While Loops - Examples of finding invariants Nov 21.

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

```
{(x ≥ 0)}
{(1 = 0!)}
y = 1;
{(y = 0!)}
z = 0;
{(y = z!)}
while (z != x){
    {(y = z!) ∧ (¬(z = x))}
    {(y*(z+1) = (z+1)!}
    z = z + 1;
    {(y*z = z!)}
    y = y * z;
    {(y = z!)}
}
{(y = z!) ∧ (z = x)}
{(y = x!)}
```

y	z	x
0! = 1	0	5
1! = 1	1	5
2! = 2	2	5
3! = 6	3	5
4! = 24	4	5
5! = 120	5	5

A possible invariant:
$y = z!$

① A useful invariant often looks very similar to the post condition.

② A useful invariant allows us to prove all the implied conditions.

While Loops

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

I changed the while test from $(z! = x)$ to $(z < x)$. The invariant $(y = z!)$ no longer works. Instead, we need to use this new invariant $((y = z!) \wedge (z \leq x))$

$\{(x \geq 0)\}$

$y = 1;$

$z = 0;$

$\{((y = z!) \wedge (z \leq x))\}$

while $(z < x)\{$

$\{(((y = z!) \wedge (z \leq x)) \wedge (z < x))\}$

$z = z + 1;$

$y = y * z;$

$\{((y = z!) \wedge (z \leq x))\}$

$\}$

$\{(((y = z!) \wedge (z \leq x)) \wedge (z \geq x))\}$

$\{(y = x!)\}$

While Loops

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

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

$\{ 1 = a^0 \}$ implied (a)

$s = 1;$

$\{ s = a^0 \}$

$i = 0;$

$\{ s = a^i \}$

while $(i < n)$ {

$\{ (s = a^i) \wedge (i < n) \}$

$\{ s * a = a^{i+1} \}$ implied b

$s = s * a;$

$\{ s = a^{i+1} \}$

$i = i + 1;$

$\{ s = a^i \}$

}

$\{ s = a^i \wedge i \geq n \}$

$\{ s = a^n \}$ implied c

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

A possible invariant: $s = a^i$

① Does the invariant look similar to our post condition? Yes.

② Does the invariant allow us to prove all the implied conditions? No.

We cannot prove implied c unless $i \leq n$. Luckily, $i \leq n$ is an invariant also. So 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

I changed the while test from $(i < n)$ to $(i != n)$. Now, the invariant $s = a^i$ works for our proof.

$\{ (n \geq 0) \wedge (a \geq 0) \}$
$\{ (1 = a^0) \}$
$s = 1;$
$\{ (s = a^0) \}$
$i = 0;$
$\{ (s = a^i) \}$
while $(i != n)$ {
  $\{ ((s = a^i) \wedge (\neg (i = n))) \}$
  $\{ (s * a = a^{i+1}) \}$
  $s = s * a;$
  $\{ (s = a^{i+1}) \}$
  $i = i + 1;$
  $\{ (s = a^i) \}$
}
$\{ ((s = a^i) \wedge (i = n)) \}$
$\{ s = a^n \}$