Weakest Preconditions

- w is the **weakest precondition of S and q** (we write $w = wp\ (S, q)$ or $w \Leftrightarrow wp\ (S, q)$) if w is a precondition for S and q that $\{w\}\ S\ \{q\}$ is totally valid and w can't be weakened. In other word, $\vDash_{tot} \{w\}\ S\ \{q\}$ and there is no r weaker than w such that $\vDash_{tot} \{r\}\ S\ \{q\}$.
  - o In terms of collection of states: $wp\ (S, q) = \{\sigma \in \Sigma \mid M(S, \sigma) \vDash q\}$.

1. Let's consider $w = wp(x \coloneqq x + 1, x \geq 2)$.
   If we use terms of states, we can see w is the collection of all σ that makes $M(x \coloneqq x + 1, \sigma) \vDash (x \geq 2)$. This collection containing states such as $\{x = 5\}, \{x = 1, y = 3\}, \{x = 100, z = 1, y = 4\}$ ... In general, we can say that is the collection of states that satisfy $x \geq 1$.

2. Let $w = wp\ (S, q)$. Decide true or false.
   a. If $\vDash_{tot} \{r\}\ S\ \{q\}$, then $r \Rightarrow w$. True.

   b. If $r \Rightarrow w$, then $\vDash_{tot} \{r\}\ S\ \{q\}$. True.
   o We can say that if $w = wp\ (S, q)$, then $\vDash_{tot} \{r\}\ S\ \{q\}$ if and only if $r \Rightarrow w$.

   c. If $\sigma \nvDash w$, then we know nothing interesting about $M(S, \sigma)$.
   False. Since any w is the most general precondition for S and q, if a state σ doesn't satisfy w then $M(S, \sigma) \nvDash q$.

   d. Assuming that q won't be evaluated to $\perp$ in any state. If S is deterministic, then $\vDash \{\neg w\}\ S\ \{\neg q\}$.
   True. For any state σ, if $\sigma \vDash \neg w$ and $M(S, \sigma) = \{\tau\}$, we must have $\tau \nvDash q$; in other words, $\tau = \perp$ or $\tau \vDash \neg q$.

   e. If $u \Leftrightarrow w$, then u is also the weakest precondition of S and q.
   True. For example, if $wp(S, q)$ is $x \geq 1$, then $x > 0$ or $1 \leq x$ can also be used as the weakest precondition.

- The **weakest liberal precondition for S and q**, written $wlp\ (S, q)$, is like $wp(S, q)$ but for partial correctness. In other words, $wlp\ (S, q)$ is a valid precondition for q under partial correctness where no weaker valid precondition exists.
  - o In terms of collection of states: $wlp\ (S, q) = \{\sigma \in \Sigma \mid M(S, \sigma) - \perp \vDash q\}$.
  - o We can say that, if $w = wlp\ (S, q)$, then $\vDash \{r\}\ S\ \{q\}$ if and only if $r \Rightarrow w$.

- We care about wp and wlp since they are the most general conditions a program requires to run "successfully" in when we want to get a certain postcondition.
  - o From one of the above examples, we learned that if a state σ does not satisfy wp, then it is guaranteed that $M(S, \sigma) \nvDash q$. Similarly, for wlp, if $\sigma \nvDash wlp$, then $M(S, \sigma) - \perp \nvDash q$.

  - o Also remind that, we sometimes say a state $\sigma \vDash wlp(S, q)$ and we sometimes say a statement $\sigma \in wlp(S, q)$; they have the same meaning.

(wp and wlp for deterministic program)

- The following figure illustrates the relationships between wp and wlp for *deterministic* programs (here, we assume that $\tau(q) \neq \perp$ if $\tau \neq \perp$.). Here it uses the definitions of wp and wlp as they are set of states.

$wlp(S,q)$	$\sigma \in wp(S,q)$ iff $M(S,\sigma)=\{\tau\} \models q$	
	$M(S,\sigma)=\{\perp\}$	
	$\sigma \in wp(S,\neg q)$ iff $M(S,\sigma)=\{\tau\} \models \neg q$	$wlp(S,\neg q)$

  - For a state σ and a deterministic program S, we can have three possible outcomes for $M(S,\sigma)$:

1) $M(S,\sigma) = \{\tau\}$ and $\{\tau\} \models q$.
2) $M(S,\sigma) = \{\perp\}$.
3) $M(S,\sigma) = \{\tau\}$ and $\{\tau\} \models \neg q$.

  - $wp\ (S,q)$ is set of all σ in situation 1 .
  - $wp\ (S,\neg q)$ is set of all σ in situation 3).
  - $wlp\ (S,q)$ is set of all σ in situation 1) and 2).
  - $wlp\ (S,\neg q)$ is set of all σ in situation 2) and 3).

3. True or False.
   a. Let S be deterministic. $wlp(S,T) \Leftrightarrow T$.
   True. Because, for any state σ, either $M(S,\sigma) = \perp$ or $M(S,\sigma) \neq \perp$. If $M(S,\sigma) = \perp$, then $\sigma \in wlp(S,T)$; if $M(S,\sigma) \neq \perp$, then $M(S,\sigma) \models T$. Thus, all states are in $wlp(S,T)$; in other words, $wlp(S,T) \Leftrightarrow T$.

   b. Let S be deterministic. $wp(S,F) \Leftrightarrow F$.
   True. For any state σ, either $M(S,\sigma) = \perp$ or $M(S,\sigma) \neq \perp$. If $M(S,\sigma) = \perp$, then $\sigma \notin wp(S,F)$; if $M(S,\sigma) \neq \perp$, then $M(S,\sigma) \not\models F$. Thus, $wp(S,F)$ is an empty set; in other words, $wp(S,F) \Leftrightarrow F$.

   c. $wp(y \coloneqq x * x,\ y \geq 4) \Leftrightarrow wlp(y \coloneqq x * x,\ y \geq 4)$
   True, because the statement $y \coloneqq x * x$ is loop-free and cannot create a runtime error, the postcondition $y \geq 4$ cannot be evaluated to $\perp$. As an aside, using *backward assignment* rule, we can get $wp(y \coloneqq x * x,\ y \geq 4) \Leftrightarrow x * x \geq 4$.

(wp and wlp in general programs)

- We need to be careful when nondeterminism is considered, $M(S,\sigma)$ might contain more than one states.
  - $\sigma \in wp(S,q)$ iff $M(S,\sigma) \models q$.
  - $\sigma \in wlp(S,q)$ iff $M(S,\sigma) - \perp \models q$.
  - $\sigma \notin wp(S,q)$ iff there exist some $\tau \in M(S,\sigma)$ such that $\tau = \perp$ or $\tau \not\models q$.
  - $\sigma \notin wlp(S,q)$ iff there exist some $\tau \in M(S,\sigma)$ such that $\tau \neq \perp$ and $\tau \not\models q$.

4. Show the following property: $wp(S,q_1) \wedge wp\ (S,q_2) \Leftrightarrow wp(S,q_1 \wedge q_2)$.
   - If a state $\sigma \in wp(S,q_1) \wedge wp\ (S,q_2)$, then $\sigma \in wp(S,q_1)$ and $\sigma \in wp(S,q_2)$; then $M(S,\sigma) \models q_1$ and $M(S,\sigma) \models q_2$; thus $M(S,\sigma) \models q_1 \wedge q_2$, which implies $\sigma \in wp(S,q_1 \wedge q_2)$.

- If a state $\sigma \in wp(S, q_1 \wedge q_2)$, then $M(S,\sigma) \vDash q_1 \wedge q_2$; thus $M(S,\sigma) \vDash q_1$ and $M(S,\sigma) \vDash q_2$, which implies $\sigma \in wp(S, q_1) \wedge wp\ (S, q_2)$.

- Using a similar proof, we can also show the following property: $wlp(S, q_1) \wedge wlp\ (S, q_2) \Leftrightarrow wlp(S, q_1 \wedge q_2)$.

5. Is it true that $wp(S, q_1) \vee wp\ (S, q_2) \Leftrightarrow wp(S, q_1 \vee q_2)$?
   First, let's show that: $wp(S, q_1) \vee wp\ (S, q_2) \Rightarrow wp(S, q_1 \vee q_2)$.
   - If a state $\sigma \in wp(S, q_1) \vee wp\ (S, q_2)$, then $\sigma \in wp(S, q_1)$ **or** $\sigma \in wp(S, q_2)$; then $M(S,\sigma) \vDash q_1$ **or** $M(S,\sigma) \vDash q_2$; thus $M(S,\sigma) \vDash q_1 \vee q_2$, which implies $\sigma \in wp(S, q_1 \vee q_2)$.

   How about the inverse of this property? Is it true that "$wp(S, q_1) \vee wp\ (S, q_2) \Leftarrow wp(S, q_1 \vee q_2)$ " ?

   - When $M(S,\sigma) = \{\tau\}$ ($M(S,\sigma)$ contains only one state):
     If $\sigma \in wp(S, q_1 \vee q_2)$, then $\tau \vDash q_1 \vee q_2$, and $\tau \vDash q_1$ or $\tau \vDash q_2$; then $\sigma \in wp(S, q_1)$ or $\sigma \in wp(S, q_2)$ which implies $\sigma \in wp(S, q_1) \vee wp\ (S, q_2)$.

   - When $M(S,\sigma)$ contains more than one states, then the statement is not necessarily true:
     Let $M(S,\sigma) \supseteq \{\tau_1, \tau_2\}$. When $M(S,\sigma) \vDash q_1 \vee q_2$, it is possible that $\tau_1 \vDash q_1$ and $\tau_2 \vDash q_2$. So, even if we can have $M(S,\sigma) \vDash q_1 \vee q_2$, but don't necessarily have $M(S,\sigma) \vDash q_1$ or $M(S,\sigma) \vDash q_2$.

   To sum up, $wp(S, q_1) \vee wp\ (S, q_2) \Leftarrow wp(S, q_1 \vee q_2)$ is not necessarily true when $M(S,\sigma)$ contains more than one state. In other words, $wp(S, q_1) \vee wp\ (S, q_2) \Leftarrow wp(S, q_1 \vee q_2)$ is definitely true when S is deterministic.

   Using a similar proof, we can also show the following property: $wlp(S, q_1) \vee wlp\ (S, q_2) \Rightarrow wlp(S, q_1 \vee q_2)$. But $wlp(S, q_1) \vee wlp\ (S, q_2) \Leftarrow wlp(S, q_1 \vee q_2)$ only holds when S is deterministic (or $M(S,\sigma)$ contains only one state).

6. Let $flip \equiv \mathbf{if}\ T \rightarrow x \coloneqq 0\ \ \square\ T \rightarrow x \coloneqq 1\ \mathbf{fi}$, $head \equiv x = 0$, and $tail \equiv x = 1$.
   a. What is $M(flip, \emptyset)$? (here, $\emptyset$ is an empty state).
      $M(flip, \emptyset) = \big\{\{head\},\ \{tail\}\big\}$.

   b. What is $wp(flip,\ head \vee tail)$?
      For any state σ (let's assume that x is not defined in σ to simplify the notation), we have $M(flip, \sigma) = \big\{\sigma \cup \{head\},\ \sigma \cup \{tail\}\big\}$, and it satisfies $head \vee tail$, thus $wp(flip,\ head \vee tail) \Leftrightarrow T$.

   c. What is $wp(flip,\ head)$? And what is $wp(flip,\ tail)$?
      For any state σ, we have $M(flip, \sigma) = \big\{\sigma \cup \{head\},\ \sigma \cup \{tail\}\big\}$, it doesn't satisfy $head$ and it doesn't satisfy $tail$; thus $wp(flip,\ head) \Leftrightarrow wp(flip,\ tail) \Leftrightarrow F$.