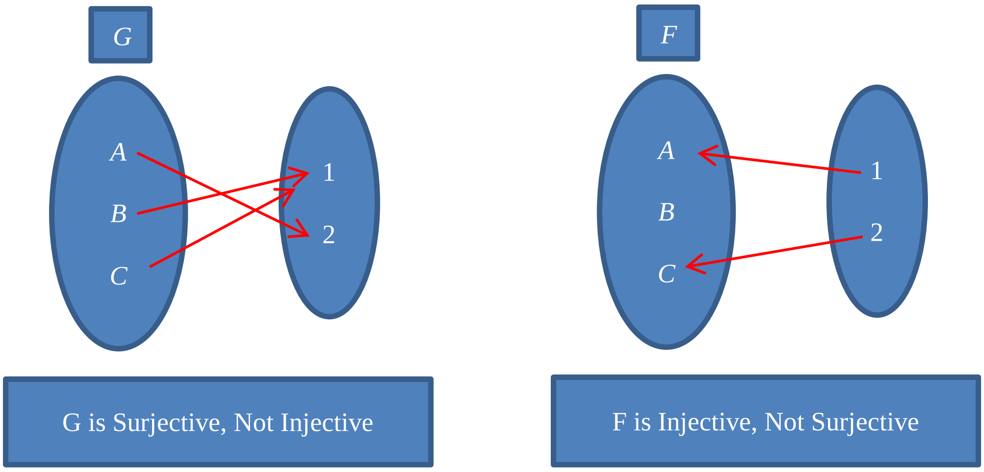
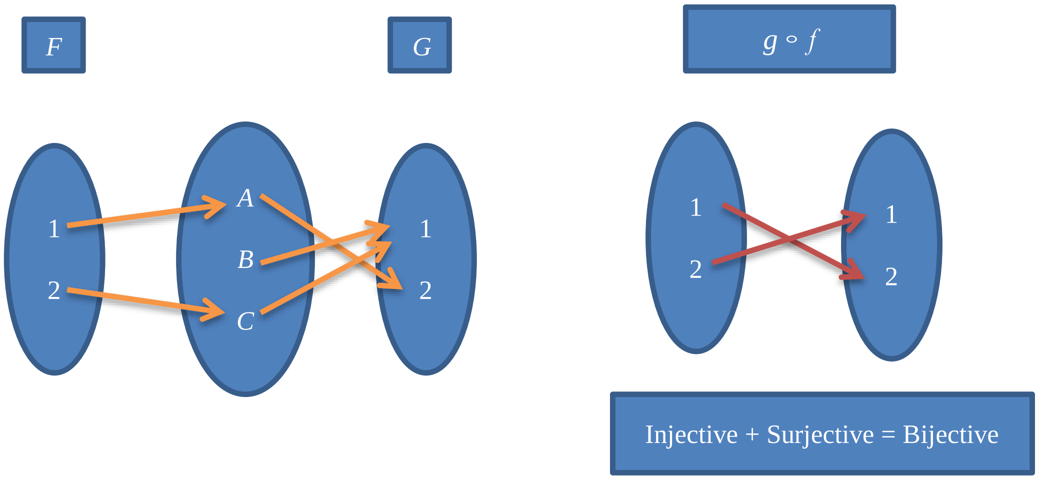
Attempt ALL seven questions

1. The functions $g : \{a, b, c\} \rightarrow \{1, 2\}$ and $f : \{1, 2\} \rightarrow \{a, b, c\}$ are given by $g(a) = 2$, $g(b) = 1$, $g(c) = 1$, $f(1) = a$, $f(2) = c$.
   (a) Classify each of f and g as bijective, injective, surjective, or neither.



   (b) Find $g \circ f$.



$= g \circ f^{-1} (1, 2), (2, 1)$

   (c) Either find the inverse of $g \circ f$ or explain why $g \circ f$ is not invertible.

There is inverse of $g \circ f$ because it is bijective.

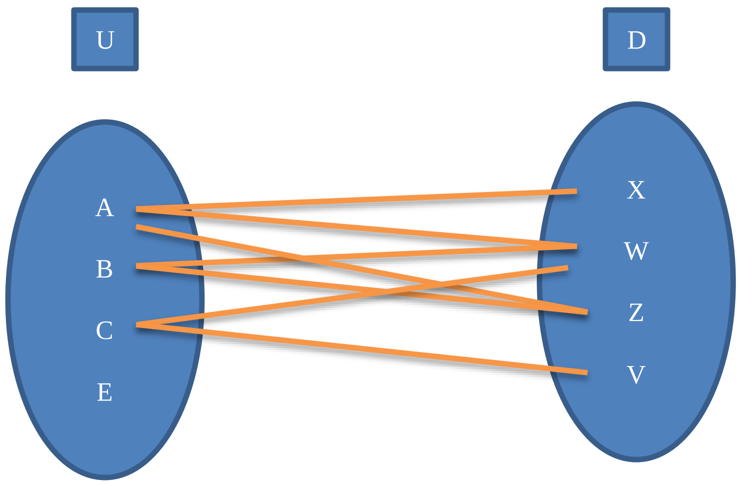
2. As part of a computer security system, you need to control which users have access to which drives. Albert has access to drives X, W and Z. Belinda has access to drives W and Z. Charlotte has access to drives V and X. Eoin has access to drives Z and W. Denoting by U the set of users and D the set of drives,

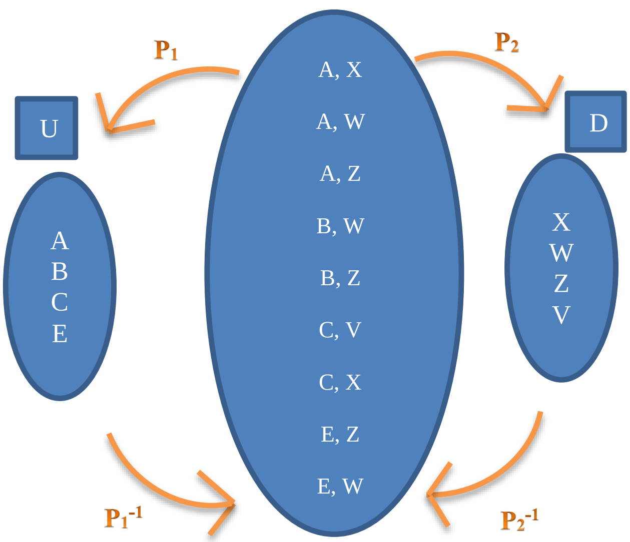
   (a) Give the relation R on U × D which represents this information. (You may use appropriate abbreviations.)

   U = Users × D = Drivers

   A – Albert = X, W, Z
   B – Belinda = W, Z
   C – Charlotte = V, X
   D – Eoin = Z, W

   (Relation) R = {(A, X), (A, W), (A, Z), (B, W), (B, Z), (C, V), (C, X), (E, Z), (E, W)}





(b) Find the combination of projection and inverse projection maps which find those users with access to drive W.

$P_1 \circ P_2^{-1}(W)$

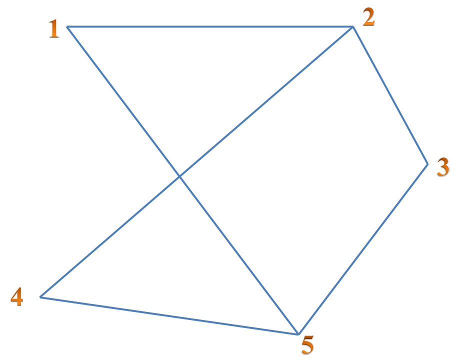
(c) Find the combination of projection and inverse projection maps which find drives accessible to Albert or Belinda.

$P_2 \circ P_1^{-1}(A) \cup P_2 \circ P_1^{-1}(B)$

3. (a) Draw the graph with adjacency matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Where the columns and rows label vertices 1 to 5 in order.



(b) Use the adjacency matrix connectivity algorithm, starting by marking row 2 and crossing out column 2, to show whether this graph is connected.

$$A=\begin{array}{rc} & \begin{array}{ccccc}1&2&3&4&5\end{array}\\ \begin{array}{r}2\to1\\1\to2\\3\to3\\4\to4\\5\to5\end{array} & \begin{pmatrix} \cancel{0} & \cancel{1} & \cancel{0} & \cancel{0} & \cancel{1} \\ \cancel{1} & \cancel{0} & \cancel{1} & \cancel{1} & \cancel{0} \\ \cancel{0} & \cancel{1} & \cancel{0} & \cancel{0} & \cancel{1} \\ \cancel{0} & \cancel{1} & \cancel{0} & \cancel{0} & \cancel{1} \\ \cancel{1} & \cancel{0} & \cancel{1} & \cancel{1} & \cancel{0} \end{pmatrix}\end{array}$$

- Starting at vertex 2, Mark row 2, label it with No 1, cross out row 2, and look for surviving 1s in the row. 1s in column 1, 3 & 4 which gives (2, 1), (2, 3) and (2, 4). Label the rows 1, 3, 4 with No 2, No 3 and No 4.
- Starting at the lowest labelled row 2, 3 & 4, select the label 2 (row 1). Only surviving 1s in row 1 is in column 5 which gives (1, 5). Cross out column 5. Now all vertices are taken and all columns crossed out and therefore shows the graph is connected.

(c) Calculate A^2 and hence find the number of paths of length 2 from vertex 3 to vertex 4.

$$A^2= \begin{array}{c} 1\rightarrow \\ 2\rightarrow \\ 3\rightarrow \\ 4\rightarrow \\ 5\rightarrow \end{array} \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

$$= \begin{array}{c|c} & \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} & \begin{pmatrix} 2 & 0 & 2 & 2 & 0 \\ 0 & 3 & 0 & 0 & 3 \\ 2 & 0 & 2 & 2 & 0 \\ 2 & 0 & 2 & 2 & 0 \\ 0 & 3 & 0 & 0 & 3 \end{pmatrix} \end{array}$$

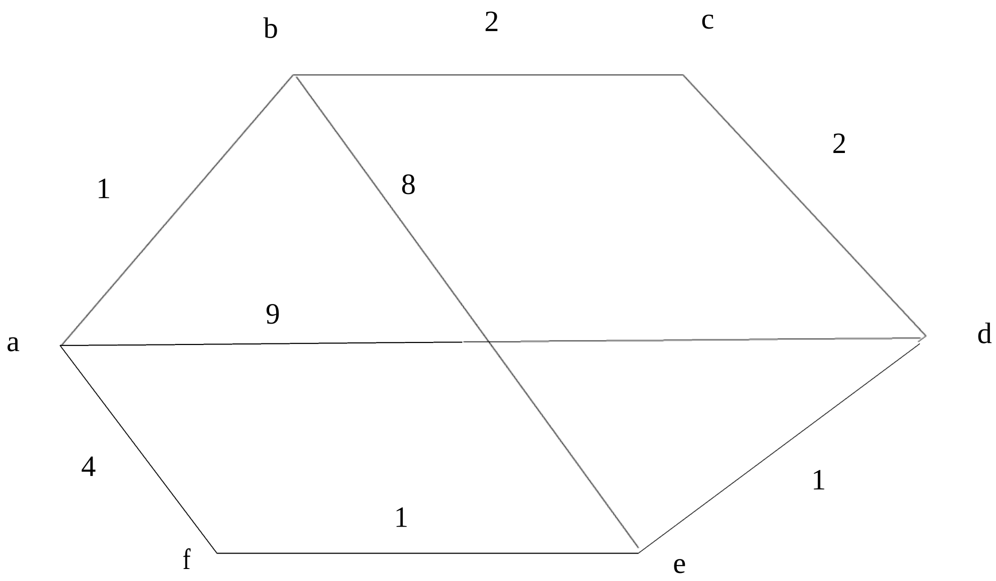
- Number of paths of length 2 from vertex 3 to 4 = 2

(d) Find a depth first spanning tree starting at vertex 2.

$$\begin{array}{c|c} & \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} & \begin{pmatrix} \cancel{0}_2 & \cancel{1}_2 & \cancel{0}_2 & \cancel{0}_2 & \cancel{1}_2 \\ \cancel{1}_1 & \cancel{0}_1 & \cancel{1}_1 & \cancel{1}_1 & \cancel{0}_1 \\ \cancel{0}_4 & \cancel{1}_4 & \cancel{0}_4 & \cancel{0}_4 & \cancel{1}_4 \\ \cancel{0}_5 & \cancel{1}_5 & \cancel{0}_5 & \cancel{0}_5 & \cancel{1}_5 \\ \cancel{1}_3 & \cancel{0}_3 & \cancel{1}_3 & \cancel{1}_3 & \cancel{0}_3 \end{pmatrix} \end{array}$$

- Mark Row 2 with 1, Cross out Column 2. In highest marked row (2), First non-Zero in Column 1. Remember edge (2,1)
- Mark Row 1 with 2, Cross out Column 1. In highest marked row (1), First non-Zero in Column 5. Remember edge (1,5)
- Mark Row 5 with 3, Cross out Column 5. In highest marked row (5), First non-Zero in Column 3. Remember edge (5,3)
- Mark Row 3 with 4, Cross out Column 4. In the highest marked row (3), remember (3,4)
- Mark Row 4 with 5, Cross out Column 4. Unmark row 4. In the Highest marked row 3, First Non-Zero in Column 4, Cross out Column 4.

4. Use Dijkstra's algorithm to find the shortest path from node b to node e, and its length, in the following graph.



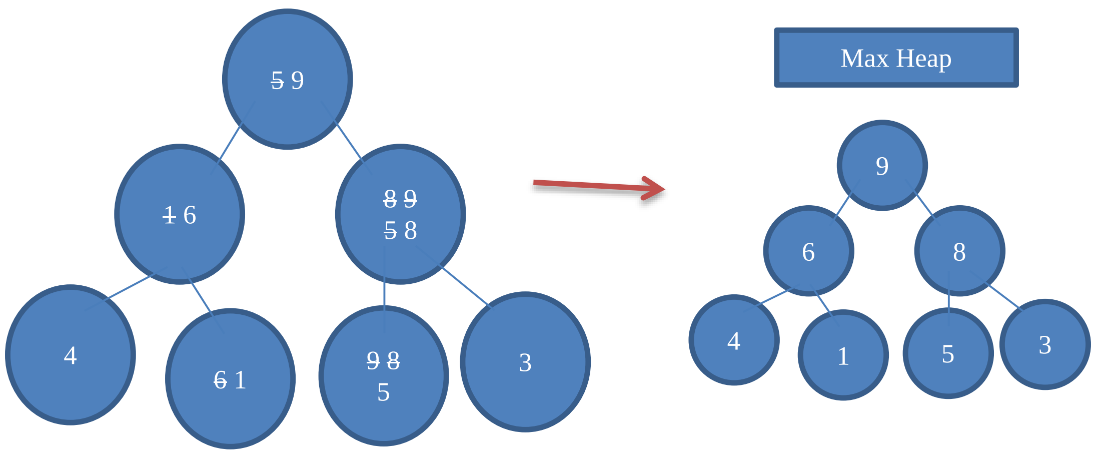
	A	B	C	D	E	F
Step 0	∞	0_B	∞	∞	∞	∞
Step 1	1_B	-	2_B	∞	8_B	∞
Step 2	-		2_B	10_A	8_B	5_A
Step 3			-	4_C	8_B	5_A
Step 4				-	5_D	5_A
Step 5					5_D	-

The shortest path from node b to node e = B→C→D→E
Length = 5

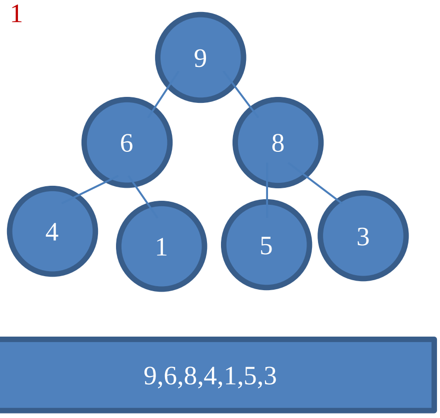
5. Use the heapsort algorithm to put the following list of numbers in decreasing order:

5 1 8 4 6 9 3

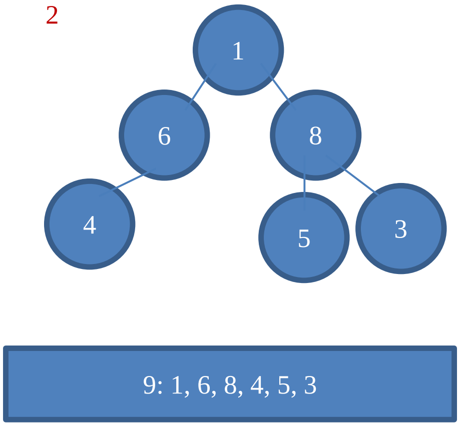
You should explain in detail how the original heap is obtained, and then show your sequence of heaps and partial ordered lists.



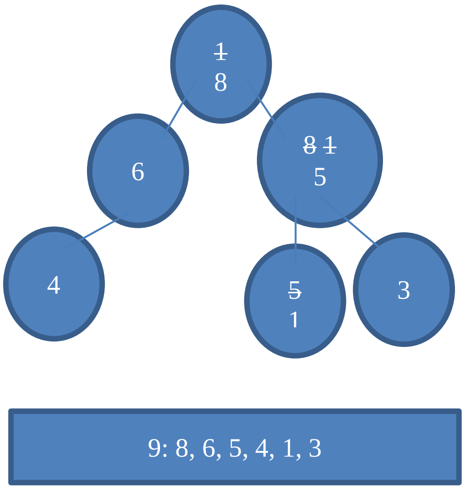
1


9
6
8
4
1
5
3
9,6,8,4,1,5,3

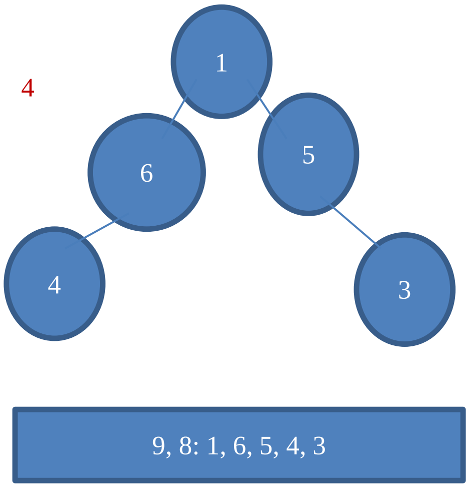
2


1
6
8
4
5
3
9: 1, 6, 8, 4, 5, 3

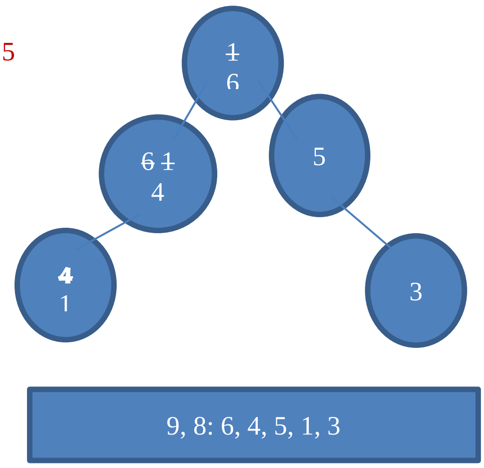
3


~~1~~ 8
6
~~8~~ ~~1~~ 5
4
~~5~~ 1
3
9: 8, 6, 5, 4, 1, 3

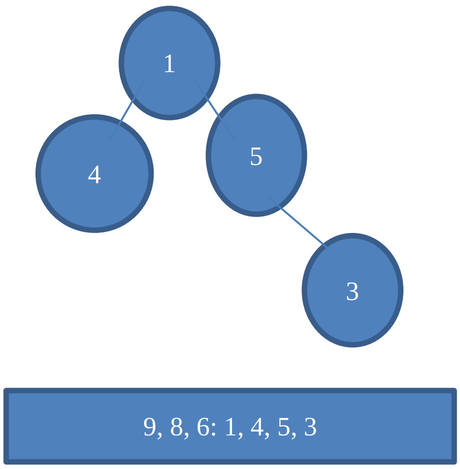
4


1
6
5
4
3
9, 8: 1, 6, 5, 4, 3

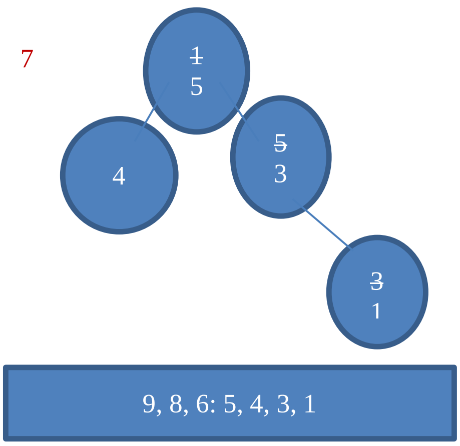
5


~~1~~ 6
~~6~~ ~~1~~ 4
5
~~4~~ 1
3
9, 8: 6, 4, 5, 1, 3

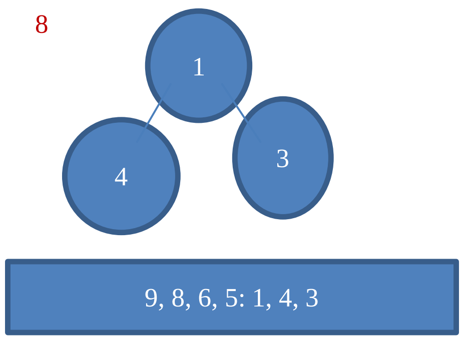
6


1
4
5
3
9, 8, 6: 1, 4, 5, 3

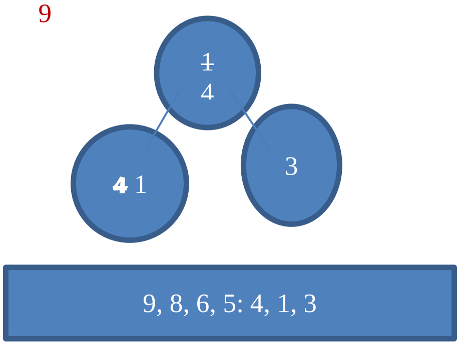
7


~~1~~ 5
4
~~5~~ 3
~~3~~ 1
9, 8, 6: 5, 4, 3, 1

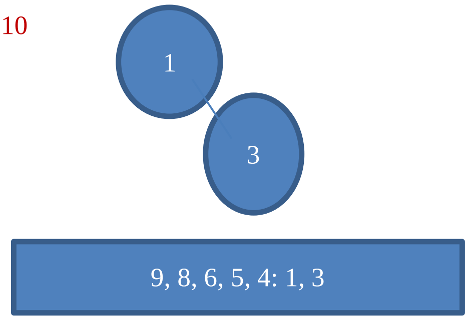
8


1
4
3
9, 8, 6, 5: 1, 4, 3

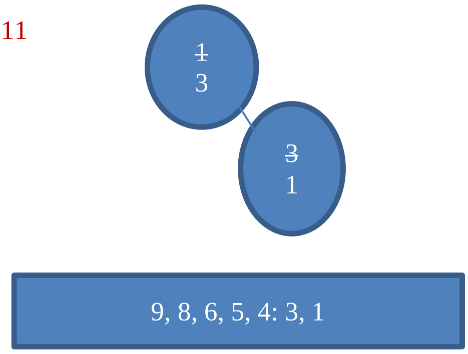
9



10



11



12

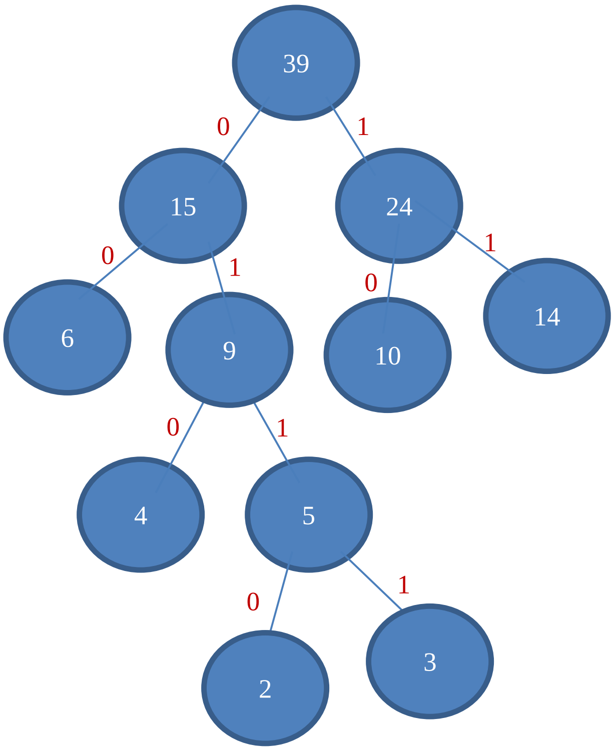
6. Consider the symbols and frequencies:

e : 14 t : 10 a : 6 o : 4 i : 3 n : 2

(a) Find a Huffman code for this situation, and the average length of an encoded symbol.

e : 14 t : 10 a : 6 o : 4 i : 3 n : 2

= 14, 10, 6, 4, 3, 2
= 2, 3, 4, 6, 10, 14
= 2+3 = 5
= 4, 5, 6, 10, 14
= 4+5 =9
= 6, 9, 10, 14
= 6+9 = 15
= 10, 14, 15
= 10 +14 = 24
= 15, 24
= 15+24 = 39



e : 14 t : 10 a : 6 o : 4 i : 3 n : 2

e: 11 t: 01 a: 00 o: 010 i: 1110 n: 0110

Symbol	Code Word	Length
e	11	2
t	01	2
a	00	2
o	010	3
i	1110	4
n	0110	4

AESL = $\frac{14x2+10x2+6x2+4x3+3x4+2x4}{39}$

$= \frac{92}{39}$

$=$ 2.35897436

= 2.35

(b) Assign the symbols to these code words in a different order, and comment on the resulting average length.

Symbol	Code Word	Length
e	0110	4
t	1110	4
a	010	3
o	00	2
i	01	2
n	11	2

AESL = $\frac{14x4+10x4+6x3+4x2+3x2+2x2}{39}$

$= \frac{132}{39}$

$=$ 3.38461538

= 3.38

Average length changes when the order of the length changes, in this case the average length has increased.

7. Bob decides to use $n = 493 = 17 \times 29$ and $e = 37$ as his public key for an RSA Cryptosystem.

(a) Show that the decryption exponent is 109.

Ne = 1 (Mod Ƶ) 29=28+1

Ƶ= (p-1) (q-1) where n=p x q

$n = 493 = 17 \times 29$

Ƶ=16x28=448

e = 37 d=109 Ƶ=448

37x109=4033=9x448+1=1(448)

d=e^{-1} (mod Ƶ) = 1 → 109 = $\frac{1}{37}$ (mod 448)

4033 mod 448 = 1

(b) Find the encrypted form of the message 27.

$$C=M^e \pmod n$$

$C=27^{37} \pmod{493}$ $37= 32+4+1$

$27^2 = 729 = 236 \pmod{493}$

$27^4 = 236^2 = 55696 = 480 \pmod{493}$

$27^8 = 480^2 = 230400 = 169 \pmod{493}$

$27^{16} = 169^2 = 28561 = 460 \pmod{493}$

$27^{32} = 460^2 = 211600 = 103 (493)$

$27^{37} = 27^{32} \text{ x } 27^4 \text{ x } 27 = 103 \text{ x } 480 \text{ x } 27 = 1334880 = 329 \pmod{493}$