CSE 5/7350 – Test #3
November 30, 2022

Name: _____

ID: _____

1. [8 pts] Answer the following questions:

   (i) A program requires 1000s to process an input size of C = 7 and S = 700. If the running time is Θ (C * S) about how long would it take to process an input size of C=14 and S=700?

   2000 sec

   (ii) A program requires 1000s to process an input size of C = 7 and S = 700. If the running time is Θ (C * S) about how long would it take to process an input size of C=7 and S=1400?

   2000 sec

   (iii) A program requires 1000s to process an input size of C = 7 and S = 700. If the running time is Θ (C + S) about how long would it take to process an input size of C=7 and S=1400?

   $\approx$ 2000 sec

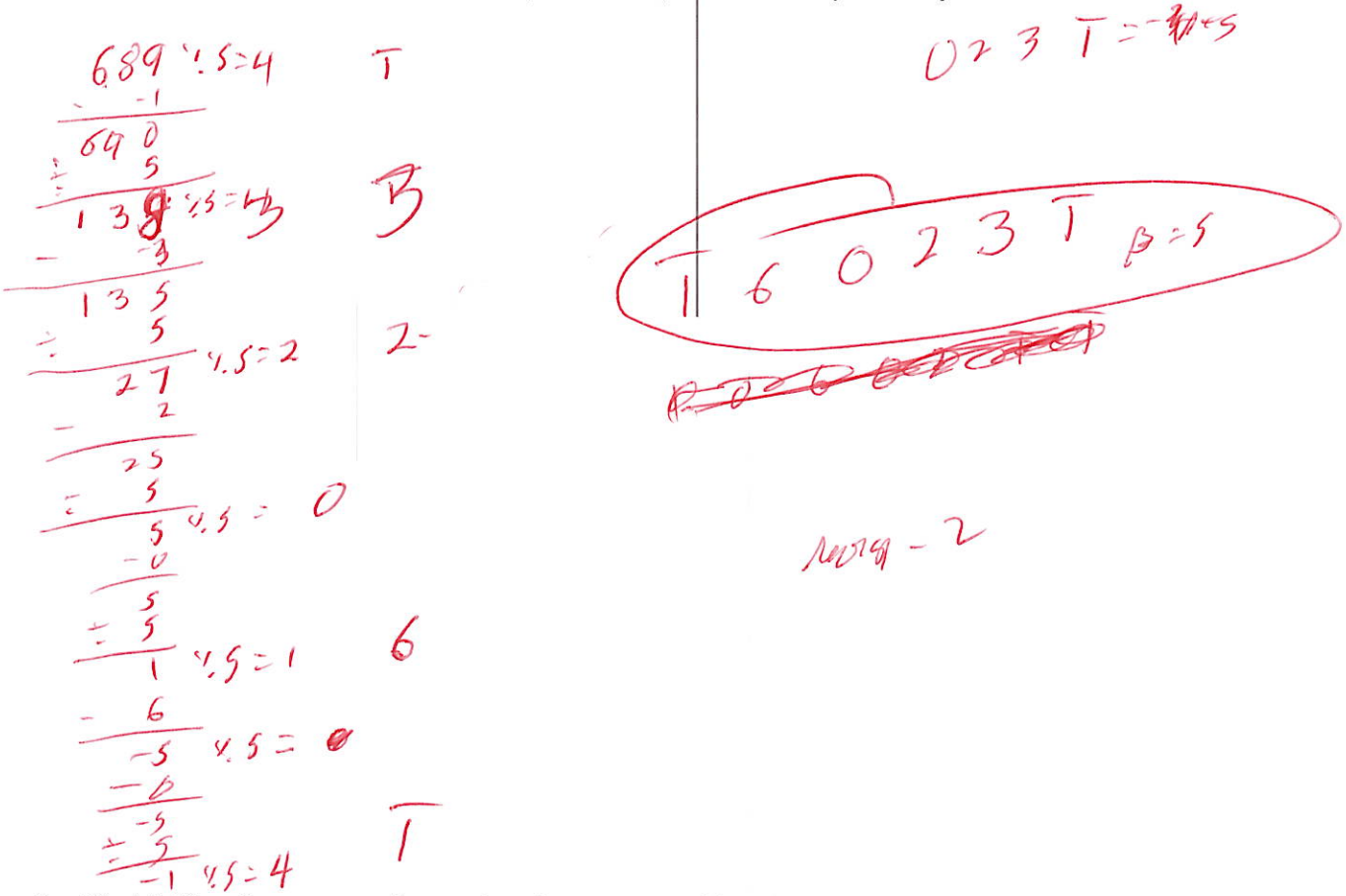
   (iv) A program requires 1000s to process an input size of C = 7 and S = 700. If the running time is Θ ($C * S^2$) about how long would it take to process an input size of C=7 and S=1400?

   4000 sec

   (v) A program requires 1000s to process an input size of C = 7 and S = 700. If the running time is Θ (2^{CS}) about how long would it take to process an input size of C=7 and S=1400?

   2^{700} sec = - lol 1000×2^{4900} sec

2. [6 pts] Use the DGT algorithm discussed in class to determine how to represent the value 689 using the number system β=5, D = { -1, 0, 2, 3 ,6 }. Show your work.



3. [8 pts] Give the asymptotic running time supported by the following tables:

a.

n	time (ms)
1	1
2	4
3	27
4	256
5	3125
6	46656
7	823543
8	16777216
9	3.87E+08
10	1E+10
11	2.85E+11

$\Theta(n^n)$

b

n	time (ms)
1	2
2	4
3	12
4	48
5	240
6	1440
7	10080
8	80640
9	725760
10	7257600
11	79833600

$\Theta(n!)$

c

n	time (ms)
1	3
2	48
3	243
4	768
5	1875
6	3888
7	7203
8	12288
9	19683
10	30000
11	43923

$\Theta(n^4)$

d

n	time (ms)
2	3
3	4.754888
4	6
5	6.965784
6	7.754888
7	8.422065
8	9
9	9.509775
10	9.965784
11	10.37829
12	10.75489

$\Theta(\lg(n))$

4. [10 pts] Consider the following NP completeness questions. Answer them with the best answer of "some" "all" "none" or "unknown"

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

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

   (iii) Which Problems in NP-Hard are also in NP? ("some" "all" "none" "unknown")

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

   (v) The set of problems matching question (iii) is exactly the same as the set of problems matching question (iv) (true or false)

   (vi) If someone can solve an NP-Hard problem in Polynomial Time, then all NP problems can be solved in polynomial time. (true or false)

   (vii) If someone can solve an NP-Complete problem in Polynomial Time, then all NP and all NP-Complete problems can be solved in polynomial time. (true or false)

   (viii) At least 1 NP problem can be solved in polynomial time? (True or False)

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

   (x) To show a problem is NP-Complete, you must show it is NP and that a solver for that problem can also solve some other NP-Complete problem with polynomial extra time. (True or False)

5. [8 pts] Set up a table to compute the length of the Longest **Common Subsequence** for the following two strings:

A C T T C G C C and C T A C G A C

	A	C	T	T	C	G	C	C	
	0	0	0	0	0	0	0	0	
C	0	1	1	1	1	1	1	1	
T	0	1	2	2	2	2	2	2	
A	0	1	2	2	2	2	2	2	
C	0	1	2	2	2	3	3	3	3
G	0	1	2	2	2	3	4	4	4
A	0	1	2	2	2	3	4	4	4
C	0	1	2	2	2	3	4	5	5

6. [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 11 and decide on 2 as the base. Person A chooses a random value of 9 and performs the appropriate computations. Person B chooses a random value of 3 and performs the appropriate computations:

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

   6

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

   8

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

   7

7. [8 pts] You have 5 different dice. The table for the summation of the dice is listed below for die 1,2 and 3. Die #4 has 4 sides of values {1, 2, 3, 4} and Die #5 has 4 sides of values {-1, -1, 0, 0}.

   a. Fill in the table for Die 4 and Die 5.

   b. How many sides and of what values is Die #1? 6 1, 22, 33, 4

   c. What is the probability of rolling a 6 with these dice? 418/2684 15.6%

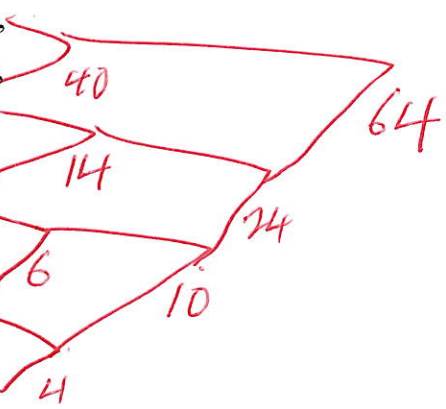
0	0	0	0		
1	1	1	0		
2	2	4	2		4
3	2	7	11	2	30
4	1	7	28	13	108
5	0	4	43	41	250
6	0	1	43	84	418
7	0	0	28	~~41~~ 125	534
8	0	0	11	147	534
9	0	0	2	125	418
10	0	0	0	84	250
11	0	0	0	41	108
12	0	0	0	13	36

2

8. [10 pts] Determine a Huffman encoding for each symbol in a message that contains:

Encoding

00	20 As,
01	20 Bs,
100	7 Ds,
101	7 Es,
1100	3 Fs,
1101	3 Gs,
1110	2 Hs
1111	2 Ks



(3)

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

(1) 192

How many bits are in the entire Huffman coded message?

(1) 40+40+40+42 = 162

How much entropy is in the entire message (Give a number)?

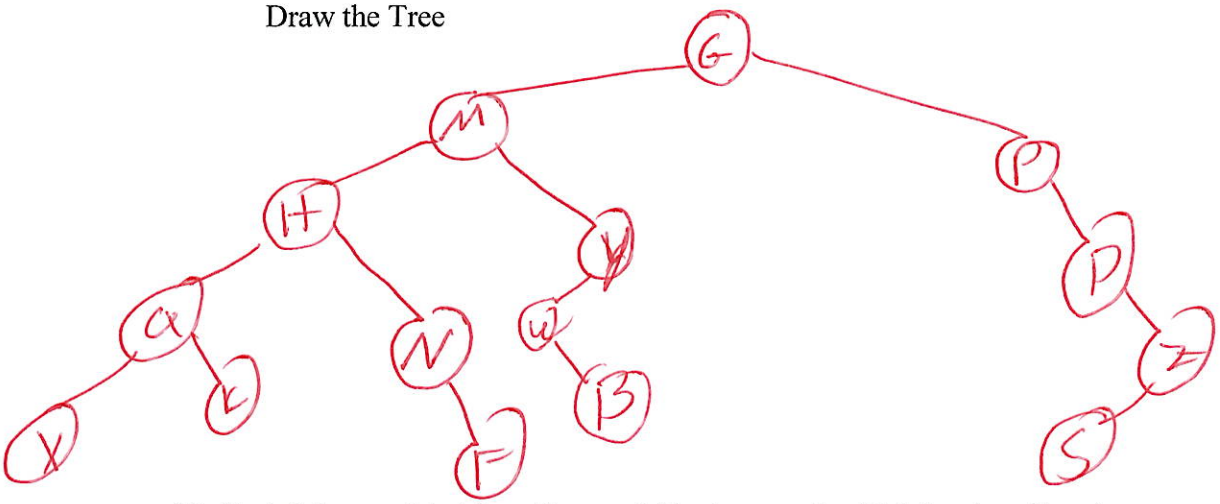
1.67 A 3.91 D 4.41 5

(3) 158.9

9. [6 pts] Argue that the problem of sorting an array of numbers is just as hard or possibly harder (within $\Theta(1)$) than the problem of finding a median of an array of numbers.

10. [5 pts] A rooted tree has an
    a. In-order Traversal of X Q K H N F M W B Y G P D S Z
    b. Pre-Order Traversal of G M H Q X K N F Y M B P D Z S

Draw the Tree



11. [9 pts] A complete bi-partite graph $B_{j,k}$ is a graph which has j vertices in one partition and k vertices in another partition and all possible edges are present. Answer the following questions:

    (i) For which values of j and k does $B_{j,k}$ have an Euler Tour?

    even j even K

    (ii) For which values of j and k is $B_{j,k}$ two-colorable?

    all

    (iii) For which values of j and k is $B_{j,k}$ a tree?

    J or K = 1

    (iv) If every edge of tree of $B_{j,k}$ has a weight of w, what is the weight of the minimum spanning tree of $B_{j,k}$. $w(j+k-1)$

    (v) If every edge of tree of $B_{j,k}$ has a weight of w, what is the maximum flow between the two partitions of $B_{j,k}$ ~~$w(Min(j,k))$~~ $w \cdot J \cdot K$

    (vi) For which values of j and k does $B_{j,k}$ have a Hamiltonian Cycle?

    J = K

12. [10 pts] Consider an RSA encryption system that has a public key of 1109 for the value of e and 2881 for the value of the modulus n. A message was encrypted with this key and this encrypted message has the value 2.

(7) (i) [6 pts] With a quantum computer, you were able to factor the modulus 2881 into the product of two primes: 43*67. Using this information, determine the private key. Be sure to show your table for the Extended Euclidian Algorithm

(3) (ii) [2 pts] What is the unencrypted message?

42
66
252
252
2772

k	A	B	q	R	α	β
-1	~~2772~~	~~1109~~	~~2~~	~~554~~	1	0
0	2772	1109	2	554	0	1
1	1109	554	2	1	1	-2
2	554	1	554	0	-2	(5)

5 — private key.

$2^5 \% 2881 = 32$ unencrypted msg

$5 \times 1109 = 5545 \% 2772 = 1$

$2772 \times 2 = 5544$

13. [6 pts] Answer the Following:

(i) -3 mod 7 = 4

(ii) 1/3 mod 11 = 4

(iii) – (1/3) mod 13 = 4

(iv) 2^{122} mod 11 4

(v) 1 $\bar{4}$ base 8 = 4 base 10

(vi) A message has 160 symbols in it. The symbol Z occurs 10 times. How much entropy does each 'Z' contain in the message? 4

(vii) What is the length of the longest common subsequence of the two strings: AABBBBCC and ZZBBBBYY 4

(viii) What are the maximum number of swaps might be necessary to insert an element into a heap that has 16 elements in it already? 4

(ix) What is 2 + 2? 4

Yall asked for a question like this! ☺