While Loops - Examples of finding invariants

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

\[ q(x \geq 0) \land y \land z \land x \]
\[ q(1=0!) \land 0! = 1 \land 0 \land 5 \]
\[ y = 1 \]
\[ ! = 1 \land 1 \land 5 \]
\[ q(y=0!) \land 2! = 2 \land 2 \land 5 \]
\[ z = 0 \]
\[ 3! = 6 \land 3 \land 5 \]
\[ q(y=z!) \land 4! = 24 \land 4 \land 5 \]

while \( z \neq x \) do
\[ q(y=z!) \land \neg (z=x) \]
\[ q(y*(z+1) = (z+1)! \]
\[ z = z + 1 \]
\[ A \text{ possible invariant: } y = z! \]
\[ q(y*z = z!) \]
\[ y = y * z \]
\[ q(y = z!) \land (z = x) \]
\[ q(y = x!) \]

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

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

Nov 21.
While Loops

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

\[ q(x \geq 0) \]

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

\[ y = 1; \]

\[ z = 0; \]

\[ q((y = z!) \land (z \leq x)) \]

while \((z \leq x)\) {

\[ q(((y = z!) \land (z \leq x)) \land (z < x)) \]

\[ z = z + 1; \]

\[ y = y * z; \]

\[ q((y = z!) \land (z \leq x)) \]

\[ y \]

\[ q(((y = z!) \land (z \leq x)) \land (z > x)) \]

\[ q(y = x!) \]
While Loops

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

\[
\begin{align*}
&\{ (n \geq 0) \land (a \geq 0) \} \quad S \quad i \quad n \quad a \\
&\{ \quad i = a^0 \} \quad \text{implies (a)} \quad 2^0 = 1 \quad 0 \quad 5 \quad 2 \\
&\{ S = 1 \} \quad 2^1 = 2 \quad 1 \quad 5 \quad 2 \\
&\{ S = a^0 \} \quad 2^2 = 4 \quad 2 \quad 5 \quad 2 \\
&\{ i = 0 \} \quad 2^3 = 8 \quad 3 \quad 5 \quad 2 \\
&\{ S = a^0 \} \quad 2^4 = 16 \quad 4 \quad 5 \quad 2 \\
\text{while} \ (i < n) \} \quad \uparrow \quad 2^5 = 32 \quad 5 \quad 5 \quad 2 \\
&\{ (S = a^2) \land (i < n) \} \\
&\{ S \times a = a^{i+1} \} \quad \text{implies: A possible invariant:} \\
&\quad S = S \times a \quad S = a^2 \\
&\{ S = a^{i+1} \} \\
&\quad i = i + 1 \quad \text{Does the invariant look similar to our post-condition? Yes.} \\
&\{ S = a^2 \} \\
&\quad S = a^2 \land i \geq n \quad \text{Does the invariant allow us to prove all the implied conditions? No.} \\
\end{align*}
\]

We cannot prove implied c unless \(i \leq n\). Luckily, \(i \leq n\) is an invariant also. So try this new invariant:

\[
(S = a^2) \land (i \leq n)
\]
While Loops

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

I changed the while test from 

\[ (\downarrow < n) \] to \[ (\downarrow \uparrow = n) \]. Now, the invariant \( S = a^x \) works for our proof.

\( S = 1 \); \\
\( a(S = a^0) \) D \\
\( \downarrow = 0 \); \\
\( a(S = a^0) \) D \\
\textbf{while} (\( \downarrow \uparrow = n \)) \{ \\
\( a(S = a^2) \wedge (\neg (\downarrow \uparrow = n)) \) D \\
\( a(S * a = a^{2+1}) \) D \\
\( S = S * a \); \\
\( a(S = a^{2+1}) \) D \\
\( \downarrow = \downarrow + 1 \); \\
\( a(S = a^2) \) D \\
\( a((S = a^2) \wedge (\downarrow \uparrow = n)) \) D \\
\( a(S = a^n) \) D \\
\( a(S = a^n) \) D \\
\( a(S = a^n) \) D