# 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:
  - $\forall \sigma, \sigma' \,.\, \sigma \in P \wedge (\sigma, \mathsf{c}) \hookrightarrow^* (\sigma', \mathsf{skip}) \Rightarrow \sigma' \in Q$
- Using FOL formulae $P$ and $Q$ to express sets of states, we can now use the symbolic semantics $\rho(\mathsf{c})$:
  - $\forall V, V' \,.\, P \wedge \rho(\mathsf{c}) \rightarrow Q[V'/V]$
- 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
  - 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?
  - $\{wp(P, \mathsf{c})\}\ \mathsf{c}\ \{P\}$
  - $\{P\}\ \mathsf{c}\ \{sp(P, \mathsf{c})\}$
- Homework: Prove this formally using the definitions!

# INFERENCE RULES

## FORMAT

PREMISES → $\{P_1\}S_1\{Q_1\} \quad \{P_2\}S_2\{Q_2\} \quad \dots \quad \{P_n\}S_n\{Q_n\}$

CONCLUSION → $\{P\}S\{Q\}$

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

# INFERENCE RULES

## PRIMITIVE STATEMENTS

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

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

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

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

# 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 $\{ \top \}$ y := x $\{y = x\}$.
  - Notice that $y = 10 \Rightarrow \top$ .

# PRE-CONDITION STRENGTHENING

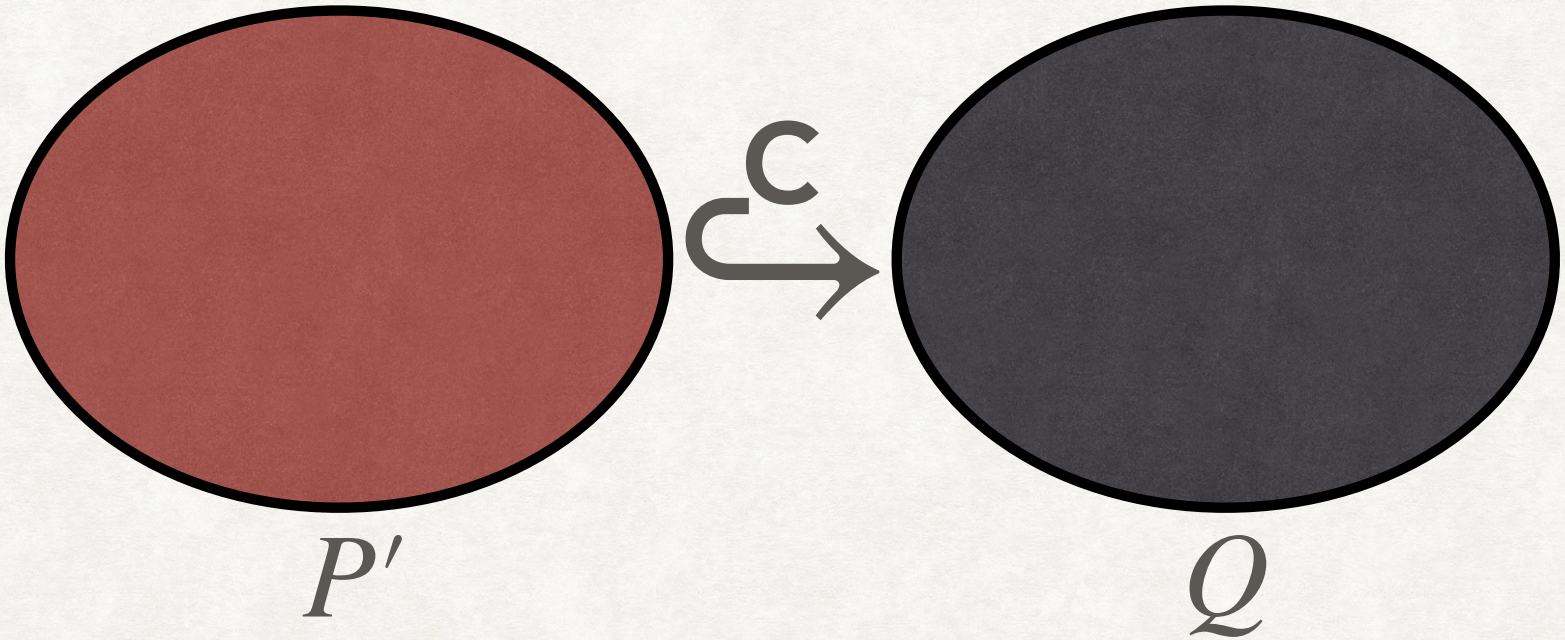
$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}$$

[R-STRENGTHEN-PRE]

# PRE-CONDITION STRENGTHENING

$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}$$

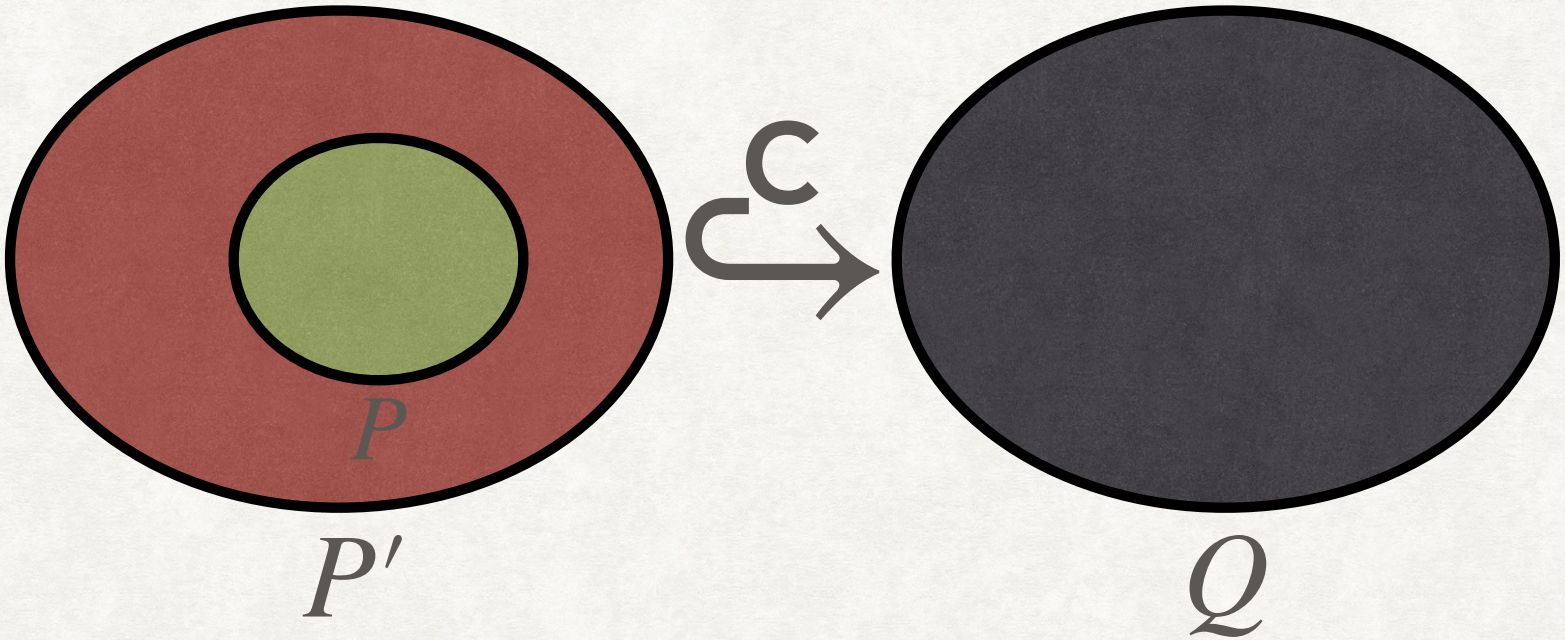
[R-STRENGTHEN-PRE]



# PRE-CONDITION STRENGTHENING

$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}$$

[R-STRENGTHEN-PRE]



# PRE-CONDITION STRENGTHENING

$$\frac{\{P'\}\ \mathsf{c}\ \{Q\} \qquad P \Rightarrow P'}{\{P\}\ \mathsf{c}\ \{Q\}}$$

[R-STRENGTHEN-PRE]