While Loops (annotation template)

$(\!\vert\ P\ \vert\!)$	invariant	
$(\!\vert\ I\ \vert\!)$		implied (a)
while (B) {		
$\quad (\!\vert\ (I \wedge B)\ \vert\!)$	①	partial-while
$\quad\quad C$		
$\quad (\!\vert\ I\ \vert\!)$		[justify based on C]
}		
$(\!\vert\ (I \wedge (\neg B))\ \vert\!)$	②	partial-while
$(\!\vert\ Q\ \vert\!)$		implied (b)

proof of implied (a) $\vdash (P \rightarrow I)$

(b) $\vdash ((I \wedge (\neg B)) \rightarrow Q)$.

I is a loop invariant $\sim$ "does not change".

the body of the loop

How do we find an invariant to complete our proof?

- An invariant expresses a relationship among the variables
  $(\!\vert\ (I \wedge B)\ \vert\!)\ C\ (\!\vert\ I\ \vert\!)$ is true
- Many invariants exist, but which one works for our proof?

the precondition ① $(P \rightarrow I)$ is true

② $((I \wedge (\neg B)) \rightarrow Q)$ is true

the postcondition

While Loops

Prove that the following program satisfies the given triple under partial correctness.

$\{ (n \geq 0) \land (a \geq 0) \}$

$s = 1;$

$i = 0;$

The loop guard

→ while $(i < n)$ {

$s = s * a;$

$i = i + 1;$

}

$\{ s = a^n \}$

Trace the program.

s	i	n	a
1	0	5	2
2	1	5	2
4	2	5	2
8	3	5	2
16	4	5	2
32	5	5	2

① Which one is NOT an invariant?

(a) $s \geq i$ — if $a = 1$, then $s = 1$ and s can be less than i.

(b) $s = a^i$

(c) $i \leq n$

② Which invariant is useful for our proof?

$s = a^i$ because it is very similar to our postcondition. $s = a^n$.

While Loops

Prove that the following program satisfies the given triple under partial correctness. $I = (s = a^i)$

1 $(\!|\ (n \geq 0) \wedge (a \geq 0)\ |\!)$
2 $(\!|\ (1 = a^0)\ |\!)$
$s = 1;$
$(\!|\ (s = a^0)\ |\!)$
$i = 0;$
☆ $(\!|\ (s = a^i)\ |\!)$
$\text{while } (i < n)\ \{$
☆ $(\!|\ ((s = a^i) \wedge (i < n))\ |\!)$

$s = s * a;$

$i = i + 1;$
☆ $(\!|\ (s = a^i)\ |\!)$
$\}$
☆ 15 $(\!|\ ((s = a^i) \wedge (i \geq n))\ |\!)$
16 $(\!|\ s = a^n\ |\!)$

Check 2 things.

① Does the precondition imply I? $1 \to 2$?
(a) YES (b) NO.

② Does $(I \wedge (\neg B))$ imply the postcondition?
(a) YES (b) NO

Scenario 1: $i = n$, $s = a^i = a^n$.
15 is True
16 is True.

Scenario 2: $i = n+1$, $s = a^i = a^{n+1}$
15 is True.
16 is False.

How do we fix this? It would be amazing if we also know $i \leq n$.

Let's try this new invariant
$((s = a^i) \wedge (i \leq n))$

While Loops

Prove that the following program satisfies the given triple under partial correctness

$(\!|\ (n \geq 0) \wedge (a \geq 0)\ |\!)$

$(\!|\ ((1 = a^0) \wedge (0 \leq n))\ |\!)$ implied (a)

$s = 1;$

$(\!|\ ((s = a^0) \wedge (0 \leq n))\ |\!)$ assignment

$i = 0;$

$(\!|\ ((s = a^i) \wedge (i \leq n))\ |\!)$ assignment

while $(i < n)$ {

$\quad (\!|\ (((s = a^i) \wedge (i \leq n)) \wedge (i < n))\ |\!)$ partial-while

$\quad (\!|\ ((s * a = a^{i+1}) \wedge ((i+1) \leq n))\ |\!)$ implied (b)

$\quad s = s * a;$

$\quad (\!|\ ((s = a^{i+1}) \wedge ((i+1) \leq n))\ |\!)$ assignment

$\quad i = i + 1;$

$\quad (\!|\ ((s = a^i) \wedge (i \leq n))\ |\!)$ assignment

}

$(\!|\ (((s = a^i) \wedge (i \leq n)) \wedge (i \geq n))\ |\!)$ partial-while

$(\!|\ s = a^n\ |\!)$ implied (c)

Proof of implied (a): $((n \geq 0) \wedge (a \geq 0)) \vdash ((1 = a^0) \wedge (0 \leq n))$

1.	$((n \geq 0) \wedge (a \geq 0)$	assumption
2	$n \geq 0$ (or $0 \leq n$)	$\wedge e$: 1
3.	$1 = a^0$	def. of factorial
4.	$((1 = a^0) \wedge (0 \leq n))$	$\wedge i$: 2, 3

Proof of implied (b):

$(((s=a^i) \wedge (i \leq n)) \wedge (i<n)) \vdash ((s*a=a^{i+1}) \wedge ((i+1) \leq n))$.

1. $(((s=a^i) \wedge (i \leq n)) \wedge (i<n))$ premise
2. $i<n$ $\wedge e$: 1
3. $(i+1) \leq n$ def of $<$ & $\leq$.
4. $((s=a^i) \wedge (i \leq n))$ $\wedge e$: 1
5. $(s=a^i)$. $\wedge e$: 4.
6. $s*a=a^{i+1}$ EQsubs $(*a)$: 5.
7. $((s*a=a^{i+1}) \wedge ((i+1) \leq n))$ $\wedge i$: 3, 6.

Proof of implied (c):

$(((s=a^i) \wedge (i \leq n)) \wedge (i \geq n)) \vdash (s=a^n)$.

1. $(((s=a^i) \wedge (i \leq n)) \wedge (i \geq n))$ premise
2. $(i \geq n)$ $\wedge e$: 1.
3. $((s=a^i) \wedge (i \leq n))$ $\wedge e$: 1.
4. $(i \leq n)$ $\wedge e$: 3.
5. $(i=n)$ def. of $\geq, \leq, =$: 2 & 4.
6. $(a^i=a^n)$ EQsubs (a^z): 5.
7. $(s=a^i)$ $\wedge e$: 3.
8. $(s=a^n)$ EQtrans(1): 6, 7.

Proving Termination.

How do we prove that a while-loop terminates?

Identify an integer expression that is.

① non-negative throughout the execution of the program.

② decreasing by at least 1 every time the loop runs.

Variant "changes".

$(n-i)$ is a suitable variant.

① $(n-i)$ is always non-negative.

Before the loop starts, $n \geq 0$ in the precondition and $i = 0$ by assignment. So $(n-i) \geq 0$. The loop guard $i < n$ ensures that $(n-i) \geq 0$.

② $(n-i)$ decreases by 1 every time the loop runs.

- n does not change. no assignment to it.
- i increases by 1 by assignment.
- Thus, $(n-i)$ decreases by 1.

Therefore, the loop will run a finite # of times and will end when $(n-i)$ reaches 0.

To prove termination, why is it sufficient to find a variant?

A non-negative integer can only decrease a finite # of times before reaching zero. The loop will terminate in a finite # of iterations.

How do we find a variant?

The loop guard usually helps.

While Loops

Prove that the following program satisfies the given triple under partial correctness.

$(\!|(x \geq 0)|\!)$

$(\!|(1 = 0!)|\!)$ implied (a)

$y = 1;$

$(\!|(y = 0!)|\!)$ assignment

$z = 0;$

$(\!|(y = z!)|\!)$ assignment

while $(z \mathrel{!}= x)$ {

$(\!|((y = z!) \land (\neg(z = x)))|\!)$ partial-while

$(\!|(y \cdot (z+1) = (z+1)!)|\!)$ implied. (b)

$z = z + 1;$

$(\!|(y \cdot z = z!)|\!)$ assignment.

$y = y * z;$

$(\!|(y = z!)|\!)$ assignment.

}

$(\!|((y = z!) \land (z = x))|\!)$ partial while

$(\!|(y = x!)|\!)$ implied (c)

② Proof of implied (b): $(((y = z!) \land (\neg(z = x))) \vdash (y \cdot (z+1) = (z+1)!)$

Proof:

1.	$(y = z!) \land (\neg(z = x))$	premise
2.	$y = z!$	$\land e$: 1.
3.	$y \cdot (z+1) = z! \cdot (z+1)$	EQsubs$(\cdot(z+1))$: 2
4	$z! \cdot (z+1) = (z+1)!$	def. of factorial: 3
5.	$y \cdot (z+1) = (z+1)!$	EQtrans: 3,4

③ Proof of implied (c): $((y=z!)\wedge(z=x)) \vdash (y=x!)$

1. $((y=z!)\wedge(z=x))$ premise
2. $(y=z!)$ $\wedge e$: 1
3. $(z=x)$ $\wedge e$: 1.
4. $(z!=x!)$ EQsubs(factorial): 3
5. $(y=x!)$ EQtrans: 2,4.

② Proof of implied (a): $(x\geq 0) \vdash (1=0!)$

1. $(x\geq 0)$ premise
2. $1=0!$ by def. of factorial.