Specifying and Verifying Programs (Part 1)

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

- State Relations: \( c : [P \Rightarrow Q]^{x \ldots} \)
  - 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.

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

- 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

\[
P \Rightarrow P' \quad \{P'\} c \{Q'\} \quad Q' \Rightarrow Q
\]

- Logical derivation: \(\frac{A_1 \quad A_2}{B}\)
  - 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

\[
\begin{array}{l}
\{P\} \text{skip} \{P\} \\
\{P\} \text{abort} \{\text{false}\}
\end{array}
\]

- The \text{skip} command does not change the state; if \(P\) holds before its execution, then \(P\) thus holds afterwards as well.
- The \text{abort} command aborts execution and thus trivially satisfies partial correctness.
  - Axiom implies \(\{P\} \text{abort} \{Q\}\) 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.
    \[
    \begin{array}{l}
    \{x + 3 < 5\} \quad x := x + 3 \quad \{x < 5\} \\
    \{x < 2\} \quad x := x + 3 \quad \{x < 5\}
    \end{array}
    \]
**Array Assignments**

\{Q[a[i \mapsto 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 \(a[i \mapsto e]\) ("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 "\(a := a[i \mapsto e]\)".

\{a[i \mapsto x][1] > 0\} a[i] := x \{a[1] > 0\}

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

**Command Sequences**

\{P\} c_1 \{R\} \{R\} \varnothing \{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\} y := y - 1 \{x + y > 0\} \{x + y > 0\}
\{x + y - 1 > 0\} y := y - 1; x := x + y \{x > 0\}

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

**Conditionals**

\{P \land b\} c_1 \{Q\} \{P \land \neg b\} c_2 \{Q\}

- \{P\} if \(b\) then \(c_1\) else \(c_2\) \{Q\}

\{P \land b\} c \{Q\} \{P \land \neg b\} \Rightarrow Q

- \{P\} if \(b\) then \(c\) \{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 \neq 0 \land x \geq 0\} y := x \{y > 0\} \{x \neq 0 \land x \geq 0\} y := -x \{y > 0\}
\{x \neq 0\} if x \geq 0 then y := x else y := -x \{y > 0\}

- Problem: find suitable \(R\).
Loops

\{true\} loop \{false\} \{I \land b\} c \{I\} \{I\} \{I\}
\{I\} \{I\} \{I\} \{I\} \{I\} \{I\} \{I\} \{I\} \{I\} \{I\} \{I\}

**Interpretation:**
- The loop command does not terminate and thus trivially satisfies partial correctness.
- Axiom implies \{P\} loop \{Q\} for arbitrary \(P, Q\).
- If it is the case that \(I\) holds before the execution of the 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 while-loop does not have arbitrary pre/post-conditions \(P, Q\).
In practice, we combine this rule with the strengthening/weakening-rule.

Wolfgang Schreiner http://www.risc.jku.at 13/70

---

Loops (Generalized)

\(P \Rightarrow I\) \{I \land b\} c \{I\} \{I \land \neg b\} \Rightarrow Q \{P\} \{Q\}

**Interpretation:**
- To show that, if before the execution of a while-loop the property \(P\) holds, after its termination the property \(Q\) holds, it suffices to show for some property \(I\) (the loop invariant) that
  - \(I\) holds before the loop is executed (i.e. that \(P\) implies \(I\)),
  - if \(I\) holds when the loop body is entered (i.e. if also \(b\) holds), that after the execution of the loop body \(I\) still holds,
  - when the loop terminates (i.e. if \(b\) does not hold), \(I\) implies \(Q\).
- **Problem:** find appropriate loop invariant \(I\).
  - Strongest relationship between all variables modified in loop body.
The calculus itself does not indicate how to find suitable loop invariant.

Wolfgang Schreiner http://www.risc.jku.at 14/70

---

Example

\(I : \equiv s = \sum_{j=1}^{i-1} j \land 1 \leq i \leq n + 1\)
\(\{n \geq 0 \land s = 0 \land i = 1\} \Rightarrow I\)
\(\{I \land i \leq n\} s := s + i; i := i + 1\ \{I\}\)
\(\{I \land i \leq n\} \Rightarrow s = \sum_{j=1}^{i-1} j\)
\(\{n \geq 0 \land s = 0 \land i = 1\} \text{ while } i \leq n \text{ do } (s := s + i; i := i + 1)\ \{s = \sum_{j=1}^{n} j\}\)

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

Wolfgang Schreiner http://www.risc.jku.at 15/70

---

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

Wolfgang Schreiner http://www.risc.jku.at 16/70
A Program Verification

- Verification of the following Hoare triple:
  \[ \{ \text{Input} \} \text{ while } i \leq n \text{ do } (s := s + i; i := i + 1) \{ \text{Output} \} \]
- Auxiliary predicates:
  \begin{align*}
  \text{Input} & : \iff n \geq 0 \land s = 0 \land i = 1 \\
  \text{Output} & : \iff s = \sum_{j=1}^{n} j \\
  \text{Invariant} & : \iff s = \sum_{j=1}^{n} j \land 1 \leq i \leq n + 1
  \end{align*}
- Verification conditions:
  \begin{align*}
  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 \not\leq n \Rightarrow \text{Output}
  \end{align*}

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. j;
{ 
  var s:result := 0;
  var i:index := 1;
  while i \leq n do 
    invariant s = \sum_{j=1}^{n} j \land 1 \leq j \leq i-1. j;
    invariant 1 \leq 1 \land 1 \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:
\[ \{ \text{olda = a \land oldx = x} \} \]
\begin{align*}
  i & := 0; r := -1; n = |a| \\
  \text{while } i < n \land r = -1 \text{ do } \\
  & \text{if } a[i] = x \\
  & \quad \text{then } r := i \\
  & \quad \text{else } i := i + 1
  \end{align*}
\begin{align*}
  \{ & a = \text{olda \land x = oldx} \land \\
  & ((r = -1 \land \forall i: 0 \leq i < |a| \Rightarrow a[i] \not= x) \lor \\
  & (0 \leq r < |a| \land a[r] = x \land \forall i: 0 \leq i < r \Rightarrow a[i] \not= x)) \}
\end{align*}

\[ \text{Invariant} : \iff \text{olda = a \land oldx = x \land n = |a|} \land \\
0 \leq i \leq n \land \forall j: 0 \leq j < i \Rightarrow a[j] \not= x \land \\
(r = -1 \lor (r = i \land i < n \land a[r] = x)) \]

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 Program Execution

val N: N; val M: N;
type index = Z[-1,N]; type elem = N[M]; type array = Array[N,elem];

proc search(a:array, x:elem): index
ensures (result = -1 ∧ ∀ i: index. 0 ≤ i ∧ i < N ⇒ a[i] ≠ x) ∨
(0 ≤ result ∧ result < N ∧
 a[result] = x ∧ ∀ i: index. 0 ≤ i ∧ i < result ⇒ a[i] ≠ x);
{ 
 var i:index = 0;
 var r:index = -1;
 while i < N ∧ r = -1 do
 invariant 0 ≤ i ∧ i ≤ N ∧ ∀ j: index. 0 ≤ j ∧ j < i ⇒ a[j] ≠ x;
 invariant r = -1 ∨ (r = i ∧ i < N ∧ a[r] = x);
 { if a[i] = x
then r := i;
 else i := i+1;
 } 
} return r;

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

RISCAL: Checking Verification Conditions

pred Input(i:index, r:index) ⇔ i = 0 ∧ r = -1;
pred Output(a:array, x:elem, i:index, r:index) ⇔
(0 ≤ result ∧ result < N ∧
 a[result] = x ∧ ∀ i: index. 0 ≤ i ∧ i < result ⇒ a[i] ≠ x);
{ 
 var i:index = 0;
 var r:index = -1;
 while i < N ∧ r = -1 do
 invariant 0 ≤ i ∧ i ≤ N ∧ ∀ j: index. 0 ≤ j ∧ j < i ⇒ a[j] ≠ x;
 invariant r = -1 ∨ (r = i ∧ i < N ∧ a[r] = x);
 { if a[i] = x
then r := i;
 else i := i+1;
 } 
} return r;

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

The Verification Conditions

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

Output :⇔ a = olda ∧ x = oldx ∧
((r = -1 ∧ ∀ i: index. 0 ≤ i < length(a) ⇒ a[i] ≠ x) ∨
(0 ≤ r < length(a) ∧ a[r] = x ∧ ∀ i: index. 0 ≤ i < r ⇒ a[i] ≠ x))

Invariant :⇔ olda = a ∧ oldx = x ∧ n = |a| ∧
0 ≤ i ≤ n ∧ ∀ j: index. 0 ≤ j < i ⇒ a[j] ≠ x ∧
(r = -1 ∨ (r = i ∧ i < n ∧ a[r] = x))

$A : ⇔ Input ⇒ Invariant$
$B_1 : ⇔ Invariant ∧ i < n ∧ r = -1 ∧ a[i] = x ⇒ Invariant[i/r]
B_2 : ⇔ 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.

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
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.

\[
\begin{align*}
\{P\} & : x := x+1; \\
\{P\} & : y := 2x; \\
\{P\} & : z := x+y \\
\{P\} & : z = 15
\end{align*}
\]

\[
P \Rightarrow x = 4
\]

Weakest Preconditions

The weakest precondition of each program construct.

- \(wp(\text{skip}, Q) = Q\)
- \(wp(\text{abort}, Q) = \text{true}\)
- \(wp(x := e, Q) = Q[e/x]\)
- \(wp(c_1; c_2, Q) = wp(c_1, wp(c_2, Q))\)
- \(wp(\text{if } b \text{ then } c_1 \text{ else } c_2, Q) = (b \Rightarrow wp(c_1, Q)) \land (\neg b \Rightarrow wp(c_2, Q))\)
- \(wp(\text{while } b \text{ do } c, Q) = \ldots\)

Loops represent a special problem (see later).

Weakest Preconditions

A calculus for “backward reasoning” (E.W. Dijkstra).
- **Predicate transformer wp**
  - Function \(wp\) that takes a command \(c\) and a postcondition \(Q\) and returns a precondition.
  - Read \(wp(c, Q)\) as “the weakest precondition of \(c\) w.r.t. \(Q\)”. \(wp(c, Q)\) is a **precondition** for \(c\) that ensures \(Q\) as a postcondition.
  - Must satisfy \(\{wp(c, Q)\} c \ {Q}\).
  - \(wp(c, Q)\) is the **weakest** such precondition.
  - Take any \(P\) such that \(\{P\} c \ {Q}\).
  - Then \(P \Rightarrow wp(c, Q)\).

**Consequence**: \(\{P\} \ c \ \{Q\} \iff (P \Rightarrow wp(c, Q))\)
- We want to prove \(\{P\} \ c \ {Q}\).
- We may prove \(P \Rightarrow wp(c, Q)\) instead.

Verification is reduced to the calculation of weakest preconditions.

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 \(e[x_0/x]\).

\[
\begin{align*}
\{x \geq 0 \land y = a\} & : x := x + 1 \\
\{\exists x_0 : x_0 \geq 0 \land x = x_0 + 1\} & : (\iff (\exists x_0 : x_0 \geq 0 \land x = x_0 + 1) \land y = a) \\
(\iff x > 0 \land y = a) & : (\iff x > 0 \land y = a)
\end{align*}
\]
**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.

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

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

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

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

**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$_{i+1} = \text{if } b \text{ then } (c; \text{if}_i)$
Example

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

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”:
  - \( \forall i \in \mathbb{N} : \text{wp(while } b \text{ do } c, Q) \Rightarrow L_i(Q) \).
  - \( \forall P : (\forall i \in \mathbb{N} : P \Rightarrow L_i(Q)) \Rightarrow (P \Rightarrow \text{wp(while } b \text{ do } c, Q)) \).
- 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\} while \( b \) 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\} while \( b \) 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.

Falsification is possible by use of approximation \( L_i \), but verification is not.

Example

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

- Loop body \( c \) only modifies variables \( x, \ldots \)
- Loop is annotated with invariant \( L \).
  - May refer to new values \( x, \ldots \) of variables after every iteration.
  - May refer to original values \( \text{olds}, \ldots \) when loop started execution.
- Generated verification condition ensures:
  1. \( L \) holds in the initial state of the loop.
  2. \( L \) is preserved by the execution of the loop body \( c \).
  3. When the loop terminates, \( L \) ensures postcondition \( Q \).
- This precondition is only “weakest” relative to the invariant.

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

Termination

Hoare rules for loop and while are replaced as follows:

\[
\begin{align*}
\{\text{false}\} \text{ loop } \{\text{false}\} & \quad \Rightarrow t \geq 0 \quad \{l \land b \land t = N\} \quad c \quad \{l \land t < N\} \\
\{l\} \text{ while } b \text{ do } c \quad \{l \land \neg b\} & \quad \Rightarrow p \quad \Rightarrow t \geq 0 \quad \{l \land b \land t = N\} \quad c \quad \{l \land t < N\} \quad (l \land \neg b) \Rightarrow q \quad \{p\} \text{ while } b \text{ do } c \quad \{q\}
\end{align*}
\]

- New interpretation of \(\{P\} \quad c \quad \{Q\}\):
  - If execution of \(c\) starts in a state where \(P\) holds, then execution terminates in a state where \(Q\) holds, unless it aborts.
  - Non-termination is ruled out, abortion not (yet).
  - The \texttt{loop} command thus does not satisfy total correctness.
- Termination measure \(t\) (term type-checked to denote an integer).
  - Becomes smaller by every iteration of the loop.
  - But does not become negative.
  - Consequently, the loop must eventually terminate.

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

Example

\[
l :\iff s = \sum_{j=1}^{i-1} j \land 1 \leq i \leq n + 1 \\
t := n - i + 1
\]

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

{\(n \geq 0 \land i = 1 \land s = 0\)} while \(i \leq n\) do \(s := s + i; i := i + 1\) \(\{s = \sum_{j=1}^{i} j\}\)

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

Termination in RISCAL

while \(i \leq n\) do
  invariant \(s = \sum_{j=1}^{\min(i, n)} j\land i \leq j \leq i+1\), \(j\);
  invariant \(i \leq 1 \land i \leq n+1\);
  decreases \(n+1-i\);
  \}
  \} = s+i;
  i := i+1;

fun Termination(n:number, s:result, i:index): number = n+1-i;
  theorem T(n:number, s:result, i:index) \iff
    Invariant(n, s, i) \Rightarrow Termination(n, s, i) \geq 0;
  theorem B(n:number, s:result, i:index) \iff
    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);
**Termi nation in RISCAL**

\[
\text{while } i < N \land r = -1 \text{ do}
\]
\[
\begin{align*}
\text{invariant } & 0 \leq i \land i \leq N; \\
\text{invariant } & \forall j:\text{index. } 0 \leq j \land j < i \Rightarrow a[j] \neq x; \\
\text{invariant } & r = -1 \lor (r = 1 \land i < N \land a[r] = x); \\
\text{decreases if } & r = -1 \text{ then } N-i \text{ else } 0; \\
\end{align*}
\]

\[
\begin{align*}
\{ & \text{if } a[i] = x \\
& \text{ then } r := i; \\
& \text{ else } i := i+1; \\
\}
\]

\[
\text{fun } \text{Termination}(a:\text{array}, x:\text{elem}, i:\text{index}, r:\text{index}): \text{index} =
\]
\[
\begin{align*}
& \text{if } r = -1 \text{ then } N-i \text{ else } 0; \\
& \text{theorem } T(a:\text{array}, x:\text{elem}, i:\text{index}, r:\text{index}) \Leftrightarrow \\
& \text{Invariant}(a, x, i, r) \Rightarrow \text{Termination}(a, x, i, r) \geq 0; \\
& \text{theorem } B1(a:\text{array}, x:\text{elem}, i:\text{index}, r:\text{index}) \Leftrightarrow \\
& \text{Invariant}(a, x, i, r) \land i < N \land r = -1 \land a[i] = x \Rightarrow \\
& \text{Termination}(a, x, i, i) \land \\
& \text{theorem } B2(a:\text{array}, x:\text{elem}, i:\text{index}, r:\text{index}) \Rightarrow ...
\end{align*}
\]

**Example**

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

**Weakest Preconditions for Loops**

\[
\begin{align*}
\text{wp}(\text{loop}, Q) &= \text{false} \\
\text{wp}(\text{while } b \text{ do } c, Q) &= L_0(Q) \lor L_1(Q) \lor L_2(Q) \lor ...
\end{align*}
\]

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

- 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: \( \{P\} \ c \ \{Q\} \iff (P \Rightarrow \text{wp}(c, Q)) \)
- Now for total correctness interpretation of Hoare calculus.
- Preserves alternative view: \( L_i(Q) \Leftrightarrow \text{wp}(if_i, Q) \)
  - \( if_0 = \text{loop} \)
  - \( if_{i+1} = \text{if } b \text{ then } (c; if_i) \)

We can only compute a stronger approximation \( L_i(Q) \).

We want to prove \( \{P\} \ c \ \{Q\} \).

- It suffices to prove \( P \Rightarrow \text{wp}(\text{while } b \text{ do } c, Q) \).
- It thus also suffices to prove \( P \Rightarrow L_i(Q) \).
- If proof fails, we may try the easier proof \( P \Rightarrow L_{i+1}(Q) \)

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

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

- Loop body c only modifies variables \( x, \ldots \).
- Loop is annotated with termination measure (term) \( t \).
- May refer to new values \( x, \ldots \) 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 here any well-founded ordering may be used as the domain of \( t \).

Example

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

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

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

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.

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?

```plaintext
s = (∑j:number with (1 ≤ j) ∧ (j ≤ (i-1)). j)
```

```plaintext
theorem _summation_0_LoopOp3(n:number)
requires n ≥ 0:
⇔ ∀Vs:result, i:index. (((s = (∑j:number with (1 ≤ j) ∧ (j ≤ (i-1)). j)) ∧ (1 ≤ i) ∧ (i ≤ (n+1)))) ∧ (i ≤ n) ⇒ 
(let s = s+i in (let i = i+1 in 
(s = (∑j:number with (1 ≤ j) ∧ (j ≤ (i-1)). j)))));
```

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.
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;

The Verification Conditions

newcontext "linsearch";
% declaration
% of arrays
... a: ARR;
olda: ARR;
x: ELEM;
oldx: ELEM;
i: NAT;
% declaration
% of inputs
Input: BOOLEAN = olda = a AND oldx = x AND
n = length(a) AND i = 0 AND r = -1;
% declaration
% of outputs
Output: BOOLEAN = a = olda AND
((r = -1 AND
  (FORALL(j:NAT): j < length(a) =>
   get(a,j) /= x)) OR
  (0 <= r AND r < length(a) AND get(a,r) = x AND
   (FORALL(j:NAT):
    j < r =>
    get(a,j) /= x)));
% declaration
% of invariants
Invariant: (ARR, ELEM, NAT, NAT, INT) -> BOOLEAN =
  LAMBDA(a: ARR, x: ELEM, i: NAT, n: NAT, r: INT):
  olda = a AND oldx = x AND
  n = length(a) AND i <= n AND
  (FORALL(j:NAT): j < i =>
   get(a,j) /= x) AND
  (r = -1 OR (r = i AND i < n AND get(a,r) = x));

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 (Contd)

... A: FORMULA
  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 Proofs

A:
- [bca]: expand Input, Invariant
  - [fuo]: scatter
  - [bxg]: proved (CVCL)

(2 user actions)

B1:
- [p1b]: expand Invariant
  - [f6]: proved (CVCL)

(1 user action)

B2:
- [q1b]: expand Invariant in 6kv
  - [six]: scatter
  - [a1y]: auto
  - [och]: proved (CVCL)
- [b1y]: proved (CVCL)
- [c1y]: proved (CVCL)
- [d1y]: proved (CVCL)
- [e1y]: proved (CVCL)

(3 user actions)

C:
- [dca]: expand Invariant, Output in zfg
  - [ivy]: scatter
  - [dou]: auto
  - [uoc]: proved (CVCL)
  - [ecu]: split peg
  - [kel]: proved (CVCL)
  - [lei]: scatter
  - [tvn]: auto
  - [lsap]: proved (CVCL)
  - [fcu]: auto
  - [bit]: proved (CVCL)
  - [gou]: proved (CVCL)

(6 user actions)

Termination

Termination: (ARR, ELEM, NAT, NAT, INT) -> INT =
LAMBDA(a: ARR, x: ELEM, i: NAT, n: NAT, r: INT):
  IF r=-1 THEN n-i ELSE 0 ENDIF;

T: FORMULA
Invariant(a, x, i, n, r) => Termination(a, x, i, n, r) >= 0;

B1: FORMULA
Invariant(a, x, i, n, r) AND i < n AND r = -1 AND get(a,i) = x AND
Termination(a, x, i, n, r) = N
  => Invariant(a,x,i,n,i) AND Termination(a,x,i,n,i) < N;

B2: FORMULA
Invariant(a, x, i, n, r) AND i < n AND r = -1 AND get(a,i) /= x AND
Termination(a, x, i, n, r) = N
  => Invariant(a,x,i+1,n,r) AND Termination(a,x,i+1,n,r) < N;

Abortion

New rules to prevent abortion.

{-false} abort {true}
{Q[e/x] ∧ D(e)} x := e {Q}
{Q[a[i ↦→ e]/a] ∧ D(e) ∧ D(i) ∧ 0 ≤ i < length(a)} a[i] := e {Q}

- 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.
Abortion

Slight modification of existing rules.

\[ P \Rightarrow D(b) \{P \land b\} c_1 \{Q\} \{P \land \neg b\} c_2 \{Q\} \]

\[ \{P\} \text{if } b \text{ then } c_1 \text{ else } c_2 \{Q\} \]

\[ P \Rightarrow D(b) \{P \land b\} c \{Q\} \{P \land \neg b\} \Rightarrow Q \]

\[ \{P\} \text{if } b \text{ then } c \{Q\} \]

\[ I \Rightarrow (t \geq 0 \land D(b)) \{I \land b \land t = N\} c \{I \land t < N\} \]

\[ \{I\} \text{while } b \text{ do } c \{I \land \neg b\} \]

Expressions must be defined in any context.

Abortion

Similar modifications of weakest preconditions.

\[ wp(abort, Q) = \text{false} \]

\[ wp(x := e, Q) = Q[e/x] \land D(e) \]

\[ wp(\text{if } b \text{ then } c_1 \text{ else } c_2, Q) = \]

\[ D(b) \land (b \Rightarrow wp(c_1, Q)) \land (\neg b \Rightarrow wp(c_2, Q)) \]

\[ wp(\text{if } b \text{ then } c, Q) = D(b) \land (b \Rightarrow wp(c, Q)) \land (\neg b \Rightarrow Q) \]

\[ wp(\text{while } b \text{ do } c, Q) = (L_0(Q) \lor L_1(Q) \lor L_2(Q) \lor \ldots) \]

\[ L_0(Q) = \text{false} \]

\[ L_{i+1}(Q) = D(b) \land (\neg b \Rightarrow Q) \land (b \Rightarrow wp(c, L_i(Q))) \]

\[ wp(c, Q) \text{ now makes sure that the execution of } c \text{ does not abort but} \]

\[ \text{eventually terminates in a state in which } Q \text{ holds.} \]
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, g₀).
  - g₀ denotes the value of g before the execution of p.

- Proof obligation
  \{ \text{Pre} \wedge i₀ = i \wedge g₀ = g \} \text{ c } \{ \text{Post}[i₀/i] \}

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

Example

- Procedure specification:
  ```
  \begin{align*}
  \text{global } g &; \\
  \text{requires } g \geq 0 \wedge i > 0 &; \\
  \text{ensures } g₀ = g \cdot i + o \wedge 0 \leq o < i &; \\
  o &:= p(i) \{ o := g \% i; \quad g := g / i \}
  \end{align*}
  ```

- Proof obligation:
  ```
  \{ g \geq 0 \wedge i > 0 \wedge i₀ = i \wedge g₀ = g \} \\
  o := g \% i; \quad g := g / i \\
  \{ g₀ = g \cdot i₀ + o \wedge 0 \leq o < i₀ \}
  ```

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

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) \wedge Q[e/x] \} \\
  x := e \\
  \{ Q \}
  ```

- Alternative:
  ```
  \{ D(e) \wedge \forall x': x' = e \Rightarrow Q[x'/x] \} \\
  x := e \\
  \{ Q \}
  ```

The new value of x is given name x' in the precondition.
Corresponding Predicate Transformers

wp(x = p(e), Q) =
\[ D(e) \land \text{Pre}[e/i] \land \forall x', g' : \]
\[ \text{Post}[e/i, x'/o, g/g_0, g'/g] \Rightarrow Q[x'/x, g'/g] \]

sp(P, x = p(e)) =
\[ \exists x_0, g_0 : \]
\[ P[x_0/y, g_0/g] \land \]
\[ (\text{Pre}[e[x_0/x, g_0/g]/i, g_0/g]) \Rightarrow \text{Post}[e[x_0/x, g_0/g]/i, x/o]) \]

Explicit naming of old/new values required.

Example

Procedure specification:

\begin{itemize}
  \item global \( g \)
  \item requires \( g \geq 0 \land i > 0 \)
  \item ensures \( g_0 = g \cdot i + o \land 0 \leq o < i \)
  \item \( o = p(i) \) \{ \( o := g \% i; \ g := g / i \) \}
\end{itemize}

Procedure call:

\begin{itemize}
  \item \( \{ g \geq 0 \land g = N \land b \geq 0 \} \)
  \item \( x = p(b + 1) \)
  \item \( \{ g \cdot (b + 1) \leq N < (g + 1) \cdot (b + 1) \} \)
\end{itemize}

To be proved:

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