Module: CA648 Formal Programming

Course: M.Sc. in Software Engineering

Year: 1

Examiners: Dr. A. Butterfield, Mr. D. Brady, Dr. G. Hamilton, Ext no. 5017.

Time Allowed: 3 hours

Instructions: Please answer all 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.
QUESTION 1  [TOTAL MARKS: 20]

Consider the following partial correctness specification:

\[
\{ T \} \\
R := X; \\
Q := 0; \\
WHILE Y \leq R DO \\
BEGIN \\
\quad R := R - Y; \\
\quad Q := Q + 1 \\
END \\
\{ X = R + (Y \times Q) \land R < Y \}
\]

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.

QUESTION 2  [TOTAL MARKS: 20]

Consider the following total correctness specification:

\[
[X = n \land n \geq 0] \\
Y := 1; \\
WHILE X > 0 DO \\
BEGIN \\
\quad X := X - 1; \\
\quad Y := 2 \times Y \\
END \\
[Y = 2^n]
\]

2(a)  [5 Marks]
Explain what is meant by an invariant, and define a suitable invariant for the loop in the above specification.

2(b)  [5 Marks]
Explain what is meant by a variant, and define a suitable variant for the loop in the above specification.

2(c)  [10 Marks]
Show that the above specification is true.
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:

\[N = n \land n > 0, FACT = n!\]

4(a) [4 Marks]
Define the context for an Event-B specification of the hotel reservation system.

4(b) [6 Marks]
Define the variables for an Event-B specification of the hotel reservation system. Define a suitable invariant for these variables, and show their initialisation, ensuring that this initialisation satisfies the invariant.

4(c) [10 Marks]
Specify the events for an Event-B specification of the hotel reservation system, making use of the definitions in 4(a) and 4(b).
QUESTION 5

5(a) [7 Marks]
Write an Event-B specification for a program computing the maximum value in an array \( a : 1..n \rightarrow \mathbb{N} \) where \( n \geq 1 \). The specification should have a result variable \( \text{result} \) and two abstract events \( \text{Initialisation} \) and \( \text{Maximum} \) which give appropriate preconditions and postconditions respectively for \( \text{result} \).

5(b) [8 Marks]
Give a refinement of the specification in 5(a) which adds variables \( \text{index} \) and \( \text{maxsofar} \), giving the value of the current index in the array, and the maximum of the elements in the array up to this index, respectively. Your refinement should also add two further events \( \text{Update} \) and \( \text{Progress} \). The \( \text{Update} \) event should update the value of the \( \text{maxsofar} \) variable if the array value at the current index is greater than it. The convergent event \( \text{Progress} \) should be used to ensure termination by decreasing the variant. You should also refine the events \( \text{Initialisation} \) and \( \text{Maximum} \) to give precise initial and final values for the \( \text{result} \) variable.

5(c) [5 Marks]
Give a program which computes the maximum of all the numbers in an array and is a refinement of your answers given in 5(a) and 5(b).