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) $\models wlp(\textbf{while } B \textbf{ do } S_1 \textbf{ od}, q) \wedge B \rightarrow wlp(S_1, wlp(\textbf{while } B \textbf{ do } S_1 \textbf{ od}, q))$ 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 $\sigma \in \Sigma$, $\mathcal{M}[\![S]\!](\sigma) = \{\tau \in \Sigma \mid \langle S, \sigma\rangle \rightarrow^* \langle E, \tau\rangle\}$, $\mathcal{M}[\![S]\!](\bot) = \emptyset$, and, for $X \subseteq \Sigma \cup \{\bot\}$, $\mathcal{M}[\![S]\!](X) = \bigcup_{\sigma \in X} \mathcal{M}[\![S]\!](\sigma)$.

   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 q with some other assertion p expressible in the same assertion language.

   (a) We show that, for every $\sigma \in \Sigma$, $\sigma \models wlp(\textbf{while } B \textbf{ do } S_1 \textbf{ od}, q) \wedge B$ implies $\sigma \models wlp(S_1, wlp(\textbf{while } B \textbf{ do } S_1 \textbf{ od}, q))$. From the operational semantics, we have $\langle \textbf{while } B \textbf{ do } S \textbf{ od}, \sigma\rangle \rightarrow \langle S; \textbf{while } B \textbf{ do } S \textbf{ od}, \sigma\rangle$, when $\sigma \models B$. It follows that $\mathcal{M}[\![S_1; \textbf{while } B \textbf{ do } S_1 \textbf{ od}]\!](\sigma) = \mathcal{M}[\![\textbf{while } B \textbf{ do } S_1 \textbf{ od}]\!](\sigma)$, when $\sigma \models B$.

   For every $\sigma \in \Sigma$,

   $$
   \begin{array}{ll}
   & \sigma \models wlp(\textbf{while } B \textbf{ do } S_1 \textbf{ od}, q) \wedge B \\
   \text{iff} & \quad \{ \text{ Semantics of } \wedge \text{ } \} \\
   & \sigma \models wlp(\textbf{while } B \textbf{ do } S_1 \textbf{ od}, q) \text{ and } \sigma \models B \\
   \text{iff} & \quad \{ \text{ Semantics of } wlp(S, q) \text{ } \} \\
   & \sigma \in wlp(\textbf{while } B \textbf{ do } S_1 \textbf{ od}, [\![q]\!]) \text{ and } \sigma \models B \\
   \text{iff} & \quad \{ \text{ Definition of } wlp(S, [\![q]\!]) \text{ } \} \\
   & \mathcal{M}[\![\textbf{while } B \textbf{ do } S_1 \textbf{ od}]\!](\sigma) \subseteq [\![q]\!] \text{ and } \sigma \models B \\
   \text{implies} & \quad \{ \text{ } \mathcal{M}[\![S_1; \textbf{while } B \textbf{ do } S_1 \textbf{ od}]\!](\sigma) = \mathcal{M}[\![\textbf{while } B \textbf{ do } S_1 \textbf{ od}]\!](\sigma), \text{ when } \sigma \models B \text{ } \} \\
   & \mathcal{M}[\![S_1; \textbf{while } B \textbf{ do } S_1 \textbf{ od}]\!](\sigma) \subseteq [\![q]\!] \\
   \text{iff} & \quad \{ \text{ Definition of } wlp(S, [\![q]\!]) \text{ } \} \\
   & \sigma \in wlp(S_1; \textbf{while } B \textbf{ do } S_1 \textbf{ od}, [\![q]\!]) \\
   \text{iff} & \quad \{ \text{ Semantics of } wlp(S, q) \text{ } \} \\
   & \sigma \models wlp(S_1; \textbf{while } B \textbf{ do } S_1 \textbf{ od}, q) \\
   \text{iff} & \quad \{ \text{ } wlp(S_1; S_2, q) \leftrightarrow wlp(S_1, wlp(S_2, q)) \text{ } \} \\
   & \sigma \models wlp(S_1, wlp(\textbf{while } B \textbf{ do } S_1 \textbf{ od}, q)).
   \end{array}
   $$

(b)

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

□

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

- **Law of the Excluded Miracle**: $wp(S, false) \equiv false$.
- **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.

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

$\square$

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.

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

α :

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

$\square$