Simplest-Possible Hoare Logic While-Loop Example in JAPE
Program

m := 0;
while m < n
do
  m := m + 1
od
Program With Assertions

{n ≥ 0}  
Assumption

m := 0;

{m ≤ n}  
Loop Invariant

while m < n
  do
    m := m + 1
  od

{m = n}  
Expectation
What we enter

WHERE DISTINCT m, n IS \{n \geq 0\} (m := 0) \{m \leq n\} while m < n do m := m+1 od \{m = n\}
As it appears initially in JAPE

\[\ldots\]

\[1: \{n \geq 0\}(m := 0\{m \leq n\)while m < n do m := m + 1 od\{m = n\}\]
Use the Ntuple Rule

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

```
... 
1: \{n \geq 0\}(m:=0){m \leq n}
... 
2: \{m \leq n\}while m < n do m:=m+1 od\{m=n\}
3: \{n \geq 0\}(m:=0){m \leq n}while m < n do m:=m+1 od\{m=n\} Ntuple 1,2
```
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.

...  
1: \( n \geq 0 \rightarrow 0 \leq n \)  
2: \( \{0 \leq n\}(m:=0)\{m \leq n\} \)  
3: \( \{n \geq 0\}(m:=0)\{m \leq n\} \)
Proving the Implication

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

```plaintext
1: \([n \geq 0 \rightarrow 0 \leq n]\)
2: \{0 \leq n\}(m := 0){m \leq n}\)
3: \{n \geq 0\}(m := 0){m \leq n}\)
```

variable-assignment
consequence(L) 1,2

```plaintext
4: \{m \leq n\} while m < n do m := m + 1 od{m = n}\)
5: \{n \geq 0\}(m := 0){m \leq n\} while m < n do m := m + 1 od{m = n}\) Ntuple 3,4
```
Resolve the gap using a Rule from the Comparison menu \[ A \leq B \iff B \geq A \]

1: \( n \geq 0 \)
2: \( 0 \leq n \)
3: \( n \geq 0 \rightarrow 0 \leq n \)
4: \( \{0 \leq n\}(m := 0)\{m \leq n\} \)
5: \( \{n \geq 0\}(m := 0)\{m \leq n\} \)

assumption
\( \rightarrow \) intro 1–2
variable-assignment
consequence(L) 3,4

1: \( n \geq 0 \)
2: \( 0 \leq n \)
3: \( n \geq 0 \rightarrow 0 \leq n \)
4: \( \{0 \leq n\}(m := 0)\{m \leq n\} \)
5: \( \{n \geq 0\}(m := 0)\{m \leq n\} \)

assumption
\( A \leq B \iff B \geq A \) 1
\( \rightarrow \) intro 1–2
variable-assignment
consequence(L) 3,4
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
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.
Proof of Upper Implication

6: \( m \leq n \land m < n \)  
7: \( m \leq n \)  
8: \( m < n \)  
9: \( m + 1 \leq n \)

Close using another Comparison rule on line 9.

\[ A + 1 \leq B \Leftrightarrow A < B \]

6: \( m \leq n \land m < n \)  
7: \( m < n \)  
8: \( m + 1 \leq n \)  

assumption  
\land\ elim 6  
\land\ elim 6  
A + 1 \leq B \Leftrightarrow A < B  
7
Proof of Lower Implication

Use a Lemma we’ve introduced:

15: \( m \leq n \land \neg (m < n) \rightarrow m = n \)
What Remains

- We need a variant that unifies with \( _M \)
- The variant \( n-m \) should work.
Prove the Upper Implication

...  
12: \( m \leq n \land m < n \rightarrow n - m > 0 \)

Apply another “obvious” lemma

12: \( m \leq n \land m < n \)  
13: \( m < n \)  
14: \( n - m > 0 \)  
15: \( m \leq n \land m < n \rightarrow n - m > 0 \)
Prove the while termination body

Another consequence (L) is introduced:

```
16: integer Km
...
17: \{m \leq n \land m < n \land n - m = Km\}(m := m + 1){n - m < Km}
```

```
16: integer Km
...
17: m \leq n \land m < n \land n - m = Km \rightarrow n - (m + 1) < Km
18: \{n - (m + 1) < Km\}(m := m + 1){n - m < Km}
19: \{m \leq n \land m < n \land n - m = Km\}(m := m + 1){n - m < Km}
```
One more “obvious” lemma completes the proof.
\begin{align*}
1: & \quad n \geq 0 \\
2: & \quad 0 \leq n \\
3: & \quad n \geq 0 \rightarrow 0 \leq n \\
4: & \quad \{0 \leq n\}(m := 0)\{m \leq n\} \\
5: & \quad \{n \geq 0\}(m := 0)\{m \leq n\} \\
6: & \quad m \leq n \land m < n \\
7: & \quad m < n \\
8: & \quad m + 1 \leq n \\
9: & \quad m \leq n \land m < n \rightarrow m + 1 \leq n \\
10: & \quad \{m + 1 \leq n\}(m := m + 1)\{m \leq n\} \\
11: & \quad \{m \leq n \land m < n\}(m := m + 1)\{m \leq n\} \\
12: & \quad m \leq n \land m < n \\
13: & \quad m < n \\
14: & \quad n - m > 0 \\
15: & \quad m \leq n \land m < n \rightarrow n - m > 0 \\
16: & \quad \text{integer } K_m \\
17: & \quad m \leq n \land m < n \land n - m = K_m \\
18: & \quad n - m = K_m \\
19: & \quad n - (m + 1) < K_m \\
20: & \quad m \leq n \land m < n \land n - m = K_m \rightarrow n - (m + 1) < K_m \\
21: & \quad \{n - (m + 1) < K_m\}(m := m + 1)\{n - m < K_m\} \\
22: & \quad \{m \leq n \land m < n \land n - m = K_m\}(m := m + 1)\{n - m < K_m\}
\end{align*}

assumption
A \leq B \equiv B \geq A \quad 1
\rightarrow \quad \text{intro } 1-2
variable-assignment
\rightarrow \quad \text{consequence(L) } 3, 4
assumption
\land \quad \text{elim } 6
A - 1 \leq B \equiv A < B \quad 7
\rightarrow \quad \text{intro } 6-8
variable-assignment
\rightarrow \quad \text{consequence(L) } 9, 10
assumption
\land \quad \text{elim } 12
m < n \leftarrow n - m > 0 \quad 13
\rightarrow \quad \text{intro } 12-14
assumption
assumption
\land \quad \text{elim } 17
n - m = X \leftarrow n - (m + 1) < X \quad 18
\rightarrow \quad \text{intro } 17-19
variable-assignment
\rightarrow \quad \text{consequence(L) } 20, 21

Provided:
DISTINCT m, n