SEMESTER TWO EXAMINATIONS 2012

MODULE: CA648 Formal Programming

COURSE: M.Sc. in Software Engineering

YEAR: 1

EXAMINERS: Dr. A. Grzenkowicz,
Prof. M. Hinchey,
Dr. D. Gray, Ext no. 8056,
Dr. D. Sinclair, Ext no. 5510.

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:

\[
\{N \geq 0\}
S := 0;
I := -N;
WHILE I \leq N DO
    BEGIN
        S := S + I;
        I := I + 1
    END
\{S = 0\}
\]

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

1(b)  [8 Marks]
List the verification conditions which would be generated for the annotated specification in 1(a).

1(c)  [6 Marks]
Verify this specification by showing that the verification conditions in 1(b) are true.

QUESTION 2  [TOTAL MARKS: 20]

Using the partial correctness specification given in Question 1, give a total correctness specification for the program given in Question 1, and prove the total correctness of the program.
QUESTION 3 [TOTAL MARKS: 20]

3(a) [4 Marks]
What is the difference between program refinement and program verification? Give two advantages of using program refinement.

3(b) [4 Marks]
Define the program refinement law for WHILE commands.

3(c) [12 Marks]
Refine the following specification to a corresponding program:

\[ N \geq 0 \land T \geq 0, P = \text{product}(N, T) \]

where
\[ \text{product}(N, T) = N \times (N + 1) \times (N + 2) \times \cdots \times (N + T - 1) \]

and
\[ \text{product}(N, 0) = 1 \]
A tennis club needs to keep track of court bookings and also which members have been assigned to which courts. No member can reserve more than one court, no member can be assigned to more than one court, no member can be assigned a court without a prior booking and no court can be assigned to more than one pair of members. The number of courts in the tennis club is given by numcourts. The following events should be handled:

**book:** book a court for the given member; this member must have no previous booking, and there must be a court available

**checkin:** allocate the given pair of members to any available court; one of the members must have a booking, which will subsequently be removed

**checkout:** make the given court available; this court must have been assigned to a member

**courtquery:** output the court which has been allocated to the given member; this member must have been allocated a court

4(a) [4 Marks]
Define the context for an Event-B specification of the tennis club booking system.

4(b) [6 Marks]
Define the variables for an Event-B specification of the tennis club booking 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 tennis club booking 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 minimum value in an array $a : 1..n \rightarrow \mathbb{N}$ where $n \geq 1$. The specification should have a result variable $result$ and two abstract events $Initialisation$ and $Minimum$ which give appropriate preconditions and postconditions respectively for $result$.

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

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