

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 $\tau \in \Sigma \cup \{\perp\}$.
 - a. For which $\sigma \models w$ do we have $\sigma \models [w] S [q]$?
 - b. For which $\sigma \models \neg w$ do we have $\sigma \models [\neg w] S [q]$? How about $\sigma \models \{\neg w\} S \{q\}$?
 - c. For which $\sigma \models w$ do we have $\sigma \models [w] S [\neg q]$?
 - d. For which $\sigma \models \neg w$ do we have $\sigma \models \{\neg w\} S \{\neg q\}$?
 - e. If S is nondeterministic, how do we have to modify the statement in part (d)?

2. If $\sigma \models w$ and $\sigma \models \{w\} S \{q\}$ and $\sigma \not\models [w] S [q]$,
 - a. What can we conclude about $M(S, \sigma)$?
 - b. If in addition, S is deterministic, what more can we conclude about $M(S, \sigma)$?

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 $\sigma \in \Sigma$, $\sigma \models wp(S, q)$ iff $M(S, \sigma) \models q$
 - b. For all $\sigma \in \Sigma$, $\sigma \models wlp(S, q)$ iff $M(S, \sigma) \dashv \perp \models q$
 - c. $\models [wp(S, q)] S [q]$
 - d. $\models \{wlp(S, q)\} S \{q\}$
 - e. $\models [p] S [q]$ iff $\models p \rightarrow wp(S, q)$
 - f. $\models \{p\} S \{q\}$ iff $\models p \rightarrow wlp(S, q)$
 - g. $\models \{\neg wp(S, q)\} S \{\neg q\}$, if S is deterministic
 - h. $\models [\neg wlp(S, q)] S [\neg q]$, if S is deterministic
 - i. $\not\models p \rightarrow wp(S, q)$ iff $\not\models_{tot} \{p\} S \{q\}$
 - j. $\not\models p \rightarrow wlp(S, q)$ iff $\not\models \{p\} S \{q\}$

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

2. (Partial but not total correctness when the wp is satisfied)
 - a. If $\sigma \models w$ and $\sigma \models \{w\} S \{q\}$ then $M(S, \sigma) - \{\perp\} \models q$. If $\sigma \not\models [w] S [q]$ then $M(S, \sigma) \not\models q$. This can only happen if $\perp \in M(S, \sigma)$. (I.e., S can diverge under σ .)
 - b. If in addition S is deterministic, then we don't just have $\perp \in M(S, \sigma)$, we have $\{\perp\} = M(S, \sigma)$. (I.e., S diverges 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. $M(S, \sigma) = \{\perp\}$ implies $wlp(S, q) \wedge wlp(S, \neg q)$
 - b. $M(S, \sigma) = \{\perp\}$ implies $\sigma \models \neg wp(S, q) \wedge \neg wp(S, \neg q)$.
 - 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 $wp(S, q)$.