CS245 Tutorial

Nov. 23, 2015

1. For the following code fragment, determine how to modify the pre-condition and post-condition such that one can prove that the triple (pre-condition, program, post-condition) is satisfied under partial correctness.

$(\!| A[i] = x_0 \wedge A[j] = y_0 |\!)$
```
A[i] = A[i] + A[j] ;
A[j] = A[i] - A[j] ;
A[i] = A[i] - A[j] ;
```
$(\!| A[i] = y_0 \wedge A[j] = x_0 |\!)$

Solution:

Pre-condition and post-condition:

As written the triple is incorrect. We must add the condition $i \neq j$ to the pre-condition and the post-condition to establish the correctness of the code.

Annotated Program:

$(\!| A[i] = x_0 \ \wedge \ A[j] = y_0 \ \wedge \ i \neq j |\!)$ pre-condition

$(\!| A\{i \leftarrow A[i] + A[j]\}[j] = y_0 \ \wedge$
$A\{i \leftarrow A[i] + A[j]\}[i] - A\{i \leftarrow A[i] + A[j]\}[j] = x_0 \ \wedge \ i \neq j |\!)$ implied (a)

```
A[i] = A[i] + A[j];
```

$(\!| A[j] = y_0 \ \wedge \ A[i] - A[j] = x_0 \ \wedge \ i \neq j |\!)$ assignment

$(\!| A\{j \leftarrow A[i] - A[j]\}[i] - A\{j \leftarrow A[i] - A[j]\}[j] = y_0 \ \wedge$
$A\{j \leftarrow A[i] - A[j]\}[j] = x_0 \ \wedge \ i \neq j |\!)$ implied (b)

```
A[j] = A[i] - A[j];
```

$(\!| A[i] - A[j] = y_0 \ \wedge \ A[j] = x_0 \ \wedge \ i \neq j |\!)$ assignment

$(\!| A\{i \leftarrow A[i] - A[j]\}[i] = y_0 \ \wedge$
$A\{i \leftarrow A[i] - \ A[j]\}[j] = x_0 \ \wedge \ i \neq j |\!)$ implied (c)

```
A[i] = A[i] - A[j];
```

$(\!| A[i] = y_0 \ \wedge \ A[j] = x_0 \ \wedge \ i \neq j |\!)$ assignment

Note: in the annotated program we work backwards through an assignment and then simplify the assertion before working backwards through the next assignment. Alternatively, it is possible to work backwards through all three assignments and only then simplify the assertion, but this becomes too unwieldy.

Proofs of implied conditions

Each of the implied conditions labeled with (a, b, c) can be shown to follow from their preceding condition using the definition of array assignment,

$$A\{i \leftarrow e\}[j] = \begin{cases} e & \text{if } i = j \\ A[j] & \text{if } i \neq j \end{cases}$$

and simple algebraic manipulation.

We suggest that you first sketch out part of the "proof" for the original triple, without $i \neq j$. Work backwards from the original post-condition,

$(\!| A\{i \leftarrow A[i] - A[j]\}[i] = y_0 \ \wedge \ A\{i \leftarrow A[i] - A[j]\}[j] = x_0 \ \wedge \ i \neq j \,|\!)$

```
A[i] = A[i] - A[j];
```

$(\!| A[i] = y_0 \ \wedge \ A[j] = x_0 \,|\!)$ `assignment`

and show how the condition,

$(\!| A\{i \leftarrow A[i] - A[j]\}[i] = y_0 \wedge A\{i \leftarrow A[i] - A[j]\}[j] = x_0 \,|\!)$

is simplified. The first conjunct simplifies as before. For the second conjunct, consider the case when $i = j$ and $i \neq j$. When $i = j$, the expression

$A\{i \leftarrow A[i] - A[j]\}[j] = x_0$

simplifies to

$A[i] - A[j] = x_0$

which, in turn, simplifies to

$0 = x_0$,

which looks like trouble and indicates the proof will fail.