CS 5/7350 – Test 2
April 21, 2021

Name: ________________________

- This exam is **closed book** and **closed notes**.

[redacted]

- 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 10 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 #2
April 21, 2021

Name: ________________________

P & NP on Test 3 Spr 2023

ID:______________________________

1. [8 pts] Consider the following NP completeness questions. Answer them with "some" "all" "none" or "unknown"

(i) Which Problems in NP are also in P? ("some" "all" "none" or "unknown")

Unknown

(ii) Which problems in NP are also in NP-Hard? ("some" "all" "none" or "unknown")

Some

(iii) If someone can solve the Circuit Sat problem in Polynomial Time, then all NP and all NP complete problems can be solved in Polynomial Time? (True or False)

<Skip - Circuit Sat problem not covered>

(iv) NP means Non-Polynomial? (True or False)

False - Nondeterministic Polynomial-time

(v) Some NP problems can be solved in polynomial time? (True or False)

True

(vi) Which NP-Hard Problems are also NP-Complete? ("some" "all" "none" or "unknown")

Some

2. [8 pts] Argue that the Hamiltonian Cycle is NP-Complete given that the Hamiltonian Path is NP-Complete

<Skipping - Not covered yet>

3. [7 pts] Compute the value for Z given that ((161 * Z) + 5729) modulo 11609 = 11169
161Z mod 11609 + 5729 mod 11609 = 11169 mod 11609
161Z mod 11609 = (11169 - 5729) mod 11609
161Z mod 11609 = 5440 mod 11609
Z mod 11609 = 1/161 mod 11609 * 5440 mod 11609

k	A	B	Q	R	alpha	beta
-1					1	0
0	11609	161	72	17	0	1
1	161	17	9	8	1	-72
2	17	8	2	1	-9	649
3	8	1	8	0	19	-1370

19*11609 mod 11609 -1370*161 mod 11609 = 1 mod 11609
(11609 - 1370) mod 11609 = 1/161 mod 11609
1/161 mod 11609 = 10239
Z mod 11609 = (10239*5440) mod 11609
Z mod 11609 = 178 mod 11609
Z = 178 + i*11609, where i is an integer.
When i = 0, Z = 178

4. [8 pts] How many colors are needed to color the following special graphs:

(i) A complete graph with |V| vertices. |V| colors - Every vertex is connected to every other vertex and no two adjacent vertices can have the same color, so |V| distinct colors are required.

(ii) A cycle with an odd number of vertices 3 colors - Vertices all have max degree 2, so max 3 colors are required. Because the graph has an odd number of vertices, if you begin coloring at one vertex, you can alternate between colors until the last vertex. The last vertex would require a different color or else it would get the same color as the starting vertex that it shares an edge with.

(iii) A tree. 2 colors - All trees are bipartite. All bipartite graphs are 2-colored because vertices belong to either one set or the other with no shared edges between vertices in the same set.

(iv) A bipartite graph with 8 vertices in one partition and 9 vertices in the other partition. 2 colors - All bipartite graphs are 2-colored because vertices belong to either one set or the other with no shared edges between vertices in the same set.

5. [12 pts] You have 4 dice. Each one is different. Die #1 has sides { -1, 0, 1 }. Die #2 has sides { -2, -2, 0, 0 } Die #3 has sides {1, 1, 1, 1} and Die #4 has sides {0,0,0, 2,2,2}

(i) Fill in the table below

(ii) How many ways can you roll a 0 with these 4 dice?

72 ways

(iii) What is the probability of rolling a 0 with these 4 dice?

Total possible rolls = 3 * 4 * 4 * 6 = 288

P(6) = 72/288 = 1/4

(iv) How many ways can you roll a 4 with these 4 dice?

24 ways

(v) What is the probability of rolling a 4 with these 4 dice?

P(4) = 24/288 = 1/12

Roll	Die 1	Die 2	Die 3	Die 4
-3	0	(-1,-2) 2	0	0
-2	0	(0, -2) 2	(-3,1) 8	(-2,0) 24
-1	1	(-1,0) 2 (1,-2) 2 4	(-2,1)8	(-1,0) 24
0	1	(0,0) 2	(-1,1) 16	(-2,2) 24 (0,0) 48 72
1	1	(1,0) 2	(0,1) 8	
2	0	0	(1,1) 8	
3	0	0	0	
4	0	0	0	(2,2) 24

6. [12 pts] In the standard definition of a longest increasing subsequence of integers, each value must be at least 1 greater than the one before it. Consider, now, a longest 2-increasing subsequence where each value must differ by at least 2 instead of 1.

As an example, if the original sequence is 6,2,3,4,7 a regular longest increasing subsequence would be 2,3,4,7 but a longest 2-increasing subsequence would be 2,4,7.

Create the table for the longest 2-increasing subsequence of the sequence below and give the sequence:

3, 9, 6, 7, 14, 8, 11, 17, 12, 13, 20, 16, 17, 18, 23, 20, 24

	1	2	3	4	5	6	7	8	9	
3	3									
9	3	9								
6	3	6								
7	3	6								
14	3	6	14							
8	3	6	8							
11	3	6	8	11						
17	3	6	8	11	17					
12	3	6	8	11	17					
13	3	6	8	11	13					
20	3	6	8	11	13	20				
16	3	6	8	11	13	16				
17	3	6	8	11	13	16				
18	3	6	8	11	13	16	18			
23	3	6	8	11	13	16	18	23		
20	3	6	8	11	13	16	18	20		
24	3	6	8	11	13	16	18	20	24	

The longest 2-incraseing subsequence is: 3, 6, 8, 11, 13, 16, 18, 20, 24

7.]12 pts] You have received a message that was compressed with LZW. Remember that A=65, B=66, C=67, D=68 and E=69. The dictionary starts with entry 256. The message you received was

67 65 68 65 257 256 69 258 260

(i) What was the original message and what is your dictionary after decompression?

w start	Read k	Entry	Output	Dictionary Add	Next w
Nil	67	C	C		C
C	65	A	A	CA 256	A
A	68	D	D	AD 257	D
D	65	A	A	DA 258	A
A	257	AD	AD	AA 259	AD
AD	256	CA	CA	ADC 260	CA
CA	69	E	E	CAE 261	E
E	258	DA	DA	ED 262	DA
DA	260	ADC	ADC	**DA 263**	ADC

Original Message: CADAADCAEDAADC
Dictionary: 256 - CA, 257 - AD, 258 - DA, 259 - AA, 260 - ADC, 261 - CAE, 262 - ED, 263 - DA

(ii) Assuming 8 bits per character, how many bits were in the uncompressed message?

14 uncompressed characters * 8 bits/character = 112 bits

(iii) Assuming the last entry of your dictionary was 1023, how many bits were in the compressed message

9 compressed characters * 10 bits/compressed character = 90 bits

8. [12 pts] Consider an RSA encryption system that has a public key of 7433 for the value of e and 21353 for the value of the modulus n. With a quantum computer, you are able to factor the 21353 into the product of two primes: 131 x 163.

Using this information, set up the table for the GCD (Extended Euclidian Algorithm)

n = 21353 = 131*163
phi(n) = 130*162 = 21060
d = modular inverse of e mod phi(n) = 1/7433 mod 21060

k	A	B	Q	R	alpha	beta
-1					1	0
0	21060	7433	2	6194	0	1
1	7433	6194	1	1239	1	-2
2	6194	1239	4	1238	-1	3
3	1239	1238	1	1	5	-14
4	1238	1	1238	0	-6	17

What is the private key?
-6*21060 mod 21060 +17*7433 mod 21060 = 1 mod 21060
1/7433*7433 * 17 mod 21060 = 1/7433 mod 21060
d = 1/7433 mod 21060 = 17
Private key (d,n) = (17, 21353)

If you wanted to sign a message of value 3, what is the cipher text? (Compute the number)
M = 3

$C = M^d \bmod n = 3^{17} \bmod 21353 = 18572$

9. [12 pts] You are interested in purchasing the items listed below. You have 14 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 purchase with points to minimize the cash you would have to spend for the rest.

Item 1: 3 points, $12
Item 2 4 points, $14
Item 3: 7 points, $18
Item 4: 4 points, $10
Item 5: 2 points, $7

Pts	Item 1	Item 2	Item 3	Item 4	Item 5	
0	0	0	0	0	0	
1	0	0	0	0	0	
2	0	0	0	0	$7	
3	$12	$12	$12	$12	$12	
4	$12	$14	$14	$14	$14	
5	$12	$14	$14	$14	$19	
6	$12	$14	$14	$14	$21	
7	$12	$26	$26	$26	$26	
8	$12	$26	$26	$26	$26	
9	$12	$26	$26	$26	$33	
10	$12	$26	$30	$30	$33	
11	$12	$26	$32	$36	$36	
12	$12	$26	$32	$36	$37	
13	$12	$26	$32	$36	$43	
14	$12	$26	$44	$44	$44	

Which items would you take: Use points for items 3, 2 and 1

10. [9 pts] The Levensthein Edit Distance determines the edit distance between two strings when Addition, Deletion and Substitution are allowed. Consider a different edit distance where only Addition and Deletion are allowed and Substituion is not.

    Assume you have two strings: A and B. The i^{th} character of A is Ai and the j^{th} character of B is Bj.

(i) When considering the The i^{th} character of A and the j^{th} character of B, what is the "formula" for you would use for determining the value placed in the table at location i,j when finding the standard Levensthein Edit Distance

Base cases:
For i = 0 or j = 0, T[0, j] = j and T[i,0] = i

For i > 0 and j > 0,
If Ai = Bj, T[i, j] = T[i-1, j-1]
Otherwise, T[i,j] = 1 + min{T[i-1, j], T[i, j-1], T[i-1, j-1]}

(ii) When considering the The i^{th} character of A and the j^{th} character of B, what is the "formula" for you would use for determining the value placed in the table at location i,j when finding the modified Levensthein Edit Distance without substitution

Base cases:
For i = 0 or j = 0, T[0, j] = j and T[i,0] = i

For i > 0 and j > 0,
If Ai = Bj, T[i, j] = T[i-1, j-1]
Otherwise, T[i,j] = 1 + min{T[i-1, j], T[i, j-1]}

(iii) When considering the The i^{th} character of A and the j^{th} character of B, what is the "formula" for you would use for determining the value placed in the table at location i,j when finding the Longest Common Subsequence

Base cases:
For i = 0 or j = 0, T[0, j] = 0 and T[i,0] = 0

For i > 0 and j > 0,
If Ai = Bj, T[i, j] = 1 + T[i-1, j-1]
Otherwise, T[i,j] = max{T[i-1, j], T[i, j-1]}