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.

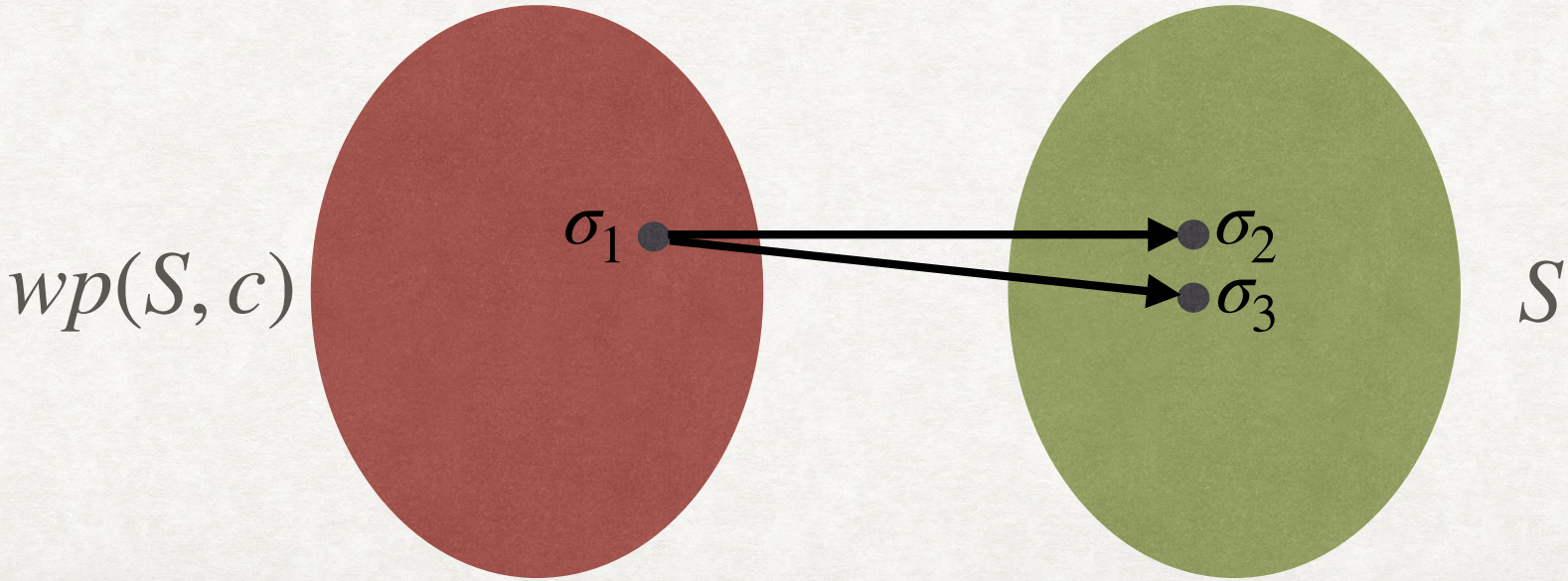
$$wp(S, c) \triangleq \{\sigma \mid \forall \sigma' \,.\, (\sigma, c) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \in S\}$$

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.

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

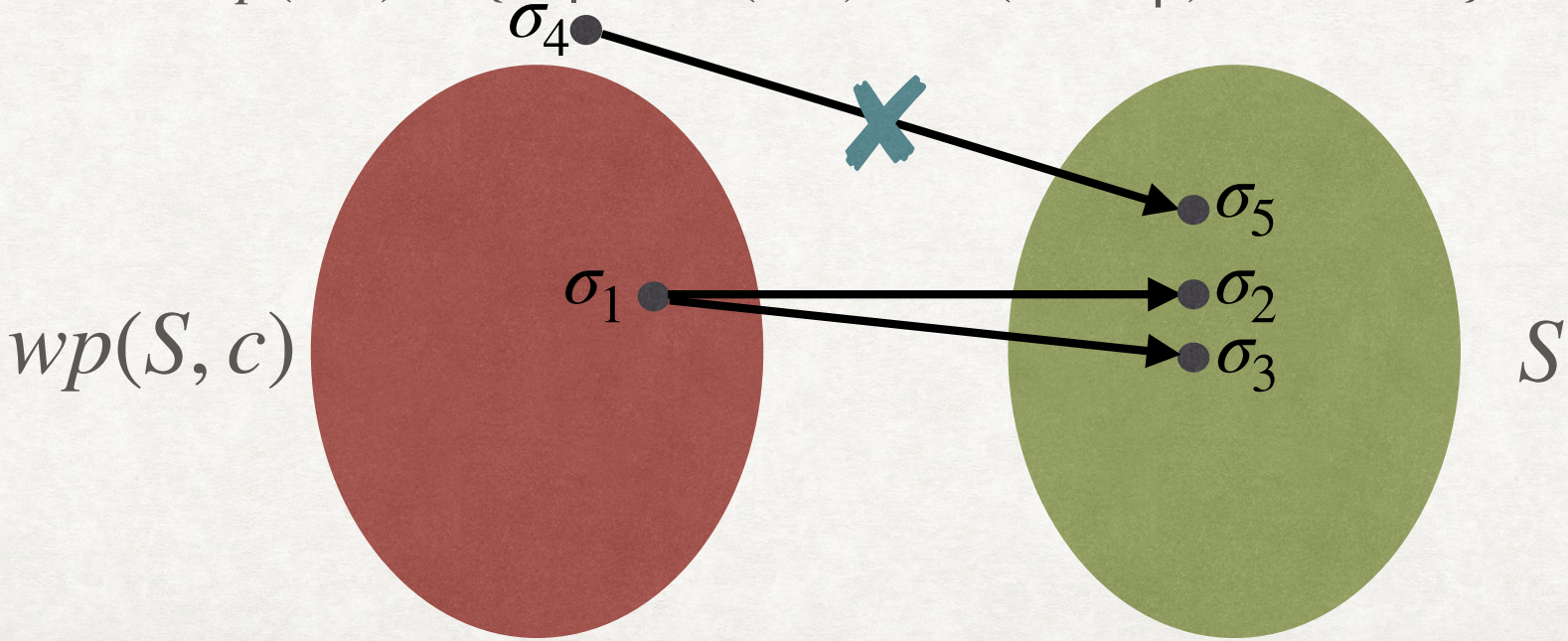


WEAKEST-PRECONDITION

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.

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

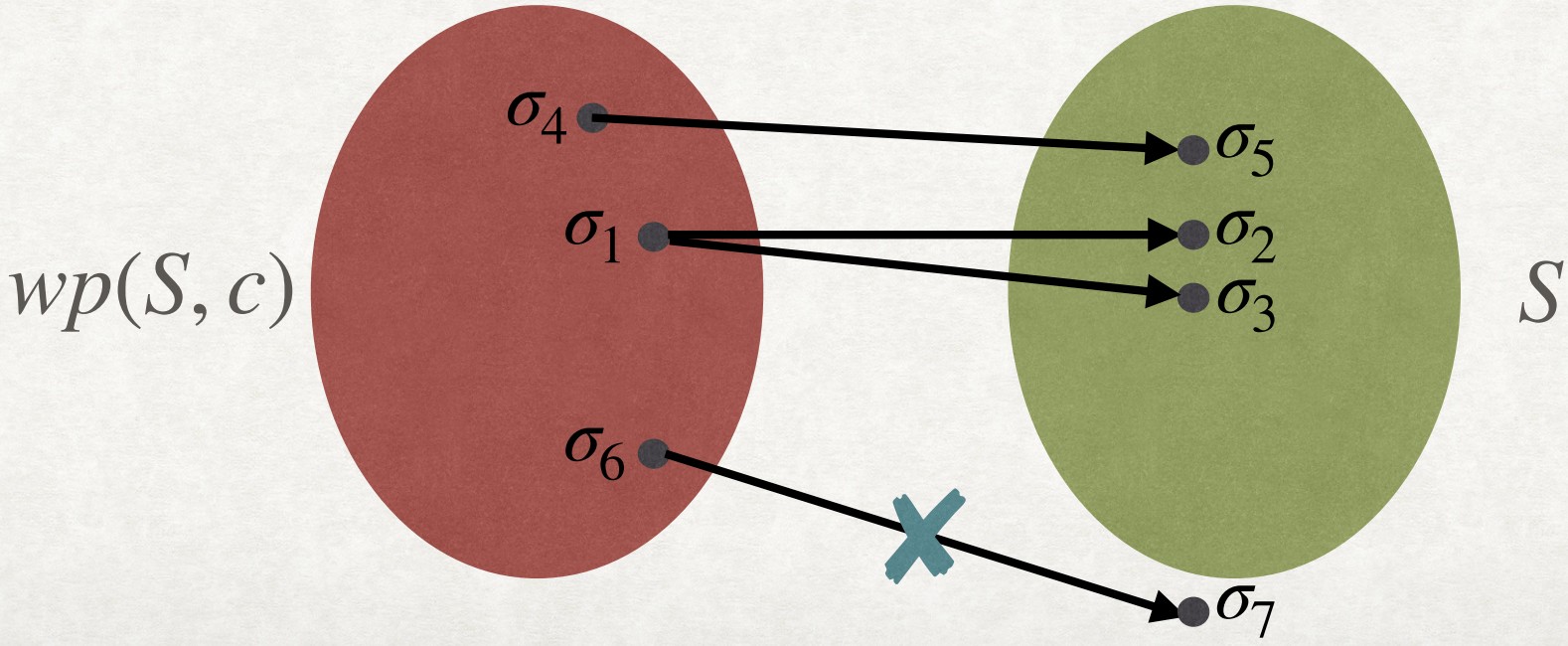


WEAKEST-PRECONDITION

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.

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

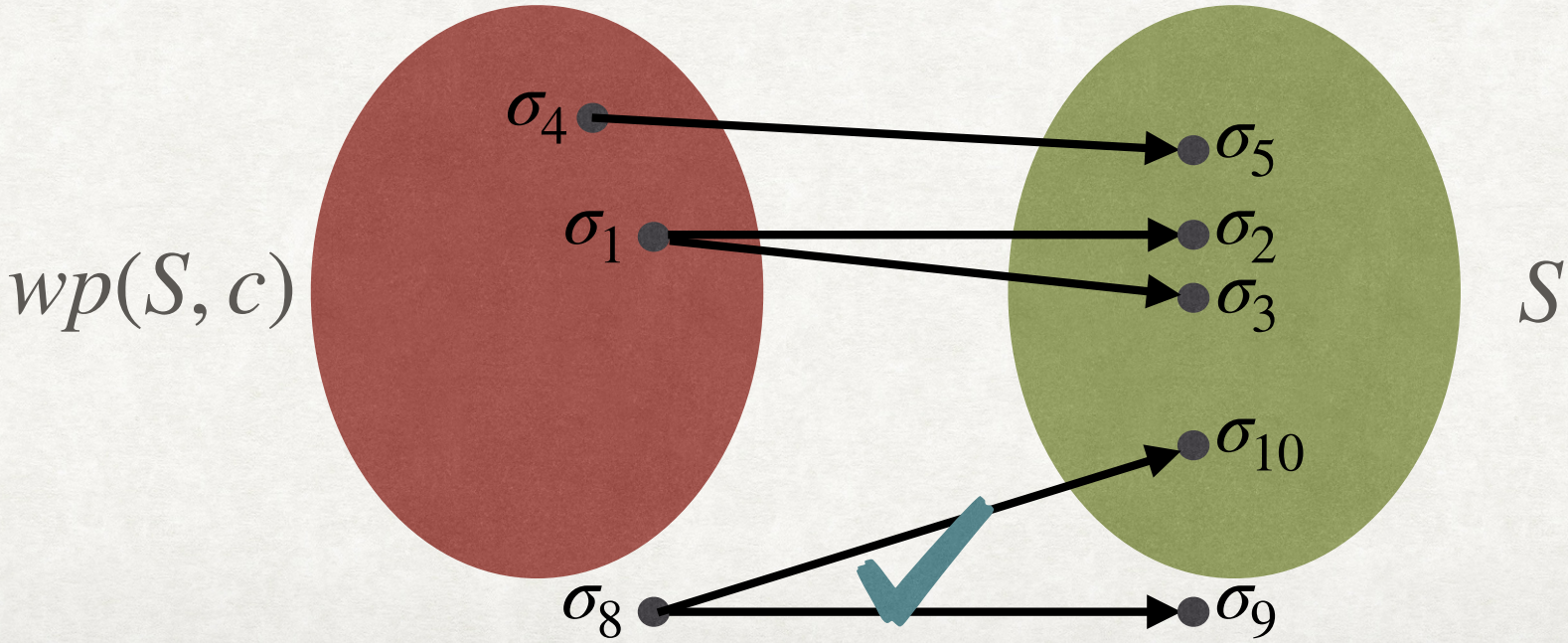


WEAKEST-PRECONDITION

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.

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



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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

$wp(true, c) \equiv true$

$wp(false, c) \equiv ???$

WEAKEST PRE-CONDITION

EXAMPLES

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

$wp(true, c) \equiv true$

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

WEAKEST PRE-CONDITION

EXAMPLES

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

$wp(true, c) \equiv true$

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

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

WEAKEST PRE-CONDITION

EXAMPLES

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

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

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

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

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:

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

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:

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

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:

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

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

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME

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

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME

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

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

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

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 $F \neq true$.
  - Assumption makes sense because we do not want error $= 1$ after assert.

ANNOUNCEMENT

- Assignment : Late Submission Policy
  - 1 Day late : 25% Penalty
  - 2 Day late : 50% Penalty
  - No submissions allowed after 2 days.

WEAKEST PRE-CONDITION

ASSERT

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

WEAKEST PRE-CONDITION

ASSERT

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

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 $wp(S, c_1; c_2) = wp(wp(S, c_2), c_1)$

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
$wp(S, c_1; c_2) \subseteq wp(wp(S, c_2), c_1)$.

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].

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

Then, $\sigma'' \in wp(S, c_2)$. Because otherwise, [3] would be violated.

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

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, [3] would be violated.

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

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

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

WEAKEST PRE-CONDITION

IF-THEN-ELSE

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

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

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

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

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

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

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

Consider σ' such that $(\sigma, c_2) \hookrightarrow^* (\sigma', \text{skip})$. 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

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

WEAKEST PRE-CONDITION

IF-THEN-ELSE

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

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

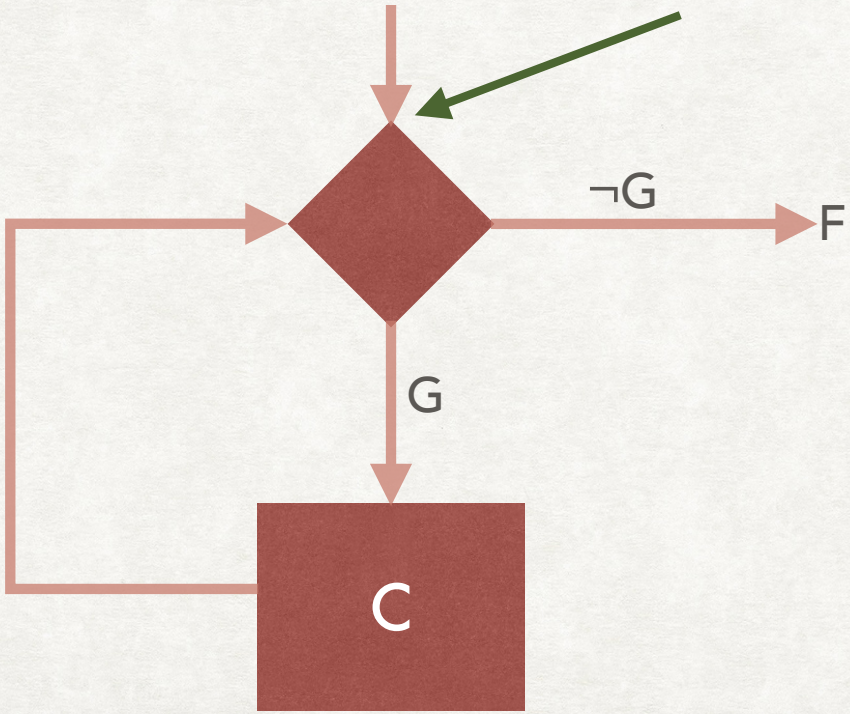
$\equiv (\mathsf{x} > 10 \rightarrow wp(\mathsf{y} = 0, \mathsf{y}:=\mathsf{z}+1)) \wedge (\neg(\mathsf{x} > 10) \rightarrow wp(\mathsf{y} = 0, \mathsf{y}:=\mathsf{z}-1))$

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

WEAKEST PRE-CONDITION

WHILE LOOPS

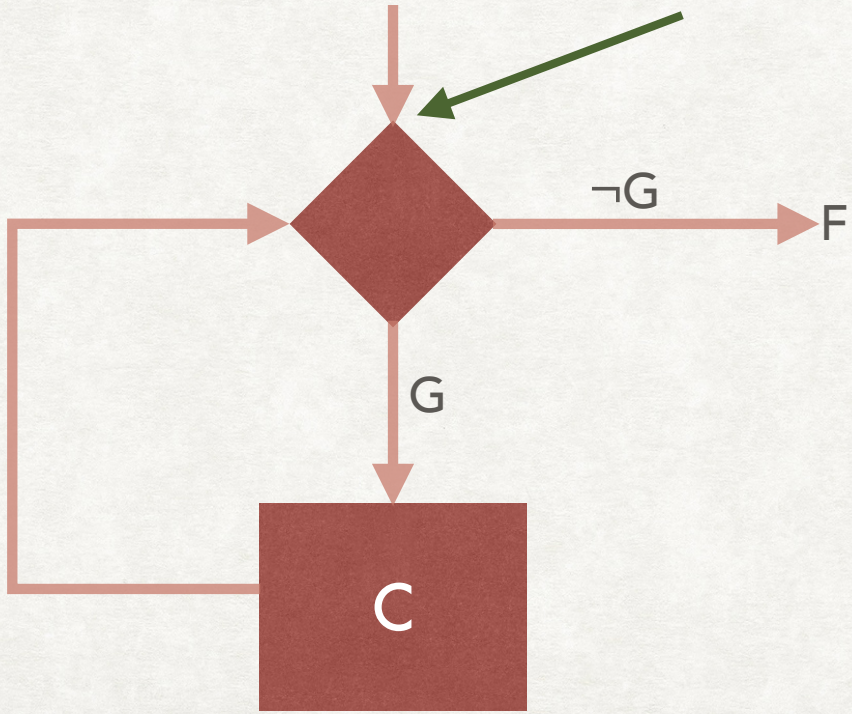
- wp(F, while(G) do c) ≡ ???
  - Collect all states at the beginning of loop, which would lead to a state in F if the loop exits after k iterations (for $k = 0,1,2,\ldots$)



WEAKEST PRE-CONDITION

WHILE LOOPS

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

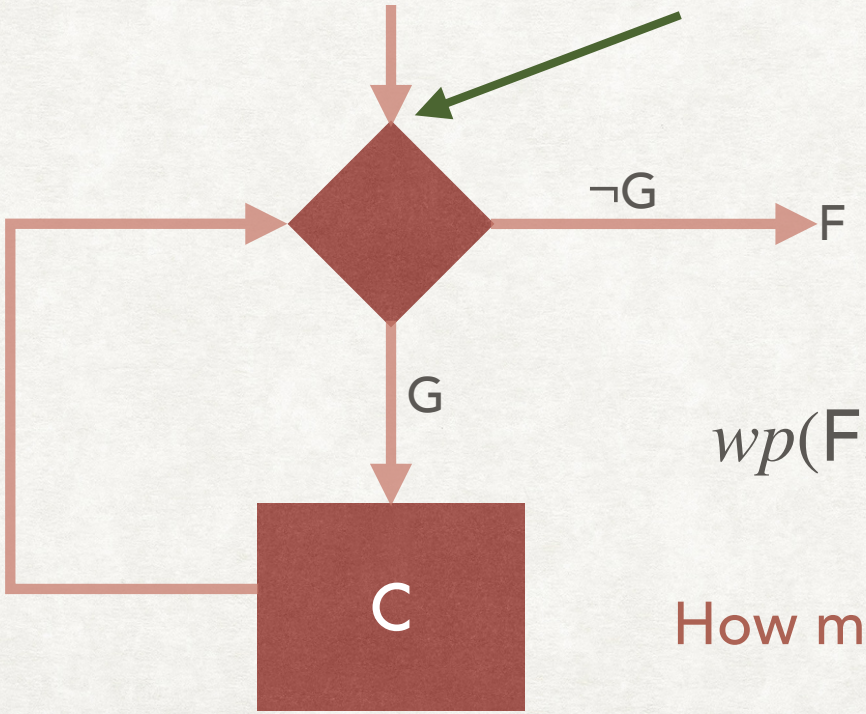


Iteration k	Initial State for exit after k iterations
0	$\neg G \wedge F$
1	$G \wedge wp(\neg G \wedge F, c)$
2	$G \wedge wp(G \wedge wp(\neg G \wedge F, c))$
…	…

WEAKEST PRE-CONDITION

WHILE LOOPS

- wp(F, while(G) do c) ≡ ???
  - 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 $F^k \rightarrow F^{k-1}$

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION AND VERIFICATION

- Given a program c with assertions, then c is safe if error $= 0 \rightarrow wp(\text{error} = 0, \text{c})$ is valid.
- The Hoare Triple $\{P\}\text{c}\{Q\}$ is valid if $P \rightarrow wp(Q, \text{c})$ 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.

ANNOUNCEMENTS

- Change in Assignment 2 schedule
  - ~~Out on Oct 19, Due Oct 28~~
  - Out on Oct 26, Due Nov 4
- Project Timeline
  - Proposal Due on Oct 18
  - Final Presentation (20 Minutes + 5 Minutes Q&A): First week of December.
  - Project Report Due December 6.
  - Friday slot will be used for project discussions.
- Final Exam (Tentative)
  - Take-home Exam
  - 3 Days in the week of December 7.

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 $sp(wp(P, \mathsf{c}), \mathsf{c}) \neq P$