More Examples on Loop Invariants

1 Example 1

Consider the following pseudo-code:

\[
\begin{align*}
&x \leftarrow 2, y \leftarrow 0 \\
&\textbf{while } y < n \textbf{ do} \\
&\quad x \leftarrow x^3 \\
&\quad y \leftarrow y + 1 \\
&\textbf{end while}
\end{align*}
\]

Assuming that \(n\) is a non-negative integer, use a loop invariant to prove that \(x = 2^{3^n}\) when the loop terminates. First, find your pre-loop and post-loop states \(P\) and \(Q\). Then design and prove a loop invariant \(I\), which leads to the above conclusion. Recall to prove a loop invariant, one needs to show (1) \(P \rightarrow I\) (2) \((I \land C) \implies B(I)\) (3) \((I \land \neg C) \rightarrow Q\). (HINT: Remember that \(a^b \times a^c = a^{b+c}\).)

Solution: We will use \((x = 2^{3^n}) \land (0 \leq y \leq n)\) as the loop invariant \(I\). Then it is easy to see that \(P\) is \(x = 2, y = 0\) and \(Q\) is \(y = n, x = 2^{3^n}\). Let us prove the loop invariant \(I\).

- \(P \rightarrow I\). Initially, \(2^{3^0} = 2 = x\), so the invariant holds before the start of the loop.
- \((I \land C) \implies B(I)\). Let \(x'\) and \(y'\) be the new values of \(x\) and \(y\) at the end of the loop. In the loop, we have
  \[
  x' = x^3, \quad y' = y + 1.
  \]

  Then we have
  \[
  x' = x^3 = 2^{3^n} \cdot 2^{3^y} = 2^{3^n+3^y} = 2^{3^{y+1}} = 2^{3^{y'}}.
  \]

  Because the condition (C) \(y < n\) holds, then \(y' \leq n\). Thus, we have the loop invariant \((x' = 2^{3^{y'}}) \land (0 \leq y' \leq n)\) holds for the new value \(x'\) and \(y'\).
- \((I \land \neg C) \rightarrow Q\). When \(C\) does not hold, combined with \(I\), it implies \(y = n\). By the loop invariant \(I\), then we have \(x = 2^{3^n}\).

2 Example 2

Consider the following pseudo-code:

\[
\begin{align*}
&x \leftarrow 2, y \leftarrow 0 \\
&\textbf{while } y < n \textbf{ do} \\
&\quad y \leftarrow y + 1 \\
&\quad x \leftarrow x^y \\
&\textbf{end while}
\end{align*}
\]

Assuming that \(n\) is a non-negative integer, use a loop invariant to prove that \(x = 2^{n^y}\) when the loop terminates. First, find your pre-loop and post-loop states \(P\) and \(Q\). Then design and prove a loop invariant \(I\), which leads to the above conclusion. Recall to prove a loop invariant, one needs to show (1) \(P \rightarrow I\) (2) \((I \land C) \implies B(I)\) (3) \((I \land \neg C) \rightarrow Q\). (HINT: Remember that \(a^b \times a^c = a^{b+c}\).)
Solution: We will use \((x = 2^y) \land (0 \leq y \leq n)\) as the loop invariant \(I\). Then it is easy to see that \(P\) is \(x = 2, y = 0\) and \(Q\) is \(y = n, x = 2^n\). Let us prove the loop invariant \(I\).

- \(P \rightarrow I\). Initially, \(2^0 = 2^0 = 2 = x\), so the invariant holds before the start of the loop.

- \((I \land C)B(I)\). Let \(x'\) and \(y'\) be the new values of \(x\) and \(y\) at the end of the loop. In the loop, we have
  \[
  x' = x^y, \quad y' = y + 1.
  \]

  Then we have
  \[
  x' = x^y = (2^y)^{y+1} = 2^{y(y+1)} = 2^{(y+1)!} = 2^{y'!}.
  \]

  Because the condition (C) \(y < n\) holds, then \(y' \leq n\). Thus, we have the loop invariant \((x' = 2^{y'}) \land (0 \leq y' \leq n)\) holds for the new value \(x'\) and \(y'\).

- \((I \land \neg C) \rightarrow Q\). When \(C\) does not hold, combined with \(I\), it implies \(y = n\). By the loop invariant \(I\), then we have \(x = 2^n\).