Simplest-Possible Hoare Logic
While-Loop Example in JAPE

Program

\[
\begin{align*}
m &:= 0; \\
\text{while } m < n &\text{ do} \\
& \quad m := m + 1 \\
\text{od}
\end{align*}
\]

Program With Assertions

{\(n \geq 0\)} Assumption
\n
\[
m := 0; \\
\{m \leq n\} \quad \text{Loop Invariant}
\]

while \(m < n\) do
\[
\quad m := m + 1 \\
\text{od}
\]

\{\(m = n\}\} Expectation

What we enter

WHERE DISTINCT \(m, n\) IS \(\{n \geq 0\}\) \(\{m \geq 0\}\) \(\{m \leq n\}\) while \(m < n\) do \(m := m + 1\) od \(m = n\)

As it appears initially in JAPE

Use the Ntuple Rule

- Ntuple creates two separate triples: one for the initialization and one for the while loop.

\[
\begin{align*}
1: \{n \geq 0\}(m := 0)(m, n) &\text{while } m < n\text{ do } m := m + 1\text{ od } m = n \\
2: \{m \leq n\}(m := 0)(m, n) &\text{while } m < n\text{ do } m := m + 1\text{ od } m = n \text{ Ntuple 1, 2}
\end{align*}
\]
Proving the Initialization

Because the derived pre-condition is not identical to the assumption, a use of the consequence(L) rule is automatically introduced, along with a companion logical implication.

Resolve the gap using a Rule from the Comparison menu

Partial correctness of loop body

Use the assignment rule, with an implied consequence(L). This generates a logic implication for the consequence(L) rule.

The logic implication remains to be proved.

Proving the Implication

Click on the upper portion to prove the implication as a consequence (rather than using it as a hypothesis).

Now Expand the while

This generates several unfinished sub-proofs:

Partial correctness of loop body

Continuation condition for loop body

Termination condition for loop body

Exit consequence implication for loop

Proof of Upper Implication

Close using another Comparison rule on line 9.
Proof of Lower Implication

Use a Lemma we’ve introduced:

What Remains

• We need a variant that unifies with \( \text{\_M} \)
• The variant \( n-m \) should work.

Prove the Upper Implication

Apply another “obvious” lemma

Prove the while termination body

Another consequence(L) is introduced:

One more “obvious” lemma completes the proof.