

**Introduction and Vocabulary**
- Test case, test suite, test execution.
- Positive and negative outcomes.

**Limits of Software Testing**
- **Glass-Box Testing**
  - Statement-, branch-, term-coverage.

**Testing: Rest**
- When to stop testing?
- Model-based testing
- Testing in the development process

**Program Verification**
- Partial and total correctness,
- Proof System PD.

**Other Approaches**
- Runtime verification.
- Review

**Software quality assurance wrap-up**
Content

- Formal Program Verification
  - Proof System PD

- The Verifier for Concurrent C
  - Assertions, Modular Verification, VCC

- Runtime-Verification
  - Assertions, LSC-Observers

- Reviews
  - Roles and artefacts
  - Review procedure
  - Stronger and weaker variants

- Code QA Techniques Revisited
  - Test, Runtime-Verification, Review,
  - Static Checking, Formal Verification

- Do’s and Don’ts in Code QA

- Dependability
Recall: Deterministic Programs, Correctness

**Deterministic Programs**

**Syntax:**

\[ S := \text{skip} \mid u := t \mid S_1; S_2 \mid \text{if } B \text{ then } S_1 \text{ else } S_2 \mid \text{while } B \text{ do } S_1 \text{ od} \]

where \( u \in V \) is a variable, \( t \) is a type-compatible expression, \( B \) is a Boolean expression.

**Semantics:** (is induced by the following transition relation) \( \Vdash : V \to D(V) \)

(i) \( \Vdash (\text{skip}, \sigma) \rightarrow (E, \sigma) \)

(ii) \( \Vdash (u := t, \sigma) \rightarrow (E, \sigma[u := t]) \)

(iii) \( \Vdash (S_1; S_2, \sigma) \rightarrow (S_2, \sigma) \)

(iv) \( S \) is an empty program; define \( E, S \equiv S \).

**Note:** the first component of \( (S, \sigma) \) is a program (structural operational semantics (SOS)).

**Example**

Consider program

\[ S \equiv a[0] := 1; a[1] := 0; \text{while } a[x] \neq 0 \text{ do } x := x + 1 \text{ od} \]

and a state \( \sigma \) with \( x = 0 \).

\begin{align*}
(S, \sigma) \xrightarrow{(vii),(vi)} (a[1] := 0; \text{while } a[x] \neq 0 \text{ do } x := x + 1 \text{ od}, \sigma') \\
(S, \sigma) \xrightarrow{(vi),(v)} (a[1] := 0; \text{while } a[x] \neq 0 \text{ do } x := x + 1 \text{ od}, \sigma') \\
(S, \sigma) \xrightarrow{(v),(i)} (a[1] := 0; \text{while } a[x] \neq 0 \text{ do } x := x + 1 \text{ od}, \sigma') \\
(S, \sigma) \xrightarrow{(i)} (a[1] := 0; \text{while } a[x] \neq 0 \text{ do } x := x + 1 \text{ od}, \sigma') \\
(S, \sigma) \xrightarrow{(i)} (a[1] := 0; \text{while } a[x] \neq 0 \text{ do } x := x + 1 \text{ od}, \sigma') \\
\end{align*}

where \( \sigma' = \sigma[a[0] := 1][a[1] := 0]. \)

---

**Input/Output Semantics of Deterministic Programs**

**Definition.** Let \( S \) be a deterministic program.

(i) The **semantics of partial correctness** is the function

\[ \mathcal{M}[S] : \Sigma \to 2^\Sigma \]

with \( \mathcal{M}[S](\sigma) = \{ \tau \mid (S, \sigma) \xrightarrow{} (E, \tau) \} \).

(ii) The **semantics of total correctness** is the function

\[ \mathcal{M}_{\text{tot}}[S] : \Sigma \to 2^\Sigma \cup \{\infty\} \]

with \( \mathcal{M}_{\text{tot}}[S](\sigma) = \mathcal{M}[S](\sigma) \cup \{\infty \mid S \text{ can diverge from } \sigma\}. \)

\( \infty \) is an error state representing divergence.

**Note:** \( \mathcal{M}_{\text{tot}}[S](\sigma) \) has exactly one element, \( \mathcal{M}[S](\sigma) \) at most one.

**Example:** \( \mathcal{M}[S](\sigma) = \mathcal{M}_{\text{tot}}[S](\sigma) = \{ \tau \mid \tau(x) = \sigma(x) \land \tau(y) = \sigma(x)^2 \}, \ \sigma \in \Sigma \).

(Recall: \( S \equiv y := x; y := (x - 1) \cdot x + y \))

---

**Correctness of Deterministic Programs**

**Definition.** Let \( S \) be a program over variables \( V \), and \( p \) and \( q \) be Boolean expressions over \( V \).

(i) The **correctness formula**

\[ (p \ S \ q) \]

holds in the sense of partial correctness, denoted by \( \models \ S \), if and only if

\[ \mathcal{M}[S](\sigma) \subseteq \{ q \} \]

We say \( S \) is **partially correct** wrt. \( p \) and \( q \).

(ii) A correctness formula

\[ (p \ S \ q) \]

holds in the sense of total correctness, denoted by \( \models_{\text{tot}} (p \ S \ q) \), if and only if

\[ \mathcal{M}_{\text{tot}}[S](\sigma) \subseteq \{ q \} \]

We say \( S \) is **totally correct** wrt. \( p \) and \( q \).
Proof-System PD
Proof-System PD (for sequential, deterministic programs)

Axiom 1: Skip-Statement

\[ \{ p \} \text{skip} \{ p \} \]

Axiom 2: Assignment

\[ \{ p[u := t] \} \ u := t \{ p \} \]

Rule 3: Sequential Composition

\[ \{ p \} S_1 \{ r \}, \{ r \} S_2 \{ q \} \]
\[ \{ p \} S_1; S_2 \{ q \} \]

Rule 4: Conditional Statement

\[ \{ p \wedge B \} S_1 \{ q \}, \{ p \wedge \neg B \} S_2 \{ q \}, \]
\[ \{ p \} \text{if} \ B \text{then} \ S_1 \text{else} \ S_2 \text{fi} \{ q \} \]

Rule 5: While-Loop

\[ \{ p \wedge B \} S \{ p \} \]
\[ \{ p \} \text{while} \ B \text{do} \ S \text{od} \{ p \wedge \neg B \} \]

Rule 6: Consequence

\[ p \rightarrow p_1, \{ p_1 \} S \{ q_1 \}, q_1 \rightarrow q \]
\[ \{ p \} S \{ q \} \]

Theorem. PD is correct ("sound") and (relative) complete for partial correctness of deterministic programs, i.e. \( \vdash_{PD} \{ p \} S \{ q \} \) if and only if \( \models \{ p \} S \{ q \} \).
Example Proof

\[ \text{DIV} \equiv a := 0; \ b := x; \ \text{while} \ b \geq y \ \text{do} \ b := b - y; \ a := a + 1 \ \text{od} \]

(The first (textually represented) program that has been formally verified (?)�

We can prove \( \models \{ x \geq 0 \land y \geq 0 \} \text{DIV} \{ a \cdot y + b = x \land b < y \}\)

by showing \( \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} \text{DIV} \{ a \cdot y + b = x \land b < y \}, \) i.e., derivability in PD:

\[ \begin{align*}
(1) & \quad P \rightarrow P, \\
(2) & \quad \{ P \} \text{ while } B^D \text{ do } S^D_1 \text{ od } \{ P \} \\
(3) & \quad \{ P \} \text{ while } B^D \text{ do } S^D_1 \text{ od } \{ q^D \} \\
\end{align*} \]

\[ \begin{align*}
(1) & \quad \{ p^D \} S^D_0 \{ P \}, \\
(2) & \quad \{ P \} \text{ while } B^D \text{ do } S^D_1 \text{ od } \{ P \} \\
(3) & \quad \{ P \} \text{ while } B^D \text{ do } S^D_1 \text{ od } \{ q^D \} \\
\end{align*} \]
In the following, we show

(1) \( \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} a := 0; b := x \{ P \}, \)

(2) \( \vdash_{PD} \{ P \land b \geq y \} b := b - y; a := a + 1 \{ P \}, \)

(3) \( \models P \land \neg (b \geq y) \rightarrow a \cdot y + b = x \land b < y. \)

As loop invariant, we choose (creative act!):

\[ P \equiv a \cdot y + b = x \land b \geq 0 \]
Proof of (1)

- (1) claims:
  \[ \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} \ a := 0; \ b := x \ \{ P \} \]
  where \( P \equiv a \cdot y + b = x \land b \geq 0 \).

- \[ \vdash_{PD} \{ 0 \cdot y + x = x \land x \geq 0 \} \ a := 0 \ {\{ a \cdot y + x = x \land x \geq 0 \} \text{ by (A2)},} \]

\[
\begin{align*}
\text{(A1) } \{ p \} \ & \text{skip } \{ p \} \\
\text{(R4) } \{ p \land B \} \ & S_1 \{ q \}, \ \{ p \land \neg B \} \ & S_2 \{ q \} \\
\text{(A2) } \{ p[u := t] \} \ u := t \ \{ p \} \\
\text{(R5) } \{ p \land B \} \ & S \{ p \} \\
\text{(R3) } \{ p \} \ S_1 \{ r \}, \ \{ r \} \ S_2 \{ q \} \\
\text{(R6) } \{ p \} \ S \{ q \} \\
\end{align*}
\]
Proof of (1)

- (1) claims:
  \[ \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} \ a := 0; \ b := x \ {P} \]
  where \( P \equiv a \cdot y + b = x \land b \geq 0 \).

- \[ \vdash_{PD} \{ 0 \cdot y + x = x \land x \geq 0 \} \ a := 0 \ a \cdot y + x = x \land x \geq 0 \]
  by (A2),

- \[ \vdash_{PD} \{ a \cdot y + x = x \land x \geq 0 \} \ b := x \ a \cdot y + b = x \land b \geq 0 \]
  by (A2),

- \[ \vdash_{PD} \{ a \cdot y + x = x \land x \geq 0 \} \ b := x \ a \cdot y + b = x \land b \geq 0 \]
  \[ \equiv P \]
Proof of (1)

• (1) claims:
  \[ \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} \; a := 0; \; b := x \; \{ P \} \]
  where \( P \equiv a \cdot y + b = x \land b \geq 0 \).

• \[ \vdash_{PD} \{ 0 \cdot y + x = x \land x \geq 0 \} \; a := 0 \; \{ a \cdot y + x = x \land x \geq 0 \} \quad \text{by (A2),} \]

• \[ \vdash_{PD} \{ a \cdot y + x = x \land x \geq 0 \} \; b := x \; \{ a \cdot y + b = x \land b \geq 0 \} \quad \text{by (A2),} \]

• thus, \[ \vdash_{PD} \{ 0 \cdot y + x = x \land x \geq 0 \} \; a := 0; \; b := x \; \{ P \} \quad \text{by (R3),} \]

\[ \begin{array}{ll}
(A1) \{ p \} \; \text{skip} \; \{ p \} & (R4) \{ p \land B \} \; S_1 \; \{ q \}, \; \{ p \land \neg B \} \; S_2 \; \{ q \} \\
\{ p \} \; \text{if} \; B \; \text{then} \; S_1 \; \text{else} \; S_2 \; \text{fi} \; \{ q \} & \\
(A2) \{ p[u := t] \} \; u := t \; \{ p \} & (R5) \{ p \land B \} \; S \; \{ p \} \\
\{ p \} \; \text{while} \; B \; \text{do} \; S \; \text{od} \; \{ p \land \neg B \} & \\
(R3) \{ p \} \; S_1 \; \{ r \}, \; \{ r \} \; S_2 \; \{ q \} & (R6) \{ p \to p_1, \; \{ p_1 \} \; S \; \{ q_1 \}, \; q_1 \to q \} \\
\{ p \} \; S \; \{ q \} \\ 
\end{array} \]
Proof of (1)

• (1) claims:

\[ \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} a := 0; b := x \{ P \} \]

where \( P \equiv a \cdot y + b = x \land b \geq 0. \)

\[ \vdash_{PD} \{ 0 \cdot y + x = x \land x \geq 0 \} a := 0 \{ a \cdot y + x = x \land x \geq 0 \} \]

by (A2),

\[ \vdash_{PD} \{ a \cdot y + x = x \land x \geq 0 \} b := x \{ a \cdot y + b = x \land b \geq 0 \} \]

by (A2),

\[ \equiv P \]

thus, \( \vdash_{PD} \{ 0 \cdot y + x = x \land x \geq 0 \} a := 0; b := x \{ P \} \)

by (R3),

using \( x \geq 0 \land y \geq 0 \rightarrow 0 \cdot y + x = x \land x \geq 0 \) and \( P \rightarrow P \), we obtain

\[ \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} a := 0; b := x \{ P \} \]

by (R6).
The rule ‘Assignment’ uses (syntactical) substitution: \( \{ p[u := t] \} \ u := t \ \{ p \} \)
(In formula \( p \), replace all (free) occurrences of (program or logical) variable \( u \) by term \( t \).)

Defined as usual, only indexed and bound variables need to be treated specially:

\[
\begin{align*}
\alpha \triangleright x \ [ \ x := u + 3 \ ] & \quad \rightarrow \quad \alpha \triangleright u + 3 \\
\alpha \triangleright x & \land \forall x \cdot b \triangleright x \ [ \ x := u + 3 \ ] \quad \rightarrow \quad \alpha \triangleright u + 3 \land \forall x \cdot b \triangleright x \\
\underbrace{c \triangleright x} \geq 0 & \ [ \ \underbrace{c[0] := 2 +} \ ] \quad \rightarrow \quad ( x = 0 \ ? \ 2 + \ : \ c[\underbrace{x}])
\end{align*}
\]
Substitution

The rule ‘Assignment’ uses (syntactical) substitution: \( \{ p[u := t] \} u := t \{ p \} \)
(In formula \( p \), replace all (free) occurrences of (program or logical) variable \( u \) by term \( t \).)

Defined as usual, only indexed and bound variables need to be treated specially:

**Expressions:**
- plain variable \( x \): \( x[u := t] \equiv \begin{cases} t & \text{if } x = u \\ x & \text{otherwise} \end{cases} \)
- constant \( c \):
  \( c[u := t] \equiv c \).
- constant \( op \), terms \( s_i \):
  \( op(s_1, \ldots, s_n)[u := t] \equiv op(s_1[u := t], \ldots, s_n[u := t]). \)
- conditional expression:
  \( (B ? s_1 : s_2)[u := t] \equiv (B[u := t] ? s_1[u := t] : s_2[u := t]) \)
- indexed variable, \( u \) plain or \( u \equiv b[t_1, \ldots, t_m] \) and \( a \neq b \):
  \( (a[s_1, \ldots, s_n])[u := t] \equiv a[s_1[u := t], \ldots, s_n[u := t]] \)
- indexed variable, \( u \equiv a[t_1, \ldots, t_m] \):
  \( (a[s_1, \ldots, s_n])[u := t] \equiv (\bigwedge_{i=1}^n s_i[u := t] = t_i \? t : a[s_1[u := t], \ldots, s_n[u := t]]) \)

**Formulae:**
- boolean expression \( p \equiv s \):
  \( p[u := t] \equiv s[u := t] \)
- negation:
  \( (\neg q)[u := t] \equiv \neg(q[u := t]) \)
- conjunction etc.:
  \( (q \land r)[u := t] \equiv q[u := t] \land r[u := t] \)
- quantifier:
  \( (\forall x : q)[u := t] \equiv (\forall y : q[x := y][u := t]) \)
y fresh (not in \( q, t, u \), same type as \( x \).)
Example Proof Cont’d

\[ x \geq 0 \land y \geq 0 \] \[ a := 0; \ b := x \{P\}, \]

\[ \{P \land (b \geq y)\} \ b := b - y; \ a := a + 1 \{P\} \]

\[ P \rightarrow P, \ {P} \quad \text{while } b \geq y \text{ do } b := b - y; \ a := a + 1 \text{ od } \{P \land (b \geq y)\}, \]

\[ P \land (b \geq y) \rightarrow a \cdot y + b = x \land b < y \]

In the following, we show

\[ (1) \vdash_{PD} \{x \geq 0 \land y \geq 0\} \ a := 0; \ b := x \{P\}, \]

\[ (2) \vdash_{PD} \{P \land b \geq y\} \ b := b - y; \ a := a + 1 \{P\}, \]

\[ (3) P \land \neg (b \geq y) \rightarrow a \cdot y + b = x \land b < y. \]

As loop invariant, we choose (creative act!):

\[ P = a \cdot y + b = x \land b \geq 0 \]
Proof of (2)

- (2) claims:

\[ \vdash_{PD} \{ P \land b \geq y \} \quad b := b - y; \quad a := a + 1 \{ P \} \]

where \( P \equiv a \cdot y + b = x \land b \geq 0. \)

- \( \vdash_{PD} \quad (a + 1) \cdot y + (b - y) = x \land (b - y) \geq 0 \)

\( b := b - y \quad (a + 1) \cdot y + b = x \land b \geq 0 \)

by (A2).

- \( \vdash_{PD} \quad (a + 1) \cdot y + b = x \land b \geq 0 \quad a := a + 1 \quad a \cdot y + b = x \land b \geq 0 \)

\[ \equiv P \]

by (A2).

- \( \vdash_{PD} \quad (a + 1) \cdot y + (b - y) = x \land (b - y) \geq 0 \)

\( b := b - y; \quad a := a + 1 \{ P \} \)

by (R3).
Proof of (2)

(2) claims:
\[\vdash_{PD} \{ P \land b \geq y \} \ \text{b := } b - y; \ \text{a := a + 1 } \{ P \} \]
where \( P \equiv a \cdot y + b = x \land b \geq 0 \).

\[\vdash_{PD} \{(a + 1) \cdot y + (b - y) = x \land (b - y) \geq 0 \} \ \text{b := b - y } \{(a + 1) \cdot y + b = x \land b \geq 0 \} \]
by (A2).

\[\vdash_{PD} \{(a + 1) \cdot y + b = x \land b \geq 0 \} \ \text{a := a + 1 } \{ a \cdot y + b = x \land b \geq 0 \} \]
by (A2), \( \equiv P \).

\[\vdash_{PD} \{(a + 1) \cdot y + (b - y) = x \land (b - y) \geq 0 \} \ \text{b := b - y; a := a + 1 } \{ P \} \]
by (R3),

using \( P \land b \geq y \rightarrow (a + 1) \cdot y + (b - y) = x \land (b - y) \geq 0 \) and \( P \rightarrow P \) we obtain,

\[\vdash_{PD} \{ P \land b \geq y \} \ \text{b := b - y; a := a + 1 } \{ P \} \]
by (R6).
Example Proof Cont’d

In the following, we show

(1) \( \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} ; a := 0; b := x \{ P \}, \checkmark \)

(2) \( \vdash_{PD} \{ P \land b \geq y \} ; a := a + 1; b := b - y \{ P \} \)

(3) \( \models P \land \neg(b \geq y) \rightarrow a \cdot y + b = x \land b < y. \)

As loop invariant, we choose (creative act!):

\[ P \equiv a \cdot y + b = x \land b \geq 0 \]
Proof of (3)

(3) claims

\[ P \land \neg (b \geq y) \rightarrow a \cdot y + b = x \land b < y. \]

where \( P \equiv a \cdot y + b = x \land b \geq 0. \)

Proof: easy.
We have shown:

(1) \( \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} a := 0; b := x \{ P \} \).

(2) \( \vdash_{PD} \{ P \land b \geq y \} b := b - y; a := a + 1 \{ P \} \).

(3) \( \models P \land \neg (b \geq y) \rightarrow a \cdot y + b = x \land b < y \).

and

\[
\begin{array}{c}
\{ x \geq 0 \land y \geq 0 \} a := 0; b := x \{ P \}, \\
\hline
\mid \hline
\{ P \} \text{ while } b \geq y \text{ do } b := b - y; a := a + 1 \od \{ P \land \neg (b \geq y) \}, \\
\hline
\{ P \} \text{ while } b \geq y \text{ do } b := b - y; a := a + 1 \od \{ a \cdot y + b = x \land b < y \}, \\
\hline
\{ x \geq 0 \land y \geq 0 \} a := 0; b := x; \text{ while } b \geq y \text{ do } b := b - y; a := a + 1 \od \{ a \cdot y + b = x \land b < y \}, \\
\hline
\end{array}
\]

thus

(1) \( \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} a := 0; b := x \{ P \} \).

(2) \( \vdash_{PD} \{ P \} \text{ while } b \geq y \text{ do } b := b - y; a := a + 1 \od \{ P \land \neg (b \geq y) \}, \\
\hline
\{ P \land (b \geq y) \} b := b - y; a := a + 1 \{ P \}, \\
\hline
\{ P \land \neg (b \geq y) \rightarrow a \cdot y + b = x \land b < y \}, \\
\hline
\end{array}
\]

(1) \( \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} a := 0; b := x \{ P \} \).

Thus

\( \vdash_{PD} \{ x \geq 0 \land y \geq 0 \} a := 0; b := x; \text{ while } b \geq y \text{ do } b := b - y; a := a + 1 \od \{ a \cdot y + b = x \land b < y \} \equiv DIV \)

and thus (since PD is sound) \( DIV \) is **partially correct** wrt.

- **pre-condition**: \( x \geq 0 \land y \geq 0 \),
- **post-condition**: \( a \cdot y + b = x \land b < y \).

IOW: whenever \( DIV \) is called with \( x \) and \( y \) such that \( x \geq 0 \land y \geq 0 \), then (if \( DIV \) terminates) \( a \cdot y + b = x \land b < y \) will hold.
Once Again

- $P \equiv a \cdot y + b = x \land b \geq 0$

  \[
  \begin{align*}
  \{x \geq 0 \land y \geq 0\} \\
  \{0 \cdot y + x = x \land x \geq 0\}
  \end{align*}
  \]

- $a := 0$;
  \[
  \begin{align*}
  \{a \cdot y + x = x \land x \geq 0\} \\
  \{a \cdot y + b = x \land b \geq 0\}
  \end{align*}
  \]

- while $b \geq y$ do
  \[
  \begin{align*}
  \{P \land b \geq y\} \\
  \{(a + 1) \cdot y + (b - y) = x \land (b - y) \geq 0\}
  \end{align*}
  \]

- $b := b - y$;
  \[
  \begin{align*}
  \{(a + 1) \cdot y + b = x \land b \geq 0\} \\
  \{a := a + 1\}
  \end{align*}
  \]

- od
  \[
  \begin{align*}
  \{P \land \neg(b \geq y)\} \\
  \{a \cdot y + b = x \land b < y\}
  \end{align*}
  \]
Literature Recommendation

Content

- Formal Program Verification
  - Proof System PD

- The Verifier for Concurrent C
  - Assertions, Modular Verification, VCC

- Runtime-Verification
  - Assertions, LSC-Observers

- Reviews
  - Roles and artefacts
  - Review procedure
  - Stronger and weaker variants

- Code QA Techniques Revisited
  - Test, Runtime-Verification, Review,
  - Static Checking, Formal Verification

- Do’s and Don’ts in Code QA

- Dependability
Assertions
Assertions

- Extend the syntax of deterministic programs by

\[ S ::= \cdots \mid \text{assert}(B) \]

- and the semantics by rule

\[ \langle \text{assert}(B), \sigma \rangle \rightarrow \langle E, \sigma \rangle \] if \( \sigma \models B. \)

(If the asserted boolean expression \( B \) does not hold in state \( \sigma \), the empty program is not reached; otherwise the assertion remains in the first component: abnormal program termination).

Extend PD by axiom:

\( (A7) \{p\} \text{assert}(p) \{p\} \)

- That is, if \( p \) holds before the assertion, then we can continue with the derivation in PD. If \( p \) does not hold, we “get stuck” (and cannot complete the derivation).

- So we cannot derive \( \{true\} x := 0; \text{assert}(x = 27) \{true\} \) in PD.
Modular Reasoning
We can add another rule for calls of functions $f : F$ (simplest case: only global variables):

$$(R7) \quad \frac{\{p\} F \{q\}}{\{p\} f() \{q\}}$$

“If we have $\vdash \{p\} F \{q\}$ for the implementation of function $f$, then if $f$ is called in a state satisfying $p$, the state after return of $f$ will satisfy $q$.”

$p$ is called pre-condition and $q$ is called post-condition of $f$.

**Example:** if we have

- $\{true\}$ read_number $\{0 \leq result < 10^8\}$
- $\{0 \leq x \land 0 \leq y\}$ add $\{(old(x) + old(y) < 10^8 \land result = old(x) + old(y)) \lor result < 0\}$
- $\{true\}$ display $\{(0 \leq old(sum) < 10^8 \implies "old(sum)"\) \land (old(sum) < 0 \implies "-E-"\}\}$

we may be able to prove our pocket calculator correct.

```plaintext
int x, y, sum;
int main() {
    while (true) {
        x = read_number();
        y = read_number();
        sum = add(); // add 'x' and 'y'
        display(); // display 'sum'
    }
}
```
For **modular reasoning**, it's often useful to refer in the post-condition to

- the **return value** as \( \text{result} \),
- the **values of variable** \( x \) **at calling time** as \( \text{old}(x) \).

Can be defined using **auxiliary variables**:

- Transform function

\[
T \ f() \{ \ldots \; \text{return} \; \text{expr}; \}
\]

(over variables \( V = \{v_1, \ldots, v_n\}; \text{where result, } v_i^{\text{old}} \notin V \)) into

\[
T \ f() \{
    v_1^{\text{old}} := v_1; \ldots; v_n^{\text{old}} := v_n;
    \ldots;
    \text{result} := \text{expr};
    \text{return} \; \text{result};
\}
\]

over \( V' = V \cup \{v_i^{\text{old}} \mid v \in V\} \cup \{\text{result}\} \).

Then \( \text{old}(x) \) is just an abbreviation for \( x^{\text{old}} \).
The Verifier for Concurrent C
The **Verifier for Concurrent C** (VCC) basically implements Hoare-style reasoning.

**Special syntax:**
- `#include <vcc.h>`
- `_(requires p)` – **pre-condition**, `p` is (basically) a C expression
- `_(ensures q)` – **post-condition**, `q` is (basically) a C expression
- `_(invariant expr)` – **loop invariant**, `expr` is (basically) a C expression
- `_(assert p)` – **intermediate invariant**, `p` is (basically) a C expression
- `_(writes &v)` – VCC considers **concurrent** C programs; we need to declare for each procedure which global variables it is allowed to write to (also checked by VCC)

**Special expressions:**
- `\texttt{thread\_local}(\&v)` – no other thread writes to variable `v` (in pre-conditions)
- `\texttt{old}(v)` – the value of `v` when procedure was called (useful for post-conditions)
- `\texttt{result}` – return value of procedure (useful for post-conditions)
VCC Syntax Example

```c
#include <vcc.h>

int a, b;

void div(int x, int y)
  _(requires \( x \geq 0 \land y \geq 0 \))
  _(ensures \( a \times y + b = x \land b < y \))
  _(writes &a)
  _(writes &b)
{
  a = 0;
  b = x;
  while (b >= y)
    _(invariant \( a \times y + b = x \land b \geq 0 \))
    {
      b = b - y;
      a = a + 1;
    }
}
```

\[
DIV \equiv a := 0; \ b := x; \ while \ b \geq y \ do \ b := b - y; \ a := a + 1 \ od
\]

\[
\{ x \geq 0 \land y \geq 0 \} \ DIV \ \{ x \geq 0 \land y \geq 0 \}
\]
VCC

Does this C program always work?

```c
#include <vcc.h>
int a, b;
void div( int x, int y )
    _(requires x >= 0 && y > 0)
    _(ensures a * y + b == x && b < y)
    _(writes &a)
    _(writes &b)
{
    a = 0;
    b = x;
    while (b >= y)
        _(invariant a * y + b == x && b >= 0)
        b = b - y;
    a = a + 1;
}
```

Example program DIV: http://rise4fun.com/Vcc/4Kqe
Interpretation of Results

- VCC result: “verification succeeded”

- We can only conclude that the tool
  – under its interpretation of the C-standard, under its platform assumptions (32-bit), etc. –
  claims that there is a proof for $\models \{p\} \text{DIV} \{q\}$.

- May be due to an error in the tool! (That’s a false negative then.)
  Yet we can ask for a printout of the proof and check it manually (hardly possible in practice) or with other tools like interactive theorem provers.

- **Note:** $\models \{false\} f \{q\}$ always holds.
  That is, a mistake in writing down the pre-condition can make errors in the program go undetected!

- VCC result: “verification failed”

- May be a false positive (wrt. the goal of finding errors).
  The tool does not provide counter-examples in the form of a computation path, it (only) gives hints on input values satisfying $p$ and causing a violation of $q$.

- $\rightarrow$ try to construct a (true) counter-example from the hints.
  or: make loop-invariant(s) (or pre-condition $p$) stronger, and try again.

- Other case: “timeout” etc. – completely inconclusive outcome.
For the exercises, we use VCC only for **sequential, single-thread programs**.

VCC checks a number of **implicit assertions**:

- no arithmetic overflow in expressions (according to C-standard),
- array-out-of-bounds access,
- NULL-pointer dereference,
- and many more.

Verification **does not always succeed**:

- The backend SMT-solver may not be able to discharge proof-obligations (in particular non-linear multiplication and division are challenging);
- In many cases, we need to provide **loop invariants** manually.

VCC also supports:

- **concurrency**: different threads may write to shared global variables; VCC can check whether concurrent access to shared variables is properly managed;
- **data structure invariants**: we may declare invariants that have to hold for, e.g., records (e.g. the length field $l$ is always equal to the length of the string field $str$); those invariants may **temporarily** be violated when updating the data structure.
- and much more.
Tell Them What You’ve Told Them…

Testing:

- Define criteria for “testing done” (like coverage, or cost per error).
- Process: tester and developer should be different persons.

Formal Verification:

- There are more approaches to software quality assurance than just testing.
- For example, program verification.
- Proof System PD can be used
  - to prove
  - that a given program is
  - correct wrt. its specification.

This approach considers all inputs inside the specification!
- Tools like VCC implement this approach.
Content

- Formal Program Verification
  - Proof System PD
- The Verifier for Concurrent C
  - Assertions, Modular Verification, VCC
- Runtime-Verification
  - Assertions, LSC-Observers
- Reviews
  - Roles and artefacts
  - Review procedure
  - Stronger and weaker variants
- Code QA Techniques Revisited
  - Test, Runtime-Verification, Review,
  - Static Checking, Formal Verification
- Do’s and Don’ts in Code QA
- Dependability
Run-Time Verification
Run-Time Verification: Idea

- Assume, there is a function $f$ in software $S$ with the following specification:
  - **pre-condition**: $p$, **post-condition**: $q$.

- Computation paths of $S$ may look like this:

\[
\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots \xrightarrow{\alpha_{n-1}} \sigma_n \xrightarrow{\text{call } f} \sigma_{n+1} \cdots \sigma_m \xrightarrow{\text{returns}} \sigma_{m+1} \cdots
\]

- Assume there are functions $\text{check}_p$ and $\text{check}_q$, which check whether $p$ and $q$ hold at the current program state, and which do not modify the program state (except for program counter).

- **Idea**: create software $S'$ by
  - (i) extending $S$ by implementations of $\text{check}_p$ and $\text{check}_q$, (ii) call $\text{check}_p$ right after entering $f$, (iii) call $\text{check}_q$ right before returning from $f$.

- For $S'$, obtain computation paths like:

\[
\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots \xrightarrow{\alpha_{n-1}} \sigma_n \xrightarrow{\text{call } f} \sigma_{n+1} \xrightarrow{\text{check}_p} \sigma'_{n+1} \cdots \sigma_m \xrightarrow{\text{check}_q} \sigma'_m \xrightarrow{\text{returns}} \sigma_{m+1} \cdots
\]

- If $\text{check}_p$ and $\text{check}_q$ notify us of violations of $p$ or $q$, then we are notified of $f$ violating its specification when running $S'$ (= at run-time).
Run-Time Verification: Example

```c
int x, y, sum;

int main() {
    while (true) {
        x = read_number();
        y = read_number();
        sum = add(x, y);
        verify_sum(x, y, sum);
        display();
    }
}
```

```c
void verify_sum(int x, int y, int sum) {
    if (sum != (x+y) || (x + y > 99999999 && !(sum < 0))) {
        printf(stderr, "verify_sum: error\n");
        abort();
    }
}
```
A Very Useful Special Case: Assertions

- Maybe the simplest instance of runtime verification: Assertions.
- Available in standard libraries of many programming languages (C, C++, Java, ...).

- For example, the C standard library manual reads:

```
#include <assert.h>

void assert(scalar expression);
```

- In C code, `assert` can be **disabled** in production code (`-D NDEBUG`).
- Use `java -ea ...` to **enable assertion checking** (disabled by default).

(cf. https://docs.oracle.com/javase/8/docs/technotes/guides/language/assert.html)
The abstract \( f \)-example from run-time verification: 
(specification: \( \{ p \} f \{ q \} \))

\[
\begin{verbatim}
void f(...) {
    assert(p);
    ...
    assert(q);
}
\end{verbatim}
\]

Compute the width of a progress bar:

\[
\begin{verbatim}
int progress_bar_width(int progress, int window_left, int window_right) {
    assert(window_left <= window_right); /* pre-condition */
    ...
    /* treat special cases 0 and 100 */
    ...
    assert(0 < progress && progress < 100); // extremal cases already treated
    ...
    assert(window_left <= r && r <= window_right); /* post-condition */
    return r;
}
\end{verbatim}
\]
Recall the **structure model** with Proto-OCL constraint from Exercise Sheet 4.

Assume, we add a method `set_key()` to class **TreeNode**:

```java
class TreeNode {
    private int key;
    TreeNode parent, leftChild, rightChild;

    public int get_key() { return key; }

    public void set_key(int new_key) {
        key = new_key;
    }
}
```

We can **check consistency** with the Proto-OCL constraint at runtime by using assertions:

```java
public void set_key(int new_key) {
    assert (parent == null || parent.get_key() <= new_key);
    assert (leftChild == null || new_key <= leftChild.get_key());
    assert (rightChild == null || new_key <= rightChild.get_key());

    key = new_key;
}
```
More Complex Run-Time Verification: LSC Observers

ChoicePanel:

```
st : { idle, wsel, ssel, tsel, reqs, half }; 

take_event( E : { TAU, WATER, SOFT, TEA, ... } ){
  bool stable = 1;
  switch (st) {
    case idle :
      switch (E) {
        case WATER :
          if (water_enabled) { st := wsel; stable := 0; } ;;
        case SOFT :
          ... 
      }
    case wsel:
      switch (E) {
        case TAU :
          send_DWATER(); st := reqs; 
          hey_observer_I_just_sent_DWATER();
          ;;
      }
  }
}
```
Experience:
During development, **assertions** for pre/post conditions and intermediate invariants are an extremely powerful tool with a very attractive gain/effort ratio (low effort, high gain).

- Assertions effectively work as **safe-guard against unexpected use** of functions and **regression**, e.g. during later maintenance or efficiency improvement.
- Can serve as **formal** (support of) **documentation**:
  “Dear reader, at this point in the program, I expect condition `expr` to hold, because…”
By the Way: Development vs. Release Versions

- Development- vs. Release Versions:
  - Common practice:
    - development version with run-time verification enabled (cf. `assert(3)`),
    - release version without run-time verification.

If run-time verification is enabled in a release version,
- software should terminate as gracefully as possible (e.g. try to save data),
- save information from assertion failure if possible for future analysis.

Risk: with bad luck, the software only behaves well because of the run-time verification code…

Then disabling run-time verification “breaks” the software. Yet very complex run-time verification may significantly slow down the software, so needs to be disabled…

```
assert (x == 0);
assert (x == 0);
```
Content

- Formal Program Verification
  - Proof System PD

- The Verifier for Concurrent C
  - Assertions, Modular Verification, VCC

- Runtime-Verification
  - Assertions, LSC-Observers

- Reviews
  - Roles and artefacts
  - Review procedure
  - Stronger and weaker variants

- Code QA Techniques Revisited
  - Test, Runtime-Verification, Review,
  - Static Checking, Formal Verification

- Do’s and Don’ts in Code QA

- Dependability
Review
Recall: Three Basic Directions

- (Σ × A)^ω defines all computation paths satisfying the specification.
- Expected outcomes \( S_{\text{oll}} \) expected outcomes.
- Testing: input → output.
- Review: review.
- Formal Verification: proves \( S \models \mathcal{I} \), concludes \( [S] \in \mathcal{I} \).
**Input to Review Session:**

- **Review item:** can be every closed, human-readable part of software (documentation, module, test data, installation manual, etc.)

  **Social aspect:** it is an **artefact** which is examined, not the **human** (who created it).

- **Reference documents:** need to enable an assessment (requirements specification, guidelines (e.g. coding conventions), catalogue of questions (“all variables initialised?”), etc.)

**Roles:**

- **Moderator:** leads session, responsible for properly conducted procedure.

- **Author:** (representative of the) creator(s) of the artefact under review; is present to listen to the discussions; can answer questions; does not speak up if not asked.

- **Reviewer(s):** person who is able to judge the artefact under review; maybe different reviewers for different aspects (programming, tool usage, etc.), at best experienced in detecting inconsistencies or incompleteness.

- **Transcript Writer:** keeps minutes of review session, can be assumed by author.

- **The review team** consists of everybody but the author(s).
Review Procedure Over Time

**Planning**
- **Initiation**: Review organisation under guidance of moderator
- **Approval of review item**

**Preparation**
- **Review Session**: Reviewers report, evaluate, and document issues; resolve open questions.
- **“3rd hour”**: Time for informal chat, reviewers may state proposals for solutions or improvements.
- **Initiation**
- **Approval of review item**

**Postparation**
- Reviewers re-work review item; responsibility of the author(s).

**Review**
- **Session (2 h)**
- "3rd hour" (1 h)

**Analysis**
- **improve development and review process.**

- **Reviewers re-assess** reworked review item (until **approval** is declared).

**a review is triggered**, e.g., by a submission to the revision control system: the moderator invites (include review item in invitation), and states **review missions**.

**planning**: reviews need **time** in the project plan.

**preparation**: reviewers **investigate** review item.

**review session**: reviewers **report**, evaluate, and document issues; resolve open questions.

- **postparation**: rework review item; responsibility of the author(s).
Review Rules

(i) The moderator organises the review, issues invitations, supervises the review session.

(ii) The moderator may terminate the review if conduction is not possible, e.g., due to inputs, preparation, or people missing.

(iii) The review session is limited to 2 hours. If needed: organise more sessions.

(iv) The review item is under review, not the author(s). Reviewers choose their words accordingly. Authors neither defend themselves nor the review item.

(v) Roles are not mixed up, e.g., the moderator does not act as reviewer. (Exception: author may write transcript.)

(vi) Style issues (outside fixed conventions) are not discussed.

(vii) The review team is not supposed to develop solutions. Issues are not noted down in form of tasks for the author(s).

(viii) Each reviewer gets the opportunity to present her/his findings appropriately.

(ix) Reviewers need to reach consensus on issues, consensus is noted down.

(x) Issues are classified as:
- critical (review unusable for purpose),
- major (usability severely affected),
- minor (usability hardly affected),
- good (no problem).

(xi) The review team declares:
- accept without changes,
- accept with changes,
- do not accept.

(xii) The protocol is signed by all participants.
Stronger and Weaker Review Variants

- **Design and Code Inspection**
  - deluxe variant of review,
  - approx. 50% more time, approx. 50% more errors found.

- **Review**

- **Structured Walkthrough**
  - simple variant of review:
    - developer moderates walkthrough-session,
    - developer presents artefact(s),
    - reviewer poses (prepared or spontaneous) questions,
    - issues are noted down,
  - Variation point: do reviewers see the artefact before the session?
  - less effort, less effective.
  - → disadvantages: unclear responsibilities; “salesman”-developer may trick reviewers.

- **Comment** ('Stellungnahme')
  - colleague(s) of developer read artefacts,
  - developer considers feedback.
  - → advantage: low organisational effort;
  - → disadvantages: choice of colleagues may be biased; no protocol;
    consideration of comments at discretion of developer.

- **Careful Reading** ('Durchsicht')
  - done by developer,
  - recommendation: “away from screen” (use print-out or different device and situation)
Content

- Formal Program Verification
  - Proof System PD

- The Verifier for Concurrent C
  - Assertions, Modular Verification, VCC

- Runtime-Verification
  - Assertions, LSC-Observers

- Reviews
  - Roles and artefacts
  - Review procedure
  - Stronger and weaker variants

- Code QA Techniques Revisited
  - Test, Runtime-Verification, Review,
  - Static Checking, Formal Verification

- Do’s and Don’ts in Code QA

- Dependability
Code Quality Assurance Techniques Revisited
## Techniques Revisited

<table>
<thead>
<tr>
<th>Test</th>
<th>automatic</th>
<th>prove “can run”</th>
<th>toolchain considered</th>
<th>exhaustive</th>
<th>prove correct</th>
<th>partial results</th>
<th>entry cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Runtime-Verification</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Review</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static Checking Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Strengths:
- can be fully automatic (yet not easy for GUI programs);
- negative test proves “program not completely broken”, “can run” (or positive scenarios);
- final product is examined, thus toolchain and platform considered;
- one can stop at any time and take partial results;
- few, simple test cases are usually easy to obtain;
- provides reproducible counter-examples (good starting point for repair).

### Weaknesses:
- (in most cases) vastly incomplete, thus no proofs of correctness;
- creating test cases for complex functions (or complex conditions) can be difficult;
- maintenance of many, complex test cases be challenging.
- executing many tests may need substantial time (but: can sometimes be run in parallel);
### Strengths:
- **fully automatic** (once observers are in place);
- provides counter-example;
- (nearly) **final product is examined**, thus toolchain and platform considered;
- one can stop at any time and take **partial results**;
- assert-statements have a very good effort/effect ratio.

### Weaknesses:
- counter-examples **not necessarily reproducible**;
- may negatively affect **performance**;
- code is changed, program may only run **because of** the observers;
- completeness depends on usage, may also be **vastly incomplete**, so no correctness proofs;
- constructing observers for complex properties may be **difficult**, one needs to learn how to construct observers.
<table>
<thead>
<tr>
<th></th>
<th>automatic</th>
<th>prove “can run”</th>
<th>toolchain considered</th>
<th>exhaustive</th>
<th>prove correct</th>
<th>partial results</th>
<th>entry cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>×</td>
<td>×</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Runtime-Verification</td>
<td>✔</td>
<td>(✔)</td>
<td>✔</td>
<td>(✘)</td>
<td>×</td>
<td>✔</td>
<td>(✔)</td>
</tr>
<tr>
<td>Review</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>(✔)</td>
<td>(✔)</td>
<td>✔</td>
<td>(✔)</td>
</tr>
<tr>
<td>Static Checking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Strengths:**
- Human readers can **understand the code**, may spot point errors;
- Reported to be **highly effective**;
- One can stop at any time and take **partial results**;
- Intermediate **entry costs**;
  - Good effort/effect ratio achievable.

**Weaknesses:**
- No **tool support**;
- No results on actual execution, **toolchain not reviewed**;
- Human readers may **overlook** errors; usually not aiming at proofs.
- Does (in general) **not provide counter-examples**, developers may deny existence of error.
### Techniques Revisited

<table>
<thead>
<tr>
<th></th>
<th>automatic</th>
<th>prove &quot;can run&quot;</th>
<th>toolchain considered</th>
<th>exhaustive</th>
<th>prove correct</th>
<th>partial results</th>
<th>entry cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✘</td>
<td>✘</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Runtime-Verification</td>
<td>✔ (✔)</td>
<td>✔</td>
<td>(✘)</td>
<td>✔</td>
<td>✘</td>
<td>✗</td>
<td>(✔)</td>
</tr>
<tr>
<td>Review</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>(✔)</td>
<td>(✔)</td>
<td>✔</td>
<td>(✔)</td>
</tr>
<tr>
<td>Static Checking</td>
<td>✔ (✘)</td>
<td>✘</td>
<td>✘</td>
<td>✔</td>
<td>(✔)</td>
<td>✔</td>
<td>(✘)</td>
</tr>
<tr>
<td>Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Strengths:**
- there are (commercial), **fully automatic** tools (lint, Coverity, Polyspace, etc.);
- some tools are **complete** (relative to assumptions on language semantics, platform, etc.);
- can be **faster than testing**;
- one can stop at any time and take **partial results**.

**Weaknesses:**
- no results on actual execution, **toolchain not reviewed**;
- can be very **resource consuming** (if few false positives wanted), e.g., code may need to be "designed for static analysis";
- many false positives can be very **annoying to developers** (if fast checks wanted);
- distinguish **false from true positives** can be challenging;
- configuring the tools (to limit false positives) can be challenging.
Techniques Revisited

<table>
<thead>
<tr>
<th></th>
<th>automatic</th>
<th>prove “can run”</th>
<th>toolchain considered</th>
<th>exhaustive</th>
<th>prove correct</th>
<th>partial results</th>
<th>entry cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Runtime-Verification</td>
<td>✔</td>
<td>(✓)</td>
<td>✔</td>
<td>(✗)</td>
<td>❌</td>
<td>✔</td>
<td>(✓)</td>
</tr>
<tr>
<td>Review</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
<td>(✓)</td>
<td>✔</td>
<td>(✓)</td>
</tr>
<tr>
<td>Static Checking</td>
<td>✔</td>
<td>(✗)</td>
<td>❌</td>
<td>✔</td>
<td>(✓)</td>
<td>✔</td>
<td>(✗)</td>
</tr>
<tr>
<td>Verification</td>
<td>(✓)</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
<td>✔</td>
<td>(✗)</td>
<td>✗</td>
</tr>
</tbody>
</table>

Strengths:

- some tool support available (few commercial tools);
- complete (relative to assumptions on language semantics, platform, etc.);
- thus can provide correctness proofs;
- can prove correctness for multiple language semantics and platforms at a time;
- can be more efficient than other techniques.

Weaknesses:

- no results on actual execution, toolchain not reviewed;
- not many intermediate results: “half of a proof” may not allow any useful conclusions;
- entry cost high: significant training is useful to know how to deal with tool limitations;
- proving things is challenging: failing to find a proof does not allow any useful conclusion;
- false negatives (broken program “proved” correct) hard to detect.
## Techniques Revisited

<table>
<thead>
<tr>
<th></th>
<th>automatic</th>
<th>prove “can run”</th>
<th>toolchain considered</th>
<th>exhaustive</th>
<th>prove correct</th>
<th>partial results</th>
<th>entry cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✘</td>
<td>✘</td>
<td>✔</td>
<td>✔️</td>
</tr>
<tr>
<td>Runtime-Verification</td>
<td>✔️</td>
<td>(✔️)</td>
<td>✔️</td>
<td>(✘)</td>
<td>✘</td>
<td>✔</td>
<td>(✔️)</td>
</tr>
<tr>
<td>Review</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>(✔️)</td>
<td>(✔️)</td>
<td>✔</td>
<td>(✔️)</td>
</tr>
<tr>
<td>Static Checking</td>
<td>✔️</td>
<td>(✘)</td>
<td>✘</td>
<td>✔</td>
<td>(✔️)</td>
<td>✔</td>
<td>(✘)</td>
</tr>
<tr>
<td>Verification</td>
<td>(✔️)</td>
<td>✘</td>
<td>✘</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>(✘)</td>
</tr>
</tbody>
</table>
Dependability Case
A dependable system is one you can depend on — that is, you can place your trust in it.

“Developers [should] express the critical properties and make an explicit argument that the system satisfies them.”

Proposed Approach:

- Identify the critical requirements, and determine what level of confidence is needed. (Most systems do also have non-critical requirements.)
- Construct a dependability case, i.e. an argument, that the software, in concert with other components, establishes the critical properties.
- The dependability case should be:
  - auditable: can (easily) be evaluated by third-party certifier.
  - complete: no holes in the argument; any assumptions that are not justified should be noted (e.g. assumptions on compiler, on protocol obeyed by users, etc.)
  - sound: e.g. should not claim full correctness [...] based on nonexhaustive testing; should not make unwarranted assumptions on independence of component failures; etc.
Tell Them What You’ve Told Them...

- **Runtime Verification**
  - (as the name suggests) checks properties at **program run-time**,
  - generous use of `assert`'s can be a valuable safe-guard against
    - **regressions**, usage **outside specification**, etc.
  
  and serve as **formal documentation** of (intermediate) assumptions.

  Very attractive **effort / effect** ratio.

- **Review** (structured examination of artefacts by humans)
  - (mild variant) advocated in the XP approach,
  - **not uncommon**:
    - lead programmer reviews **all commits** from team members,
  
  - literature reports good effort/effect ratio achievable.

- **All approaches to code quality assurance** have their
  - **advantages** and **drawbacks**.

  Which to use? It depends!

- **Overall: Consider Dependability Cases**
  - an (auditable, complete, sound) argument, that a software has the **critical properties**.
Looking Back:
17 Lectures on Software Engineering
Contents of the Course

<table>
<thead>
<tr>
<th>Introduction</th>
<th>L 1: 18.4., Mon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scales, Metrics, Costs</td>
<td>L 2: 21.4., Thu</td>
</tr>
<tr>
<td></td>
<td>L 3: 25.4., Mon</td>
</tr>
<tr>
<td></td>
<td>L 4: 2.5., Mon</td>
</tr>
<tr>
<td>Development</td>
<td>L 5: 9.5., Mon</td>
</tr>
<tr>
<td></td>
<td>L 6: 12.5., Thu</td>
</tr>
<tr>
<td></td>
<td>L 7: 16.5., Mon</td>
</tr>
<tr>
<td></td>
<td>L 8: 19.5., Thu</td>
</tr>
<tr>
<td>Process</td>
<td>L 5: 28.4., Thu</td>
</tr>
<tr>
<td></td>
<td>L 4: 5.5., Thu</td>
</tr>
<tr>
<td></td>
<td>L 5: 9.5., Mon</td>
</tr>
<tr>
<td>Requirements Engineering</td>
<td>L 6: 12.5., Thu</td>
</tr>
<tr>
<td></td>
<td>L 7: 16.5., Mon</td>
</tr>
<tr>
<td></td>
<td>L 8: 19.5., Thu</td>
</tr>
<tr>
<td></td>
<td>T 2: 23.5., Mon</td>
</tr>
<tr>
<td></td>
<td>L 7: 26.5., Thu</td>
</tr>
<tr>
<td>Architecture &amp; Design</td>
<td>L 7: 30.5., Mon</td>
</tr>
<tr>
<td></td>
<td>L 8: 2.6., Thu</td>
</tr>
<tr>
<td></td>
<td>L 9: 6.6., Mon</td>
</tr>
<tr>
<td></td>
<td>L 10: 9.6., Thu</td>
</tr>
<tr>
<td></td>
<td>L 10: 13.6., Mon</td>
</tr>
<tr>
<td></td>
<td>L 11: 16.6., Thu</td>
</tr>
<tr>
<td></td>
<td>L 12: 20.6., Mon</td>
</tr>
<tr>
<td></td>
<td>T 3: 23.6., Thu</td>
</tr>
<tr>
<td>Software Modelling</td>
<td>L 13: 27.6., Mon</td>
</tr>
<tr>
<td></td>
<td>L 14: 30.6., Thu</td>
</tr>
<tr>
<td></td>
<td>L 15: 4.7., Mon</td>
</tr>
<tr>
<td></td>
<td>T 5: 7.7., Thu</td>
</tr>
<tr>
<td>Quality Assurance (Testing, Formal Verification)</td>
<td>L 16: 11.7., Mon</td>
</tr>
<tr>
<td></td>
<td>L 17: 14.7., Thu</td>
</tr>
<tr>
<td></td>
<td>L 18: 18.7., Mon</td>
</tr>
<tr>
<td></td>
<td>L 19: 21.7., Thu</td>
</tr>
<tr>
<td>Wrap-Up</td>
<td>L 19: 21.7., Thu</td>
</tr>
</tbody>
</table>
What Did We Do?
That’s Today’s Software Engineering — More or Less...
Questions?
Advertisements
Further studies:

- **Real-Time Systems → Winter 2017/18**
  (specification and verification of real-time systems)

- **Software Design, Modelling, and Analysis in UML** (not in 2017/18)
  (a formal, in-depth view on structural and behavioural modelling)

- **Cyber-Physical Systems I - Discrete Models**
  (more on variants of CFA and queries (LTL, CTL, CTL*))

- **Cyber-Physical Systems - Hybrid Models**
  (Modelling and analysis of cyber-physical systems with hybrid automata)

- **Program Verification**
  (the theory behind tools like VCC)

- **Formal Methods for Java**
  (JML and “VCC for Java”)

- **Decision Procedures**
  (the basis for program verification)

→ [https://swt.informatik.uni-freiburg.de/teaching](https://swt.informatik.uni-freiburg.de/teaching)
• **Individual Projects**  
  (BSc/MSc project, Lab Project, BSc/MSc thesis)  
  • formal modelling of industrial case studies  
  • improving analysis techniques  
  • own topics  
  → contact us (3–6 months before planned start).

• Want to be a **tutor**, e.g. Software Engineering 2018?  
  → contact us (around September / March).
Thanks For Your Participation...
References
References


