# *Solution – HW 4: Hoare Triples, wp/wlp, Syntactic Substitution*

*CS 536: Science of Programming, Fall 2019*

**Lectures 8 & 9: Hoare Triples**

1. If $\sigma \vDash \{p\}\ S\ \{q\}$ but $\sigma \vDash \neg p$, then we don't know whether $\bot \in$ or $\notin M(S, \sigma)$ or $M(S, \sigma) - \{\bot\} \vDash$ or $\nvDash q$. If $\sigma \vDash \{p\}\ S\ \{q\}$, then $\sigma \vDash p$ tells us either $\bot \in M(S, \sigma)$ or ($\bot \notin M(S, \sigma)$ and $M(S, \sigma) - \{\bot\} \vDash q$).

2. $\vDash_{tot} \{p\}\ S\ \{q\}$ iff ($\vDash \{p\}\ S\ \{q\}$ and $\vDash_{tot} \{p\}\ S\ \{\mathtt{T}\}$)

3. $\sigma \nvDash p$ must hold. If $\sigma \vDash p$, then $\sigma \vDash_{tot} \{p\}\ S\ \{\mathtt{T}\}$ tells us that $M(S, \sigma)$ always terminates. So $\bot \in M(S, \sigma)$, we can't have $\sigma \vDash p$.

4. For $\sigma \nvDash \{p\}\ S\ \{q\}$, we must have $\sigma \vDash p$, $\bot \notin M(S, \sigma)$, and $M(S, \sigma) - \{\bot\} \nvDash q$. If $S$ is deterministic, then $M(S, \sigma) - \{\bot\}$ contains just one state $\tau$ that $\nvDash q$. Since $\tau \neq \bot$, we have $\tau \vDash \neg q$. If $S$ is nondeterministic, then $M(S, \sigma) - \{\bot\} \nvDash q$ must contain at least one state $\tau$ such that $\tau \vDash \neg q$. It may or may not contain other states and those states may $\vDash q$ or $\vDash \neg q$.

5. First, if $\sigma \nvDash p$ then $\sigma \vDash$ and $\vDash_{tot}$ all triples $\{p\}\ S$ {anything}. So assume $\sigma \vDash p$. For $\sigma \nvDash \{p\}\ S\ \{q\}$, we must have then that $M(S, \sigma)$ does not $\bot$ and $\nvDash q$ (and since $S$ is deterministic, $M(S, \sigma) \vDash \neg q$). So $\sigma \vDash_{tot} \{p\}\ S\ \{\neg q\}$.

6. First, $\sigma \nvDash_{tot} \{p\}\ S\ \{q\}$ implies $\sigma \vDash p$ and $\bot \in M(S, \sigma)$ or $M(S, \sigma) - \{\bot\} \nvDash q$. For deterministic $S$, $M(S, \sigma) = \{\tau\}$ where $\tau = \bot$ or $\tau \neq \bot$ and $\tau \vDash \neg q$. If $\tau = \bot$ then $\sigma \vDash \{p\}\ S\ \{q\}$ and $\{p\}\ S\ \{\neg q\}$. If $\tau \vDash \neg q$, then $\sigma \vDash_{tot} \{p\}\ S\ \{\neg q\}$

7. With $IF_N \equiv$ **`if`** $B_1 \rightarrow S_1 \ \square\ B_2 \rightarrow S_2$ **`fi`**, $wp(IF_N, q)$ is not always $\Leftrightarrow (B_1 \wedge wp(S_1, q)) \vee (B_2 \wedge wp(S_2, q))$. If $B_1$ and $B_2$ are both true, we need both $wp(S_1, q)$ and $wp(S_2, q)$ to hold because we might execute either $S_1$ or $S_2$. To get $\Leftrightarrow$, we have to add a third disjunct, $(B_1 \wedge wp(S_1, q) \wedge B_2 \wedge wp(S_2, q))$. This doesn't come up with deterministic **`if`** statements because they have $B_2 \leftrightarrow \neg B_1$, so our third disjunct would always be false.

8. We can we always strengthen preconditions or weaken postconditions (up to a limit of precondition $\Leftrightarrow \mathtt{F}$ and postcondition $\Leftrightarrow \mathtt{T}$). Strengthening preconditions and weakening postconditions isn't always useful: in the limit, we get $\{\mathtt{F}\}\ S\ \{\mathtt{T}\}$, which is valid for both partial and total correctness but says nothing about how $S$ runs. On the other hand, these can certainly be useful. Say we know $\{p_1\}\ S_1\ \{q_1\}$. If we want to form a sequence with a triple $\{p_0\}\ S_0\ \{q_0\}$ to form $\{p_0\}\ S_0 \mathtt{;}\ S_1\ \{q_1\}$, if we know $q_0 \rightarrow p_1$, then we know we can form the sequence by strengthening the precondition: $\{p_1\}\ S_1\ \{q_1\}$ implies $\{q_0\}\ S_1\ \{q_1\}$. Similarly, if we

 

have a triple $\{p_2\}\ S_2\ \{q_2\}$ and want to form $\{p_1\}\ S_1\texttt{;}\ S_2\ \{q_2\}$, it's sufficient to know $q_1 \rightarrow p_2$, which lets us weaken the postcondition of $S_1$ to get $\{p_1\}\ S_1\ \{p_2\}$.

9. The implication $wp(S, p \vee q) \rightarrow wp(S, p) \vee wp(S, q)$ holds for deterministic $S$ but not necessarily for nondeterministic $S$. The standard example is a coin-flip program that nondeterministically returns $coin = heads$ or $coin = tails$. Then $wp(S, coin = heads \vee coin = tails) \Leftrightarrow \texttt{T}$, since the coin always comes up as one of heads or tails. But $wp(S, coin = heads)$ and $wp(S, coin = tails)$ are both $\Leftrightarrow \texttt{F}$ because there's no way to guarantee that the next coin-flip will return heads, and no way to guarantee that the next coin-flip will return tails. In this case, $wp(S, p \vee q) \nrightarrow wp(S, p) \vee wp(S, q)$ because $\texttt{T} \nrightarrow \texttt{F}$.

**Lectures 10 & 11: wp and wlp**

10. (Relationships between $\{p_0\}\ S\ \{q\}$, $\{p_1\}\ S\ \{q\}$, $\{\neg p_0\}\ S\ \{\neg q\}$, $\{\neg p_1\}\ S\ \{\neg q\}$).
We are given $p_0 \rightarrow w \rightarrow p_1$ where $w \Leftrightarrow wp(S, q)$.
    - 10a. $\models_{\text{tot}} \{p_0\}\ S\ \{q\}$ always holds because $p_0$ is stronger than the weakest precondition $w$.
    - 10b. If $w$ is strictly stronger than $p_1$ (i.e., $w \rightarrow p_1$ but $p_1 \nrightarrow w$), then $\not\models_{\text{tot}} \{p_1\}\ S\ \{q\}$ because $w$ is the *weakest* precondition and $p_1$ is weaker than that.
    - 10c. We can show $\models \{\neg p_0\}\ S\ \{\neg q\}$ iff $\models w \leftrightarrow p_0$. Because $w$ is the *wp*, we know $\models \{\neg w\}\ S\ \{\neg q\}$, so certainly $\models \{\neg p_0 \wedge \neg w\}\ S\ \{\neg q\}$. Also, we know $\models_{\text{tot}} \{w\}\ S\ \{q\}$ so we know $\models_{\text{tot}} \{\neg p_0 \wedge w\}\ S\ \{q\}$ and therefore $\not\models \{\neg p_0 \wedge w\}\ S\ \{\neg q\}$. So it follows that $\models \{\neg p_0\}\ S\ \{\neg q\}$ iff $\sigma \models \neg p_0 \rightarrow \neg w$ iff $\sigma \models w \rightarrow p_0$ iff $\sigma \models w \leftrightarrow p_0$ (since we're given $p_0 \rightarrow w$).
    - 10d. Since $w$ is the weakest precondition, we know $\models \{\neg w\}\ S\ \{\neg q\}$. Since $w \rightarrow p_1$, we know $\neg p_1 \rightarrow \neg w$, so it follows that $\models \{\neg p_1\}\ S\ \{\neg q\}$.

11. (Calculate *wp* or *wlp*)
    - 11a. (Calculate $wlp(\texttt{x := x + y; y := x*z+y, x - y - z < f(x, y, z)})$)
    Let $S_1 \equiv$ `x := x + y` and $S_2 \equiv$ `y := x*z+y` and $q \equiv$ `x−y−z < f(x, y, z)`,
    We know $wlp(S_1\texttt{;}\ S_2, q) \equiv wlp(S_1, wlp(S_2, q))$.
    Calculate $wlp(S_2, q)) \equiv wlp($`y := x*z+y, x−y−z < f(x, y, z)`$)$
    $\equiv$ `x−(x*z+y)−z < f(x, x*z+y, z)`
    So $wlp(S_1, wlp(S_2, q)) \equiv wlp($`x := x + y, x−(x*z+y)−z < f(x, x*z+y, z)`$)$
    $\equiv$ `(x−(x*z+y)−z < f(x, x*z+y, z))[x+y/x]`
    $\equiv$ `x+y−((x+y)*z+y)−z < f(x+y, (x+y)*z+y, z)`

    - 11b. (Calculate $wlp($**`if`** `x ≥ y` **`then`** `x := x−y` **`fi;`** `y := f(f(x/2, y), x-y), x < y`$)$)
    Let $S \equiv$ **`if`** `x ≥ y` **`then`** `x := x−y` **`else skip fi`** and $e \equiv$ `f(f(x/2, y), x−y)`.
    Our goal is $wlp(S\texttt{;}$ `y` $:= e$, `x < y`$)$
    First calculate $p_1 \equiv wlp($`y` $:= e$, `x < y`$) \equiv$ `x` $< e \equiv$ `x < f(f(x/2, y), x−y)`.

Now calculate $p_2 \equiv wlp(S\texttt{;}\ \texttt{y} := e, \texttt{x} < \texttt{y})$

$\equiv wlp(S, wlp(\texttt{y} := e, \texttt{x} < \texttt{y}))$

$\equiv wlp(S, p_1)$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow wlp(\texttt{x} := \texttt{x-y}, p_1)) \wedge (\texttt{x} < \texttt{y} \rightarrow wlp(\textbf{skip}, p_1))$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow p_1[\texttt{x-y/x}]) \wedge (\texttt{x} < \texttt{y} \rightarrow p_1)$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow (\texttt{x} < \texttt{f(f(x/2, y), x-y))[x-y/x]}) \wedge (\texttt{x} < \texttt{y} \rightarrow p_1)$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow (\texttt{x-y} < \texttt{f(f((x-y)/2, y))))} \wedge (\texttt{x} < \texttt{y} \rightarrow \texttt{x} < \texttt{f(f(x/2, y), x-y)}$

11c. (Calculate $wp(\textbf{if}\ \texttt{x} \geq \texttt{y}\ \textbf{then}\ \texttt{x} := \texttt{x-y}\ \textbf{fi;}\ \texttt{y} := \texttt{f(f(x/2, y), x*y)}, \texttt{x} < \texttt{y})$)

As in part (b), let $S \equiv \textbf{if}\ \texttt{x} \geq \texttt{y}\ \textbf{then}\ \texttt{x} := \texttt{x-y}\ \textbf{else skip fi}$ and $e \equiv \texttt{f(f(x/2, y), x-y)}$. Also as in part (b) again let $p_1 \equiv wlp(\texttt{y} := e, \texttt{x} < \texttt{y}) \equiv \texttt{x} < \texttt{f(f(x/2, y), x-y)}$.

Now let $q_1 \equiv D(\texttt{y} := e) \equiv D(e) \equiv D(\texttt{f(f(x/2, y), x-y)})$

$\equiv \texttt{f(x/2, y)} > \texttt{x-y} \wedge D(\texttt{f(x/2, y)})$ (recall that $\mathrm{f}(u, v) \equiv u > v$)

$\equiv \texttt{f(x/2, y)} > \texttt{x-y} \wedge \texttt{x/2} > \texttt{y}$

Then let $w_1 \equiv wp(\texttt{y} := e, \texttt{x} < \texttt{y}) \equiv wlp(\texttt{y} := e, \texttt{x} < \texttt{y}) \wedge D(\texttt{y} := e) \equiv p_1 \wedge q_1$

And let $w_2 \equiv wp(S\texttt{;}\ \texttt{y} := e, \texttt{x} < \texttt{y}) \equiv wp(S, wp(\texttt{y} := e, \texttt{x} < \texttt{y})) \equiv wp(S, p_1 \wedge q_1)$

$\equiv wlp(S, p_1 \wedge q_1) \wedge D(S)$.

$D(S)$ is easy to calculate: Since $S \equiv \textbf{if}\ \texttt{x} \geq \texttt{y}\ \textbf{then}\ \texttt{x} := \texttt{x-y}\ \textbf{else skip fi}$, nothing in $S$ can cause an error, so $D(S) \equiv \texttt{T}$.

For $wlp(S, p_1 \wedge q_1)$, there's a bit of a trick. $wlp(S, p_1 \wedge q_1) \equiv wlp(S, p_1) \wedge wlp(S, q_1)$ by the conjunction rule, and in part (b), we calculated $p_2 \equiv wlp(S, p_1)$.

We can calculate $q_2 \equiv wlp(S, q_1) \equiv wlp(\textbf{if}\ \texttt{x} \geq \texttt{y}\ \textbf{then}\ \texttt{x} := \texttt{x-y}\ \textbf{else skip fi}, q_1)$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow wlp(\texttt{x} := \texttt{x-y}, q_1)) \wedge (\texttt{x} < \texttt{y} \rightarrow wlp(\textbf{skip}, q_1))$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow q_1[\texttt{x-y/x}]) \wedge (\texttt{x} < \texttt{y} \rightarrow q_1)$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow (\texttt{f(x/2, y)} > \texttt{x-y} \wedge \texttt{x/2} > \texttt{y})[\texttt{x-y/x}]) \wedge (\texttt{x} < \texttt{y} \rightarrow \texttt{f(x/2, y)} > \texttt{x-y} \wedge \texttt{x/2} > \texttt{y})$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow \texttt{f((x-y)/2, y)} > \texttt{(x-y)-y} \wedge \texttt{(x-y)/2} > \texttt{y})$

$\wedge (\texttt{x} < \texttt{y} \rightarrow \texttt{f(x/2, y)} > \texttt{x-y} \wedge \texttt{x/2} > \texttt{y})$

So altogether, $wp(S\texttt{;}\ \texttt{y} := e, \texttt{x} < \texttt{y}) \equiv p_2 \wedge q_2$

$\equiv (\texttt{x} \geq \texttt{y} \rightarrow (\texttt{x-y} < \texttt{f(f((x-y)/2, y))))}$

$\wedge (\texttt{x} < \texttt{y} \rightarrow \texttt{x} < \texttt{f(f(x/2, y), x-y)})$

$\wedge (\texttt{x} \geq \texttt{y} \rightarrow \texttt{f((x-y)/2, y)} > \texttt{(x-y)-y} \wedge \texttt{(x-y)/2} > \texttt{y})$

$\wedge (\texttt{x} < \texttt{y} \rightarrow \texttt{f(x/2, y)} > \texttt{x-y} \wedge \texttt{x/2} > \texttt{y})$

 

**Lecture 12: Syntactic Substitution**

12. (Substitute into $p \equiv (\mathtt{z} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y}) \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z}) \wedge (\exists\, \mathtt{y} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y}))$

12a. (Calculate $p[\mathtt{z}/\mathtt{x}]$) Note the $\exists\, \mathtt{x}$ hides the uses of x in its body from the substitution.

$$\begin{aligned} p[\mathtt{z}/\mathtt{x}] &\equiv ((\mathtt{z} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y}) \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z}) \wedge (\exists\, \mathtt{y} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y}))[\mathtt{z}/\mathtt{x}] \\ &\equiv (\mathtt{z} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y})[\mathtt{z}/\mathtt{x}] \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z})[\mathtt{z}/\mathtt{x}] \wedge (\exists\, \mathtt{y} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y})[\mathtt{z}/\mathtt{x}] \\ &\equiv (\mathtt{z} < 2{*}\mathtt{z} \vee \mathtt{z} \le \mathtt{y}) \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z}) \wedge (\exists\, \mathtt{y} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{z} * \mathtt{y}) \end{aligned}$$

12b. (Calculate $p[(\mathtt{z+a})/\mathtt{z}]$) Since neither x nor y appear in the substituting value z+a, we can substitute z+a for z in the body of the $\exists\, \mathtt{x}$ and $\exists\, \mathtt{y}$ (no renaming is needed).

$$\begin{aligned} p[(\mathtt{z+a})/\mathtt{z}] &\equiv ((\mathtt{z} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y}) \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z}) \wedge (\exists\, \mathtt{y} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y}))[(\mathtt{z+a})/\mathtt{z}] \\ &\equiv (\mathtt{z} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y})[(\mathtt{z+a})/\mathtt{z}] \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z})[(\mathtt{z+a})/\mathtt{z}] \\ &\qquad \wedge (\exists \mathtt{y} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y})[(\mathtt{z+a})/\mathtt{z}] \\ &\equiv (\mathtt{z+a} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y}) \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z+a}) \wedge (\exists\, \mathtt{y} \,.\, \mathtt{g}((\mathtt{z+a})\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y}) \end{aligned}$$

12c. (Calculate $p[\mathtt{x+y}/\mathtt{z}]$) Both x and y appear in the substituting value x+y, so we must rename the quantified variables. For $\exists\, \mathtt{x}$, we need a variable other than a, x, y, or z; we use v below. for $\exists\, \mathtt{y}$, we need a variable other than a, g, x, y, or z; we use w (note we could reuse v but that might confuse people).

$$\begin{aligned} p[\mathtt{x+y}/\mathtt{z}] &\equiv ((\mathtt{z} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y}) \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z}) \wedge (\exists\, \mathtt{y} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y}))[\mathtt{x+y}/\mathtt{z}] \\ &\equiv (\mathtt{z} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y})[\mathtt{x+y}/\mathtt{z}] \\ &\qquad \wedge (\exists\, \mathtt{x} \,.\, \mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z})[\mathtt{x+y}/\mathtt{z}] \\ &\qquad \wedge (\exists\, \mathtt{y} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y})[\mathtt{x+y}/\mathtt{z}] \\ &\equiv (\mathtt{x+y} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y}) \\ &\qquad \wedge\ (\exists\, \mathtt{v} \,.\, (\mathtt{x} \div \mathtt{y} > \mathtt{y} \div \mathtt{z})[\mathtt{v}/\mathtt{x}])[\mathtt{x+y}/\mathtt{z}] \\ &\qquad \wedge\ (\exists\, \mathtt{w} \,.\, (\mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{y})[\mathtt{w}/\mathtt{y}])[\mathtt{x+y}/\mathtt{z}] \\ &\equiv (\mathtt{x+y} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y}) \\ &\qquad \wedge\ (\exists\, \mathtt{v} \,.\, \mathtt{v} \div \mathtt{y} > \mathtt{y} \div \mathtt{z})[\mathtt{x+y}/\mathtt{z}] \\ &\qquad \wedge\ (\exists\, \mathtt{w} \,.\, \mathtt{g}(\mathtt{z}\hat{\ }2 + \mathtt{z}) < \mathtt{x} * \mathtt{w})[\mathtt{x+y}/\mathtt{z}] \\ &\equiv (\mathtt{x+y} < 2{*}\mathtt{x} \vee \mathtt{x} \le \mathtt{y}) \\ &\qquad \wedge\ (\exists\, \mathtt{v} \,.\, \mathtt{v} \div \mathtt{y} > \mathtt{y} \div (\mathtt{x+y})) \\ &\qquad \wedge\ (\exists\, \mathtt{w} \,.\, \mathtt{g}((\mathtt{x+y})\hat{\ }2 + (\mathtt{x+y})) < \mathtt{x} * \mathtt{w}) \end{aligned}$$

 