8					
9	-2	6	7	8	9				
7	-2	6	7	8	9				
~~5~~	5	6	7	8	9				
2	2	6	7	8	9				

∴ The longest increasing sub-sequence is : 5 6 7 8 9

10

5. [10 pts] Consider the Levensthein Edit Distance for two strings A and B.

(i) Write the equation describing what you would put in the table for location T[i,j].

if (i==0) { T[i,j] = T[0,j] }
if (j==0) { T[i,j] = T[i,0] }
if (Ai == Bj) { T[i,j] = min { T[i-1,j]+1, T[i,j-1]+1, T[i-1,j-1] } }
else { T[i,j] = min { T[i-1,j]+1, T[i,j-1]+1, T[i-1,j-1]+1 } }.

(ii) Fill in the following table for finding the "Levensthein Edit Distance" for two strings, M and N

M = A B X B Y C N = A Z X B C Y

N \ M	-	A	B	X	B	Y	C	
-	0	1	2	3	4	5	6	
A	1	0	1	2	3	4	5	
Z	2	1	1	2	3	4	5	
X	3	2	2	1	2	3	4	
B	4	3	2	2	1	2	3	
C	5	4	3	3	2	2	2	
Y	6	5	4	4	3	2	3	

The "Levensthein Edit Distance is 3.

6

6. [6 pts] Using n_0 equal to 10, find the tightest C_1 and C_2 possible to show that

$f(n) = 5n^3 + 6n^2 + 2n + 18$ is $\Theta(n^3)$.

Sol: $\Omega(n^3)$: $0 \le c_1 g(n) \le f(n)$, $\forall n \ge n_0 = 10$

$0 \le c_1 n^3 \le 5n^3 + 6n^2 + 2n + 18$, $\forall n \ge n_0 = 10$

$c_1 \le 5 + \frac{6}{n} + \frac{2}{n^2} + \frac{18}{n^3}$, $\forall n \ge n_0 = 10$

$c_1 \le 5 + \frac{6}{10} + \frac{2}{10^2} + \frac{18}{10^3}$

$c_1 \le 5 + 0.6 + 0.02 + 0.018$

$c_1 \le 5.638$

$\therefore$ c_1 can be 5

$O(n^3)$: $0 \le f(n) \le c_2 g(n)$, $\forall n \ge n_0 = 10$

$0 \le 5n^3 + 6n^2 + 2n + 18 \le c_2 n^3$, $\forall n \ge 10$

$5 + \frac{6}{n} + \frac{2}{n^2} + \frac{18}{n^3} \le c_2$

$5 + \frac{6}{10} + \frac{2}{10^2} + \frac{18}{10^3} \le c_2$

$5.638 \le c_2$

$\therefore$ c_2 can be 5.638

$\therefore$ We can find the tightest $c_1 = 5$, $c_2 = 5.638$ possible to show $f(n) = 5n^3 + 6n^2 + 2n + 18$ is $\Theta(n^3)$

7. [10 pts] Consider the Longest Common Subsequence for two strings A and B.

10

(iii) Write the equation describing what you would put in the table for location T[i,j].

if (i==0){ T[i,j]=0}
if (j==0){ T[i,j]=0}
if (Ai == Bj) { T[i,j] = T[i-1, j-1]+1 }
else { T[i,j] = max{T[i-1, j], T[i, j-1]} }

(iv) Fill in the following table for finding the "Longest Common Subsequence" for two strings, M and N

M = A B X B Y C   N = A Z X B C Y

N \ M	-	A	B	X	B	Y	C	
-	0	0	0	0	0	0	0	
A	0	1	1	1	1	1	1	
Z	0	1	1	1	1	1	1	
X	0	1	1	2	2	2	2	
B	0	1	2	2	3	3	3	
C	0	1	2	2	3	3	4	
Y	0	1	2	2	3	4	4	

The longest Common Subsequence is A X B C

10

8. [10 pts] You are interested in purchasing the items listed below. You have 12 points you can use to purchase items and you plan to pay cash for the rest. Setup and fill in the entire dynamic programming table for the problem and indicate which items you would use points for.

Item 1: 3 points, $5
Item 2 5 points, $8
Item 3: 7 points, $9
Item 4: 4 points, $5
Item 5: 2 points, $4

$ items / points	item 1	item 1, 2	item 1, 2, 3	item 1, 2, 3, 4	item 1, 2, 3, 4, 5	
2	0	0	0	0	4	
3	5	5	5	5	5	
4	5	5	5	5	5	
5	5	8	8	8	9	
6	5	8	8	8	9	
7	5	8	9	10	12	
8	5	13	13	13	13	
9	5	13	13	13	14	
10	5	13	14	14	17	
11	5	13	14	14	17	
12	5	13	17	18	18	

item 1, item 3, item 5

10

9. [10 pts] You have 3 different dice that are not evenly weighted:
   - Dice 1 has sides {1,2,3} and a 20% chance of rolling a 1, a 30% chance of rolling a 2 and a 50% chance of rolling a 3. 20% 30% 50%
   - Dice 2 has sides {2,2,3,3,3,4,4} with a 20% chance for each 2, a 10% chance for each 3 and a 15% chance for each 4. 40% 30% 30%
   - Dice 3 has sides {1,1,2,2} with a 20% chance for each 1, a 30% chance for each 2 40% 60%
   - Set up the table for the dynamic programming algorithm (using percentages instead of counts) and fill in the complete column for Dice 1 and Dice 2 and Dice 3.
   - What is the probability of rolling a 6 with these dice?

Probability \ Dices / roll	1	1,2	1,2,3	
1	20%	0	0	
2	30%	0	0	
3	50%	8%	0	
4	0	18%	3.2%	
5	0	35%	12%	
6	0	24%	24.8%	
7	0	15%	30.6%	
8	0	0	20.4%	
9	0	0	9%	
Sum probility	1	1	1	

∴ The probability of rolling a 6 with these dice is 24.8%.

54321
12345
54321

6

10. [6 pts] Argue that the Problem I of finding the longest increasing subsequence is just as hard or possibly harder (with in $\Theta(n)$ extra work) than the Problem D of finding the longest decreasing subsequence

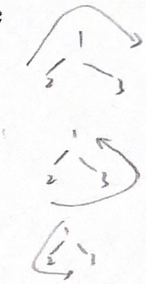
Sol: Assume we have a solver for Problem I of finding the longest increasing subsequence. We can use the solver to find the longest decreasing subsequence with $\Theta(n)$ extra work: Reversing the sequence first + find the longest increasing subsequence + Reverse the result!

11. [6 pts] You have a tree with the following in-order and pre-order traversals. Draw the tree:

in:

post:

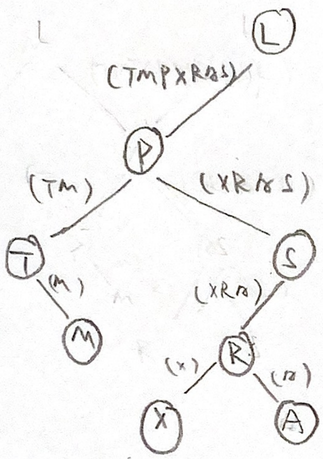
pre



6

IN ORDER: T M P X R A S L
POST_ORDER: M T X A R S P L

sol:

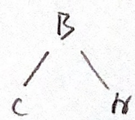


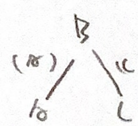
12. [6 pts] Give an in-order and pre-order traversal that cannot form a tree:

6

In order: A B C

pre order: B C A





Pre: BAC is not BCA.