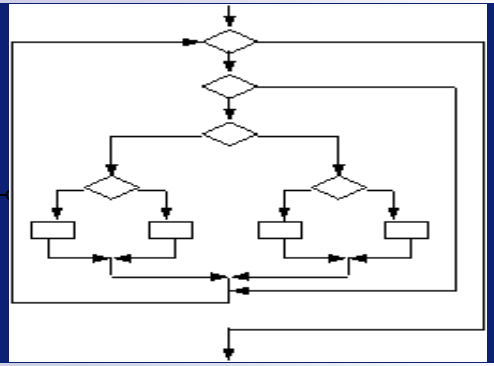
Spring 2008



Program correctness

Arrays

Marcello Bonsangue

Leiden Institute of Advanced Computer Science
Research & Education

Array Types and Array Syntax

- Let a[1 … n] denote an array with as index an integer between 1 and n (included)
- Then a[e] denotes the element at position i in the array a if the evaluation of the expression e is the integer i with $1 \leq i \leq n$
- And |a| denote the length of the array a,
  - i.e. |a| = n

Meaning of array assignments

- Let a, b be two array variables. Then:
  - a:=b assigns the value of array a to the array variable b
  - a[e]:=e' assigns the value of e' to position e in the array a
  - but a[e]:=e' fails, or 'goes wrong', if $e \leq 0$ or $e < |a|$
- In partial correctness, we do not need to take array boundaries into account
  - For example, {true}a[|a|+1] {true} is valid

Array assignments and aliasing

- Simple assignments remain simple:
  $\{\psi[b/a]\}\ a:=b\ \{\psi\}$
  is valid (partial correctness)
- But what about a[e]:=e' ?
- How can we substitute a[e] by e' ?
- Moreover, a[e] may have aliases:
  a[3], a[1+2], a[5-2], etc. all denote the same location

Arrays as functions

- An array a[1…|a|] of values can be seen as a function a from the index values to the element values

  update: a[e] := e’ is the same as a :=a[e’/e]

  reading: a[e] is the same as a(e)

- Recall that $a[e'/e](i) = \begin{cases} e' & \text{if } e=i \\ a(i) & \text{otherwise} \end{cases}$

The solution: function substitution

- Since an array is just a variable whose type happens to be “function”, we can simply replace the entire function

- a[i] := e is the same as a := a[e/i] thus along the lines of the ordinary assignment axiom we have

$$\{\psi[a[e'/e]/a]\}\ a[e] := e'\ \{\psi\}$$

Weakest precondition of array updates

- The formula $\psi[a[e'/e]/a]$ is not the weakest precondition of ψ w.r.t. an array update a[e]:=e'

  Why?

  Because the value e may fall outside that of the array a, so update may also fail! For total correctness we have to prove that assignment doesn't fail.

- $wp(a[e] := e', \psi) = \psi[a[e'/e]/a] \wedge 0 < e \leq |a|$

Example I

- $\{ true \}\ a[3] := 5\ \{ a[3] = 5 \}$

  We get:

  $(a[3] = 5)[a[5/3]/a] \Leftrightarrow a[5/3][3] = 5$

  Clearly, $true \Rightarrow a[5/3][3]=5$

Example II

- {a[j] = 4} a[i] := a[j]+1 {a[i] = 5}

(a[i] = 5)[a[a[j]+1/i]/a]

$\Leftrightarrow$ a[a[j]+1/i][i] =5

$\Leftrightarrow$ a[j]+1 = 5

$\Leftrightarrow$ a[j] = 4

Example 3

- {|b|>2} a:=b; a[1]:=3; a[1]:= a[1]+1; b:=a {b[1]=4}

Example 4

$\{ a[i] = i \}\ a[a[i]] := i\ \{ a[i] = i \}$

$(a[i] = i)[(a[i/a[i]])/a]$

$\Leftrightarrow a[i/a[i]](i) = i$

$\Leftrightarrow (a[i] = i \wedge i = i) \vee (a[i] \neq i \wedge a[i] = i)$

$\Leftrightarrow a[i] = i$