HOARE LOGIC

HOARE LOGIC

INTRODUCTION

- Since finding the exact wp or sp for while-loops is difficult, we will use an over-approximation in the form of an Inductive Invariant which preserves soundness.
  - Much of the rest of the course (and majority of research in verification) deals with how to handle the verification problem for loops/loop-like constructs!
- Hoare Logic is a program logic/verification strategy which can be directly used to prove the validity of Hoare Triples.
  - Also provides a framework for specifying and verifying Inductive Loop Invariants.

DEFINITION

- Given sets of states P and Q, a program c satisfies the specification $\{P\}\mathsf{c}\{Q\}$ if:
  - $\forall \sigma \,.\, \sigma \in P \wedge (\sigma, \mathsf{c}) \hookrightarrow^* (\sigma', \mathsf{skip}) \Rightarrow \sigma' \in Q$
- Using FOL formulae P and Q to express sets of states, we can now use the symbolic semantics $\rho(\mathsf{c})$:
  - $\forall V \,.\, P \wedge \rho(\mathsf{c}) \rightarrow Q[V'/V]$
- Hoare Logic is a program logic/proof system to directly prove the validity of Hoare Triples.
- We will study it in two forms:
  - A set of inference rules to write pen-and-paper proofs
  - A procedure to generate verification conditions (VCs) in FOL

RELATION WITH WP AND SP

- How are Hoare Triples, Weakest Pre-condition and Strongest Post-condition related with each other?
  - $\{wp(P, \mathsf{c})\}\ \mathsf{c}\ \{P\}$
  - $\{P\}\ \mathsf{c}\ \{sp(P, \mathsf{c})\}$
- Prove this from the definitions!

INFERENCE RULES

FORMAT

PREMISES $\rightarrow$ CONCLUSION $\rightarrow$

$$\frac{\{P_1\}S_1\{Q_1\} \quad \{P_2\}S_2\{Q_2\} \quad \dots \quad \{P_n\}S_n\{Q_n\}}{\{P\}S\{Q\}}$$

Key Idea: Use the validity of Hoare triples for smaller statements to establish validity for compound statements

INFERENCE RULES

PRIMITIVE STATEMENTS

$$\frac{}{\{P[\mathsf{e}/\mathsf{x}]\}\ \mathsf{x} := \mathsf{e}\ \{P\}}\ \text{[R-ASSIGN]}$$

$$\frac{}{\{\forall \mathsf{x}\,.\,P\}\ \mathsf{x} := \mathsf{havoc}\ \{P\}}\ \text{[R-HAVOC]}$$

$$\frac{}{\{Q \rightarrow P\}\ \mathsf{assume}(Q)\ \{P\}}\ \text{[R-ASSUME]}$$

$$\frac{}{\{Q \wedge P\}\ \mathsf{assert}(Q)\ \{P\}}\ \text{[R-ASSERT]}$$

EXAMPLES

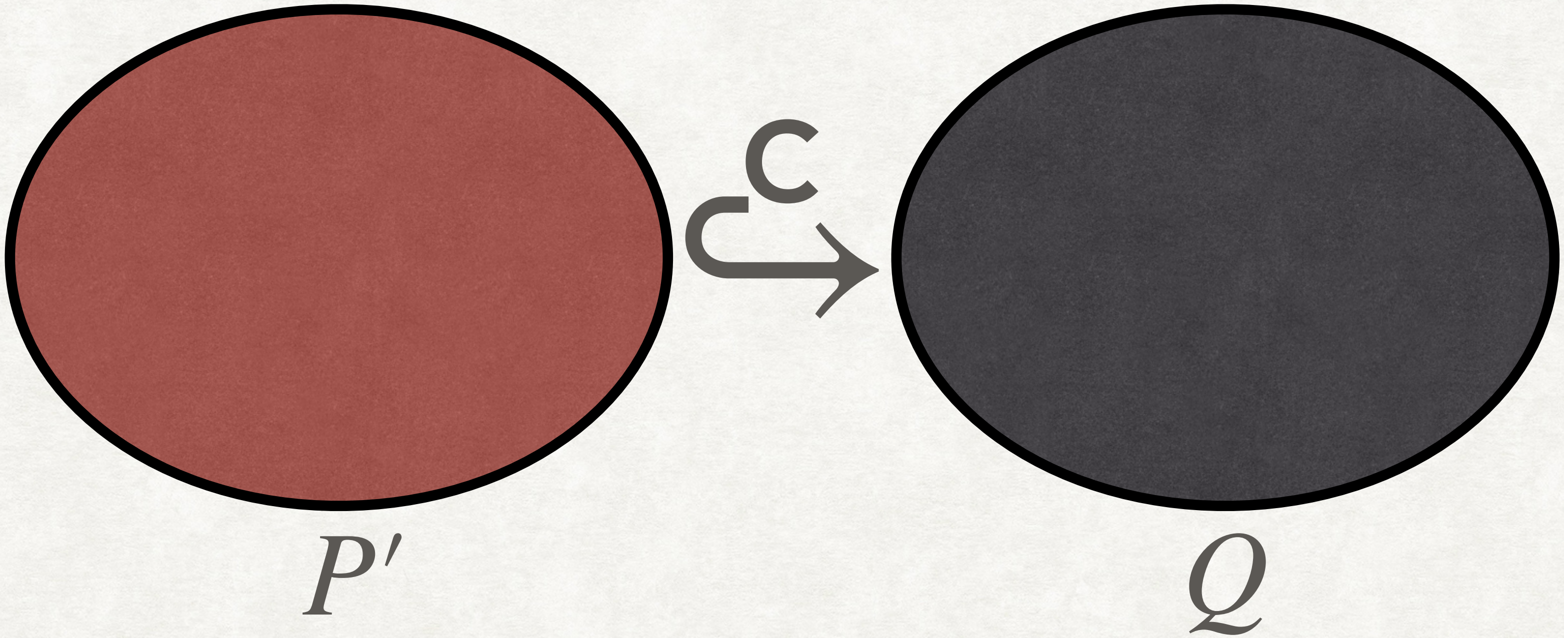
- Which of the following are true?
  - $\{y = 10\}$ x := 10 $\{y = x\}$
  - $\{x = n - 1\}$ x := x + 1 $\{x = n\}$
  - $\{y = x\}$ y := 2 $\{y = x\}$
  - $\{z = 10\}$ y := 2 $\{z = 10\}$
  - $\{y = 10\}$ y := x $\{y = x\}$
- The last Hoare triple is valid, but we cannot prove it using [R-ASSIGN].
  - According to [R-ASSIGN], we have $\{y = x[x/y]\}$ y := x $\{y = x\}$. Hence, $\{x = x\}$ y := x $\{y = x\}$, which simplifies to $\{true\}$ y := x $\{y = x\}$. Notice that $y = 10 \Rightarrow true$.

PRE-CONDITION STRENGTHENING

$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}\ \text{[R-STRENGTHEN-PRE]}$$

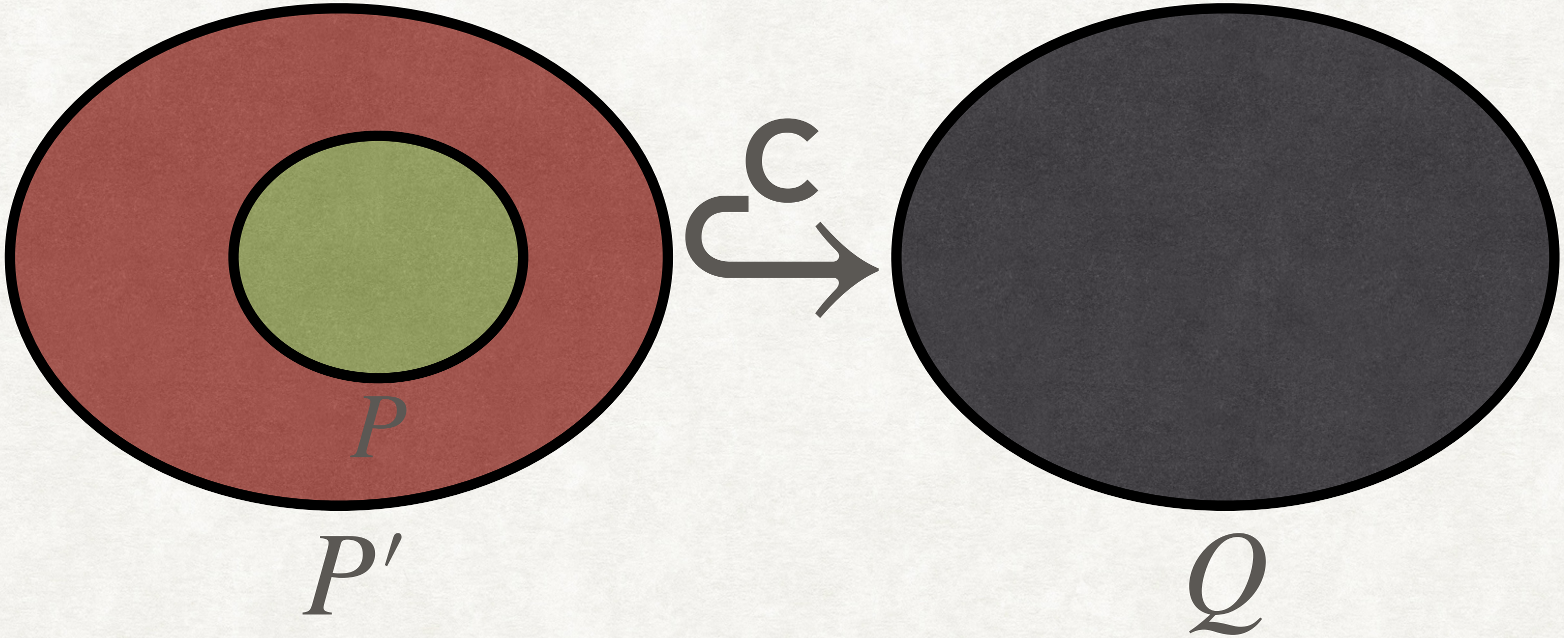
PRE-CONDITION STRENGTHENING

$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}\ \text{[R-STRENGTHEN-PRE]}$$



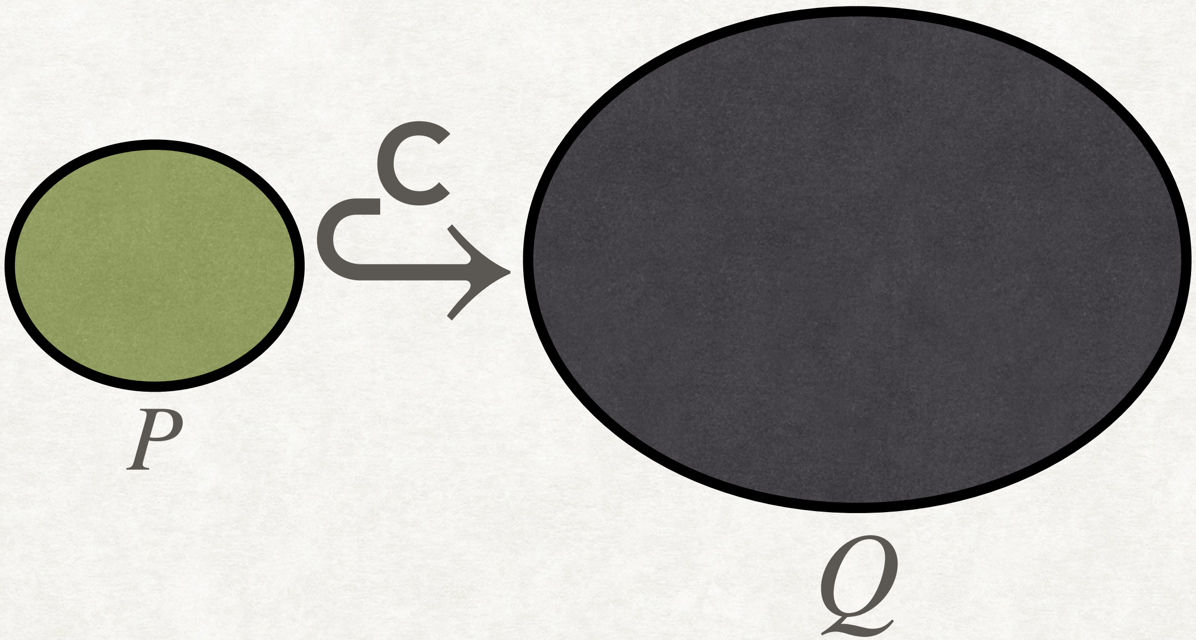
PRE-CONDITION STRENGTHENING

$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}\ \text{[R-STRENGTHEN-PRE]}$$



PRE-CONDITION STRENGTHENING

$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}\ \text{[R-STRENGTHEN-PRE]}$$



PRE-CONDITION STRENGTHENING

$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}\ \text{[R-STRENGTHEN-PRE]}$$

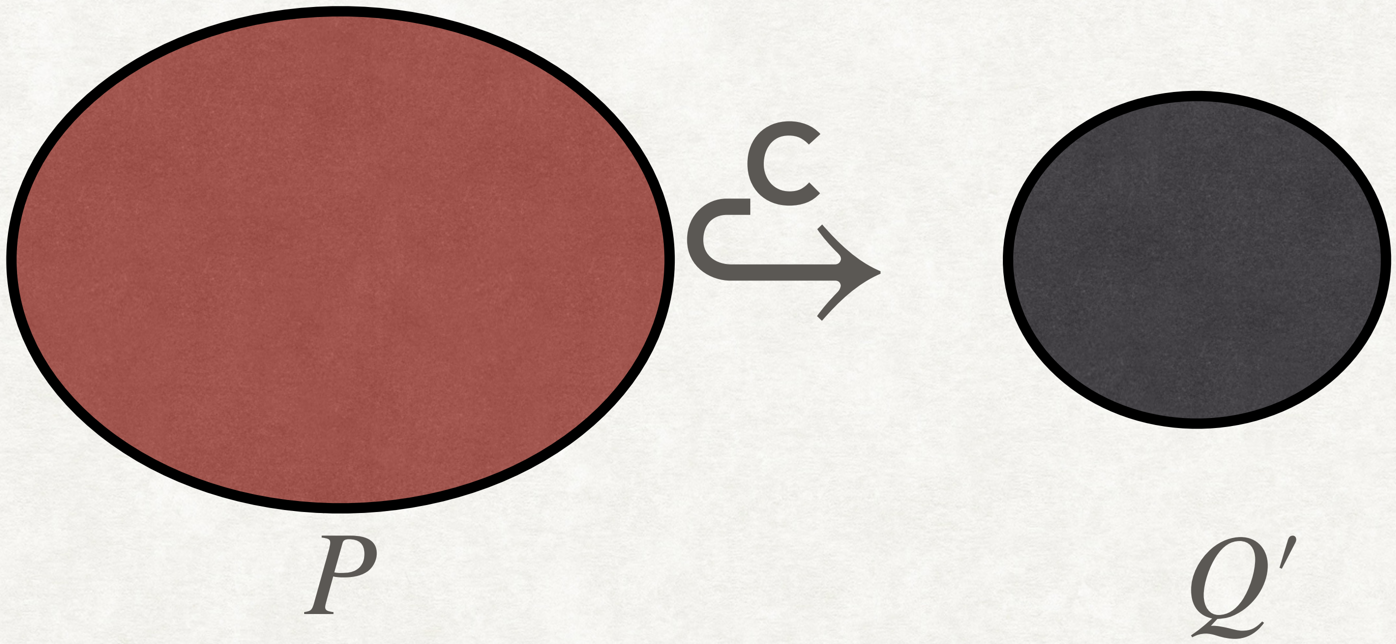
$$\frac{\dfrac{}{\{true\}\ \mathsf{y} := \mathsf{x}\ \{\mathsf{y} = \mathsf{x}\}} \qquad \mathsf{y} = 10 \Rightarrow true}{\{\mathsf{y} = 10\}\ \mathsf{y} := \mathsf{x}\ \{\mathsf{y} = \mathsf{x}\}}$$

POST-CONDITION WEAKENING

$$\frac{\{P\}\ \mathsf{c}\ \{Q'\} \qquad Q' \Rightarrow Q}{\{P\}\ \mathsf{c}\ \{Q\}}\ \text{[R-WEAKEN-POST]}$$

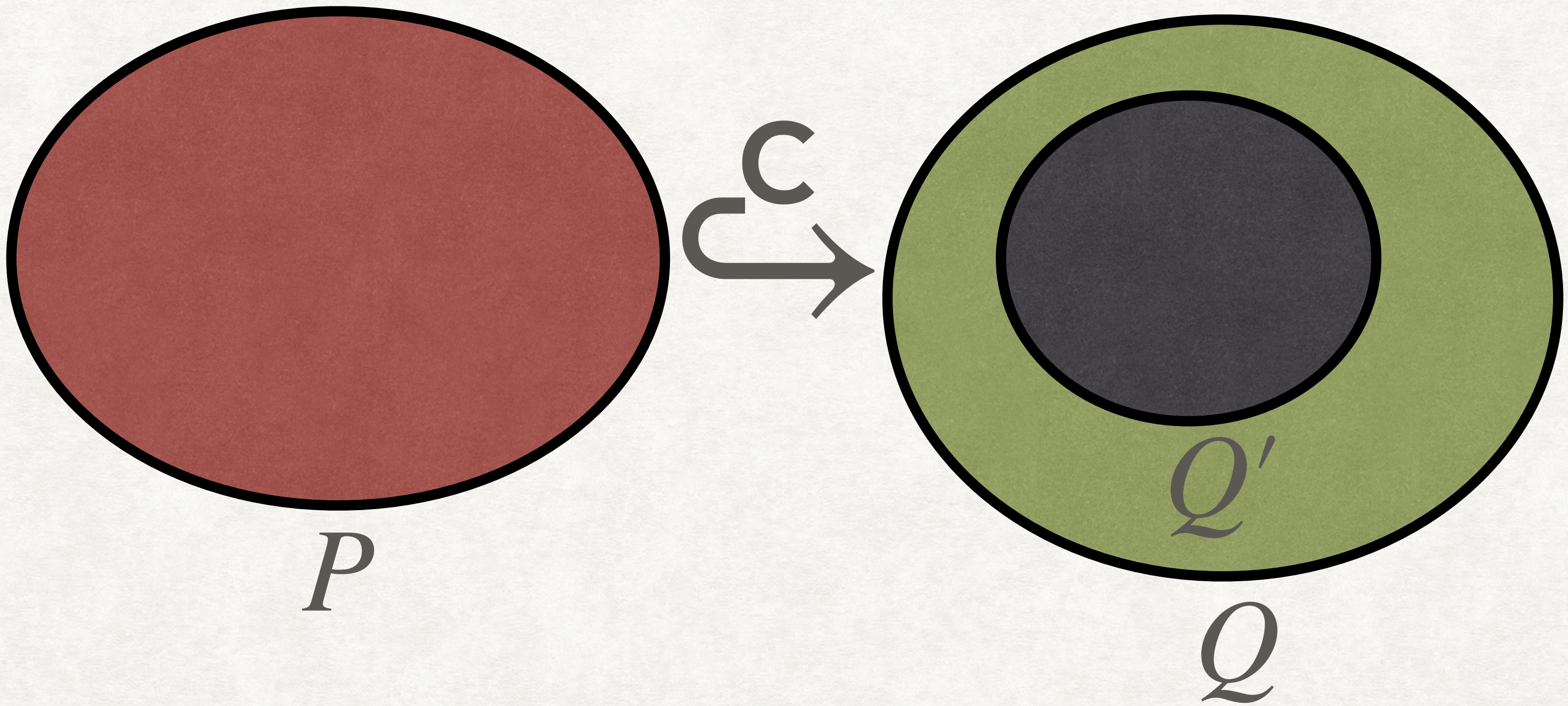
POST-CONDITION WEAKENING

$$\frac{\{P\}\ \mathsf{c}\ \{Q'\} \qquad Q' \Rightarrow Q}{\{P\}\ \mathsf{c}\ \{Q\}}\ \text{[R-WEAKEN-POST]}$$



POST-CONDITION WEAKENING

$$\frac{\{P\}\ \mathsf{c}\ \{Q'\} \qquad Q' \Rightarrow Q}{\{P\}\ \mathsf{c}\ \{Q\}}\ \text{[R-WEAKEN-POST]}$$



INFERENCE RULES

COMPOUND STATEMENTS

$$\frac{\{P\}\ \mathsf{c}_1\ \{R\} \qquad \{R\}\ \mathsf{c}_2\ \{Q\}}{\{P\}\ \mathsf{c}_1; \mathsf{c}_2\ \{Q\}} \quad \text{[R-SEQ]}$$

INFERENCE RULES

COMPOUND STATEMENTS

$$\frac{\{P\}\ \mathsf{c}_1\ \{R\} \qquad \{R\}\ \mathsf{c}_2\ \{Q\}}{\{P\}\ \mathsf{c}_1; \mathsf{c}_2\ \{Q\}}$$

[R-SEQ]

$$\frac{\{P \wedge F\}\ \mathsf{c}_1\ \{Q\} \qquad \{P \wedge \neg F\}\ \mathsf{c}_2\ \{Q\}}{\{P\}\ \text{if } (F) \text{ then } \mathsf{c}_1 \text{ else } \mathsf{c}_2\ \{Q\}}$$

[R-IF-THEN-ELSE]

INFERENCE RULES

COMPOUND STATEMENTS

$$\frac{\{P\}\ \mathsf{c}_1\ \{R\} \qquad \{R\}\ \mathsf{c}_2\ \{Q\}}{\{P\}\ \mathsf{c}_1; \mathsf{c}_2\ \{Q\}}$$

[R-SEQ]

$$\frac{\{P \wedge F\}\ \mathsf{c}_1\ \{Q\} \qquad \{P \wedge \neg F\}\ \mathsf{c}_2\ \{Q\}}{\{P\}\ \text{if } (F) \text{ then } \mathsf{c}_1 \text{ else } \mathsf{c}_2\ \{Q\}}$$

[R-IF-THEN-ELSE]

Prove This!

SEQUENCING

EXAMPLE

$$\frac{\{P\}\ \mathsf{c}_1\ \{R\} \qquad \{R\}\ \mathsf{c}_2\ \{Q\}}{\{P\}\ \mathsf{c}_1; \mathsf{c}_2\ \{Q\}} \quad \text{[R-SEQ]}$$

$$\frac{\dfrac{}{\{true\}\ \mathsf{x} := 2\ \{\mathsf{x} = 2\}} \qquad \dfrac{}{\{\mathsf{x} = 2\}\ \mathsf{y} := \mathsf{x}\ \{\mathsf{y} = 2 \land \mathsf{x} = 2\}}}{\{true\}\ \mathsf{x} := 2; \mathsf{y} := \mathsf{x}\ \{\mathsf{y} = 2 \land \mathsf{x} = 2\}}$$

IF-THEN-ELSE

EXAMPLE

$$\frac{\{P \wedge F\}\ \mathsf{c}_1\ \{Q\} \qquad \{P \wedge \neg F\}\ \mathsf{c}_2\ \{Q\}}{\{P\}\ \text{if } (F) \text{ then } \mathsf{c}_1 \text{ else } \mathsf{c}_2\ \{Q\}} \ \text{[R-IF-THEN-ELSE]}$$

$$\dfrac{\dfrac{\dfrac{}{\{\mathsf{x} \geq 0\}\ \mathsf{y} := \mathsf{x}\ \{\mathsf{y} \geq 0\}} \qquad \mathsf{x} > 0 \Rightarrow \mathsf{x} \geq 0}{\{\mathsf{x} > 0\}\ \mathsf{y} := \mathsf{x}\ \{\mathsf{y} \geq 0\}} \qquad \dfrac{}{\{\mathsf{x} \leq 0\}\ \mathsf{y} := \text{-}\mathsf{x}\ \{\mathsf{y} \geq 0\}}}{\{true\}\ \text{if } (\mathsf{x} > 0) \text{ then } \mathsf{y} := \mathsf{x} \text{ else } \mathsf{y} := \text{-}\mathsf{x}\{\mathsf{y} \geq 0\}}$$