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.

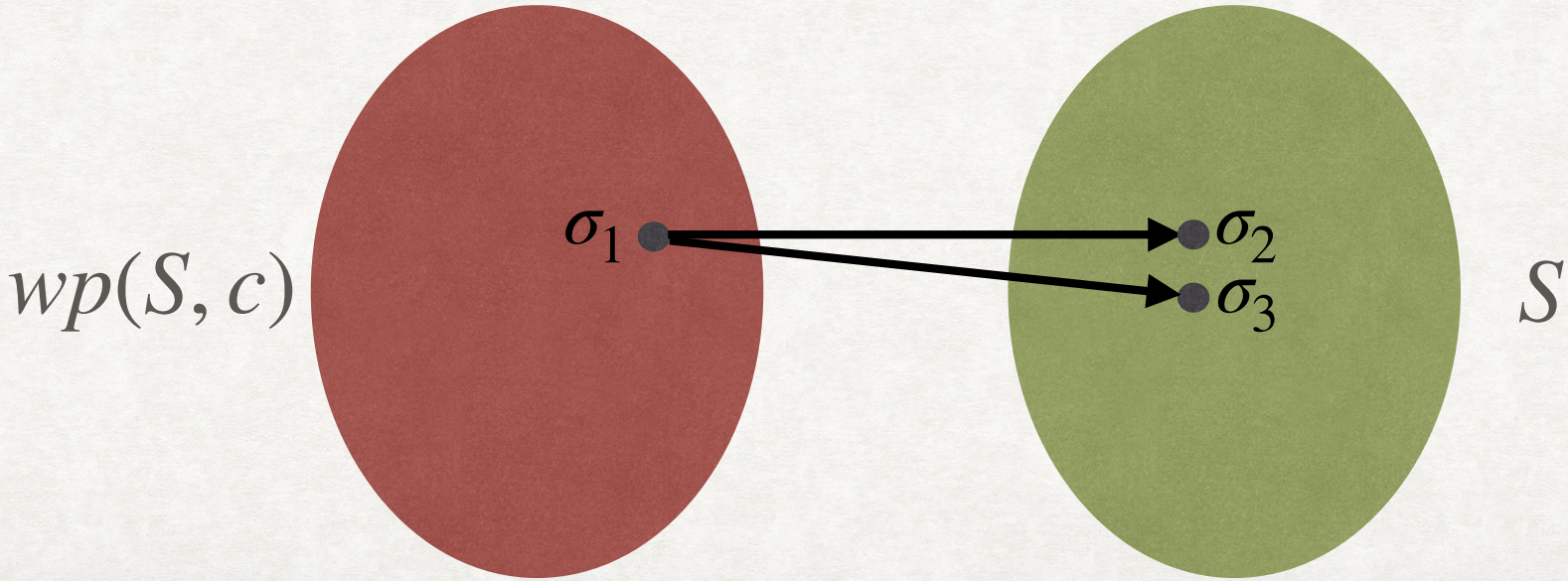
$$wp(S, c) \triangleq \{\sigma \mid \forall \sigma' \,.\, (\sigma, c) \hookrightarrow^* (\sigma', \mathsf{skip}) \rightarrow \sigma' \in S\}$$

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.

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

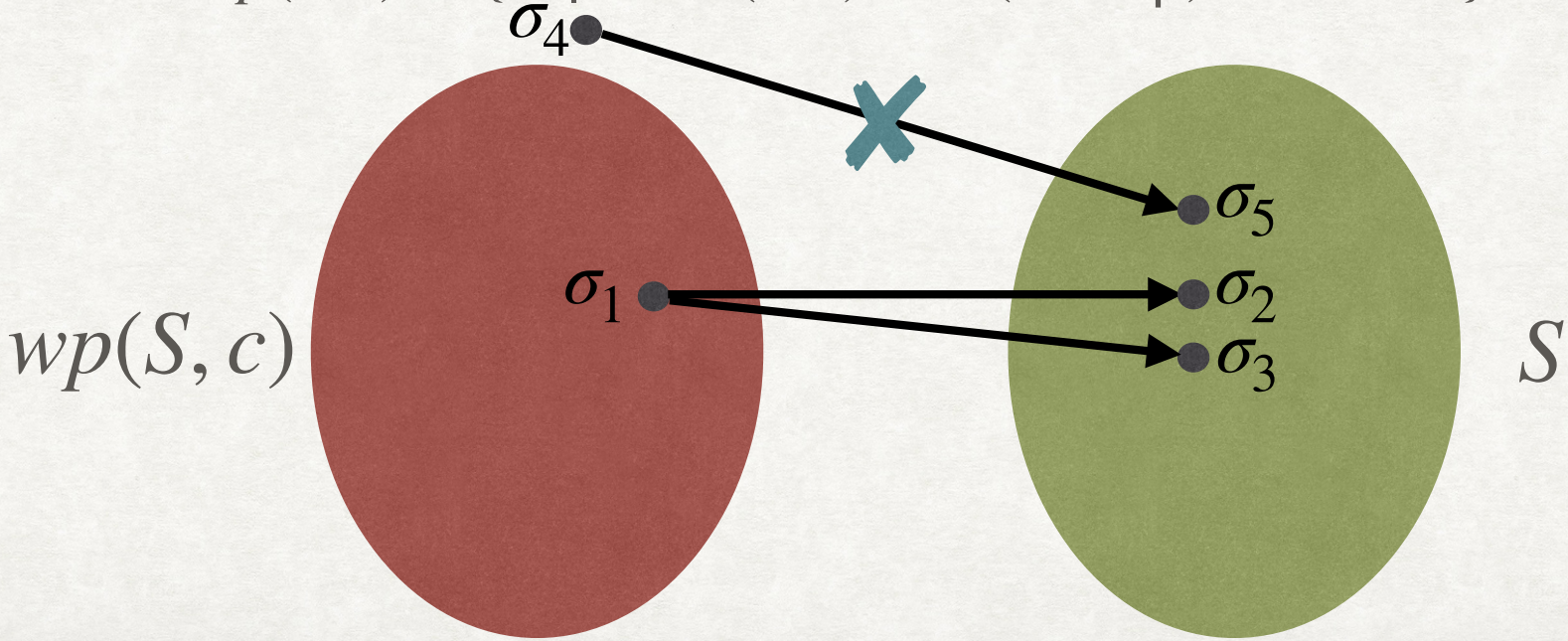


WEAKEST-PRECONDITION

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.

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

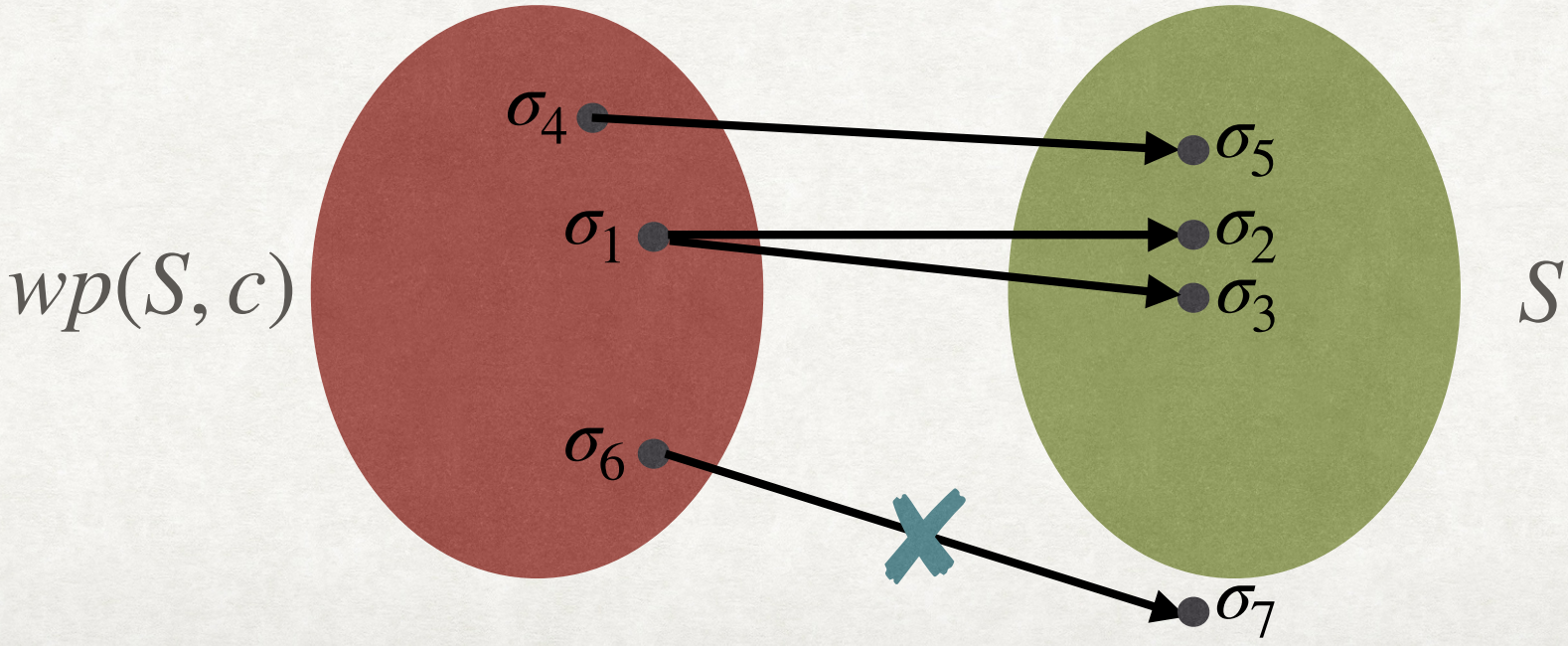


WEAKEST-PRECONDITION

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.

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

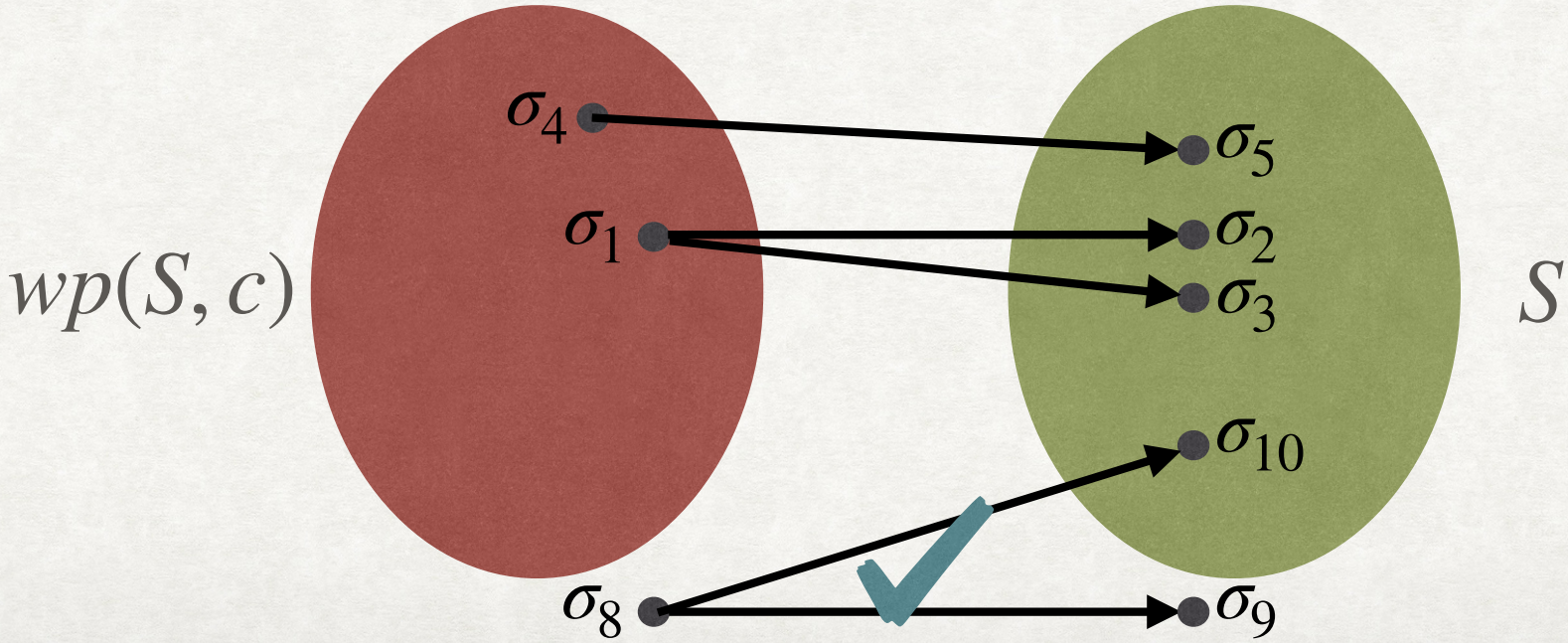


WEAKEST-PRECONDITION

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

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

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