Weakest Preconditions

Part 1: Definitions and Basic Properties

CS 536: Science of Programming, Spring 2022

1. Let $w \Leftrightarrow wp(S, q)$, let S be deterministic, and let $\{\tau\} = M(S, \sigma)$ where $\tau \in \Sigma \cup \{\bot\}$.
   a. For which $\sigma \vDash w$ do we have $\sigma \vDash [w]\ S\ [q]$?
   b. For which $\sigma \vDash \neg w$ do we have $\sigma \vDash [\neg w]\ S\ [q]$? How about $\sigma \vDash \{\neg w\}\ S\ \{q\}$?
   c. For which $\sigma \vDash w$ do we have $\sigma \vDash [w]\ S\ [\neg q]$?
   d. For which $\sigma \vDash \neg w$ do we have $\sigma \vDash \{\neg w\}\ S\ \{\neg q\}$?

2. If $\sigma \vDash w$ and $\sigma \vDash \{w\}\ S\ \{q\}$ and $\sigma \nvDash [w]\ S\ [q]$,
   a. What can we conclude about $M(S, \sigma)$?

5. Briefly explain why each of the following statements about *wp* and *wlp* are correct. (Answers like "That's how *X* is defined" are allowed.)
   a. For all $\sigma \in \Sigma$, $\sigma \vDash wp(S, q)$ iff $M(S, \sigma) \vDash q$
   b. For all $\sigma \in \Sigma$, $\sigma \vDash wlp(S, q)$ iff $M(S, \sigma) - \bot \vDash q$
   c. $\vDash [wp(S, q)]\ S\ [q]$
   d. $\vDash \{wlp(S, q)\}\ S\ \{q\}$
   e. $\vDash [p]\ S\ [q]$ iff $\vDash p \rightarrow wp(S, q)$
   f. $\vDash \{p\}\ S\ \{q\}$ iff $\vDash p \rightarrow wlp(S, q)$
   g. $\vDash \{\neg wp(S, q)\}\ S\ \{\neg q\}$, if S is deterministic
   h. $\vDash [\neg wlp(S, q)]\ S\ [\neg q]$, if S is deterministic
   i. $\nvDash p \rightarrow wp(S, q)$ iff $\nvDash [p]\ S\ [q]$
   j. $\nvDash p \rightarrow wlp(S, q)$ iff $\nvDash \{p\}\ S\ \{q\}$

6. Which of the following statements about relationships between *wp* and *wlp* are possible (i.e., satisfied in a state) and which are impossible (i.e. contradictions)? Briefly explain.
   a. $wlp(S, q) \wedge wlp(S, \neg q)$

b. $\neg wp(S, q) \wedge \neg wp(S, \neg q)$

c. $wp(S, q) \wedge \neg wlp(S, q)$

d. $wlp(S, q) \wedge \neg wp(S, \neg q)$

e. $wp(S, q) \wedge \neg wlp(S, \neg q)$

Solution to Practice 10 (Weakest Preconditions, pt. 1)

1. (Properties of weakest preconditions)
   a. For all $\sigma \vDash w$, we have $\sigma \vDash [w]\ S\ [q]$, since w is a precondition for $\vDash [\ldots]\ S\ [q]$.
   b. For no $\sigma \vDash \neg w$ do we have $\sigma \vDash [\neg w]\ S\ [q]$ because for w to be the weakest precondition for S and q, it cannot be that $M(S, \sigma) \vDash q$. For partial correctness, however, if $M(S, \sigma) = \{\bot\}$, then σ satisfies $\{\neg w\}\ S\ \{q\}$.
   c. For no $\sigma \vDash w$ do we have $\sigma \vDash [w]\ S\ [\neg q]$ because w is a precondition for $\vDash [\ldots]\ S\ [q]$.
   d. For all $\sigma \vDash \neg w$, we have $\sigma \vDash \{\neg w\}\ S\ \{\neg q\}$ because for w to be the weakest precondition for S and q, $\sigma \vDash \neg w$ implies $M(S, \sigma) \nvDash q$. Since S is deterministic, either $M(S, \sigma) = \{\bot\}$ or $M(S, \sigma) \vDash \neg q$. Either way, $\sigma \vDash \{\neg w\}\ S\ \{\neg q\}$.

2. (Partial but not total correctness when the *wp* is satisfied)
   a. If $\sigma \vDash w$ and $\sigma \vDash \{w\}\ S\ \{q\}$ then $M(S, \sigma) - \{\bot\} \vDash q$. If $\sigma \nvDash [w]\ S\ [q]$ then $M(S, \sigma) \nvDash q$. This can only happen if $\bot = M(S, \sigma)$ *or* $M(S, \sigma) = \{\}$. (I.e., S can diverge under σ.)

5. (Properties of *wp* and *wlp*)

   (a) and (b) are the basic definitions of *wp* and *wlp*
   (c) and (d) say that *wp* and *wlp* are preconditions
   (e) and (f) say that *wp* and *wlp* are weakest preconditions
   (g) and (h) also say that *wp* and *wlp* are weakest
   (i) and (j) are the contrapositives of (e) and (f).

6. (Situations involving *wp* and *wlp*)
   a. $M(S, \sigma) = \{\bot\}$ implies $wlp(S, q) \wedge wlp(S, \neg q)$
   b. $M(S, \sigma) = \{\bot\}$ implies $\sigma \vDash \neg wp(S, q) \wedge \neg wp(S, \neg q)$.
   c. $wp(S, q)$ implies $\neg wlp(S, q)$, so $wp(S, q) \wedge \neg wlp(S, q)$ is impossible.
   d. Since $wlp(S, q)$ implies $\neg wp(S, \neg q)$, we must have $wlp(S, q) \wedge \neg wp(S, \neg q)$ whenever $wlp(S, q)$.
   e. $wp(S, q) \Rightarrow \neg wlp(S, \neg q)$ is the contrapositive of the implication for (d) [if you swap q and $\neg q$], so $wp(S, q) \wedge \neg wlp(S, \neg q)$ must happen if $wp(S, q)$.