SEMESTER 2 EXAMINATIONS 2013/2014

MODULE: CA648/A - Formal Programming

PROGRAMME(S):
  MCM - M.Sc. in Computing
  EEPT - PhD-track
  ECSAO - Study Abroad (Engineering and Computing)

YEAR OF STUDY: 1, 2, 0

EXAMINERS: Dr Geoffrey Hamilton (Ext:5017)
            Dr. Brian Lee

TIME ALLOWED: 3 hours

INSTRUCTIONS: Answer 5 questions. All questions carry equal marks.

PLEASE DO NOT TURN OVER THIS PAGE UNTIL INSTRUCTED TO DO SO

The use of programmable or text storing calculators is expressly forbidden.
Please note that where a candidate answers more than the required number of questions,
the examiner will mark all questions attempted and then select the highest scoring ones.

Requirements for this paper (Please mark (X) as appropriate)

- Log Tables
- Graph Paper
- Dictionaries
- Statistical Tables
- Thermodynamic Tables
- Actuarial Tables
- MCQ Only - Do not publish
- Attached Answer Sheet
QUESTION 1

Consider the following partial correctness specification:

{N ≥ 0}
X := 0;
Y := 0;
WHILE X < N DO
    BEGIN
    X := X + 1;
    Y := Y + X
    END
{Y = (N × (N + 1))/2}

1(a)  [6 Marks]
Add appropriate annotations to this specification to allow it to be verified.

1(b)  [6 Marks]
List the verification conditions which would be generated for the annotated specification in 1(a).

1(c)  [8 Marks]
Verify this specification by showing that the verification conditions in 1(b) are true.

[End Question 1]

QUESTION 2

Give a total correctness specification for the program in Question 1, and prove the total correctness of the program.

[End Question 2]

QUESTION 3

3(a)  [4 Marks]
Describe how a theory of program refinement can be defined on top of Floyd-Hoare logic.

3(b)  [4 Marks]
Define the specification notation [P, Q].
3(c) [12 Marks]

Refine the following specification to a corresponding program:

\[ N \geq 0, S = \sum_{i=0}^{N} i^2 \]

[End Question 3]

QUESTION 4 [Total marks: 20]

A project marking system needs to keep track of which students are assigned to which project, and their marks for this project. No student can be assigned to more than one project, no project can be assigned to more than one student and no student can be given a mark unless they have been assigned a project. The following events need to be handled:

**drop:** remove the specified student from the system; if this student was allocated a project, then this project will become available again.

**assign:** assign the given student to the given project; the student should not already have an assigned project and the assigned project should be available.

**studentquery:** gives the project which has been allocated to the specified student; the specified student must have an assigned project.

**projectquery:** gives the student who has been allocated the specified project; the specified project must have been assigned.

**entermark:** assigns the specified mark to the specified student for their project; the specified student must have an assigned project.

**markquery:** gives the mark for the project of the specified student; the specified student must have an assigned mark.

4(a) [2 Marks]

Define the context for an Event-B specification of the project marking system.

4(b) [6 Marks]

Define the variables for an Event-B specification of the project marking system. Define a suitable invariant for these variables, and show their initialisation, ensuring that this initialisation satisfies the invariant.

4(c) [12 Marks]

Specify the events for an Event-B specification of the project marking system, making use of the definitions in 4(a) and 4(b).

[End Question 4]
QUESTION 5  [Total marks: 20]

A car park consists of a set of car parking spaces, which may or may not be occupied. The following events should be handled:

park: assign the given car to an available parking space; this event is only enabled if there is a parking space available.

leave: remove the given car from the car park; this event is only enabled if the given car was previously assigned a parking space.

spaces: gives the number of available spaces in the car park.

5(a) [8 Marks]

Write an Event-B specification for this car park in which the state is represented by a single variable \textit{parked}, which gives the set of cars which are currently parked, and in which the capacity of the car park is given by the constant \textit{MaxSpaces}.

5(b) [4 Marks]

The car park specified in 5(a) is to be refined to one in which the state is represented by two variables: \textit{allocation}, which maps cars to unique parking spaces, and \textit{numspaces}, which gives the number of spaces currently available in the car park. Give a suitable linking invariant for this refinement.

5(c) [8 Marks]

Give a refinement for the car park specified in 5(a), which has been refined as described in 5(b).

[End Question 5]

[END OF EXAM]