CS 5/7350 - Test#2
April 21, 2021

Name: Bingying Liang
ID: 48999397

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

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

   Solution: unknown

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

   Solution: $<$ Skip not cover yet $>$

   (c) 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)

   Solution: False

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

   Solution: False

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

   Solution: True

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

   Solution: some

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

   Solution: $<$ Skip not cover yet $>$

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

   Solution:

$$
\begin{aligned}
&(161 \times Z + 5729) \bmod 11609 = 11169\\
&(161 \times Z) \bmod 11609 + 5729 \bmod 11609 = 11169\\
&(161 \times Z) \bmod 11609 + 5729 = 11169\\
&(161 \times Z) \bmod 11609 = 5540\\
&(161 \times Z) \bmod 11609 = 5540 \bmod 11609\\
&(\frac{1}{161} \times 161 \times Z) \bmod 11609 = (\frac{1}{161} \bmod 11609) \times (5540 \bmod 11609)\\
&Z \bmod 11609 = (\frac{1}{161} \bmod 11609) \times (5540 \bmod 11609)
\end{aligned}
$$

	A	B	Q	R	α	β
-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
4	1	0	-	-	-161	11609

$$19 \times 11609 - 1370 \times 161 = 1$$
$$(19 \times 11609) \bmod 11609 - (1370 \times 161) \bmod 11609 = 1 \bmod 11609$$
$$(19 \times 11609 - 1370 \times 161) \bmod 11609 = 1$$
$$(-1370 \times 161) \bmod 11609 = 1$$
$$(\frac{1}{161}) \times 161 \bmod 11609 = 1$$
$$\therefore (\frac{1}{161}) \bmod 11609 = (-1370) \bmod 11609$$
$$(\frac{1}{161} \bmod 11609) = (11609 - 1370) \bmod 11609$$
$$(\frac{1}{161}) \bmod 11609 = 102309$$
$$\therefore Z \bmod 11609 = 102309 \times (5540 \bmod 11609)$$
$$Z \bmod 11609 = (102309 \times 5540) \bmod 11609$$
$$Z \bmod 11609 = 2486$$
$\therefore Z = 11609i + 2486$, where i is an integer.

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

(a) A complete graph with $|V|$ vertices.

Solution: $|V|$

(b) A cycle with an odd number of vertices

Solution: 3

(c) A tree

Solution: 2

(d) A bipartite graph with 8 vertices in one partition and 9 vertices in the other partition.

Solution: 2

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}

(a) Fill in the table below

Solution:

	Die#1	Die #1,#2	Die #1, #2, #3	Die #1,#2,#3,#4
-3	0	2	0	0
-2	0	2	8	24
-1	1	4	8	24
0	1	2	16	72
1	1	2	8	48
2	0	0	8	72
3	0	0	0	24
4	0	0	0	24
5	0	0	0	0
Sum	3	12	48	288

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

Solution: 72

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

Solution: $\frac{1}{4}$

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

Solution: 24

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

Solution: $\frac{1}{12}$

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:

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

The longest 2-incraseing subsequence is:

Solution:

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

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

Solution:

Dictionary
A = 65
B = 66
C = 67
D = 68
E = 69
...
256 = CA
257 = AD
258 = DA
259 = AA
260 = ADC
261 = CAE
262 = ED
263 = DAA

	start w	read k	entry	output	Dictionary add	next w
0	-	67	C	C		C
1	C	65	A	A	CA = 256	A
2	A	68	D	D	AD = 257	D
3	D	65	A	A	DA = 258	A
4	A	257	AD	AD	AA = 259	AD
5	AD	256	CA	CA	ADC = 260	CA
6	CA	69	E	E	CAE = 261	E
7	E	258	DA	DA	ED = 262	DA
8	DA	260	ADC	ADC	DAA = 263	ADC
9						

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

Solution: 112 bits.

Entry:C,A,D,A,AD,CA,E,DA,ADC

$$14 \times 11 = 112 \; bits$$

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

Solution: 90 bits.

$$\log_2 (1023 + 1) = \log_2 1024 = 10$$
$$10 \times 9 = 90 \; bits$$

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.

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

Solution:
public key: (e,n) = (7433, 21353)
private key: (d,n)

$$d = \frac{1}{e} \bmod \Phi(n) = \frac{1}{7433} \bmod \Phi(21353)$$
$$\Phi(21353) = \Phi(131 \times 163) = (131 - 1) \times (163 - 1) = 130 \times 162 = 21060$$
$$\therefore d = \frac{1}{7433} \bmod 21060$$

	A	B	Q	R	α	β
-1					1	0
	21060	7433	2	6194	0	1
	7433	6194	1	1239	1	-2
	6194	1239	4	1238	-1	3
	1239	1238	1	1	5	-14
	1238	1	1238	0	-6	17
	1	0	-	-	7433	-21060

$$
\begin{aligned}
&-(6)\times(21060)+17\times 7433=1\\
&(-6\times 21060)\bmod 21060+(17\times 7433)\bmod 21060=1\\
&(17\times 7433)\bmod 21060=1\\
&\because (\frac{1}{7433}\times 7433)\bmod 21060=1\\
&\therefore d=\frac{1}{17}\bmod 21060=17
\end{aligned}
$$

(b) What is the private key?

Solution: (17, 21353)

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

Solution:

$$3^{17} \bmod 21353 = 18572$$

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.

$$
\begin{aligned}
&\text{Item } 1: 3 \text{ points, } \$12\\
&\text{Item } 2: 4 \text{ points, } \$14\\
&\text{Item } 3: 7 \text{ points, } \$18\\
&\text{Item } 4: 4 \text{ points, } \$10\\
&\text{Item } 5: 2 \text{ points, } \$7
\end{aligned}
$$

Which items would you take:

Solution:

Sum points / items	1	1, 2	1, 2, 3	1, 2, 3, 4	1, 2, 3, 4, 5
2	0	0	0	0	7
3	12	12	12	12	12
4	12	14	14	14	14
5	12	14	14	14	14
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

44; item1, item2, item3.

10. [9 pts] The Levenstheim 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.

 (a) 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 Levenstheim Edit Distance

 Solution:

```
// Base case
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};
}
```

 (b) 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 Levenstheim Edit Distance without substitution

Solution:

```
// Base case
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]+2};
}
```

(c) 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

Solution:

```
// Base case
if (i == 0){
     T[i, j] = T[0,j];
     }
if (j == 0){
     T[i, j] = T[i,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]};
}
```