Assignment 1: Background theory

Maxwell Bo   4392687

March 23, 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)

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

Assuming that P is quantified over all possible predicates,

$$\{P\}\ x := x + y\ \{P[x \backslash x + y]\} \tag{1}$$

does not hold, due to the choice of P determining the validity of the Hoare Triple.
As a counter example, let $P \equiv (x = 0)$, such that the Triple is

$$\{x = 0\}\ x := x + y\ \{x = 0[x \backslash x + y]\} \tag{2}$$

Given that

$$\begin{aligned} wp(x := x + y,\ x = 0[x\backslash x + y]) &\equiv x = 0[x\backslash x + 2y] \\ &\equiv x + 2y = 0 \end{aligned}$$

$$(x = 0) \not\Rrightarrow (x + 2y = 0) \tag{3}$$

$$\therefore \not\forall P : (\{P\}\ S\ \{Q\}) \to (P \Rrightarrow wp(S, Q)) \tag{4}$$

Thus, the Hoare Triple is false.

4. (a)

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

(b)

$$\begin{aligned} & y : [y < 10, y > 0] \\ \not\sqsubseteq\ & \{\text{Selection: } y < 10 \not\Rrightarrow ((x > 0) \land (y < 10))\} \\ & \textbf{if } ((x > 0) \land (y < 10)) \to y : [((x > 0) \land (y < 10)) \land (y < 10),\ y > 0]\ \textbf{fi} \end{aligned}$$

5.

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

$\therefore$

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

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

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

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

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