Universiti Malaysia PAHANG

Engineering • Technology • Creativity

FACULTY OF COMPUTER SYSTEMS & SOFTWARE ENGINEERING

FINAL EXAMINATION

COURSE	:	**FORMAL METHODS**
COURSE CODE	:	**BCS2213**
LECTURER	:	**VITALIY MEZHUYEV**
DATE	:	**08 JANUARY 2015**
DURATION	:	**3 HOURS**
SESSION/SEMESTER	:	**SESSION 2014/2015 SEMESTER I**
PROGRAMME CODE	:	**BCS / BCN / BCG**

INSTRUCTIONS TO CANDIDATE:

1. This question paper consists of **FIVE (5)** questions. Answer **ALL** questions.
2. Write your answers in the answer booklet provided.
3. Answer EACH question on a new page.
4. All calculations and assumptions must be clearly shown.

EXAMINATION REQUIREMENTS:

NONE

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO

This examination paper consists of **FIVE (5)** printed pages including the front page.

TOTAL MARKS **[100 MARKS]**

QUESTION 1 **[10 Marks]**

a) Using predicate logic translate the following sentences into logical expressions.

(i) Every software class inherits a superclass.

[1 Mark]

(ii) A superclass is inherited by its classes.

[1 Mark]

(iii) Every recursion function calls itself.

[1 Mark]

(iv) A function is called by other function.

[1 Mark]

(v) All the functions call all the other functions.

[1 Mark]

b) Write temporal logic formulas that capture the meanings of the properties described in English below (p and q are the properties of states).

(i) if p is true infinitely often, then q

[1 Mark]

(ii) if p is eventually always true, then eventually q

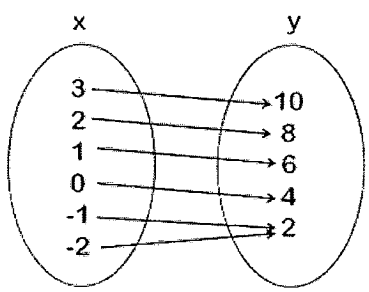
[1 Mark]

(iii) whenever p is true, q is true then at some later time

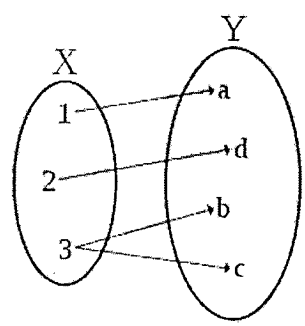
[1 Mark]

c) Which of the diagrams a), b) or both, as shown on Figure 1, define functions from X to Y? Justify your answer.

[2 Marks]



a)



b)

Figure 1

QUESTION 2 **[22 Marks]**

a) Express underlying mathematical methods for Z, TLA, and UPAALL notations.

[3 Marks]

b) Specify *types* of systems, which can be modelled with Z, TLA, and UPAALL notations.

[3 Marks]

c) Explain the neediness of the 'Schema' in Z notation. State the difference between *state* schema and *operation* schema.

[2 Marks]

d) Explain the difference between Z schema, marked by Δ (Delta) symbol and Z schema, marked by Ξ (Xi) symbol.

[2 Marks]

e) Discuss the principles of model based verification.

[2 Marks]

f) There is transition system M = $(S, \rightarrow, L)$ where
$S = \{s_0, s_1, s_2\}$,
transitions = $s_0 \rightarrow s_1$, $s_0 \rightarrow s_0$, $s_1 \rightarrow s_2$, $s_2 \rightarrow s_0$, $s_2 \rightarrow s_1$,
$L(s_0) = \{p\}$
$L(s_1) = \{q\}$
$L(s_2) = \{r\}$

(i) Draw a state transition diagram.

[2 Marks]

(ii) Build a computation tree by unwinding state transitions of *M*.

[3 Marks]

g) The mutual exclusion problem (*mutex*) is avoiding the simultaneous access to some kind of resources by use of the critical sections of concurrent processes. Express by formulas of temporal logic the *safety* and *liveness* property of the *mutex*.

(i) Only one process is in its critical section at any time (*safety*).

[2 Marks]

(ii) Whenever any process requests to enter its critical section, it will eventually be permitted to do so (*liveness*).

[3 Marks]

QUESTION 3 **[23 Marks]**

Modelling tasks communication in concurrent software system

Tasks in a concurrent software system cannot communicate directly, but via special synchronisation entities – let's call it Ports. Task can send a data to and receive a data from a Port. Communication between tasks and Port is *synchronous,* i.e. has *waiting* semantics. Task *send* a data to Port and *wait*, till other task takes the data. Data in a Port is stored in a FIFO, which has a limit on a maximum size of stored data.

Develop TLA specifications of this problem. Specify *safety* property, that not all tasks in the system are waiting and *liveness* property that after waiting a task eventually becomes runnable again. You can use TLATEX or ASCII notation. Comment your statements.

QUESTION 4 **[22 Marks]**

Develop model of an elevator control system in Z notation. Comment your statements.

An elevator system is to be installed in a building with m floors

The problem concerns the logic to move elevators between floors according to the following constraints:

- an elevator has a set of buttons, one for each floor. These illuminate when pressed and cause the elevator to visit the corresponding floor. The illumination is cancelled when the corresponding floor is visited by the elevator;
- each floor has two buttons (except the top and bottom floors), one to request upward travel and one to request downward travel. These buttons illuminate when pressed. The illumination is cancelled when an elevator visits the floor and is either moving in the desired direction or has no outstanding requests;
- when an elevator has no requests to service, it should remain at its final destination with its doors closed and await further requests.

QUESTION 5 **[23 Marks]**

Develop model of the following mutex problem as Timed Automata Diagram using UPPAALL notation.

A room with two doors which cannot be opened at the same time

Take into account following constraints:

- a door starts to open if a user pushes a button;
- the door opens for six seconds, thereafter it stays open for at least four seconds, but no more than eight seconds;
- the door takes six seconds to close and it stays closed for at least five seconds.

END OF QUESTION PAPER