WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given an error condition or a post-condition, propagate the condition backwards through the program.
- Given a set of states S and a command c, the weakest pre-condition operator $wp(S, c)$ consists of all states that would always lead to a state in S after executing c.

$$wp(S, c) \triangleq \{\sigma \mid \forall \sigma' \,.\, (\sigma, c) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \in S\}$$

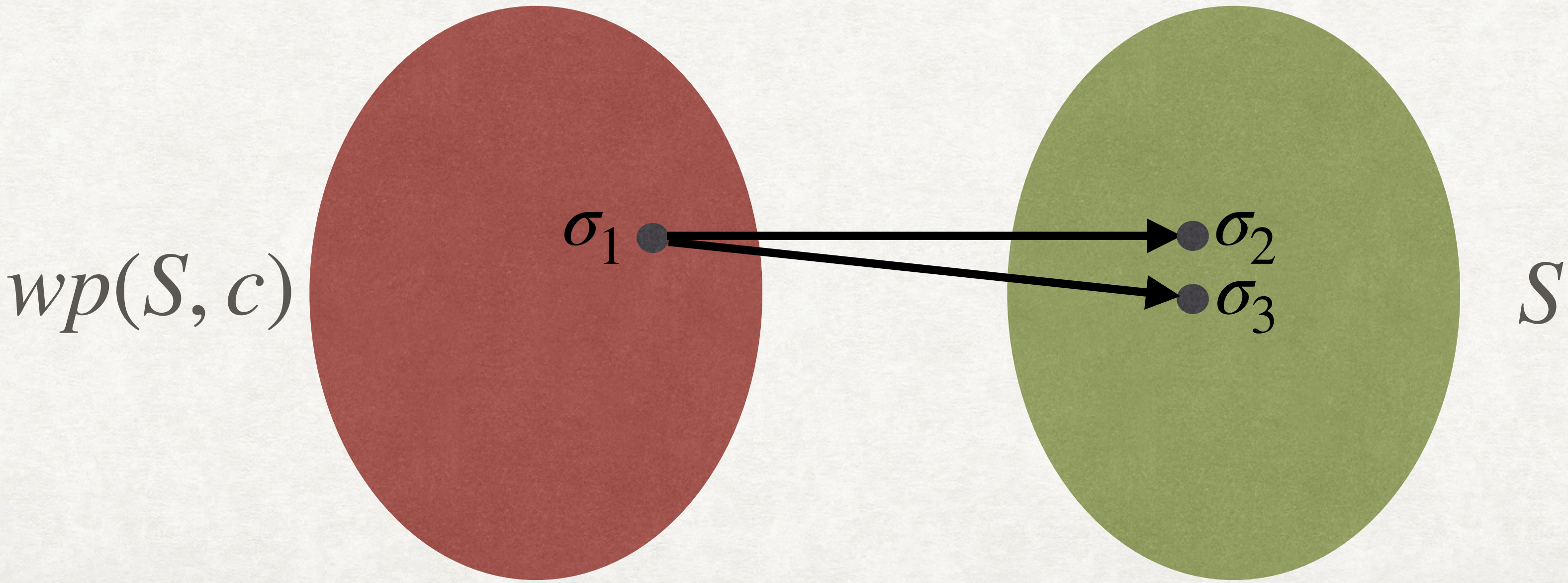
Equivalently, $\sigma \in wp(S, c) \Leftrightarrow \forall \sigma' \,.\, (\sigma, c) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \in S$

WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given an error condition or a post-condition, propagate the condition backwards through the program.
- Given a set of states S and a command c, the weakest pre-condition operator $wp(S, c)$ consists of all states that would always lead to a state in S after executing c.

$$\sigma \in wp(S, c) \Leftrightarrow \forall \sigma' \,.\, (\sigma, c) \hookrightarrow^* (\sigma', \text{skip}) \rightarrow \sigma' \in S$$

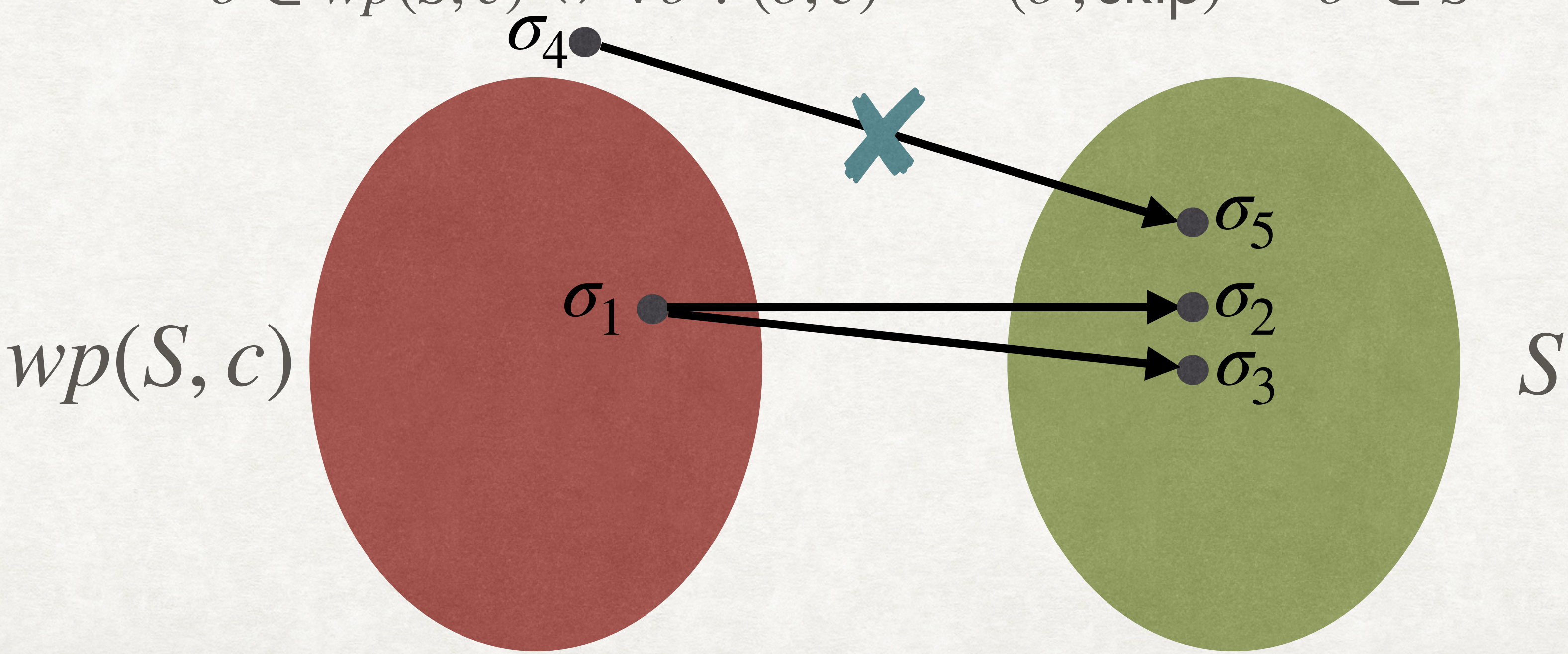


WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given an error condition or a post-condition, propagate the condition backwards through the program.
- Given a set of states S and a command c, the weakest pre-condition operator $wp(S, c)$ consists of all states that would always lead to a state in S after executing c.

$$\sigma \in wp(S, c) \Leftrightarrow \forall \sigma' \, . \, (\sigma, c) \hookrightarrow^* (\sigma', \text{skip}) \rightarrow \sigma' \in S$$

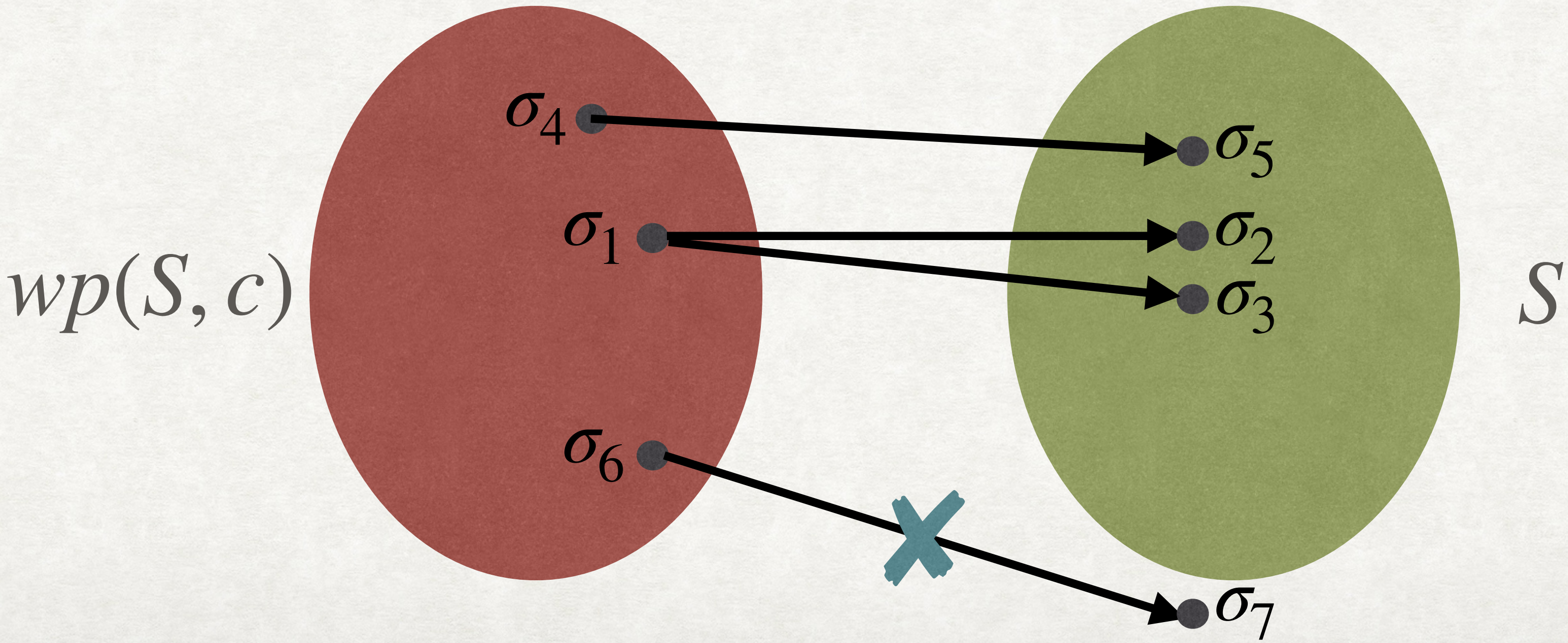


WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given an error condition or a post-condition, propagate the condition backwards through the program.
- Given a set of states S and a command c, the weakest pre-condition operator $wp(S, c)$ consists of all states that would always lead to a state in S after executing c.

$$\sigma \in wp(S, c) \Leftrightarrow \forall \sigma' \,.\, (\sigma, c) \hookrightarrow^* (\sigma', \text{skip}) \rightarrow \sigma' \in S$$

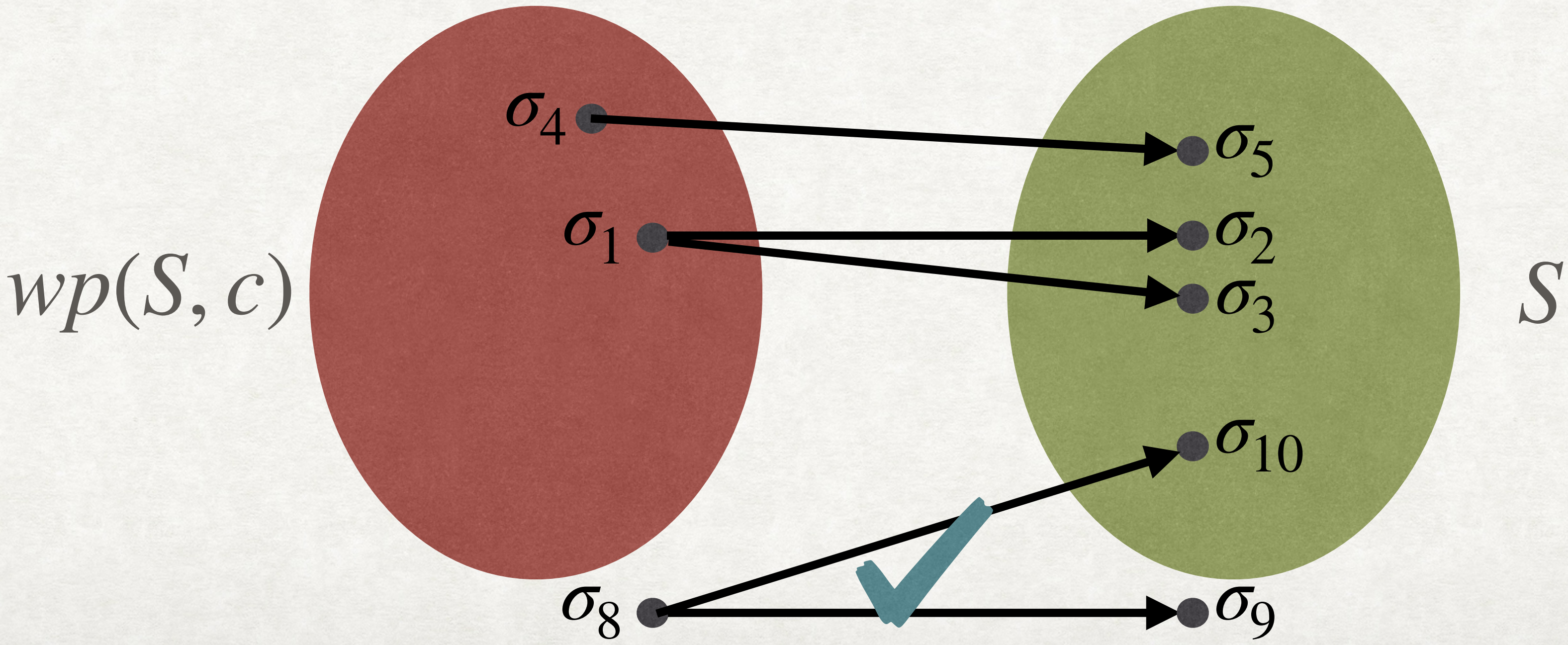


WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given an error condition or a post-condition, propagate the condition backwards through the program.
- Given a set of states S and a command c, the weakest pre-condition operator $wp(S, c)$ consists of all states that would always lead to a state in S after executing c.

$$\sigma \in wp(S, c) \Leftrightarrow \forall \sigma' \,.\, (\sigma, c) \hookrightarrow^* (\sigma', \text{skip}) \rightarrow \sigma' \in S$$



WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

$$wp(S, c) \triangleq \{\sigma \mid \forall \sigma' .\ (\sigma, c) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \in S\}$$

- We can use a FOL formula F to represent a set of states.
- The symbolic weakest pre-condition operator can be defined as:

$$\sigma \vDash wp(F, \mathsf{c}) \Leftrightarrow \forall \sigma' .\ (\sigma, \mathsf{c}) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \vDash F$$

- We now use the symbolic FOL semantics (ρ) for individual commands:

$$wp(F, \mathsf{c}) \triangleq \forall V' .\ \rho(\mathsf{c}) \rightarrow F[V'/V]$$

WEAKEST PRE-CONDITION

EXAMPLES

$$wp(\mathsf{x} > 10, \mathsf{x}{:=}\mathsf{x}{+}1) \triangleq \forall \mathsf{x}' \,.\, \mathsf{x}' = \mathsf{x} + 1 \rightarrow \mathsf{x}' > 10$$

$$\equiv \mathsf{x} + 1 > 10 \equiv \mathsf{x} > 9$$

WEAKEST PRE-CONDITION

EXAMPLES

$$wp(\mathsf{x} > 10, \mathsf{x}{:=}\mathsf{x}{+}1) \triangleq \forall \mathsf{x}' .\ \mathsf{x}' = \mathsf{x} + 1 \rightarrow \mathsf{x}' > 10$$

$$\equiv \mathsf{x} + 1 > 10 \equiv \mathsf{x} > 9$$

$$wp(\ \top\ , \mathsf{c}) \equiv ???$$

WEAKEST PRE-CONDITION

EXAMPLES

$$wp(\mathsf{x} > 10, \mathsf{x{:=}x{+}1}) \triangleq \forall \mathsf{x}' \,.\, \mathsf{x}' = \mathsf{x} + 1 \rightarrow \mathsf{x}' > 10$$

$$\equiv \mathsf{x} + 1 > 10 \equiv \mathsf{x} > 9$$

$$wp(\top, \mathsf{c}) \equiv \top$$

WEAKEST PRE-CONDITION

EXAMPLES

$$wp(\mathsf{x} > 10, \mathsf{x{:=}x{+}1}) \triangleq \forall \mathsf{x}' .\ \mathsf{x}' = \mathsf{x} + 1 \rightarrow \mathsf{x}' > 10$$

$$\equiv \mathsf{x} + 1 > 10 \equiv \mathsf{x} > 9$$

$wp(\ \top\ , \mathsf{c}) \equiv \top$

$wp(\ \bot\ , \mathsf{c}) \equiv\ ???$

WEAKEST PRE-CONDITION

EXAMPLES

$$wp(\mathrm{x} > 10, \mathrm{x}{:=}\mathrm{x}{+}1) \triangleq \forall \mathrm{x}' .\ \mathrm{x}' = \mathrm{x} + 1 \rightarrow \mathrm{x}' > 10$$

$$\equiv \mathrm{x} + 1 > 10 \equiv \mathrm{x} > 9$$

$wp(\ \top\ , \mathrm{c}) \equiv \top$

$wp(\ \perp\ , \mathrm{c}) \equiv$ All states for which c does not terminate

WEAKEST PRE-CONDITION

EXAMPLES

$$wp(x > 10, x{:=}x{+}1) \triangleq \forall x' .\ x' = x + 1 \rightarrow x' > 10$$

$$\equiv x + 1 > 10 \equiv x > 9$$

$wp(\top, c) \equiv \top$

$wp(\bot, c) \equiv$ All states for which c does not terminate

$wp(\bot, \text{assume}(x{>}0)) \equiv ???$

WEAKEST PRE-CONDITION

EXAMPLES

$$wp(\mathrm{x} > 10, \mathrm{x{:=}x{+}1}) \triangleq \forall \mathrm{x'} .\ \mathrm{x'} = \mathrm{x} + 1 \rightarrow \mathrm{x'} > 10$$
$$\equiv \mathrm{x} + 1 > 10 \equiv \mathrm{x} > 9$$

$wp(\ \top\ , \mathrm{c}) \equiv \top$

$wp(\ \bot\ , \mathrm{c}) \equiv$ All states for which c does not terminate

$$wp(\ \bot\ , \mathrm{assume(x{>}0)}) \equiv \forall \mathrm{x'} .\ \mathrm{x} > 0 \land \mathrm{x'} = \mathrm{x} \rightarrow \bot$$
$$\equiv \mathrm{x} \leq 0$$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

- $wp(F, \text{x:=e}) \triangleq F[\text{e/x}]$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

- $wp(F, \text{x:=e}) \triangleq F[\text{e/x}]$

$$
\begin{aligned}
wp(F, \text{x:=e}) &\triangleq \forall V' \,.\, \rho(\text{x:=e}) \rightarrow F[V'/V] \\
&\equiv \forall V' \,.\, \text{x'} = \text{e} \wedge frame(\text{x'}) \rightarrow F[V'/V] \\
&\equiv F[\text{e/x}]
\end{aligned}
$$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

- $wp(F, \text{x:=e}) \triangleq F[\text{e/x}]$

$$wp(F, \text{x:=e}) \triangleq \forall V' \,.\, \rho(\text{x:=e}) \rightarrow F[V'/V]$$
$$\equiv \forall V' \,.\, \text{x}' = \text{e} \wedge frame(\text{x}') \rightarrow F[V'/V]$$
$$\equiv F[\text{e/x}]$$

EXAMPLES:

- $wp(\text{x} = 5, \text{x:=6}) \equiv ???$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

- $wp(F, \text{x:=e}) \triangleq F[\text{e/x}]$

$$
\begin{aligned}
wp(F, \text{x:=e}) &\triangleq \forall V' \,.\, \rho(\text{x:=e}) \rightarrow F[V'/V] \\
&\equiv \forall V' \,.\, \text{x}' = \text{e} \wedge frame(\text{x}') \rightarrow F[V'/V] \\
&\equiv F[\text{e/x}]
\end{aligned}
$$

EXAMPLES:

- $wp(\text{x} = 5, \text{x:=6}) \equiv \bot$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

- $wp(F, \text{x:=e}) \triangleq F[\text{e/x}]$

$$
\begin{aligned}
wp(F, \text{x:=e}) &\triangleq \forall V' \,.\, \rho(\text{x:=e}) \rightarrow F[V'/V] \\
&\equiv \forall V' \,.\, \text{x}' = \text{e} \wedge frame(\text{x}') \rightarrow F[V'/V] \\
&\equiv F[\text{e/x}]
\end{aligned}
$$

EXAMPLES:

- $wp(\text{x} = 5, \text{x:=6}) \equiv \bot$
- $wp(\text{x} = 5, \text{x:=5}) \equiv ???$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

- $wp(F, \mathsf{x{:=}e}) \triangleq F[\mathsf{e/x}]$

$$
\begin{aligned}
wp(F, \mathsf{x{:=}e}) &\triangleq \forall V' \,.\, \rho(\mathsf{x{:=}e}) \rightarrow F[V'/V] \\
&\equiv \forall V' \,.\, \mathsf{x' = e} \wedge frame(\mathsf{x'}) \rightarrow F[V'/V] \\
&\equiv F[\mathsf{e/x}]
\end{aligned}
$$

EXAMPLES:

- $wp(\mathsf{x} = 5, \mathsf{x{:=}6}) \equiv \bot$
- $wp(\mathsf{x} = 5, \mathsf{x{:=}5}) \equiv \top$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

- $wp(F, \text{x:=e}) \triangleq F[\text{e/x}]$

$$
\begin{aligned}
wp(F, \text{x:=e}) &\triangleq \forall V' \,.\, \rho(\text{x:=e}) \rightarrow F[V'/V] \\
&\equiv \forall V' \,.\, \text{x}' = \text{e} \wedge frame(\text{x}') \rightarrow F[V'/V] \\
&\equiv F[\text{e/x}]
\end{aligned}
$$

EXAMPLES:

- $wp(\text{x} = 5, \text{x:=6}) \equiv \bot$
- $wp(\text{x} = 5, \text{x:=5}) \equiv \top$
- $wp(\text{x} > 5, \text{x:=y+1}) \equiv ???$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

- $wp(F, \text{x:=e}) \triangleq F[\text{e/x}]$

$$wp(F, \text{x:=e}) \triangleq \forall V' . \rho(\text{x:=e}) \rightarrow F[V'/V]$$
$$\equiv \forall V' . \text{x}' = \text{e} \wedge frame(\text{x}') \rightarrow F[V'/V]$$
$$\equiv F[\text{e/x}]$$

EXAMPLES:

- $wp(\text{x} = 5, \text{x:=6}) \equiv \bot$
- $wp(\text{x} = 5, \text{x:=5}) \equiv \top$
- $wp(\text{x} > 5, \text{x:=y+1}) \equiv \text{x} > 5[(\text{y} + 1)/\text{x}] \equiv \text{y} > 4$

WEAKEST PRE-CONDITION

HAVOC, ASSUME

- $wp(F, \text{x:=havoc}) \equiv \forall \text{x} \,.\, F$

$$wp(F, \text{x:=havoc}) \triangleq \forall V' \,.\, frame(\text{x}) \rightarrow F[V'/V]$$
$$\equiv \forall \text{x'} \,.\, F[\text{x'/x}] \equiv \forall \text{x} \,.\, F$$

- $wp(\text{F, assume(G)}) \equiv ???$

WEAKEST PRE-CONDITION

HAVOC, ASSUME

- $wp(F, \text{x:=havoc}) \equiv \forall \text{x} \,.\, F$

$$wp(F, \text{x:=havoc}) \triangleq \forall V' \,.\, frame(\text{x}) \rightarrow F[V'/V]$$
$$\equiv \forall \text{x}' \,.\, F[\text{x}'/\text{x}] \equiv \forall \text{x} \,.\, F$$

- $wp(\text{F}, \text{assume(G)}) \equiv \text{G} \rightarrow \text{F}$

$$wp(\text{F}, \text{assume(G)}) \triangleq \forall \text{V}' \,.\, \text{G} \land frame(\varnothing) \rightarrow \text{F[V'/V]}$$
$$\equiv \forall \text{V}' \,.\, \text{G} \rightarrow \text{F} \equiv \text{G} \rightarrow \text{F}$$