Assignment 1: Background theory

Maxwell Bo   4392687

March 22, 2017

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

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

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

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

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

   (b) Assuming

$$
\begin{array}{rcl}
wp(x := x + y,\ P[x \backslash x + y]) & \equiv & (P[x \backslash x + y])[x \backslash x + y] \\
& \equiv & P[x \backslash (x + y) + y] \\
& \equiv & P[x \backslash x + 2y]
\end{array}
$$

Using this

$$\{\text{true}[x \backslash x + 2y]\}\ x := x + y\ \{\text{true}[x \backslash x + y]\}$$

holds but

$$\{(x > 8)[x \backslash x + 2y]\}\ x := x + y\ \{(x > 8)[x \backslash x + y]\} \quad \equiv \quad \{x + 2y > 8\}\ x := x + y\ \{x + y > 8\}$$

does not. Therefore, the choice of P determines the validity of the Hoare Triple, due to P having arbitrary. Assuming that P is quantified over all possible predicates, the Hoare Triple does not hold

4. (a)

$$
\begin{array}{ll}
& y : [y < 10, y > 0] \\
\sqsubseteq & \{\text{Selection: } y < 10 \Rrightarrow (x > 0 \vee y < 10)\} \\
& \textbf{if } (x > 0 \vee y < 10) \rightarrow y : [(x > 0 \vee y < 10) \wedge (y < 10),\ y > 0] \textbf{ fi} \\
\sqsubseteq & \{\text{Absorption 1: } (x > 0 \vee y < 10) \wedge (y < 10) = y < 10\} \\
& \textbf{if } (x > 0 \vee y < 10) \rightarrow y : [y < 10,\ y > 0] \textbf{ fi} \\
\sqsubseteq & \{\text{Assignment: } y < 10 \Rrightarrow y > 0[y\backslash 10]\} \\
& \textbf{if } (x > 0 \vee y < 10) \rightarrow y := 10 \textbf{ fi}
\end{array}
$$

(b)

$$
\begin{array}{ll}
& y : [y < 10, y > 0] \\
\not\sqsubseteq & \{\text{Selection: } y < 10 \not\Rrightarrow ((x > 0) \wedge (y < 10))\} \\
& \textbf{if } ((x > 0) \wedge (y < 10)) \rightarrow y : [((x > 0) \wedge (y < 10)) \wedge (y < 10),\ y > 0] \textbf{ fi}
\end{array}
$$

5.

$$\forall\, S, B \ \cdot\ (\textbf{repeat } S \textbf{ until } B \ \equiv\ S;\ \textbf{do } \neg B \rightarrow S \textbf{ od})$$

$\therefore$

$$
\begin{array}{ll}
& w : [P, Q] \\
\sqsubseteq & \{\text{Composition}\} \\
& w : [P, I];\ w : [I, Q] \\
\sqsubseteq & \{\text{Strengthen Postcondition: } I \wedge \neg(\neg B) \Rrightarrow Q\} \\
& w : [P, I];\ w : P[I, I \wedge \neg(\neg B)] \\
\sqsubseteq & \{\text{Repetition}\} \\
& w : [P, I];\ \textbf{do } (\neg B) \rightarrow w : [I \wedge \neg B,\ I \wedge (0 \leqslant V < V_0)] \textbf{ od}
\end{array}
$$

$w : [P, I]$ and $w : [I \wedge \neg B,\ I \wedge (0 \leqslant V < V_0)]$ can both refine to the same program, S.

Thus, $P \Rrightarrow I \wedge \neg B$, so such that for an arbitrary S with precondition P, S can preserve the requirements of the **do** loop.

Given both $I \wedge \neg(\neg B) \Rrightarrow Q$ and $P \Rrightarrow I \wedge \neg B$, we can formulate

$$\text{if } P \Rrightarrow I \wedge \neg B \text{ then } w : [P, I \wedge B] \ \sqsubseteq\ \textbf{repeat } w : [I \wedge \neg B,\ I \wedge (0 \leqslant V < V_0)] \textbf{ until } B$$
$$\text{where } I \text{ is a loop invariant, and } V \text{ is a loop variant}$$