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

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

STRONGEST POST-CONDITION

MORE EXAMPLES

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

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

STRONGEST POST-CONDITION

MORE EXAMPLES

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

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

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

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

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

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

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

STRONGEST POST-CONDITION

MORE EXAMPLES

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

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

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

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

STRONGEST POST-CONDITION

MORE EXAMPLES

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

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

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

$$sp(\text{F}, \text{assert(G)}) \triangleq \exists V \,.\, F \land (G \rightarrow frame(\emptyset))$$

$$\equiv \exists V \,.\, F \land (\neg G \lor frame(\emptyset))$$

$$\equiv \exists V \,.\, (F \land \neg G) \lor \exists V \,.\, (F \land frame(\emptyset))$$

$$\equiv \exists V \,.\, (F \land \neg G) \lor F[V'/V] \longleftarrow$$

$$\equiv (\exists V \,.\, F \land \neg G) \lor F \longleftarrow$$

STRONGEST POST-CONDITION

MORE EXAMPLES

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

$\triangleq \mathsf{y} > 0$

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

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

STRONGEST POST-CONDITION

MORE EXAMPLES

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

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

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

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

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

STRONGEST POST-CONDITION

EXAMPLES

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

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

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

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

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

EXAMPLES

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

STRONGEST POST-CONDITION

COMPOUND STATEMENTS

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

STRONGEST POST-CONDITION

COMPOUND STATEMENTS

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

STRONGEST POST-CONDITION

COMPOUND STATEMENTS

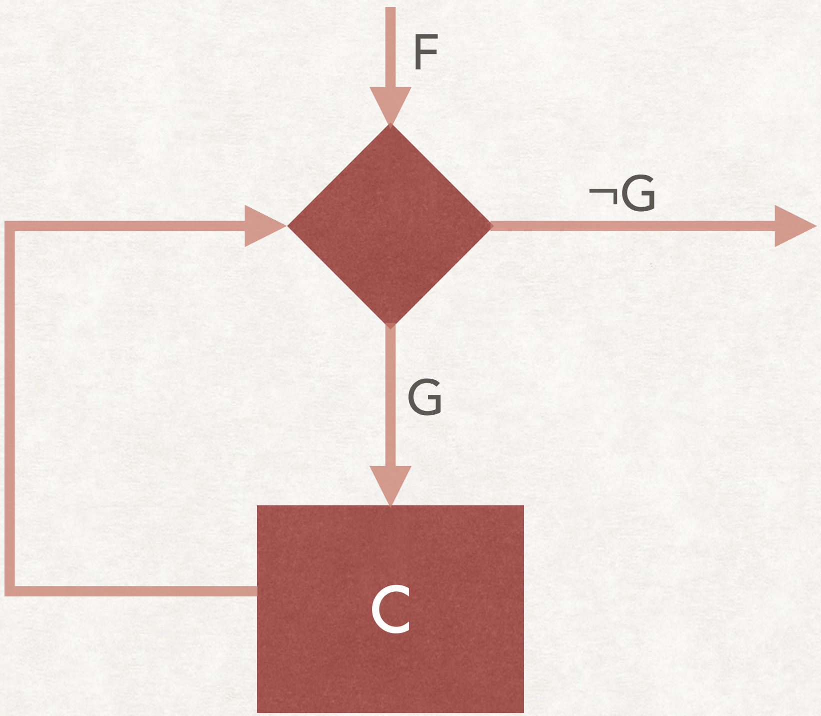
- $sp(\mathrm{F}, \mathrm{c;c'}) \triangleq sp(sp(\mathrm{F}, \mathrm{c}), \mathrm{c'})$
- $sp(\mathrm{F}, \text{if(G) then c else c'}) \triangleq sp(\mathrm{F} \wedge \mathrm{G}, \mathrm{c}) \vee sp(\mathrm{F} \wedge \neg\mathrm{G}, \mathrm{c'})$

HOMEWORK: PROVE USING DEFINITION OF SP

STRONGEST POST-CONDITION

WHILE LOOPS

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

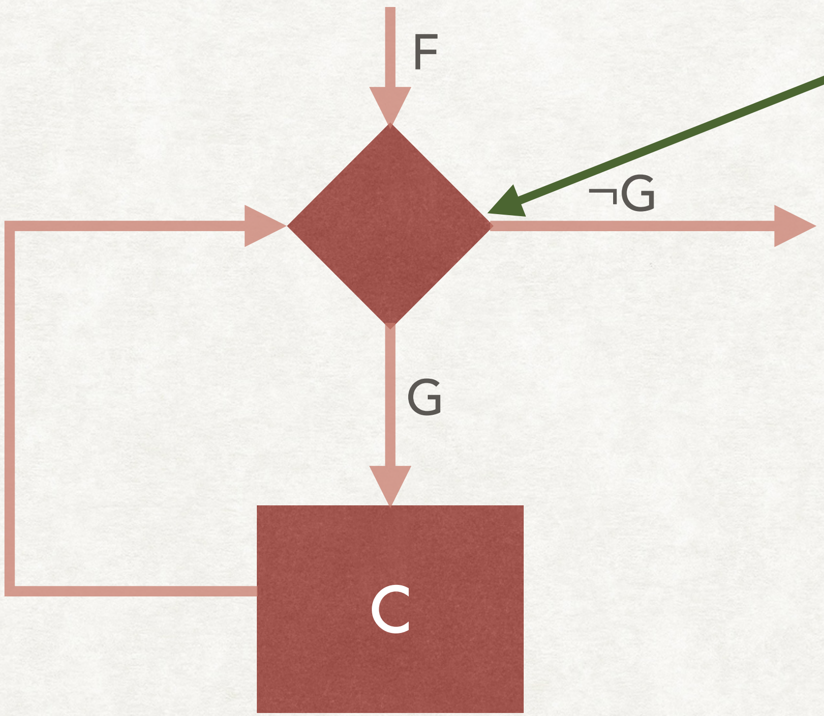


STRONGEST POST-CONDITION

WHILE LOOPS

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

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

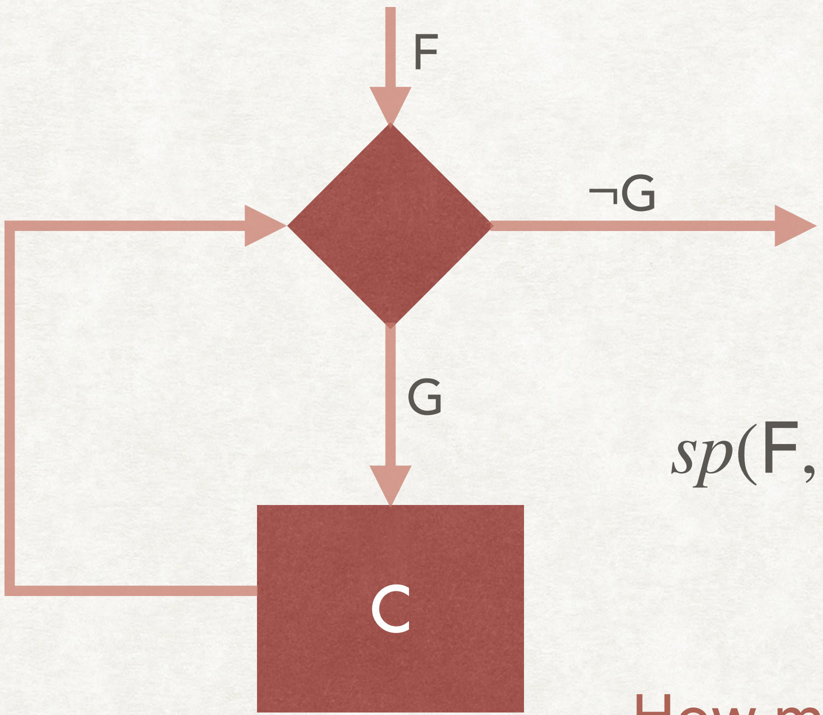


Iteration i	States possible upto iteration i
0	F
1	$F \lor sp(F \land G, c)$
2	$F \lor sp(F \land G, c) \lor sp(sp(F \land G, c) \land G, c)$
…	…

STRONGEST POST-CONDITION

WHILE LOOPS

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



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

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

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

How many F^k should be calculated?

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