Homework Assignment #5

Due Time/Date

2:20PM Wednesday, November 22, 2023. Late submission will be penalized by 20% for each working day overdue.

How to Submit

Please write or type your answers on A4 (or similar size) paper. Put your completed homework on the instructor's desk before the class starts. For late submissions, please drop them in Yih-Kuen Tsay's mail box on the first floor of Management Building 2. You may discuss the problems with others, but copying answers is strictly forbidden.

Problems

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 $p \rightarrow wlp(S, q)$

   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 $X \subseteq \Sigma \cup \{\bot\}$, $\mathcal{M}[\![S]\!](X) = \bigcup_{\sigma \in X} \mathcal{M}[\![S]\!](\sigma)$.

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 $wp(S, Q_1) \Rightarrow wp(S, Q_2)$.

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

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 $z := y$;