Weakest Preconditions 1 & 2; Domain Predicates

Draft Solution

Class 10: Weakest Preconditions part 1

1. If $B_1 \wedge B_2$, then $p \equiv (B_1 \rightarrow w_1) \wedge (B_2 \rightarrow w_2)$ implies $w_1 \wedge w_2$, so we execute whichever arm is selected with its *wp* true. On the other hand, q implies $B_1 \wedge B_2 \wedge (w_1 \vee w_2)$, which leaves open the possibility of executing S_1 when w_1 doesn't hold and of executing S_2 when w_2 doesn't hold.

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.
   - $wp(S, p) \vee wp(S, q) \rightarrow wp(S, p \vee q)$
   - $wp(S, p \wedge q) \rightarrow wp(S, p) \wedge wp(S, q)$
   - $wp(S, p) \wedge wp(S, q) \rightarrow wp(S, p \wedge q)$

(For Problem 3) Reference 1: If $w \Leftrightarrow wp(S, q)$, then $\models_{\text{tot}} \{w\}\ S\ \{q\}$ and $\not\models_{\text{tot}} \{\neg w\}\ S\ \{q\}$ so for some σ, $\sigma \models \{\neg w\}\ S\ \{\neg q\}$). If S is deterministic, $\not\models_{\text{tot}} \{\neg w\}\ S\ \{q\}$ also implies $\models \{\neg w\}\ S\ \{\neg q\}$. Reference 2: $p \rightarrow q$ is strict iff $q \wedge \neg p$ is satisfiable.

3. (Correctness properties related to $wp(S, q)$) We're given $w \Leftrightarrow wp(S, q)$ and strict $b \rightarrow w$ and $w \rightarrow c$. Are the below statements: Always true? / Always false? / Might be true = Might be false?

3a. If S is deterministic then $\models_{\text{tot}} \{b\}\ S\ \{q\}$.

Always true. From $\models_{\text{tot}} \{w\}\ S\ \{q\}$ we get $\models_{\text{tot}} \{b\}\ S\ \{q\}$ by precond. strengthening, since $b \rightarrow w$.

3b. If S is nondeterministic there exists σ such that $\sigma \models \{\neg c\}\ S\ \{\neg q\}$.

Might be true. We know $\not\models_{tot} \{\neg w\}\ S\ \{q\}$ i.e., for some σ, $M(S, \sigma) \not\models q$. Let $M(S, \sigma) = \Sigma_1 \cup \Sigma_2 \cup \Sigma_3$ where $\Sigma_1 \models q$, $\Sigma_2 \models \neg q$, and $\Sigma_3 \subseteq \{\bot\}$. $M(S, \sigma) \not\models q$ implies that $\Sigma_2 \cup \Sigma_3 \neq \emptyset$. It's possible (but not guaranteed) that $\Sigma_1 = \Sigma_3 = \emptyset$, in which case $M(S, \sigma) = \Sigma_2 \models \neg q$.

3c. If S is nondeterministic, then there exist $\sigma \models \neg c$ and $\tau \in M(S, \sigma)$ such that $\tau \models q$.

Might be true. Since S is nondeterministic, $\models_{\text{tot}} \{w\}\ S\ \{q\}$ implies that for every $\sigma \models \neg w$, we have $\sigma \not\models_{\text{tot}} \{w\}\ S\ \{q\}$. Since $w \rightarrow c$, we know $\neg c \rightarrow \neg w$, so we can restrict ourselves to $\sigma \models \neg c$ and still know $\sigma \not\models_{\text{tot}} \{w\}\ S\ \{q\}$, which in turn implies $M(S, \sigma) \not\models q$. But this only implies that there is some $\tau \in M(S, \sigma)$ that $\not\models q$. There can also be some $\tau \in M(S, \sigma)$ that $\models q$, which is what we wanted.

Class 11: Weakest Preconditions part 2

4. $wlp(u := u*k;\ k := u,\ u > h(k)) \equiv wlp(u := u*k,\ wlp(k := u,\ u > h(k))) \equiv wlp(u := u*k,\ u > h(u)) \equiv u*k > h(u*k))$.

5. $wlp(\textbf{if}\ x < 0\ \textbf{then}\ x := -x\ \textbf{fi},\ x^2 \geq x) \equiv (x < 0 \rightarrow wlp(x := -x,\ x^2 \geq x)) \wedge (x \geq 0 \rightarrow wlp(\textbf{skip},\ x^2 \geq x)) \equiv (x < 0 \rightarrow (-x)^2 \geq -x) \wedge (x \geq 0 \rightarrow x^2 \geq x)$. You were asked to not logically simplify, so that's the answer, along with the acceptable alternative $(x < 0 \wedge (-x)^2 \geq -x) \vee (x \geq 0 \wedge x^2 \geq x)$.

Class 11: Domain Predicates [18 points]

6. (Calculate $wp(y := y/x,\ sqrt(y) < x)$)
   - We want $D(y := y/x) \wedge D(w) \wedge w$ where $w \equiv wlp(y := y/x,\ sqrt(y) < x)$. Calculating,
   - $w \equiv sqrt(y/x) < x$
   - $D(w) \equiv D(sqrt(y/x)) \equiv D(y/x) \wedge y/x \geq 0 \equiv x \neq 0 \wedge y/x \geq 0$
   - $D(y := y/x) \equiv D(y/x) \equiv x \neq 0$
   - So $wp(y := y/x,\ sqrt(y) < x)$

     $\equiv D(y := y/x) \wedge D(w) \wedge w$

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

     $\Leftrightarrow x \neq 0 \wedge y/x \geq 0 \wedge sqrt(y/x) < x$ (After some simplification)

7. (Calculate $wp(\textbf{if}\ y \geq 0\ \textbf{then}\ x := y / x\ \textbf{else}\ x := -x / y\ \textbf{fi},\ r < x \leq y)$)
   - Let $S \equiv \textbf{if}\ y \geq 0\ \textbf{then}\ x := y / x\ \textbf{else}\ x := -x / y\ \textbf{fi}$ and $q \equiv r < x \leq y$.
   - We want $D(S) \wedge D(w) \wedge w$ where $w \equiv wlp(S,\ q)$. We can calculate
   - $w \equiv wlp(S,\ q) \equiv wlp(\textbf{if}\ y \geq 0\ \textbf{then}\ x := y / x\ \textbf{else}\ x := -x / y\ \textbf{fi},\ q)$

     $\equiv (y \geq 0 \rightarrow wlp(x := y / x,\ q)) \wedge (y < 0 \rightarrow wlp(x := -x / y,\ q))$

     $\equiv (y \geq 0 \rightarrow wlp(x := y / x,\ r < x \leq y)) \wedge (y < 0 \rightarrow wlp(x := -x / y,\ r < x \leq y))$

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

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

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

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

     $\equiv D(y / x) \wedge D(-x / y)$ (After some quick simplification of $T \wedge D(y / x) \wedge T$, etc.)

     $\equiv x \neq 0 \wedge y \neq 0$
   - $D(S) \equiv D(wlp(\textbf{if}\ y \geq 0\ \textbf{then}\ x := y / x\ \textbf{else}\ x := -x / y\ \textbf{fi})$

     $\equiv D(y \geq 0) \wedge (y \geq 0 \rightarrow D(x := y / x)) \wedge (y < 0 \rightarrow D(x := -x / y))$

     $\equiv (y \geq 0 \rightarrow D(y / x)) \wedge (y < 0 \rightarrow D(-x / y))$ (Since $D(y \geq 0) \equiv T$ and $D(var := exp) \equiv D(exp)$.)

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

- So $wp(S, q) \equiv D(S) \wedge D(w) \wedge w$

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

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

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

- We can do some simplification to get

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

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

