Section 1: Code Reasoning

cse331-staff@cs.washington.edu
Today’s Goals

• Review of code reasoning
• Practice forward and backward reasoning on straight-line and if-statement code
• Practice identifying the strongest assertion
Before we begin . . .

- “=” vs. “==”
- Read the lecture notes
Reasoning About Code

- Two purposes
  - Prove our code is correct
  - Understand why code is correct

- Forward reasoning: determine what follows from initial conditions
- Backward reasoning: determine sufficient conditions to obtain a certain result
Worksheet

• Problems 1 through 4
• 15 Minutes – get as far as you can
• You can collaborate with other students
• Grab a TA if you feel stuck
Forward Reasoning

\{x \geq 0, y \geq 0\}
y = 16;
\{x \geq 0, y = 16\}
x = x + y
\{x \geq 16, y = 16\}
x = \sqrt{x}
\{x \geq 4, y = 16\}
y = y - x
\{x \geq 4, y \leq 12\}
Forward Reasoning

\[
\begin{align*}
\{ & \text{true} \} \\
\text{if } (x > 0) \{ & \\
& \{ x > 0 \} \\
& \text{abs} = x \\
& \{ x > 0, \text{abs} = x \} \\
\} \\
\text{else} \{ & \\
& \{ x \leq 0 \} \\
& \text{abs} = -x \\
& \{ x \leq 0, \text{abs} = -x \} \\
\} \\
\{ & x > 0, \text{abs} = x \text{ OR } x \leq 0, \text{abs} = -x \} \\
\{ & \text{abs} = |x| \}
\end{align*}
\]
Backward Reasoning

\{x + 3b - 4 > 0\}
\[a = x + b;\]
\{a + 2b - 4 > 0\}
c = 2b - 4
\{a + c > 0\}
x = a + c
\{x > 0\}
Backward Reasoning

\{y > 15 \text{ || } (y <= 5 \text{ && } y + z > 17)\}\}

\textbf{if} (y > 5) \{ \\
    \{y > 15\} \\
    x = y + 2 \\
    \{x > 17\}
\}

\textbf{else} \{ \\
    \{y + z > 17\} \\
    x = y + z; \\
    \{x > 17\}
\}

\{x > 17\}
Implication

- Hoare triples are just an extension of logical implication
  - Hoare triple: \{P\} S \{Q\}
  - \(P \rightarrow Q\) after statement \(S\)
- Everything implies true
- False implies everything

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>(P \rightarrow Q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>
Weaker vs. Stronger

- If $P_1 \rightarrow P_2$, then
  - $P_1$ is stronger than $P_2$
  - $P_2$ is weaker than $P_1$

- Weaker statements are more general
- Stronger statements are more restrictive
Worksheet

- Problem 6
Worksheet

• “I attend quiz sections.”  “I attend quiz sections on Thursdays.”
• “y > 23”       “y >= 23”
• “y = 23”       “y >= 23”
• “y < 0.00023” “y < 0.23”
• “y is prime”   “y <= 17”
Worksheet

- “I attend quiz sections.”
- “y > 23”
- “y = 23”
- “y < 0.00023”
- “y is prime”
- “I attend quiz sections on Thursdays.”
- “y >= 23”
- “y >= 23”
- “y < 0.23”
- “y <= 17”
Worksheet

- “I attend quiz sections.” → “I attend quiz sections on Thursdays.”
- “y > 23” → “y >= 23”
- “y = 23” → “y >= 23”
- “y < 0.00023” → “y < 0.23”
- “y is prime” → “y <= 17”
Worksheet

- "I attend quiz sections." → "I attend quiz sections on Thursdays."
- "y > 23" → "y >= 23"
- "y = 23" → "y >= 23"
- "y < 0.00023" → "y < 0.23"
- "y is prime" → "y <= 17"
Worksheet

- “I attend quiz sections.”  “I attend quiz sections on Thursdays.”
- “y > 23”  “y >= 23”
- “y = 23”  “y >= 23”
- “y < 0.00023”  “y < 0.23”
- “y is prime”  “y <= 17”
Worksheet

- “I attend quiz sections.”
- “$y > 23$”
- “$y = 23$”
- “$y < 0.00023$”
- “$y$ is prime”

- “I attend quiz sections on Thursdays.”
- “$y \geq 23$”
- “$y \geq 23$”
- “$y < 0.23$”
- “$y \leq 17$” -- ?
Weakest Precondition

• The most lenient assumptions such that a postcondition will be satisfied

• If P* is the weakest precondition for \{P\} S \{Q\}, then P → P* for all P that make the Hoare triple valid

• Notation: WP = wp(S, Q)
Weakest Precondition

\[ wp(x = y \times y, \ x > 4) \]
Weakest Precondition

\[ wp(x = y^2, x > 4) \]

| \( |y| > 2 \) |
Weakest Precondition

\( wp(x = y*y, x > 4) \)

\(|y| > 2\)

\( wp(y = x+1; z = y-3, z = 10) \)
Weakest Precondition

\[ wp(x = y \times y, \ x > 4) \]
\[ |y| > 2 \]

\[ wp(y = x + 1; z = y - 3, \ z = 10) \]
\[ wp(y = x + 1, \ wp(z = y - 3, \ z = 10)) \]
\[ wp(y = x + 1, \ y - 3 = 10) \]
\[ wp(y = x + 1, \ y = 13) \]
\[ x = 12 \]
Questions