Invariants, Total Correctness
Tutorial 3

Jonathan Cederberg
Oct. 29th 2010

1 An Example

\{ Q : a \geq 0 \land b \geq 0 \}
\begin{align*}
z, x, y &:= 0, a, b \\
\{ \text{inv } P : (x \geq 0) \land (z + x \cdot y = a \cdot b) \} \\
\{ \text{bound } t : x \} \\
\textbf{do} & \quad x \geq 1 \rightarrow \textbf{if} \quad \text{odd}(x) \rightarrow z := z + y \\
& \quad \textbf{fi}; \\
& \quad x, y := x \div 2, 2 \cdot y \\
\textbf{od} \\
\{ R : z = a \cdot b \}
\end{align*}

Prove the following points:

1. \((a \geq 0) \land (b \geq 0) \Rightarrow \wp("z, x, y := 0, a, b", P)\)
2. \(P \land (x \geq 1) \Rightarrow \wp("\text{IF; } x, y := x \div 2, 2 \cdot y", P)\)
3. \(P \land \neg(x \geq 1) \Rightarrow (z = a \cdot b)\)
4. \(P \land (x \geq 1) \Rightarrow t > 0\)
5. \(P \land (x \geq 1) \Rightarrow \wp("t_1 := t; \text{IF; } x, y := x \div 2, 2 \cdot y", t < t_1)\)

1.1 Proof of 1

Assume \(a \geq 0\)
Assume \(b \geq 0\)

\[ \wp("z, x, y := 0, a, b", (x \geq 0) \land (z + x \cdot y = a \cdot b)) \]
\[ \quad = \{ \text{Definition of multiple assignment } \} \]
\[ \quad = (a \geq 0) \land (0 + a \cdot b = a \cdot b) \]
\[ \quad = \{ \text{Arithmetic and and-simplification } \} \]
\[ \quad a \geq 0 \]
= \{ \text{Assumption: } \text{“} a \geq 0 \text{”} \ \} \\

\[ T \ \square \]

1.2 Proof of 2

To prove “P ∧ (x ≥ 1) ⇒ wp (“IF; x, y := x ÷ 2, 2 * y”, P)” directly is horrible. Here, we need to break it down. We know that the alternative command theorem allows us to do this, but we cannot apply it directly.

However, it can serve as inspiration. Let “P’ = wp (“x, y := x ÷ 2, 2 * y”, P)” and prove the following lemmas:

1. P ∧ (x ≥ 1) ⇒ odd(x) ∨ even(x)
2. P ∧ (x ≥ 1) ∧ odd(x) ⇒ wp (“z := z + y”, P’)
3. P ∧ (x ≥ 1) ∧ even(x) ⇒ wp (“skip”, P’)
4. p ⇒ (q_1 ∧ q_2 ∧ q_3) = (p ⇒ q_1) ∧ (p ⇒ q_2) ∧ (p ⇒ q_3)

1.2.1 Proof of lemma 1

Assume

x ≥ 0

Assume

z + x * y = a * b

Assume

x ≥ 1

odd(x) ∨ even(x)

\[ = \{ \text{Arithmetic} \} \]

\[ T \ \square \]

1.2.2 Proof of lemma 2

Assume

x ≥ 0

Assume

z + x * y = a * b

Assume

x ≥ 1

Assume

odd(x)

wp (“z := z + y”, P’)

\[ = \{ \text{Definition of } P' \} \]

wp (“z := z + y”, wp (“x, y := x ÷ 2, 2 * y”, P))

\[ = \{ \text{Definition of } P \} \]

wp(z := z + y, wp (“x, y := x ÷ 2, 2 * y”, x ≥ 0 ∧ z + x * y = a * b))
\[ wp\left(z := z + y, \quad \frac{x}{2} \geq 0 \land z + \left(\frac{x}{2}\right) \cdot 2 \cdot y = a \cdot b\right) \]

= \{ Definition of multiple assignment \}
\[ wp\left(x := \frac{x}{2}, \frac{2}{2} \cdot y = a \cdot b\right) \]

= \{ Definition of multiple assignment \}
\[ (x \div 2 \geq 0) \land (z + y + (x \div 2) \cdot 2 \cdot y = a \cdot b) \]

= \{ Conditional Substitution: “odd(x)” and arithmetic: “odd(x) ⇒ (x \div 2) = (x - 1)\div 2” \}
\[ ((x - 1)\div 2 \geq 0) \land (z + y + ((x - 1)\div 2) \cdot 2 \cdot y = a \cdot b) \]

= \{ Arithmetic: “(x\div 2 \geq 0) = (x \geq 0)” \}
\[ ((x - 1) \geq 0) \land (z + y + ((x - 1)\div 2) \cdot 2 \cdot y = a \cdot b) \]

= \{ Arithmetic \}
\[ (x \geq 1) \land (z + y + (x - 1) \cdot y = a \cdot b) \]

= \{ Arithmetic \}
\[ (x \geq 1) \land (z + x \cdot y = a \cdot b) \]

= \{ Assumptions: “x \geq 1” and “z + x \cdot y = a \cdot b” \}
\[ T \land T \]

= \{ and-simplification \}
\[ T \]

\[ \square \]

1.2.3 Proof of lemma 3

Assume \( x \geq 0 \)
Assume \( z + x \cdot y = a \cdot b \)
Assume \( x \geq 1 \)
Assume \( even(x) \)

\[ wp\left(“skip”, P’\right) \]

= \{ Definition of \( P’ \) \}
\[ wp\left(“skip”, wp\left(x, y := x \div 2, 2 \cdot y”, P\right)\right) \]

= \{ Definition of \( P \) \}
\[ wp\left(“skip”, wp\left(“x, y := x \div 2, 2 \cdot y”, \quad \frac{x}{2} \geq 0 \land z + x \cdot y = a \cdot b\right)\right) \]

= \{ Definition of multiple assignment \}
\[ wp\left(“skip”, \quad z + \left(\frac{x}{2}\right) \cdot 2 \cdot y = a \cdot b\right) \]

= \{ Definition of \( skip \) \}
\[ x \div 2 \geq 0 \land z + (x \div 2) \cdot 2 \cdot y = a \cdot b \]

= \{ Conditional Substitution: : “even(x)” and “even(x) ⇒ (x \div 2 = x/2)” \}
\[ x/2 \geq 0 \land z + (x/2) \cdot 2 \cdot y = a \cdot b \]

= \{ Arithmetic: “2 \cdot (x/2) = x” \}
\[ x/2 \geq 0 \land z + x \cdot y = a \cdot b \]
= \{ \text{Arithmetic: } \text{“}(x/2 \geq 0) = (x \geq 0)\text{”} \} \\
x \geq 0 \land z + x \ast y = a \ast b \\
= \{ \text{Assumptions: } “x \geq 0” \text{ and } “z + x \ast y = a \ast b” \text{ and and-simplification } \} \\
T \quad \Box

1.2.4 Proof of lemma 4

Exercise.

1.2.5 Main proof

\begin{align*}
P \land (x \geq 1) & \Rightarrow \text{wp(“IF; } x, y := x \div 2, 2 \ast y”, P) \\
= & \{ \text{Definition of Sequential Composition } \} \\
P \land (x \geq 1) & \Rightarrow \text{wp(“IF”, wp(“x, y := x \div 2, 2 \ast y”, P))} \\
= & \{ \text{Definition of } P’ \} \\
P \land (x \geq 1) & \Rightarrow \text{wp(“IF”, } P’) \\
= & \{ \text{Definition of Alternative Command } \} \\
P \land (x \geq 1) & \Rightarrow ((\text{odd}(x) \lor \text{even}(x)) \land (\text{odd}(x) \Rightarrow \text{wp(“z := z + y”, } P’)) \land (\text{even}(x) \Rightarrow \text{wp(“skip”, } P’)) \\
= & \{ \text{Lemma 4} \} \\
(P \land (x \geq 1) & \Rightarrow (\text{odd}(x) \lor \text{even}(x)) \land (P \land (x \geq 1) \Rightarrow (\text{odd}(x) \Rightarrow \text{wp(“z := z + y”, } P’)) \land (P \land (x \geq 1) \Rightarrow (\text{even}(x) \Rightarrow \text{wp(“skip”, } P’)) \\
= & \{ \text{Shunting } \} \\
(P \land (x \geq 1) & \Rightarrow (\text{odd}(x) \lor \text{even}(x)) \land (P \land (x \geq 1) \land \text{odd}(x) \Rightarrow \text{wp(“z := z + y”, } P’)) \land (P \land (x \geq 1) \land \text{even}(x) \Rightarrow \text{wp(“skip”, } P’)) \\
= & \{ \text{Lemma 1,2,3} \} \\
T \land T \land T & \\
= & \{ \text{and-simplification } \} \\
T & \quad \Box
\end{align*}

1.3 Proof of 3

Assume \( x \geq 0 \) \\
Assume \( z + x \ast y = a \ast b \) \\
Assume \( \neg(x \geq 1) \)

\( z = a \ast b \)
\[ z = z + x \times y \]

1.4 Proof of 4

Assume \( x \geq 0 \)
Assume \( z + x \times y = a \times b \)
Assume \( x \geq 1 \)

\[ t > 0 \]
\[ = \left\{ \text{Definition of } t \right\} \]
\[ x > 0 \]
\[ = \left\{ \text{Arithmetic} \right\} \]
\[ x \geq 1 \]
1.5 Proof of 5

Assume \( x \geq 0 \)
Assume \( z + x \cdot y = a \cdot b \)
Assume \( x \geq 1 \)

\[
wp\left( t_1 := t; \text{IF}; x, y := x \div 2, 2 \cdot y'', t < t_1 \right)
\]
\[
= \begin{cases} 
\text{Definition of } t \\
wp\left( t_1 := x; \text{IF}; x, y := x \div 2, 2 \cdot y'', x < t_1 \right) \\
\text{Definition of sequential composition} \\
wp\left( t_1 := x'', wp\left( \text{IF}; wp\left( x, y := x \div 2, 2 \cdot y'', x < t_1 \right) \right) \right) \\
\text{Definition of multiple assignment} \\
wp\left( t_1 := x'', wp\left( \text{IF}; wp\left( \text{skip}, x \div 2 < t_1 \right) \right) \right)
\end{cases}
\]
\[
= \begin{cases} 
\text{Definition of assignment and Definition of skip} \\
\left( \text{odd}(x) \lor \text{even}(x) \right) \land (x \div 2 < x) \\
\text{Definition of assignment and Definition of skip} \\
(x \div 2 < x) \Rightarrow x \div 2 < x
\end{cases}
\]
\[
= \begin{cases} 
\text{Proof by Cases} \\
(x \div 2 < x) \Rightarrow \left( \text{odd}(x) \lor \text{even}(x) \right) \land \text{odd}(x) \lor \text{even}(x) \Rightarrow x \div 2 < x
\end{cases}
\]
\[
= \begin{cases} 
\text{Arithmetic} \\
T \land (T \Rightarrow (x \div 2 < x)) \\
\text{and-simplification and Left identity of } \Rightarrow \\
x \div 2 < x
\end{cases}
\]
\[
= \begin{cases} 
\text{Arithmetic: } 0 < x = (x \div 2 < x) \\
0 < x
\end{cases}
\]
\[
= \begin{cases} 
\text{Arithmetic} \\
x \geq 1
\end{cases}
\]
\[
= \begin{cases} 
\text{Assumption: } x \geq 1
\end{cases}
\]
\[
T \quad \square
\]
2 Developing Invariants

Given a program and a postcondition $R$, find the invariant $P$ and bound $t$.

To develop an invariant, weaken $R$.

Different strategies of weakening $R$ exists.

1. Delete a conjunct
2. Replace a constant with a variable
3. Enlarge the range of a variable
4. Add a disjunct (Too hard!)

2.1 Delete a Conjunct

Problem: Linear Search

Given an array $b[0:m]$, find the first value $x$ in $b[0:m]$, the value is known to exist.

Precondition $Q : 0 < m \land x \in b[0 : m]$

$$i := 0$$

$$\text{do}$$

$$x \neq b[i] \rightarrow i := i + 1$$

$$\text{od}$$

Postcondition $R : 0 \leq i \leq m \land x \not\in b[0 : i - 1] \land x = b[i]$

$P : 0 \leq i \leq m \land x \not\in b[0 : i - 1]$

$t : m - i$

2.2 Replace a constant with a variable

Problem: Accumulated Sum

Given an array $b[0:m]$, compute the sum of all the elements of $b[0:m]$.

Precondition $Q : m + 1 \geq 0$

$$r, j := 0, 0$$

$$\text{do}$$

$$j \neq m + 1 \rightarrow r := r + b[j]; j := j + 1$$

$$\text{od}$$

Postcondition $R : r = (\Sigma i : 0 \leq i < m + 1 : b[0 : i])$

$$P : r = (\Sigma i : 0 \leq i < j : b[i]) \land 0 \leq j \leq m + 1$$

$$t : m + 1 - j$$
2.3 Enlarge the range of a variable

Example: Linear Search
Given an array $b[0:m]$, find the first value $x$ in $b[0:m]$, the value is known to exist.

Let $ix$ denote the smallest value satisfying $0 \leq ix \land x = b[ix]$.

Precondition $Q : 0 \leq m \land x \in b[0 : m]$

$$i := 0$$
$$\text{do}$$
$$i \neq ix \rightarrow i := i + 1$$
$$\text{od}$$

Postcondition $R : i = ix$

$$P : 0 \leq i \leq ix$$
$$t : m - i$$

2.4 Example: Reversed French Flag

2.4.1 Problem
We are given a row of buckets, each containing a pebble. The pebble is either red, white or blue. There are two robot arms, each supplied with a camera that can decide the color of the pebble. Using the robot arms we can swap the pebbles in buckets $i$ and $j$. Sort the pebbles according to the colours of the French flag.

2.4.2 Formally
We represent the buckets as an array $A[0 : n - 1]$, where $n$ is the number of the buckets. Each array entry has one of the values

1. red
2. white
3. blue

Precondition $Q \forall i : 0 \leq i < n : A[i] = \text{red} \lor A[i] = \text{white} \lor A[i] = \text{blue}$

Postcondition $R$
\[ A[0 : r - 1] = \text{red} \]
\[ \land \]
\[ A[r : w - 1] = \text{white} \]
\[ \land \]
\[ A[w : n - 1] = \text{blue} \]
\[ \land \]
\[ 0 \leq r \leq w \leq n \]

2.4.3 Solution:

Program:

\[
\begin{align*}
m, r, w &:= n, 0, n \\
do &
\begin{align*}
r \neq m &\land A[m - 1] = \text{white} \quad \rightarrow \quad m := m - 1 \\
r \neq m &\land A[m - 1] = \text{red} \quad \rightarrow \quad A[r], A[m - 1], r := \\
&\quad A[m - 1], A[r], r + 1 \\
r \neq m &\land A[m - 1] = \text{blue} \quad \rightarrow \quad A[m - 1], A[w - 1], m, w := \\
&\quad A[w - 1], A[m - 1], m - 1, w - 1 \\
\end{align*}
\end{align*}
\]

od

Invariant \( P \):

\[
\begin{align*}
A[0 : r - 1] & = \text{red} \\
\land \\
A[m : w - 1] & = \text{white} \\
\land \\
A[w : n - 1] & = \text{blue} \\
\land \end{align*}
\]
\[ 0 \leq r \leq m \leq w \leq n \]

Bound function \( t \):

We see that we decrease the "mixed" section. This gives us the bound function \( t := m - r \).