Weakest Preconditions 1 & 2; Domain Predicates

CS 536: Science of Programming, Spring 2023

Solution

Class 10: Weakest Preconditions part 1

1. If $B_1 \wedge B_2$, then $(B_1 \rightarrow w_1) \wedge (B_2 \rightarrow w_2)$ implies $w_1 \wedge w_2$, so whichever arm we execute is run with its *wp* satisfied. On the other hand, $B_1 \wedge B_2$ with $(B_1 \wedge w_1) \vee (B_2 \wedge w_2)$ implies $B_1 \wedge B_2 \wedge (w_1 \vee w_2)$, which leaves open the possibilities of executing S_1 when w_1 isn't satisfied and of executing S_2 when w_2 isn't satisfied.

2. $wp(S, p \vee q) \rightarrow wp(S, p) \vee wp(S, q)$ holds if S is deterministic but might not hold if S is nondeterministic. The other three statements (below) hold for both deterministic and nondeterministic programs.
   - $wp(S, p) \vee wp(S, q) \rightarrow wp(S, p \vee q)$
   - $wp(S, p \wedge q) \rightarrow wp(S, p) \wedge wp(S, q)$
   - $wp(S, p) \wedge wp(S, q) \rightarrow wp(S, p \wedge q)$

3. (Descriptions of wp/wlp properties when σ satisfies the precondition)
   For all the cases below, we're assuming that σ satisfies the precondition of the correctness triple. (This only affects cases (b), (c), and (e), since (a) and (d) have to have that satisfaction.)

   a. $\sigma \not\models \{wlp(S,q)\}\ S\ \{q\}$
      This holds iff $\sigma \models wlp(S,q)$ but $M(S,\sigma)-\bot \not\models q$. But $\sigma \models wlp(S,q)$, so, we're guaranteed $M(S,\sigma)-\bot \models q$. The contradiction tells us that $\sigma \not\models \{wlp(S,q)\}\ S\ \{q\}$ can never happen.

   b. Since $\sigma \models \neg wlp(S,q)$, we know $M(S,\sigma) \not\models q$. Since S is deterministic, we get $M(S,\sigma)$ = some $\{\tau\}$ where $\tau \not\models q$; hence $\tau = \bot$ or $\tau \models \neg q$. So we have partial correctness: $\sigma \models \{\neg wlp(S, q)\}\ S\ \{\neg q\}$. But for $\sigma \models_{\text{tot}} \{\neg wlp(S,q)\}\ S\ \{\neg q\}$, we need $M(S,\sigma) = \{\tau\} \models \neg q$. This is stronger than saying $\tau = \bot$ or $\tau \models \neg q$. So though we know partial correctness (under σ) of $\{\neg wlp(S, q)\}\ S\ \{\neg q\}$, we don't know total correctness.

   c. From the definition, $\sigma \models_{\text{tot}} \{wp(S,q)\}S\{q\}$ iff $M(S,\sigma) \models q$ iff for all $\tau \in M(S,\sigma)$, $\tau \models q$.

d. To know $\sigma \not\models_{tot} \{wp(S,q)\}\ S\ \{q\}$, we need $\sigma \models wp(S,q)$ and $M(S,\sigma) \not\models q$. But by definition of wp, $\sigma \models wp(S,q)$ implies $M(S,\sigma) \models q$, so this situation can never happen.

e. To know $\sigma \models \{\neg wp(S,q)\}\ S\ \{\neg q\}$, we meed $\sigma \models \neg wp(S,q)$ to imply $M(S,\sigma) - \bot \models \neg q$. By definition of wp, $\sigma \models \neg wp(S,q)$ tells us that $M(S,\sigma) \not\models q$. Since S is deterministic, we know $M(S,\sigma)$ = some $\{\tau\}$, so $M(S,\sigma) \not\models q$ tells us $\tau = \bot$ or $\tau \models \neg q$. But then $M(S,\sigma) - \bot$ does $\models \neg q$. So this situation always happens.

Class 11: Weakest Preconditions part 2

4. (The *wlp of* ***if*** $x < 0$ ***then*** $x := -x$ ***fi***, $x^2 \geq x$)

a. The *wlp* of the true branch is $(x < 0 \rightarrow wlp(x := -x,\ x^2 \geq x)) \equiv (x < 0 \rightarrow (-x)^2 \geq -x)$.

b. The *wlp* of the false branch is $(x \geq 0 \rightarrow wlp(\textbf{skip},\ x^2 \geq x)) \equiv (x \geq 0 \rightarrow x^2 \geq x)$.

c. The overall *wlp* is part (a) ∧ part (b): $(x < 0 \rightarrow (-x)^2 \geq -x) \wedge (x \geq 0 \rightarrow x^2 \geq x)$.

d. The overall *wlp* simplifies to just true.

Class 11: Domain Predicates [18 points]

5. (Calculate $wp(S,q)$ where $S \equiv y := y/x$ *and* $q \equiv sqrt(y) < x$.)

   a. $D(S) \equiv D(y := y/x) \equiv D(y/x) \equiv x \neq 0$

   b. $w \equiv wlp(S,q) \equiv sqrt(y/x) < x$

   c. $D(w) \equiv D(sqrt(y/x)) \equiv D(y/x) \wedge y/x \geq 0 \equiv x \neq 0 \wedge y/x \geq 0$

   d. $wp(S, q) \equiv D(S) \wedge D(w) \wedge w$
      $\equiv (x \neq 0) \wedge (sqrt(y/x) < x) \wedge (x \neq 0 \wedge y/x \geq 0)$
      $\Leftrightarrow x \neq 0 \wedge y/x \geq 0 \wedge sqrt(y/x) < x$ (After some simplification)

6. (Calculate $wp(S,q)$ where $S \equiv$ ***if*** $y \geq 0$ ***then*** $x := y/x$ ***else*** $x := -x/y$ ***fi*** and $q \equiv r < x \leq y$)

   a. $D(S) \equiv D(\textbf{if } y \geq 0 \textbf{ then } x := y / x \textbf{ else } x := -x / y \textbf{ fi})$
      $\equiv D(y \geq 0) \wedge (y \geq 0 \rightarrow D(x := y / x)) \wedge (y < 0 \rightarrow D(x := -x / y))$
      $\equiv T \wedge (y \geq 0 \rightarrow D(y / x)) \wedge (y < 0 \rightarrow D(-x / y))$
      $\equiv (y \geq 0 \rightarrow x \neq 0) \wedge (y < 0 \rightarrow y \neq 0)$
      $\Leftrightarrow y \geq 0 \rightarrow x \neq 0$ (after some simplification)

   b. $w \equiv wlp(S, q) \equiv wlp(\textbf{if } y \geq 0 \textbf{ then } x := y / x \textbf{ else } x := -x / y \textbf{ fi},\ r < x \leq y)$
      $\equiv (y \geq 0 \rightarrow wlp(x := y / x,\ r < x \leq y)) \wedge (y < 0 \rightarrow wlp(x := -x / y,\ r < x \leq y))$
      $\equiv (y \geq 0 \rightarrow r < y / x \leq y) \wedge (y < 0 \rightarrow r < -x / y \leq y)$

c. $D(w) \equiv D((y \geq 0 \rightarrow r < y / x \leq y) \wedge (y < 0 \rightarrow r < -x / y \leq y)$

$\equiv D(y \geq 0 \rightarrow r < y / x \leq y) \wedge D(y < 0 \rightarrow r < -x / y \leq y)$

$\equiv (T \wedge D(r < y / x \leq y)) \wedge (T \wedge D(r < -x / y \leq y))$

$\equiv D(y / x) \wedge D(-x / y)$ (Taking *D* of both implications)

$\equiv x \neq 0 \wedge y \neq 0$

d. $wp(S, q) \equiv D(S) \wedge D(w) \wedge w$

$\equiv ((y \geq 0 \rightarrow x \neq 0) \wedge (y < 0 \rightarrow y \neq 0))$

$\wedge (x \neq 0 \wedge y \neq 0)$

$\wedge ((y \geq 0 \rightarrow r < y / x \leq y) \wedge (y < 0 \rightarrow r < -x / y \leq y))$.

We can do some simplification to get

$wp(S, q) \Leftrightarrow x \neq 0 \wedge y \neq 0$

$\wedge ((y > 0 \rightarrow r < y / x \leq y) \wedge (y < 0 \rightarrow r < -x / y \leq y))$.

