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.

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

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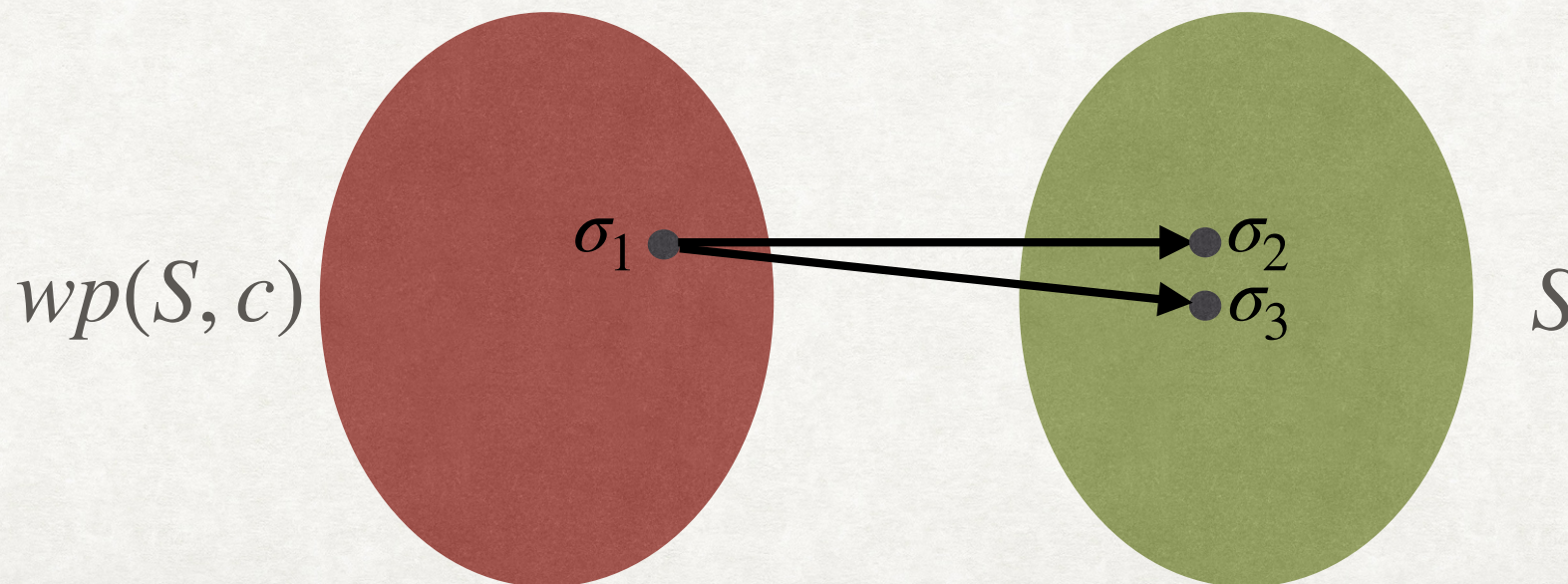
WEAKEST-PRECONDITION

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.

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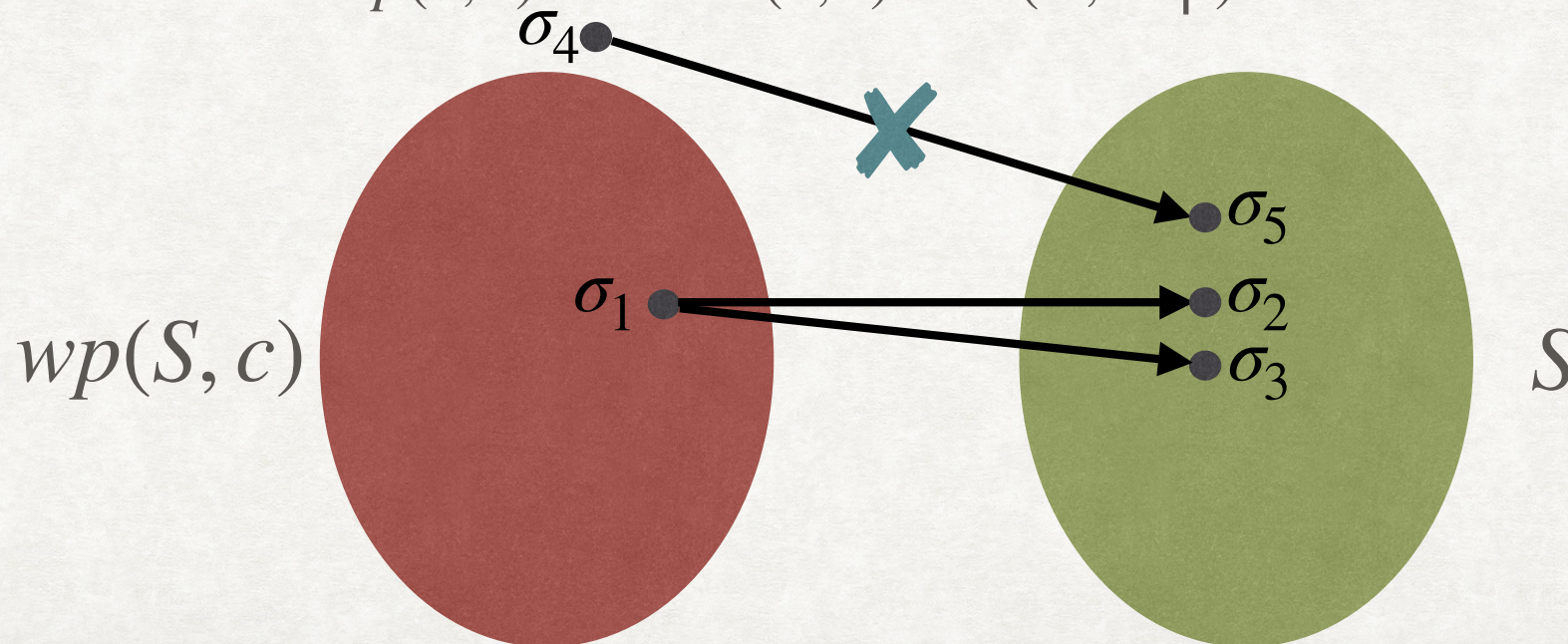
WEAKEST-PRECONDITION

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.

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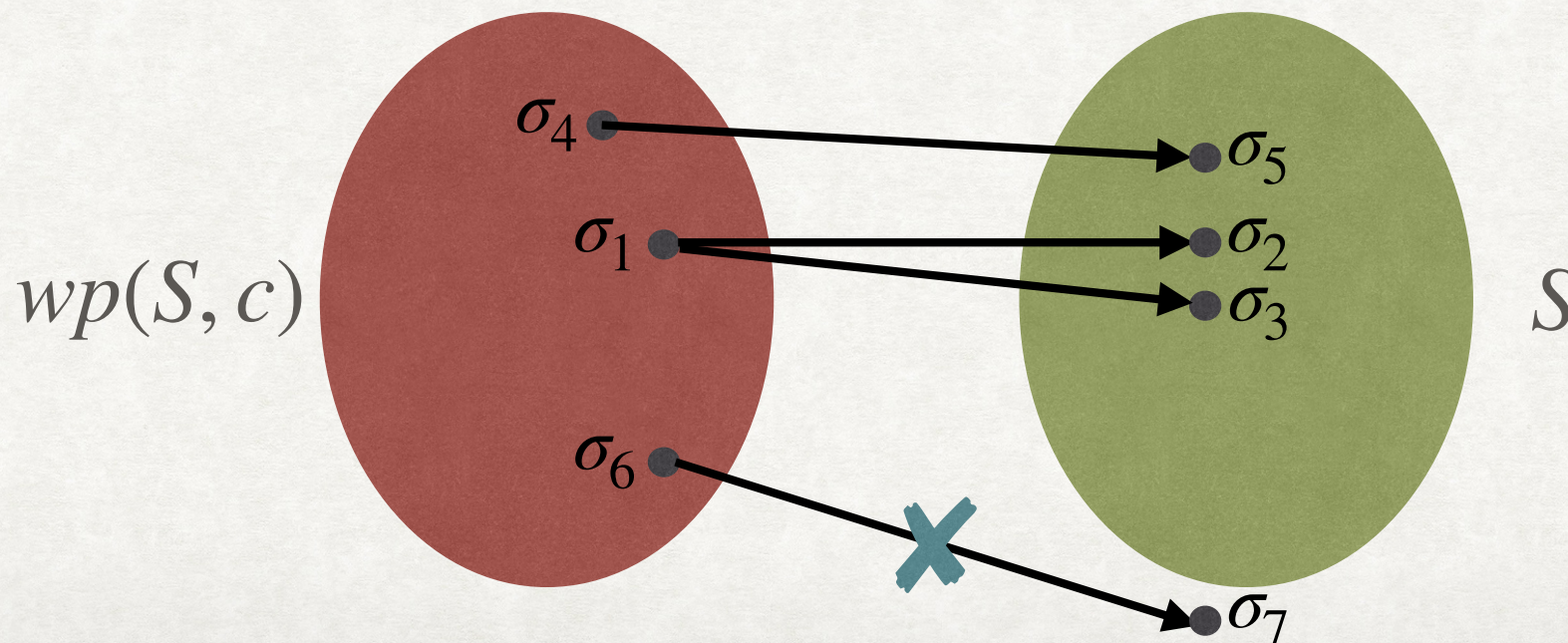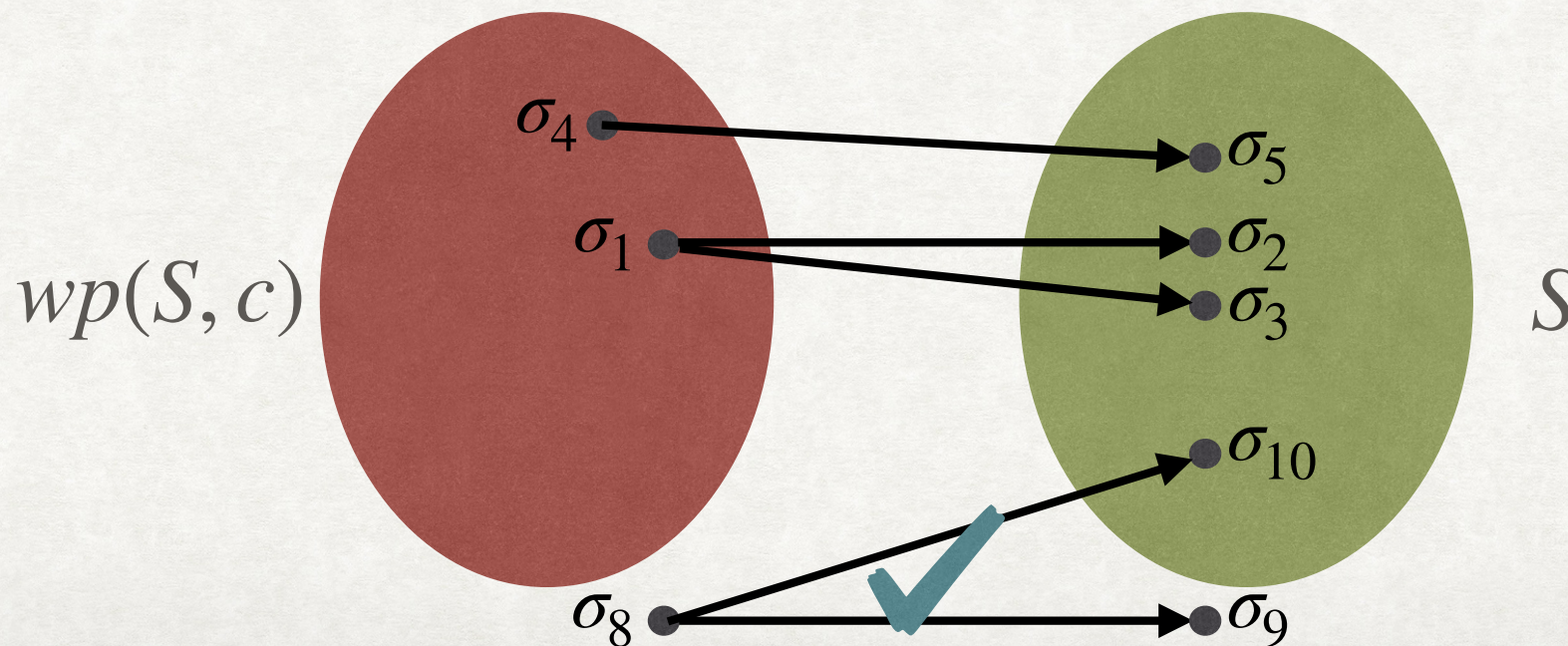
WEAKEST-PRECONDITION

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

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

- We can use a FOL formula F to represent a set of states.

- The symbolic weakest pre-condition operator can be defined as:

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

EXAMPLES

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

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

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

wp(x > 10,x:=x+1) ≜ ∀x' . x' = x + 1 → x' > 10

≡ x + 1 > 10 ≡ x > 9

wp(⊤ , c) ≡ ⊤

wp(⊥ , c) ≡ All states for which c does not terminate

wp(⊥ , assume(x>0)) ≡ ???

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

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

$\equiv x \leq 0$

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

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

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

$$\equiv F[e/x]$$

WEAKEST PRE-CONDITION
ASSIGNMENT STATEMENT

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

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

$\qquad\qquad \equiv \forall V' . \text{x'} = \text{e} \wedge frame(\text{x'}) \rightarrow F[V'/V]$

$\qquad\qquad \equiv F[e/x]$

EXAMPLES:

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

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

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

WEAKEST PRE-CONDITION
ASSIGNMENT STATEMENT

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

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

$\qquad\qquad \equiv \forall V' . \text{x'} = \text{e} \wedge frame(\text{x'}) \rightarrow F[V'/V]$

$\qquad\qquad \equiv F[e/\text{x}]$

EXAMPLES:

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

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

WEAKEST PRE-CONDITION
ASSIGNMENT STATEMENT

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

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

$\qquad\qquad \equiv \forall V'.\, \text{x'} = \text{e} \wedge \textit{frame}(\text{x'}) \rightarrow F[V'/V]$

$\qquad\qquad \equiv F[\text{e/x}]$

EXAMPLES:

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

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

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

WEAKEST PRE-CONDITION
ASSIGNMENT STATEMENT

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

$wp(F, \mathsf{x}{:=}\mathsf{e}) \triangleq \forall V'.\, \rho(\mathsf{x}{:=}\mathsf{e}) \to F[V'/V]$

$\qquad\qquad\qquad \equiv \forall V'.\, \mathsf{x}' = \mathsf{e} \wedge frame(\mathsf{x}') \to F[V'/V]$

$\qquad\qquad\qquad \equiv F[\mathsf{e}/\mathsf{x}]$

EXAMPLES:

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

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

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

WEAKEST PRE-CONDITION
HAVOC, ASSUME

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

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

$$\equiv \forall \text{x}' . F[\text{x}'/\text{x}] \equiv \forall \text{x} . F$$

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

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

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

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

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

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

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

HAVOC, ASSUME - EXAMPLES

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

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

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

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

WEAKEST PRE-CONDITION
HAVOC, ASSUME - EXAMPLES

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

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

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

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

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

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

WEAKEST PRE-CONDITION
HAVOC, ASSUME - EXAMPLES

- wp(x > 0,x:=havoc) $\equiv \forall$x . x > 0 $\equiv \perp$

- wp(x + i $\leq$ 0,x:=havoc) $\equiv \forall$x . x + i $\leq$ 0 $\equiv \perp$

- 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

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

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

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

- $wp(\text{x} > 0, \text{assume (x<0)}) \equiv \text{x} < 0 \rightarrow \text{x} > 0 \equiv \text{x} \geq 0$

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

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

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

- $wp(\text{x} > 0, \text{assume (x<0)}) \equiv \text{x} < 0 \rightarrow \text{x} > 0 \equiv \text{x} \geq 0$

- Does there exist F and G such that $wp(F, \text{assume(G)}) \equiv \bot$?

WEAKEST PRE-CONDITION

ASSERT

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

WEAKEST PRE-CONDITION

ASSERT

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

  - Assume that $F \neq \top$.

  - Assumption makes sense because we ideally want error $= 0$ after assert.

ASSERT

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

WEAKEST PRE-CONDITION

ASSERT

$$wp(F, \mathsf{assert}(G)) \triangleq \forall V' . (G \rightarrow frame(\varnothing)) \rightarrow F[V'/V]$$

$$\equiv \forall V' . (\neg G \vee frame(\varnothing)) \rightarrow F[V'/V]$$

$$\equiv \forall V' . (G \wedge \neg frame(\varnothing)) \vee F[V'/V]$$

$$\equiv \forall V' . (G \vee F[V'/V]) \wedge (\neg frame(\varnothing) \vee F[V'/V])$$

$$\equiv (G \vee \forall V' . F[V'/V]) \wedge \forall V' . (frame(\varnothing) \rightarrow F[V'/V])$$

$$\equiv (G \vee \forall V . F) \wedge F$$

$$\equiv (G \vee \bot) \wedge F$$

$$\equiv G \wedge F$$

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

ASSERT-EXAMPLES

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

- $wp(\text{x} = 2, \text{assert(x=3)}) \equiv ???$

ASSERT-EXAMPLES

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

- $wp(\text{x} = 2, \text{assert(x=3)}) \equiv \perp$

ASSERT-EXAMPLES

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

- $wp(\text{x} = 2, \text{assert(x=3)}) \equiv \perp$

- Does there exist F and G such that $wp(F, \text{assert(G)}) \equiv \top$?

WEAKEST PRE-CONDITION
SEQUENTIAL COMPOSITION

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

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

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

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

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

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

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

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

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

WEAKEST PRE-CONDITION

IF-THEN-ELSE

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

WEAKEST PRE-CONDITION

IF-THEN-ELSE

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

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

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

$\forall \sigma' . (\sigma, \mathsf{if(G)} \text{ then } \mathsf{c_1} \text{ else } \mathsf{c_2}) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \models F$ [1].

Suppose $\sigma \models G$. Then, $(\sigma, \mathsf{if(G)} \text{ then } \mathsf{c_1} \text{ else } \mathsf{c_2}) \hookrightarrow (\sigma, \mathsf{c_1})$.

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

Suppose $\sigma \not\models G$. Then, $(\sigma, \mathsf{if(G)} \text{ then } \mathsf{c_1} \text{ else } \mathsf{c_2}) \hookrightarrow (\sigma, \mathsf{c_2})$.

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

Hence, $LHS \rightarrow RHS$.

HOMEWORK: PROVE THE OTHER DIRECTION

WEAKEST PRE-CONDITION

IF-THEN-ELSE

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

WEAKEST PRE-CONDITION

IF-THEN-ELSE

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

- Example:

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

$\equiv$

WEAKEST PRE-CONDITION

IF-THEN-ELSE

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

- Example:

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

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

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

- $wp(\text{F}, \text{while(G) do c}) \equiv$???

  - Collect all states at the beginning of loop, which would lead to a state in F if the loop exits after k iterations (for $k = 0,1,2,\ldots$)
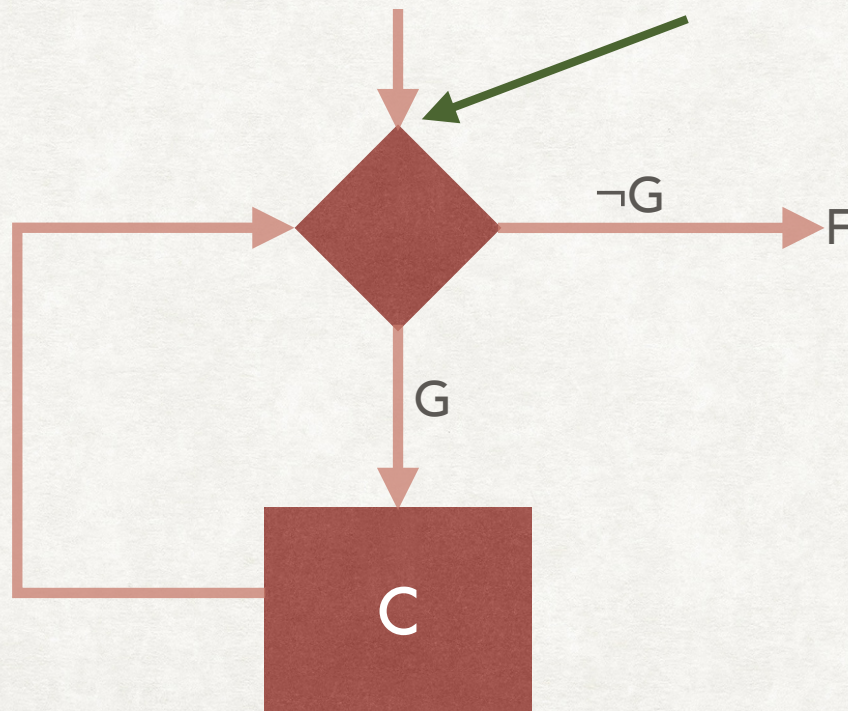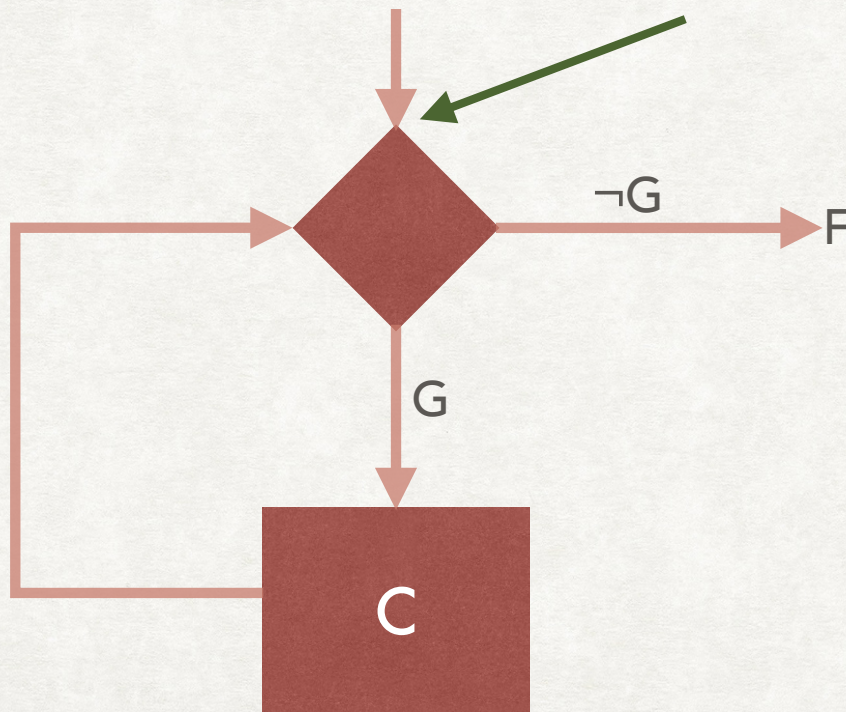
WEAKEST PRE-CONDITION

WHILE LOOPS

- $wp(\text{F}, \text{while(G) do c}) \equiv ???$

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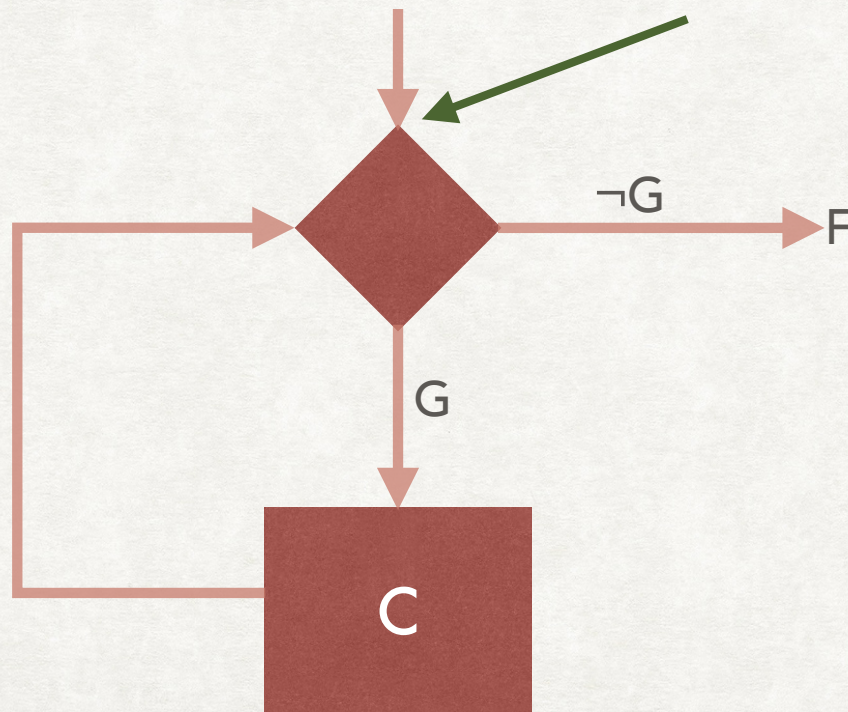

Iteration k	Initial State for exit after k iterations
0	
1	
2	
...	...

WEAKEST PRE-CONDITION
WHILE LOOPS

- $wp(\text{F}, \text{while(G) do c}) \equiv ???$

  - 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

- $wp(\text{F}, \text{while(G) do c}) \equiv ???$

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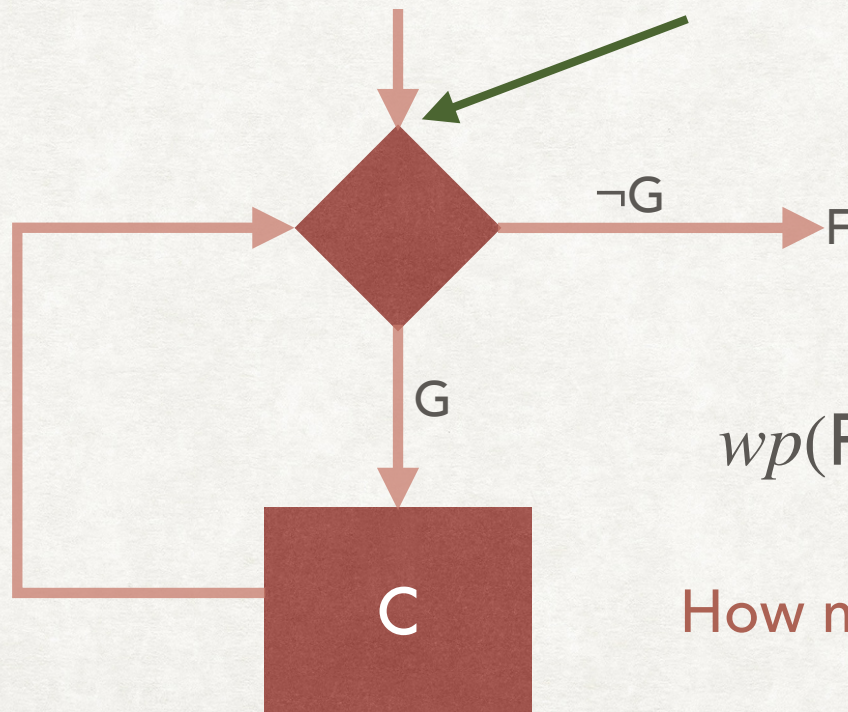
$$F^0 \equiv \neg G \wedge F$$

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

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

How many F^k should be calculated?

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

WEAKEST PRE-CONDITION
WHILE LOOPS - EXAMPLES

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

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

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

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;) $\triangleq \bot$

WHILE LOOPS - EXAMPLES

- wp(x > 0,while(x<10) do x:=x+1;) ≜ ⊤

- wp(x < 0,while(x<10) do x:=x+1;) ≜ ⊥

- wp(x = 10,while(x<10) do x:=x+1;) ≜ ???

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;) $\triangleq$ $x \leq 10$

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;) $\triangleq$ x $\leq$ 10

- wp(x = 11,while(x<10) do x:=x+1;) $\triangleq$???

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

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

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

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