CS 5/7350 - Test#3
November 30, 2022

Name: Bingying Liang
ID: 48999397

1. [8 pts] Answer the following questions:

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

   Solution: 2000s

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

   Solution: 2000s

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

   Solution: $\frac{1407}{707} \times 1000 \approx 1990.99s$

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

   Solution: 4000s

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

   Solution: $2^{4900} \times 1000s$

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

Solution: $-1 \bmod 5 = 4, 6 \bmod 5 = 1$

$$689 \bmod 5 = 4 \rightarrow -1$$
$$689 - (-1) = 690$$
$$690 \div 5 = 138$$
$$----------$$
$$138 \bmod 5 = 3$$
$$138 - 3 = 135$$
$$135 \div 5 = 27$$
$$----------$$
$$27 \bmod 5 = 2$$
$$27 - 2 = 25$$
$$25 \div 5 = 5$$
$$----------$$
$$5 \bmod 5 = 0$$
$$5 - 0 = 5$$
$$5 \div 5 = 1$$
$$----------$$
$$1 \bmod 5 = 1 \rightarrow 6$$
$$1 - 6 = -5$$
$$-5 \div 5 = -1$$
$$----------$$
$$-1 \bmod 5 = -1$$
$$-1 - (-1) = 0$$

$$\therefore \bar{1}60231$$

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

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

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

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

(a) $\Theta(n^n)$

(b) $n!$

(c) n^4

(d) $\log_2(n)$

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

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

Solution: all

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

Solution: unknown

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

Solution: some

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

Solution: some

(e) The set of problems matching question (c) is exactly the same as the set of problems matching question (d) (true or false)

Solution: true

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

Solution: true

(g) 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)

Solution: true

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

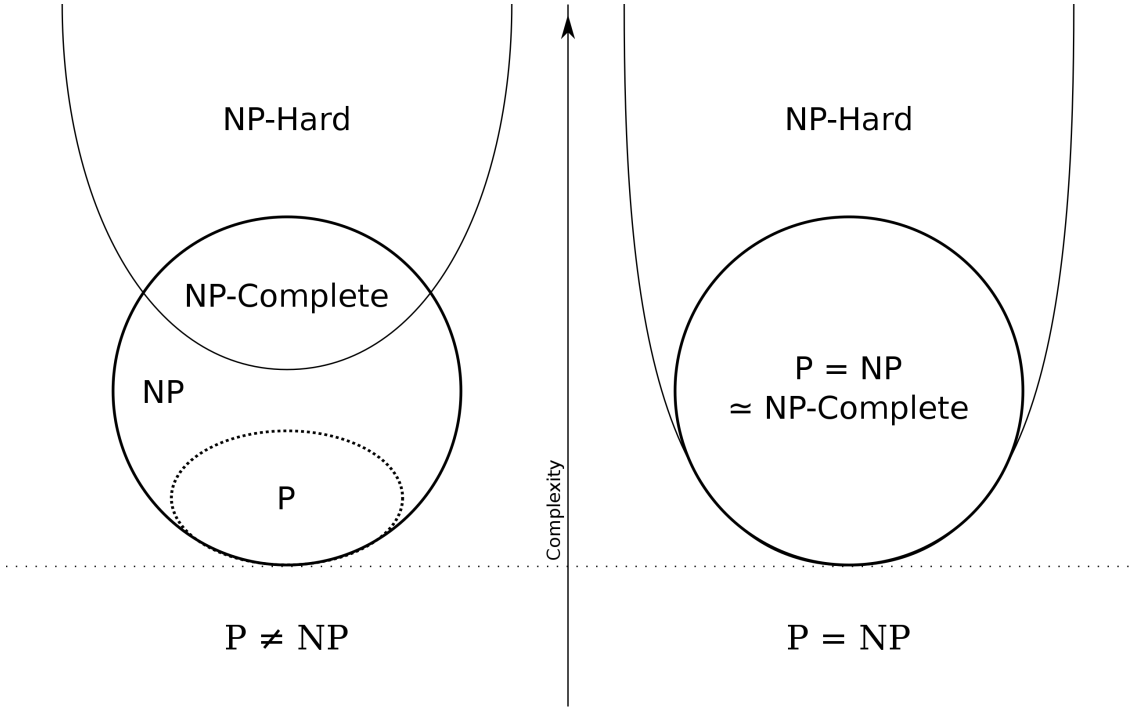
Solution: true

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

Solution: some

(j) 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)

Solution: true



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

$$A\ C\ T\ T\ C\ G\ C\ C \text{ and } C\ T\ A\ C\ G\ A\ C$$

Solution: 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

   Solution: 6

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

   Solution: 8

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

   Solution: 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.

				1	1,2	1,2,3	1,2,3,4	1,2,3,4,5
0	0	0	0	0	0
1	1	1	0	0	0
2	2	4	2	0	4
3	2	7	11	2	30
4	1	7	28	13	108
5	0	4	43	41	230
6	0	1	43	84	418
7	0	0	28	125	534
8	0	0	11	142	534
9	0	0	2	125	418
10	0	0	0	84	250
11	0	0	0	41	108
12	0	0	0	13	30
13	0	0	0	2	

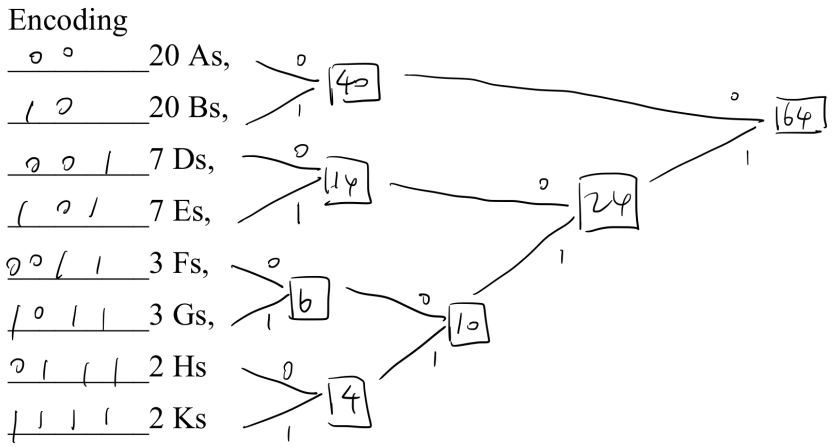
(b) How many sides and of what values is Die #1? 6 sides, value is 1, 2, 2, 3, 3, 4

(c) What is the probability of rolling a 6 with these dice?

Solution:

$$\frac{418}{(2+11+28+43+43+28+11+2)\times 4\times 4} = \frac{418}{168\times 16} = \frac{418}{2688} \approx 0.156$$

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



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

Solution: 192 bits

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

Solution: 162 bits

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

Solution: 158.35 bits

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.

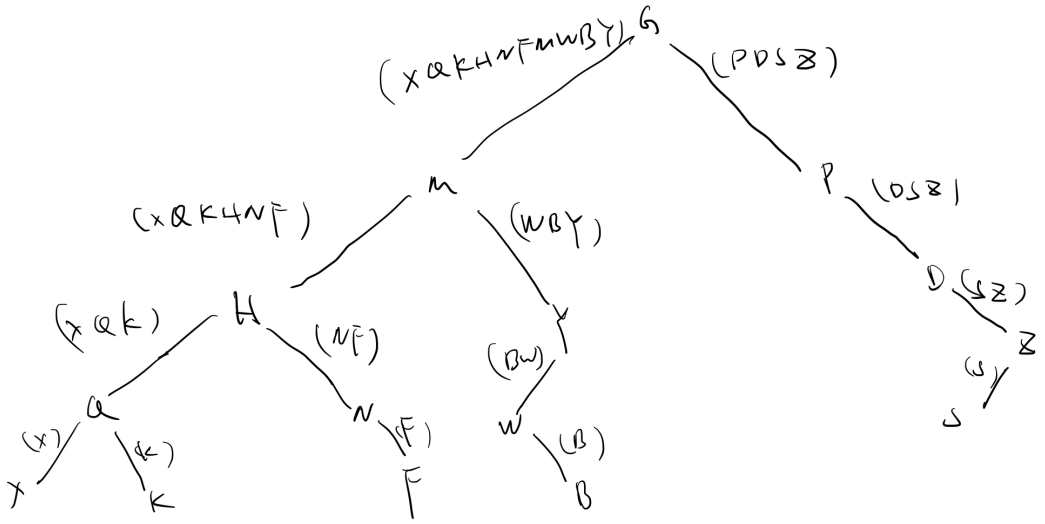
Solution: Since we can use a solver for problem of finding a median of array of numbers by sorting an array of numbers, Problem of sorting an array of numbers is just as hard or possibly harder (within $\Theta(1)$) than the problem of finding a median of an array of numbers: sorting array + pick the median($\Theta(1)$)

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:

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

Solution: even j and even k.

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

Solution: all

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

Solution: j or k = 1

(d) If every edge of tree of $B_{j,k}$ has a weight of w, what is the weight of the minimum spanning tree of $B_{j,k}$

Solution: (j + k - 1) w

(e) If every edge of tree of $B_{j,k}$ has a weight of w, what is the maximum flow between the two partitions of $B_{j,k}$

Solution: jkw

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

Solution: 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.

(a) [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

Solution: d = 5; private = (5, 2881)

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

Solution: 32

13. [6 pts] Answer the Following:

(a) -3 mod 7 =

Solution: 4

(b) 1/3 mod 11 =

Solution:

$$(\frac{1}{3} \times 3) \bmod 11 = 1$$
$$(4 \times 3) \bmod 11 = 1$$
$$(\frac{1}{3}) \bmod 11 = 4$$

(c) – (1/3) mod 13 =

Solution:

$$(-\frac{1}{3} \times 3) \bmod 13 = -1 \bmod 13 = 12$$
$$(4 \times 3) \bmod 13 = 12$$
$$-\frac{1}{3} \bmod 13 = 4$$

(d) $2^{122} \bmod 11 =$

Solution:

$$\begin{aligned} 2^{122} \bmod 11 &= 2 \times 2^{121} \bmod 11 \\ &= 2 \times (2^{11})^{11} \bmod 11 \\ &= 2 \times (2^{11} \bmod 11)^{11} \bmod 11 \\ &= 2 \times 2^{11} \bmod 11 \\ &= 2 \times 2 \\ &= 4 \end{aligned}$$

(e) $1\bar{4}$ base 8 = _____ base 10.

Solution:

$$1 \times 8^1 + (-4) \times 8^0 = 8 - 4 = 4$$

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

Solution:

$$\log_2 \frac{1}{\frac{10}{160}} = \log_2(16) = \log_2(2^4) = 4$$

(g) What is the length of the longest common subsequence of the two strings: AABBB-BCC and ZZBBBBYY

Solution: 4

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

Solution:

$$log_2(16) = 4$$

(i) What is $2 + 2$?

Solution: 4