Assignment 0

Theodore S. Norvell

5892 Due 2020 Jan 20, 14:00

You may submit in class or electronically using brightspace.

Q0 Find the first

(a) [10] Using the verification rules in the notes, list all the conditions that must be shown to be universally true in order to show that the following proof outline is partially correct. Perform all substitutions. I.e. state the condition using the substitution notation (when applicable) and then restate it after doing the substitutions. Assume state variables p and k are integers and that a is an array of integers of length at least length M, indexed from 0.

$\{\mathcal{A} : M \geq 0\}$
$p, k := 0, 0$
$\{\mathcal{B} : 0 \leq p \leq M \wedge 0 \leq k \leq M \wedge (k = p \vee a(k) = 42) \wedge (\forall i \in \{0, ..k\} \cdot a(i) \neq 42)\}$
while $p < M \wedge$ $k = p$ do
  $\{\mathcal{C} : 0 \leq p < M \wedge -1 \leq k \leq M \wedge k = p \wedge (\forall i \in \{0, ..p\} \cdot a(i) \neq 42)\}$
  if $a(p) \neq 42$ then
    $\{\mathcal{D} : 0 \leq p < M \wedge -1 \leq k \leq M \wedge k = p \wedge (\forall i \in \{0, ..p+1\} \cdot a(i) \neq 42)\}$
    $k := k + 1$
  end if
  $\{\mathcal{E} : 0 \leq p + 1 \leq M \wedge 0 \leq k \leq M \wedge (k = p + 1 \vee a(k) = 42) \wedge (\forall i \in \{0, ..k\} \cdot a(i) \neq 42)\}$
  $p := p + 1$
end while
$\{\mathcal{F} : 0 \leq k \leq M \wedge (k = M \vee a(k) = 42) \wedge (\forall i \in \{0, ..k\} \cdot a(i) \neq 42)\}$

(b) [5] Which of the conditions listed are universally true? Which are not?

Q1 [10] Log. All variables are integer. [Updated 2020-01-15.]

Complete this proof outline so that it is provably correct using the rules presented in the notes.

$\{\mathcal{P} : n = N \geq 1\}$
$\cdots$
$\left\{\mathcal{I} : n \geq 1 \wedge n \times 2^k \leq N < (n+1) \times 2^k\right\}$
while $n > 1$ do
  $\left\{\mathcal{Q} : n > 1 \wedge n \times 2^k \leq N < (n+1) \times 2^k\right\}$
  $\cdots$
end while
$\left\{\mathcal{R} : 2^k \leq N < 2^{k+1}\right\}$

Here N is a specification variable (so don't assign to it). Ensure also that any execution that starts in a state where the precondition is true will terminate.

Q2 [5] Moving average

Suppose $a : \mathbb{N} \to \mathbb{R}$ is an infinite sequence. Define $f : \mathbb{Z}^+ \to \mathbb{R}$ by

$$f(i) = (a(i-1) + a(i) + a(i+1))\,/3, \text{ for all } i \in \mathbb{Z}^+$$

where $\mathbb{Z}^+ = \{i \in \mathbb{Z} \mid i > 0\}$.

Consider this algorithm in which x, y, and z are real, p and N are integer, b is real sequence of at least N items.

$\{N > 0\}$
$x, y := a(0), a(1)$
$p := 1$
$\{\mathcal{I}\}$
while $p \neq N$ do
  $z := a(p+1)$
  $b(p) := (x + y + z)\,/3$
  $x, y := y, z$
  $p := p + 1$
end while
$\{\forall i \in \{1, ..N\} \cdot b(i) = f(i)\}$

State a loop invariant $\mathcal{I}$ that could be used to verify this algorithm.

Note: In this example, there is an assignment to an array element. We can consider the assignment $b(p) := (x + y + z)\,/3$ to be equivalent to an assignment

$$b := b[0, ..p]\hat{}\,[(x + y + z)\,/3]\hat{}\,b[p, ..\text{len}(b)]$$

In other words, we assign to b a sequence that is the same as b except that, in position p, it has the value of $(x + y + z)\,/3$. This expression is only defined when $0 \leq p \leq \text{len}(b)$. You shouldn't worry about all the technical details of showing that

$\{\mathcal{I} \wedge p \neq N\}$
$z := a(p+1)$
$b(p) := (x + y + z)\,/3$
$x, y := y, z$
$p := p + 1$
$\{\mathcal{I}\}$

is correct. Just worry about finding a condition that will make this outline correct and also meet all the other conditions of a loop invariant.