

DEDUCTIVE VERIFICATION (EXAMPLE)

Construct an invariant and prove partial correctness of the deterministic program with given pre- and post-conditions.

```
{N ≥ 1}
BEGIN
  PROD := 0;
  FOR X := 1 UNTIL N DO PROD := PROD + M
END
{PROD = M*N}
```

Solution

STEP 1: Annotation

For annotating the program we have to add

- pre-condition before each command that is not assignment, i.e. we add condition **P1** (see below).
- Invariant in the loop after keyword "DO", i.e., **R** (see below)
- To avoid long expressions in the beginning of proof we denote the whole program with **C** and its commands with **C1** and **C2**, i.e. the program **C** can be considered in symbolic form as parallel composition **C1 ; C2**

```
P ≡ {N ≥ 1}
BEGIN
  C1: PROD := 0;           ← P1 ≡ {N ≥ 1 ∧ PROD = 0}
  C2: FOR X := 1 UNTIL N DO ← R ≡ {PROD = M * (X-1) ∧ X ≤ N+1}
    C21: PROD := PROD + M
  END
Q ≡ {PROD = M*N}
```

STEP 2: Proof

$$\begin{array}{c}
\begin{array}{c} \text{====} \\ \vdash N \geq 1 \Rightarrow N \geq 1 \\ \text{====} \end{array} \quad (A \Rightarrow A) \\
\begin{array}{c} \text{====} \\ \vdash N \geq 1 \Rightarrow (N \geq 1 \wedge 0 = 0) \\ \text{====} \end{array} \quad (A \wedge \text{true} \Rightarrow A) \\
\begin{array}{c} \text{====} \\ \vdash N \geq 1 \Rightarrow (N \geq 1 \wedge \text{PROD} = 0) [0/ \text{PROD}] \\ \text{====} \end{array} \quad (\text{Substit } [0/\text{PROD}]) \\
\begin{array}{c} \text{====} \\ \vdash P \Rightarrow P1 [0/ \text{PROD}] \\ \text{====} \end{array} \quad (\text{P and P1 Substit}) \quad \begin{array}{c} \text{====} \\ \vdash \text{VC1} \quad \vdash \text{VC2} \quad \vdash \text{VC3} \quad \vdash \text{VC4} \\ \text{====} \end{array} \quad (\text{See proofs of verification conditions V1-V4 below}) \\
\begin{array}{c} \text{====} \\ \vdash \{P\} \text{PROD} := 0 \{P1\} \\ \text{====} \end{array} \quad (\text{Asgn}) \\
\begin{array}{c} \text{====} \\ \vdash \{P\} C1 \{P1\} \\ \text{====} \end{array} \quad (\text{Term C1 substit}) \\
\begin{array}{c} \text{====} \\ \vdash \{P1\} \text{FOR } X := 1 \text{ UNTIL } N \text{ DO } C21 \{Q\} \\ \text{====} \end{array} \quad (\text{FOR}) \\
\begin{array}{c} \text{====} \\ \vdash \{P1\} C2 \{Q\} \\ \text{====} \end{array} \quad (\text{Term C2 substit}) \\
\begin{array}{c} \text{====} \\ \vdash \{P\} C1 ; C2 \{Q\} \\ \text{====} \end{array} \quad (\text{Seq}) \\
\begin{array}{c} \text{====} \\ \vdash \{P\} C \{Q\} \\ \text{====} \end{array} \quad (\text{Term C substitution})
\end{array}$$

1) $\vdash \text{VC1}$

$$\begin{array}{c}
\text{====} \quad (\text{Arithm}) \quad \text{====} \quad (A \Rightarrow A) \\
\begin{array}{c} \text{====} \\ \vdash N \geq 1 \Rightarrow 0 \leq N \\ \text{====} \end{array} \quad \begin{array}{c} \text{====} \\ \vdash \text{PROD} = 0 \Rightarrow \text{PROD} = 0 \\ \text{====} \end{array} \\
\begin{array}{c} \text{====} \\ \vdash N \geq 1 \wedge \text{PROD} = 0 \Rightarrow \text{PROD} = 0 \wedge 0 \leq N \\ \text{====} \end{array} \quad (\Rightarrow \wedge \text{ and } \wedge \Rightarrow) \\
\begin{array}{c} \text{====} \\ \vdash N \geq 1 \wedge \text{PROD} = 0 \Rightarrow \text{PROD} = M * (1-1) \wedge 1 \leq N+1 \\ \text{====} \end{array} \quad (\text{Arithm}) \\
\begin{array}{c} \text{====} \\ \vdash P1 \Rightarrow R[1/X] \\ \text{====} \end{array} \quad (\text{Term R and value } [1/X] \text{ substit}) \\
\begin{array}{c} \text{====} \\ \vdash \text{VC1} \\ \text{====} \end{array} \quad (\text{Term VC1 substit})
\end{array}$$

2) $\vdash \text{VC2}$

$$\begin{array}{c}
\text{====} \quad (A \Rightarrow A) \\
\begin{array}{c} \text{====} \\ \vdash \text{PROD} = M * N \Rightarrow \text{PROD} = M * N \\ \text{====} \end{array} \quad (\text{Term Q substit}) \\
\begin{array}{c} \text{====} \\ \vdash \text{PROD} = M * N \Rightarrow Q \\ \text{====} \end{array} \quad (A \wedge \text{true} \Rightarrow A) \\
\begin{array}{c} \text{====} \\ \vdash (\text{PROD} = M * (N+1-1) \wedge N+1 \leq N+1) \Rightarrow Q \\ \text{====} \end{array} \quad (\text{Substitution } [N+1/X]) \\
\begin{array}{c} \text{====} \\ \vdash (\text{PROD} = M * (X-1) \wedge X \leq N+1) [N+1/X] \Rightarrow Q \\ \text{====} \end{array} \quad (\text{Term R substit}) \\
\begin{array}{c} \text{====} \\ \vdash R[N+1/X] \Rightarrow Q \\ \text{====} \end{array} \quad (\text{Term VC2 substit}) \\
\begin{array}{c} \text{====} \\ \vdash \text{VC2} \\ \text{====} \end{array}
\end{array}$$

3) $\vdash \text{VC3}$

$$\begin{array}{c}
\text{====} \quad (\text{Definition of } \Rightarrow) \\
\begin{array}{c} \text{====} \\ \vdash \text{false} \Rightarrow Q \\ \text{====} \end{array} \quad (\text{Definition of } \Rightarrow) \\
\begin{array}{c} \text{====} \\ \vdash N \geq 1 \wedge \text{PROD} = 0 \wedge N < 1 \Rightarrow \text{false} \\ \text{====} \end{array} \quad (N \geq 1 \wedge N < 1 \Rightarrow \text{false}) \\
\begin{array}{c} \text{====} \\ \vdash P1 \wedge (N < 1) \Rightarrow Q \\ \text{====} \end{array} \quad (\text{Term P1 substit}) \\
\begin{array}{c} \text{====} \\ \vdash \text{VC3} \\ \text{====} \end{array} \quad (\text{Term VC3 substit})
\end{array}$$

4) $\vdash \text{VC4}$

$$\begin{array}{c}
\text{====} \quad (A \Rightarrow A) \\
\begin{array}{c} \text{====} \\ \vdash \text{PROD} = M * (X-1) \Rightarrow \text{PROD} = M * (X-1) \\ \text{====} \end{array} \quad (\text{Arithm}) \\
\begin{array}{c} \text{====} \\ \vdash \text{PROD} = M * (X-1) \Rightarrow \text{PROD} + M = M * X \\ \text{====} \end{array} \quad (\text{Subs R}) \quad \begin{array}{c} \text{====} \\ \vdash X \leq N \Rightarrow X \leq N \\ \text{====} \end{array} \quad (A \Rightarrow A) \\
\begin{array}{c} \text{====} \\ \vdash R \Rightarrow \text{PROD} + M = M * X \\ \text{====} \end{array} \quad \begin{array}{c} \text{====} \\ \vdash X \leq N \Rightarrow X \leq N \\ \text{====} \end{array} \quad (\Rightarrow \wedge \text{ and } \wedge \Rightarrow) \\
\begin{array}{c} \text{====} \\ \vdash R \wedge 1 \leq X \wedge X \leq N \Rightarrow \text{PROD} + M = M * X \wedge X \leq N \\ \text{====} \end{array} \\
\begin{array}{c} \text{====} \\ \vdash R \wedge 1 \leq X \wedge X \leq N \Rightarrow \text{PROD} = M * X \wedge X \leq N [\text{PROD} + M / \text{PROD}] \\ \text{====} \end{array} \quad ((\text{PROD} + M / \text{PROD}) \text{substit}) \\
\begin{array}{c} \text{====} \\ \vdash \{R \wedge 1 \leq X \wedge X \leq N\} C21 \{ \text{PROD} = M * X \wedge X \leq N \} \\ \text{====} \end{array} \quad (\text{Asgn}) \\
\begin{array}{c} \text{====} \\ \vdash \{R \wedge 1 \leq X \wedge X \leq N\} C21 \{ \text{PROD} = M * (X+1-1) \wedge X+1 \leq N+1 \} \\ \text{====} \end{array} \quad (\text{Arithm simplification}) \\
\begin{array}{c} \text{====} \\ \vdash \{R \wedge 1 \leq X \wedge X \leq N\} C21 \{ \text{PROD} = M * (X+1-1) \wedge X+1 \leq N+1 \} \\ \text{====} \end{array} \quad ([X+1/X] \text{ substit}) \\
\begin{array}{c} \text{====} \\ \vdash \{R \wedge 1 \leq X \wedge X \leq N\} C21 \{ \text{PROD} = M * (X-1) \wedge X \leq N+1 [X+1/X] \} \\ \text{====} \end{array} \quad (\text{Term R substit in post-cond}) \\
\begin{array}{c} \text{====} \\ \vdash \{R \wedge 1 \leq X \wedge X \leq N\} C21 \{R[X+1/X]\} \\ \text{====} \end{array} \quad (\text{Term VC4 substit}) \\
\begin{array}{c} \text{====} \\ \vdash \text{VC4} \\ \text{====} \end{array}
\end{array}$$