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.

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

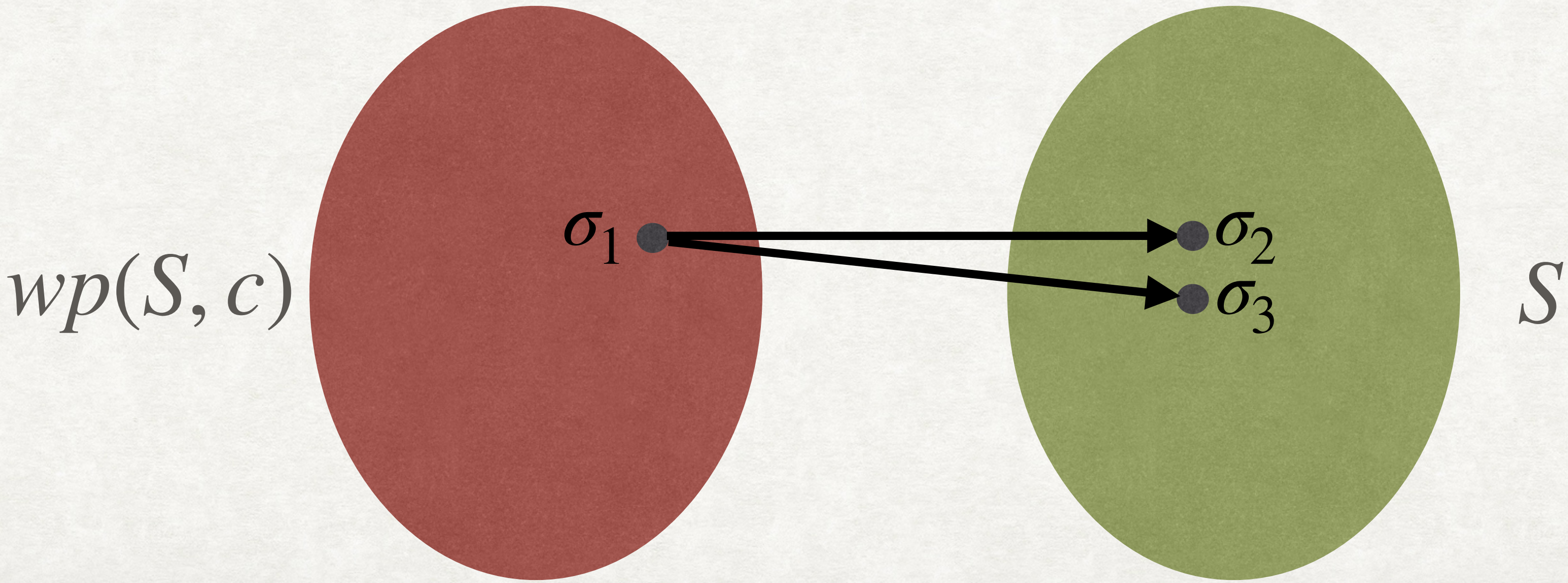
Equivalently, $\sigma \in wp(S, c) \Leftrightarrow \forall \sigma' .\ (\sigma, c) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \in S$

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.

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

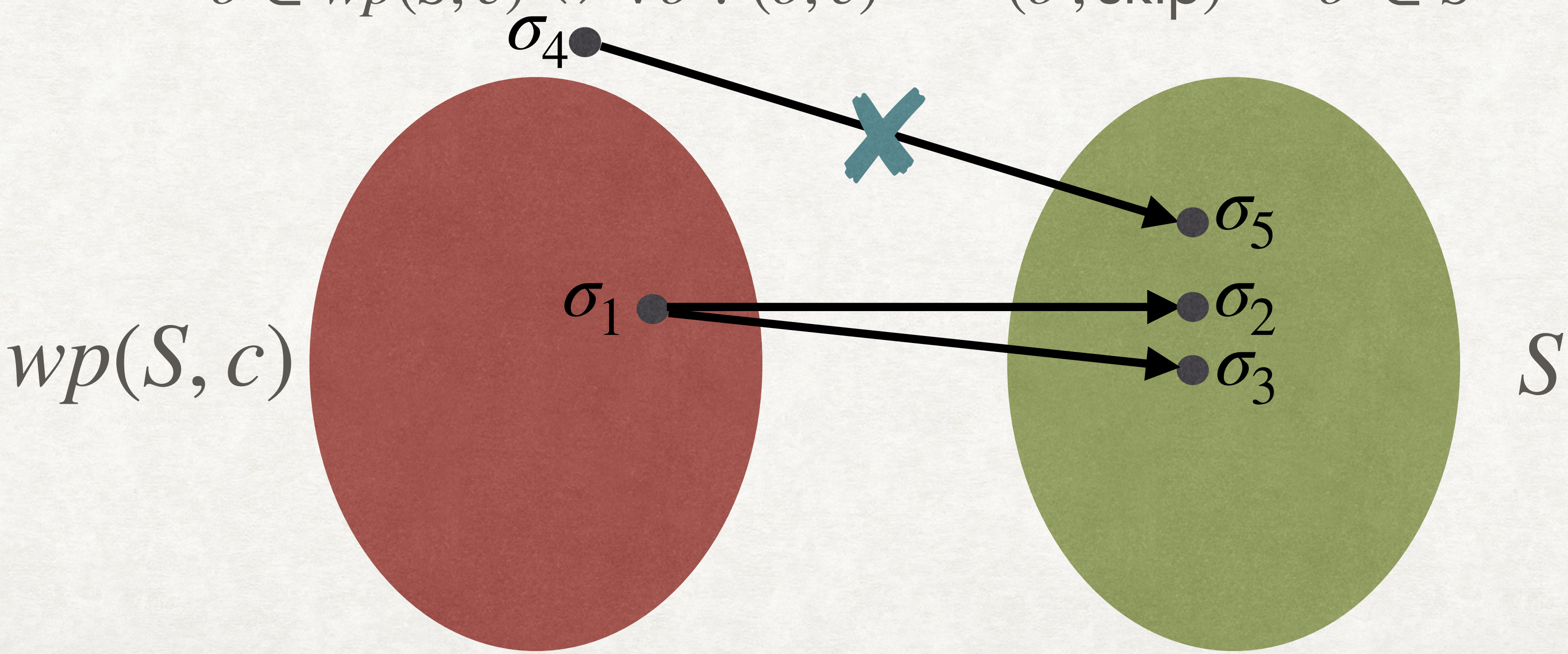


WEAKEST-PRECONDITION

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.

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

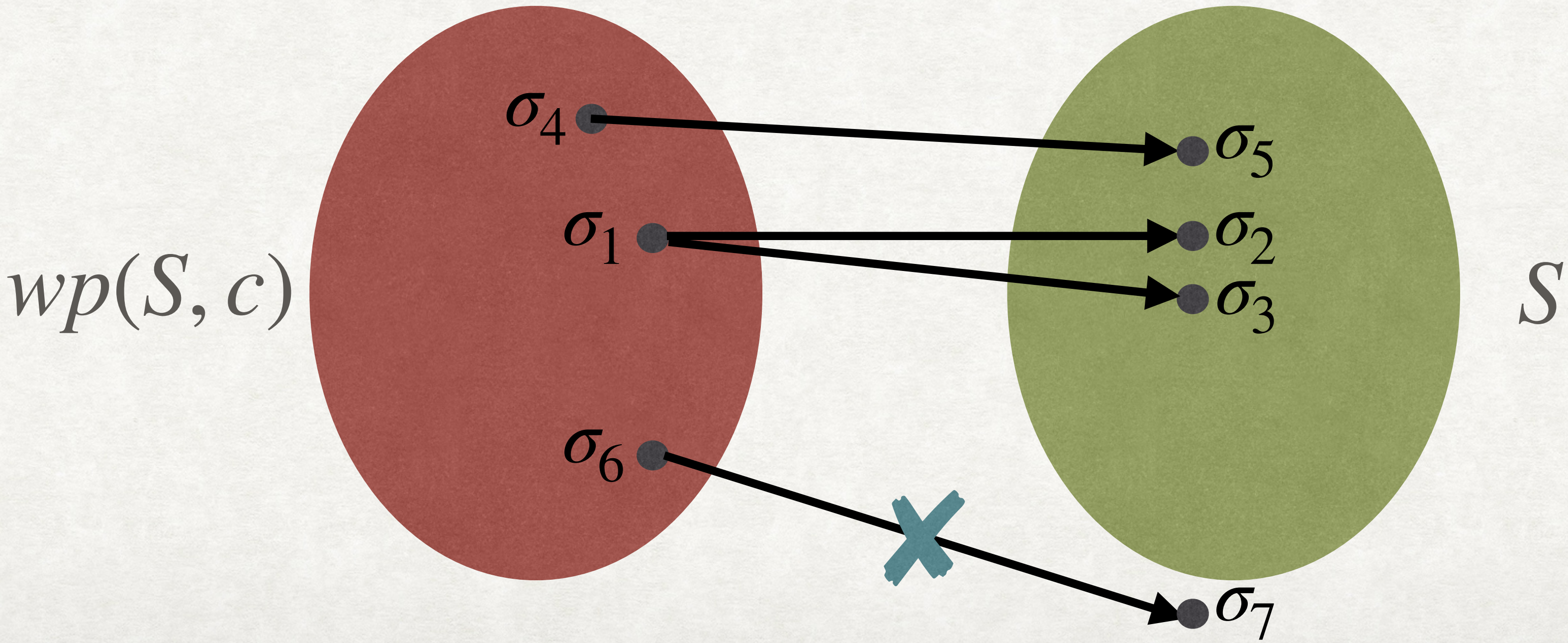


WEAKEST-PRECONDITION

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.

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

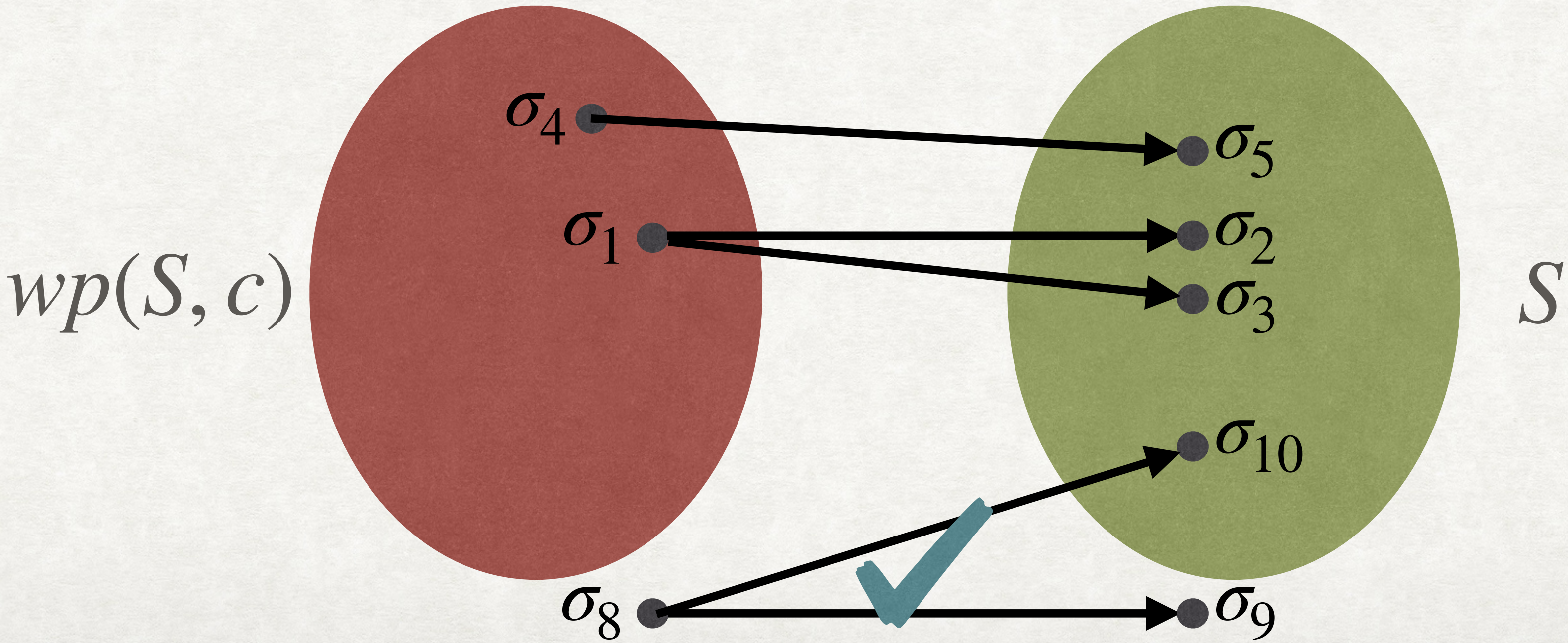


WEAKEST-PRECONDITION

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

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

- 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

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

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

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

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

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

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

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

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

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

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

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

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

$$\equiv \mathrm{x} \leq 0$$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

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

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

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

EXAMPLES:

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

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

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

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

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

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME

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

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

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\text{x} > 0, \text{x:=havoc}) \equiv ???$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\mathrm{x} > 0, \mathrm{x{:=}havoc}) \equiv \forall \mathrm{x}\ .\ \mathrm{x} > 0 \equiv \bot$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\text{x} > 0, \text{x:=havoc}) \equiv \forall \text{x} \,.\, \text{x} > 0 \equiv \bot$
- $wp(\text{x} + \text{i} \leq 0, \text{x:=havoc}) \equiv ???$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\mathrm{x} > 0, \mathrm{x}{:=}\mathrm{havoc}) \equiv \forall \mathrm{x}\,.\ \mathrm{x} > 0 \equiv \bot$
- $wp(\mathrm{x} + \mathrm{i} \leq 0, \mathrm{x}{:=}\mathrm{havoc}) \equiv \forall \mathrm{x}\,.\,\mathrm{x} + \mathrm{i} \leq 0 \equiv \bot$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp($x > 0,x:=havoc$) \equiv \forall$x . x $> 0 \equiv \bot$
- $wp($x $+$ i ≤ 0,x:=havoc$) \equiv \forall$x . x $+$ i $\leq 0 \equiv \bot$
- $wp($x ≥ 0,assume(x=1)$) \equiv ???$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\mathrm{x} > 0, \mathrm{x}{:=}\mathrm{havoc}) \equiv \forall \mathrm{x}\,.\; \mathrm{x} > 0 \equiv \bot$
- $wp(\mathrm{x} + \mathrm{i} \leq 0, \mathrm{x}{:=}\mathrm{havoc}) \equiv \forall \mathrm{x}\,.\,\mathrm{x} + \mathrm{i} \leq 0 \equiv \bot$
- $wp(\mathrm{x} \geq 0, \mathrm{assume}(\mathrm{x}{=}1)) \equiv \mathrm{x}{=}1 \rightarrow \mathrm{x} \geq 0 \equiv \top$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- wp(x $>$ 0,x:=havoc) $\equiv$ $\forall$x . x $>$ 0 $\equiv$ $\bot$
- wp(x + i $\leq$ 0,x:=havoc) $\equiv$ $\forall$x . x + i $\leq$ 0 $\equiv$ $\bot$
- wp(x $\geq$ 0,assume(x=1)) $\equiv$ x=1 $\rightarrow$ x $\geq$ 0 $\equiv$ $\top$
- wp(x $>$ 0,assume (x<0)) $\equiv$???

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\mathrm{x} > 0, \mathrm{x{:=}havoc}) \equiv \forall \mathrm{x}\,.\; \mathrm{x} > 0 \equiv \bot$
- $wp(\mathrm{x} + \mathrm{i} \leq 0, \mathrm{x{:=}havoc}) \equiv \forall \mathrm{x}\,.\, \mathrm{x} + \mathrm{i} \leq 0 \equiv \bot$
- $wp(\mathrm{x} \geq 0, \mathrm{assume(x{=}1)}) \equiv \mathrm{x{=}1} \rightarrow \mathrm{x} \geq 0 \equiv \top$
- $wp(\mathrm{x} > 0, \mathrm{assume\ (x{<}0)}) \equiv \mathrm{x} < 0 \rightarrow \mathrm{x} > 0 \equiv \mathrm{x} \geq 0$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\text{x} > 0, \text{x:=havoc}) \equiv \forall \text{x} .\ \text{x} > 0 \equiv \bot$
- $wp(\text{x} + \text{i} \leq 0, \text{x:=havoc}) \equiv \forall \text{x} . \text{x} + \text{i} \leq 0 \equiv \bot$
- $wp(\text{x} \geq 0, \text{assume(x=1)}) \equiv \text{x=1} \rightarrow \text{x} \geq 0 \equiv \top$
- $wp(\text{x} > 0, \text{assume (x<0)}) \equiv \text{x} < 0 \rightarrow \text{x} > 0 \equiv \text{x} \geq 0$
- Does there exist F and G such that $wp(F, \text{assume(G)}) \equiv \bot$?

WEAKEST PRE-CONDITION

ASSERT

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

WEAKEST PRE-CONDITION

ASSERT

- $wp(F, \text{assert}(G)) \equiv F \wedge G$
  - Assume that $F \neq \top$.
  - Assumption makes sense because we ideally want error $= 0$ after assert.

WEAKEST PRE-CONDITION

ASSERT

$wp(F, \text{assert}(G)) \triangleq$

WEAKEST PRE-CONDITION

ASSERT

$$
\begin{aligned}
wp(F, \text{assert}(G)) &\triangleq \forall V' \,.\, (G \rightarrow \mathit{frame}(\emptyset)) \rightarrow F[V'/V] \\
&\equiv \forall V' \,.\, (\neg G \vee \mathit{frame}(\emptyset)) \rightarrow F[V'/V] \\
&\equiv \forall V' \,.\, (G \wedge \neg \mathit{frame}(\emptyset)) \vee F[V'/V] \\
&\equiv \forall V' \,.\, (G \vee F[V'/V]) \wedge (\neg \mathit{frame}(\emptyset) \vee F[V'/V]) \\
&\equiv (G \vee \forall V' \,.\, F[V'/V]) \wedge \forall V' \,.\, (\mathit{frame}(\emptyset) \rightarrow F[V'/V]) \\
&\equiv (G \vee \forall V \,.\, F) \wedge F \\
&\equiv (G \vee \bot) \wedge F \\
&\equiv G \wedge F
\end{aligned}
$$

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

- $wp(\text{x} \geq 0, \text{assert(x=1)}) \equiv ???$

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

- $wp(\mathrm{x} \geq 0, \mathrm{assert(x{=}1)}) \equiv \mathrm{x} = 1$

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

- $wp(\mathsf{x} \geq 0, \mathsf{assert(x=1)}) \equiv \mathsf{x} = 1$
- $wp(\mathsf{x} = 2, \mathsf{assert(x=3)}) \equiv ???$

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

- $wp(\mathsf{x} \geq 0, \mathsf{assert(x=1)}) \equiv \mathsf{x} = 1$
- $wp(\mathsf{x} = 2, \mathsf{assert(x=3)}) \equiv \bot$

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

- $wp(\text{x} \geq 0, \text{assert(x=1)}) \equiv \text{x} = 1$
- $wp(\text{x} = 2, \text{assert(x=3)}) \equiv \bot$
- Does there exist F and G such that $wp(F, \text{assert(G)}) \equiv \top$?

WEAKEST PRE-CONDITION

SEQUENTIAL COMPOSITION

- $wp(F, c_1; c_2) \equiv ???$

WEAKEST PRE-CONDITION

SEQUENTIAL COMPOSITION

- $wp(F, c_1; c_2) \equiv wp(wp(F, c_2), c_1)$
  - We will show that $wp(S, c_1; c_2) = wp(wp(S, c_2), c_1)$

WEAKEST PRE-CONDITION

SEQUENTIAL COMPOSITION

- $wp(F, c_1; c_2) \equiv wp(wp(F, c_2), c_1)$
  - We will show that $wp(S, c_1; c_2) = wp(wp(S, c_2), c_1)$

Proof: First, we show that $wp(wp(S, c_2), c_1) \subseteq wp(S, c_1; c_2)$.

Consider $\sigma \in wp(wp(S, c_2), c_1)$.

By definition, $\forall \sigma''.\, (\sigma, c_1) \hookrightarrow^* (\sigma'', \text{skip}) \rightarrow \sigma'' \in wp(S, c_2)$ [1]

Further, for $\sigma'' \in wp(S, c_2)$, $\forall \sigma'.\, (\sigma'', c_2) \hookrightarrow^* (\sigma', \text{skip}) \rightarrow \sigma' \in S$ [2]

Now, consider σ' such that $(\sigma, c_1; c_2) \hookrightarrow^* (\sigma', \text{skip})$. Then, there exists σ'' such that $(\sigma, c_1) \hookrightarrow^* (\sigma'', \text{skip})$ and $(\sigma'', c_2) \hookrightarrow^* (\sigma', \text{skip})$. By [1], $\sigma'' \in wp(S, c_2)$ and hence by [2], $\sigma' \in S$.

Thus, $\sigma \in wp(S, c_1; c_2)$.