

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 .

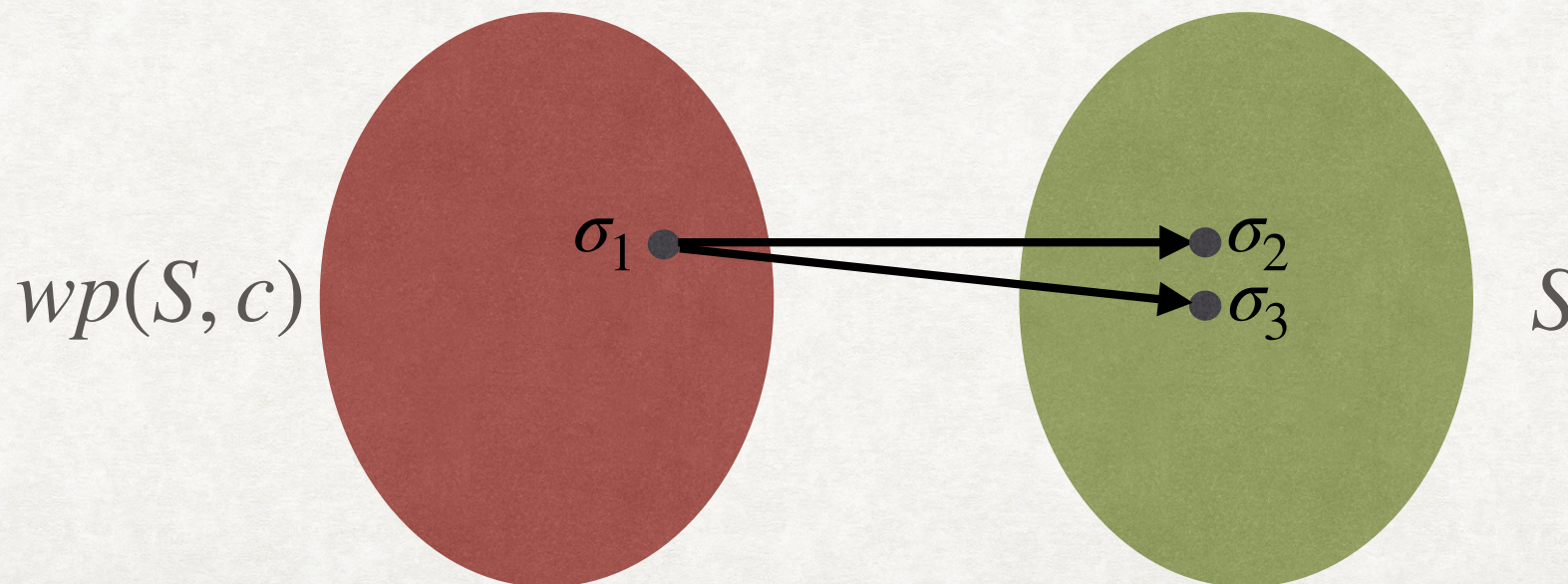
$$wp(S, c) \triangleq \{\sigma \mid \forall \sigma'. (\sigma, c) \hookrightarrow^* (\sigma', \text{skip}) \rightarrow \sigma' \in S\}$$

WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given 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 .

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

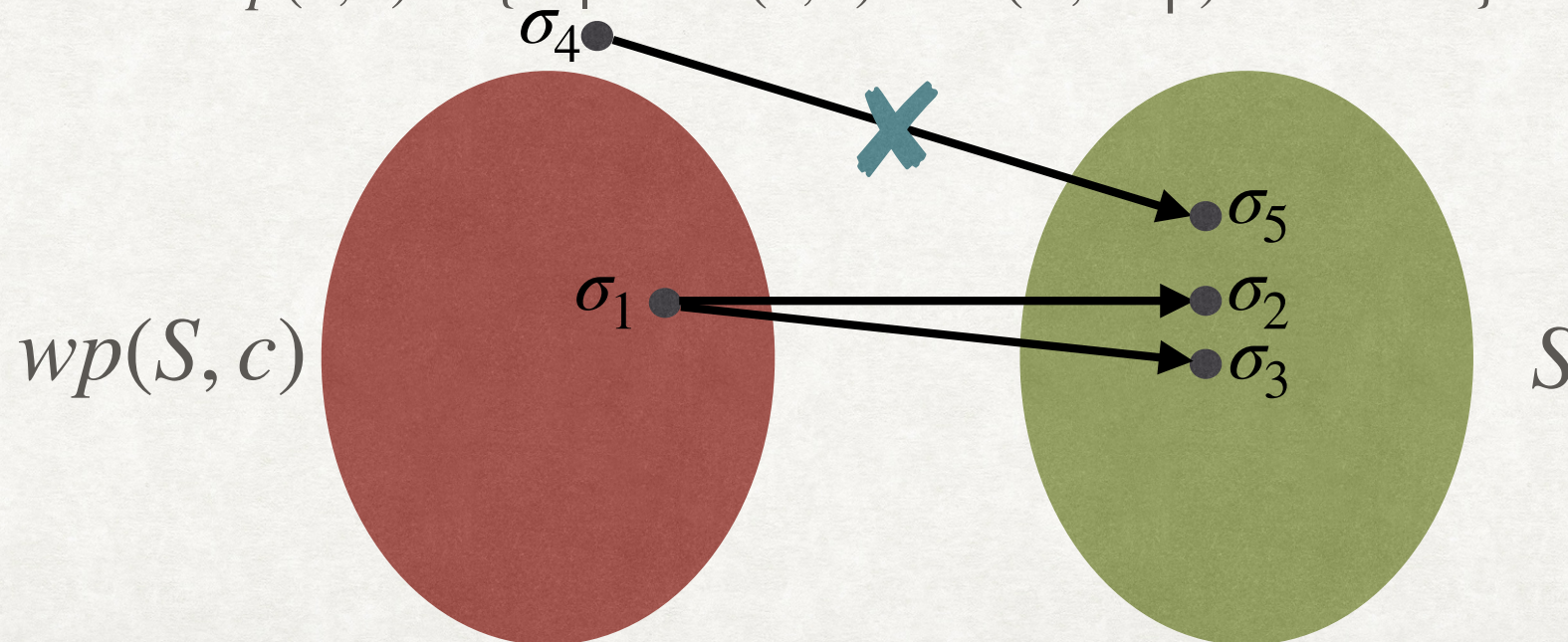


WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given 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 .

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

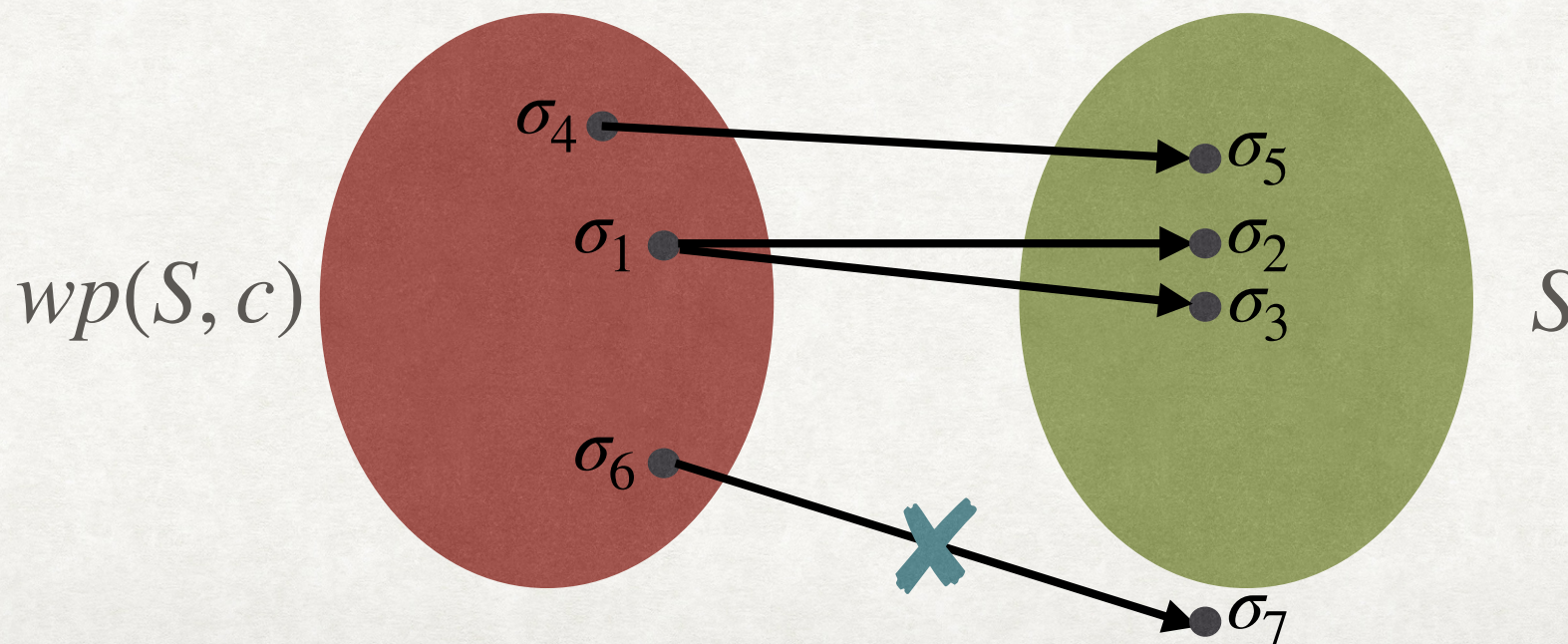


WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given 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 .

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

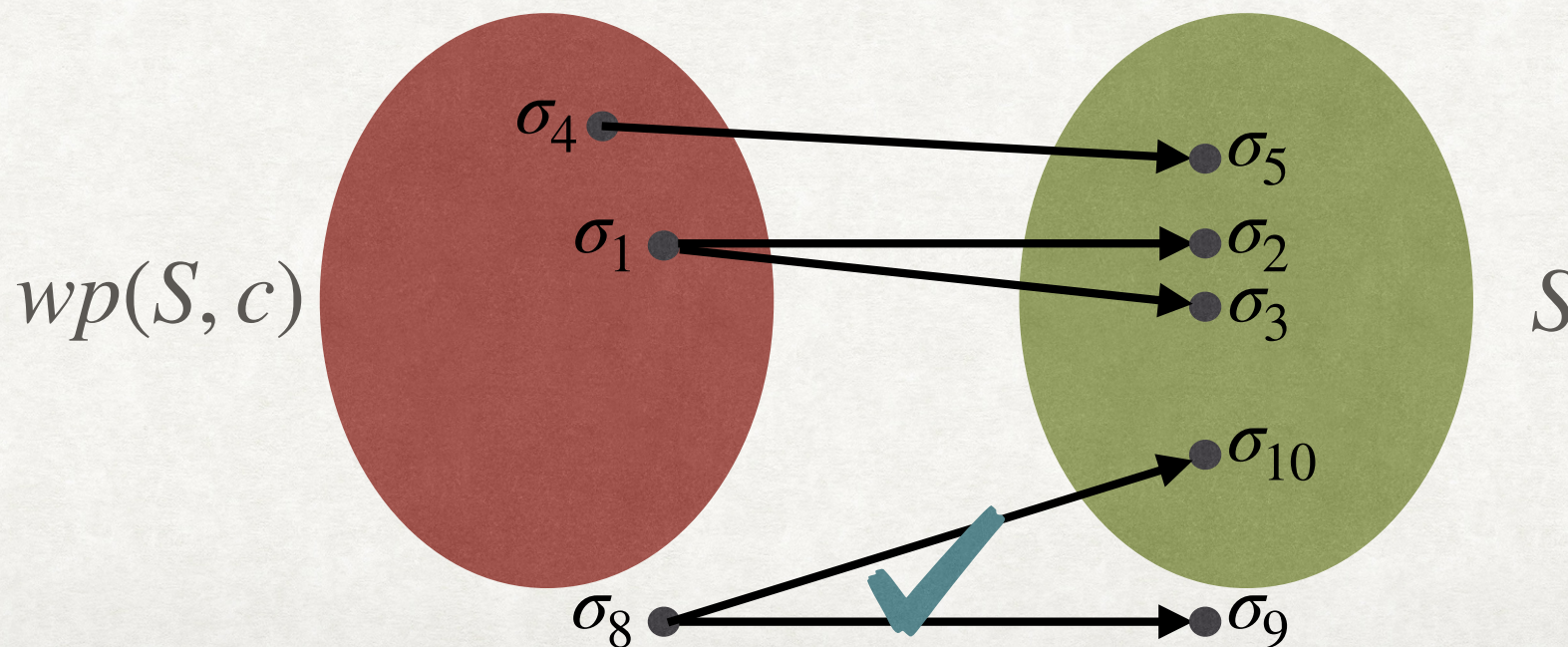


WEAKEST-PRECONDITION

SYMBOLIC EXECUTION IN THE BACKWARD DIRECTION

- Given 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 precondition operator $wp(S, c)$ consists of all states that would always lead to a state in S after executing c .

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

- We can use a FOL formula F to represent a set of states.
- The symbolic weakest precondition operator can be defined as:

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

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

$$wp(F, c) \triangleq \forall V'. \rho(c) \rightarrow F[V'/V]$$

WEAKEST PRE-CONDITION

EXAMPLES

$$\begin{aligned}wp(x > 10, x := x + 1) &\triangleq \forall x'. x' = x + 1 \rightarrow x' > 10 \\ &\equiv x + 1 > 10 \equiv x > 9\end{aligned}$$

WEAKEST PRE-CONDITION

EXAMPLES

$$\begin{aligned} wp(x > 10, x := x + 1) &\triangleq \forall x'. x' = x + 1 \rightarrow x' > 10 \\ &\equiv x + 1 > 10 \equiv x > 9 \end{aligned}$$

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

WEAKEST PRE-CONDITION

EXAMPLES

$$\begin{aligned} wp(x > 10, x := x + 1) &\triangleq \forall x'. x' = x + 1 \rightarrow x' > 10 \\ &\equiv x + 1 > 10 \equiv x > 9 \end{aligned}$$

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

WEAKEST PRE-CONDITION

EXAMPLES

$$\begin{aligned} wp(x > 10, x := x + 1) &\triangleq \forall x'. x' = x + 1 \rightarrow x' > 10 \\ &\equiv x + 1 > 10 \equiv x > 9 \end{aligned}$$

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

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

WEAKEST PRE-CONDITION

EXAMPLES

$$\begin{aligned} wp(x > 10, x := x + 1) &\triangleq \forall x'. x' = x + 1 \rightarrow x' > 10 \\ &\equiv x + 1 > 10 \equiv x > 9 \end{aligned}$$

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

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

WEAKEST PRE-CONDITION

EXAMPLES

$$\begin{aligned} wp(x > 10, x := x + 1) &\triangleq \forall x'. x' = x + 1 \rightarrow x' > 10 \\ &\equiv x + 1 > 10 \equiv x > 9 \end{aligned}$$

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

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

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

WEAKEST PRE-CONDITION

EXAMPLES

$$\begin{aligned} wp(x > 10, x := x + 1) &\triangleq \forall x'. x' = x + 1 \rightarrow x' > 10 \\ &\equiv x + 1 > 10 \equiv x > 9 \end{aligned}$$

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

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

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

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

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

ASSIGNMENT STATEMENT

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

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

EXAMPLES:

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME

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

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME

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

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

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

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

WEAKEST PRE-CONDITION

HAVOC, ASSUME - EXAMPLES

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

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 $F \neq \text{true}$.
 - 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

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

WEAKEST PRE-CONDITION

ASSERT

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

WEAKEST PRE-CONDITION

ASSERT-EXAMPLES

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

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

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

WEAKEST PRE-CONDITION

IF-THEN-ELSE

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

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

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

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

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

Consider σ' such that $(\sigma, c_1) \hookrightarrow^* (\sigma', \text{skip})$. 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, $(\sigma, \text{if}(G) \text{ then } c_1 \text{ else } c_2) \hookrightarrow (\sigma, c_2)$.

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

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

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:

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

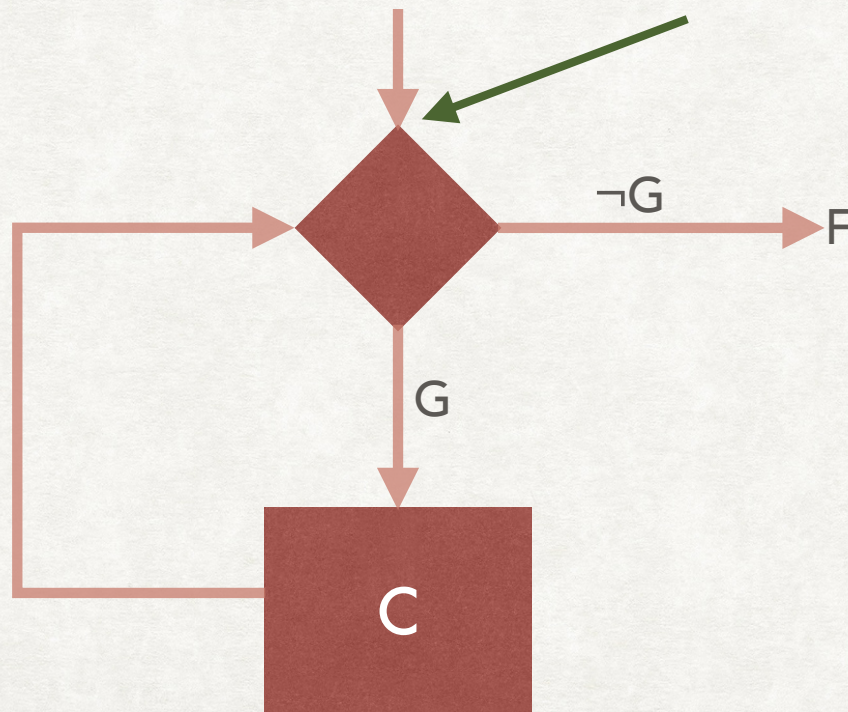
$$\equiv (x > 10 \rightarrow wp(y = 0, y := z + 1)) \wedge (\neg(x > 10) \rightarrow wp(y = 0, y := z - 1))$$

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

WEAKEST PRE-CONDITION

WHILE LOOPS

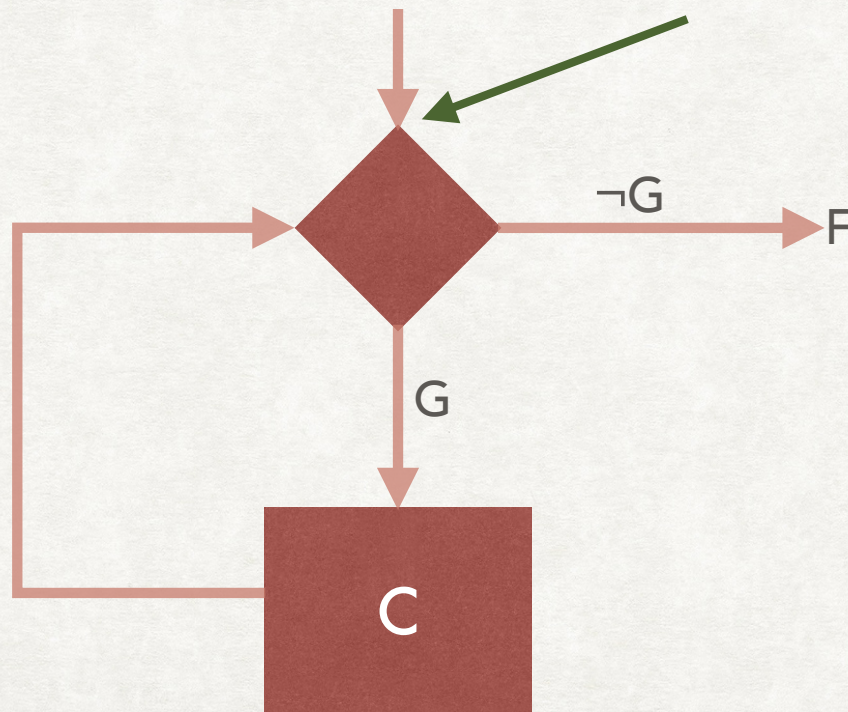
- $wp(F, \text{while}(G) \text{ do } c) \equiv ???$
- Collect all states at the beginning of loop, which would lead to a state in F if the loop exits after k iterations (for $k = 0, 1, 2, \dots$)



WEAKEST PRE-CONDITION

WHILE LOOPS

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

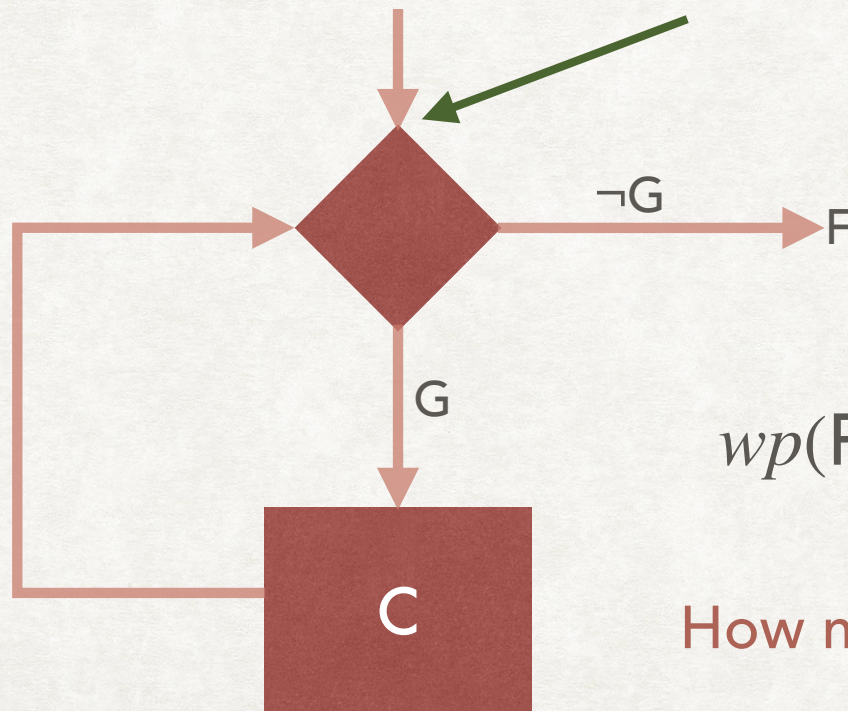


Iteration k	Initial State for exit after k iterations
0	$\neg G \wedge F$
1	$G \wedge wp(\neg G \wedge F, c)$
2	$G \wedge wp(G \wedge wp(\neg G \wedge F, c))$
...	...

WEAKEST PRE-CONDITION

WHILE LOOPS

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



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

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

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

How many F^k should be calculated?

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION

WHILE LOOPS - EXAMPLES

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

WEAKEST PRE-CONDITION AND VERIFICATION

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