Specifying and Verifying Programs

Wolfgang Schreiner
Wolfgang.Schreiner@risc.jku.at
Research Institute for Symbolic Computation (RISC)
Johannes Kepler University, Linz, Austria
http://www.risc.jku.at

We will discuss three (closely interrelated) calculi.

- **Hoare Calculus**: \( \{ P \} c \{ Q \} \)
  - If command \( c \) is executed in a pre-state with property \( P \) and terminates, it yields a post-state with property \( Q \).
  \[
  \{ x = a \land y = b \} x := x + y \{ x = a + y \land y = b \}
  \]

- **Predicate Transformers**: \( \text{wp}(c, Q) = P \)
  - If the execution of command \( c \) shall yield a post-state with property \( Q \), it must be executed in a pre-state with property \( P \).
  \[
  \text{wp}(x := x + y, x = a + y \land y = b) = (x + y = a + y \land y = b)
  \]

- **State Relations**: \( c : [P \Rightarrow Q]^x \)
  - The post-state generated by the execution of command \( c \) is related to the pre-state by \( P \Rightarrow Q \) (where only variables \( x, \ldots \) have changed).
  \[
  x = x + y : [\text{var } x = \text{old } x + \text{old } y]^x
  \]

The Hoare Calculus

First and best-known calculus for program reasoning (C.A.R. Hoare).

- "Hoare triple": \( \{ P \} c \{ Q \} \)
  - Logical propositions \( P \) and \( Q \), program command \( c \).
  - The Hoare triple is itself a logical proposition.
  - The Hoare calculus gives rules for constructing true Hoare triples.

- **Partial correctness** interpretation of \( \{ P \} c \{ Q \} \):
  "If \( c \) is executed in a state in which \( P \) holds, then it terminates in a state in which \( Q \) holds unless it aborts or runs forever."
  - Program does not produce wrong result.
  - But program also need not produce any result.
  - Abortion and non-termination are not (yet) ruled out.

- **Total correctness** interpretation of \( \{ P \} c \{ Q \} \):
  "If \( c \) is executed in a state in which \( P \) holds, then it terminates in a state in which \( Q \) holds."
  - Program produces the correct result.

We will use the partial correctness interpretation for the moment.
The Rules of the Hoare Calculus

Hoare calculus rules are inference rules with Hoare triples as proof goals.

\[
\begin{align*}
\{P_1\} c_1 \{Q_1\} \ldots \{P_n\} c_n \{Q_n\} & \quad VC_1, \ldots, VC_m \\
\{P\} c \{Q\} & \\
\end{align*}
\]

- Application of a rule to a triple \(\{P\} c \{Q\}\) to be verified yields
  - other triples \(\{P_1\} c_1 \{Q_1\} \ldots \{P_n\} c_n \{Q_n\}\) to be verified, and
  - formulas \(VC_1, \ldots, VC_m\) (the verification conditions) to be proved.

- Given a Hoare triple \(\{P\} c \{Q\}\) as the root of the verification tree:
  - The rules are repeatedly applied until the leaves of the tree do not contain any more Hoare triples.
  - If all verification conditions in the tree can be proved, the root of the tree represents a valid Hoare triple.

The Hoare calculus generates verification conditions such that the validity of the conditions implies the validity of the original Hoare triple.

Weakening and Strengthening

\[
\begin{align*}
P & \Rightarrow P' \\
\{P'\} c \{Q'\} & \\
Q' & \Rightarrow Q \\
\{P\} c \{Q\} & \\
\end{align*}
\]

- Logical derivation: \(\frac{A_1 \ A_2}{B}\)
  - Forward: If we have shown \(A_1\) and \(A_2\), then we have also shown \(B\).
  - Backward: To show \(B\), it suffices to show \(A_1\) and \(A_2\).

Interpretation of above sentence:
- To show that, if \(P\) holds, then \(Q\) holds after executing \(c\), it suffices to show this for a \(P'\) weaker than \(P\) and a \(Q'\) stronger than \(Q\).

Precondition may be weakened, postcondition may be strengthened.

Special Commands

- \(\{P\}\) skip \(\{P\}\)
- \(\{\text{true}\}\) abort \(\{\text{false}\}\)

- The skip command does not change the state; if \(P\) holds before its execution, then \(P\) thus holds afterwards as well.
- The abort command aborts execution and thus trivially satisfies partial correctness.
- Axiom implies \(\{P\}\) abort \(\{Q\}\) for arbitrary \(P, Q\).

Useful commands for reasoning and program transformations.

Scalar Assignments

- \(\{Q[e/x]\}\) \(x := e\) \(\{Q\}\)

- Syntax
  - Variable \(x\), expression \(e\).
  - \(Q[e/x]\) \(\ldots\) \(Q\) where every free occurrence of \(x\) is replaced by \(e\).

- Interpretation
  - To make sure that \(Q\) holds for \(x\) after the assignment of \(e\) to \(x\), it suffices to make sure that \(Q\) holds for \(e\) before the assignment.

- Partial correctness
  - Evaluation of \(e\) may abort.

\[
\begin{align*}
\{x + 3 < 5\} & \quad x := x + 3 \quad \{x < 5\} \\
\{x < 2\} & \quad x := x + 3 \quad \{x < 5\}
\end{align*}
\]
Array Assignments

\{ Q[a[i ↦→ e]/a] \} a[i] := e \{ Q \}

- An array is modelled as a function \( a : I \rightarrow V \).
- Index set \( I \), value set \( V \).
- \( a[i] = e \) ... array \( a \) contains at index \( i \) the value \( e \).
- Term \( a[i ↦→ e] \) (“array \( a \) updated by assigning value \( e \) to index \( i \)”)
  - A new array that contains at index \( i \) the value \( e \).
  - All other elements of the array are the same as in \( a \).
- Thus array assignment becomes a special case of scalar assignment.
  - Think of “\( a[i] := e \)” as “\( a := a[i ↦→ e] \)”.

\( \{ a[i ↦→ x][1] > 0 \} \quad a[i] := x \quad \{ a[1] > 0 \} \)

Arrays are here considered as basic values (no pointer semantics).

Command Sequences

\{ P \} c_1 \{ R \} \{ R \} \{ R \} \{ Q \}

- Interpretation
  - To show that, if \( P \) holds before the execution of \( c_1; c_2 \), then \( Q \) holds afterwards, it suffices to show for some \( R \) that
    - if \( P \) holds before \( c_1 \), that \( R \) holds afterwards, and that
    - if \( R \) holds before \( c_2 \), then \( Q \) holds afterwards.
- Problem: find suitable \( R \).
- Easy in many cases (see later).

\( \{ x + y - 1 > 0 \} \quad y := y - 1 \quad \{ x + y > 0 \} \quad x := x + y \quad \{ x > 0 \} \)
\( \{ x + y - 1 > 0 \} \quad y := y - 1 \quad x := x + y \quad \{ x > 0 \} \)

The calculus itself does not indicate how to find intermediate property.

Conditionals

\{ P \} c_1 \{ Q \} \{ P \} \{ Q \}

- Interpretation
  - To show that, if \( P \) holds before the execution of the conditional, then \( Q \) holds afterwards,
    - it suffices to show that the same is true for each conditional branch, under the additional assumption that this branch is executed.

\( \{ x ≠ 0 ∧ x ≥ 0 \} \quad y := x \quad \{ y > 0 \} \quad \{ x ≠ 0 ∧ x ≤ 0 \} \quad y := −x \quad \{ y > 0 \} \)
\( \{ x ≠ 0 \} \quad if \ x ≥ 0 \ then \ y := x \quad else \ y := −x \quad \{ y > 0 \} \)
Loops

\{true\} \text{loop} \{false\} \quad \{l \land b\} \quad c \quad \{l\} \\
{\{I\} \text{while} \ b \text{ do} \ c \quad \{l \land \neg b\}}

- **Interpretation:**
  - The \text{loop} command does not terminate and thus trivially satisfies partial correctness.
  - Axiom implies \{P\} \text{loop} \{Q\} for arbitrary \(P, Q\).
  - If it is the case that \(I\) holds before the execution of the \text{while}-loop and \(I\) also holds after every iteration of the loop body, then \(I\) holds also after the execution of the loop (together with the negation of the loop condition \(b\)).
  - \(I\) is a loop invariant.
- **Problem:**
  - Rule for \text{while}-loop does not have arbitrary pre/post-conditions \(P, Q\). In practice, we combine this rule with the strengthening/weakening-rule.

Example

\begin{align*}
I : & \iff s = \sum_{j=1}^{i-1} j \land 1 \leq i \leq n + 1 \\
(n \geq 0 \land s = 0 \land i = 1) & \implies I \\
\{I \land i \leq n\} & \text{s := s + i; i := i + 1} \quad \{I\} \\
(I \land i \not\leq n) & \implies s = \sum_{j=1}^{n} j \\
\{n \geq 0 \land s = 0 \land i = 1\} \text{ while } i \leq n \text{ do } (s := s + i; i := i + 1) \quad \{s = \sum_{j=1}^{n} j\}
\end{align*}

The invariant captures the “essence” of a loop; only by giving its invariant, a true understanding of a loop is demonstrated.
A Program Verification

- Verification of the following Hoare triple:
  \{ Input \} while \( i \leq n \) do \( (s := s + i; i := i + 1) \) \{ Output \}
- Auxiliary predicates:
  - Input \( \iff n \geq 0 \land s = 0 \land i = 1 \)
  - Output \( \iff s = \sum_{j=1}^{n} j \)
  - Invariant \( \iff s = \sum_{j=1}^{i-1} j \land 1 \leq i \leq n + 1 \)
- Verification conditions:
  - \( A \iff \text{Input} \Rightarrow \text{Invariant} \)
  - \( B \iff \text{Invariant} \land i \leq n \Rightarrow \text{Invariant}[i+1/i][s+i/s] \)
  - \( C \iff \text{Invariant} \land i \leq n \Rightarrow \text{Output} \)

If the verification conditions are valid, the Hoare triple is true.

RISCAL: Checking Program Execution

val N::Nat; type number = N[N]; type index = N[N+1]; type result = N[N-(1+N)/2];

proc summation(n:number): result
  requires n \geq 0;
  ensures result = \sum{j=1}^{n} j \land 1 \leq j \leq n.
  \{ 
    var s: result := 0;
    var i: index := 1;
    while i \leq n do
      invariant s = \sum{j=1}^{i-1} j \land 1 \leq j \land i \leq n+1;
      invariant i \leq 1 \land i \leq n+1;
      \{ 
        s := s+i;
        i := i+1;
      \}
      return s;
  \}

We check for some \( N \) the program execution; this implies that the invariant is not too strong.

Another Program Verification

Verification of the following Hoare triple:

\{ olda = a \land oldx = x \}
\( i := 0; r := -1; n = |a| \)
while \( i < n \land r = -1 \) do
  if \( a[i] = x \)
    then \( r := i \)
  else \( i := i + 1 \)
  \{ 
    \{ a = olda \land x = oldx \land 
    (r = -1 \land \forall i: 0 \leq i < |a| \Rightarrow a[i] \neq x) \land 
    (0 \leq r < |a| \land a[r] = x \land \forall i: 0 \leq i < r \Rightarrow a[i] \neq x)) \land 
  \}
Invariant \( \iff olda = a \land oldx = x \land n = |a| \land 
0 \leq i \leq n \land \forall j: 0 \leq j < i \Rightarrow a[j] \neq x \land 
(r = -1 \lor (r = i \land i < n \land a[r] = x)) \land 
\}

Find the smallest index \( r \) of an occurrence of value \( x \) in array \( a \) (\( r = -1 \), if \( x \) does not occur in \( a \)).
RISCAL: Checking Verification Conditions

We check for some $N, M$ that the verification conditions are valid.

RISCAL: Checking Program Execution

We check for some $N, M$ that the program execution.

The Verification Conditions

Input :⇔ olda = a ∧ oldx = x ∧ n = length(a) ∧ i = 0 ∧ r = -1

Output :⇔ a = olda ∧ x = oldx ∧

((r = -1 ∧ ∀i : 0 ≤ i < length(a) ⇒ a[i] ≠ x) ∨
(0 ≤ r < length(a) ∧ a[r] = x ∧ ∀i : 0 ≤ i < r ⇒ a[i] ≠ x))

Invariant :⇔ olda = a ∧ oldx = x ∧ n = |a| ∧

0 ≤ i < n ∧ ∀j : 0 ≤ j < i ⇒ a[j] ≠ x ∧

(r = -1 ∨ (r = i ∧ i < n ∧ a[r] = x))

A :⇔ Input ⇒ Invariant

B1 :⇔ Invariant ∧ i < n ∧ r = -1 ∧ a[i] = x ⇒ Invariant[i/r]

B2 :⇔ Invariant ∧ i < n ∧ r = -1 ∧ a[i] ≠ x ⇒ Invariant[i + 1/i]

C :⇔ Invariant ∧ ¬(i < n ∧ r = -1) ⇒ Output

The verification conditions $A, B_1, B_2, C$ must be valid.
Weakest Preconditions

The weakest precondition of each program construct.

- \( \text{wp}(\text{skip}, Q) = Q \)
- \( \text{wp}(\text{abort}, Q) = \text{true} \)
- \( \text{wp}(\text{x := e; } b \text{ do } c, Q) = \ldots \)

Loops represent a special problem (see later).

Forward Reasoning

Sometimes, we want to derive a postcondition from a given precondition.

\[ \{ P \} x := e \{ \exists x_0 : P[x_0/x] \land x = e[x_0/x] \} \]

- **Forward Reasoning**
  - What is the maximum we know about the post-state of an assignment \( x := e \), if the pre-state satisfies \( P \)?
  - We know that \( P \) holds for some value \( x_0 \) (the value of \( x \) in the pre-state) and that \( x \) equals \( e[x_0/x] \).

Verification is reduced to the calculation of weakest preconditions.

Backward Reasoning

Implication of rule for command sequences and rule for assignments:

\[ \{ P \} \ c \ \{ Q[e/x] \} \]
\[ \{ P \} \ c; \ x := e \ \{ Q \} \]

- **Interpretation**
  - If the last command of a sequence is an assignment, we can remove the assignment from the proof obligation.
  - By multiple application, assignment sequences can be removed from the back to the front.

<table>
<thead>
<tr>
<th>( { P } )</th>
<th>( { P } )</th>
<th>( { P } )</th>
<th>( { P } )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x := x + 1; )</td>
<td>( x := x + 1; )</td>
<td>( x := x + 1; )</td>
<td>( x + 1 = 5 )</td>
</tr>
<tr>
<td>( y := 2x; )</td>
<td>( y := 2x; )</td>
<td>( x + 2x = 15 )</td>
<td>( \iff x = 4 )</td>
</tr>
<tr>
<td>( z := x + y )</td>
<td>( x + y = 15 )</td>
<td>( 3x = 15 )</td>
<td>( \iff x = 5 )</td>
</tr>
<tr>
<td>( z = 15 )</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ P \Rightarrow x = 4 \]

Wolfgang Schreiner http://www.risc.jku.at 26/70
Strongest Postcondition

A calculus for forward reasoning.
- Predicate transformer $sp$
  - Function "sp" that takes a precondition $P$ and a command $c$ and returns a postcondition.
  - Read $sp(c, P)$ as "the strongest postcondition of $c$ w.r.t. $P$".
- $sp(c, P)$ is a postcondition for $c$ that is ensured by precondition $P$.
  - Must satisfy $\{P\}c\{sp(c, P)\}$.
- $sp(c, P)$ is the strongest such postcondition.
  - Take any $P, Q$ such that $\{P\}c\{Q\}$.
  - Then $sp(c, P) \Rightarrow Q$.
- Consequence: $\{P\}c\{Q\}$ iff $(sp(c, P) \Rightarrow Q)$.
  - We want to prove $\{P\}c\{Q\}$.
  - We may prove $sp(c, P) \Rightarrow Q$ instead.

Verification is reduced to the calculation of strongest postconditions.

Strongest Postconditions

The strongest postcondition of each program construct.

$sp(skip, P) = P$
$sp(abort, P) = false$
$sp(x := e, P) = \exists x_0 : P[x_0/x] \land x = e[x_0/x]$
$sp(c_1; c_2, P) = sp(c_2, sp(c_1, P))$
$sp(if b then c_1 else c_2, P) \Leftrightarrow sp(c_1, P \land b) \lor sp(c_2, P \land \neg b)$
$sp(if b then c, P) = sp(c, P \land b) \lor (P \land \neg b)$
$sp(while b do c, P) = \ldots$

Forward reasoning as a (less-known) alternative to backward-reasoning.

Weakest Liberal Preconditions for Loops

Why not apply predicate transformers to loops?

$wp(\text{loop}, Q) = true$
$wp(\text{while } b \text{ do } c, Q) = L_0(Q) \land L_1(Q) \land L_2(Q) \land \ldots$

$L_0(Q) = true$
$L_{i+1}(Q) = (\neg b \Rightarrow Q) \land (b \Rightarrow wp(c, L_i(Q)))$

Interpretation
- Weakest precondition that ensures that loops stops in a state satisfying $Q$, unless it aborts or runs forever.
- Infinite sequence of predicates $L_i(Q)$:
  - Weakest precondition that ensures that after less than $i$ iterations the state satisfies $Q$, unless the loop aborts or does not yet terminate.
- Alternative view: $L_i(Q) = wp(if_i, Q)$
  - $if_0 = \text{loop}$
  - $if_{i+1} = \text{if } b \text{ then } (c; if_i)$

Hoare Calc. and Predicate Transformers

In practice, often a combination of the calculi is applied.

$\{P\}c_1; \text{while } b \text{ do } c; c_2 \{Q\}$

- Assume $c_1$ and $c_2$ do not contain loop commands.
- It suffices to prove

$\{sp(P, c_1)\} \text{while } b \text{ do } c \{wp(c_2, Q)\}$

Predicate transformers are applied to reduce the verification of a program to the Hoare-style verification of loops.
**Example**

\[
\begin{align*}
\text{wp(while } i < n \text{ do } & i := i + 1, Q) \\
L_0(Q) &= \text{true} \\
L_1(Q) &= (i \neq n \Rightarrow Q) \land (i < n \Rightarrow \text{wp}(i := i + 1, \text{true})) \\
&\quad \Rightarrow (i \neq n \Rightarrow Q) \land (i < n \Rightarrow \text{true}) \\
L_2(Q) &= (i \neq n \Rightarrow Q) \land (i < n \Rightarrow \text{wp}(i := i + 1, i \neq n \Rightarrow Q)) \\
&\quad \Rightarrow (i \neq n \Rightarrow Q) \land (i < n \Rightarrow \text{wp}(i := i + 1, i \neq n \Rightarrow Q[i + 1/i]))) \\
L_3(Q) &= (i \neq n \Rightarrow Q) \land (i < n \Rightarrow \text{wp}(i := i + 1, \\
&\quad (i \neq n \Rightarrow Q) \land (i < n \Rightarrow (i + 1 \neq n \Rightarrow Q[i + 1/i]))) \\
&\quad \Rightarrow (i < n \Rightarrow ((i + 1 \neq n \Rightarrow Q[i + 1/i]) \land \\
&\quad (i + 1 < n \Rightarrow (i + 2 \neq n \Rightarrow Q[i + 2/i]))) \\
\end{align*}
\]

**Weakest Liberal Preconditions for Loops**

- Sequence \( L_i(Q) \) is monotonically increasing in strength:
  - \( \forall i \in \mathbb{N} : L_{i+1}(Q) \Rightarrow L_i(Q) \).
- The weakest precondition is the “lowest upper bound”:
  - \( \forall i \in \mathbb{N} : \text{wp(while } b \text{ do } c, Q) \Rightarrow L_i(Q) \).
  - \( \forall P : (\forall i \in \mathbb{N} : L_i(Q)) \Rightarrow (P \Rightarrow \text{wp(while } b \text{ do } c, Q)) \).
- We can only compute weaker approximation \( L_i(Q) \).
  - \( \text{wp(while } b \text{ do } c, Q) \Rightarrow L_i(Q) \).
- We want to prove \( \{ P \} \text{ while } b \text{ do } c \{ Q \} \).
  - This is equivalent to proving \( P \Rightarrow \text{wp(while } b \text{ do } c, Q) \).
  - Thus \( P \Rightarrow L_i(Q) \) must hold as well.
- If we can prove \( \neg(P \Rightarrow L_i(Q)) \), ...  
  - \( \{ P \} \text{ while } b \text{ do } c \{ Q \} \) does not hold.
  - If we fail, we may try the easier proof \( \neg(P \Rightarrow L_{i+1}(Q)) \).
  
  Falsification is possible by use of approximation \( L_i \), but verification is not.

**Preconditions for Loops with Invariants**

\[
\begin{align*}
\text{wp(while } b \text{ do invariant } I; c^{x \cdots}, Q) = \\
&\quad \text{let } oldx = x, \ldots \text{ in} \\
&\quad I \land (\forall x, \ldots : I \land b \Rightarrow \text{wp}(c, I)) \land \\
&\quad (\forall x, \ldots : I \land \neg b \Rightarrow Q)
\end{align*}
\]

- Loop body \( c \) only modifies variables \( x, \ldots \)
- Loop is annotated with invariant \( I \).
  - May refer to new values \( x, \ldots \) of variables after every iteration.
  - May refer to original values \( oldx, \ldots \) when loop started execution.
- Generated verification condition ensures:
  1. \( I \) holds in the initial state of the loop.
  2. \( I \) is preserved by the execution of the loop body \( c \).
  3. When the loop terminates, \( I \) ensures postcondition \( Q \).

This precondition is only “weakest” relative to the invariant.

**Example**

\[
\begin{align*}
\text{while } i \leq n \text{ do } (s := s + i; i := i + 1) \\
&\quad c^{s,i} := (s := s + i; i := i + 1) \\
&\quad \begin{align*}
&\quad I := s = \text{olds} + \left(\sum_{j=0}^{i-1} j \right) \land \text{oldi} \leq i \leq n + 1 \\
&\quad \text{Weakest precondition:} \\
&\quad \text{wp(while } i \leq n \text{ do invariant } I; c^{s,i}, Q) = \\
&\quad \text{let } olds = s, oldi = i \text{ in} \\
&\quad I \land (\forall s, i : I \land i \leq n \Rightarrow I[i + 1/i][s + i/s]) \land \\
&\quad (\forall s, i : I \land \neg(i \leq n) \Rightarrow Q)
\end{align*}
\end{align*}
\]

- Verification condition:
  - \( n \geq 0 \land i = 1 \land s = 0 \Rightarrow \text{wp(..., s = } \sum_{j=1}^{n} j) \)

Many verification systems implement (a variant of) this calculus.
Example

\[ I \iff s = \sum_{j=1}^{i-1} j \land 1 \leq i \leq n + 1 \]
\[ t := n - i + 1 \]
\[ (n \geq 0 \land i = 1 \land s = 0) \Rightarrow I \]
\[ I \Rightarrow n - i + 1 \geq 0 \]
\[ \{ I \land i \leq n \land n - i + 1 = N \} s := s + i; i := i + 1 \{ I \land n - i + 1 < N \} \]
\[ (I \land i \leq n) \Rightarrow s = \sum_{j=1}^{n} j \]

In practice, termination is easy to show (compared to partial correctness).

Termination in RISCAL

while \( i \leq n \) do
\[
invariant s = \sum_{j=1}^{i} j \land 1 \leq j \leq i-1 \cdot j; \]
\[
invariant I \land i \leq n + 1; \]
\[
decreases n+1-i; \]
\[
\{ \}
\[
\{ s := s + i; i := i + 1 \} \{ s = \sum_{j=1}^{i} j \}\]

fun Termination(n:number, s:result, i:index): number = n+1-i;

theorem T(n:number, s:result, i:index) ⇔
\[
Invariant(n, s, i) \Rightarrow Termination(n, s, i) \geq 0; \]

theorem B(n:number, s:result, i:index) ⇔
\[
Invariant(n, s, i) \land i \leq n \Rightarrow \]
\[
Invariant(n, s+i, i+1) \land \]
\[
Termination(n, s+i, i+1) < Termination(n, s, i); \]
Termination in RISCAL

while i < N ∧ r = -1 do
invariant 0 ≤ i ∧ i ≤ N;
invariant ∀j:index. 0 ≤ j ∧ j < i ⇒ a[j] ≠ x;
invariant r = -1 ∨ (r = 1 ∧ 1 < N ∧ a[i] = x);
decreases if r = -1 then N-i else 0;
{ if a[i] = x
  then r := i;
  else i := i+1;
}

fun Termination(a:array, x:elem, i:index, r:index): index =
  if r = -1 then N-i else 0;
theorem T(a:array, x:elem, i:index, r:index) ⇔ 
  Invariant(a, x, i, r) ⇒ Termination(a, x, i, r) ≥ 0;
theorem B1(a:array, x:elem, i:index, r:index) ⇔ 
  Invariant(a, x, i, r) ∧ i < N ∧ r = -1 ∧ a[i] = x ⇒ 
  Invariant(a, x, i, i) ∧ 
  Termination(a, x, i, i) < Termination(a, x, i, r);
theorem B2(a:array, x:elem, i:index, r:index) ⇔ ...

Weakest Preconditions for Loops

wp(loop, Q) = false
wp(while b do c, Q) = L0(Q) ∨ L1(Q) ∨ L2(Q) ∨...
L0(Q) = false
L_{i+1}(Q) = (¬b ⇒ Q) ∧ (b ⇒ wp(c, L_i(Q)))

New interpretation
- Weakest precondition that ensures that the loop terminates in a state in which Q holds, unless it aborts.
- New interpretation of L_i(Q)
- Weakest precondition that ensures that the loop terminates after less than i iterations in a state in which Q holds, unless it aborts.
- Preserves property: {P} c {Q} iff (P ⇒ wp(c, Q))
- Now for total correctness interpretation of Hoare calculus.
- Preserves alternative view: L_i(Q) ⇔ wp(if_i, Q)
  if_{i+1} = if b then (c;if_i)
  if_0 = loop

Example

wp(while i < n do i := i + 1, Q)
L_0(Q) = false
L_1(Q) = (i < n ⇒ Q) ∧ (i < n ⇒ wp(i := i + 1, L_0(Q)))
  ⇒ (i < n ⇒ Q) ∧ (i < n ⇒ false)
L_2(Q) = (i < n ⇒ Q) ∧ (i < n ⇒ wp(i := i + 1, L_1(Q)))
  ⇒ (i < n ⇒ Q) ∧
      (i < n ⇒ (i + 1 < n ∧ Q[i[1/i])))
L_3(Q) = (i < n ⇒ Q) ∧ (i < n ⇒ wp(i := i + 1, L_2(Q)))
  ⇒ (i < n ⇒ Q) ∧
      (i < n ⇒ ((i + 1 < n ⇒ Q[i[1/i]]) ∧
              (i + 1 < n ⇒ (i + 2 < n ∧ Q[i+2/i]))))
...

Weakest Preconditions for Loops

- Sequence L_i(Q) is now monotonically decreasing in strength:
  - ∀i ∈ N : L_i(Q) ⇒ L_{i+1}(Q).
- The weakest precondition is the "greatest lower bound":
  - ∀i ∈ N : L_i(Q) ⇒ wp(while b do c, Q).
  - ∀P : (∀i ∈ N : L_i(Q) ⇒ P) ⇒ (wp(while b do c, Q) ⇒ P).
- We can only compute a stronger approximation L_i(Q).
  - L_i(Q) ⇒ wp(while b do c, Q).
- We want to prove {P} c {Q}.
  - It suffices to prove P ⇒ wp(while b do c, Q).
  - It thus also suffices to prove P ⇒ L_i(Q).
  - If proof fails, we may try the easier proof P ⇒ L_{i+1}(Q)

However, verifications are typically not successful with any finite approximation of the weakest precondition.
Weakest Precondition with Measures

\[
\text{wp(while } b \text{ do invariant } I; \text{ decreases } t; \ c^x, ..., Q) = \\
\text{ let } oldx = x, ..., \text{ in} \\
I \land (\forall x, ..., I \land b \Rightarrow \text{wp}(C, I)) \land \\
(\forall x, ..., I \land \lnot b \Rightarrow Q) \land \\
(\forall x, ..., I \Rightarrow t \geq 0) \land \\
(\forall x, ..., I \land b \Rightarrow \text{let } T = t \text{ in wp}(c, t < T))
\]

- Loop body \( c \) only modifies variables \( x, ... \).
- Loop is annotated with termination measure (term) \( t \).
- May refer to new values \( x, ... \) of variables after every iteration.

Generated verification condition ensures:
1. \( t \) is non-negative before/after every loop iteration.
2. \( t \) is decremented by the execution of the loop body \( c \).

Also any well-founded ordering may be used as the domain of \( t \).

Example

\[
\text{while } i \leq n \text{ do (} s := s + i; i := i + 1) \\
c^{s,i} := (s := s + i; i := i + 1) \\
I :\iff s = olds + \left(\sum_{j=oldi}^{i-1} j\right) \land oldi \leq i \leq n + 1 \\
t := n + 1 - i
\]

- Weakest precondition:
  \[
  \text{wp(while } i \leq n \text{ do invariant } I; \ c^{s,i}, Q) = \\
  \text{ let } olds = s, oldi = i \text{ in} \\
  I \land (\forall s, i : I \land i \leq n \Rightarrow I[s+i/s, i+1/i]) \land \\
  (\forall s, i : I \land -(i \leq n) \Rightarrow Q) \land \\
  (\forall s, i : I \Rightarrow t \geq 0) \land \\
  (\forall s, i : I \land i \leq n \Rightarrow \text{let } T = n + 1 - i \text{ in } n + 1 - (i + 1) < T)
  \]
- Verification condition:
  \[
  n \geq 0 \land i = 1 \land s = 0 \Rightarrow \text{wp}(..., s = \sum_{j=1}^{n} j)
  \]

RISCAL and Verification Conditions

1. The Hoare Calculus
2. Checking Verification Conditions
3. Predicate Transformers
4. Termination
5. Generating Verification Conditions
6. Proving Verification Conditions
7. Abortion
8. Procedures
RISCAL Verification Conditions

RISCAL splits Dijkstra's single condition $\text{Input} \Rightarrow \text{wp}(C, \text{Output})$ into many “fine-grained” verification conditions:

- Is result correct?
  - One condition for every $\text{ensures}$ clause.

- Does loop invariant initially hold? Is loop invariant preserved?
  - Partial correctness.
  - One condition for every $\text{invariant}$ clause.

- Is loop measure non-negative? Is loop measure decreased?
  - Termination.
  - One condition for every $\text{decreases}$ clause.

- Specification and implementation preconditions
  - Well-definedness of formulas and commands (later).
  - One condition for every partial function/predicate application.

Click on a condition to see the affected commands; if the procedure contains conditionals, a condition is generated for each execution branch.

Example: is loop invariant preserved?

$$s = \left( \sum j : \text{number} \; \text{with} \; (1 \leq j) \land (j \leq (i-1)). j \right)$$

```plaintext
theorem _summation_0_LoopOp3(n:number)
requires n \geq 0;
<=> \forall s:result, i:index. (((s = \left( \sum j : \text{number} \; \text{with} \; (1 \leq j) \land (j \leq (i-1)). j \right))
\land (1 \leq i) \land (i \leq (n+1))))) \land (i \leq n))
\Rightarrow (\text{let } s = s+i \text{ in } (\text{let } i = i+1 \text{ in }
(s = \left( \sum j : \text{number} \; \text{with} \; (1 \leq j) \land (j \leq (i-1)). j \right)))) ;
```

Important: check models with small type sizes.

Proving Verification Conditions

RISCAL also provides an interface to automated theorem provers.

- Menu “TP” and menu entry “Apply Theorem Prover”
  - Tries to prove condition for arbitrary type sizes.
  - “Print Prover Output:” shows details of proof attempt.
  - “Apply Prover to All Theorems:” multiple proofs (in parallel).

Many (but typically not all) automatic proof attempts may succeed.

Checking Verification Conditions

- Double-click a condition to have it checked.
  - Checked conditions turn from red to blue.

- Right-click a condition to see a pop-up menu.
  - Check verification condition (same as double-click)
  - Show variable values that invalidate condition.
  - Print relevant program information (e.g. invariant).
  - Print verification condition itself.
  - Apply SMT solver for faster checking (see menu “SMT”).

Example: is loop invariant preserved?

```
th閚or _summation_0_LoopOp3(n:number)
requires n \geq 0;
<=> \forall s:result, i:index. (((s = \left( \sum j : \text{number} \; \text{with} \; (1 \leq j) \land (j \leq (i-1)). j \right))
\land (1 \leq i) \land (i \leq (n+1))))) \land (i \leq n))
\Rightarrow (\text{let } s = s+i \text{ in } (\text{let } i = i+1 \text{ in }
(s = \left( \sum j : \text{number} \; \text{with} \; (1 \leq j) \land (j \leq (i-1)). j \right)))) ;
```

Important: check models with small type sizes.
RISC ProofNavigator: A Theory of Arrays

% constructive array definition
newcontext "arrays2";
% the types
INDEX: TYPE = NAT;
ELEM: TYPE;
ARR: TYPE = [INDEX, ARRAY INDEX OF ELEM];
% error constants
any: ARRAY INDEX OF ELEM;
anyelem: ELEM;
anyarray: ARR;
% a selector operation
content: ARR -> (ARRAY INDEX OF ELEM) =
LAMBDA(a:ARR): a.1;
% the array operations
length: ARR -> INDEX =
LAMBDA(a:ARR): a.0;
new: INDEX -> ARR =
LAMBDA(n:INDEX): (n, any);
put: (ARR, INDEX, ELEM) -> ARR =
LAMBDA(a:ARR, i:INDEX, e:ELEM):
IF i < length(a)
THEN (length(a),
content(a) WITH [i]:=e)
ELSE anyarray
ENDIF;
get: (ARR, INDEX) -> ELEM =
LAMBDA(a:ARR, i:INDEX):
IF i < length(a)
THEN content(a)[i]
ELSE anyelem ENDIF;

Proof of Fundamental Array Properties
% the classical array axioms as formulas to be proved
length1: FORMULA
FORALL(n:INDEX): length(new(n)) = n;
length2: FORMULA
FORALL(a:ARR, i:INDEX, e:ELEM):
i < length(a) => length(put(a, i, e)) = length(a);
get1: FORMULA
FORALL(a:ARR, i:INDEX, e:ELEM):
i < length(a) => get(put(a, i, e), i) = e;
get2: FORMULA
FORALL(a:ARR, i,j:INDEX, e:ELEM):
i < length(a) AND j < length(a) AND
i /= j =>
get(put(a, i, e), j) = get(a, j);

The Verification Conditions
newcontext
"linsearch";
% declaration
% of arrays
a: ARR;
olda: ARR;
x: ELEM;
oldx: ELEM;
i: NAT;
n: NAT;
r: INT;
% declaration
Output: BOOLEAN = olda = a AND oldx = x AND
n = length(a) AND i = 0 AND r = -1;
Input => Invariant(a, x, i, n, r);
B1: FORMULA
Invariant(a, x, i, n, r) AND i < n AND r = -1 AND get(a, i) = x
=> Invariant(a, x, i, n, i);
B2: FORMULA
Invariant(a, x, i, n, r) AND i < n AND r = -1 AND get(a, i) /= x
=> Invariant(a, x, i-1, n, r);
C: FORMULA
Invariant(a, x, i, n, r) AND NOT(i < n AND r = -1)
=> Output;

The Verification Conditions (Contd)
### Termination

**Termination**: \((\text{ARR}, \text{ELEM}, \text{NAT}, \text{NAT}, \text{INT}) \to \text{INT}) = \text{LAMBDA}(a:\ \text{ARR}, \ x:\ \text{ELEM}, \ i:\ \text{NAT}, \ n:\ \text{NAT}, \ r:\ \text{INT}):\
\text{IF } r=-1 \text{ THEN } n-i \text{ ELSE } 0 \text{ ENDIF;}

**T**: \text{FORMULA}

\[ \text{Invariant}(a, x, i, n, r) \Rightarrow \text{Termination}(a, x, i, n, r) \geq 0; \]

**B1**: \text{FORMULA}

\[ \text{Invariant}(a, x, i, n, r) \ \&\& \ i < n \ \&\& \ r = -1 \ \&\& \ \text{get}(a, i) = x \ \&\& \ \text{Termination}(a, x, i, n, r) = N \]
\[ \Rightarrow \text{Invariant}(a, x, i+1, n, r) \ \&\& \ \text{Termination}(a, x, i+1, n, r) < N; \]

**B2**: \text{FORMULA}

\[ \text{Invariant}(a, x, i, n, r) \ \&\& \ i < n \ \&\& \ r = -1 \ \&\& \ \text{get}(a, i) /= x \ \&\& \ \text{Termination}(a, x, i, n, r) = N \]
\[ \Rightarrow \text{Invariant}(a, x, i+1, n, r) \ \&\& \ \text{Termination}(a, x, i+1, n, r) < N; \]

### Abortion

New rules to prevent abortion.

\[
\begin{align*}
\{ \text{false} \} \ & \text{abort} \ {\text{true}} \\
\{ Q[e/x] \land D(e) \} \ & x := e \ {\{ Q \}} \\
\{ Q[a[i \mapsto e]/a] \land D(e) \land D(i) \land 0 \leq i \leq \text{length}(a) \} \ & a[i] := e \ {\{ Q \}}
\end{align*}
\]

- New interpretation of \( \{ P \} \ c \ {\{ Q \}}. 
  - If execution of \( c \) starts in a state, in which property \( P \) holds, then it does not abort and eventually terminates in a state in which \( Q \) holds.
- Sources of abortion.
  - Division by zero.
  - Index out of bounds exception.

\( D(e) \) makes sure that every subexpression of \( e \) is well defined.
## Definedness of Expressions

\[ D(0) = \text{true} \]
\[ D(1) = \text{true} \]
\[ D(x) = \text{true} \]
\[ D(a[i]) = D(i) \land 0 \leq i < \text{length}(a) \]
\[ D(e_1 + e_2) = D(e_1) \land D(e_2) \]
\[ D(e_1 \cdot e_2) = D(e_1) \land D(e_2) \]
\[ D(e_1 / e_2) = D(e_1) \land D(e_2) \land e_2 \neq 0 \]
\[ D(\text{true}) = \text{true} \]
\[ D(\text{false}) = \text{true} \]
\[ D(-b) = D(b) \]

Assumes that expressions have already been type-checked.

## Abortion

Slight modification of existing rules.

\[
P \Rightarrow D(b) \quad \{P \land b\} \quad c_1 \quad \{P \land \neg b\} \quad c_2 \quad \{Q\}
\]
\[
\{P\} \text{if } b \text{ then } c_1 \text{ else } c_2 \quad \{Q\}
\]

\[
P \Rightarrow D(b) \quad \{P \land b\} \quad c \quad \{P \land \neg b\} \Rightarrow Q
\]
\[
\{P\} \text{if } b \text{ then } c \quad \{Q\}
\]

\[
I \Rightarrow (t \geq 0 \land D(b)) \quad \{I \land b \land t = N\} \quad c \quad \{I \land t < N\}
\]
\[
\{I\} \text{while } b \text{ do } c \quad \{I \land \neg b\}
\]

Expressions must be defined in any context.

## Similar modifications of weakest preconditions.

\[
w\text{p}(\text{abort}, Q) = \text{false}
\]
\[
w\text{p}(x := e, Q) = Q[e/x] \land D(e)
\]
\[
w\text{p}(\text{if } b \text{ then } c_1 \text{ else } c_2, Q) =
\]
\[
D(b) \land (b \Rightarrow w\text{p}(c_1, Q)) \land (\neg b \Rightarrow w\text{p}(c_2, Q))
\]
\[
w\text{p}(\text{if } b \text{ then } c, Q) = D(b) \land (b \Rightarrow w\text{p}(c, Q)) \land (\neg b \Rightarrow Q)
\]
\[
w\text{p}(\text{while } b \text{ do } c, Q) = (L_0(Q) \lor L_1(Q) \lor L_2(Q) \lor \ldots)
\]

\[
L_0(Q) = \text{false}
\]
\[
L_{i+1}(Q) = D(b) \land (\neg b \Rightarrow Q) \land (b \Rightarrow w\text{p}(c, L_i(Q)))
\]

\[w\text{p}(c, Q)\] now makes sure that the execution of \(c\) does not abort but eventually terminates in a state in which \(Q\) holds.
Procedure Specifications

- global $g$;
- requires $Pre$;
- ensures $Post$;
- $o := p(i) \{c\}$

### Specification of a procedure $p$ implemented by a command $c$.
- Input parameter $i$, output parameter $o$, global variable $g$.
- Command $c$ may read/write $i$, $o$, and $g$.
- Precondition $Pre$ (may refer to $i, g$).
- Postcondition $Post$ (may refer to $i, o, g, g_0$).
- $g_0$ denotes the value of $g$ before the execution of $p$.

### Proof obligation

$$\{Pre \land i_0 = i \land g_0 = g\} \land \{Post[i_0/i]\}$$

Proof of the correctness of the implementation of a procedure with respect to its specification.

---

Procedure Calls

A call of $p$ provides actual input argument $e$ and output variable $x$.

$$x := p(e)$$

Similar to assignment statement; we thus first give an alternative (equivalent) version of the assignment rule.

- **Original:**
  $$\{D(e) \land Q[e/x]\}$$
  $$x := e$$
  $$\{Q\}$$

- **Alternative:**
  $$\{D(e) \land \forall x': x' = e \Rightarrow Q[x'/x]\}$$
  $$x := e$$
  $$\{Q\}$$

The new value of $x$ is given name $x'$ in the precondition.

---

Example

- **Procedure specification:**
  
  ```plaintext
  global $g$
  requires $g \geq 0 \land i > 0$
  ensures $g_0 = g \cdot i + o \land 0 \leq o < i$
  $$o := p(i) \{o := g \% i; \ g := g/i\}$$
  ```

- **Proof obligation:**
  
  $$\{g \geq 0 \land i > 0 \land i_0 = i \land g_0 = g\}$$
  $$o := g \% i; \ g := g/i$$
  $$\{g_0 = g \cdot i_0 + o \land 0 \leq o < i_0\}$$

A procedure that divides $g$ by $i$ and returns the remainder.

---

Procedure Calls

From this, we can derive a rule for the correctness of procedure calls.

$$\{D(e) \land Pre[e/i] \land \forall x', g': Post[e/i, x', g/g_0, g'/g] \Rightarrow Q[x'/x, g'/g]\}$$

$$x := p(e)$$

$$\{Q\}$$

- **$Pre[e/i]$** refers to the values of the actual argument $e$ (rather than to the formal parameter $i$).
- **$x'$ and $g'$** denote the values of the vars $x$ and $g$ after the call.
- **$Post[\ldots]$** refers to the argument values before and after the call.
- **$Q[x'/x, g'/g]$** refers to the argument values after the call.

Modular reasoning: rule only relies on the specification of $p$, not on its implementation.
Corresponding Predicate Transformers

\[
\text{wp}(x = p(e), Q) = \\
D(e) \land \text{Pre}[e/i] \land \\
\forall x', g' : \\
P[\underbrace{e[i/x, g_0/g, g'/g]}_{Q[x'/x, g'/g]}.]
\]

Explicit naming of old/new values required.

Example

Procedure specification:

\[
\begin{align*}
global & \quad g \\
\text{requires} & \quad g \geq 0 \land i > 0 \\
\text{ensures} & \quad g_0 = g \cdot i + o \land 0 \leq o < i \\
o & = p(i) \quad \{ \quad o := g \% i; \quad g := g / i \quad \}
\end{align*}
\]

Procedure call:

\[
\begin{align*}
\{ & g \geq 0 \land g = N \land b \geq 0 \\
& x = p(b+1) \\
& \{ g \cdot (b+1) \leq N < (g + 1) \cdot (b+1) \}
\end{align*}
\]

To be proved:

\[
\begin{align*}
g \geq 0 \land g = N \land b \geq 0 \Rightarrow \\
D(b+1) \land g \geq 0 \land b + 1 > 0 \land \\
\forall x', g' : \\
g = g' \cdot (b + 1) + x' \land 0 \leq x' < b + 1 \Rightarrow \\
g' \cdot (b + 1) \leq N < (g' + 1) \cdot (b + 1)
\end{align*}
\]