



# Program Correctness 1 of 2

## Program Correctness

If the proper condition to run the program holds, and the program is run, then the program will halt, and when it halts, the desired result follows.

Precondition Post condition  
Termination

Pre + Post : Specification

In general,  $\text{Precon} \Rightarrow (\text{Termination and Postcon})$

Prove 2 parts (iterative code)

(i)  $\text{Precon} \Rightarrow \text{Termination}$

"Proving Termination"

(ii)  $(\text{Precon and Termination}) \Rightarrow \text{Postcon}$

"Proving Partial Correctness"

Corollary: (PWO)

Every (strictly) decreasing sequence of natural numbers is finite.

Loop Invariant (LI):

A statement that's true on entry to the loop, and after every iteration.

Special Induction for proving LI

Basis: Prove LI holds on entry to loop

IS: For any, if LI holds before the iteration, then LI holds after the iteration.

Ex 1:

Prove correctness for the following program.

Pre:  $n \in \mathbb{N}$

Post: Return  $n^2$

SQ(n)

Trace:  $n=4$

1.  $S = 0$ ;  $d = 1$ ;  $i = 0$
2. while  $i < n$ :
3.      $S = S + d$
4.      $d = d + 2$
5.      $i = i + 1$
6. return  $S$

Iteration	S	d	i
0	0	1	0
1	1	3	1
2	4	5	2
3	9	7	3
4	16	9	4

## Ex 1 Continued ...

Step 1: Find an LI

$$(i) \ s = i^2 \quad (ii) \ d = 2i + 1 \quad (iii) \ 0 \leq i \leq n$$

Step 2: Prove LI

Basis: On entry to loop

$$s = 0, i = 0, d = 1$$

$$s = i^2, d = 2i + 1, 0 \leq i \leq n$$

I.S: Consider an arbitrary iteration

Suppose LI holds before the iteration [IH]

WTP LI holds after the iteration.

$$s' = s + d \quad [\text{Line 3}] \quad i' = i + 1 \quad [\text{Line 5}]$$

$$= i^2 + 2i + 1 \quad [\text{IH}]$$

$$= (i+1)^2$$

$$= i'^2, \text{ as wanted}$$

$$d' = d + 2 \quad [\text{Line 4}]$$

$$= (2i+1) + 2 \quad [\text{IH}]$$

$$= 2(i+1) + 1$$

$$= 2i' + 1, \text{ as wanted}$$

$$i < n \quad [\text{because of the while condition}]$$

$$\therefore 0 \leq i < i+1 \leq n, \text{ as wanted}$$

Step 3: Prove Partial Correctness (i.e. LI + exit condition  $\Rightarrow$  Post condition)

Suppose loop terminates and consider the values of  $s, d, i$  on exit.

By LI (iii),  $i \leq n$

By exit condition,  $i \geq n$

Hence  $i = n$  (\*)

$$\begin{aligned} \text{By LI (i), } s &= i^2 \\ &= n^2 \quad [*] \end{aligned}$$

By line 6,  $s = n^2$  is returned as wanted

## Ex 1 Continued ...:

Step 4: Find expression  $e$  to associate with each iteration of loop.

$$e = n - i$$

Step 5: Prove  $e \geq 0$  and  $e$  is strictly decreasing. WTS  $e' = e - 1 < e$

By LI(iii),  $i \leq n \therefore e = n - i \geq 0$

Consider an arbitrary iteration:

$$\begin{aligned} e' &= n - i' \\ &= n - (i + 1) \quad [\text{Line 5}] \\ &= n - i - 1 \\ &= e - 1 < e \quad \text{as wanted} \end{aligned}$$

## Ex 2:

Pre:  $n \in \mathbb{N}$

Post: return  $n^2$

SQ(n)

1. if  $n = 0$ :
2.     result = 0
3. else:
4.     result = SQ(n-1) + 2n - 1
5. return result

General Form

$Q(k)$ : if precondition and  $k = \text{"input size"}$ , then program halts and postcondition follows.

(i.e. the program is correct when input size is  $k$ .)

Then use PCI to prove  $Q(k)$  holds for all valid values of  $k$ .

Proof:

$Q(k)$ : If  $n \in \mathbb{N}$  and  $k = n$ , then SQ(n) halts and returns  $n^2$ .

$Q(n)$ : If  $n \in \mathbb{N}$ , then  $Q(n)$  returns  $n^2$

Use PCI to prove  $Q(n) \forall n \in \mathbb{N}$ , then correctness follows.

Base cases: Let  $n = 0$

SQ(n) returns 0 [lines 1, 2, 5]

$\therefore$  SQ(n) returns  $n^2$ , as wanted.

## Ex 2 continued...

Proof:

I.S: Let  $n > 0$

Suppose  $Q(j)$  holds whenever  $0 \leq j < n$  [I.H.]

WTP  $Q(n)$  holds

Since  $n > 0$ ,  $SQ(n)$  runs line 4 [line 1]

Also, since  $n > 0$ , then  $0 \leq n-1 < n$ .

Hence I.H. applies to  $SQ(n-1)$

By I.H.,  $SQ(n-1)$  returns  $(n-1)^2$

By lines 4,5,  $SQ(n)$  returns  $(n-1)^2 + 2n - 1 = n^2 - 2n + 1 + 2n - 1$   
 $= n^2$ , as wanted