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}
```

<u>Solution</u>

<u>STEP 1:</u> <u>Annotation</u>

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

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

1) $\vdash$ VC1

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

2) $\vdash$ VC2

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

3) $\vdash$ VC3

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \text{false} \Rightarrow Q}\,(\text{Definition of} \Rightarrow)}{\vdash N \geq 1 \wedge PROD = 0 \wedge N<1 \Rightarrow Q}\,(N \geq 1 \wedge N<1 \Rightarrow \text{false})\ )}{\vdash P1 \wedge (N<1) \Rightarrow Q}\,(\text{Term P1 substit})}{\vdash VC3}\,(\text{Term VC3 substit})$$

4) $\vdash$ VC4

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