CS 5/7350 - Test#3
Fall, 2021

Name: Bingying Liang
ID: 48999397

1. [5 pts] The following numbers are in the number system $\beta = \frac{1}{\sqrt[3]{2}}$ (one over the cube root of 2) and D = $\{0,1\}$. Add the numbers and give the answer in the same number system:

Solution:

$$\begin{array}{r} 1\,1\,0\,0\,0\,1\,0\,0\,1\,0\,.\,1\,1\,0\,0\,1\,1 \\ +\ \underline{1\,0\,1\,0\,0\,1\,1\,0\,0\,0\,.\,1\,1\,0\,0\,0\,1} \end{array}$$

0111001000.010100011

NOT on Test 3 Spring '23

2. [8 pts] You want to prove that some problem H is NP-Complete. You know that problem G is NP-Hard. Mark **True** for each of the following statements of things you need to prove. Mark **False** if you do not need to prove the statement.

   (a) You need to prove that H can be verified in polynomial time.

   Solution: True

   (b) You need to prove that G can be verified in polynomial time.

   Solution: False

   (c) You need to prove that a solver for G can also solve H.

   Solution: False

   (d) You need to prove that a solver for H can also solve G.

   Solution: True

   (e) You need to prove that H is NP-Hard

   Solution: True

3. [7 pts] Compute the integer value for Z given that ((161 * Z) + 3879) modulo 11609 = 11169. Show your table for the Extended Euclidian Algorithm.

Solution:

$$
\begin{aligned}
&(161 \times Z + 3879) \bmod 11609 = 11169 \\
&(161 \times Z) \bmod 11609 + 3879 \bmod 11609 = 11169 \\
&(161 \times Z) \bmod 11609 + 3879 = 11169 \\
&(161 \times Z) \bmod 11609 = 7290 \\
&(161 \times Z) \bmod 11609 = 7290 \bmod 11609 \\
&(\frac{1}{161} \times 161 \times Z) \bmod 11609 = (\frac{1}{161} \bmod 11609) \times (7290 \bmod 11609) \\
&Z \bmod 11609 = (\frac{1}{161} \bmod 11609) \times (7290 \bmod 11609)
\end{aligned}
$$

	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

$$
\begin{aligned}
&19 \times 11609 = 220571 \\
&1370 \times 161 = 220570 \\
&19 \times 11609 - 1370 \times 161 = 1 \\
&(19 \times 11609) \bmod 11609 - (1370 \times 161) \bmod 11609 = 1 \bmod 11609 \\
&0 + (-1370 \times 161) \bmod 11609 = 1 \\
&(-1370 \times 161) \bmod 11609 = 1 \\
&(\frac{1}{161}) \times 161 \bmod 11609 = 1 \\
&\therefore (\frac{1}{161}) \bmod 11609 = (-1370) \bmod 11609 \\
&(\frac{1}{161} \bmod 11609) = (11609 - 1370) \bmod 11609 \\
&(\frac{1}{161}) \bmod 11609 = 102309 \bmod 11609 \\
&\therefore Z \bmod 11609 = 102309 \times (7290 \bmod 11609) \\
&Z \bmod 11609 = (102309 \times 7290) \bmod 11609 \\
&Z \bmod 11609 = 8049 \\
&\therefore Z = 11609i + 8049, \text{where i is an integer.}
\end{aligned}
$$

4. [6 pts] Show the addition table required for addition that adds two numbers from the number system β= 7 and D = { -4 -3, -2, -1, 0, 1, 2, 3, 4 } giving a number in the same number system.

Ensure the addition can be performed in parallel without having to “ripple” a carry. (You do not need to fill in the grey areas:

Solution:

	-4	-3	-2	-1	0	1	2	3	4
-4	$\bar{1}\bar{1}$	$\bar{1}0$	$\bar{1}1$	$\bar{1}2$	$\bar{1}3$	$0\bar{3}$	$0\bar{2}$	$0\bar{1}$	00
-3									01
-2									02
-1									03
0									$1\bar{3}$
1									$1\bar{2}$
2									$1\bar{1}$
3									10
4									11

NOT on Test 3 Spr 23

5. [8 pts] You have 3 dice. Each one is different.

- Die #1 has sides { 0, 1, 2 } with a
  - 20% chance of rolling a 0, a
  - 30% chance of rolling a 1 and a
  - 50% chance of rolling a 2.
- Die #2 has sides { 2, 2, 0 } with a
  - 35% chance of rolling the first 2 and a
  - 35% chance of rolling the other 2 and a
  - 30% chance of rolling a 0
- Die #3 has sides {0, 1} with a
  - 25% chance of rolling a 0 and a
  - 75% chance of rolling a 1

(a) Fill in the table for the dynamic programming algorithm to solve the problem.

Solution:

Sum	Die 1	1,2	1,2,3	
0	0.2	0.06	0.015	
1	0.3	0.09	0.0675	
2	0.5	0.29	0.14	
3	0	0.21	0.27	
4	0	0.35	0.245	
5	0	0	0.2625	
	1	1	1	

(b) What is the probability of rolling a 0?

Solution: 0.015

(c) What is the probability of rolling a 1?

Solution: 0.9675

(d) What is the probability of rolling a 2?

Solution: 0.14

(e) What is the probability of rolling a 3?

Solution: 0.27

(f) What is the probability of rolling a 4?

Solution: 0.245

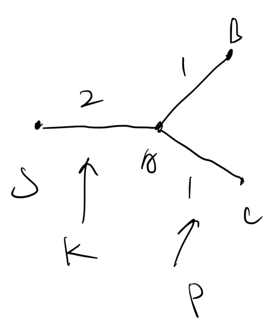
(g) What is the probability of rolling a 5?

Solution: 0.2625

6. [8 pts] Create a graph with a starting vertex of "S" (when required) where:

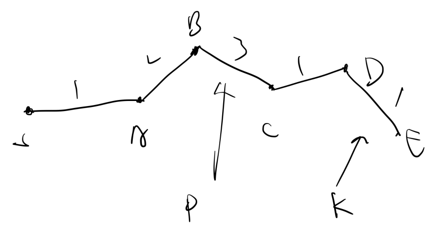
(a) The weight of the third edge chosen with Prims Minimum Spanning Tree Algorithm is less than the weight of the third edge chosen with Kruskal's Minimum Spanning Tree Algorithm. Mark the third edge chosen by prim's algorithm with a "P" and the third edge chosen by Kruskal's algorithm with a "K".

Solution:



(b) 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".

Solution:



7. [8 pts] Answer the following questions.:

(a) A program requires 3s to brute force attack an encryption key of 64 bits. If the running time is $\Theta(2^n)$ about how many years would it take to brute force attack an encryption key of 256 bits? (note there are about 32 million seconds in a year)

Solution: $2^{192} \times 3 \times \frac{1}{32 \times 10^6} s$

(b) A program requires 3s to brute force attack an encryption key of 64 bits. If you have access to a quantum computer where the running time is $\Theta(n^2)$ about how many seconds would it take to brute force attack an encryption key of 256 bits?

Solution: 48s

8. [7 pts] Use the DGT algorithm discussed in class to determine how to represent the value 282 using the number system β=5, D = { -2, -1, 0, 7 }. Show your work.

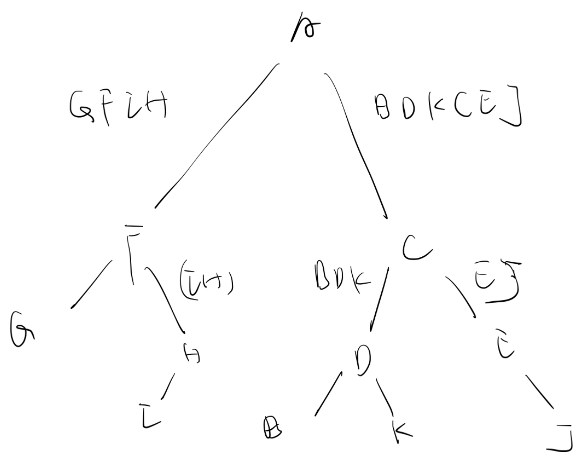
Solution:

$$-2 \bmod 5 = 3, -1 \bmod 5 = 4, 7 \bmod 5 = 2$$
$$282 \bmod 5 = 2 \rightarrow 7$$
$$282 - 7 = 275$$
$$275 \div 5 = 55$$
$$----------------$$
$$55 \bmod 5 = 0$$
$$55 - 0 = 55$$
$$55 \div 5 = 11$$
$$----------------$$
$$11 \div 5 = 1 \rightarrow No\ digit\ is = 1.$$
$\therefore$ 282can not be represented in this number system

9. [7 pts] A tree has the following pre-order and in-order traversals. Draw the tree and give the post-order traversal.

In-Order: GFIHABDKCEJ
Pre-Order: AFGHICDBKEJ

Solution:



10. [8 pts] You have two strings, A and B.

  - String A has a length of 8.
  - String B has an unknown length.
  - The Lowenstein Edit Distance between the two strings is 5.

  (a) What is the minimum length of String B?

  Solution: 3

  (b) What is the maximum length of String B?

  Solution: 13

  (c) What is the minimum length of the Longest Common Subsequence of String A and String B

  Solution: 3

  (d) What is the maximum length of the Longest Common Subsequence of String A and String B?

  Solution: 8

11. [8 pts] You run different programs for various values of "n" and sometimes "m" and create 4 tables of the runtimes. Give the asymptotic bounds that each table supports?

a.

n	time (ms)
5	11
6	66
7	462
8	3696
9	33264
10	332640
11	3659040
12	43908480

b.

n	time (ms)
100	12156
200	12156
300	12156
400	12156
500	12156
600	12156
700	12156
800	12156

c.

m	n	time (ms)
100	100	104
100	200	156
100	300	208
100	400	260
200	100	156
200	200	208
200	300	260
200	400	832

d.

m	n	time (ms)
100	100	52
100	200	104
100	400	208
100	800	416
200	100	104
200	200	208
200	400	416
200	800	832

Solution:

(a) $\Theta(n!)$

(b) $\Theta(1)$

(c) $\Theta(n+m)$

(d) $\Theta(mn)$

12. [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

Solution: 3

(b) What is the value Person B sends to Person A

Solution: 5

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

Solution: 1

13. [6 pts] Using n_0 equal to 10, determine the maximum value for c_1 and the minimum value for c2, required to show that $f(n) = 7n^2 + 3n + 5$ is $\Theta(n^2)$.

Solution:

$$\begin{aligned}
\Omega(n^2) :& 0 \leq c_1 g(n) \leq f(n), \forall n = n_0 = 10 \\
& c_1 n^2 \leq 7n^2 + 3n + 5, \forall n = n_0 = 10 \\
& c_1 \leq 7 + \frac{3}{n} + \frac{5}{n^2}, \forall n = n_0 = 10 \\
& c_1 \leq 7 + \frac{3}{10} + \frac{5}{10^2} \\
& \therefore c_1 = 7 \text{ can let } f(n) \text{ is } \Omega(n^2), \forall n = n_0 = 10
\end{aligned}$$

$$
\begin{aligned}
O(n^2) :& 0 \le f(n) \le c_2 g(n), \forall n = n_0 = 10 \\
& 7n^2 + 3n + 5 \le c_2 n^2, \forall n = n_0 = 10 \\
& 7 + \frac{3}{n} + \frac{5}{n^2} \le c_2, \forall n = n_0 = 10 \\
& 7 + \frac{3}{10} + \frac{5}{10^2} \le c_2 \\
& 7.35 \le c_2 \\
& \therefore c_2 = 7.35 \text{ can let } f(n) \text{ is } O(n^2), \forall n = n_0 = 10
\end{aligned}
$$

14. [8 pts] Determine a Huffman encoding for each symbol in a message that contains:

20 A's, 7 B's, 7 C's, 5 D's, 2 E's and 2 F's.

(a) How many bits are in the entire message if each symbol is encoded with 3 bits?

Solution: 129 bits

(b) How many bits are in the entire Huffman coded message?

Solution: 93 bits

(c) How much entropy does each "B" have in the message?

Solution: $\log_2(\frac{43}{7})$ bits