

pre-condition
 - program code
post-condition
 if pre-cond. then post-cond

Oct 20-10:02 AM

Loops:
 pre-cond
 while (G) { // G is guard
 // no break/continue
 }
 post-cond.

Oct 20-10:05 AM

compute $m \cdot x$ $product = m \cdot x$
 Pre-cond: m is non-neg integer,
 x is a real number,
 and $product = 0$, and $i = 0$
 while ($i \neq m$)
 (1) $product := product + x$
 (2) $i := i + 1$ $\underbrace{x + x + \dots + x}_m$
 end while
 Post cond: $product = m \cdot x$

Oct 20-10:09 AM

Loop invariant: predicate over integers $I(k)$
 satisfies:
 1) True prior to first iteration of loop
 2) For each iteration if it is true before iteration then it is true after
 3) If the loop terminates in a finite # of steps then the truth of I ensures correctness of the loop.

Oct 20-10:15 AM

Given a loop w/ a guard G , pre/post cond. and an invariant $I(n)$ show
 I. Basis: pre-cond implies that $I(0)$ is true
 II. Inductive Property: for $k \geq 0$ $k \in \mathbb{Z}$
 if $G \wedge I(k)$ then $I(k+1)$
 III. Eventual falsity of the guard
 in a finite # of steps, G is false
 IV. Correctness of the post cond.
 If N is the least number of iterations after which G is false and $I(N)$ then post cond. is true.

Oct 20-10:19 AM

Product Guard: $i \neq m$
 $I(n)$: $i = n$ and $product = nx$
 pre-cond: $m \in \text{non-neg int}$
 $x \in \text{real}$
 $i = 0$
 $product = 0$
 post-cond: $product = m \cdot x$

Oct 20-10:27 AM

Basis

I(0) $i=0$ and $\text{product}=0 \cdot x=0$
true by pre-cond.

II If $G \wedge I(k)$ then $I(k+1)$
for $k \geq 0$

Suppose: $i \neq m$ and $i=k$ and
 $\text{product}=k \cdot x$

[Show: $i=k+1$ and $\text{product}=(k+1)x$]

Since G is true statements 1,2
will be executed

Prior to (1) $\text{product}_{\text{old}}=kx$
after (1) $\text{product}_{\text{new}}=\text{product}_{\text{old}}+x$
 $= kx + x$
 $= (k+1)x$

$i_{\text{new}}=i_{\text{old}}+1$ $i_{\text{old}}=k$
 $= k+1$

$\therefore I(k+1)$ is true after the iteration

Oct 20-10:31 AM

III: falsity of the guard
 $G: i \neq m$ and m is non-neg.
from I, II we know that
if the loop is terminated n times
then $i=n$
 \therefore after m iterations G is false

IV Correctness of post-cond.
[$\text{product}=m \cdot x$]

if G is false after N iterations
then $I(N)$ ensures post-cond
is true.

G is false so $i=m$

$I(N)$ is true so $i=N$ and
 $\text{product}=N \cdot x$

so $\text{product}=N \cdot x = i \cdot x = m \cdot x$
which is the post cond. QED

Oct 20-10:40 AM