Section 1: Code Reasoning

cse331-staff@cs.washington.edu

My name is: Vincent Liew
Email: vliew@cs
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
  o Prove our code is correct
  o Understand why code is correct

• Forward reasoning: determine what follows from initial conditions
• Backward reasoning: determine sufficient conditions to obtain a certain result
Reasoning about “if”

```plaintext
{{ P }} if (b) {S1} else {S2} {{ Q }}
```

- When S1 executes, we know \( P \) and \( b \)
- When S2 executes, we know \( P \) and not \( b \)

- Triple is valid iff: there are assertions \( Q_1 \) and \( Q_2 \) such that
  - \( {{ P \ and \ b } } \{S1\} {{ Q_1 } } \) is valid and
  - \( {{ P \ and \ not \ b } } \{S2\} {{ Q_2 } } \) is valid and
  - \( Q_1 \ or \ Q_2 \) implies \( Q \)
    - we only know that one holds (which depends on \( b \))
Reasoning about “if”

\[
\{\{P\}\} \text{ if } (b) \{S1\} \text{ else } \{S2\} \{\{Q\}\}
\]

- When S1 executes, we know \(P \text{ and } b\)
- When S2 executes, we know \(P \text{ and not } b\)

- Triple is valid iff: there are assertions \(Q1\) and \(Q2\) such that
  - \(\{\{P \text{ and } b \}\} S1 \{\{Q1\}\}\) is valid and
  - \(\{\{P \text{ and not } b \}\} S2 \{\{Q2\}\}\) is valid and
  - \(Q1 \text{ or } Q2\) implies \(Q\)
  - we only know that one holds (which depends on \(b\))
  - Equivalent to \((Q1 \rightarrow Q \text{ and } Q2 \rightarrow Q)\)
    - May be easier to prove in this form
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

{true}
if (x > 0) {
    {x > 0}
    abs = x
    {x > 0, abs = x}
}
else {
    {x <= 0}
    abs = -x
    {x <= 0, abs = -x}
}
{x > 0, abs = x OR x <= 0, abs = -x}
{abs = |x|}
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 || (y <= 5 && y + z > 17)}

if (y > 5) {
    {y > 15}
    x = y + 2
    {x > 17}
}
else {
    {y + z > 17}
    x = y + z;
    {x > 17}
}
{x > 17}
Implication

• Hoare triples are just an extension of logical implication
  o Hoare triple: \{P\} S \{Q\}
  o \(P \rightarrow Q\) after statement S
• Everything implies true
• False implies everything
Weaker vs. Stronger

• If $P_1 \rightarrow P_2$, then
  o $P_1$ is stronger than $P_2$
  o $P_2$ 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.”  “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.” “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 >= 23”
- “y <= 0.23”
- “y <= 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 $P \rightarrow P^*$ for all $P$ that make the Hoare triple valid

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

\( \text{wp}(x = y \times y, x > 4) \)
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

\( \text{wp}(x = y \cdot y, x > 4) \)

\( |y| > 2 \)

\( \text{wp}(y = x+1; z = y-3, z = 10) \)

\( \text{wp}(y = x+1, \text{wp}(z = y-3, z = 10)) \)

\( \text{wp}(y = x+1, y-3 = 10) \)

\( \text{wp}(y = x+1, y = 13) \)

\( x = 12 \)
Questions