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.

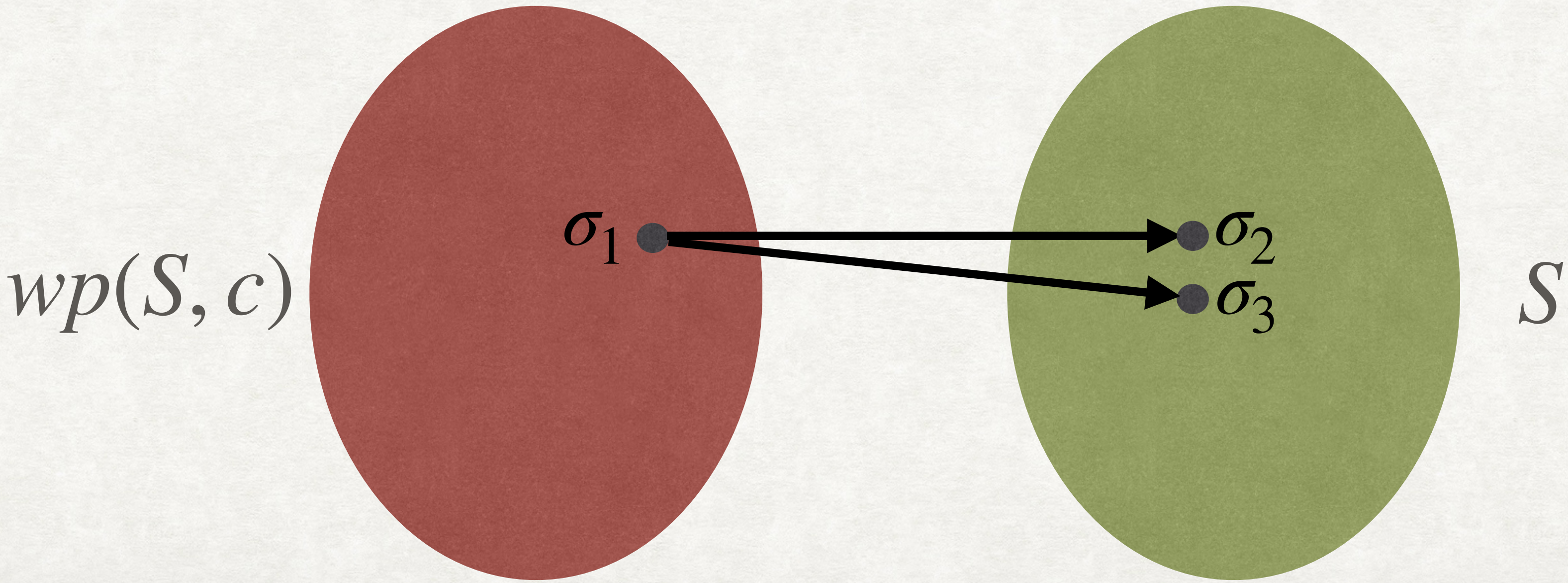
$$wp(S, c) \triangleq \{\sigma \mid \forall \sigma' .\ (\sigma, c) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \in S\}$$

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.

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

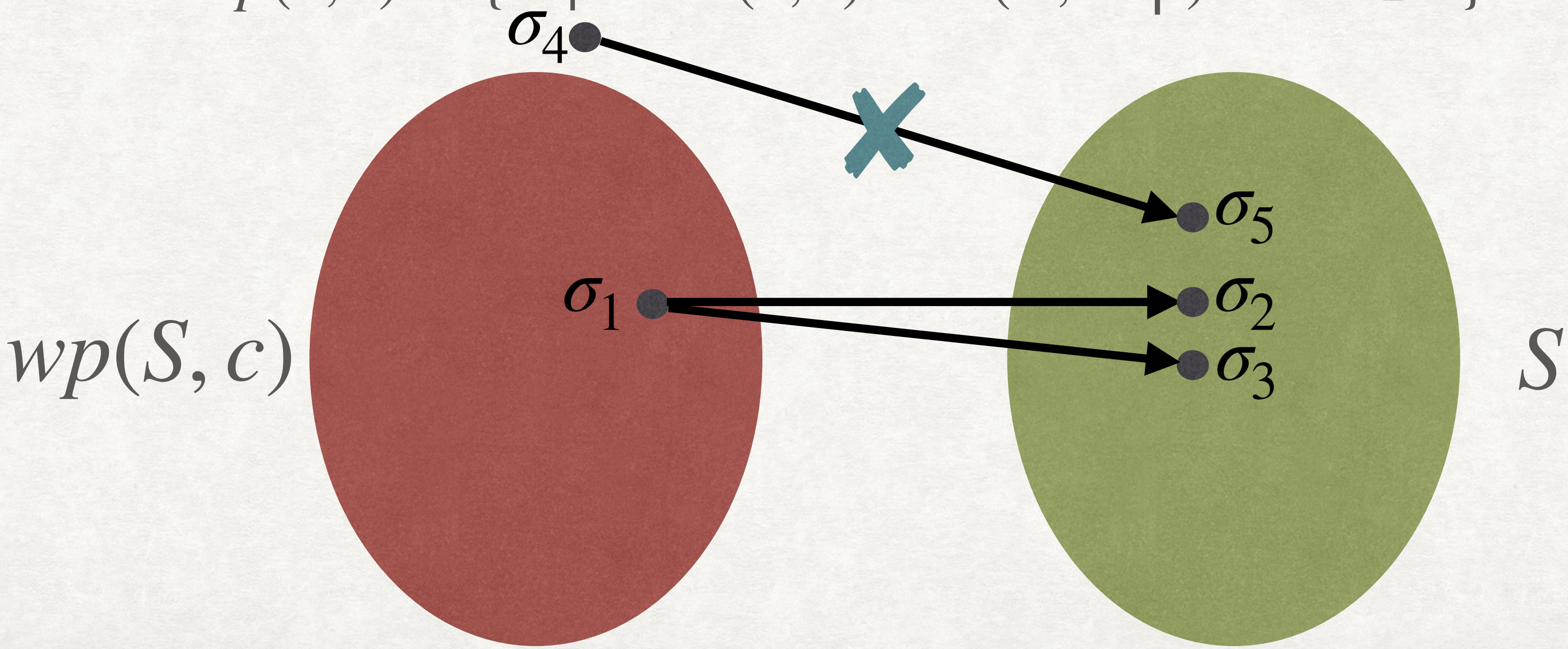


WEAKEST-PRECONDITION

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.

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

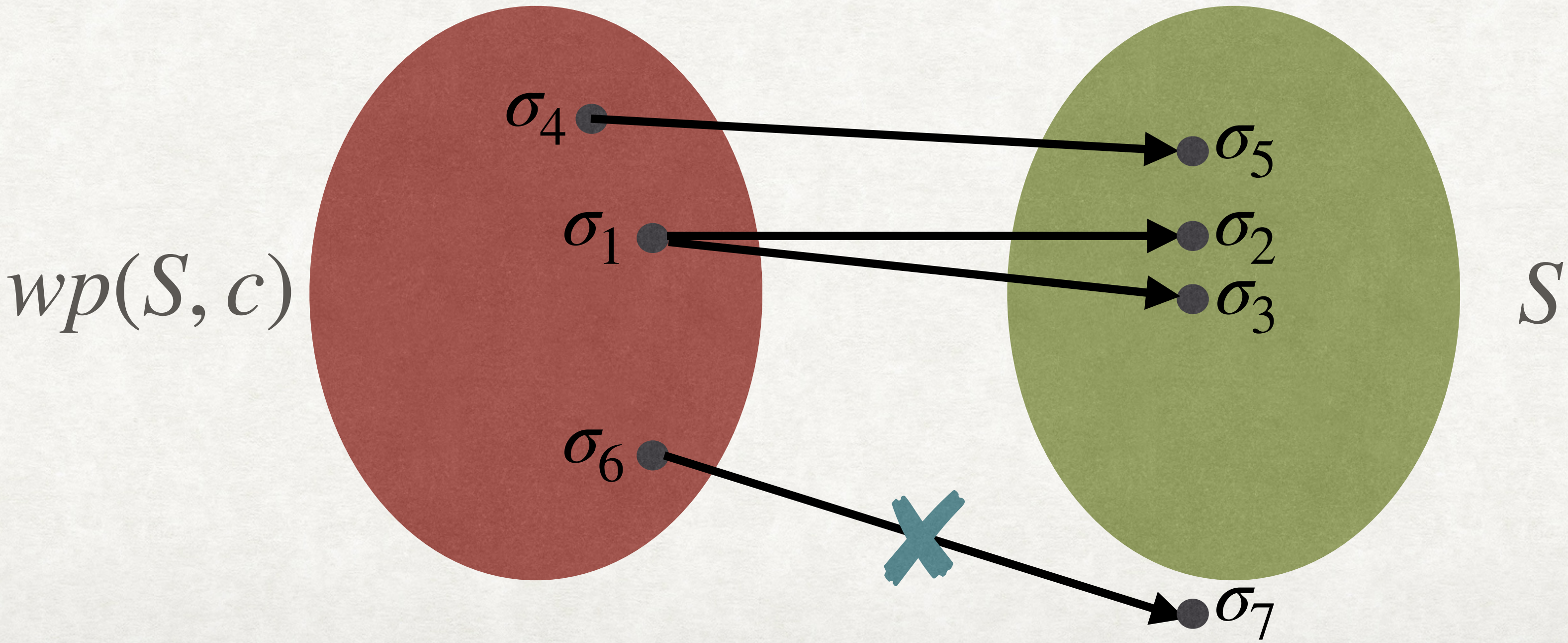


WEAKEST-PRECONDITION

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.

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

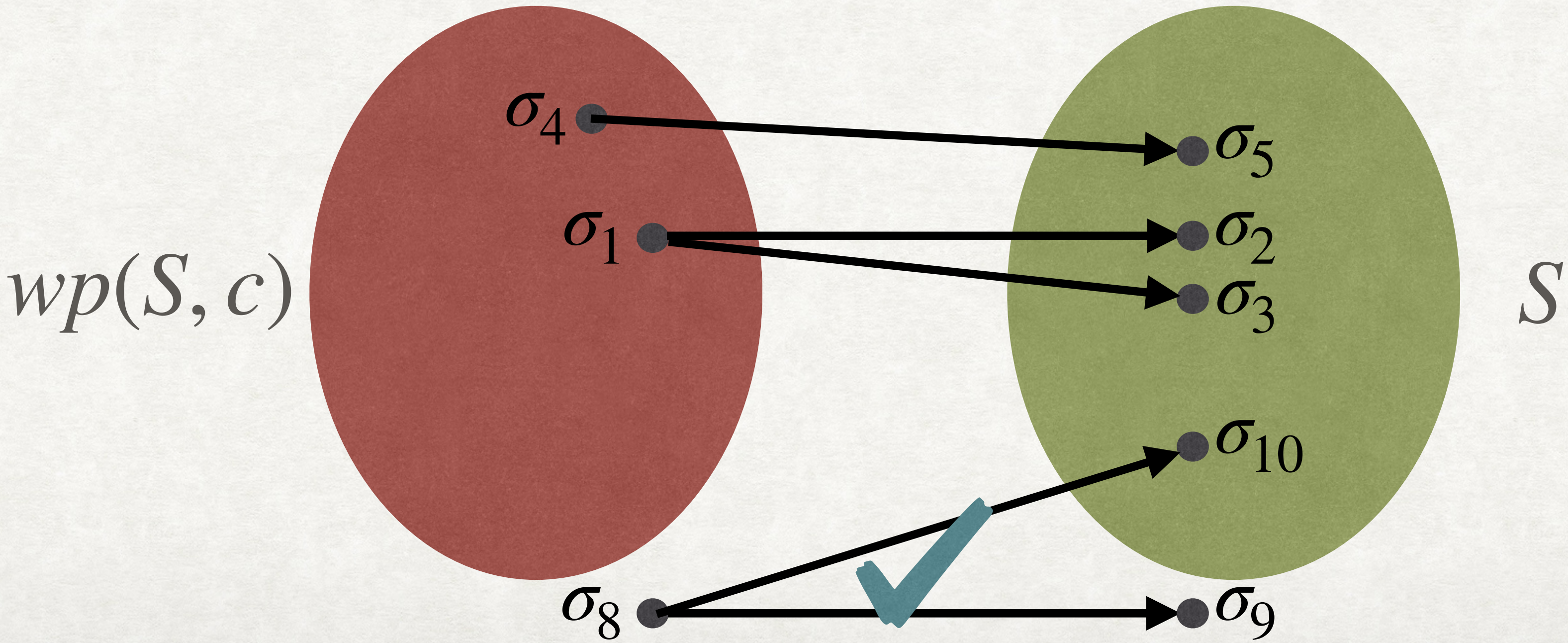


WEAKEST-PRECONDITION

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.

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



WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- 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.

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

- 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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

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

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

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

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

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

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

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:

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

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:

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

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:

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

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:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

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

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

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

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\mathrm{x} > 0, \mathrm{x{:=}havoc}) \equiv \forall \mathrm{x}\,.\ \mathrm{x} > 0 \equiv \mathit{false}$
- $wp(\mathrm{x} + \mathrm{i} \leq 0, \mathrm{x{:=}havoc}) \equiv \forall \mathrm{x}\,.\, \mathrm{x} + \mathrm{i} \leq 0 \equiv \mathit{false}$
- $wp(\mathrm{x} \geq 0, \mathrm{assume(x{=}1)}) \equiv\ ???$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\text{x} > 0, \text{x:=havoc}) \equiv \forall \text{x} .\ \text{x} > 0 \equiv \mathit{false}$
- $wp(\text{x} + \text{i} \leq 0, \text{x:=havoc}) \equiv \forall \text{x} . \text{x} + \text{i} \leq 0 \equiv \mathit{false}$
- $wp(\text{x} \geq 0, \text{assume(x=1)}) \equiv \text{x=1} \rightarrow \text{x} \geq 0 \equiv \mathit{true}$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\text{x} > 0, \text{x:=havoc}) \equiv \forall \text{x} .\ \text{x} > 0 \equiv \textit{false}$
- $wp(\text{x} + \text{i} \leq 0, \text{x:=havoc}) \equiv \forall \text{x} . \text{x} + \text{i} \leq 0 \equiv \textit{false}$
- $wp(\text{x} \geq 0, \text{assume(x=1)}) \equiv \text{x=1} \rightarrow \text{x} \geq 0 \equiv \textit{true}$
- $wp(\text{x} > 0, \text{assume (x<0)}) \equiv ???$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

- $wp(\text{x} > 0, \text{x:=havoc}) \equiv \forall \text{x} .\ \text{x} > 0 \equiv \mathit{false}$
- $wp(\text{x} + \text{i} \leq 0, \text{x:=havoc}) \equiv \forall \text{x} . \text{x} + \text{i} \leq 0 \equiv \mathit{false}$
- $wp(\text{x} \geq 0, \text{assume(x=1)}) \equiv \text{x=1} \rightarrow \text{x} \geq 0 \equiv \mathit{true}$
- $wp(\text{x} > 0, \text{assume (x<0)}) \equiv \text{x} < 0 \rightarrow \text{x} > 0 \equiv \text{x} \geq 0$

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT

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

WEAKEST PRE-CONDITION

ASSERT

- $wp(F, \text{assert}(G)) \equiv F \wedge G$
  - Assume that $F \neq true$.
  - Assumption makes sense because we do not want error $= 1$ after assert.