Assignment 0

Engi-8893 / Engi-9869 Theodore Norvell

Due 9:00 Thursday 2006 Jan 26.

Please submit on paper. Solutions must be typed. Diagrams, if any, may be hand drawn.

Q0[10]

Let a and b be arrays (indexed from 0 to $n-1$) of integers.

(a)[5] Develop a proof outline that shows that

```
int c ;
c := 0 ;
while( c < n ) {
      b[c] := a[c] ;
      c := c + 1 ; }
```

Has a postcondition of

$$\forall i \in \{0, 1, ..., n-1\} \cdot b[i] = a[i]$$

Hint: Use

$$(0 \leq c \leq n) \wedge (\forall i \in \{0, 1, ..., c-1\} \cdot b[i] = a[i])$$

as a loop invariant.

(b)[5] Complete the proof, by listing the Hoare triples and other formulae that must be shown valid and explaining why each one is valid.[1]

[1] One issue not covered in the notes, is assignment to array items. If a is an array and all mentions of a in Q are of the form $a[i]$, then we have

$$\frac{P \Rightarrow Q_{a[i] \leftarrow E}}{\{P\}\ a[i] := E\ \{Q\}}$$

Q1 [10]. Consider the following proof outline.[2]

$\#\# \neg f \wedge w = W \wedge x = X \wedge x = X \wedge y = Y \wedge z = Z$
Global Inv: $f \Rightarrow w = W * Z$
co

$\quad \#\# w = W \wedge z = Z$
$\quad \langle w, f := w * z, true \rangle$

//

$\quad \#\# x = X \wedge y = Y$
$\quad \langle x := x * y; \rangle$
$\quad \#\# x = X * Y$
$\quad \langle$**await** $(f) \rangle$
$\quad \#\# x = X * Y \wedge f$
$\quad \langle x := x * w; \rangle$
$\quad \#\# x = X * Y * W * Z$

oc
$\#\# x = X * Y * W * Z$

(i)[5] Show that the global invariant really is invariant. I.e., show that it is implied by the precondition and that each atomic action preserves it.

(ii)[5] In order to show that the two parallel statements do not interfere with each other, a number of Hoare triples must be shown to be valid. List all these Hoare triples and explain why each one is in fact valid.

Q2 [20]. Consider the following array copy algorithm

```
int buf ;
int p := 0, c := 0 ;
co
    while( p < n ) {
        < await ( p=c ) ; >
        < buf := a[p] ; >
        < p := p + 1 ; > }
```

[2] As a notational convenience, rather than repeating the global invariant everywhere, I'm just stating it once at the start of the co-statement. One should consider the global invariant to be conjoined to each assertion within the co-statement. For example the precondition of the first assignment statement is

$$w = W \wedge z = Z \wedge (f \Rightarrow w = W * Y)$$

```
//
      while( c < n ) {
           <await ( p > c ) ; >
           < b[c] := buf ; >
           < c := c+1 ; > }
oc
```

(a)[10] Develop a valid proof outline that has *true* as precondition and

$$\forall i \in \{0, 1, ..., n-1\} \cdot b[i] = a[i]$$

as a postcondition. There is no requirement to demonstrate that the proof outline is valid (yet).

Be sure that your proof outline is in fact valid and in particular, free of interference.

Hint: Use the following as global invariants

$$0 \leq p \leq n$$
$$0 \leq c \leq n$$
$$p = c \vee p = c + 1$$
$$p = c + 1 \Rightarrow buf = a[c]$$

Use as a loop invariant for the second loop

$$\forall i \in \{0, 1, ..., c-1\} \cdot b[i] = a[i]$$

Try to keep additional assertions as weak as possible.

Meta-hint. If you don't follow the above hint, then part (b) may not even make sense!

My advice is to simply list the global invariants prior to the co-statement, rather than duplicating them all over the place (see Q1 for an example.)

(b) [10] The answers to the five subparts of this question should constitute the nontrivial aspects of a proof that your outline from part (a) is valid. Remember that you can use any of the global invariants as (a part of) the precondition of any atomic action in the co-statement. For each subpart write out the Hoare triple(s) that must be shown valid and provide an argument that it/they are valid.[3]

(i) Show that $p = c \vee p = c + 1$ is a global invariant by showing it is a post-condition of each action that changes either p or c.

[3] See footnote 1 about assignments to array elements.

(ii) Show that $p = c + 1 \Rightarrow buf = a[c]$ is a global invariant, in the same manner.

(iii) Show that $b[c] = a[c]$ is is a postcondition of the assignment $b[c] := buf$.

(iv) For any assertions, other than the global invariants, that appear in the producer and that involve variables b or c, list the Hoare triples that must be shown valid to ensure there is no interference from the consumer. Explain why each of these Hoare triples is valid.

(v) Likewise, for any assertions, other than the global invariants, that appear in the consumer and that involve variables buf or p, list the Hoare triples that must be shown to be valid to ensure that there is no interference from the producer. Explain why each of these Hoare triples is valid.

Q3[10] Consider the following algorithm

---

int $x := 0$;
co

$\langle x := x - 2; \rangle$

//

$\langle x := x - 3; \rangle$

//

$\langle x := x + 5; \rangle$

oc

Develop a proof outline to show that the final value of x is 0.

To do this, you will need to introduce at least one ghost-variable. Show that the resulting proof-outline is valid.