531 2013-02-21

Note Title 2013-02-21

An example of use of axiomatic semantics to prove correctness of a simple program.
(This example is written in Modula-2.)

(* Pre : $a \le b+1$ *)

$i := a$; $sum := \phi$;

Pre' → **while** $i \ne b+1$ **do**

$sum := sum + A[i]$;

$i := i+1$;

end;

Pre': $a \le b+1 \wedge i = a \wedge sum = \phi$

~~Claim: $sum = \sum_{j=a}^{i} A[j]$ is a loop invariant.~~

~~**Check:** $I \wedge \neg B \Rightarrow Post$~~

~~$sum = \sum_{j=a}^{i} A[j] \wedge i = b+1 \Rightarrow sum = \sum_{j=a}^{b} A[j]$~~ ? No

$$(* \text{Post} : \text{sum} = \sum_{j=a}^{b} A[j] *)$$

To prove correctness of a loop, we use the method of loop invariants.

Another guess at a loop invariant is $\text{sum} = \sum_{j=a}^{i-1} A[j]$

$$I \wedge \neg B \Rightarrow \text{Post}$$

$$\text{sum} = \sum_{j=a}^{i-1} A[j] \wedge i = b+1 \Rightarrow \text{sum} = \sum_{j=a}^{b} A[j]$$

$Pre' \Rightarrow I$

$a \leq b+1 \wedge i = a \wedge sum = 0 \Rightarrow sum = \sum_{j=a}^{i-1} A[j]$ (TBD)

$sum = \sum_{j=a}^{i-1} A[j]$ is invariant. (TBD)

(To be contined.)