Section 1: Code Reasoning

Bryan Van Draanen

Fall 2017

General staff email: cse331-staff@cs.washington.edu

My email: bryanvd@cs.washington.edu

Grading TA email: waylonh@cs.washington.edu

Introduction to code reasoning

- Determine what *facts* are true at each line of the program
- Accomplish two major goals:
  - Prove code is correct
  - Understand what your code is doing
- Essential for creating high quality and high complexity programs

Reasoning Techniques

- Forward Reasoning – determine what assertions follow from initial conditions
- Backward Reasoning – determine sufficient conditions which make a specific result true

Forward Reasoning Example 1

Suppose we know initially that: `i >= 2`
We want to ensure `z > 1` by the end

```
x = i * 2;
   // x = i * 2 and i >= 2
y = x;
   // y = x and x = i * 2 and i >= 2
z = (x + y) / 2;
   // z = (x + y) / 2 and i >= 2 and x = i * 2 and y = x
   // z = (i * 2 + i * 2) / 2 = i * 2
   // z >= 2 * 2 = 4
```

Since we can imply that `z >= 4` by the end, it follows that `z > 1` as well

Forward Reasoning Example 2

Suppose $x >= 1$ **and** $y >= 1$

We want to see what possible values z evaluates to by the end

```
x = x + y;
   // x1 = x0 + y and x0 >= 1 and y >= 1
y = 20;
   // y1 = 20 and y0 >= 1 and x1 = x0 + y0 and x0 >= 1
z = y - x;
   // z = y1 - x1 and y1 = 20 and x1 = x0 + y0 and y0 >= 1 and x0 >= 1
➡ // z = 20 - x1 and x1 >= 1 + 1 = 2
➡ // z <= 20 - 2 = 18
```

The possible values of z are all integers less than or equal to 18

Forward Reasoning Example 3

Suppose `x != 0 and w >= 3`

We want to know what values `z` is greater than or equal to by the end

```
q = w / 2;
   // q >= 1 and x != 0 and w >= 3
y = x * x;
   // q >= 1 and y > 0 and x != 0 and w >= 3
z = q * y;
   // z = q * y and q >= 1 and y > 0 and x != 0 and w >= 3
→  // z >= 1 * 1 = 1
```

`z` is greater than or equal to 1

Backward Reasoning Example 1

Suppose we want to show that `z >= 6` by the end

What needs to be true about `i`?

```
   // i * 4 >= 8 or equivalently i >= 2
x = i * 4;
   // x + 4 >= 12 or equivalently x >= 8
i = x + 4;
   // i / 2 >= 6 or equivalently i >= 12
z = i / 2;
   // z >= 6
```

Backward Reasoning Example 2

Suppose we want to show that `z <= 10` by the end

What needs to be true about **`x`** and **`y`**?

```
   // x + y >= 10
x = x + y;
   // 20 - x <= 10 or equivalently x >= 10
y = 20;
   // y - x <= 10
z = y - x;
   // z <= 10
```

Backward Reasoning Example 3

Suppose we want to show that `x > 0` by the end

What needs to be true initially?

```
   // x + 3 * c > 4
a = x + c
   // a + 2 * c > 4
b = 2 * c - 4
   // a + b > 0
x = a + b
   // x > 0
```

Worksheet

- 20 Minutes – Get as far as you can and don’t worry if you get stuck!
- Feel free to collaborate with other students and ask me questions
- Go over solutions in slides after

Forward Reasoning Solutions

Worksheet – Problem 1

What is the value of `z` by the end in terms of `x` and `y`?

```
   // x > 0 and y > 0
w = x * y;
   // w = x * y and x > 0 and y > 0
q = x * x;
   // q = x * x and w = x * y and x > 0 and y > 0
z = w / q;
   // z = y/x and x > 0 and y > 0
```

Worksheet – Problem 2

What are the possible values of `z` by the end of the code?

```
   // x >= 0 and y >= 0
y = 25;
   // y = 25 and x >= 0
x = x + y;
   // x >= 25 and y = 25
x = sqrt(x);
   // x >= 5 and y = 25
z = y - x;
   // z <= 20
```

Worksheet – Problem 3

What are the possible values for `z` by the end?

```
   // x != 0 and y < 0
z = x * x;
   // z > 0 and x != 0 and y < 0
z = z * y;
   // z < 0 and x != 0 and y < 0
z = z * x;
   // z > 0 or z < 0
   // z != 0
```

Backward Reasoning Solutions

Worksheet – Problem 4

What are the sufficient conditions to ensure `z != -1` by the end?

```
   // y != -2 and y != -3
x = y / 2;
   // x != -1
z = x * 2;
   // z != -2
z = z + 1;
   // z != -1
```

Worksheet – Problem 5

What must be true initially for `y > 20` by the end?

```
   // x < 1
x = 1 - x;
   // x > 0
x = x + 10;
   // x > 10
y = 2 * x;
   // y > 20
```

Worksheet – Problem 6

What must be true initially for `x > y` and `y > z` by the end?

```
   // a < 4 and b < -a
b = -b;
   // a < 4 and b > a
z = a * 2;
   // a < 4 and a + b > z
x = b + 4
   // x > a + b and a + b > z
y = a + b;
   // x > y and y > z
```

Conditional Reasoning (Forward)

What are the possible values of `z` after the if statement?

```
   // y = 5
if (x < 0) {
      // y = 5 and x < 0
   z = x - y + 1;
      // z <= -5
}
else {
      // y = 5 and x >= 0
   z = x + y;
      // z >= 5
}
   // z >= 5 or z <= -5
```

Conditional Reasoning (Backward)

What must be true initially to ensure `z = 0` at the end?

```
   // (bCondition and a + b = 0) or (!bCondition and x + y = 0)
if (bCondition) {
      // a + b = 0
   z = a + b;
      // z = 0
}
else {
      // x + y = 0
   z = x + y;
      // z = 0
}
   // z = 0
```

Conditional Reasoning Solution

Worksheet – Problem 7 (Forward Reasoning)

Prove that the following code calculates the absolute value of `x`

```
    // true
if (x > 0) {
       // x > 0
    abs = x;
       // x > 0 and abs = x
}
else {
       // x <= 0
    abs = -x;
       // x <= 0 and abs = -x
}
    // (x > 0 and abs = x) or (x <= 0 and abs = -x)
    // abs = |x|
```