CS142 Problem Solving Lecture

Sumanth Dathathri

California Institute of Technology

October 6, 2017
Hoare Logic Properties (Left Hand Side Strengthening)

Is this property true?

\[ [R \Rightarrow P] \land \{ P \} a\{ Q \} \Rightarrow \{ R \} a\{ Q \} \]
Hoare Logic Properties (Left Hand Side Strengthening)

Is this property true?

\[ [R \Rightarrow P] \land \{P\} a\{Q\} \Rightarrow \{R\} a\{Q\} \]
Is this property true?

\[ [R \Rightarrow P] \land \{P\}a\{Q\} \Rightarrow \{R\}a\{Q\} \]

Yes.

See similarity with implication:

\[ (R \Rightarrow P) \land (P \Rightarrow Q) \Rightarrow (R \Rightarrow Q) \]
Hoare Logic Properties (Right-Hand Side Weakening)

Is this property true?

\[ ([Q \Rightarrow R] \land \{P\}a\{Q\} \Rightarrow \{P\}a\{R\} \]

S. Dathathri (sdathath@caltech.edu)
Is this property true?

\[
([Q \Rightarrow R] \land \{P\}a\{Q\} \Rightarrow \{P\}a\{R\})
\]
Hoare Logic Properties (Right-Hand Side Weakening)

Is this property true?

\[ ([Q \Rightarrow R] \land \{P\} a\{Q\} \Rightarrow \{P\} a\{R\} \]

Yes.

Similar to the following rule for implication:

\[ (Q \Rightarrow R) \land (P \Rightarrow Q) \Rightarrow (P \Rightarrow R) \]
Hoare Logic Properties (Left Hand Side Weakening)

Is this property true?

\[ [P \Rightarrow R] \land \{ P \} a\{ Q \} \Rightarrow \{ R \} a\{ Q \} \]
Is this property true?

\[
[P \Rightarrow R] \land \{P\}a\{Q\} \Rightarrow \{R\}a\{Q\}
\]

False
Hoare Logic Properties (Disjunction of LHS)

Is this property true?

\[ \{ P_1 \} a \{ Q \} \land \{ P_2 \} a \{ Q \} \Rightarrow \{ P_1 \lor P_2 \} a \{ Q \} \]
Hoare Logic Properties (Disjunction of LHS)

Is this property true?

\[
\{ P_1 \} a \{ Q \} \land \{ P_2 \} a \{ Q \} \implies \{ P_1 \lor P_2 \} a \{ Q \}
\]
Hoare Logic Properties (Disjunction of LHS)

Is this property true?

\[
\{P_1\}a\{Q\} \land \{P_2\}a\{Q\} \Rightarrow \{P_1 \lor P_2\}a\{Q\}
\]

Yes. Similar to:

\[
(P_1 \Rightarrow Q) \land (P_2 \Rightarrow Q) \Rightarrow ((P_1 \lor P_2) \Rightarrow Q)
\]
Hoare Logic Properties (Conjunction of RHS)

Is this property true?

\[
\{ P \} a \{ Q_1 \} \land \{ P \} a \{ Q_2 \} \implies \{ P \} a \{ Q_1 \land Q_2 \}
\]
Hoare Logic Properties (Conjunction of RHS)

Is this property true?

$$\{P\} a \{Q_1\} \land \{P\} a \{Q_2\} \Rightarrow \{P\} a \{Q_1 \land Q_2\}$$

Yes. Similar to:

$$(P \Rightarrow Q_1) \land (P \Rightarrow Q_2) \Rightarrow (P \Rightarrow (Q_1 \land Q_2))$$
Hoare Logic Properties (Conjunction of RHS)

Is this property true?

$$\{ P \} a\{ Q_1 \} \land \{ P \} a\{ Q_2 \} \Rightarrow \{ P \} a\{ Q_1 \land Q_2 \}$$

Yes. Similar to:

$$(P \Rightarrow Q_1) \land (P \Rightarrow Q_2) \Rightarrow (P \Rightarrow (Q_1 \land Q_2))$$
Is this property true?

\[
\{ P_1 \} a \{ Q_1 \} \vee \{ P_2 \} a \{ Q_2 \} \implies \{ P_1 \lor P_2 \} a \{ Q_1 \lor Q_2 \}
\]
Hoare Logic Properties

Is this property true?

\[
\{P_1\} a\{Q_1\} \lor \{P_2\} a\{Q_2\} \Rightarrow \{P_1 \lor P_2\} a\{Q_1 \lor Q_2\}
\]

False
Is this property true?

\[ \{ P_1 \} a \{ Q_1 \} \land \{ P_2 \} a \{ Q_2 \} \Rightarrow \{ P_1 \lor P_2 \} a \{ Q_1 \lor Q_2 \} \]
Hoare Logic Properties (Disjunction Rule)

Is this property true?

\[ \{ P_1 \} a \{ Q_1 \} \land \{ P_2 \} a \{ Q_2 \} \Rightarrow \{ P_1 \lor P_2 \} a \{ Q_1 \lor Q_2 \} \]

Yes. Let us prove this:
Is this property true?

\[ \{P_1\} a\{Q_1\} \land \{P_2\} a\{Q_2\} \Rightarrow \{P_1 \lor P_2\} a\{Q_1 \lor Q_2\} \]

Yes. Let us prove this:

- Weaken RHS to \( Q_1 \lor Q_2 \)
Is this property true?

\[ \{ P_1 \} a \{ Q_1 \} \land \{ P_2 \} a \{ Q_2 \} \implies \{ P_1 \lor P_2 \} a \{ Q_1 \lor Q_2 \} \]

Yes. Let us prove this:

- Weaken RHS to \( Q_1 \lor Q_2 \)
- Disjunction Rule
Is this property true?

\[ \{ P_1 \} a \{ Q_1 \} \land \{ P_2 \} a \{ Q_2 \} \Rightarrow \{ P_1 \land P_2 \} a \{ Q_1 \land Q_2 \} \]
Hoare Logic Properties (Conjunction Rule)

Is this property true?

\[ \{ P_1 \} a \{ Q_1 \} \land \{ P_2 \} a \{ Q_2 \} \Rightarrow \{ P_1 \land P_2 \} a \{ Q_1 \land Q_2 \} \]

Yes. Exercise: Prove this

For HW

- Can prove properties about \textbf{next} by lifting to Hoare logic
- Can prove properties about \textbf{stable} by lifting to \textbf{next}
Example – Find weakest precondition

\{P\}x := x + 1; y = x + y \{y > 5\}

Answer: Weakest precondition $P$ is $x + y > 4$

Proof: (Be more complete/rigorous on the homework!)

$P \Rightarrow x + y + 1 > 5$
Example – Find weakest precondition

\{ P \} x := x + 1; y = x + y \{ y > 5 \}

Answer: Weakest precondition $P$ is $x + y > 4$

Proof: (Be more complete/rigorous on the homework!)

\[ P \iff x + y + 1 > 5 \]
Example – Find weakest precondition

\{ P \} x > 0 \implies y := x; x \leq 0 \implies y := -x \{ y > 5 \}
Example – Find weakest precondition

\{P\}x > 0 \implies y := x; x \leq 0 \implies y := -x \{y > 5\}

Answer: \((x > 5 \lor x < -5)\)

Proof:
\((x > 0 \implies x > 5) \lor (x \leq 0 \implies x < -5)\)
Example – Strongest postcondition

All the following Hoare Triples hold. Identify the Triple with the strongest post condition:

\[ \{ x = 5 \} \ x := x \times 2 \{ true \} \]
\[ \{ x = 5 \} \ x := x \times 2 \{ x > 0 \} \]
\[ \{ x = 5 \} \ x := x \times 2 \{ x = 10 \lor x = 5 \} \]
\[ \{ x = 5 \} \ x := x \times 2 \{ x = 10 \} \]
Example – Strongest postcondition

All the following Hoare Triples hold. Identify the Triple with the strongest post condition:

\[
\begin{align*}
\{x = 5\} &\ x := x \times 2\{true\} \\
\{x = 5\} &\ x := x \times 2\{x > 0\} \\
\{x = 5\} &\ x := x \times 2\{x = 10 \lor x = 5\} \\
\{x = 5\} &\ x := x \times 2\{x = 10\}
\end{align*}
\]

Answer:

\[
\{x = 5\} \ x := x \times 2\{x = 10\}
\]
Invariants

- Proving property $P$ is an invariant has two parts:
  - Prove Initially $P$ holds
  - Prove Stability of $P$
- We will only consider safety today. Progress and termination next week
Example - What color is the last marble?

A jar initially has $b$ Blue Marbles and $r$ Red Marbles. Denote the set of Blue (Red) Marbles in the jar at any state of execution as $B$ ($R$). Consider a second receptacle of red marbles $\bar{R} = \{\bar{R}_1, \ldots, \bar{R}_{|R|+|B|}\}$

**Program** \textit{EmptyJar}  
**Initially** 
\[ B = \{B_1, \ldots, B_b\}, R = \{R_1, \ldots, R_r\}, \quad \bar{R} = \{\bar{R}_1, \ldots, \bar{R}_{|R|+|B|}\} \]

**Var** Sets $B$, $R$, $\bar{R}$  
**Assignment**  
\[
\begin{align*}
&[\] x \in B, y \in R : R := R \setminus \{y\} \\
&[\] x \in B, y \in B, z \in \bar{R} : R := R \cup \{z\}, B := B \setminus \{x, y\}, \quad \bar{R} := \bar{R} \setminus \{z\} \\
&[\] x \in R, y \in R, z \in \bar{R} : R := (R \setminus \{x, y\}) \cup \{z\}, \quad \bar{R} := \bar{R} \setminus \{z\}
\end{align*}
\]

- We will not show termination, but find invariants
- Can you suggest invariant(s) for the above program?
Informal Description

- You randomly sample two marbles \( x, y \) from the first jar.
- If both marbles have the same color, you discard them; transfer marble from second jar to the first
- If they are different colors, discard the red one
What can you say about the number of marbles at the end of the execution of any of the assignment actions?
What can you say about the number of marbles at the end of the execution of any of the assignment actions?

- **Stable**($|B|$.even)
- **Stable**($|B|$.odd)

If $|B|$ is even initially, then the *invariant*.($|B|$.even) holds.

If $|B|$ is odd initially, then the *invariant*.($|B|$.even) holds.
Bonus Question: What is the color of the last marble?
Bonus Question: What is the color of the last marble?

The procedure can be repeated until the first jar is empty (use variants to show termination; next week’s lecture)

The last marble is a blue marble if $B$ is odd, last marble is a red one if $B$ is even