COMP 317: Semantics of Programming Languages

Program Verification Exercise Solutions

Specification

Exercises

1. Specify a program that doubles the value of the variable `'x`.

   ```
   ops  pre post : Store Int -> Bool .

   var S : Store .
   var X : Int .

   eq  pre(S,X)  =  (S[['x]]) is X .
   eq  post(S,X) =  (S[['x]]) is 2 * X .
   ```

2. Specify a program that sets `'x` to the sum of the values of the variables `'y` and `'z`.

   ```
   ops  pre post : Store Int Int -> Bool .

   var  S : Store .
   vars Y Z : Int .

   eq  pre(S,Y,Z)  =  (S[['y]]) is Y and (S[['z]]) is Z .
   eq  post(S,Y,Z) =  (S[['x]]) is Y + Z .
   ```

3. Specify a program that adds the value of `'x` to the variable `'y`.

   ```
   eq  pre(S,X,Y)  =  (S[['x]]) is X and (S[['y]]) is Y .
   eq  post(S,X,Y) =  (S[['y]]) is Y + X .
   ```

4. Specify a program that sets `'x` to the maximum of the values of `'a` and `'b`.

   ```
   eq  pre(S,A,B)  =  (S[['a]]) is A and (S[['b]]) is B .
   eq  post(S,A,B) =  (S[['x]]) is max(A,B) .
   ```

5. Explain in words what the following specification requires:

   ```
     ops pre post : Store Int -> Bool .
     var S : Store .
     var X0 : Int .
     eq  pre(S,X0)  =  (S[['x]]) is X0  and  0 <= X0 .
     eq  post(S,X0) =  2 * (S[['p]]) + (S[['r]]) is X0  and  0 <= (S[['r]])  and  (S[['r]]) < 2 .
   ```

Integer division by 2, with remainder!

6. Specify a program that sets `'p` to 2 to the power of the (initial) value of `'e`, where (the initial value of) `'e` is at least 0.

```
eq  pre(S,X)  =  (S[['e]]) is X  and  0 <= X .
eq  post(S,X,Y) =  (S[['p]]) is 2 ^ X .
```

Implementation

Exercise 7

Give implementations for each of the specifications in the Exercises above.

1. `'x := 2 * 'x`
2. `'x := 'y + 'z`
3. `'y := 'y + 'x`
4. `if 'a < 'b then 'x := 'b else 'x := 'a endif`
5. See the "While-loops" section below.

And (6) is implemented by

```
'p := 1 ;
while 0 < 'e
do
  'p := 'p * 2 ;
  'e := 'e - 1
od
```

Verification

Exercise 8

Show that the following program also satisfies the "swap" specification:

```
'x := 'x + 'y  ;  'y := 'x - 'y  ;  'x := 'x - 'y .
```

Done in Problem Sheet 7.

Conditionals

Exercise 9

Give a program that sets `'x` to the maximum of the values of `'a` and `'b` (cf. Exercise 4 above). Give a Maude proof score that shows the program is correct.

Done in Problem Sheet 7.

While-loops

Exercises

1. The following program also computes `2 ** 'x`:

   ```
   'p := 1 ;
   while 0 < 'x
   do
      'p := 'p * 2 ;
      'x := 'x - 1
   od
   ```

   Give a Maude proof score that verifies this.

   See pow.maude.

2. Exercise 5 above (in the section on Specification) specifies a program that computes the results of integer division by two (the result is stored in `'p`) and remainder on division by two (the result is stored in `'r`). Give a program that satisfies this specification, and prove it correct.

   See div.maude.

Grant Malcolm