Assignment 1: Background theory

Maxwell Bo 4392687

March 21, 2017

1. (a) $y : [\ \text{true},\ (x = 0 \land y = 0) \lor (y = y_0/x \land x \neq 0)\ ]$
   (b) $y : [\ \text{true},\ (x = 0) \lor (y = y_0/x \land x \neq 0)\ ]$
   (c) TODO

2. $$\begin{array}{ll} & x, y : [\text{true}, x = z^2 \land y = z^4] \\ \sqsubseteq & \{\text{Composition}\} \\ & x, y : [\text{true}, x = z^2];\ x, y : [x = z^2, x = z^2 \land y = z^4] \\ \sqsubseteq & \{\text{Assignment: true} \Rrightarrow x = z^2[x \backslash z^2]\} \\ & x = z^2;\ x, y : [x = z^2, x = z^2 \land y = z^4] \\ \sqsubseteq & \{\text{Assignment: } x = z^2 \Rrightarrow x = z^2 \land y = z^4[y \backslash x^2]\} \\ & x := z^2;\ y := x^2 \end{array}$$

3. (a) Assuming

$$\begin{array}{rcl} wp(y := 10,\ \text{true}) & \equiv & \text{true}[y \backslash 10] \\ & \equiv & \text{true} \end{array}$$

we can conclude that

$$\begin{array}{rcl} wp(\textbf{if}\ (x > 0\ \lor\ y < 10) \to y := 10\ \textbf{fi},\ \text{true}) & \equiv & (x > 0\ \lor\ y < 10)\ \land \\ & & ((x > 0\ \lor\ y < 10) \to wp(y := 10,\ \text{true})) \\ & \equiv & (x > 0\ \lor\ y < 10)\ \land\ \text{true} \\ & \equiv & (x > 0\ \lor\ y < 10) \end{array}$$

As $y < 10 \Rrightarrow (x > 0 \lor y < 10)$, the Hoare triple is true.

   (b) Assuming

$$wp(x := x + y,\ P[x \backslash x + y]) \quad \equiv \quad (P[x \backslash x + y])[x \backslash x + y]$$

TODO

4. (a) $$\begin{array}{ll} & y : [y < 10, y > 0] \\ \sqsubseteq & \{\text{Selection: } y < 10 \Rrightarrow (x > 0 \lor y < 10)\} \\ & \textbf{if}\ (x > 0 \lor y < 10) \to y : [(x > 0 \lor y < 10) \land (y < 10),\ y > 0]\ \textbf{fi} \\ \sqsubseteq & \{\text{Absorption 1: } (x > 0 \lor y < 10) \land (y < 10) = y < 10\} \\ & \textbf{if}\ (x > 0 \lor y < 10) \to y : [y < 10,\ y > 0]\ \textbf{fi} \\ \sqsubseteq & \{\text{Assignment: } y < 10 \Rrightarrow y > 0[y \backslash 10]\} \\ & \textbf{if}\ (x > 0 \lor y < 10) \to y := 10\ \textbf{fi} \end{array}$$

(b) $y : [y < 10, y > 0]$

$\not\sqsubseteq$ {Selection: $y < 10 \not\Rrightarrow ((x > 0) \wedge (y < 10))$}

if $((x > 0) \wedge (y < 10)) \rightarrow y : [((x > 0) \wedge (y < 10)) \wedge (y < 10),\ y > 0]$ **fi**

5. TODO

Given

$$max(A, l, h, i) \ == \ \forall j \in [l, h) \cdot (A_j \leq A_i) \wedge (l \leq i < h)$$

suppose we wanted to show that the specification

$$i, j : [A.len > 0, max(A, 0, A.len, i)]$$

is refined by

$i, j := 0, 1;$
do $j < A.len \rightarrow$
  if $A_j > A_i \rightarrow i := j$
  $[\!]$ $A_j \leq A_i \rightarrow$ **skip**
  fi;
  $j := j + 1$
od

Parts of the proof follow:

$i, j : [A.len > 0, max(A, 0, A.len, i)]$

$\sqsubseteq$ {Strengthen post: $inv \wedge max(A, 0, A.len, i) \Rrightarrow max(A, 0, A.len, i)$}

$i, j : [A.len > 0, inv \wedge max(A, 0, A.len, i)]$

$\equiv$ {$max(A, 0, A.len, i)$ is equivalent to $j = A.len$ when inv is true}

$i, j : [A.len > 0, inv \wedge j = A.len]$

$\sqsubseteq$ {Composition: mid predicate is inv}

$i, j : [A.len > 0, inv];\ i, j : [inv, inv \wedge j = A.len]$

$\sqsubseteq$ {Assignment: $A.len > 0 \Rrightarrow inv[i, j \backslash 0, 1]$}

$i, j := 0, 1;\ i, j : [inv, inv \wedge j = A.len]$

The proof of the final step above is:

$inv[i, j \backslash 0, 1]$

$\equiv$ {definition of inv}

$max(A, 0, j, i)[i, j \backslash 0, 1]$

$\equiv$ {apply substitution}

$max(A, 0, 1, 0)$

$\equiv$ {since A_0 only element in $A_{[0,1)}$}

true

Continuing the refinement:

$$
\begin{array}{ll}
 & i, j : [inv, inv \wedge j = A.len] \\
\sqsubseteq & \{\text{Repetition: } A.len - j \text{ is variant}\} \\
 & \textbf{do } j \neq A.len \rightarrow \\
 & \quad i, j : [inv \wedge j < A.len, inv \wedge (0 \leq A.len - j < A.len - j_0)] \\
 & \textbf{od}
\end{array}
$$

Here is another part of the proof involving other GCL notation:

$$
\begin{array}{ll}
 & i : [inv \wedge j < A.len, max(A, 0, j+1, i)] \\
\sqsubseteq & \{\text{Selection: } P \Rrightarrow A_i > A_j \vee A_j \leq A_i, \text{ for any } P\} \\
 & \textbf{if } A_j > A_i \rightarrow i : [A_j > A_i \wedge inv \wedge j < A.len, max(A, 0, j+1, i)] \\
 & [\!] \; A_j \leq A_i \rightarrow i : [A_j \leq A_i \wedge inv \wedge j < A.len, max(A, 0, j+1, i)] \\
 & \textbf{fi} \\
\sqsubseteq & \{\text{Assignment: } A_j > A_i \wedge inv \wedge j < A.len \Rrightarrow max(A, 0, j+1, i)[i \backslash j]\} \\
 & \textbf{if } A_j > A_i \rightarrow i := j \\
 & [\!] \; A_j \leq A_i \rightarrow i : [A_j \leq A_i \wedge inv \wedge j < A.len, max(A, 0, j+1, i)] \\
 & \textbf{fi} \\
\sqsubseteq & \{\text{Skip: } A_j \leq A_i \wedge inv \wedge j < A.len \Rrightarrow max(A, 0, j+1, i)\} \\
 & \textbf{if } A_j > A_i \rightarrow i := j \\
 & [\!] \; A_j \leq A_i \rightarrow \textbf{skip} \\
 & \textbf{fi}
\end{array}
$$