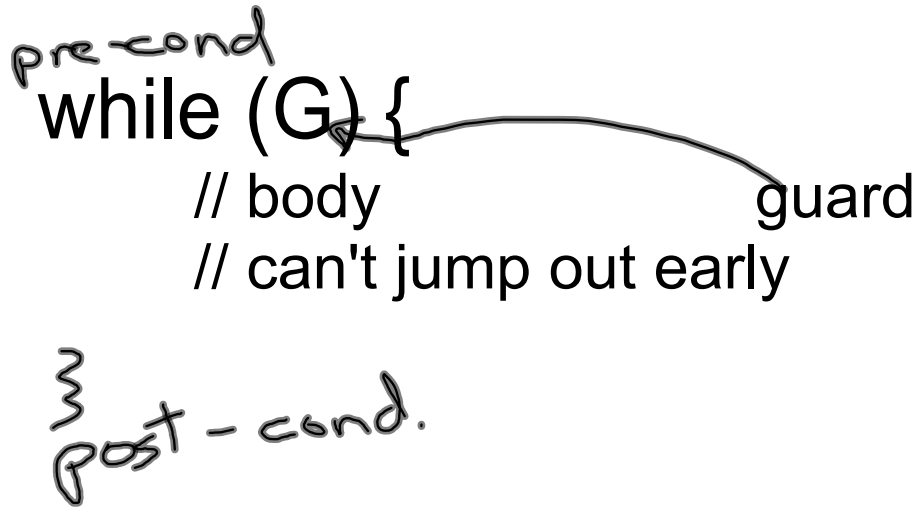
Correctness of loops (method of loop invariants)



Loop invariant

- Predicate over the set of integers

1. true before the first iteration $P(0)$
2. For each iteration
   if it is true before,
   then it is true after.
3. If the loop finishes after finite steps, then the truth of the invariant ensures the truth of the post-cond.

Given: a while loop
a guard G
an invariant $I(n)$

If the following are true,
then the loop is correct

I. Basis $I(0)$ is true

II. Induction $\forall k \geq 0, k \in \mathbb{Z}$
if $G \wedge I(k)$ then $I(k+1)$

III. Eventual falsity of G

IV. Correctness of the post condition

product $m \cdot x$

Pre-cond: m is a non-neg int, x is real, $i = 0$ and product $= 0$

```
while ( i ≠ m)
    product := product + x
    i := i + 1
end while
```

Postcondition: product $= m \cdot x$

Loop invariant: $I(n)$: $i = n$ and product $= n \cdot x$

I. Basis $I(0)$

Show $i=0$ and product $=0 \cdot x$ true from precondition.

II. Induction: if $I(k) \wedge G$ then $I(k+1)$

Suppose $I(k)$ and G are true for some k, prior to an iteration of the loop

Show $I(k+1)$ is true after that iteration.

$I(k)$ is true so $i=k$ and product $= k \cdot x$

G is true so $i \neq m$

Since G is true, statement 1 is executed.

$\text{product}_{new} = \text{product}_{old} + x$

and $\text{product}_{old} = k \cdot x$

so $\text{product}_{new} = k \cdot x + x$ (subst. ind. hyp)

$= (k+1) \cdot x$

Also stat. 2 is executed

so $i_{new} = i_{old} + 1$

and $i_{old} = k$

so $i_{new} = k+1$

So $I(k+1)$ is true.

III Eventual falsity of the Guard.

G: $i \neq m$

m is a non-neg. int

from I and II

for all $n \geq 0$ if the loop is iterated n Times then $i = n$ and product $= n \cdot X$

So after m iterations $i = m$.

So G is false

IV Correctness of the post condition

post-cond: product $= m \cdot X$ after execution of the loop

G is false after m iterations (from III)

and I(m) was true

so product $= mX$

QED

Pre-cond	i = 0	product = 0
I(0)	0	0
I(1)	1	x
I(2)	2	2 · x
⋮		
I(m)	m	m · x
post-cond		m · x