Weakest Preconditions

2/21/[illegible]

As we've seen, there can be many valid preconditions for a Hoare triple.

$$[p]\ \text{if } (x > 0) \text{ then } \{z := 1\} \text{ else } \{z := 0\}\ [z = 1]$$

$$F \Rightarrow \dots \Rightarrow \underbrace{x = 1 \wedge y = 2 \Rightarrow x = 1 \Rightarrow x > 0}_{\text{Valid}} \Rightarrow \underbrace{x > -5 \Rightarrow x \in \mathbb{Z} \Rightarrow \dots \Rightarrow T}_{\text{Invalid}}$$

Can always make precond. weaker (but less useful) ← → Can only make it weaker to a point

Weaker preconditions are more useful
Is there a weakest precondition p s.t. $\models [p]\ s\ [q]$? Yes.

Weakest precondition: $wp(s, q)$
What do we mean by weakest?
For all p s.t. $\models [p]\ s\ [q]$, $p \Rightarrow wp(s, q)$ (p stronger)

Another useful property
$\models [x = 1]$ if ... $[z = 1]$ - true
but what does that tell us about running the prog. w/ $x \neq 1$ - will it diverge, error or end w/ $z \neq 1$?
Not necessarily - $x = 2, x = 3 \dots$

But: if we run the prog. w/ $x \leq 0$, postcond. doesn't hold.

In general, if s is deterministic and $\sigma \not\models wp(s, q)$, then $\perp \in M(s, \sigma)$ or $M(s, \sigma) \not\models q$

Weakest liberal precondition $wlp(s, q)$
equivalent of wp for partial correctness

If $\models \{p\} s \{q\}$ then $p \Rightarrow wlp(s, q)$
For deterministic s, if $\sigma \not\models wlp(s,q)$,
then $M(s, \sigma) \not\models q$.

$wp(y := x*x,\ x \geq 0 \wedge y \geq 4) = x \geq 2 = wlp(y := x*x,\ x \geq 0 \wedge y \geq 4)$
Why? Let $\sigma(x) < 2$.
If $\sigma(x) \in [0, 1]$, then $M(s, \sigma)(y) < 4$.
If $\sigma(x) < 0$, then $M(s, \sigma)(x) < 0$.

If program can't diverge or error, wp = wlp.

$(= wlp)$
$wp(\text{if } y \leq x \text{ then } \{m := x\} \text{ else } \{skip\},\ m = max(x, y)) = y > x \rightarrow m = y$
$y \leq x \Rightarrow$ postcond. holds
$y > x \Rightarrow$ postcond doesn't hold unless $m = max(x, y) = y$
(postcond. holds already)

$$
\begin{aligned}
(y \leq x \wedge T) \vee (y > x \wedge m = y) &\Leftrightarrow y \leq x \vee (y > x \wedge m = y) \\
&\Leftrightarrow (y \leq x \vee y > x) \wedge (y \leq x \vee m = y) \\
&\Leftrightarrow T \wedge (\neg(y > x) \vee m = y) \\
&\Leftrightarrow y > x \rightarrow m = y
\end{aligned}
$$

So, $wp(\text{if } y \leq x \ldots,\ m = max(x, y)) = (y \leq x \wedge T) \vee (y > x \wedge m = y)$ also.
$wp(s, q)$ is unique, but only up to logical equivalence
Remember: If $\models [p]\, s\, [q]$ then $p \Rightarrow wp(s, q)$
so if $p = wp(s, q)$ and $p' = wp(s, q)$
then $p' \Rightarrow p$ and $p \Rightarrow p'$, so $p \Leftrightarrow p'$ $(p = p')$

$wp(\text{while } x \neq 0 \ \{x := x-1\}, x=0) = x \geq 0$

If $x < 0$, s doesn't terminate

$wlp(\text{while } x \neq 0 \ \{x := x-1\}, x=0) = T$

If s terminates, $x = 0$ at the end.

$wp(\text{while } x > 0 \ \{x := x-1\}, x \leq 0) = T$

$= wlp$

In general, $wp(s, T)$ is the conditions under which s terminates

$wlp(s, T) = T$

<u>Other facts about wp and wlp</u>

1. Total correctness implies partial correctness, so $wp(s,q) \Rightarrow wlp(s,q)$

   Contrapositive: $\neg wlp(s,q) \Rightarrow \neg wp(s,q)$

   If a state fails partial correctness, it definitely fails total

2. Technically, wp and wlp are sets of states, not predicates
   - There are some sets of states that are hard to write as predicates

   So can write $\sigma \in wp(s,q)$ instead of $\sigma \models wp(s,q)$, but both will be clear

So what if $\sigma \in wlp(s,q)$ but $\sigma \notin wp(s,q)$

then $M(s, \sigma) = \{\perp\}$