Weakest Preconditions

Part 1: Definitions and Basic Properties

CS 536: Science of Programming, Fall 2022

A. Why

- Weakest liberal preconditions (*wlp*) and weakest preconditions (*wp*) are the most general requirements that a program must meet to be correct.

B. Objectives

At the end of this activity you should be able to

- Define what a weakest liberal precondition (*wlp*) and weakest precondition (*wp*) is and how it's related to (and different from) preconditions in general
- Be able to calculate the *wlp* of a simple loop-free program.

C. Problems

1. Let $w \Leftrightarrow wp(S, q)$, let S be deterministic, and let $\{\tau\} = M(S, \sigma)$ where $\tau \in \Sigma \cup \{\perp\}$.
   a. For which $\sigma \vDash w$ do we have $\sigma \vDash_{tot} \{w\}\ S\ \{q\}$?
   b. For which $\sigma \vDash \neg w$ do we have $\sigma \vDash_{tot} \{\neg w\}\ S\ \{q\}$? How about $\sigma \vDash \{\neg w\}\ S\ \{q\}$?
   c. For which $\sigma \vDash w$ do we have $\sigma \vDash_{tot} \{w\}\ S\ \{\neg q\}$?
   d. For which $\sigma \vDash \neg w$ do we have $\sigma \vDash_{tot} \{\neg w\}\ S\ \{\neg q\}$? How about $\sigma \vDash \{\neg w\}\ S\ \{\neg q\}$?
   e. If S is nondeterministic, how do we have to modify the statement in part (d)?

2. If $\sigma \vDash w$ and $\sigma \vDash \{w\}\ S\ \{q\}$ and $\sigma \nvDash_{tot} \{w\}\ S\ \{q\}$,
   a. What can we conclude about $M(S, \sigma)$?
   b. If in addition, S is deterministic, what more can we conclude about $M(S, \sigma)$?

3. For an arbitrary p (not necessarily one that implies w), what $\vDash$ and $\vDash_{tot}$ properties relationships do the triples
   a. $\{p \wedge w\}\ S\ \{q\}$ and $\{\neg p \wedge w\}\ S\ \{q\}$ have?
   b. $\{p \wedge \neg w\}\ S\ \{\neg \boldsymbol{q}\}$ and $\{\neg p \wedge \neg w\}\ S\ \{\neg q\}$ have, if S is deterministic?
   c. $\{p \wedge \neg w\}\ S\ \{q\}$ and $\{\neg p \wedge \neg w\}\ S\ \{q\}$ have, if S is nondeterministic?

4. How are $wp(S, q_1 \vee q_2)$ and $wp(S, q_1) \cup wp(S, q_2)$ related if S is deterministic? If S is nondeterministic?

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 $M(S, \sigma) -\perp \vDash q$
   c. $\vDash_{tot} \{wp(S, q)\}\ S\ \{q\}$
   d. $\vDash \{wlp(S, q)\}\ S\ \{q\}$
   e. $\vDash_{tot} \{p\}\ S\ \{q\}$ 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. $\vDash_{tot} \{\neg wlp(S, q)\}\ S\ \{\neg q\}$, if S is deterministic
   i. $\nvDash p \rightarrow wp(S, q)$ iff $\nvDash_{tot} \{p\}\ S\ \{q\}$
   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 and which are impossible? Briefly explain why or why not.
   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. $wp(S, q) \wedge \neg wlp(S, \neg q)$
   f. For deterministic S, $\neg wp(S, q) \wedge \neg wp(S, \neg q)$ and $M(S, \sigma) - \perp \neq \varnothing$
   g. For deterministic S, $\neg wp(S, q) \wedge \neg wp(S, \neg q)$ and $\perp \notin M(S, \sigma)$

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

1. (Properties of weakest preconditions)
   a. For all $\sigma \vDash w$, we have $\sigma \vDash_{tot} \{w\}\ S\ \{q\}$, since w is a precondition for $\vDash_{tot} \{\ldots\}\ S\ \{q\}$.
   b. For no $\sigma \vDash \neg w$ do we have $\sigma \vDash_{tot} \{\neg w\}\ S\ \{q\}$ 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 $\sigma \vDash_{tot} \{w\}\ S\ \{\neg q\}$ because w is a precondition for $\vDash_{tot} \{\ldots\}\ S\ \{q\}$.
   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, $\sigma \vDash \{\neg w\}\ S\ \{\neg q\}$.
   e. If S is nondeterministic and $M(S, \sigma) \nvDash q$, then as in the deterministic case, nontermination is a possibility ($\bot \in M(S, \sigma)$ can happen). Regardless, we no longer know $M(S, \sigma) \vDash \neg q$ because we can have $M(S, \sigma) \nvDash q$ and $M(S, \sigma) \nvDash \neg q$ simultaneously.

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 $\sigma \nvDash_{tot} \{w\}\ S\ \{q\}$ then $M(S, \sigma) \nvDash q$. This can only happen if $\bot \in M(S, \sigma)$. (I.e., S can diverge under σ.)
   b. If in addition S is deterministic, then we don't just have $\bot \in M(S, \sigma)$, we have $\{\bot\} = M(S, \sigma)$. (I.e., S diverges under σ.)

3. (Intersection with *wp*)
   a. $\vDash_{tot} \{p \wedge w\}\ S\ \{q\}$ and $\vDash_{tot} \{\neg p \wedge w\}\ S\ \{q\}$ follow from w being a precondition under $\vDash_{tot}$.
   b. Because w is weakest, we have for all $\sigma \vDash p \wedge \neg w$, that $\sigma \nvDash_{tot}. \{p \wedge \neg w\}\ S\ \{q\}$. If S is deterministic, this implies $\sigma \vDash \{p \wedge \neg w\}\ S\ \{\neg q\}$. Similarly, for all $\sigma \vDash \neg p \wedge \neg w$, we have $\sigma \vDash \{p \wedge \neg w\}\ S\ \{\neg q\}$.
   c. If S is nondeterministic then if $\sigma \vDash p \wedge \neg w$, we still know $\sigma \nvDash_{tot}. \{p \wedge \neg w\}\ S\ \{q\}$ but both $\sigma \vDash$ and $\sigma \nvDash \{p \wedge \neg w\}\ S\ \{\neg q\}$ are possible. Similarly, if $\sigma \vDash \neg p \wedge \neg w$, we know $\sigma \nvDash_{\text{tot}} \{\neg p \wedge \neg w\}\ S\ \{q\}$, but both $\sigma \vDash$ and $\sigma \nvDash \{p \wedge \neg w\}\ S\ \{\neg q\}$ are possible.

4. For deterministic S, $wp(S, q_1 \vee q_2) = wp(S, q_1) \cup wp(S, q_2)$. For nondeterministic S, we have $\supseteq$ instead of =.

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. $M(S, \sigma) = \{\perp\}$ implies $wlp(S, q) \wedge wlp(S, \neg q)$

   b. $M(S, \sigma) = \{\perp\}$ 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 $wp(S, q)$.

   f. For deterministic S, $\neg wp(S, q) \wedge \neg wp(S, \neg q)$ implies $M(S, \sigma) = \{\perp\}$, so $M(S, \sigma) - \perp$ is empty.

   g. For nondeterministic S, it's possible to have $M(S, \sigma) = \{\tau_1, \tau_2\}$ where $\tau_1 \vDash q$ and $\tau_2 \vDash \neg q$. When that happens, $wp(S, q)$ and $wp(S, \neg q)$ are both false but $\perp \notin M(S, \sigma)$.

