CS 5/7350 - Test#1
September 29, 2021

Name: Bingying Liang
ID: 48999397

1. [6 pts] Define the following Terms as succinctly as possible:

   (a) Algorithm

   Solution: A step-by-step procedure for solving a problem in a finite amount of time.

   (b) Big Omega

   Solution: Is a possibly tight lower bound on a function

   (c) Power Set

   Solution: A power set is the set of all subsets. For example:

$$S = 1, 2, 3$$
$$P(S) = \{\{\}, 1, 2, 3, 1, 2, 1, 3, 2, 3, 1, 2, 3\}$$
$$|P(S)| = 2^s$$

   (d) Compression

   Solution: Compression means that we can use algorithms to reduce the number of bytes required to represent data and the amount of memory required to store images.

   (e) Entropy

   Solution: In information theory, the entropy of a random variable is the average level of "information", "surprise", or "uncertainty" inherent to the variable's possible outcomes. Given a discrete random variable X, X, which takes values in the alphabet X and is distributed according to $p : X \to [0, 1], \log_2 \frac{1}{p(x)}$

   (f) Merge Sort

   Solution: The Merge sort algorithm closely follows the divide-and-conquer method. In each step, it sorts a subarray $A[p : r]$, starting with the entire array $A[1 : n]$ and recursing down to smaller and smaller subarrays.

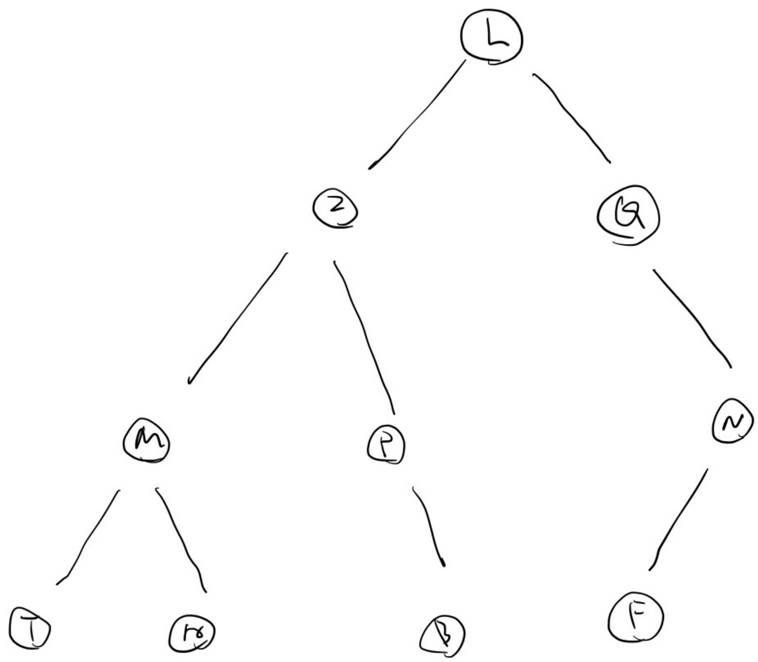
2. [7 pts] Argue that the problem, S, of sorting an unsorted array of integers of length greater than 100 elements is at least as hard - and maybe even harder - than the problem, L, of finding the ten largest elements of the same unsorted array of integers

   Solution: The solution of problem can used to solve problem L, problem L can use the sorted array to find the ten largest elements. Therefore, problem S is at least as hard and maybe even harder than the problem L.
   Since we can use a solver for problem S to solve problem L by sorting the array and then printing the last ten elements, Problem S must be just as hard or possibly harder than Problem L.

3. [8 pts] A tree has the following In-Order and Pre-Order traversals. Draw the tree and give the Post order traversal

In Order: T M A Z P B L Q F N
Pre Order: L Z M T A P B Q N F

Solution: T A M B P Z F N Q L



Post order: T A M B P Z F N Q L

4. [7 pts] Using n_0 equal to 10, show that $f(n) = 8n^2 + 5n + 1$ is $O(n^3)$.

Solution:

$$O(g(n)) = \{f(n) : \text{ there exist positive constants } c \text{ and } n_0 \text{ such that}$$
$$0 \le f(n) \le cg(n) \text{ for all } n \ge n_0\}$$
$$Assume\ n_0 = 10, g(n) = n^3$$
$$0 \le 8n^3 + 5n + 1 \le cn^3$$
$$8 + \frac{5}{n^2} + \frac{1}{n^3} \le c$$
$$if\ c = 80, n = 10$$
$$8 + \frac{5}{10^2} + \frac{1}{10^3} \le 80$$
$$\therefore \text{ there exist positive constants } c \text{ and } n_0 \text{ such that } 0 \le f(n) \le cg(n) \text{ for all } n \ge n_0$$
$$\therefore f(n) = 8n^2 + 5n + 1\ is\ O(n^3)$$

5. [8 pts] You run different programs for various values of "n" and create 4 tables of the runtimes. Give the Asymptotic bounds that each of the tables support?

a. n	time(ms)	b. n	time(ms)	c. n	time(ms)	d. n	time(ms)
1000	2120	1000	58913	100	21564	52	20
2000	4120	2000	60913	200	81564	53	60
3000	6120	4000	62913	300	181564	54	180
4000	8120	8000	64913	400	321564	55	540
5000	10120	16000	66913	500	501564	56	1620
6000	12120	32000	68913	600	721564	57	4860
7000	14120	64000	70913	700	981564	58	14580
8000	16120	128000	72913	800	1281564	59	43740
9000	18120	256000	74913	900	1621564	60	131220
10000	20120	512000	76913	1000	2001564	61	393660

(a) $\Theta(n)$

(b) $\Theta(logn)$

Solution:

$$\frac{\log_2(2000)}{\log_2(1000)} = \log_2(20001000) = \log_2(2) = 1$$
$$\frac{60913}{58913} = 1.033948365 \approx 1$$

(c) $\Theta(n^2)$

(d) $\Theta(3^n)$

6. [8 pts] Answer the following Questions:

(a) Given that $M > 100$ and $7^{31121} \bmod M = 8$; Find $7^{31122} \bmod M =$

Solution: 56

$$7^{31122} \bmod M = 7^{31121+1} \bmod M = (7^{31121} \bmod 7) \times (7 \bmod M) = 8 \times 7 = 56$$

(b) How much entropy does an entire message with 40A's and 60 B's have?

Solution:

$$\begin{aligned}
&p_A = \frac{40}{100} = \frac{2}{5}, p_B = \frac{60}{100} = \frac{3}{5} \\
&= 40 \times \log_2(\frac{1}{p_A}) + 60 \times \log_2(\frac{1}{p_B}) \\
&= 40 \times 1.321928095 + 60 \times 0.736965594 \\
&= 52.8771238 + 44.21793565 = 97.09505945 \approx 97.1\ bits
\end{aligned}$$

(c) How much entropy does an entire message with 50A's and 50 B's have?

Solution:

$$\begin{aligned}
&p_A = \frac{50}{100} = \frac{1}{2}, p_B = \frac{50}{100} = \frac{1}{2} \\
&= 50 \times \log_2(\frac{1}{p_A}) + 50 \times \log_2(\frac{1}{p_B}) \\
&= 100\ bits
\end{aligned}$$

(d) Compute $(-\frac{1}{4}) \bmod 11 =$

Solution:

$$\begin{aligned}
&(-\frac{1}{4} \times (-4)) \bmod 11 = 1 \bmod 11 = 1 \\
&(-4) \times 8 \bmod 11 = -32 \bmod 11 = 1 \\
&(-\frac{1}{4}) \bmod 11 = 8
\end{aligned}$$

7. [8 pts] Consider a method of encoding a string where instead of using regular bits that take on values of 0 or 1, you use "ternary bits" with values 0, 1, or 2. For the following message:

30 A's, 14 B's, 10 C's, 9 D's, 7 E's, 4 F's, 2 G's, 1 H and 1 K.

(a) How many of these ternary bits are in the entire message if each symbol is encoded with 2 of these "ternary bits" like this: A = 00; B = 01; C = 02; D = 10; E = 11; F = 12; G = 20; H = 21; K = 22

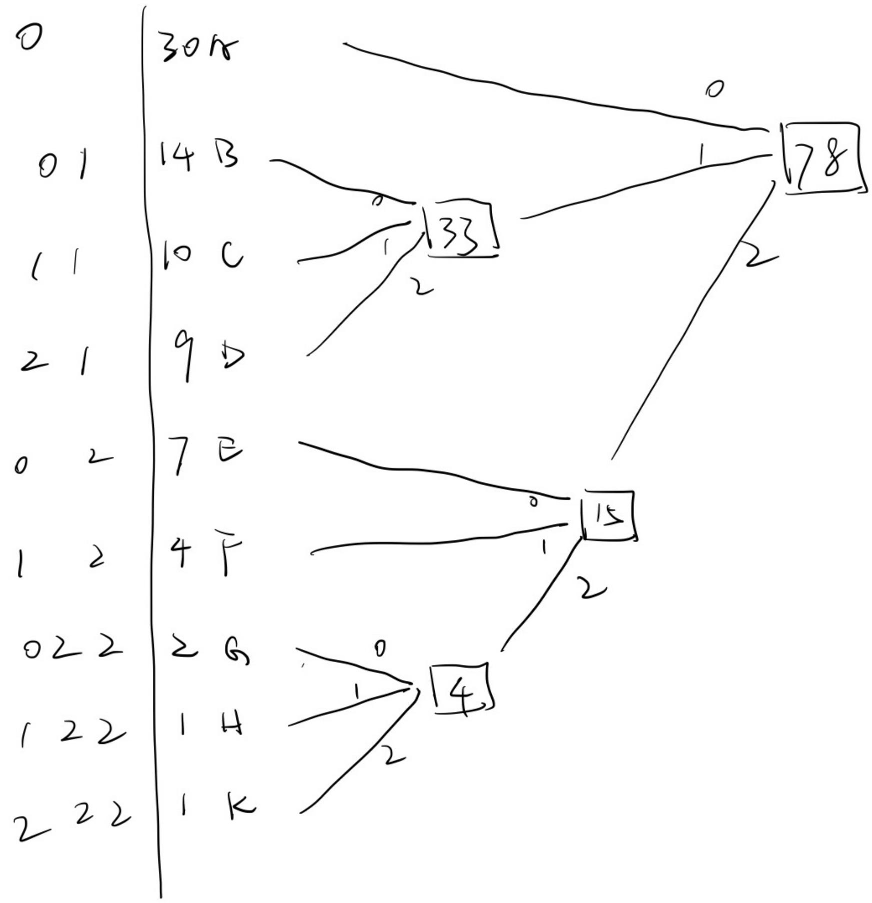
Solution:

$$(30 + 14 + 10 + 9 + 7 + 4 + 2 + 1 + 1) \times 2 = 78 \times 2 = 156\ bits$$

(b) Draw the tree and create a Huffman encoding of the ternary bits for each symbol:

(c) How many "ternary bits" are in the entire ternary Huffman coded message?

Solution:
(b)(c)



$$30 \times 1 + (14 + 10 + 9 + 7 + 4) \times 2 + (2 + 1 + 1) \times 3$$
$$= 30 + (24 + 16 + 4) \times 2 + 4 \times 3$$
$$= 30 + (24 + 20) \times 2 + 12$$
$$= 30 + (44) \times 2 + 12$$
$$= 30 + 88 + 12$$
$$= 30 + 100$$
$$= 130 \text{ bits}$$

8. [5 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 performs the appropriate computations and sends the value 6 to person B. Person B chooses a random value of 3 and performs the appropriate computations:

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

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

Solution: (a)(b)

A base 2 mod 11 B

3

$2^a \% 11 = 6$ $\xrightarrow{6}$ $2^3 \% 11 = 8 \% 11 = 8$

$\xleftarrow{8}$

$(2^a \% 11)^3 \% 11 = (2^3 \% 11)^a \% 11$

$6^3 \% 11 = 216 \% 11 = 7$

1) 8

2) 7

9. [10 pts] Consider two different algorithms that each solve a different problem.

- Implementation X solves Problem P_x and Implementation X is $\Theta(n)$
- Implementation Y solves Problem P_y and Implementation Y is $\Theta(2^n)$

Determine if each of these "Yes it is true", "Maybe it is true but doesn't have to be", or "No it is not true"

(a) Problem Px is harder than Problem Py: M

(b) Problem Py is harder than Problem Px: M

(c) Implementation X is harder than Implementation Y: N

(d) Problem X is $\Omega(n)$: M

Solution: Because Implementation X is $\Theta(n)$, Problem X should be equal or less than that. Problem lower bound should be lower or equal than Implementation.

(e) Problem X is $\omega(n)$: N

(f) Problem X is $O(n)$: Yes

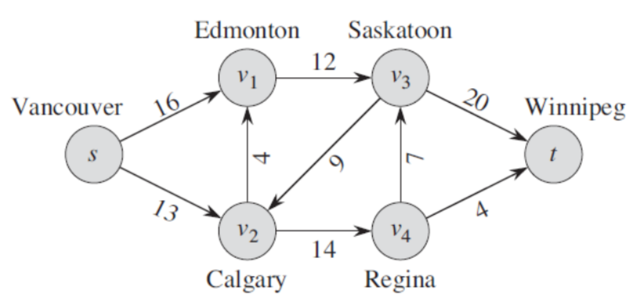
(g) Problem X is $o(n)$:M

Solution: Problem x o(n) can be equal or smaller than $O(n)$, for example, the Problem $\Theta(\log n)$ and the $O(\log n)$ which is satisfied the lower bound should lower than Implementation.

(h) Implementation X is $\Omega(n)$:Y

(i) Implementation X is $\omega(n)$:N

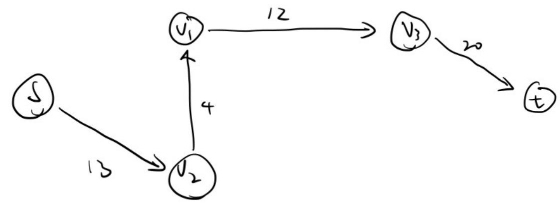
10. [8 pts] The graph below represents containers that are transported between these cities each day. You are determining the maximum flow from vertex S, Vancouver, to vertex T, Winnipeg, using the Ford-Fulkerson algorithm in the graph below.



A Path Search finds the path $s \to v_2 \to v_1 \to v_3 \to t$

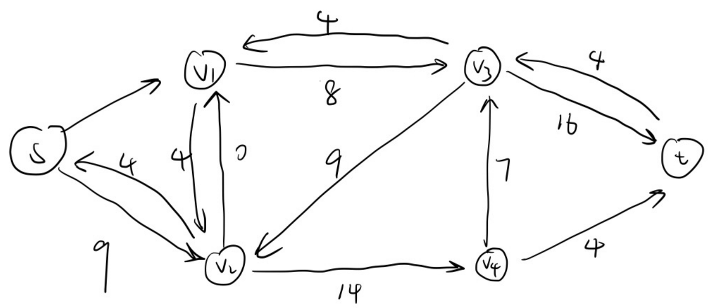
(a) How much flow is in this path?

(b) What does the new graph look like after "removing" this flow



a. flow is 4

b.



Solution:

A Path Search now finds the path $s \to v_1 \to v_2 \to v_4 \to v_3 \to t$ on the new graph.

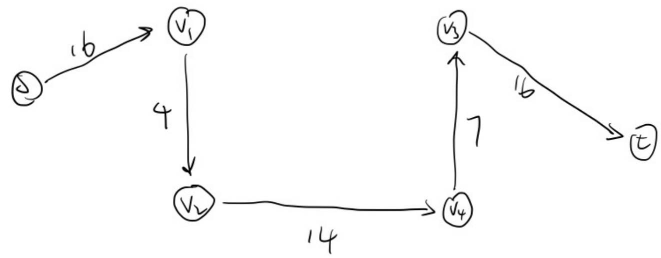
(c) Is it possible to find this path?

(d) If so, how much flow is in this path?

(e) If so, what does the new graph look like after "removing" this flow?

Solution:

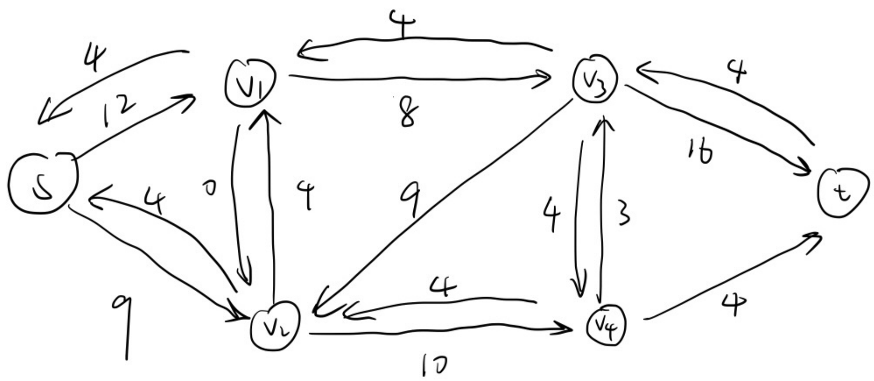
c.



Yes

d. 4

e.



11. [10 pts] Answer the following questions.:

(a) A program requires 6 seconds to process an input size of 80. If the running time is $\Theta(\sqrt{n})$ about how large of an input set could you process in 600s?

Solution:

$$\frac{\sqrt{n}}{\sqrt{80}} \times 6 = 600 \rightarrow n = 800000$$

(b) A program requires 5 DAYS to brute force attack a password of 50 bits. Since the running time is $\Theta(2^n)$ about how MANY YEARS would it take for the program to brute force attack a password of 512 bits?

Solution:

$$\frac{\frac{2^{512}}{2^{50}} \times 5}{365}\, years$$

(c) A program requires 5 DAYS to brute force attack a password of 50 bits. Since the running time is $\Theta(2^n)$ about how MANY DAYS would it take for the program to brute force attack a password of 512 bits if the running time were $\Theta(n^2)$ instead of exponential?

Solution:

$$\frac{512^2}{50^2} \times 5 = \frac{262144}{2500} \times 5 \approx 525\ days$$

(d) A program requires 6 milliseconds to process an input size of 1000. If the running time is $\Theta(n^3)$ about how many seconds would it take to process an input size of 1 trillion items?

Solution:

$$\frac{(1 \times 10^{12})^3}{(1 \times 10^3)^3} \times 6 \times 10^{-3} = 6 \times 10^{24}\ seconds$$

(e) A program requires 6 milliseconds to process an input size of 1000. If the running time is $\Theta(n)$ about how long many seconds it take to process an input size of 1 trillion items?

Solution:

$$\frac{1 \times 10^{12}}{1 \times 10^3} \times 6 \times 10^{-3} = 6 \times 10^6\ seconds$$

12. [8 pts] Answer the following questions:

(a) What is the weight of a minimum spanning tree for a complete graph with 10 vertices where all edges have a weight of 4?

Solution: $4(|V| - 1) = 36$

(b) What is the weight of a minimum spanning tree for a cycle with 10 vertices where all edges have a weight of 4?

Solution: $4(|V| - 1) = 36$

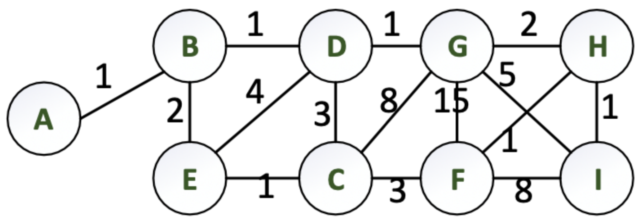
(c) A complete bi-partite graph $B_{j,k}$ is a graph which has J vertices in one partition and k vertices in another partition and all possible edges present between the partitions. For which values of j and k does a cycle exist that spans all the vertices?

Solution: $j = k\ and\ j, k \geq 2$

(d) What is the weight of a minimum spanning tree for a connected bi-partite graph Bj,k where all edges have a weight of 4?

Solution: $4(J + K - 1)$

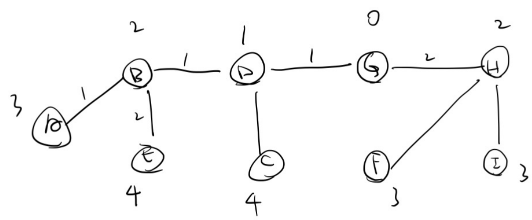
13. [7 pts] You live in city G. You want to know the cost to travel from city G to all other cities (A,B,C,D,E,F,H and I). The edges of the graph below represent the cost to travel the roads between various cities. If an edge doesn't exist, then there is no road between those two cities.



(a) What is the order in which you explore the cities using Dijkstra's Single Source Shortest Path algorithm to find the cost from city G to all other cities in the graph?

(b) Write the cost to reach each city from City G by its vertex in the graph.

Solution:



0	1	2	2	3	3	3	4	4
G	D	H	B	F	I	A	C	E