

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) Let $S = [x \neq 0, y = \frac{y_0}{x}]$, $A = \text{(a)}$ and $B = \text{(b)}$.
 B refines to A , as A has a stronger postcondition than that of B . The user may replace a program written to the specification of B with one written to A and uphold the contract. S does not refine to B . While the precondition of B is weaker than that of S , the postcondition of B is not stronger or equivalent to that of A . As S does not refine to B , S does not refine to A , by the law of transitivity.
2. $x, y : [\text{true}, x = z^2 \wedge y = z^4]$
 $\sqsubseteq \{ \text{Composition} \}$
 $x, y : [\text{true}, x = z^2]; x, y : [x = z^2, x = z^2 \wedge y = z^4]$
 $\sqsubseteq \{ \text{Assignment: } \text{true} \Rightarrow x = z^2[x \setminus z^2] \}$
 $x = z^2; x, y : [x = z^2, x = z^2 \wedge y = z^4]$
 $\sqsubseteq \{ \text{Assignment: } x = z^2 \Rightarrow x = z^2 \wedge y = z^4[y \setminus x^2] \}$
 $x := z^2; y := x^2$
3. (a) Assuming

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

we can conclude that

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

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

(b)

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

Assuming that P is quantified over all possible predicates,

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

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

$$\{x = 0\} x := x + y \{x = 0[x \setminus x + y]\} \quad (2)$$

Given that

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

$$(x = 0) \not\Rightarrow (x + 2y = 0) \quad (3)$$

$$\therefore \not\models P : (\{P\} S \{Q\}) \rightarrow (P \Rightarrow wp(S, Q)) \quad (4)$$

Thus, the Hoare Triple is false.

4. (a) $y : [y < 10, y > 0]$
 \sqsubseteq {Selection: $y < 10 \Rightarrow (x > 0 \vee y < 10)$ }
if $(x > 0 \vee y < 10) \rightarrow y : [(x > 0 \vee y < 10) \wedge (y < 10), y > 0]$ **fi**
 \sqsubseteq {Absorption 1: $(x > 0 \vee y < 10) \wedge (y < 10) = y < 10$ }
if $(x > 0 \vee y < 10) \rightarrow y : [y < 10, y > 0]$ **fi**
 \sqsubseteq {Assignment: $y < 10 \Rightarrow y > 0[y \setminus 10]$ }
if $(x > 0 \vee y < 10) \rightarrow y := 10$ **fi**
- (b) $y : [y < 10, y > 0]$
 $\not\sqsubseteq$ {Selection: $y < 10 \not\Rightarrow ((x > 0) \wedge (y < 10))$ }
if $((x > 0) \wedge (y < 10)) \rightarrow y : [((x > 0) \wedge (y < 10)) \wedge (y < 10), y > 0]$ **fi**

The precondition cannot be strengthened. Thus, we cannot refine to a selection statement using $((x > 0) \wedge (y < 10))$ as its only guard.

5.

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

\therefore

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

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

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

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

$$\text{if } P \Rightarrow I \wedge \neg B \text{ then } w : [P, I \wedge B] \sqsubseteq \text{repeat } w : [I \wedge \neg B, I \wedge (0 \leq V < V_0)] \text{ until } B$$

where I is a loop invariant, and V is a loop variant