STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

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

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

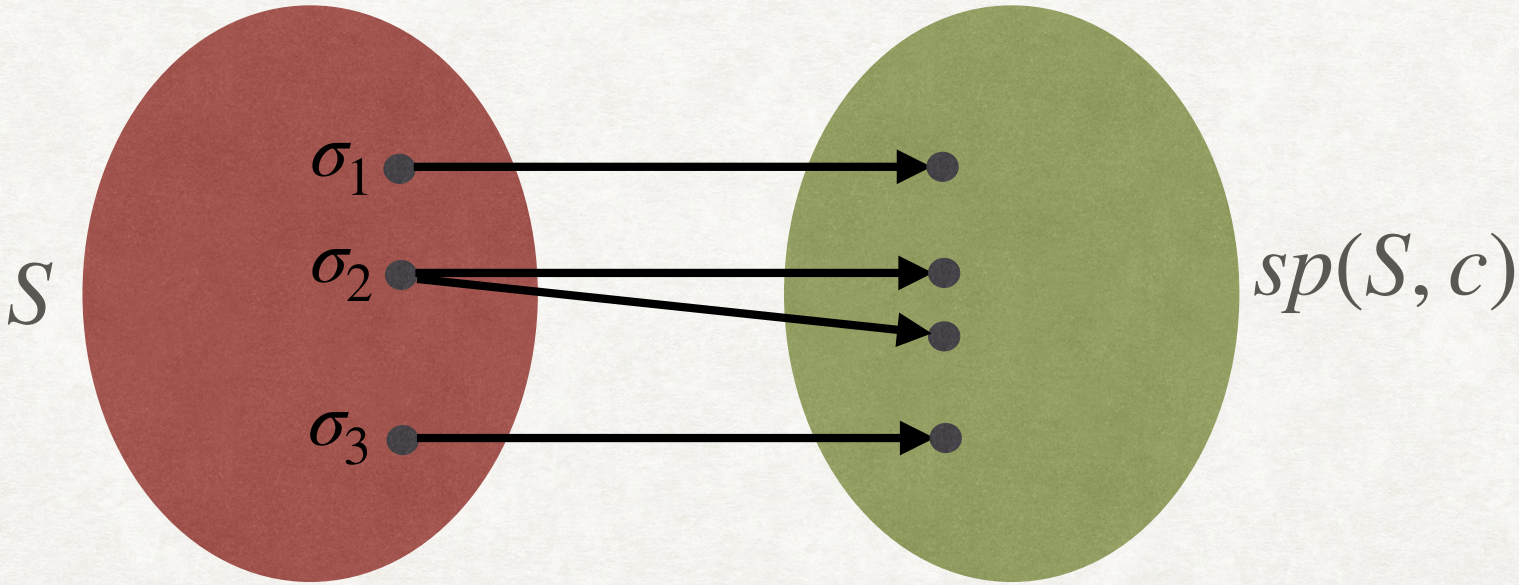
Equivalently, $\sigma' \in sp(S, c) \leftrightarrow \exists \sigma \in S \,.\, (\sigma, c) \hookrightarrow^* (\sigma', skip)$

STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

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

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

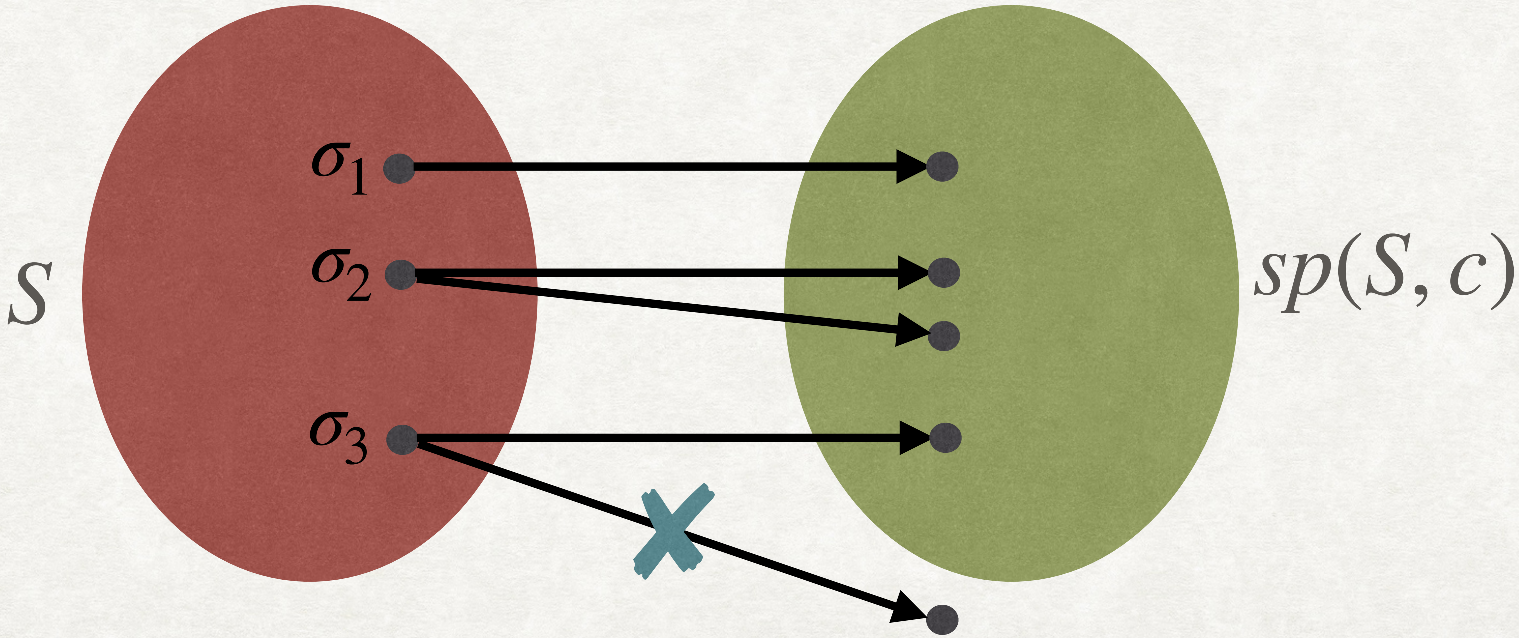


STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

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

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

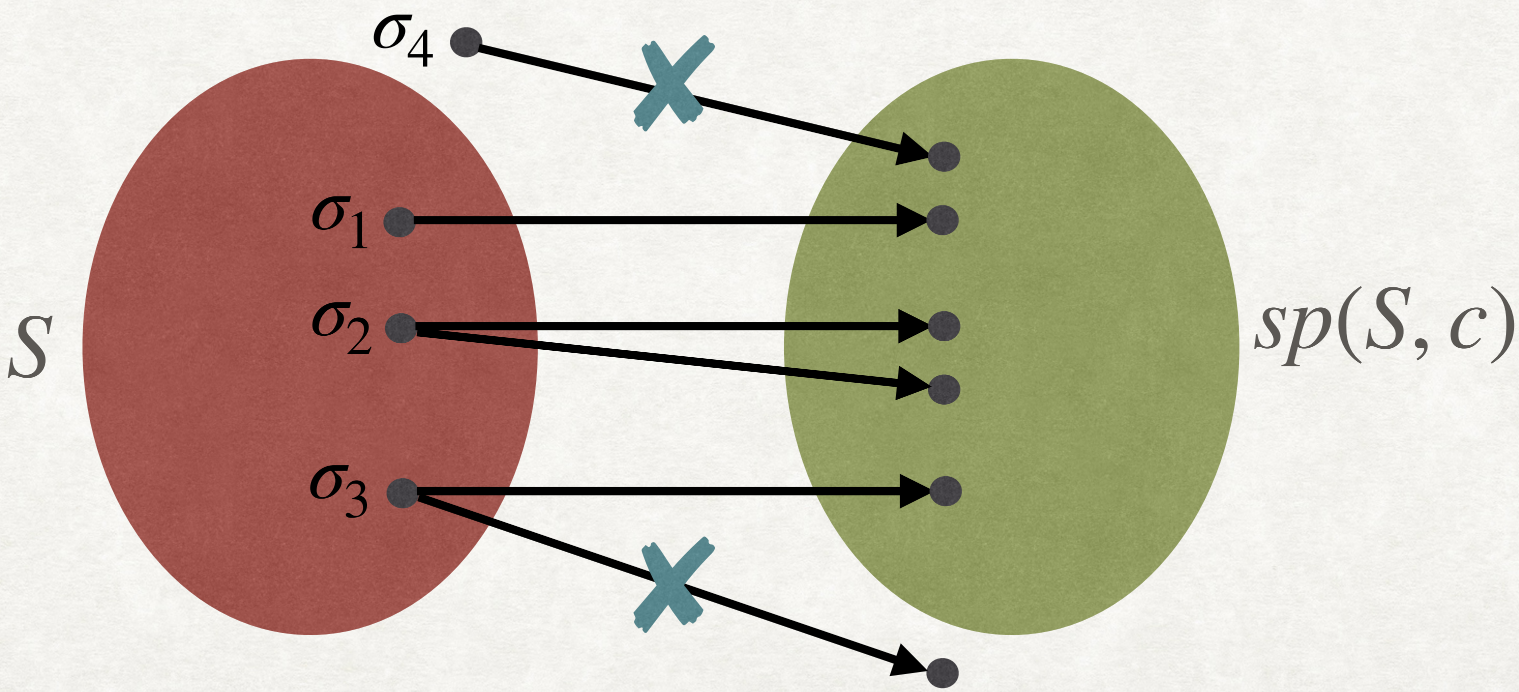


STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

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

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

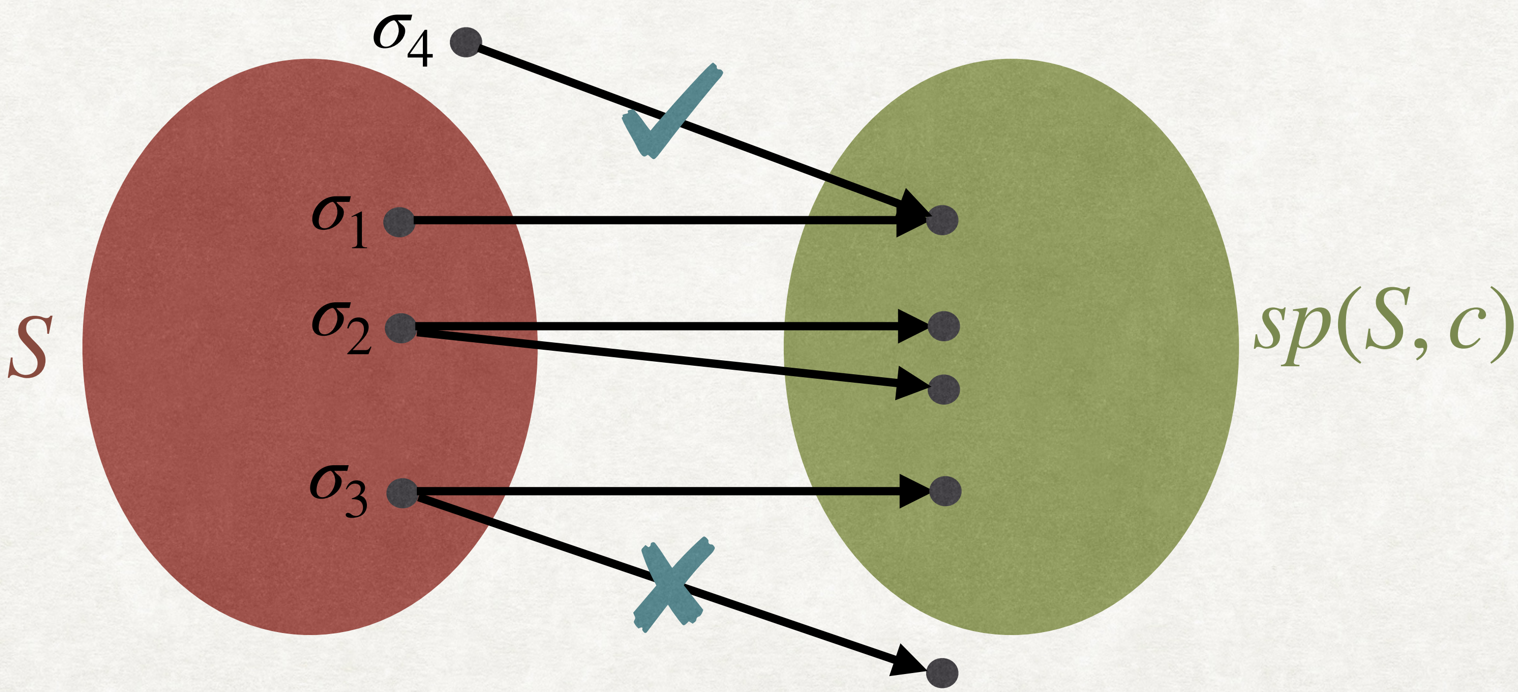


STRONGEST POST-CONDITION

SYMBOLIC EXECUTION IN THE FORWARD DIRECTION

- Given a set of states S and a command c, the strongest post-condition $sp(S, c)$ 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 $sp(S, c)$ 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: $\top$
- Consider the formula: $\exists y \,.\, y > 1 \land x = 2y$
  - Equivalent formula after eliminating y: $x > 2$
- What about $\exists y \,.\, x = 2y \land x > y$?
  - Equivalent formula: $x > 0$

STRONGEST POST-CONDITION

EXAMPLE

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

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

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

ANNOUNCEMENT

- Assignments : Late Submission Policy
  - 1 Day late : 25% Penalty
  - 2 Days late : 50% Penalty
  - Submissions after 2 days will be ignored.

STRONGEST POST-CONDITION

EXAMPLE

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

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

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

Alternative Formulation for Assignment Statement:

$$sp(F, \mathsf{x{:}{=}e}) \equiv \exists x' \,.\, F[x'/x] \wedge x = e[x'/x]$$

STRONGEST POST-CONDITION

MORE EXAMPLES

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

STRONGEST POST-CONDITION

MORE EXAMPLES

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

$$\triangleq \mathrm{y} > 0$$

STRONGEST POST-CONDITION

MORE EXAMPLES

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

$\triangleq \mathsf{y} > 0$

$sp(F, \mathsf{x{:=}havoc}) \triangleq \exists \mathsf{x}\,.\,F$

STRONGEST POST-CONDITION

MORE EXAMPLES

$sp(\mathsf{y} > 0, \mathsf{x:=havoc}) \triangleq \exists \mathsf{x} \,.\, \exists \mathsf{y} \,.\; \mathsf{y} > 0 \wedge \mathsf{y'} = \mathsf{y}$

$\triangleq \mathsf{y} > 0$

$sp(\mathsf{F}, \mathsf{assume(G)}) \triangleq\ ???$

STRONGEST POST-CONDITION

MORE EXAMPLES

$$sp(\mathrm{y} > 0, \mathrm{x}{:=}\mathrm{havoc}) \triangleq \exists \mathrm{x}\,.\,\exists \mathrm{y}\,.\; \mathrm{y} > 0 \land \mathrm{y}' = \mathrm{y}$$

$$\triangleq \mathrm{y} > 0$$

$$sp(\mathrm{F}, \mathrm{assume}(\mathrm{G})) \triangleq \mathrm{F} \land \mathrm{G}$$

STRONGEST POST-CONDITION

MORE EXAMPLES

$sp(\text{y} > 0, \text{x:=havoc}) \triangleq \exists \text{x} \,.\, \exists \text{y} \,.\; \text{y} > 0 \land \text{y}' = \text{y}$

$\triangleq \text{y} > 0$

$sp(\text{F}, \text{assume(G)}) \triangleq \text{F} \land \text{G}$

$sp(\text{F}, \text{assert(G)}) \triangleq\ ???$

STRONGEST POST-CONDITION

MORE EXAMPLES

$$sp(y > 0, x:=\text{havoc}) \triangleq \exists x\,.\,\exists y\,.\; y > 0 \wedge y' = y$$
$$\triangleq y > 0$$

$$sp(F, \text{assume}(G)) \triangleq F \wedge G$$

$$\begin{aligned} sp(F, \text{assert}(G)) &\triangleq \exists V\,.\,F \wedge (G \to frame(\varnothing)) \\ &\equiv \exists V\,.\,F \wedge (\neg G \vee frame(\varnothing)) \\ &\equiv \exists V\,.\,(F \wedge \neg G) \vee \exists V\,.\,(F \wedge frame(\varnothing)) \\ &\equiv \exists V\,.\,(F \wedge \neg G) \vee F[V'/V] \\ &\equiv (\exists V\,.\,F \wedge \neg G) \vee F \end{aligned}$$

STRONGEST POST-CONDITION

MORE EXAMPLES

$sp(\mathsf{y} > 0, \mathsf{x}{:=}\mathsf{havoc}) \triangleq \exists \mathsf{x}\,.\, \exists \mathsf{y}\,.\; \mathsf{y} > 0 \wedge \mathsf{y}' = \mathsf{y}$

$\triangleq \mathsf{y} > 0$

$sp(\mathsf{F}, \mathsf{assume}(\mathsf{G})) \triangleq \mathsf{F} \wedge \mathsf{G}$

$sp(\mathsf{F}, \mathsf{assert}(\mathsf{G})) \triangleq (\exists V\,.\, \mathsf{F} \wedge \neg \mathsf{G}) \vee \mathsf{F}$

STRONGEST POST-CONDITION

MORE EXAMPLES

$$sp(\mathsf{y} > 0, \mathsf{x{:=}havoc}) \triangleq \exists \mathsf{x}\,.\,\exists \mathsf{y}\,.\ \mathsf{y} > 0 \land \mathsf{y'} = \mathsf{y}$$

$$\triangleq \mathsf{y} > 0$$

$$sp(\mathsf{F}, \mathsf{assume(G)}) \triangleq \mathsf{F} \land \mathsf{G}$$

$$sp(\mathsf{F}, \mathsf{assert(G)}) \triangleq (\exists V\,.\,\mathsf{F} \land \neg \mathsf{G}) \lor \mathsf{F}$$

$$sp(\mathit{false}, \mathsf{c}) \triangleq ???$$

STRONGEST POST-CONDITION

EXAMPLES

$$sp(\mathsf{y} > 0, \mathsf{x} := \mathsf{havoc}) \triangleq \exists \mathsf{x} \,.\, \exists \mathsf{y} \,.\; \mathsf{y} > 0 \wedge \mathsf{y}' = \mathsf{y}$$

$$\triangleq \mathsf{y} > 0$$

$$sp(\mathsf{F}, \mathsf{assume}(\mathsf{G})) \triangleq \mathsf{F} \wedge \mathsf{G}$$

$$sp(\mathsf{F}, \mathsf{assert}(\mathsf{G})) \triangleq (\exists V \,.\, \mathsf{F} \wedge \neg \mathsf{G}) \vee \mathsf{F}$$

$$sp(\mathit{false}, \mathsf{c}) \triangleq \mathit{false}$$

EXAMPLES

- $sp(\text{x} > 5, \text{assume(x < 20)}) \equiv ???$
- $sp(\text{x} > 5, \text{assert(x < 0)}) \equiv ???$
- $sp(\text{x} > 0, \text{x:=x+1}) \equiv ???$

EXAMPLES

- $sp(\mathsf{x} > 5, \mathsf{assume}(\mathsf{x} < 20)) \equiv \mathsf{x} > 5 \wedge \mathsf{x} < 20$
- $sp(\mathsf{x} > 5, \mathsf{assert}(\mathsf{x} < 0)) \equiv true$
- $sp(\mathsf{x} > 0, \mathsf{x{:=}x{+}1}) \equiv \mathsf{x} > 1$

STRONGEST POST-CONDITION

COMPOUND STATEMENTS

- $sp(\mathsf{F}, \mathsf{c;c'}) \triangleq ???$

STRONGEST POST-CONDITION

COMPOUND STATEMENTS

- sp(F, c;c') ≜ sp(sp(F, c), c') (Homework: Prove this formally.)

STRONGEST POST-CONDITION

COMPOUND STATEMENTS

- $sp(\text{F}, \text{c;c'}) \triangleq sp(sp(\text{F}, \text{c}), \text{c'})$

- $sp(\text{F}, \text{if(G) then c else c'}) \triangleq ???$

STRONGEST POST-CONDITION

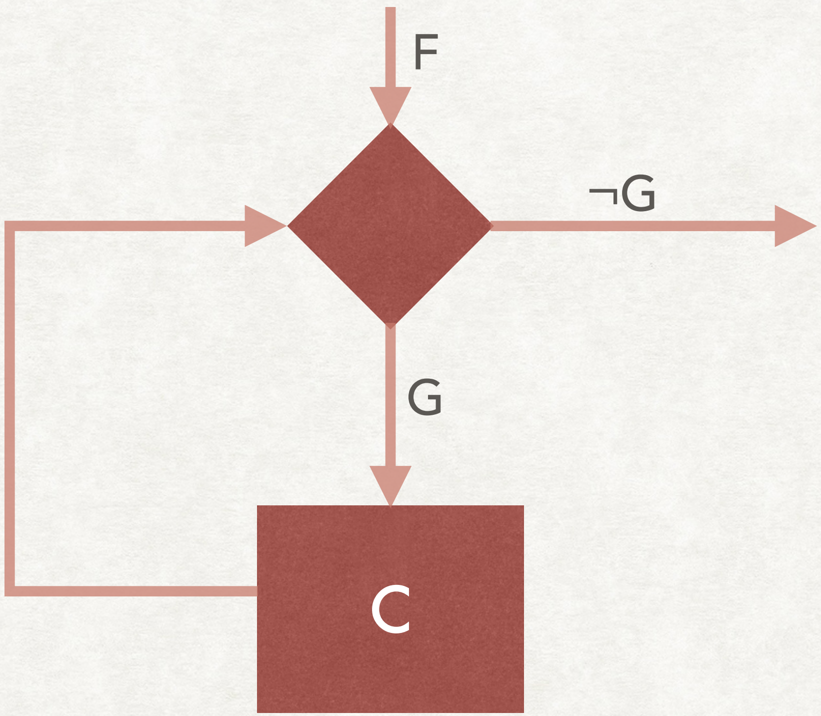
COMPOUND STATEMENTS

- sp(F, c;c') $\triangleq$ sp(sp(F, c), c')
- sp(F, if(G) then c else c') $\triangleq$ sp(F $\wedge$ G, c) $\vee$ sp(F $\wedge$ $\neg$G, c') (Homework: Prove this formally.)

STRONGEST POST-CONDITION

WHILE LOOPS

- How to find $sp(F, \text{while}(G) \text{ do c})$?

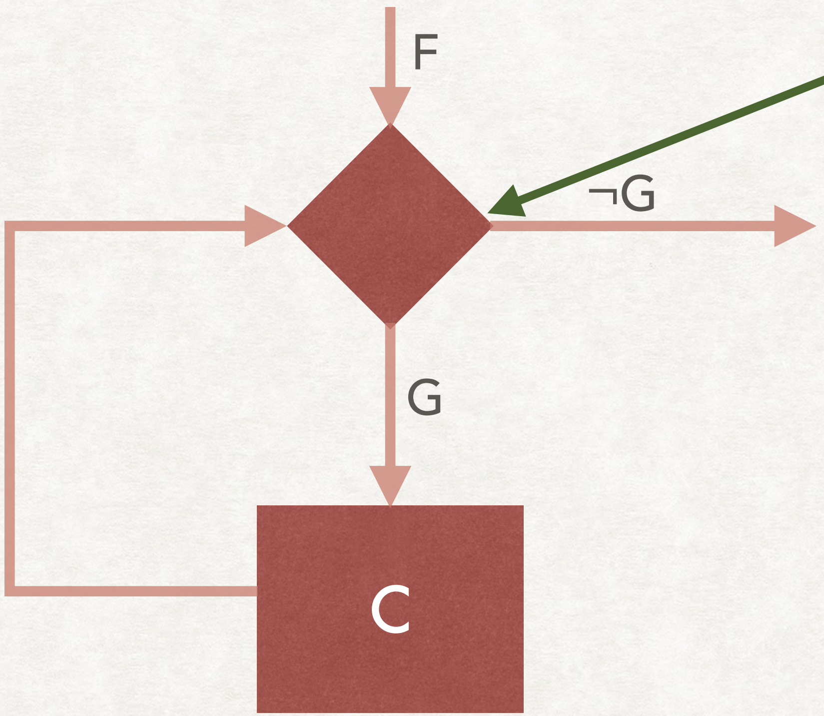


STRONGEST POST-CONDITION

WHILE LOOPS

- How to find sp(F, while(G) do c)?

Let us collect all states possible at the end of any iteration



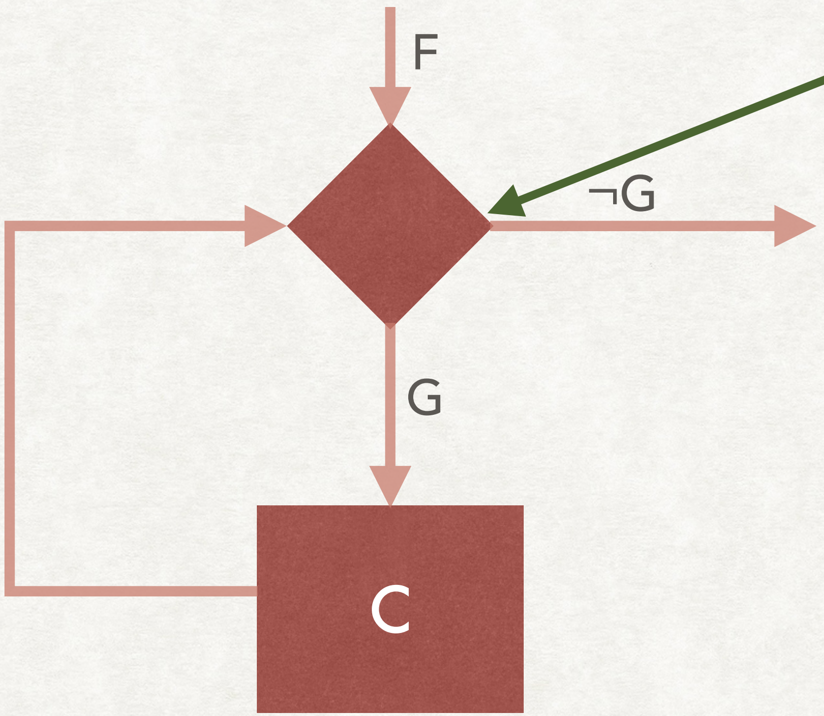
Iteration i	States possible at iteration i
0	
1	
2	
…	…

STRONGEST POST-CONDITION

WHILE LOOPS

- How to find sp(F, while(G) do c)?

Let us collect all states possible at the end of any iteration

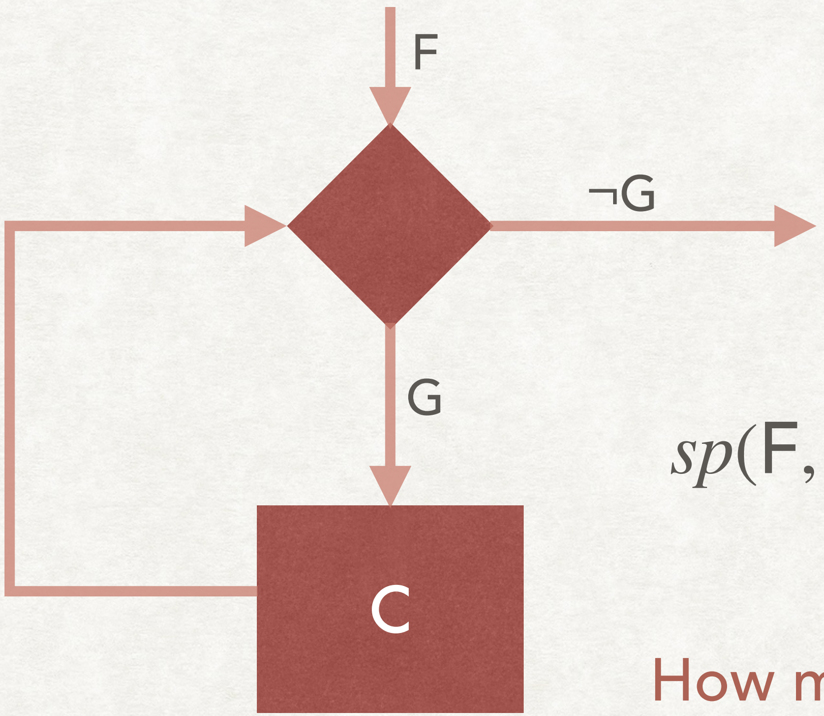


Iteration i	States possible at iteration i
0	F
1	$sp(F \wedge G, c)$
2	$sp(sp(F \wedge G, c) \wedge G, c)$
…	…

STRONGEST POST-CONDITION

WHILE LOOPS

- How to find sp(F, while(G) do c)?



$$F^0 = \mathsf{F}$$

$$F^k = sp(F^{k-1} \wedge \mathsf{G}, \mathsf{c})$$

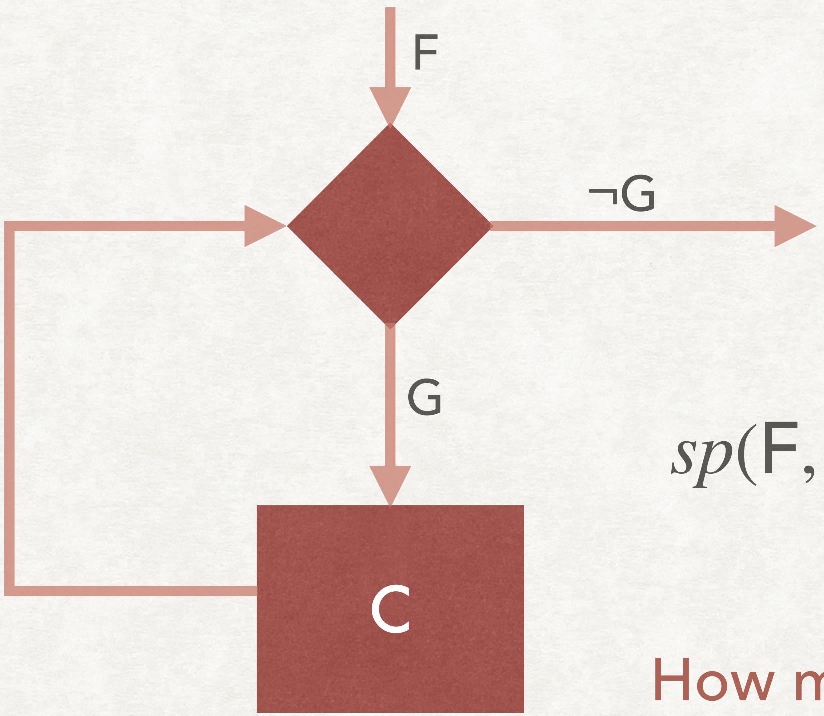
$$sp(\mathsf{F}, \text{while}(\mathsf{G}) \text{ do } \mathsf{c}) \triangleq \bigvee_{k=0}^{\infty} F^k \wedge \neg \mathsf{G}$$

How many F^k should be calculated?

STRONGEST POST-CONDITION

WHILE LOOPS

- How to find sp(F, while(G) do c)?



$$F^0 = \mathsf{F}$$

$$F^k = sp(F^{k-1} \wedge \mathsf{G}, \mathsf{c})$$

$$sp(\mathsf{F}, \mathsf{while(G)\ do\ c}) \triangleq \bigvee_{k=0}^{\infty} F^k \wedge \neg \mathsf{G}$$

How many F^k should be calculated?

Until $F^k \rightarrow \bigvee_{i=0}^{k-1} F^i$

WHILE LOOPS

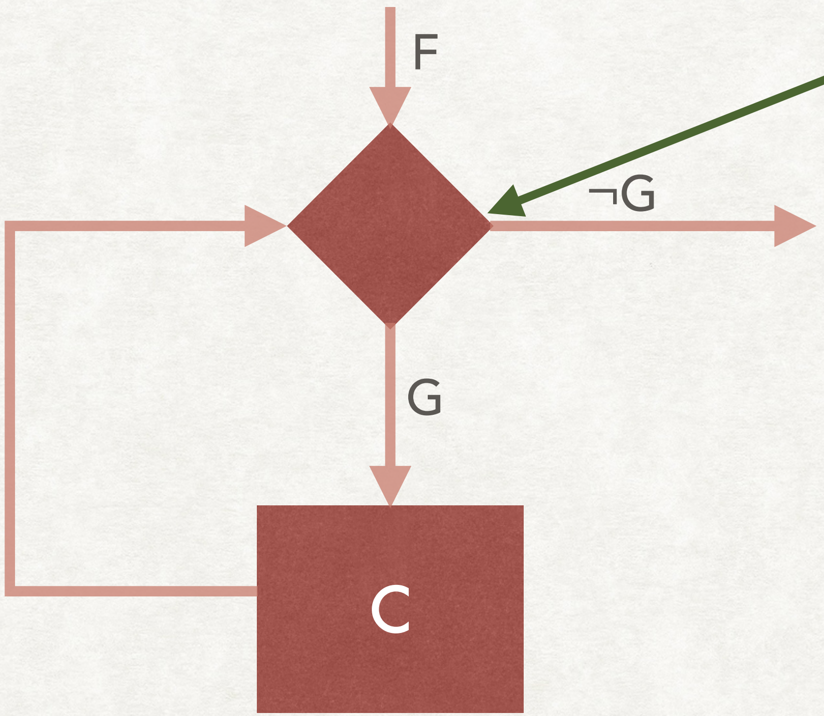
EXAMPLES

- $sp($x < 0,while(x<10) do x:=x+1;$) \triangleq ???$

WHILE LOOPS

EXAMPLES

- sp(x < 0,while(x<10) do x:=x+1;) $\triangleq$???

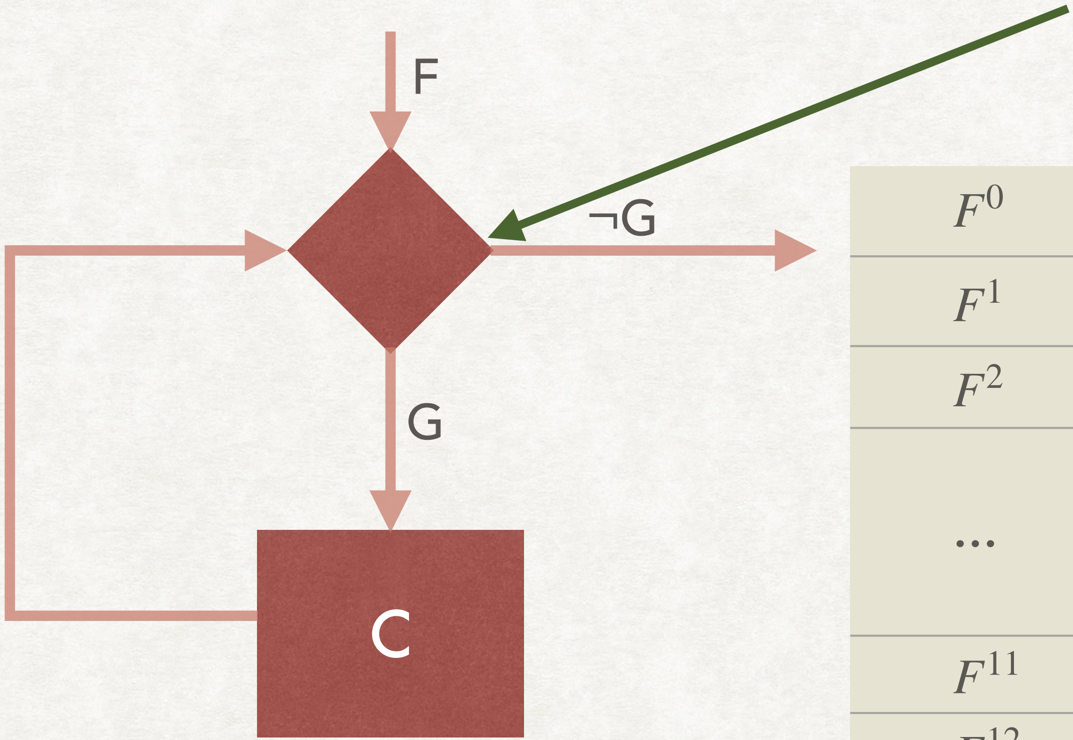


F^0	F
F^1	$sp(\mathsf{F} \wedge \mathsf{G}, \mathsf{c})$
F^2	$sp(sp(\mathsf{F} \wedge \mathsf{G}, \mathsf{c}) \wedge \mathsf{G}, \mathsf{c})$
...	...

WHILE LOOPS

EXAMPLES

- sp(x $<$ 0,while(x<10) do x:=x+1;) $\triangleq$???

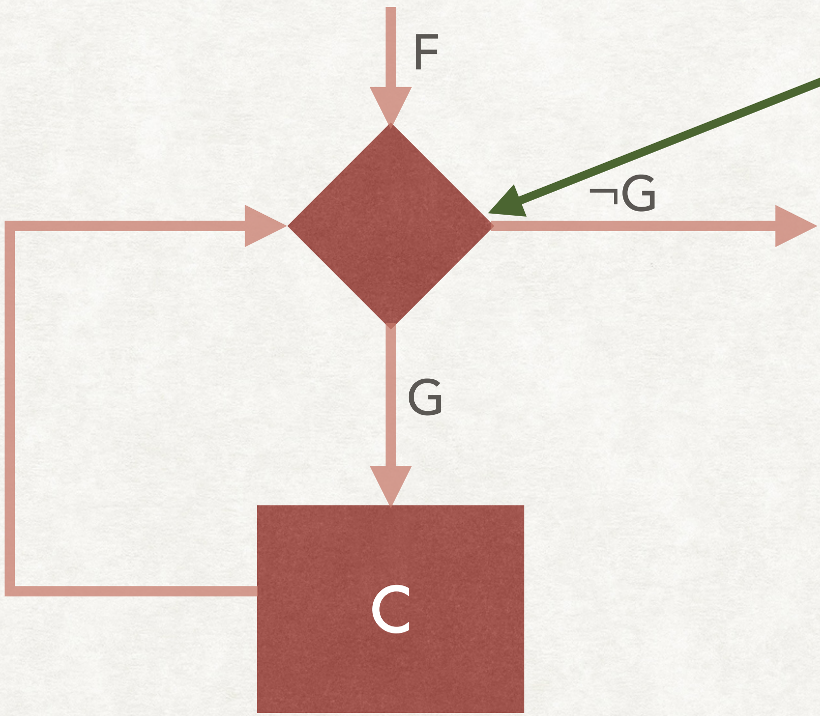


F^0	
F^1	
F^2	
…	…
F^{11}	
F^{12}	

WHILE LOOPS

EXAMPLES

- sp(x $<$ 0,while(x<10) do x:=x+1;) $\triangleq$???



F^0	$x < 0$
F^1	$x < 1$
F^2	$x < 2$
…	…
F^{11}	$x < 11$
F^{12}	$x < 11$

WHILE LOOPS

EXAMPLES

- sp(x $<$ 0,while(x<10) do x:=x+1;) $\triangleq$ x $\geq 10 \wedge$ x < 11

WHILE LOOPS

EXAMPLES

- sp(x $<$ 0,while(x<10) do x:=x+1;) $\triangleq$ x $\geq 10 \wedge$ x < 11
- sp(x $>$ 0,while(x<10) do x:=x+1;) $\triangleq$???

WHILE LOOPS

EXAMPLES

- $sp(\mathrm{x} < 0, \text{while(x<10) do x:=x+1;}) \triangleq \mathrm{x} \geq 10 \wedge \mathrm{x} < 11$
- $sp(\mathrm{x} > 0, \text{while(x<10) do x:=x+1;}) \triangleq \mathrm{x} \geq 10$

WHILE LOOPS

EXAMPLES

- $sp(x < 0, \text{while(x<10) do x:=x+1;}) \triangleq x \geq 10 \wedge x < 11$
- $sp(x > 0, \text{while(x<10) do x:=x+1;}) \triangleq x \geq 10$
- $sp(x > 0, \text{while(x>0) do x:=x+1;}) \triangleq ???$

WHILE LOOPS

EXAMPLES

- $sp(\mathrm{x} < 0, \text{while(x<10) do x:=x+1;}) \triangleq \mathrm{x} \geq 10 \wedge \mathrm{x} < 11$
- $sp(\mathrm{x} > 0, \text{while(x<10) do x:=x+1;}) \triangleq \mathrm{x} \geq 10$
- $sp(\mathrm{x} > 0, \text{while(x>0) do x:=x+1;}) \triangleq \perp$

STRONGEST POST-CONDITION AND VERIFICATION

- Given a program c with assertions, then c is safe if $sp(\text{error} = 0, \text{c}) \rightarrow \text{error} = 0$ is valid.
- The Hoare Triple $\{P\}\text{c}\{Q\}$ is valid if $sp(P, \text{c}) \rightarrow Q$ is valid.
- Do we have a decidable procedure for sp?
    - No, due to the (potentially) unbounded computation required for while loops.
    - What is an example of F and c such that $sp(F, c)$ requires unbounded computation?