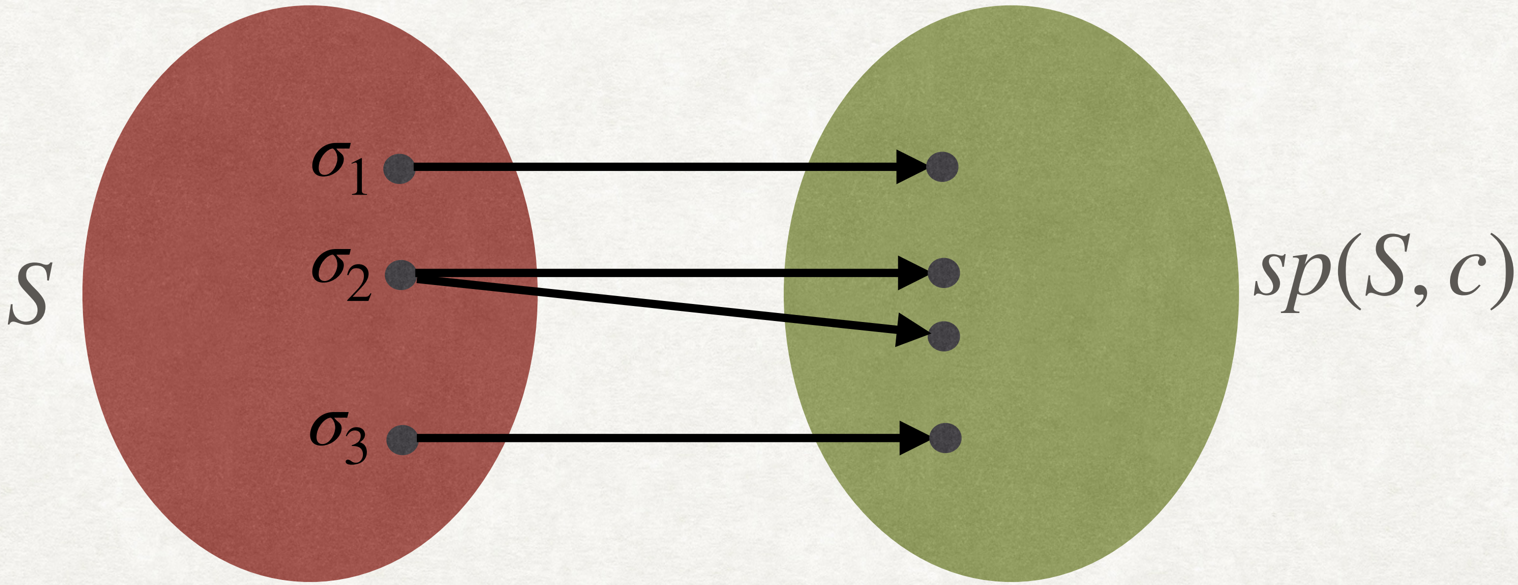
STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

- Given a set of states S and a command c, the strongest post-condition operator $sp(S, c)$ consists of all states that can be obtained after executing c on any state in S.

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

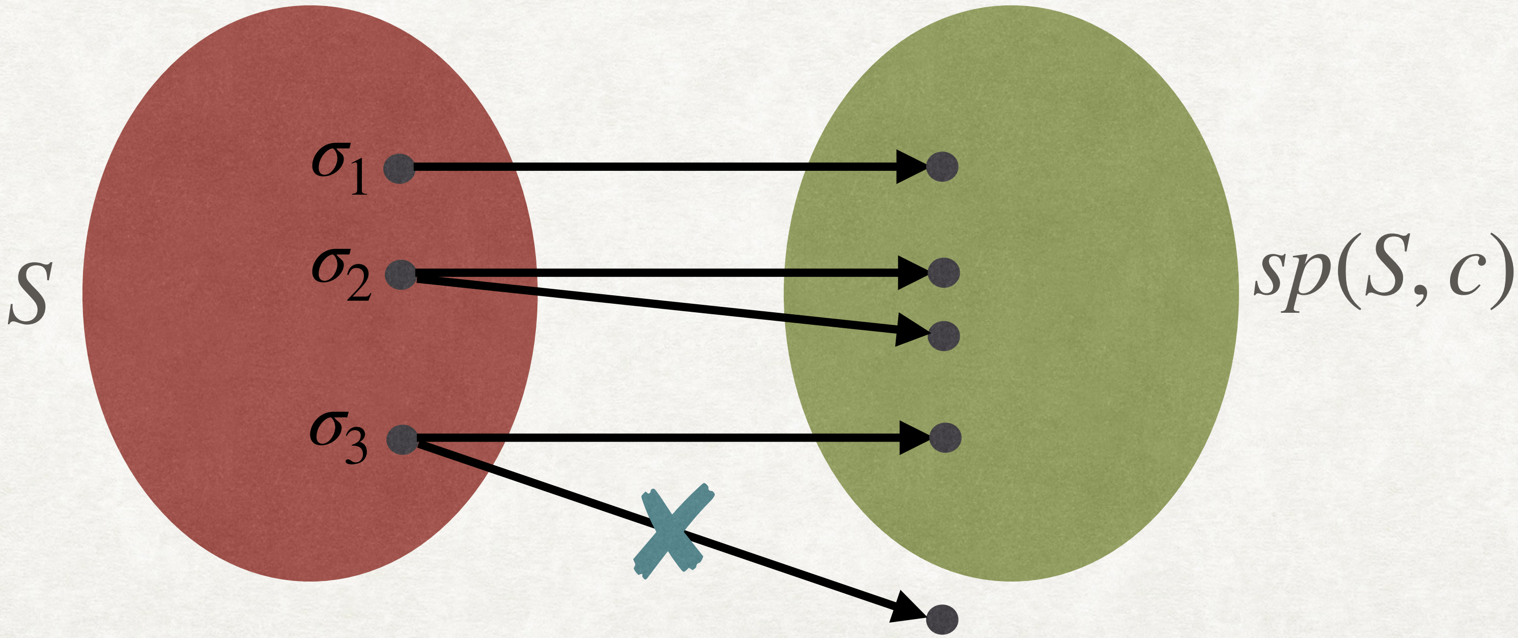


STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

- Given a set of states S and a command c, the strongest post-condition operator $sp(S, c)$ consists of all states that can be obtained after executing c on any state in S.

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

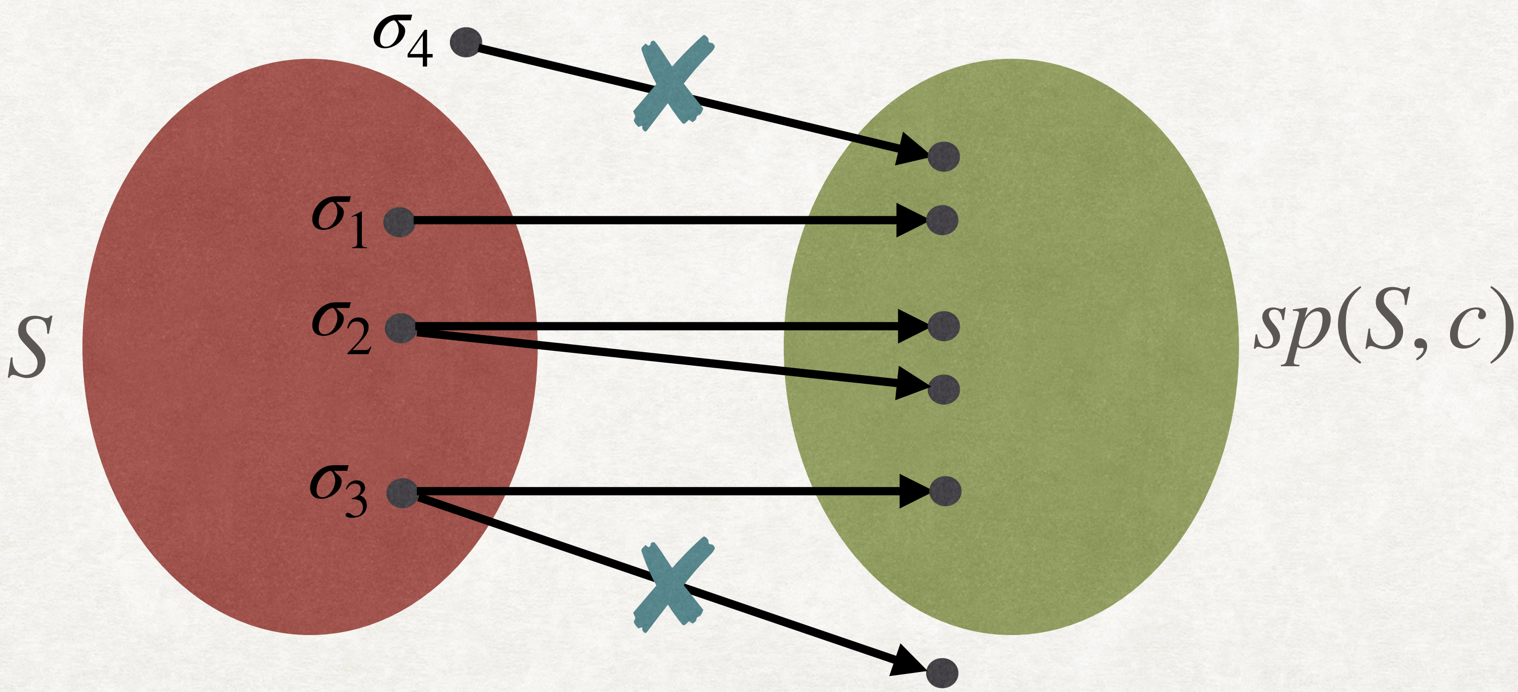


STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

- Given a set of states S and a command c, the strongest post-condition operator $sp(S, c)$ consists of all states that can be obtained after executing c on any state in S.

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

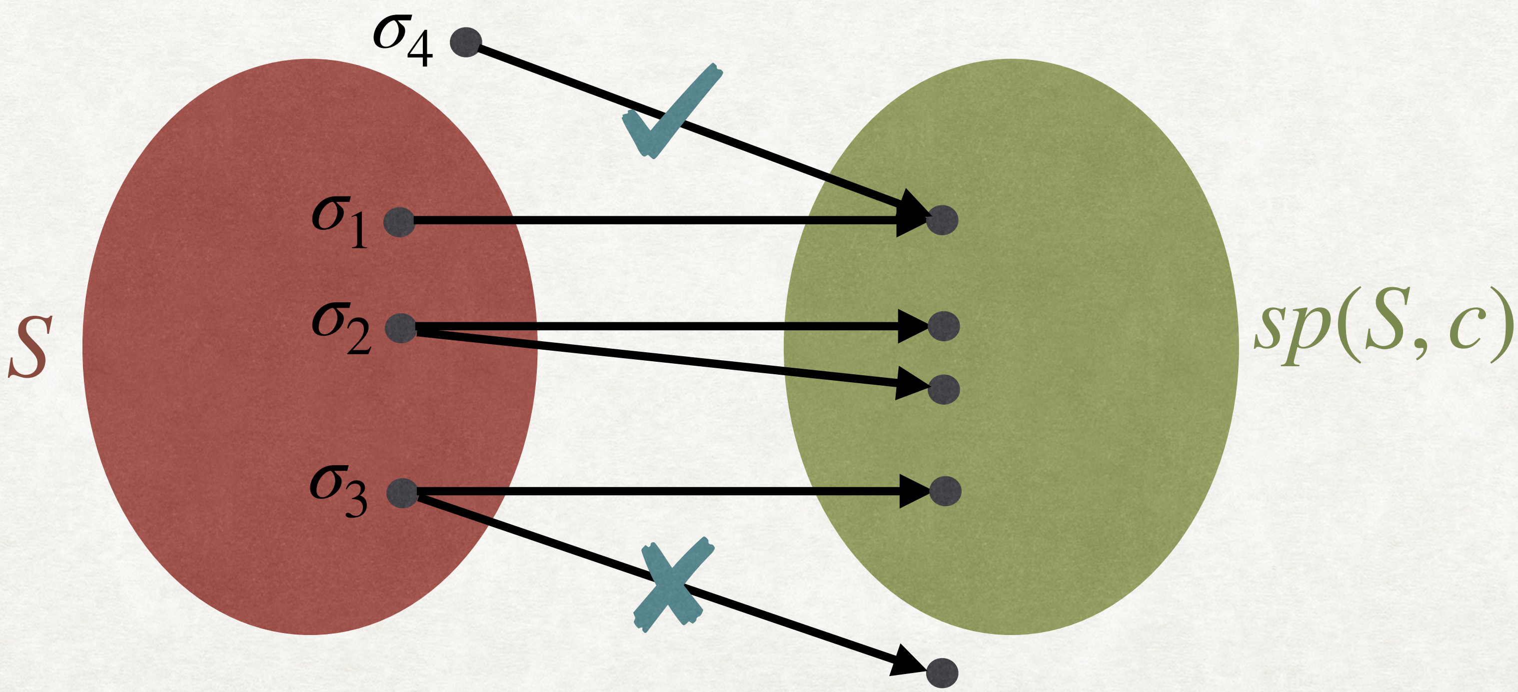


STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

- Given a set of states S and a command c, the strongest post-condition operator $sp(S, c)$ consists of all states that can be obtained after executing c on any state in S.

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



STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

- Given a set of states S and a command c, the strongest post-condition operator $sp(S, c)$ consists of all states that can be obtained after executing c on any state in S.

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

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

$$\sigma' \vDash sp(F, \mathsf{c}) \Leftrightarrow \exists \sigma \,.\, \sigma \vDash F \wedge (\sigma, \mathsf{c}) \hookrightarrow^* (\sigma', \mathsf{skip})$$

- We can now use the semantics in FOL (ρ) to define symbolic sp:

$$sp(F, \mathsf{c}) \triangleq (\exists V \,.\, F \wedge \rho(\mathsf{c}))[V/V']$$

FIRST ELIMINATE EXISTENTIAL QUANTIFICATION ON V, THEN SUBSTITUTE V FOR V′

QUANTIFIER ELIMINATION

- Eliminate quantifiers in a formula F to obtain an equivalent formula G (equivalent modulo $T_{\mathbb{Q}}$).
  - A decidable procedure exists for $T_{\mathbb{Q}}-$formulae.
  - Ferrante and Rackoff's Method (BM Chapter 7)
- Consider the formula: $\exists y \,.\, x = y + 1.$
  - Equivalent formula after eliminating y: $true$
- Consider the formula: $\exists y \,.\, y > 1 \wedge x = 2y$
  - Equivalent formula after eliminating y: $x > 2$
- What about $\exists y \,.\, x = 2y \wedge x > y$?
  - Equivalent formula: $x > 0$

STRONGEST POST-CONDITION

EXAMPLE

$$sp(F, \mathsf{c}) \triangleq (\exists V \,.\, F \land \rho(\mathsf{c}))[V/V']$$

Lets calculate $sp(\mathsf{y} > 0, \mathsf{x{:=}y{+}1})$

STRONGEST POST-CONDITION

EXAMPLE

$$sp(F, \mathsf{c}) \triangleq (\exists V \,.\, F \wedge \rho(\mathsf{c}))[V/V']$$

Lets calculate $sp(\mathsf{y} > 0, \mathsf{x{:=}y{+}1})$

$$\begin{aligned} sp(\mathsf{y} > 0, \mathsf{x{:=}y{+}1}) &\triangleq \exists \mathsf{x} \,.\, \exists \mathsf{y} \,.\, \mathsf{y} > 0 \wedge \rho(\mathsf{x{:=}y{+}1}) \\ &\equiv \exists \mathsf{x} \,.\, \exists \mathsf{y} \,.\, \mathsf{y} > 0 \wedge \mathsf{x}' = \mathsf{y} + 1 \wedge \mathsf{y}' = \mathsf{y} \\ &\equiv \mathsf{y}' > 0 \wedge \mathsf{x}' = \mathsf{y}' + 1 \longleftarrow \\ &\equiv \mathsf{y} > 0 \wedge \mathsf{x} = \mathsf{y} + 1 \longleftarrow \end{aligned}$$

Eliminate x and y

Substitute x’ and y’ with x and y

STRONGEST POST-CONDITION

MORE EXAMPLES

$sp(\mathsf{y} > 0, \mathsf{x{:=}havoc}) \triangleq\ ???$

STRONGEST POST-CONDITION

MORE EXAMPLES

$sp(\mathsf{y} > 0, \mathsf{x}{:=}\mathsf{havoc}) \triangleq \exists \mathsf{x} \,.\, \exists \mathsf{y} \,.\, \mathsf{y} > 0 \wedge \mathsf{y}' = \mathsf{y}$ $[\rho(\mathsf{x}{:=}\mathsf{havoc}) \triangleq \mathit{frame}(\mathsf{x})]$

$\triangleq \mathsf{y} > 0$