CS 536 — Solution for Homework 4 (Strength, Weakest Preconditions, Syntactic Substitution)

10/21: pp.2, 3, also added headers

Part 1: Strength

1. (Weaken/strengthen pre-/post-conditions)
   a. $\sigma \models \{p_0\} S \{q_2\}$ -- we can always strengthen preconditions and weaken postconditions.
   b. $\sigma \models_{tot} \{p_0\} S \{q_2\}$ for the same reason.

Part 2: Weakest preconditions

2. (Relationship between wp and modified triples.) Remember, we're looking only at $\sigma$ that $\vdash$ the precondition.
   a. $\sigma \models$ and $\sigma \models_{tot} \{p \wedge w\} S \{q\}$. Total correctness holds by definition of wp and total correctness implies partial correctness.
   b. Both $\sigma \vdash$ and $\not\vdash \{p \wedge \neg w\} S \{q\}$ are possible ($\vdash$ holds if $S$ leads to $\bot$, but $\not\vdash$ holds if $S$ terminates).

2c. As in (a), $\sigma \models$ and $\sigma \models\{\neg p \wedge w\} S \{q\}$.
2d. As in (b), both $\sigma \vdash$ and $\sigma \not\vdash\{\neg p \wedge w\} S \{q\}$ always.
2e. $\sigma \not\vdash$ and $\not\vdash_{tot} \{p \wedge w\} S \{q\}$. If $S$ under $\sigma$ doesn't terminate, then $\sigma \vdash$ the triple. Otherwise $S$ terminates $\vdash q$, so $\sigma \not\vdash$ the triple. Either way, $\sigma \not\vdash_{tot}$ the triple.
2f. $\sigma \vdash$ and $\not\vdash_{tot} \{p \wedge \neg w\} S \{q\}$. Since $\sigma \vdash \neg w$, running $S$ under $\sigma$ does not terminate $\vdash q$ by definition of wp. Either $S$ doesn't terminate or it terminates $\not\vdash q$ (and hence $\vdash \neg q$ because $S$ is deterministic).

Either way, $\sigma \vdash$ and $\not\vdash_{tot}$ the triple.
2g. As in (c), $\sigma \vdash$ and $\not\vdash\{\neg p \wedge w\} S \{\neg q\}$ are possible; $\not\vdash_{tot}$ always holds.
2h. As in (f), $\sigma \vdash$ and $\not\vdash_{tot} \{\neg p \wedge \neg w\} S \{\neg q\}$.

3. (Simple wp)
   a. $wp(n := n \ast (n-k), \ n < k \ast n) \equiv n \ast (n-k) < k \ast (n \ast (n-k))$
   b. $wp(x := x \ast y; y := y-x, x^2 > y^2) \equiv wp(x := x \ast y, wp(y := y-x, x^2 > y^2))$
      $\equiv wp(x := x \ast y, x^2 > (y-x^2) \equiv (x \ast y)^2 > (y - x \ast y)^2$

4. (Calculate and simplify wp) For each of the problems, we calculate the wp and logically simplify it to get the precondition for the triple.
4a. $wp(j := j+i; i := i-k, i \leq j \wedge j-i < n+k)$
   $\equiv wp(j := j+i, wp(i := i-k, i \leq j \wedge j-i < n+k))$
   $\equiv wp(j := j+i, i-k \leq j \wedge j-(i-k) < n+k)$
   $\equiv i-k \leq j+i \wedge (j+i)-(i-k) < n+k$
   $\Leftrightarrow -k \leq j \wedge j+i-i+k < n+k$
   $\Leftrightarrow -k \leq j \wedge j+k < n+k$
   $\Leftrightarrow -k \leq j < n$
4b. \( wp(j := i*j; k := j*i+k, 0 < i < j < k) \)
\[ \equiv wp(j := i*j, 0 < i < j < j*i+k) \]
\[ \equiv 0 < i < i*j < j*i+k \]
\[ \Leftrightarrow i > 0 \land j > 1 \land 0 < i*j < j*i+(k-1) \]  [10/21 this line and next]
\[ \Leftrightarrow i > 0 \land j > 1 \land k > 1 \text{ (since } i \text{ and } j \text{ > 0, we also need } k-1 > 0 \text{ to get } i*j < j*i*(k-1) > 0.) \]

4c. \( wp(\text{if } x \geq 0 \text{ then } x := x+k \text{ else } y := y-k \text{ fi}, x > y) \)
\[ \equiv (x \geq 0 \rightarrow wp(x := x+k, x > y)) \land (x < 0 \rightarrow wp(y := y-k, x > y)) \]
\[ \equiv (x \geq 0 \rightarrow x+k > y) \land (x < 0 \rightarrow x > y-k) \]
\[ \Leftrightarrow (x \geq 0 \rightarrow x > y-k) \land (x < 0 \rightarrow x > y-k) \]
\[ \Leftrightarrow T \]

4d. \( wp(\text{if } b[M] \leq v \text{ then } L := M \text{ else } R := M \text{ fi}, L < R \land b[L] \leq v < b[R]) \)
\[ \equiv (b[M] \leq v \rightarrow wp(L := M, L < R \land b[L] \leq v < b[R])) \]
\[ \land (b[M] > v \rightarrow wp(R := M, L < R \land b[L] \leq v < b[R])) \]
\[ \equiv (b[M] \leq v \rightarrow M < R \land b[M] \leq v < b[R]) \land (b[M] > v \rightarrow L < M \land b[L] \leq v < b[M]) \]
\[ \Leftrightarrow (b[M] \leq v \rightarrow M < R \land v < b[R]) \land (b[M] > v \rightarrow L < M \land b[L] \leq v) \]

(Note for an actual binary search, we'd be able to simplify further because of the larger context, but here, we can't.)

4e. For \( wp(\text{if } x < 0 \text{ then } x := 2-x \text{ else if } x < 2 \text{ then } x := x+2 \text{ fi fi, } x^2 > x) \), let's first calculate the \( wp \) of the nested \textit{if-fi}. Let \( NI \equiv \text{if } x < 2 \text{ then } x := x+2 \text{ else skip fi}. \) Then \( wp(NI, x^2 > x) \)
\[ \equiv wp(\text{if } x < 2 \text{ then } x := x+2 \text{ else skip fi}, x^2 > x) \]
\[ \equiv (x < 2 \rightarrow wp(x := x+2, x^2 > x)) \land (x \geq 2 \rightarrow wp(\text{skip, } x^2 > x))) \]
\[ \equiv (x < 2 \rightarrow (x+2)^2 > x+2) \land (x \geq 2 \rightarrow x^2 > x) \]

Now we can calculate the \( wp \) of the outer \textit{if-fi}:
\[ wp(\text{if } x < 0 \text{ then } x := 2-x \text{ else } NI \text{ fi, } x^2 > x) \]
\[ \equiv (x < 0 \rightarrow wp(x := 2-x, x^2 > x)) \land (x \geq 0 \rightarrow wp(NI, x^2 > x)) \]
\[ \equiv (x < 0 \rightarrow (2-x)^2 > 2-x) \land (x \geq 0 \rightarrow (x < 2 \rightarrow (x+2)^2 > x+2) \land (x \geq 2 \rightarrow x^2 > x)) \]

To logically simplify, if \( x < 0 \) then \( (2-x)^2 > 2-x \), if \( x < 2 \) then \( (x+2)^2 > x+2 \). Finally, if \( x \geq 2 \) then \( x^2 > x \). So the entire \( wp \) is equivalent to true, and we can use that as the precondition.
Part 3: Syntactic Substitution

5.  (Substitutions involving \( p \equiv x \times y < f(a) \lor \forall x \cdot x \geq a \rightarrow \exists y \cdot x \div y > y-a-z \))

To make the substitutions more visible, I'll underline the new pieces of text (you didn't have to do this).

5a. The occurrence of \( x \) outside the \( \forall x \) is free and should be replaced, but the ones inside the \( \forall x \) are bounded, so are shielded from substitution.

\[
p[y-z/x] = (x \times y < f(a) \lor \forall x \cdot x \geq a \rightarrow \exists y \cdot x \div y > y-a-z)[y-z/x]
\]

\[
= (y-z) \times y < f(z) \lor \forall x \cdot x \geq a \rightarrow \exists y \cdot x \div y > y-a-z
\]

5b. Similarly to (a), only the two \( y \)'s not in \( \exists y \) are free (even though one of them is in the scope of the \( \forall x \)).

\[
p[y+z/y] = (x \times y < f(a) \lor \forall x \cdot x \geq a \rightarrow \exists y \cdot x \div y > y-a-z)[y+z/y]
\]

\[
= x \times (y+z) < f(a) \lor \forall x \cdot x \geq a \times (y+z) \rightarrow \exists y \cdot x \div y > y-a-z
\]

5c. We rename the quantified \( \forall x \) (to \( \forall v \)) and \( \forall y \) (to \( \forall w \)) to avoid capture. (Free \( x \)'s are not renamed.)

\[
p[x \times y/a] = (x \times y < f(a) \lor \forall x \cdot x \geq a \times y \rightarrow \exists y \cdot x \div y > y-a-z)[x \times y/a]
\]

\[
\equiv (x \times y < f(x \times y) \lor \forall x \cdot x \geq a \times y \rightarrow \exists y \cdot x \div y > y-a-z)[x \times y/a] \quad \text{Replace the free } x
\]

\[
\equiv x \times y < f(x \times y) \lor \forall v \cdot (v \geq a \times y \rightarrow \exists w \cdot v \div w > w-a-z)[x \times y/a] \quad \text{Start renaming } x \text{ to } v
\]

\[
\equiv x \times y < f(x \times y) \lor \forall v \cdot (v \geq a \times y \rightarrow \exists w \cdot v \div w > w-a-z)[x \times y/a] \quad \text{Finish renaming}
\]

(The double-underlined \( v \)'s show where the \( x \)'s were renamed to \( v \). You didn't have to do this.)

[10/21 Next two lines]

\[
\equiv x \times y < f(x \times y) \lor \forall v \cdot (v \geq a \times y \rightarrow \exists w \cdot v \div w > w-a-z)[x \times y/a] \quad \text{Rename } y \text{ to } w
\]

\[
\equiv x \times y < f(x \times y) \lor \forall v \cdot (v \geq a \times y \rightarrow \exists w \cdot v \div w > w-a-z)[x \times y/a] \quad \text{Replace } a
\]

5d. We rename the quantified \( \exists y \) (to \( \exists w \)) to avoid capture. Just to be different, let's rename then substitute.

\[
p[x \times y/a] = (x \times y < f(a) \lor \forall x \cdot x \geq a \times y \rightarrow \exists w \cdot x \times y > y-a-z)[x \times y/a]
\]

\[
\equiv (x \times y < f(a) \lor \forall x \cdot x \geq a \times y \rightarrow \exists w \cdot (x \times y > y-a-z)[w/y])[x \times y/a] \quad \text{Start renaming } y \text{ to } w
\]

\[
\equiv (x \times y < f(a) \lor \forall x \cdot x \geq a \times y \rightarrow \exists w \cdot (x \times y > y-a-z)[y/a][x \times y/a] \quad \text{Finish renaming}
\]

\[
\equiv x \times y < f(y \div a) \lor \forall x \cdot x \geq (y \div a) \times y \rightarrow \exists w \cdot x \times w > w-(x \times y) \div a] \quad \text{Replace the free } a.
\]

5e. To calculate \( p[x+y/a][y+z/x] \), we'll first calculate \( p_1 \equiv p[x \times y/a] \) (which will involve renaming \( x \) to \( v \)), then we'll calculate \( p_1[y-z/x] \) (which involves renaming \( y \) to \( w \)).

\[
p_1 = p[x \times y/a] = (x \times y < f(a) \lor \forall x \cdot x \geq a \times y \rightarrow \exists y \cdot x \times y > y-a-z)[x \times y/a]
\]

\[
= (x \times y < f(a) \times x \times y) \lor \forall v \cdot v \geq a \rightarrow \exists y \cdot v \div y > y-a-z)[x \times y/a] \quad \text{Renaming } x \text{ to } v
\]

[10/21 here to end of problem]

\[
= (x \times y < f(a) \times x \times y) \lor \forall v \cdot v \geq a \rightarrow \exists w \cdot v \div w > w-a-z)[x \times y/a] \quad \text{Renaming } y \text{ to } w
\]

\[
= x \times y < f(x \times y) \lor \forall v \cdot v \geq x \times y \rightarrow \exists w \cdot v \div w > w-(x \times y) \div a \quad \text{Substitute for } a
\]

Then

\[
p[x \times y/a][y-z/x]
\]

\[
= (x \times y < f(x \times y) \lor \forall v \cdot v \geq x \times y \rightarrow \exists w \cdot v \div w > w-(x \times y) \div a)[y-z/x]
\]

\[
= (y-z) \times y < f(y-z+y) \lor \forall v \cdot v \geq y-z+y \rightarrow \exists w \cdot v \div w > w-(y-z+w) \div a \quad \text{Substitute for } x
\]

CS 536: Science of Programming – 3 – © James Sasaki, 2018