CSE 331
Software Design & Implementation

Kevin Zatloukal
Fall 2020
Lecture 2 – Reasoning About Straight-Line Code
Motivation for Reasoning

• Need a way to determine, sans computer, whether code is correct

• Most important part of the correctness techniques
  – tools, *inspection*, testing

• You need a way to do this in interviews
  – this is why interviews are done without computers

• This is not easy (see HW0)
Our Approach

• We will learn a set of formal tools for proving correctness
  – (later, this will also allow us to generate the code)

• Most professionals can do reasoning like this in their head
  – the interviewer is doing so while you write on the whiteboard
  – eventually, it will be the same for you

• Learning the formal version is useful
  – a “turn the crank” approach (no intuition required)
  – necessary for hard problems
    • we turn to formal tools when problems get too hard
Hoare Logic

- Classic approach to logical reasoning about code
  - named after its inventor, Sir Anthony Hoare
Terminology of Hoare Logic

• The *program state* is the values of all the (relevant) variables

• An *assertion* is a true / false claim (proposition) about the state at a given point during execution (e.g., on line 39)

• An assertion *holds* for a program state if the claim is true when the variables have those values

• An assertion before the code is a *precondition*  
  – these represent assumptions about when that code is used

• An assertion after the code is a *postcondition*  
  – these represent what we want the code to accomplish
Hoare Logic

• A Hoare triple is two assertions and one piece of code:

\{ P \} \ S \ { Q \}

- \( P \) the precondition
- \( S \) the code
- \( Q \) the postcondition

• A Hoare triple \( \{ P \} \ S \ { Q \} \) is called valid if:
  - in any state where \( P \) holds, executing \( S \) produces a state where \( Q \) holds
  - i.e., if \( P \) is true before \( S \), then \( Q \) must be true after it
  - otherwise the triple is called invalid
Notation

• Hoare logic writes assertions in {..}
  – since Java code also has {..}, I will use {{...}}
  – e.g., {{ w >= 1 }} x = 2 * w; {{ x >= 2 }}

• Assertions are math / logic not Java
  – you can use the usual math notation
    • (e.g., = instead of == for equals)
  – purpose is communication with other humans (not computers)
  – we will need and, or, not as well
    • can also write use \( \land \) (and) \( \lor \) (or) etc.

• The Java language also has assertions (assert statements)
  – throws an exception if the condition does not evaluate true
  – we will discuss these more later in the course
Example 1

Is the following Hoare triple valid or invalid?

- assume all variables are integers and there is no overflow

\[
\{ x \neq 0 \} \ y = x \times x; \ \{ y > 0 \}
\]
Example 1

Is the following Hoare triple valid or invalid?
   - assume all variables are integers and there is no overflow

\[
\{ \{ x \neq 0 \} \} \ y = x \times x; \ \{ \{ y > 0 \} \} 
\]

Valid
• \ y could only be zero if \ x \ were zero (which it isn’t)
Example 2

Is the following Hoare triple valid or invalid?
- assume all variables are integers and there is no overflow

\[
\{\{ z \neq 1 \}\} \ y = z*z; \ \{\{ y \neq z \}\}\]

Example 2

Is the following Hoare triple valid or invalid?

– assume all variables are integers and there is no overflow

\[
\{ \{ z \neq 1 \} \} \ y = z*z; \ \{ \{ y \neq z \} \}
\]

Invalid

• counterexample: \( z = 0 \)
Checking Validity

• So far: decided if a Hoare triple is valid by ... hard thinking

• Soon: “turn the crank” methods for reasoning about
  – assignment statements
  – conditionals
  – [next lecture] loops
  – (all code can be understood in terms of those 3 elements)

• Can use those to check correctness in a “turn the crank” manner

• Next: a way to compare different assertions
  – useful, e.g., to compare possible preconditions
Weaker vs. Stronger Assertions

If $P_1$ implies $P_2$ (written $P_1 \implies P_2$), then:

- $P_1$ is **stronger** than $P_2$
- $P_2$ is **weaker** than $P_1$

Whenever $P_1$ holds, $P_2$ also holds

- So it is more (or at least as) “difficult” to satisfy $P_1$
  - the program states where $P_1$ holds are a subset of the program states where $P_2$ holds
- So $P_1$ puts more constraints on program states
- So it is a stronger set of requirements on the program state
  - $P_1$ gives you more information about the state than $P_2$
Examples

• $x = 17$ is stronger than $x > 0$

• $x$ is prime is neither stronger nor weaker than $x$ is odd

• $x$ is prime and $x > 2$ is stronger than $x$ is odd
Hoare Logic Facts

• Suppose \( \{P\} S \{Q\} \) is valid.

• If \( P_1 \) is stronger than \( P \), then \( \{P_1\} S \{Q\} \) is valid.

• If \( Q_1 \) is weaker than \( Q \), then \( \{P\} S \{Q_1\} \) is valid.

• Example:
  – Suppose \( P \) is \( x \geq 0 \) and \( P_1 \) is \( x > 0 \)
  – Suppose \( Q \) is \( y > 0 \) and \( Q_1 \) is \( y \geq 0 \)
  – Since \( \{\begin{array}{c}
  x \geq 0 \\
  \end{array}\} y = x+1 \{\begin{array}{c}
  y > 0 \\
  \end{array}\} \) is valid,
    \( \{\begin{array}{c}
  x > 0 \\
  \end{array}\} y = x+1 \{\begin{array}{c}
  y \geq 0 \\
  \end{array}\} \) is also valid
Hoare Logic Facts

- Suppose \{P\} \mathcal{S} \{Q\} is valid.

- If \(P_1\) is stronger than \(P\), then \{\(P_1\)\} \mathcal{S} \{Q\} is valid.

- If \(Q_1\) is weaker than \(Q\), then \{P\} \mathcal{S} \{Q_1\} is valid.

- **Key points:**
  - always okay to **strengthen** a **precondition**
  - always okay to **weaken** a **postcondition**
Forward & Backward Reasoning
Example of Forward Reasoning

Work forward from the precondition

\[ \{ w > 0 \} \]
\[ x = 17; \]
\[ \{ \quad \} \]
\[ y = 42; \]
\[ \{ \quad \} \]
\[ z = w + x + y; \]
\[ \{ \quad \} \]
Example of Forward Reasoning

Work forward from the precondition

$$\{ w > 0 \}$$

$$x = 17;$$

$$\{ w > 0 \text{ and } x = 17 \}$$

$$y = 42;$$

$$\{ \text{_______________________________} \}$$

$$z = w + x + y;$$

$$\{ \text{_______________________________} \}$$
Example of Forward Reasoning

Work forward from the precondition

```plaintext
{{ w > 0 }}
  x = 17;
{{ w > 0 and x = 17 }}
  y = 42;
{{ w > 0 and x = 17 and y = 42 }}
  z = w + x + y;
{{ ________________________________ }}
```
Example of Forward Reasoning

Work forward from the precondition

\[
\begin{align*}
\{ &\ w > 0 \} \\
\ &\ x = 17; \\
\{ &\ w > 0 \ \text{and} \ x = 17 \} \\
\ &\ y = 42; \\
\{ &\ w > 0 \ \text{and} \ x = 17 \ \text{and} \ y = 42 \} \\
\ &\ z = w + x + y; \\
\{ &\ w > 0 \ \text{and} \ x = 17 \ \text{and} \ y = 42 \ \text{and} \ z = w + x + y \}
\end{align*}
\]
Example of Forward Reasoning

Work forward from the precondition

\( \{ w > 0 \} \)

\( x = 17; \)

\( \{ w > 0 \text{ and } x = 17 \} \)

\( y = 42; \)

\( \{ w > 0 \text{ and } x = 17 \text{ and } y = 42 \} \)

\( z = w + x + y; \)

\( \{ w > 0 \text{ and } x = 17 \text{ and } y = 42 \text{ and } z = w + 59 \} \)
Forward Reasoning

• Start with the given precondition
• Fill in the strongest postcondition

• For an assignment, \( x = y \)...
  – add the fact “\( x = y \)” to what is known
  – important subtleties here... (more on those later)

• Later: if statements and loops...
Example of Backward Reasoning

Work backward from the desired postcondition

\[
\begin{align*}
\{ & \text{_____________________________} \} \\
\ x = 17; \\
\{ & \text{_____________________________} \} \\
\ y = 42; \\
\{ & \text{_____________________________} \} \\
\ z = w + x + y; \\
\{ & z < 0 \}
\end{align*}
\]
Example of Backward Reasoning

Work backward from the desired postcondition

\{ w + x + y < 0 \}

\begin{align*}
  x &= 17; \\
  y &= 42; \\
  z &= w + x + y;
\end{align*}

\{ z < 0 \}
Example of Backward Reasoning

Work backward from the desired postcondition

\{\{ \text{______________________________} \}\}

\text{x = 17;}
\{\{ w + x + 42 < 0 \}\}
\text{y = 42;}
\{\{ w + x + y < 0 \}\}
\text{z = w + x + y;}
\{\{ z < 0 \}\}
Example of Backward Reasoning

Work backward from the desired postcondition

\[ \{ \{ w + 17 + 42 < 0 \} \} \]
\[ x = 17; \]
\[ \{ \{ w + x + 42 < 0 \} \} \]
\[ y = 42; \]
\[ \{ \{ w + x + y < 0 \} \} \]
\[ z = w + x + y; \]
\[ \{ z < 0 \} \]
Backward Reasoning

• Start with the **required** postcondition
• Fill in the **weakest** precondition

• For an assignment, \( x = y \):
  – just replace “\( x \)” with “\( y \)” in the postcondition
  – if the condition using “\( y \)” holds beforehand, then the condition with “\( x \)” will afterward since \( x = y \) then

• Later: if statements and loops...
Use forward reasoning to determine if this code is correct:

```plaintext
{{ w > 0 }}
  x = 17;
  y = 42;
  z = w + x + y;
{{ z > 50 }}
```
Example of Forward Reasoning

\[
\begin{align*}
\{ & \ w > 0 \ \} \\
\ & \ x = 17;  \\
\{ & \ w > 0 \ \text{and} \ x=17 \ \} \\
\ & \ y = 42;  \\
\{ & \ w > 0 \ \text{and} \ x=17 \ \text{and} \ y=42 \ \} \\
\ & \ z = w + x + y;  \\
\{ & \ w > 0 \ \text{and} \ x=17 \ \text{and} \ y=42 \ \text{and} \ z = w + 59 \ \}  \\
\{ & \ z > 50 \ \}\end{align*}
\]

Do the facts that are always true imply the facts we need?  
I.e., is the bottom statement weaker than the top one?

(Recall that weakening the postcondition is always okay.)
Use backward reasoning to determine if this code is correct:

\[
\begin{align*}
\{ & w < -60 \} \\
& x = 17; \\
& y = 42; \\
& z = w + x + y; \\
\{ & z < 0 \}
\end{align*}
\]
Correctness by Backward Reasoning

Use backward reasoning to determine if this code is correct:

\[ \{ w < -60 \}\]

\[ \{ w + 17 + 42 < 0 \} \iff \{ w < -59 \}\]
\( x = 17; \)

\[ \{ w + x + 42 < 0 \}\]
\( y = 42; \)

\[ \{ w + x + y < 0 \}\]
\( z = w + x + y; \)

\[ \{ z < 0 \}\]

Do the facts that are always true imply the facts we need? I.e., is the top statement stronger than the bottom one? (Recall that strengthening the precondition is always okay.)
Combining Forward & Backward

It is okay to use both types of reasoning

- Reason forward from precondition
- Reason backward from postcondition

Will meet in the middle:

\[
\{\{ P \}\} \\
S1 \\
S2 \\
\{\{ Q \}\}
\]
Combining Forward & Backward

It is okay to use both types of reasoning
  • Reason forward from precondition
  • Reason backward from postcondition

Will meet in the middle:

\[
\begin{align*}
\{\{ P \}\} \\
S1 \\
\{\{ P1 \}\} \\
\{\{ Q1 \}\} \\
S2 \\
\{\{ Q \}\}
\end{align*}
\]

Valid provided \( P1 \) implies \( Q1 \)
Combining Forward & Backward

Reasoning in either direction gives valid assertions
Just need to check adjacent assertions:
• top assertion must imply bottom one

\[
\begin{align*}
\{P\} & \quad \{Q\} \\
S1 & \quad S2 \\
\{P1\} & \quad \{Q1\} \\
\{Q\} & \quad \{Q\}
\end{align*}
\]
Subtleties in Forward Reasoning...

- Forward reasoning can **fail** if applied blindly...

```plaintext
{{ }}
  w = x + y;
{{ w = x + y }}
  x = 4;
{{ w = x + y and x = 4 }}
  y = 3;
{{ w = x + y and x = 4 and y = 3 }}
```

This implies that \( w = 7 \), but that is not true!
- \( w \) equals whatever \( x + y \) was **before** they were changed
Fix 1

- Use **subscripts** to refer to old values of the variables
- Un-subscripted variables should always mean **current** value

```plaintext
case w = x + y;
{{ w = x + y }}
  x = 4;
{{ w = x₁ + y and x = 4 }}
  y = 3;
{{ w = x₁ + y₁ and x = 4 and y = 3 }}
```
Fix 2 (better)

- Express prior values in terms of the current value

```latex
\begin{align*}
\{ & \} \\
&w = x + y; \\
\{ & w = x + y \} \\
&x = x + 4; \\
\{ & w = x_1 + y \text{ and } x = x_1 + 4 \} \quad \text{Now, } x_1 = x - 4 \\
\Rightarrow & \{ w = x - 4 + y \} \quad \text{So } w = x_1 + y \iff w = x - 4 + y
\end{align*}
```

Note for updating variables, e.g., $x = x + 4$:

- Backward reasoning just substitutes new value (no change)
- Forward reasoning requires you to invert the “+” operation
Forward vs. Backward

- **Forward reasoning:**
  - Find strongest postcondition
  - Intuitive: “simulate” the code in your head
    - BUT you need to change facts to refer to *prior values*
  - Inefficient: Introduces many irrelevant facts
    - usually need to weaken as you go to keep things sane

- **Backward reasoning**
  - Find weakest precondition
  - Formally simpler
  - Efficient
  - (Initially) unintuitive
If Statements
If Statements

Forward reasoning

{{ P }}
if (cond)
  S1
else
  S2
{{ ? }}
If Statements

Forward reasoning

```
{{ P }}
if (cond)
   {{ P and cond }}
   S1
else
   {{ P and not cond }}
   S2
{{ ? }}
```
If Statements

Forward reasoning

{{ P }}
if (cond)
    {{ P and cond }}
    S1
    {{ P1 }}
else
    {{ P and not cond }}
    S2
    {{ P2 }}
{{ ? }}
If Statements

Forward reasoning

```
{{ P }}
if (cond)
    {{ P and cond }}
    S1
else
    {{ P1 }}
    {{ P1 or P2 }}
    S2
```
If Statements

Backward reasoning

{{ ? }}
if (cond)
  S1
else
  S2
{{ Q }}
Backward reasoning

```{?}
if (cond)
  S1
else
  S2
```

```{Q}```

```{Q}```
If Statements

Backward reasoning

```plaintext
{{ ? }}
if (cond)
  {{ Q1 }}
  S1
  {{ Q }}
else
  {{ Q2 }}
  S2
  {{ Q }}
{{ Q }}
```
If Statements

Backward reasoning

\[
\begin{align*}
\{
\text{cond and Q1 or not cond and Q2}
\} \\
\text{if (cond)} \\
\{{\text{Q1}}\} \\
S1 \\
{{\text{Q}}} \\
\text{else} \\
\{{\text{Q2}}\} \\
S2 \\
{{\text{Q}}} \\
{{\text{Q}}}
\end{align*}
\]
If-Statement Example

Forward reasoning

```java
{{ }}
if (x >= 0)
    y = x;
else
    y = -x;
{{ ? }}
```
If-Statement Example

Forward reasoning

```
{{ }}
if (x >= 0)
    {{ x >= 0 }}
    y = x;
else
    {{ x < 0 }}
    y = -x;
{{ ? }}
```
If-Statement Example

Forward reasoning

```latex
\{\{ \}\}
if (x \geq 0)
\{\{ x \geq 0 \}\}
y = x;
\{\{ x \geq 0 \text{ and } y = x \}\}
else
\{\{ x < 0 \}\}
y = -x;
\{\{ x < 0 \text{ and } y = -x \}\}
\{\{ ? \}\}
```
If-Statement Example

Forward reasoning

```plaintext
if (x >= 0)
   y = x;
else
   y = -x;
```

```plaintext
(x >= 0 and y = x) or
(x < 0 and y = -x)
```
If-Statement Example

Forward reasoning

```c
{{ }}
if (x >= 0)
    {{ x >= 0 }}
    y = x;
    {{ x >= 0 and y = x }}
else
    {{ x < 0 }}
    y = -x;
    {{ x < 0 and y = -x }}
{{ y = |x| }}
```
If-Statement Example

Forward reasoning

```{eq}
if (x >= 0) 
  {eq x >= 0 } 
  y = x; 
  {eq x >= 0 and y = x } 
else 
  {eq x < 0 } 
  y = -x; 
  {eq x < 0 and y = -x } 
{eq y = |x| }
```

**Warning:** many write `{eq y >= 0 }` here
That is true but it is *strictly* weaker.
(It includes cases where y != x)
If-Statement Example

Forward reasoning

```latex
\{{ \}}
\begin{align*}
&\text{if } (x \geq 0) \\
&\quad \{{ x \geq 0 \}} \\
&\quad y = x; \\
&\quad \{{ x \geq 0 \text{ and } y = x \}} \\
&\text{else} \\
&\quad \{{ x < 0 \}} \\
&\quad y = -x; \\
&\quad \{{ x < 0 \text{ and } y = -x \}} \\
&\{{ y = |x| \}}
\end{align*}
```

Backward reasoning

```latex
\{{ ? \}}
\begin{align*}
&\text{if } (x \geq 0) \\
&\quad y = x; \\
&\text{else} \\
&\quad y = -x; \\
&\{{ y = |x| \}}
\end{align*}
```
If-Statement Example

Forward reasoning

{{ }}
if (x >= 0)
{{ x >= 0 }}
y = x;
{{ x >= 0 and y = x }}
else
{{ x < 0 }}
y = -x;
{{ x < 0 and y = -x }}
{{ y = |x| }}

Backward reasoning

{{ ? }}
if (x >= 0)
y = x;
{{ y = |x| }}
else
y = -x;
{{ y = |x| }}
{{ y = |x| }}
If-Statement Example

Forward reasoning

```plaintext
{{ }}
if (x >= 0)
  {{ x >= 0 }}
y = x;
  {{ x >= 0 and y = x }}
else
  {{ x < 0 }}
y = -x;
  {{ x < 0 and y = -x }}
{{ y = |x| }}
```

Backward reasoning

```plaintext
{{ ? }}
if (x >= 0)
  {{ x = |x| }}
y = x;
  {{ y = |x| }}
else
  {{ -x = |x| }}
y = -x;
  {{ y = |x| }}
{{ y = |x| }}
```
If-Statement Example

Forward reasoning

```latex
\{\} \\
\text{if } (x \geq 0) \\
\quad \{\ x \geq 0 \} \\
\quad y = x; \\
\quad \{\ x \geq 0 \text{ and } y = x \} \\
\text{else} \\
\quad \{\ x < 0 \} \\
\quad y = -x; \\
\quad \{\ x < 0 \text{ and } y = -x \} \\
\{\ y = |x| \}
```

Backward reasoning

```latex
\{\ ? \} \\
\text{if } (x \geq 0) \\
\quad \{\ x \geq 0 \} \\
\quad y = x; \\
\quad \{\ y = |x| \} \\
\text{else} \\
\quad \{\ x \leq 0 \} \\
\quad y = -x; \\
\quad \{\ y = |x| \} \\
\{\ y = |x| \}
```
If-Statement Example

Forward reasoning

\[
\begin{align*}
\{&\} \\
\text{if } (x \geq 0) & \{\{ x \geq 0 \}\} \\
& \{\{ x \geq 0 \text{ and } y = x \}\} \\
\text{else} & \{\{ x < 0 \}\} \\
& \{\{ x < 0 \text{ and } y = -x \}\} \\
& \{\{ y = |x| \}\}
\end{align*}
\]

Backward reasoning

\[
\begin{align*}
\{&\} \\
\text{if } (x \geq 0) & \{\{ x \geq 0 \}\} \\
& \{\{ y = |x| \}\} \\
\text{else} & \{\{ x \leq 0 \}\} \\
& \{\{ y = |x| \}\}
\end{align*}
\]
If-Statement Example

Forward reasoning

\[
\begin{align*}
\{ & \} \\
\text{if } (x \geq 0) \\
\quad \{ & \} \\
\quad y &= x; \\
\quad \{ & x \geq 0 \text{ and } y = x \} \\
\text{else} \\
\quad \{ & \} \\
\quad y &= -x; \\
\quad \{ & x < 0 \text{ and } y = -x \} \\
\{ & y = |x| \}
\end{align*}
\]

Backward reasoning

\[
\begin{align*}
\{ & x \geq 0 \text{ or } x < 0 \} \\
\text{if } (x \geq 0) \\
\quad \{ & \} \\
\quad y &= x; \\
\quad \{ & y = |x| \} \\
\text{else} \\
\quad \{ & \} \\
\quad y &= -x; \\
\quad \{ & y = |x| \} \\
\{ & y = |x| \}
\end{align*}
\]
If-Statement Example

Forward reasoning

```{}
if (x >= 0)
    {{ x >= 0 }}
y = x;
    {{ x >= 0 and y = x }}
else
    {{ x < 0 }}
y = -x;
    {{ x < 0 and y = -x }}
{{ y = |x| }}
```

Backward reasoning

```{}
if (x >= 0)
    {{ x >= 0 }}
y = x;
    {{ y = |x| }}
else
    {{ x <= 0 }}
y = -x;
    {{ y = |x| }}
{{ y = |x| }}
```
Next time: Loops...