Suggested Solutions for Homework Assignment #5

We assume the binding powers of the logical connectives and the entailment symbol decrease in this order: $\neg$, $\{\forall, \exists\}$, $\{\wedge, \vee\}$, $\rightarrow$, $\leftrightarrow$, $\vdash$.

1. (40 points) Prove that

   (a) $\models wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q) \leftrightarrow (B \wedge wlp(S_1, q)) \vee (\neg B \wedge wlp(S_2, q))$ and

   (b) $\models \{p\}\ S\ \{q\}$ iff $\models p \rightarrow wlp(S, q)$

   which we claimed when proving the completeness of System *PD* (for the validity of a Hoare triple with partial correctness semantics).

   Here, assuming a sufficiently expressive assertion language, $wlp(S, q)$ denotes the assertion p such that $[\![p]\!] = wlp(S, [\![q]\!])$, where $[\![p]\!]$ is defined as $\{\sigma \in \Sigma \mid \sigma \models p\}$ (i.e., the set of states where p holds) and $wlp(S, \Phi)$ as $\{\sigma \in \Sigma \mid \mathcal{M}[\![S]\!](\sigma) \subseteq \Phi\}$. Recall that, for $\sigma \in \Sigma$, $\mathcal{M}[\![S]\!](\sigma) = \{\tau \in \Sigma \mid \langle S, \sigma\rangle \rightarrow^* \langle E, \tau\rangle\}$, $\mathcal{M}[\![S]\!](\perp) = \emptyset$, and, for $X \subseteq \Sigma \cup \{\perp\}$, $\mathcal{M}[\![S]\!](X) = \bigcup_{\sigma \in X} \mathcal{M}[\![S]\!](\sigma)$.

   Solution. With the assumed expressive assertion language, we can equate a set of states that may arise in applying $wlp(S, [\![\cdot]\!])$ to some assertion with some other assertion expressible in the same assertion language.

   (a) We claim for immediate use and prove later that

   - $\models B \wedge wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q) \leftrightarrow B \wedge wlp(S_1, q)$ and
   - $\models \neg B \wedge wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q) \leftrightarrow \neg B \wedge wlp(S_2, q)$.

   With these claims,

   $\models wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q) \leftrightarrow (B \wedge wlp(S_1, q)) \vee (\neg B \wedge wlp(S_2, q))$

   iff $\{\ A \leftrightarrow (B \wedge A) \vee (\neg B \wedge A)\ \}$

   $\models (B \wedge wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q)) \vee (\neg B \wedge wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q))$
   $\quad \leftrightarrow (B \wedge wlp(S_1, q)) \vee (\neg B \wedge wlp(S_2, q))$

   iff $\{$ if $A_1 \leftrightarrow B_1$ and $A_2 \leftrightarrow B_2$, then $A_1 \vee A_2 \leftrightarrow B_1 \vee B_2\ \}$

   true.

   To prove the first claim $\models B \wedge wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q) \leftrightarrow B \wedge wlp(S_1, q)$ we show that, for every $\sigma \in \Sigma$, $\sigma \models B \wedge wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q)$ iff $\sigma \models B \wedge wlp(S_1, q)$; the second claim may be proven analogously.

   For every $\sigma \in \Sigma$,

$\sigma \models B \wedge wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q)$
iff $\{$ Semantics of $\wedge$ $\}$
$\sigma \models B$ and $\sigma \models wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q)$
iff $\{$ Semantics of $wlp(S, q)$ $\}$
$\sigma \models B$ and $\sigma \in wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, [\![q]\!])$
iff $\{$ Definition of $wlp(S, [\![q]\!])$ $\}$
$\sigma \models B$ and $\mathcal{M}[\![\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}]\!](\sigma) \subseteq [\![q]\!]$
iff $\{$ $\mathcal{M}[\![\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}]\!](\sigma) = \mathcal{M}[\![S_1]\!](\sigma)$, when $\sigma \models B$ $\}$
$\sigma \models B$ and $\mathcal{M}[\![S_1]\!](\sigma) \subseteq [\![q]\!]$
iff $\{$ Definition of $wlp(S, [\![q]\!])$ $\}$
$\sigma \models B$ and $\sigma \in wlp(S_1, [\![q]\!])$
iff $\{$ Semantics of $wlp(S, q)$ $\}$
$\sigma \models B$ and $\sigma \models wlp(S_1, q)$
iff $\{$ Semantics of $\wedge$ $\}$
$\sigma \models B \wedge wlp(S_1, q)$.

(b)

$\models \{p\}\ S\ \{q\}$
iff $\{$ Definition of the validity of a Hoare triple $\}$
$\mathcal{M}[\![S]\!]([\![p]\!]) \subseteq [\![q]\!]$
iff $\{$ Definition of $\mathcal{M}[\![S]\!](X)$ $\}$
$(\bigcup_{\sigma \in [\![p]\!]} \mathcal{M}[\![S]\!](\sigma)) \subseteq [\![q]\!]$
iff $\{$ $(\bigcup_{x \in X} T(x)) \subseteq U$ iff for every x, $x \in X$ implies $T(x) \subseteq U$ $\}$
for every $\sigma \in \Sigma$, $\sigma \in [\![p]\!]$ implies $\mathcal{M}[\![S]\!](\sigma) \subseteq [\![q]\!]$
iff $\{$ Restatement of $\mathcal{M}[\![S]\!](\sigma) \subseteq [\![q]\!]$ $\}$
for every $\sigma \in \Sigma$, $\sigma \in [\![p]\!]$ implies $\sigma \in \{\sigma \in \Sigma \mid \mathcal{M}[\![S]\!](\sigma) \subseteq [\![q]\!]\}$
iff $\{$ Definition of $\subseteq$ $\}$
$[\![p]\!] \subseteq \{\sigma \in \Sigma \mid \mathcal{M}[\![S]\!](\sigma) \subseteq [\![q]\!]\}$
iff $\{$ Definition of $wlp(S, [\![q]\!])$ $\}$
$[\![p]\!] \subseteq wlp(S, [\![q]\!])$
iff $\{$ Definitions of $[\![p]\!]$ and $wlp(S, q)$ $\}$
$\{\sigma \in \Sigma \mid \sigma \models p\} \subseteq \{\sigma \in \Sigma \mid \sigma \models wlp(S, q)\}$
iff $\{$ Definition of $\subseteq$ $\}$
for every $\sigma \in \Sigma, \sigma \models p$ implies $\sigma \models wlp(S, q)$
iff $\{$ Definition of $\rightarrow$ $\}$
for every $\sigma \in \Sigma, \sigma \models p \rightarrow wlp(S, q)$
iff $\{$ Validity rewritten in a conventional simpler way $\}$
$\models p \rightarrow wlp(S, q)$

□

2. (40 points) The following fundamental properties are usually taken as axioms for the predicate transformer wp (weakest precondition):

   - **Law of the Excluded Miracle**: $wp(S, \mathit{false}) \equiv \mathit{false}$.
   - **Distributivity of Conjunction**: $wp(S, Q_1) \wedge wp(S, Q_2) \equiv wp(S, Q_1 \wedge Q_2)$.
   - **Distributivity of Disjunction** for deterministic S: $wp(S, Q_1) \vee wp(S, Q_2) \equiv wp(S, Q_1 \vee Q_2)$.

   From the axioms (plus the usual logical and algebraic laws), derive the following properties of wp (Hint: not every axiom is useful):

(a) **Law of Monotonicity**: if $Q_1 \Rightarrow Q_2$, then $wp(S, Q_1) \Rightarrow wp(S, Q_2)$.

Solution.

$$\begin{array}{ll} & wp(S, Q_1) \\ \equiv & \quad \{\ Q_1 \Rightarrow Q_2, \text{ i.e., } Q_1 \equiv\ Q_1 \wedge Q_2\ \} \\ & wp(S, Q_1 \wedge Q_2) \\ \equiv & \quad \{\ \text{Distributivity of Conjunction}\ \} \\ & wp(S, Q_1) \wedge wp(S, Q_2) \\ \Rightarrow & \quad \{\ A \wedge B \rightarrow B\ \} \\ & wp(S, Q_2) \end{array}$$

□

(b) **Distributivity of Disjunction** (for any command): $wp(S, Q_1) \vee wp(S, Q_2) \Rightarrow wp(S, Q_1 \vee Q_2)$.

Solution.

$$\begin{array}{ll} & wp(S, Q_1) \vee wp(S, Q_2) \\ \Rightarrow & \quad \{\ Q_1 \Rightarrow Q_1 \vee Q_2,\ Q_2 \Rightarrow Q_1 \vee Q_2, \text{ Monotonicity of } wp\ \} \\ & wp(S, Q_1 \vee Q_2) \vee wp(S, Q_1 \vee Q_2) \\ \equiv & \quad \{\ A \vee A \equiv A\ \} \\ & wp(S, Q_1 \vee Q_2) \end{array}$$

□

3. (20 points) Prove that $\vdash \{a \geq b\}\ \min(a, b, c)\ \{c = b\}$, given the following declaration:

```
proc min(in x; in y; out z);
   if x < y then
      z := x
   else z := y;
```

Solution.

$$\dfrac{\dfrac{\dfrac{\dfrac{\text{pred. calculus + algebra}}{x \geq y \wedge x < y \rightarrow x = y} \quad \dfrac{}{\{x = y\}\ z := x\ \{z = y\}}\,\text{(assignment)}}{\{x \geq y \wedge x < y\}\ z := x\ \{z = y\}}\,\text{(stren. pre.)} \qquad \alpha}{\{x \geq y\}\ \textbf{if}\ x < y\ \textbf{then}\ z := x\ \textbf{else}\ z := y\ \{z = y\}}\,\text{(conditional)}}{\{a \geq b\}\ \min(a, b, c)\ \{c = b\}}\,\text{(procedure)}$$

α :

$$\dfrac{\dfrac{\text{pred. calculus + algebra}}{x \geq y \wedge \neg(x < y) \rightarrow y = y} \quad \dfrac{}{\{y = y\}\ z := y\ \{z = y\}}\,\text{(assignment)}}{\{x \geq y \wedge \neg(x < y)\}\ z := y\ \{z = y\}}\,\text{(stren. pre.)}$$

□