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.

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

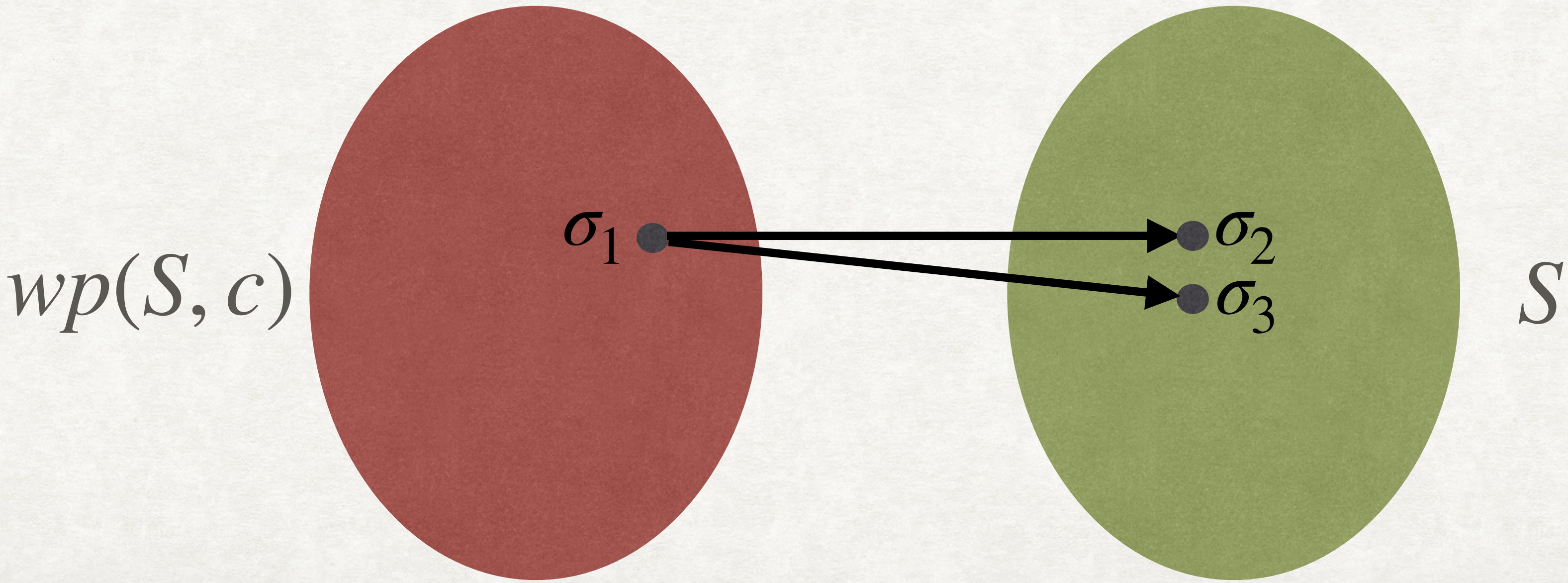
Equivalently, $\sigma \in wp(S, c) \Leftrightarrow \forall \sigma' \,.\, (\sigma, c) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \in S$

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.

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

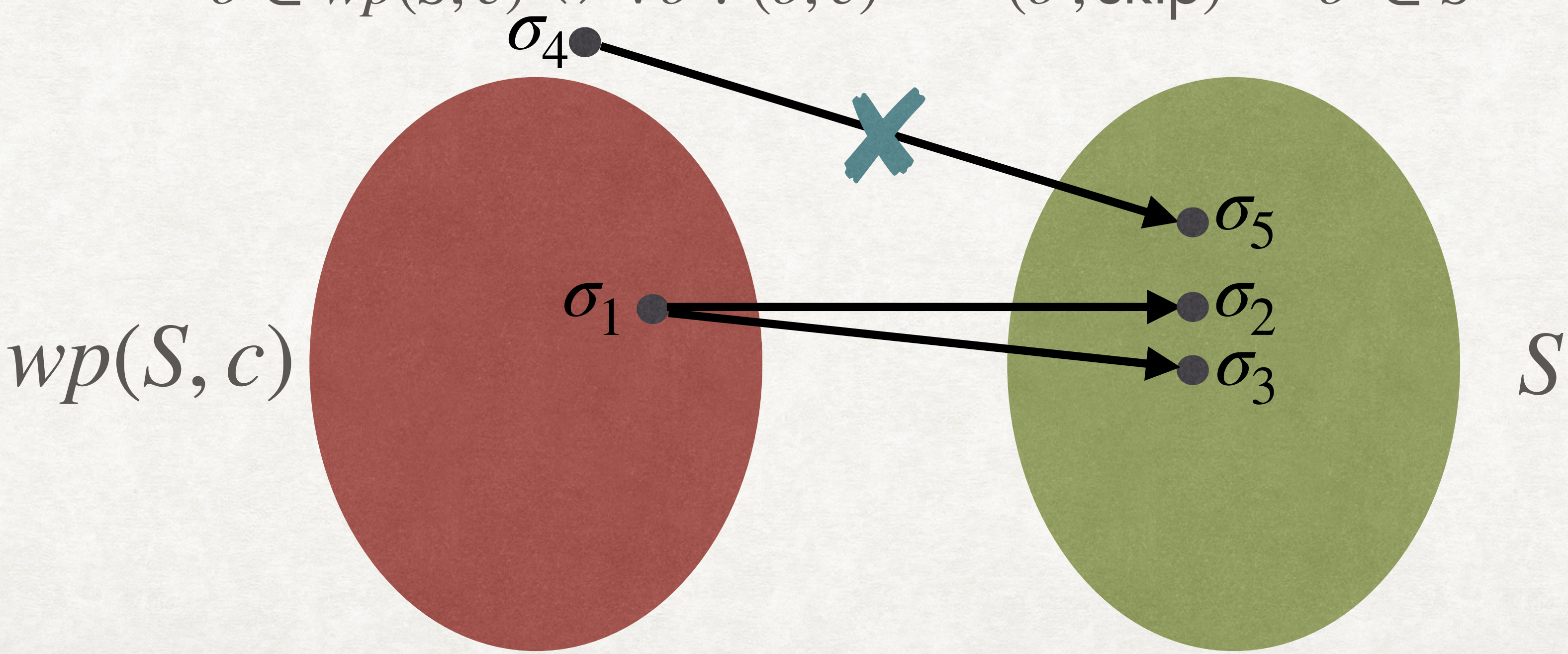


WEAKEST-PRECONDITION

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.

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

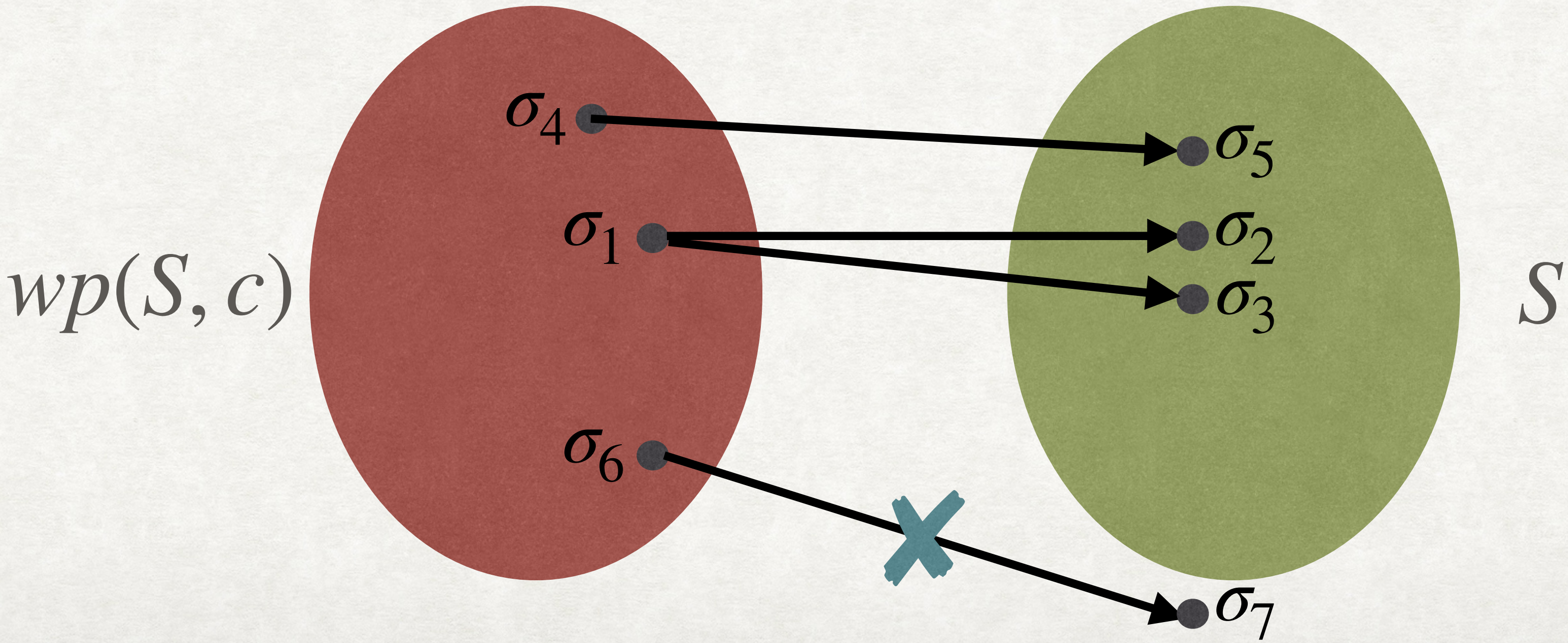


WEAKEST-PRECONDITION

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.

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

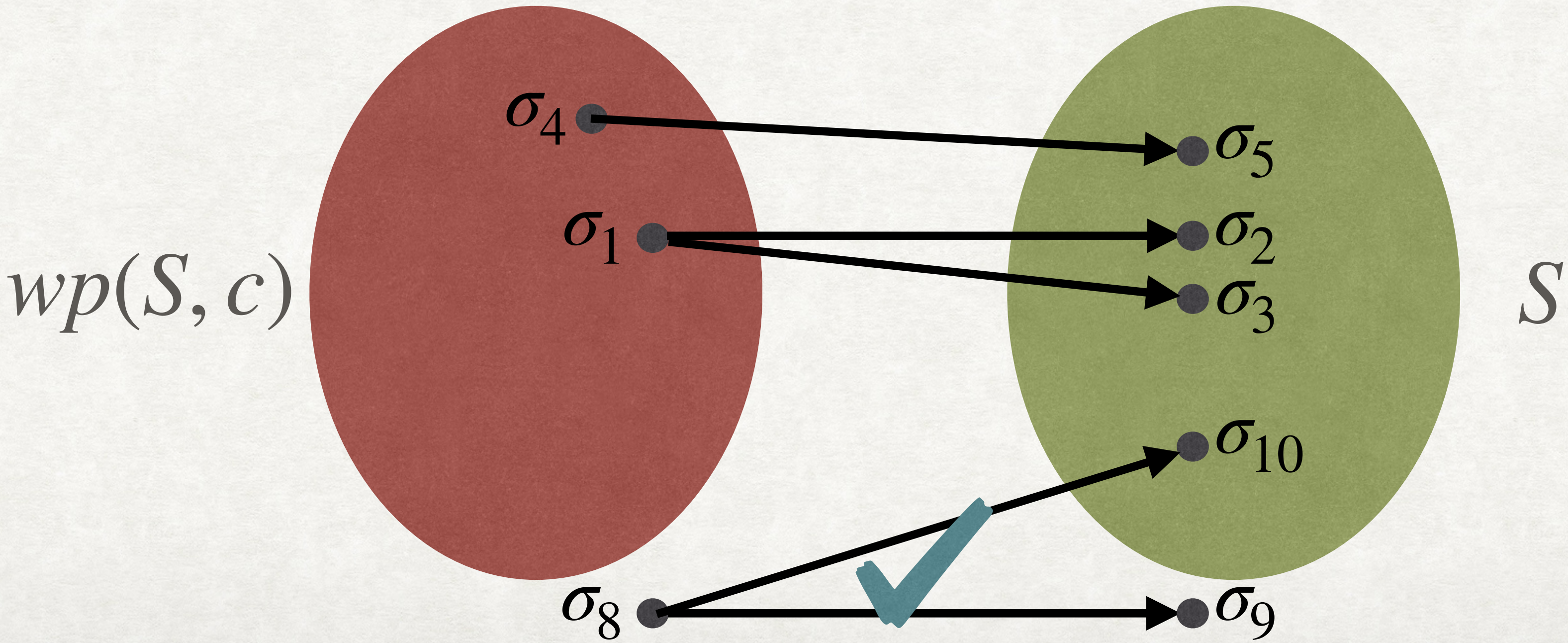


WEAKEST-PRECONDITION

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

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

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

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

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

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

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

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

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

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

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:

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

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:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

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

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

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

EXAMPLES:

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

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

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

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

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

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(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)) $\equiv$ x $< 0 \rightarrow$ x $> 0 \equiv$ x ≥ 0
- Does there exist F and G such that $wp(F,$ 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

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

- $wp($x ≥ 0,assert(x=1)$) \equiv$ x $= 1$
- $wp($x $= 2$,assert(x=3)$) \equiv ???$

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

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

WEAKEST PRE-CONDITION

SEQUENTIAL COMPOSITION

Proof[Continued]: Now, we will show that
$wp(S, c_1; c_2) \subseteq wp(wp(S, c_2), c_1)$.

WEAKEST PRE-CONDITION

SEQUENTIAL COMPOSITION

Proof[Continued]: Now, we will show that $wp(S, c_1; c_2) \subseteq wp(wp(S, c_2), c_1)$.

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

Then, $\forall \sigma' . (\sigma, c_1; c_2) \hookrightarrow^* (\sigma', \text{skip}) \rightarrow \sigma' \in S$ [3].

If $\neg \exists \sigma'' . (\sigma, c_1) \hookrightarrow^* (\sigma'', \text{skip})$, then $\sigma \in wp(wp(S, c_2), c_1)$.

Otherwise, consider σ'' such that $(\sigma, c_1) \hookrightarrow^* (\sigma'', \text{skip})$.

Then, $\sigma'' \in wp(S, c_2)$. Because otherwise, there would exist σ' such that $(\sigma'', c_2) \hookrightarrow^* (\sigma', \text{skip})$ and $\sigma' \notin S$. That would violate [3].

Hence, $\forall \sigma'' . (\sigma, c_1) \hookrightarrow^* (\sigma'', \text{skip}) \rightarrow \sigma'' \in wp(S, c_2)$.

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

WEAKEST PRE-CONDITION

IF-THEN-ELSE

- $wp(\mathrm{F}, \mathrm{if(G)\ then\ c_1\ else\ c_2}) \equiv ???$

WEAKEST PRE-CONDITION

IF-THEN-ELSE

- $wp(\text{F, if(G) then } c_1 \text{ else } c_2) \equiv (\text{G} \rightarrow wp(\text{F}, c_1)) \wedge (\neg\text{G} \rightarrow wp(\text{F}, c_2))$

WEAKEST PRE-CONDITION

IF-THEN-ELSE

- $wp(\mathsf{F}, \text{if(G) then } \mathsf{c}_1 \text{ else } \mathsf{c}_2) \equiv (\mathsf{G} \rightarrow wp(\mathsf{F}, \mathsf{c}_1)) \wedge (\neg \mathsf{G} \rightarrow wp(\mathsf{F}, \mathsf{c}_2))$

Proof: We will show that $LHS \rightarrow RHS$.

Consider $\sigma \vDash LHS$. By definition,

$\forall \sigma' . (\sigma, \text{if(G) then } \mathsf{c}_1 \text{ else } \mathsf{c}_2) \hookrightarrow^* (\sigma', \text{skip}) \rightarrow \sigma' \vDash F$ [1].

Suppose $\sigma \vDash G$. Then, $(\sigma, \text{if(G) then } \mathsf{c}_1 \text{ else } \mathsf{c}_2) \hookrightarrow (\sigma, \mathsf{c}_1)$.

Consider σ' such that $(\sigma, c_1) \hookrightarrow^* (\sigma', \text{skip})$. Then by [1], $\sigma' \vDash F$. Hence $\sigma \vDash wp(F, c_1)$. This implies that $\sigma \vDash RHS$.

Suppose $\sigma \nvDash G$. Then, $(\sigma, \text{if(G) then } \mathsf{c}_1 \text{ else } \mathsf{c}_2) \hookrightarrow (\sigma, \mathsf{c}_2)$.

Consider σ' such that $(\sigma, c_2) \hookrightarrow^* (\sigma', \text{skip})$. Then by [1], $\sigma' \vDash F$. Hence $\sigma \vDash wp(F, c_2)$. This implies that $\sigma \vDash RHS$.

Hence, $LHS \rightarrow RHS$.

HOMEWORK: PROVE THE OTHER DIRECTION

WEAKEST PRE-CONDITION

IF-THEN-ELSE

- $wp(\text{F, if(G) then } c_1 \text{ else } c_2) \equiv (\text{G} \rightarrow wp(\text{F}, c_1)) \wedge (\neg\text{G} \rightarrow wp(\text{F}, c_2))$

WEAKEST PRE-CONDITION

IF-THEN-ELSE

- $wp(\mathrm{F}, \mathrm{if(G)\ then\ c_1\ else\ c_2}) \equiv (\mathrm{G} \rightarrow wp(\mathrm{F}, \mathrm{c_1})) \wedge (\neg \mathrm{G} \rightarrow wp(\mathrm{F}, \mathrm{c_2}))$
- Example:

$wp(\mathrm{y} = 0, \mathrm{if(x>10)\ then\ y:=z+1\ else\ y:=z-1})$

$\equiv$

WEAKEST PRE-CONDITION

IF-THEN-ELSE

- $wp(\mathrm{F}, \mathrm{if(G)\ then\ c_1\ else\ c_2}) \equiv (\mathrm{G} \rightarrow wp(\mathrm{F}, \mathrm{c_1})) \wedge (\neg \mathrm{G} \rightarrow wp(\mathrm{F}, \mathrm{c_2}))$
- Example:

$wp(\mathrm{y} = 0, \mathrm{if(x>10)\ then\ y{:=}z+1\ else\ y{:=}z-1})$

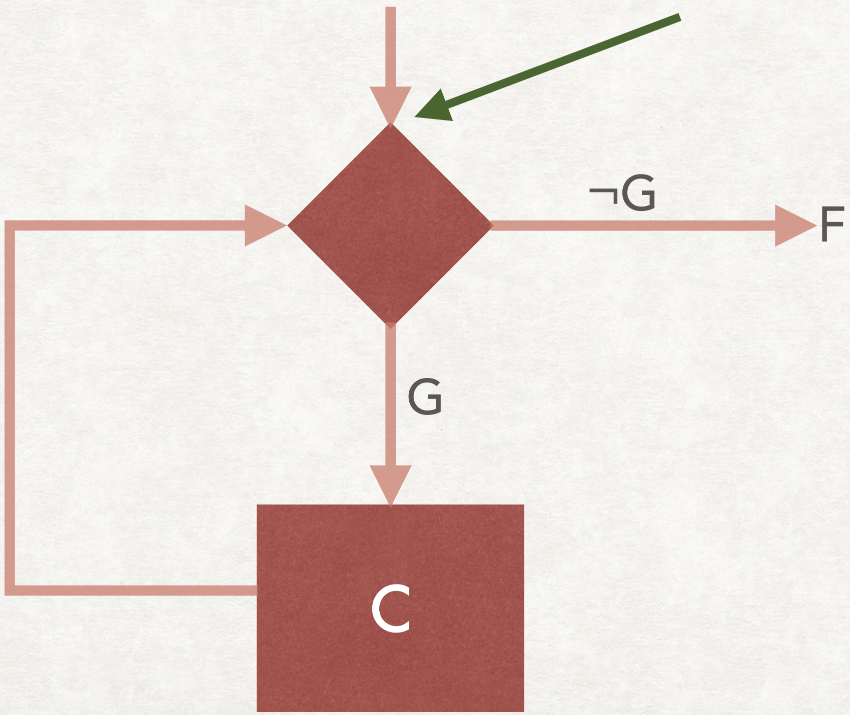
$\equiv (\mathrm{x} > 10 \rightarrow wp(\mathrm{y} = 0, \mathrm{y{:=}z+1})) \wedge (\neg(\mathrm{x} > 10) \rightarrow wp(\mathrm{y} = 0, \mathrm{y{:=}z-1}))$

$\equiv (\mathrm{x} > 10 \rightarrow \mathrm{z} = -1) \wedge (\mathrm{x} \leq 10 \rightarrow \mathrm{z} = 1)$

WEAKEST PRE-CONDITION

WHILE LOOPS

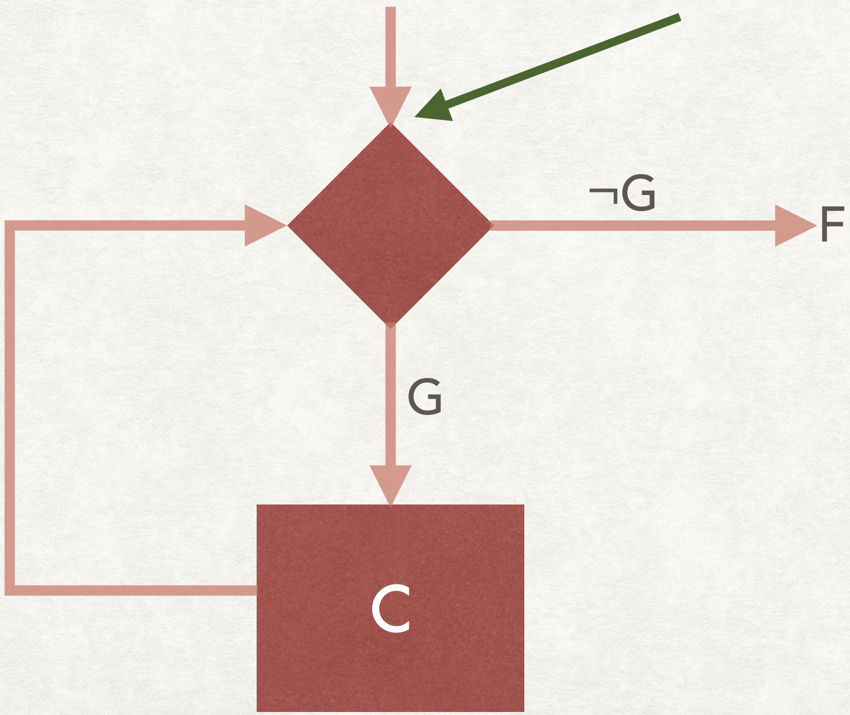
- wp(F, while(G) do c) $\equiv$???
  - Collect all states at the beginning of loop, which would lead to a state in F if the loop exits after k iterations (for $k = 0,1,2,\ldots$)



WEAKEST PRE-CONDITION

WHILE LOOPS

- wp(F, while(G) do c) $\equiv$ $???$
  - Collect all states at the beginning of loop, which would lead to a state in F if the loop exits after k iterations (for $k = 0,1,2,\ldots$)

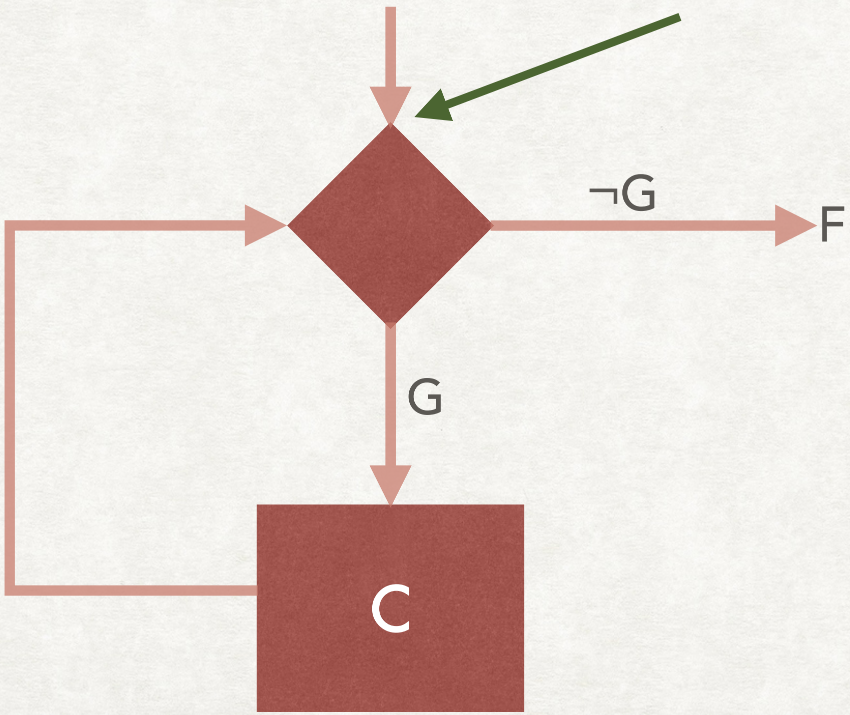


Iteration k	Initial State for exit after k iterations
0	
1	
2	
…	…

WEAKEST PRE-CONDITION

WHILE LOOPS

- wp(F, while(G) do c) $\equiv$???
  - Collect all states at the beginning of loop, which would lead to a state in F if the loop exits after k iterations (for $k = 0,1,2,\ldots$)

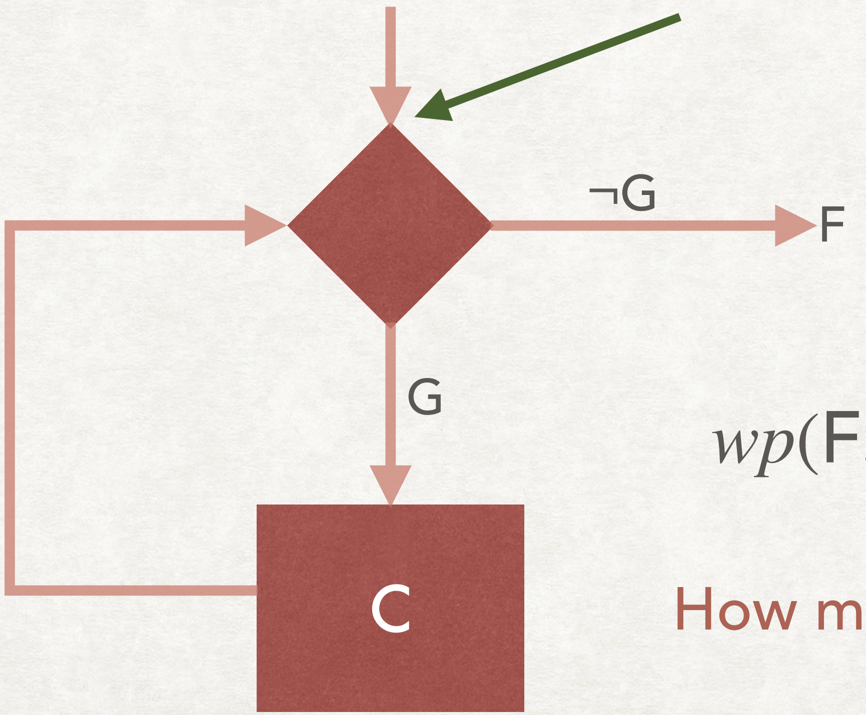


Iteration k	Initial State for exit after k iterations
0	$\neg G \wedge F$
1	$G \wedge wp(\neg G \wedge F, c)$
2	$G \wedge wp(G \wedge wp(\neg G \wedge F, c))$
…	…

WEAKEST PRE-CONDITION

WHILE LOOPS

- wp(F, while(G) do c) $\equiv$???
  - Collect all states at the beginning of loop, which would lead to a state in F if the loop exits after k iterations (for $k = 0,1,2,\ldots$)



$$F^0 \equiv \neg G \wedge F$$

$$F^k \equiv G \wedge wp(F^{k-1}, c)$$

$$wp(\text{F, while(G) do c}) \triangleq \bigvee_{k=0}^{\infty} F^k$$

How many F^k should be calculated?

Until $F^k \rightarrow \bigvee_{i}^{k-1} F^i$

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

- wp(x >0,while(x<10) do x:=x+1;) $\triangleq$???

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

- $wp($x > 0,while(x<10) do x:=x+1;$) \triangleq \top$

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

- $wp(\text{x} > 0, \text{while(x<10) do x:=x+1;}) \triangleq \top$
- $wp(\text{x} < 0, \text{while(x<10) do x:=x+1;}) \triangleq ???$

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

- $wp($x > 0,while(x<10) do x:=x+1;$) \triangleq \top$
- $wp($x < 0,while(x<10) do x:=x+1;$) \triangleq \bot$

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

- $wp($x > 0,while(x<10) do x:=x+1;$) \triangleq \top$
- $wp($x < 0,while(x<10) do x:=x+1;$) \triangleq \bot$
- $wp($x $= 10$,while(x<10) do x:=x+1;$) \triangleq ???$

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

- $wp(\text{x} > 0, \text{while(x<10) do x:=x+1;}) \triangleq \top$
- $wp(\text{x} < 0, \text{while(x<10) do x:=x+1;}) \triangleq \bot$
- $wp(\text{x} = 10, \text{while(x<10) do x:=x+1;}) \triangleq \text{x} \leq 10$

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

- $wp(\text{x} > 0, \text{while(x<10) do x:=x+1;}) \triangleq \top$
- $wp(\text{x} < 0, \text{while(x<10) do x:=x+1;}) \triangleq \bot$
- $wp(\text{x} = 10, \text{while(x<10) do x:=x+1;}) \triangleq \text{x} \leq 10$
- $wp(\text{x} = 11, \text{while(x<10) do x:=x+1;}) \triangleq ???$

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

- $wp(\text{x} > 0, \text{while(x<10) do x:=x+1;}) \triangleq \top$
- $wp(\text{x} < 0, \text{while(x<10) do x:=x+1;}) \triangleq \bot$
- $wp(\text{x} = 10, \text{while(x<10) do x:=x+1;}) \triangleq \text{x} \leq 10$
- $wp(\text{x} = 11, \text{while(x<10) do x:=x+1;}) \triangleq \text{x} = 11$

WEAKEST PRE-CONDITION AND VERIFICATION

- Given a program c with assertions, then c is safe if error $= 0 \rightarrow wp($error $= 0$,c) is valid.
- The Hoare Triple $\{P\}$c$\{Q\}$ is valid if $P \rightarrow wp(Q,$ c) is valid.
- Do we have a decidable procedure for wp?
    - No, due to the unbounded computation required for while loops.
- WP is sound and relatively complete.

SP AND WP

- What can we say about $wp(sp(P, \mathsf{c}), \mathsf{c})$, $sp(wp(P, \mathsf{c}), \mathsf{c})$, and P?
  - $sp(wp(P, \mathsf{c}), \mathsf{c}) \subseteq P \subseteq wp(sp(P, \mathsf{c}), \mathsf{c})$
  - Prove this!
- Give examples for $wp(sp(P, \mathsf{c}), \mathsf{c}) \neq P$ and $sp(wp(P, \mathsf{c}), \mathsf{c}) \neq P$