Module code:	Faculty:		Surname:
124MS	EC		Morato Almeida

Student ID:		Forename(s):
5497124		Vitor

Due Date:	Signed:
23/07/2014 16:00	
	Date:

Category:	
	Written Report
Submit Type:	
	Standard
Assessment Type:	
	Individual

Course Title:	Cohort / Occurrence
Computer Science	**Group:** 1314B
Module Title:	**Assessment**
Logic and Sets	**Reference no:** **Cw**

Assessment Title:

Module Leader:	Module Tutor:
Dr Robert Low	

Seminar Group / Tutorial Tutor and Group (if different to above):

Mark Awarded	Feedback Summary (see attached sheet for detailed feedback against assessment criteria)
Mark Signature	

124MS - Coursework 2

Vitor Morato Almeida

July 23, 2014

124MS - Coursework 2

1. **The functions f : {1, 2, 3} → {a, b} and g : {a, b} → {x, y, z} are given by f(1) = b, f(2) = b, f(3) = a, g(a) = y, g(b) = x.**

   (a) **Classify each of f and g as bijective, injective, surjective, or neither.**
   Lets draw the mapping diagrams to help to classify each function

$$f$$
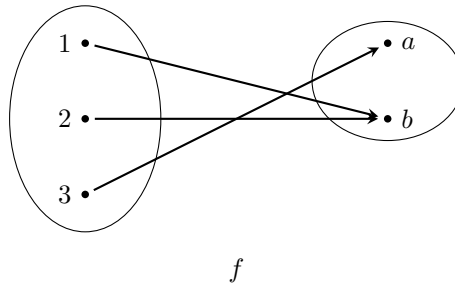
   from the diagram of function f above we can see that every element of the codomain is mapped to by at least one element of the domain, so function f is surjective

$$g$$
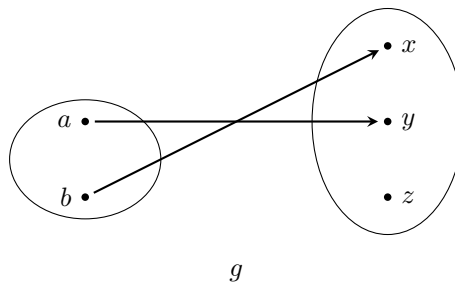
   from the diagram of function g above we can see that every element of the codomain is mapped to by at most one element of the domain, so function g is injective

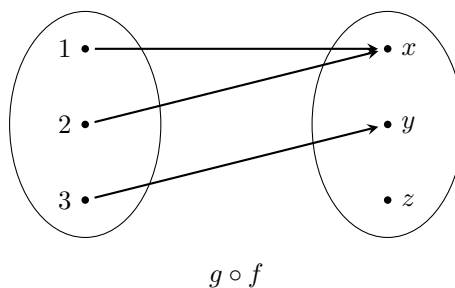   As none of the functions above is simultaneously surjective and injective, we can't classify them as bijective.

   (b) **Find g ∘ f .**
   This time I'm going to use the previous diagrams to build the diagram of the composition g ∘ f
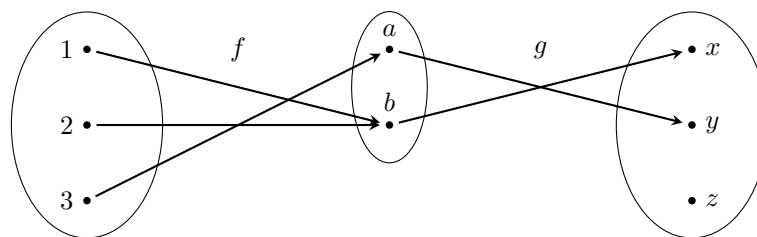
   Summarizing the diagram we have,

$$g \circ f$$

(c) **Either nd the inverse of g ◦ f or explain why g ◦ f is not invertible**

$g \circ f$ is not invertible because it cannot be classified as bijective.

2. I want to develop a database of information about my book collection, which tells me about the authors and genres of the various books I own. At the moment I have books by Isaac Asimov, China Mieville, Peter F Hamilton and Arthur C Clarke, and I denote the set of authors by A = {A, M, H, C}, abbreviating each author by the initial of his surname. I am classifying the books as science ction, fantasy, horror and non-ction, so my set of genres is G = {s, f , h, n}, again using initial letters as abbreviations. At the moment, I have science ction works by China Mieville and Isaac Asimov, I have fantasy by Peter F Hamilton and China Mieville, horror by Peter F Hamilton and Arthur C Clarke, and non-ction by Isaac Asimov.
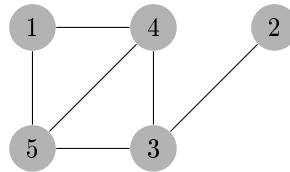
(a) Give the relation R on A Œ G which represents this information. (You may use appropriate abbreviations.)
$R = \{(A, s), (A, n), (M, s), (M, f)(H, f), (H, h), (C, h)\}$

3. (a) **Draw the graph with adjacency matrix**

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

This the graph generated from adjacency matrix:

(b) Calculate A^2 and hence nd the number of paths of length 2 from vertex 1 to vertex 5.

$$A \times A = \begin{bmatrix} 2 & 0 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 2 & 0 & 3 & 1 & 1 \\ 1 & 1 & 1 & 3 & 2 \\ 1 & 1 & 1 & 2 & 3 \end{bmatrix}$$

Looking at the position (1,5), also (5,1) once this is not a directed graph, we can see that there is only one path of length 2.

7. **Bob decides to use n = 221 = 13 Œ 17 and e = 11 as his public key for an RSA cryptosystem.**

(a) **Show that the decryption exponent is 35.**

To show that 35 is a decryption exponent, we need to check the following condition:

$ed \equiv 1 \pmod{z}$

To calculate z we use the following formula:

$z = (p-1)(q-1)$

replacing the p and q values from question into the formula we have:

4

$z = (13 - 1)(17 - 1) = 192$

now we calculate ed and its module of 192

$ed = 11 \times 35 = 385$
$385/192 = 2\frac{1}{192} \equiv 1 \pmod{z}$

(b) **Find the encrypted form of the message 16.**

$C = M^e \pmod{n}$
$C = 16^{11} \pmod{221}$

$11 = 8 + 2 + 1$

$16^1 \equiv 35 \pmod{221}$
$16^2 = 256 \equiv 35 \pmod{221}$
$16^4 \equiv 35^2 = 1225 \equiv 120 \pmod{221}$
$16^8 \equiv 120^2 = 14400 \equiv 35 \pmod{221}$

$C = 16^8 \times 16^2 \times 16 \equiv 35 \times 35 \times 16 = 19600 \equiv 152 \pmod{221}$