UNIVERSITY OF WESTMINSTER

SCHOOL OF COMPUTER SCIENCE & ENGINEERING

Module Title: **Reasoning about Programs**

Module Code: **6SENG001W, 6SENG003C**

Exam Period: **January 2020**

Time Allowed: **2 Hours**

INSTRUCTIONS FOR CANDIDATES

PLEASE WRITE YOUR STUDENT ID CLEARLY AT THE TOP OF EACH PAGE.

You are advised (but not required) to spend the first ten minutes of the examination reading the questions and planning how you will answer those you have selected.

Answer ALL questions in Section A and TWO questions from Section B.

Section A is worth a total of 50 marks.
Each question in section B is worth 25 marks.

In section B, only the TWO questions with the HIGHEST MARKS will count towards the FINAL MARK for the EXAM.

The B-Method's Abstract Machine Notation (AMN) is given in Appendix B.

THIS PAPER MUST NOT BE TAKEN OUT OF THE EXAMINATION ROOM

DO NOT TURN OVER THIS PAGE UNTIL THE INVIGILATOR INSTRUCTS YOU TO DO SO

UNIVERSITY OF WESTMINSTER

MARKING SCHEME
DO NOT COPY

SCHOOL OF
COMPUTER SCIENCE & ENGINEERING

Module Title: **Reasoning about Programs**

Module Code: **6SENG001W, 6SENG003C**

Exam Period: **January 2020**

Time Allowed: **2 Hours**

INSTRUCTIONS FOR CANDIDATES

PLEASE WRITE YOUR STUDENT ID CLEARLY AT THE TOP OF EACH PAGE.

You are advised (but not required) to spend the first ten minutes of the examination reading the questions and planning how you will answer those you have selected.

Answer ALL questions in Section A and TWO questions from Section B.

Section A is worth a total of 50 marks.
Each question in section B is worth 25 marks.

In section B, only the TWO questions with the HIGHEST MARKS will count towards the FINAL MARK for the EXAM.

THIS PAPER MUST NOT BE TAKEN OUT OF THE EXAMINATION ROOM

DO NOT TURN OVER THIS PAGE UNTIL THE INVIGILATOR INSTRUCTS YOU TO DO SO

Section A

Answer ALL questions from this section.
You may also wish to consult the B-Method notation given in Appendix B.

Question 1

You are given the following collection of B set and function declarations for the Scottish Islands:

$$Scottish\_Islands \;=\; \{\; Skye, Islay, Mull, Jura, Lewis\_and\_Harris, \\ North\_Uist, South\_Uist, Benbecula \;\}$$

$$Inner\_Hebrides \;\in\; \mathbb{P}(Scottish\_Islands)$$
$$Inner\_Hebrides \;=\; \{\; Skye, Islay, Mull, Jura \;\}$$

$$Outer\_Hebrides \;\in\; \mathbb{P}(Scottish\_Islands)$$
$$Outer\_Hebrides \;=\; \{\; Lewis\_and\_Harris, North\_Uist, South\_Uist, Benbecula \;\}$$

$$highest\_point \;\in\; Scottish\_Islands \to \mathbb{N}$$
$$highest\_point \;=\; \{\; Skye \mapsto 993,\; Islay \mapsto 491,\; Mull \mapsto 966,\; Jura \mapsto 785, \\ Lewis\_and\_Harris \mapsto 799,\; North\_Uist \mapsto 347, \\ South\_Uist \mapsto 620,\; Benbecula \mapsto 124 \;\}$$

Evaluate the following expressions:

(a) $Outer\_Hebrides \cap \{\; Skye, South\_Uist, Mull, Benbecula \;\}$ **[1 mark]**

(b) $Inner\_Hebrides - \{\; North\_Uist, Islay, Jura \;\}$ **[2 marks]**

(c) $\mathrm{card}(\; highest\_point \;)$ **[1 mark]**

(d) $Scottish\_Islands \cap \mathrm{dom}(highest\_point)$ **[1 mark]**

(e) $\mathrm{ran}(highest\_point)$ **[1 mark]**

(f) $highest\_point(Lewis\_and\_Harris)$ **[1 mark]**

(g) $Inner\_Hebrides \lhd highest\_point$ **[2 marks]**

(h) $highest\_point \rhd 0..900$ **[3 marks]**

(i) $\mathbb{P}(\; \{\; Skye, Mull, Jura \;\} \;)$ **[3 marks]**
[TOTAL 15]

Section A

Answer ALL questions from this section.

Question 1

Scottish Islands expressions:

(a) $Outer\_Hebrides \cap \{\ Skye, South\_Uist, Mull, Benbecula\ \}$
$= \{\ South\_Uist, Benbecula\ \}$ **[1 mark]**

(b) $Inner\_Hebrides - \{\ North\_Uist, Islay, Jura\ \}$
$= \{\ Skye, Mull\ \}$ **[2 marks]**

(c) $\mathrm{card}(\ highest\_point\ )$
$= 8$ **[1 mark]**

(d) $Scottish\_Islands \cap \mathrm{dom}(highest\_point)$
$= Scottish\_Islands$ **[1 mark]**

(e) $\mathrm{ran}(highest\_point)$
$= \{\ 124, 347, 491, 620, 785, 799, 993, 966\ \}$ **[1 mark]**

(f) $highest\_point(Lewis\_and\_Harris)$
$= 966$ **[1 mark]**

(g) $Inner\_Hebrides \lhd highest\_point$
$= \{\ Skye \mapsto 993,\ Islay \mapsto 491,\ Mull \mapsto 966,\ Jura \mapsto 785\ \}$
[2 marks]

(h) $highest\_point \rhd 0..900$
$= \{\ Skye \mapsto 993,\ Mull \mapsto 966\ \}$ **[3 marks]**

(i) $\mathbb{P}(\ \{\ Skye, Mull, Jura\ \}\ )$

$$= \{\ \{\},\ \{\ Skye\ \}, \{\ Mull\ \}, \{\ Jura\ \},\ \{\ Skye, Mull\ \}, \{\ Skye, Jura\ \}, \{\ Mull, Jura\ \}\ \{\ Skye, Mull, Jura\ \}\ \}$$

[3 marks]

[QUESTION Total 15]

Question 2

Given the two relations:

$$R \in LETTER \leftrightarrow \mathbb{N}$$
$$Q \in \mathbb{N} \leftrightarrow COLOUR$$

$$R = \{ (a, 1), (a, 2), (b, 2), (c, 3), (d, 4), (e, 5) \}$$
$$Q = \{ (1, red), (2, blue), (3, green), (5, purple) \}$$

(a) The two relations R and Q *could be* composed using the relational composition operator ";" in two ways:

$$R ; Q$$
$$Q ; R$$

Explain why one of these compositions is possible and why one is not possible. **[2 marks]**

(b) Evaluate the "possible" composition of R and Q. **[3 marks]**

(c) For each of the relations R and Q state whether it is just a relation or is also a function. In addition, give the justification for your decisions. **[2 marks]**

[TOTAL 7]

Question 2

(a) Can compose $R ; Q$. Since the *target* of R is the *same type* as the *source* of Q, i.e. $\mathbb{N}$, the two relations can be composed. **[2 marks]**

(b) The composition of R and Q:

$$R ; Q \ : \ LETTER \leftrightarrow COLOUR$$
$$R ; Q \ = \ \{ \ (a, \ red), \ (a, \ blue), \ (b, \ blue), \ (c, \ green), \ (e, \ purple) \ \}$$

[3 marks]

(c) Relations or Functions:

R is just a relation because one value in the domain a maps to two values in the range 1 and 2, e.g. $(a, \ 1), \ (a, \ 2)$.

Q is also a function, because no value in the domain maps to two or more values in the range. (It is a partial injection.) **[2 marks]**

[QUESTION Total 7]

Question 3

(a)

- An Abstract Machine is a specification of what a system should be like, or how it should behave (operations); but not how a system is to be built, i.e. no implementation details. **[2 marks]**
- The main logical parts of an Abstract Machine are its: *name*, *local state*, represented by "encapsulated" variables, *state invariant* defines constraints on the state variables, that define what the valid states are. the variable's values must always satisfy the *state invariant*, *collection of operations*, that can access & update the state variables, but must always ensure that the *after state* of the operation satisfies the *state invariant*. **[5 marks]**
- An B Machine is similar to the programming concepts of: modules, class definition (e.g. Java) or abstract data types. **[1 mark]**
- The most obvious logical component of a B Machine that is not represented in a Java class is the `INVARIANT` clause that defines the *state invariant*. Java classes do not have any built in language feature that defines when an instance of a class is "valid". **[2 marks]**

[PART Total 10]

Question 3

(a) The building block of a B-method specification is the concept of an *Abstract Machine (AM)*. Explain what a B Abstract Machine is, in particular, you should answer the following questions:

- What is it a specification of?
- What are its main logical parts and what are the relationships between the parts?
- What is it similar to in terms of a programming language feature?
- Are there any logical components of a B machine that are not represented in your chosen programming language feature? What does this mean for the programming language feature?

[10 marks]

(b) Describe the three categories of states that a B machine can be in and illustrate your answer by means of a diagram. What clause of a B machine determines which state is which? **[8 marks]**

[TOTAL 18]

Question 4

(a) Explain in your own words the meaning of the Hoare triple

$$[y > z + 1]\ x := z\ [x < y]$$

[2 marks]

(b) Which of the following Hoare triples are valid? Give a counterexample for each invalid triple.

(i) $[x < y]\ x := y\ [false]$ **[2 marks]**

(ii) $[x < y]\ x := y\ [true]$ **[2 marks]**

(iii) $[x < y]\ y := y + 1\ [x < y + 1]$ **[2 marks]**

(iv) $[x = 3]\ x := y\ [y = 3]$ **[2 marks]**

[TOTAL 10]

(b) See Figure 1. Three categories of system states are: *valid* states, *initial* or *start* states & *error* or *invalid* states. **[1 mark]**

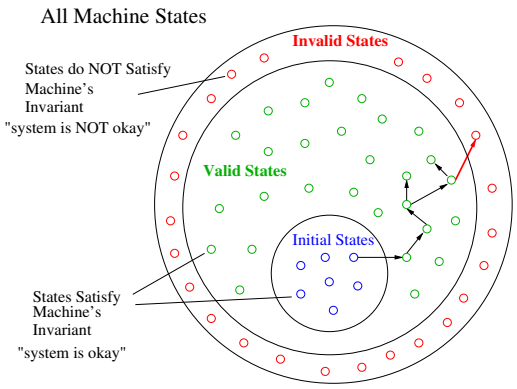

Figure 1: Possible B Machine States

[4 marks]

The *valid* states are those that satisfy the *state invariant*. The *invalid* states are those that do not satisfy the *state invariant*. The *state invariant* is the constraints & properties that the states of the machine must satisfy during its lifetime. Defined in the `INVARIANT` clause **[2 marks]**

The *initial state(s)* are the set of possible starting states of the machine. Any initial state must also be a valid state, i.e. one that satisfies the state invariant. Defined in the `INITIALISATION` clause. **[1 mark]**

[PART Total 8]

[QUESTION Total 18]

Question 4

Marking Scheme for Hoare Logic & Program Verification.

(a) The Hoare triple

$$[y > z + 1]\ x := z\ [x < y]$$

means that executing the instruction $x := z$ (i.e. assigning the value of z to x), starting from a state in which y is greater than $z + 1$, leads to a state in which x is less than y. **[2 marks]**

Question 3

(a) The building block of a B-method specification is the concept of an *Abstract Machine (AM)*. Explain what a B Abstract Machine is, in particular, you should answer the following questions:

- What is it a specification of?
- What are its main logical parts and what are the relationships between the parts?
- What is it similar to in terms of a programming language feature?
- Are there any logical components of a B machine that are not represented in your chosen programming language feature? What does this mean for the programming language feature?

[10 marks]

(b) Describe the three categories of states that a B machine can be in and illustrate your answer by means of a diagram. What clause of a B machine determines which state is which? **[8 marks]**

[TOTAL 18]

Question 4

(a) Explain in your own words the meaning of the Hoare triple

$$[y > z + 1]\ x := z\ [x < y]$$

[2 marks]

(b) Which of the following Hoare triples are valid? Give a counterexample for each invalid triple.

(i) $[x < y]\ x := y\ [false]$ **[2 marks]**

(ii) $[x < y]\ x := y\ [true]$ **[2 marks]**

(iii) $[x < y]\ y := y + 1\ [x < y + 1]$ **[2 marks]**

(iv) $[x = 3]\ x := y\ [y = 3]$ **[2 marks]**

[TOTAL 10]

[PART Total 2]

(b) **(i)** $[x < y]\ x := y\ [false]$ is invalid. **[1 mark]** Counterexample: Starting in a state with $x = 1, y = 2$ leads to a state with $x = 1, y = 1$, which (like all other states) does not satisfy $false$. **[1 mark]**

[SUBPART Total 2]

(ii) $[x < y]\ x := y\ [true]$ is valid, since any post-state satisfies $true$. **[2 marks]**

[SUBPART Total 2]

(iii) $[x < y]\ y := y + 1\ [x < y + 1]$ is valid: the weakest pre-condition is $x < y + 2$, which follows from the given pre-condition. **[2 marks]**

[SUBPART Total 2]

(iv) $[x = 3]\ x := y\ [y = 3]$ is invalid. **[1 mark]** Counterexample: Starting in a state with $x = 3, y = 0$ leads to a state with $x = 0, y = 0$, which does not satisfy $y = 3$. **[1 mark]**

[SUBPART Total 2]

[PART Total 8]

[QUESTION Total 10]

Section B

Answer TWO questions from this section.
You may wish to consult the B-Method notation given in Appendix B.

Question 5

Write a B-Method machine that specifies a *queue* of customers waiting to be served at a small village Post Office counter. Due to the Post Offices small size, the queue has to have a maximum length for customers.
Your B machine should deal with error handling where required and should include the following:

(a) Any sets, constants and variables, and any state invariant that the Post Office's customer queue requires. **[9 marks]**

(b) The Post Office queue operations:

(i) $JoinPOQueue$ – a new customer joins the end of the queue. **[7 marks]**

(ii) $GotoCounter$ – the next customer leaves the front of the queue and goes to the counter to be served. **[6 marks]**

(iii) $CustomersWaiting$ – reports via a suitable message whether the queue is empty then no; otherwise yes. **[3 marks]**

[TOTAL 25]

Section B

Answer TWO questions from this section.

Question 5

A Post Office queue B machine similar to the following is expected.
Some possible acceptable alternatives:
Uses B symbols not ASCII versions, or a mixture. Enumerates `CUSTOMER`:

```
CUSTOMER = { Jim, Joe, ... }
```

Combines **MARKING SCHEME FOR QUESTION**
& `REPORT` or uses string literals. Also likely that some less important parts are omitted, e.g. preconditions – "`report : REPORT`", use of `Nobody`. Using an ordinary sequence `seq` rather than an injective sequence `iseq`.

(a) `MACHINE PostOfficeQueue`

```
SETS
  CUSTOMER ;

  ANSWER = { Yes, No } ;

  REPORT = { Customer_Joined_Queue,
             ERROR_Queue_is_Full,
             Customer_Served,
             ERROR_Queue_Empty    }

CONSTANTS
  MaxPOqueueLength, EmptyQueue, Nobody

PROPERTIES
  MaxPOqueueLength : NAT1  &  MaxPOqueueLength = 5  &
  EmptyQueue : iseq( CUSTOMER ) &  EmptyQueue = [] &
  Nobody : CUSTOMER

VARIABLES
  POqueue
```

Section B

Answer TWO questions from this section.
You may wish to consult the B-Method notation given in Appendix B.

Question 5

Write a B-Method machine that specifies a *queue* of customers waiting to be served at a small village Post Office counter. Due to the Post Offices small size, the queue has to have a maximum length for customers.
Your B machine should deal with error handling where required and should include the following:

(a) Any sets, constants and variables, and any state invariant that the Post Office's customer queue requires. **[9 marks]**

(b) The Post Office queue operations:

(i) $JoinPOQueue$ – a new customer joins the end of the queue. **[7 marks]**

(ii) $GotoCounter$ – the next customer leaves the front of the queue and goes to the counter to be served. **[6 marks]**

(iii) $CustomersWaiting$ – reports via a suitable message whether the queue is empty then no; otherwise yes. **[3 marks]**

[TOTAL 25]

```
INVARIANT
  POqueue : iseq( CUSTOMER ) & size( POqueue ) <= MaxPOqueueLength
  & Nobody /: ran( POqueue )

INITIALISATION
  POqueue := EmptyQueue
```

Marks for each clause: SETS [**3 marks**] , CONSTANTS & PROPERTIES [**3 marks**] , VARIABLES INVARIANT & INITIALISATION [**3 marks**] .

[**PART Total 9**]

(b) OPERATIONS

```
report <-- JoinPOQueue( customer ) =
    PRE
        customer : CUSTOMER & customer /: ran( POqueue )
        & customer /= Nobody & report : REPORT
    THEN
        IF ( size( POqueue )  < MaxPOqueueLength )
        THEN
            POqueue  := POqueue <- customer       ||
            report := Customer_Joined_Queue
        ELSE
            report := ERROR_Queue_is_Full
        END
    END ;
```

[Subpart (b.i) 7 marks]

```
report, nextcustomer <-- GotoCounter =
    PRE
        nextcustomer : CUSTOMER & report : REPORT
    THEN
        IF ( POqueue /= EmptyQueue )
        THEN
            nextcustomer := first( POqueue )  ||
            POqueue  := tail( POqueue )       ||
            report := Customer_Served
        ELSE
            nextcustomer := Nobody        ||
            report := ERROR_Queue_Empty
         END
```

Section B

Answer TWO questions from this section.
You may wish to consult the B-Method notation given in Appendix B.

Question 5

Write a B-Method machine that specifies a *queue* of customers waiting to be served at a small village Post Office counter. Due to the Post Offices small size, the queue has to have a maximum length for customers.
Your B machine should deal with error handling where required and should include the following:

(a) Any sets, constants and variables, and any state invariant that the Post Office's customer queue requires. **[9 marks]**

(b) The Post Office queue operations:

(i) $JoinPOQueue$ – a new customer joins the end of the queue. **[7 marks]**

(ii) $GotoCounter$ – the next customer leaves the front of the queue and goes to the counter to be served. **[6 marks]**

(iii) $CustomersWaiting$ – reports via a suitable message whether the queue is empty then no; otherwise yes. **[3 marks]**

[TOTAL 25]

```
        END ;
```

[Subpart (b.ii) 6 marks]

```
    answer <-- CustomersWaiting =
        PRE
            answer : ANSWER
        THEN
            IF ( POqueue = EmptyQueue )
            THEN
                 answer := No
            ELSE
                 answer := Yes
            END
        END

END  /* PostOfficeQueue */
```

[Subpart (b.iii) 3 marks]

[**PART Total 16**]

[**QUESTION Total 25**]

Question 6

See the `Club` B machine given in the exam paper's Appendix A.

(a) The `Club`'s invariants:

`queuetotal < capacity` – the length of club's waiting list is less than the maximum number of members allowed. [**2 marks**]

`members <: NAME` – the club's members is a collection/list of names. [**1 mark**]

`waiting <: NAME` – the people on the club's waiting list are a collection/list of names. [**1 mark**]

`members /\ waiting = {}` – no one can be a member & on the waiting list to join the club. [**2 marks**]

Question 6

Appendix A contains the `Club` B abstract machine, this specifies a simple club's membership list scheme.
The club has a number of members. To join the club a new member must first join the waiting list then he/she can then become a club member.
The system provides the following operations:

- Joining the club as a member.
- Joining the club's waiting list to become a member.
- Leaving the club.
- Reset the club's membership and waiting lists.
- Checking if someone is a member of the club.

With reference to the `Club` machine, *using "plain English"* answer the following questions.

(a) Give the meaning of the six predicates that form the `Club`'s invariant, as given in the `INVARIANT` clause:

```
20        queuetotal < capacity  &
21        members <: NAME &
22        waiting <: NAME  &
23        members /\ waiting = {}  &
24        card(members) <= capacity  &
25        card(waiting) <= queuetotal
```

[12 marks]

(b) Explain the meaning of the *preconditions* for the operations:

(i) `join` **[2 marks]**

(ii) `join_queue` **[4 marks]**

(iii) `remove` **[2 marks]**

(c) Draw the *Structure Diagram* for the `Club` machine. **[5 marks]**

[TOTAL 25]

`card(members) <= capacity` – the club has a maximum membership (list of member's names). **[2 marks]**

`card(waiting) <= queuetotal` – the club has a maximum membership waiting list & given the first invariant it cannot be more than the maximum club size. **[2 marks]**

[PART Total 10]

(b) The meaning of the *preconditions* for the operations:

(i) `join` preconditions – the parameter `newmember` is the name of someone who is currently on the waiting list; the club is not full yet, i.e. hasn't reach maximum members. **[2 marks]**

(ii) `join_queue` preconditions – the parameter `newmember` is the name of someone who is currently not a club member or on the waiting list; the club's waiting list is not full yet, i.e. hasn't reach maximum limit. **[4 marks]**

(iii) `remove` preconditions – the parameter `member` is the name of someone who is currently a member of the club. **[2 marks]**

[PART Total 8]

(c) The `Club` machine's Structure Diagram – Figure 2. Internal structure

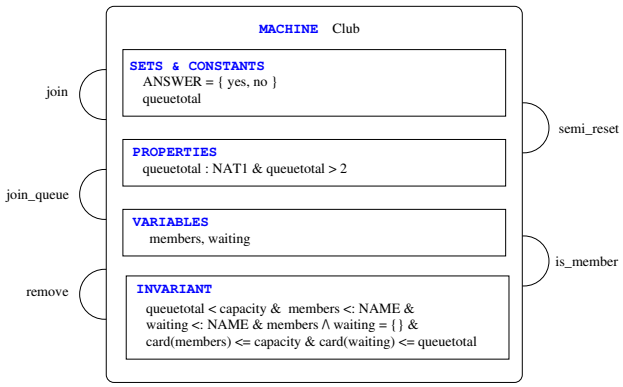

Figure 2: `Club` machine's Structure Diagram.

[4 marks] , Operations **[2 marks]** .

[PART Total 6]

[QUESTION Total 25]

Question 7

(a) Find the missing assertions using pre-condition propagation.

```
[assertion 1]
  y:=y-1;
[assertion 2]
  x:=x+z;
[assertion 3]
  y:=x+y
[x=y+1]
```

[9 marks]

(b) Find suitable intermediate assertions for the following Hoare triple; this involves finding an invariant for the loop.

```
[u>0]
x:=0;
y:=0;
[invariant]
WHILE y<v DO
[assertion 1]
  x:=x+u;
[assertion 2]
  y:=y+1
[assertion 3]
END
[x=u*v]
```

[16 marks]

[TOTAL 25]

Question 7

Marking Scheme for Hoare Logic & Program Verification.

(a) The intermediate assertions are

1. $0 = y$ **[2 marks]**
2. $0 = y + 1$ **[2 marks]**
3. $x = x + y + 1$ or $0 = y + 1$ **[2 marks]**

[PART Total 9]

(b) The invariant and intermediate assertions are:

- Invariant: $x = u * y \ \& \ y \leq v$ **[4 marks]**
- Assertion 1: $x = u * y \ \& \ y < v$ **[4 marks]**
- Assertion 2: $x = u*(y+1) \ \& \ y+1 \leq v$ (or e.g. $x = u*y+u \ \& \ y < v$) **[4 marks]**
- Assertion 3: $x = u * y \ \& \ y \leq v$

[PART Total 16]

[QUESTION Total 25]

Appendix A. Club B Machine

The following is a B Machine – `Club` that specifies a club's membership scheme.

```
1    MACHINE  Club(NAME, capacity)
2
3      CONSTRAINTS
4        capacity : NAT1  &  5 <= capacity  &
5        capacity < card(NAME)
6
7      SETS
8       ANSWER = { yes, no }
9
10     CONSTANTS
11       queuetotal
12
13     PROPERTIES
14       queuetotal : NAT1 & queuetotal > 2
15
16     VARIABLES
17       members, waiting
18
19     INVARIANT
20       queuetotal < capacity  &
21       members <: NAME &
22       waiting <: NAME  &
23       members /\ waiting = {}  &
24       card(members) <= capacity  &
25       card(waiting) <= queuetotal
26
27     INITIALISATION
28       members := {} || waiting := {}
29
```

[Continued on next page.]

```
30   OPERATIONS
31
32     join( newmember ) =
33       PRE  newmember : waiting & card(members) < capacity
34       THEN    members := members \/ { newmember }
35            || waiting := waiting - { newmember }
36       END ;
37
38     join_queue( newmember ) =
39       PRE newmember : NAME  &  newmember /: members  &
40           newmember /: waiting  &  card(waiting) < queuetotal
41       THEN waiting := waiting \/ { newmember }
42       END ;
43
44     remove( member ) =
45       PRE  member : members
46       THEN members := members - { member }
47       END ;
48
49     reset_club_lists
50       BEGIN
51          members, waiting := {}, members
52       END ;
53
54     ans <-- is_member( member ) =
55       PRE member : NAME
56       THEN
57         IF ( member : members )
58         THEN ans := yes
59         ELSE ans := no
60         END
61       END
62
63   END /* Club */
```

Appendix B. B-Method's Abstract Machine Notation (AMN)

The following tables present AMN in two versions: the "pretty printed" symbol version & the ASCII machine readable version used by the B tools: *Atelier B* and *ProB*.

B.1 AMN: Number Types & Operators

B Symbol	ASCII	Description
$\mathbb{N}$	`NAT`	Set of natural numbers from 0
$\mathbb{N}_1$	`NAT1`	Set of natural numbers from 1
$\mathbb{Z}$	`INTEGER`	Set of integers
$\mathrm{pred}(x)$	`pred(x)`	predecessor of x
$\mathrm{succ}(x)$	`succ(x)`	successor of x
$x + y$	`x + y`	x plus y
$x - y$	`x - y`	x minus y
$x * y$	`x * y`	x multiply y
$x \div y$	`x div y`	x divided by y
$x \bmod y$	`x mod y`	remainder after x divided by y
$x \mathbin{\widehat{}} y$	`x ** y`	x to the power y, x^y
$\min(A)$	`min( A )`	minimum number in set A
$\max(A)$	`max( A )`	maximum number in set A
$x \mathinner{..} y$	`x .. y`	range of numbers from x to y inclusive

B.2 AMN: Number Relations

B Symbol	ASCII	Description
$x = y$	`x = y`	x equal to y
$x \neq y$	`x /= y`	x not equal to y
$x < y$	`x < y`	x less than y
$x \leq y$	`x <= y`	x less than or equal to y
$x > y$	`x > y`	x greater than y
$x \geq y$	`x >= y`	x greater than or equal to y

B.3 AMN: Set Definitions

B Symbol	ASCII	Description
$x \in A$	`x : A`	x is an element of set A
$x \notin A$	`x /: A`	x is not an element of set A
$\varnothing$, $\{\ \}$	`{}`	Empty set
$\{\ 1\ \}$	`{ 1 }`	Singleton set (1 element)
$\{\ 1, 2, 3\ \}$	`{ 1, 2, 3 }`	Set of elements: 1, 2, 3
$x\,..\,y$	`x .. y`	Range of integers from x to y inclusive
$\mathbb{P}(A)$	`POW(A)`	Power set of A
$\mathrm{card}(A)$	`card(A)`	Cardinality, number of elements in set A

B.4 AMN: Set Operators & Relations

B Symbol	ASCII	Description
$A \cup B$	`A \/ B`	Union of A and B
$A \cap B$	`A /\ B`	Intersection of A and B
$A - B$	`A - B`	Set subtraction of A and B
$\bigcup AA$	`union( AA )`	Generalised union of set of sets AA
$\bigcap AA$	`inter( AA )`	Generalised intersection of set of sets AA
$A \subseteq B$	`A <: B`	A is a subset of or equal to B
$A \not\subseteq B$	`A /<: B`	A is not a subset of or equal to B
$A \subset B$	`A <<: B`	A is a strict subset of B
$A \not\subset B$	`A /<<: B`	A is not a strict subset of B
$\{\ x \mid x \in TS \wedge C\ \}$	`{ x | x : TS & C }`	Set comprehension

B.5 AMN: Logic

B Symbol	ASCII	Description
$\neg P$	`not P`	Logical negation (not) of P
$P \wedge Q$	`P & Q`	Logical and of P, Q
$P \vee Q$	`P or Q`	Logical or of P, Q
$P \Rightarrow Q$	`P => Q`	Logical implication of P, Q
$P \Leftrightarrow Q$	`P <=> Q`	Logical equivalence of P, Q
$\forall\, xx \cdot (P \Rightarrow Q)$	`!(xx).(P => Q)`	Universal quantification of xx over $(P \Rightarrow Q)$
$\exists\, xx \cdot (P \wedge Q)$	`#(xx).(P & Q)`	Existential quantification of xx over $(P \wedge Q)$
$TRUE$	`TRUE`	Truth value $TRUE$.
$FALSE$	`FALSE`	Truth value $FALSE$
$BOOL$	`BOOL`	Set of boolean values $\{ TRUE, FALSE \}$
$bool(P)$	`bool(P)`	Convert predicate P into $BOOL$ value

B.6 AMN: Ordered Pairs & Relations

B Symbol	ASCII	Description
$X \times Y$	`X * Y`	Cartesian product of X and Y
$x \mapsto y$	`x |-> y`	Ordered pair, maplet
$\mathrm{prj}_1(S,T)(x \mapsto y)$	`prj1(S,T)(x |-> y)`	Ordered pair projection function
$\mathrm{prj}_2(S,T)(x \mapsto y)$	`prj2(S,T)(x |-> y)`	Ordered pair projection function
$\mathbb{P}(X \times Y)$	`POW(X * Y)`	Set of relations between X and Y
$X \leftrightarrow Y$	`X <-> Y`	Set of relations between X and Y
$\mathrm{dom}(R)$	`dom(R)`	Domain of relation R
$\mathrm{ran}(R)$	`ran(R)`	Range of relation R

B.7 AMN: Relations Operators

B Symbol	ASCII	Description
$A \lhd R$	`A <| R`	Domain restriction of R to the set A
$A \lhd\!\!\!\!- R$	`A <<| R`	Domain subtraction of R by the set A
$R \rhd B$	`R |> B`	Range restriction of R to the set B
$R \rhd\!\!\!\!- B$	`R |>> B`	Range anti-restriction of R by the set B
$R[B]$	`R[B]`	Relational Image of the set B of relation R
$R_1 \lhd\!\!+ R_2$	`R1 <+ R2`	R_1 overridden by relation R_2
$R\,;Q$	`( R ; Q )`	Forward Relational composition
$\mathrm{id}(X)$	`id(X)`	Identity relation
R^{-1}	`R~`	Inverse relation
R^n	`iterate(R,n)`	Iterated Composition of R
R^+	`closure1(R)`	Transitive closure of R
R^*	`closure(R)`	Reflexive-transitive closure of R

B.8 AMN: Functions

B Symbol	ASCII	Description
$X \pfun Y$	`X +-> Y`	Partial function from X to Y
$X \fun Y$	`X --> Y`	Total function from X to Y
$X \pinj Y$	`X >+> Y`	Partial injection from X to Y
$X \inj Y$	`X >-> Y`	Total injection from X to Y
$X \psur Y$	`X +->> Y`	Partial surjection from X to Y
$X \surj Y$	`X -->> Y`	Total surjection from X to Y
$X \bij Y$	`X >->> Y`	(Total) Bijection from X to Y
$f \lhd\!\!+ g$	`f <+ g`	Function f overridden by function g

B.9 AMN: Sequences

B Symbol	ASCII	Description
$[\,]$	`[]`	Empty Sequence
$[\,e1\,]$	`[ e1 ]`	Singleton Sequence
$[\,e1,\ e2\,]$	`[ e1, e2 ]`	Constructed (enumerated) Sequence
$\mathrm{seq}(X)$	`seq( X )`	Set of Sequences over set X
$\mathrm{iseq}(X)$	`iseq( X )`	Set of injective Sequences over set X
$\mathrm{size}(s)$	`size( s )`	Size (length) of Sequence s

B.10 AMN: Sequences Operators

B Symbol	ASCII	Description
$s \frown t$	`s^t`	Concatenation of Sequences s & t
$e \rightarrow s$	`e -> s`	Insert element e to front of sequence s
$s \leftarrow e$	`s <- e`	Append element e to end of sequence s
$rev(s)$	`rev( s )`	Reverse of sequence s
$first(s)$	`first( s )`	First element of sequence s
$last(s)$	`last( s )`	Last element of sequence s
$front(s)$	`front( s )`	Front of sequence s, excluding last element
$tail(s)$	`tail( s )`	Tail of sequence s, excluding first element
$conc(SS)$	`conc(SS)`	Concatenation of sequence of sequences SS
$s \uparrow n$	`s /|\ n`	Take first n elements of sequence s
$s \downarrow n$	`s |/ n`	Drop first n elements of sequence s

B.11 AMN: Miscellaneous Symbols & Operators

B Symbol	ASCII	Description
$var := E$	`var := E`	Assignment
$S1 \,\|\|\, S2$	`S1 || S2`	Parallel execution of $S1$ and $S2$

B.12 AMN: Operation Statements

B.12.1 Assignment Statements

```
xx := xxval

xx, yy, zz := xxval, yyval, zzval

xx := xxval  ||  yy := yyval
```

B.12.2 Deterministic Statements

```
skip

BEGIN  S  END

PRE  PC  THEN  S  END

IF  B  THEN  S  END

IF  B  THEN  S1  ELSE  S2  END

IF  B1  THEN  S1  ELSIF B2  THEN  S2  ELSE  S3  END

CASE  E  OF
  EITHER  v1  THEN  S1
  OR      v2  THEN  S2
  OR      v3  THEN  S3
  ELSE
          S4
END
```

B.13 B Machine Clauses

```
MACHINE Name( Params )

  CONSTRAINTS    Cons

  EXTENDS        M1, M2, ...

  INCLUDES       M3, M4, ...
  PROMOTES       op1, op2, ...

  SEES           M5, M6, ...
  USES           M7, M8, ...

  SETS            Sets
  CONSTANTS       Consts
  PROPERTIES      Props

  VARIABLES       Vars
  INVARIANT       Inv
  INITIALISATION  Init

  OPERATIONS

    yy <-- op( xx ) =
           PRE  PC
           THEN Subst
           END ;
    ...
END
```