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

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

   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. Recall that $\models \{p\}\ S\ \{q\}$ is defined by $\mathcal{M}[\![S]\!]([\![p]\!]) \subseteq [\![q]\!]$. Note also that, 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)

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

   (b)

$\models \{wlp(S,q)\}\ S\ \{q\}$

iff $\quad$ { Definitions of $wlp(S,q)$ and the validity of a Hoare triple }

$\mathcal{M}[\![S]\!](wlp(S,[\![q]\!])) \subseteq [\![q]\!]$

iff $\quad$ { Definition of $\mathcal{M}[\![S]\!](X)$ }

$(\bigcup_{\sigma \in wlp(S,[\![q]\!])} \mathcal{M}[\![S]\!](\sigma)) \subseteq [\![q]\!]$

iff $\quad$ { $(\bigcup_{x \in X} T(x)) \subseteq U$ iff for every x, $x \in X$ implies $T(x) \subseteq U$ }

for every $\sigma \in \Sigma$, $\sigma \in wlp(S,[\![q]\!])$ implies $\mathcal{M}[\![S]\!](\sigma) \subseteq [\![q]\!]$

iff $\quad$ { Restatement of $\mathcal{M}[\![S]\!](\sigma) \subseteq [\![q]\!]$ }

for every $\sigma \in \Sigma$, $\sigma \in wlp(S,[\![q]\!])$ implies $\sigma \in \{\sigma \in \Sigma \mid \mathcal{M}[\![S]\!](\sigma) \subseteq [\![q]\!]\}$

iff $\quad$ { Definition of $wlp(S,[\![q]\!])$ }

for every $\sigma \in \Sigma$, $\sigma \in wlp(S,[\![q]\!])$ implies $\sigma \in wlp(S,[\![q]\!])$

iff $\quad$ { $A \to A$ iff *true* }

true

□

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.

   $wp(S,Q_1)$

   $\equiv \quad$ { $Q_1 \Rightarrow Q_2$, i.e., $Q_1 \equiv Q_1 \wedge Q_2$ }

   $wp(S,Q_1 \wedge Q_2)$

   $\equiv \quad$ { Distributivity of Conjunction }

   $wp(S,Q_1) \wedge wp(S,Q_2)$

   $\Rightarrow \quad$ { $A \wedge B \to B$ }

   $wp(S,Q_2)$

   □

   (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.

   $wp(S,Q_1) \vee wp(S,Q_2)$

   $\Rightarrow \quad$ { $Q_1 \Rightarrow Q_1 \vee Q_2$, $Q_2 \Rightarrow Q_1 \vee Q_2$, Monotonicity of *wp* }

   $wp(S,Q_1 \vee Q_2) \vee wp(S,Q_1 \vee Q_2)$

   $\equiv \quad$ { $A \vee A \equiv A$ }

   $wp(S,Q_1 \vee Q_2)$

   □

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

   proc max(**in** x; **in** y; **out** z);

   if $x < y$ **then**

$z := y$
else $z := x$;

Solution.

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

α :

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

□