PSOFT HW 1

Brian Wang-Chen

January 2024

Problems

Problem 1 (12 pts., 2 pts. each): Condition Strength

Order conditions from **the strongest to the weakest** by showing the longest implication chain of the form A $\rightarrow$ B $\rightarrow$ C $\rightarrow$ D ... (where A, B, C, D, ... are given conditions, $\rightarrow$ is implication). If total ordering by strength cannot be established, show all partial orderings. Prove by showing all implications. If any implication is false, provide a counterexample. You must show all work in order to get full credit. Unless otherwise stated, assume all referenced variables are defined as integers.

(1) A = { x = 2k + 1 $\wedge$ x = x + 1 $\wedge$ y = 10 }
B = { x is divisible by 6 $\wedge$ y = x + 2 }
C = { x = 18 $\wedge$ y = 20 }
D = { x % 2 = 0 $\wedge$ y is even }

Implication Chain: $(A) \rightarrow (C) \rightarrow (B) \rightarrow (D)$
Proof of implication:

- (**A**) $\rightarrow$ (**C**) True
- (**C**) $\rightarrow$ (**A**) False, x = 18, x = x + 1, 18 = 18 + 1
- (**C**) $\rightarrow$ (**B**) True
- (**B**) $\rightarrow$ (**C**) False, x = 12, divisible by 6, but contradicts x = 18
- (**B**) $\rightarrow$ (**D**) True
- (**D**) $\rightarrow$ (**B**) False, x = 4, 4 % 2 = 0, not divisible by 6

(2) A = { 5 $\leq$ k < 5 }
B = { k $\geq$ -10 }
C = { -10 < k $\leq$ 1 }
D = { 10 $\leq$ k $\leq$ -10 }

Implication Chain: $(A) \rightarrow (D) \rightarrow (C) \rightarrow (B)$
Proof of implications:

- (**A**) $\rightarrow$ (**D**) True

- (**D**) $\rightarrow$ (**A**) True
- (**C**) $\rightarrow$ (**B**) True
- (**B**) $\rightarrow$ (**C**) False, $k = -10, -10 < -10 \leq 1$
- (**D**) $\rightarrow$ (**C**) True
- (**C**) $\rightarrow$ (**D**) False, $k = 1, 10 \leq 1 \leq -10$

(3) A = { x $\geq$ 0 $\wedge$ y > x }
B = { x = 3 $\wedge$ y > 10 }
C = { x = y % 10 }
D = { xy = 0 }
E = { x > 1 $\vee$ y > 1 }

Implication Chain: $(B) \rightarrow (E)$
or (Both Works)
Implication Chain: $(B) \rightarrow (A)$
Proof of implication:

- (**B**) $\rightarrow$ (**E**) True
- (**E**) $\rightarrow$ (**B**) False, x = 2 contradicts x = 3
- (**B**) $\rightarrow$ (**A**) True
- (**A**) $\rightarrow$ (**B**) False, x = 0 contradicts x = 3
- Excluded conditions: C, D
- (**C**) $\rightarrow$ (**B**) False, $x = 4$
- (**C**) $\rightarrow$ (**E**) False, $x = 1, 1 > 1$
- (**C**) $\rightarrow$ (**A**) False, $x = 3, y = 2, 2 > 3$
- (**B**) $\rightarrow$ (**C**) False, $x = 3, y = 11, 3 = 11\%10$
- (**E**) $\rightarrow$ (**C**) False, $x = 3, y = 2, 3 = 2\%10$
- (**A**) $\rightarrow$ (**C**) False, $x = 0, y = 2, 2 = 2\%10$
- (**D**) $\rightarrow$ (**B**) False, x = 0, contradicts x = 3
- (**D**) $\rightarrow$ (**E**) False, $x = 0, 0 > 1$
- (**D**) $\rightarrow$ (**A**) False, $x = 3, y = 0, 0 > 3$
- (**B**) $\rightarrow$ (**D**) False, $x = 3, y = 11, (3)(11) = 0$
- (**E**) $\rightarrow$ (**D**) False, $x = 2, y = 2, (2)(2) = 0$
- (**A**) $\rightarrow$ (**D**) False, $x = 1, y = 2, (1)(2) = 0$

(4) Recall the names for infinite sets of numbers used in math (e.g., see "Peter Jephson Cameron (1998). *Introduction to Algebra*. Oxford University Press. p. 4. ISBN 978-0-19-850195-4.")
A = { z $\in \mathbb{Q}$ }
B = { z = $\sqrt{-1}$ }
C = { z $\in \mathbb{N}$ }
D = { z = m / n }
E = { z $\in \mathbb{Z}$ }
F = { z = y % 2 }
G = { z $\in \mathbb{R}$ }
H = { z = y / 2 }

4 possible:
Implication Chain: $(B) \rightarrow (D) \rightarrow (E) \rightarrow (A) \rightarrow (G)$
Implication Chain: $(B) \rightarrow (F) \rightarrow (E) \rightarrow (A) \rightarrow (G)$
Implication Chain: $(B) \rightarrow (H) \rightarrow (E) \rightarrow (A) \rightarrow (G)$
Implication Chain: $(B) \rightarrow (C) \rightarrow (E) \rightarrow (A) \rightarrow (G)$
Proof of implication:

- (**B**) → (**D**) True
- (**D**) → (**B**) False, z = 1/1, not irrational like $\sqrt{-1}$
- (**B**) → (**F**) True
- (**F**) → (**B**) False, z = 4 % 2 = 0, not irrational like $\sqrt{-1}$
- (**B**) → (**H**) True
- (**H**) → (**B**) False, z = 4 / 2 = 2, not irrational like $\sqrt{-1}$
- (**B**) → (**C**) True
- (**C**) → (**B**) False, z = 1, natural number not irrational
- Prove D,F,H,C are all implied by B, but they do not imply each other:
- (**D**) → (**F**) False, z = 2/0, Error, F will not error
- (**D**) → (**H**) False, z = 2/0, Error, H will not error, not dividing by 0
- (**D**) → (**C**) False, z = 2/0, Error, C is natural numbers
- (**F**) → (**D**) False, z = 0 % 2 = 0, D will error when dividing by zero
- (**H**) → (**D**) False, z = 0 / 2 = 0, D will error when dividing by zero
- (**C**) → (**D**) False, z = 1 (natural), D will error when dividing by zero
- (**F**) → (**H**) False, y = 2, 2 % 2 = 0, 2/2 = 1
- (**F**) → (**C**) False, F = 2 % 2 = 0, C (Natural set) does not contain 0
- (**H**) → (**F**) False, y = 2, 2 % 2 = 0, 2/2 = 1

- (**C**) $\rightarrow$ (**F**) False, C = 1 (natural), F = 0 % 2 = 0 not in natural set
- (**H**) $\rightarrow$ (**C**) False, H = 0 / 2 = 0, not in natural set
- (**C**) $\rightarrow$ (**H**) False, H = 1, H = 0/2 = 0, not in natural set
- Prove E,A,G all imply each other:
- (**E**) $\leftrightarrow$ (**A**) $\leftrightarrow$ (**G**) True because since we are assuming z is a integer, A is a integer ignoring rational numbers like fraction, E is integers already, and G is only the integers from the Real numbers set since we are assuming z is a integer. Therefore they all imply each other.
- Since E,A,G all imply each other we just have to prove each of D,F,H,C to imply to E and backwards. We have previously proven D,F,H,C to all be integers.
- (**D**) $\rightarrow$ (**E**) True
- (**E**) $\rightarrow$ (**D**) True
- (**F**) $\rightarrow$ (**E**) True
- (**E**) $\rightarrow$ (**F**) True
- (**H**) $\rightarrow$ (**E**) True
- (**E**) $\rightarrow$ (**H**) True
- (**C**) $\rightarrow$ (**E**) True
- (**E**) $\rightarrow$ (**C**) True

...

(5) A = { -7 < x < 0 }
B = { y = log(x) }
C = { -5 < x $\leq$ 10 }
D = { x = 1 $\land$ y $\geq$ 1 }
E = { -1 $\leq$ x $\leq$ 1 }

Implication Chain: $(D) \rightarrow (E) \rightarrow (C)$
Proof of implication:

- (**D**) $\rightarrow$ (**E**) True
- (**E**) $\rightarrow$ (**D**) False, x = -1 contradicts x = 1
- (**E**) $\rightarrow$ (**C**) True
- (**C**) $\rightarrow$ (**E**) False, $x = -4, -1 \leq -4 \leq 1$
- Excluded Conditions: A, B
- (**A**) $\rightarrow$ (**D**) False, x = -6 contradicts x = 1
- (**A**) $\rightarrow$ (**E**) False, $x = -2, -1 \leq -2 \leq 1$

- **(A)** $\rightarrow$ **(C)** False, $x = -6, -5 < -6 \leq 10$
- **(D)** $\rightarrow$ **(A)** False, $x = 1, -7 < 1 < 0$
- **(E)** $\rightarrow$ **(A)** False, $x = 1, -7 < 1 < 0$
- **(C)** $\rightarrow$ **(A)** False, $x = 2, -7 < 2 < 0$
- **(B)** $\rightarrow$ **(D)** False, $y = 0, 0 \geq 1$
- **(B)** $\rightarrow$ **(E)** False, y = logx no relation to -1 $\leq$ x $\leq$ 1
- **(B)** $\rightarrow$ **(C)** False, y = logx no relation to -5 $< x \leq$ 10
- **(D)** $\rightarrow$ **(B)** False, $x = 1, y = log(1), 0 \geq 1$
- **(E)** $\rightarrow$ **(B)** False, $x = -1, y = log(-1)$
- **(C)** $\rightarrow$ **(B)** False, $x = -4, y = log(-4)$

(6) `Assume "result is a double" and` $|\cdot|$ `is the absolute value operator.`

A = { `|result - sin(x)|` $\leq$ 1 }
B = { `|result - sin(x)|` $\leq$ 0.01 }
C = { `|result - sin(x)|` $\leq 10^{-10}$ }
D = { `|result - sin(x)|` $\leq$ -0.01 } = { false }
E = { `|result - sin(x)|` $\geq x^2$ }

Implication Chain: $(D) \rightarrow (C) \rightarrow (B) \rightarrow (A)$
Proof of implication:

- **(D)** $\rightarrow$ **(C)** True
- **(C)** $\rightarrow$ **(D)** False, $|result - sinx| = 10^{-11}$
- **(C)** $\rightarrow$ **(B)** True
- **(B)** $\rightarrow$ **(c)** False, $|result - sinx| = 10^{-9}$
- **(B)** $\rightarrow$ **(A)** True
- **(A)** $\rightarrow$ **(B)** False, $|result - sinx| = 0.5$
- Excluded Conditions: E
- **(E)** $\rightarrow$ **(D)** False, $result = x^2 + 0.01, x^2 + 0.01 - sinx \leq -0.01$
- **(E)** $\rightarrow$ **(C)** False, $result = x^2 + 10^{-9}, x^2 + 10^{-9} - sinx \leq 10^{-10}$
- **(E)** $\rightarrow$ **(B)** False, $result = x^2 + 0.1, x^2 + 0.1 - sinx \leq 0.01$
- **(E)** $\rightarrow$ **(A)** False, $result = x^2 + 2, x^2 + 2 - sinx \leq 1$
- **(D)** $\rightarrow$ **(E)** False, $result = sinx - 0.02, sinx - 0.02 - sinx \geq x^2$
- **(C)** $\rightarrow$ **(E)** False, $result = sinx + 10^{-11}, sinx + 10^{-11} - sinx \geq x^2$
- **(B)** $\rightarrow$ **(E)** False, $result = sinx + 0.005, sinx + 0.005 - sinx \geq x^2$

- **(A)** $\rightarrow$ **(E)** False, $result = sinx + 0.5, sinx + 0.5 - sinx \geq x^2$

Problem 2 (4 pts., 1 pt. each): Hoare Triples

State whether each Hoare triple is valid. If it is invalid, explain why and show how you would modify the the postcondition to make it valid. Unless otherwise stated, assume all referenced variables are defined as integers.

(1) { x = 5 }

```
x = x * 2;
```

{ x = 10 $\vee$ x $\neq$ 0}

Valid or Invalid: Valid because x = 5 * 2 which is 10 satisfying the post condition x = 10.

(2) { $\sqrt{x-1}$ > k }

```
x = x + 1;
```

{ k $\geq$ 0}

Valid or Invalid: Invalid because there is no guaranteed for the post condition to be met even if the precondition is met since K is not modified. A example of this would be if k was a negative number, like -2 which in this case -2 ¿= 0, fails the post condition. Therefore the post condition is not guaranteed, to make it valid, change the post condition to x > 1 because x has to be greater than 1 since the smallest number x can be is 1 and the code section increments x by 1.

(3) { i + j $\neq$ 0 $\wedge$ i $\cdot$ j $\neq$ 0}

```
i = j - 1;
j = i + 1;
```

{ (i = 0 $\vee$ i $\neq$ -j) $\wedge$ k $\in \mathbb{Q}$ }

Valid or Invalid: Valid because i and j both cannot be zero since i x j cannot equal zero nor can they be opposites of each other according to the precondition. The post condition therefore will be satisfied since i $\neq$ -j will always be true and we can assume K is always rational since it is a integer.

(4) { n < 0 $\wedge$ n = $\sqrt{m}$ }

```
if (n > m)
  x = n;
else
  y = m;
```

{ x $\neq$ y }

Valid or Invalid: Valid because although the precondition is not satisfied that also means the post condition is not guaranteed. Therefore there no way to prove that if the precondition is true then the post condition can't meet it.

Problem 3 (4 pts., 1 pt. each): General Hoare Triples

A, B, C, D, E, and F are logical conditions (logical formulas). The following are true:

- A $\rightarrow$ B (A implies B, i.e., A is stronger than B)
- B $\rightarrow$ C
- C $\rightarrow$ B
- D $\rightarrow$ E
- E $\rightarrow$ F
- { B } code { E }

Indicate whether the following Hoare triples are valid or possibly invalid. If possibly invalid, prove by giving an example.

(1) {C} `code` {D} Valid or Possibly Invalid: Possibly invalid because the post condition is is not guaranteed since D implies E but not the other way around. D is is a subset within E so not everything in D will be within E which.

(2) {B} `code` {C} Valid or Possibly Invalid: Possibly invalid because the post condition is not guaranteed since E and C have no relation. E does not imply C nor does C imply E.

(3) {A} `code` {D} Valid or Possibly Invalid: Valid because A implies B meaning A is a subset of B and D implies E meaning B is a subset of D.

(4) {A} `code` {F} Valid or Possibly Invalid: Possibly Invalid because E implies F, so not everything in set of F is within set E, so the post condition is not guaranteed.

Problem 4 (8 pts., 1 pt. for each condition): Forward reasoning

For each code snippet with the given precondition, find the **strongest postcondition** by inserting the appropriate condition in each blank. The first intermediate condition in part (1) is supplied as an example. Please simplify your answers as much as possible. Assume all referenced variables are defined as integers.

Copy all code to your answer file and fill in the blanks. Carry all variables forward. Show all work.

(1) { $z \neq 0$ }

```
y = 0;
    { y = 0 ∧ z ≠ 0}
x = y + 2;
```

{ $y = 0 \wedge x = 2 \wedge z \neq 0$}

```
z = x + y;
```

{ $y = 0 \wedge x = 2 \wedge z = 2$ }

(2) { |x| > 5 }

```
x = x % 10;
```

{ $0 \le x \le 9$ }

```
x = x * x;
```

{ $x \in \{0, 1, 4, 9, 16, 25, 36, 49, 64, 81\}$ }

```
x = -x;
```

{ $x \in \{0, -1, -4, -9, -16, -25, -36, -49, -64, -81\}$ }

(3) { z < 5 }

```
if (z > 0) {
```

{ $0 < z < 5$ }

```
z = -z;
```

{ $-5 < z < 0$ }

}

$\{(z \le 0) \vee (-5 < z < 0)\} = \{z \le 0\}$

Problem 5 (11 pts., 0.5 pts. each condition): Backward reasoning

Find the **weakest precondition** of each code sequence by inserting the appropriate condition in each blank. The first intermediate condition in part (1) is supplied as an example. Please simplify your answers as much as possible. Assume all referenced variables are defined as integers. Use the `wp()` notation as shown in the first example.

(1) { wp("x = -1;", y > -3x ∧ y < 10 - 3x)} = {y > 3 $\wedge y < 13\} = \{3 < y < 13\}$

$x = -1;$

$\{wp("z = 3 * x + y", 0 < z < 10)\} = \{0 > 3x + y \wedge$ y < 10 } =

{ y > -3x ∧ y < 10 - 3x }

```
z = 3 * x + y;
```

{ 0 < z < 10 }

(2) { wp("if (y > 0)", x > 0 ∧ x > y ∧ y > 0) } = {x > 0 ∧ x > y ∧ y > 0}

```
if (y > 0) {
```

{ wp("x = x / y", x > 1) } = {x > 0 ∧ x > y ∧ y > 0}

```
x = x / y;
```

{ wp("y = 0", x > 1 ∧ y = 0) } = {x > 1}

```
y = 0;
```

{ wp("else", x = 0 $\wedge x > 1)\} = \{x > 1 \wedge$ y = 0}

```
} else {
```

{ wp("y = 4 * x", x > 1 ∧ y = 0) } = {x = 0 $\wedge x > 1\}$else condition Fails

$y = 4 * x;$

$\{wp("\}", x > 1 \wedge$ y = 0) } = {x > 1 ∧ y = 0}

}

{ x > 1 ∧ y = 0 }

(3) { wp("if (x ≥ 0)", Math.min(z, x) ≠ 0 ∧ y ≥ 0 ∨ Math.min(z, x) ≥ -y} = {(Math.min(z, x) ≠ 0 ∧ y ≥ 0 ∨ Math.min(z, x) ≥ -y) ∧ (x ≥ 0) ∨ (x < 0 ∧ z ≠ 0 ∧ y ≥ 0 }

```
if (x ≥ 0) {
      { wp("z = Math.min(z, x)", z ≠ 0 ∧ y ≥ 0 ∧ x ≥ y} = {Math.min(z, x) ≠ 0
∧ y ≥ 0 ∨ Math.min(z, x) ≥ -y }
    z = Math.min(z, x);
      { wp("x = z + y", z ≠ 0 ∧ y ≥ 0 ∨ x ≥ 0)}
= {z ≠ 0 ∧ y ≥ 0 ∧ x ≥ y }
    x = z + y;
      { wp("}", z ≠ 0 ∧ y ≥ 0 ∨ x ≥ 0)} = {z ≠ 0 ∧ y ≥ 0 ∨ x ≥ 0 }
}
{ z ≠ 0 ∧ y ≥ 0 ∨ x ≥ 0}
```

(4) { wp("if (math.abs(x))",-1 ≤ x ≤ 5} = {(-1 ≤ x ≤ 5) ∨ (-9 ≤ x ≤ -5) }

```
if (Math.abs(x) <= 5) {
      { wp("z = x - 2", -3 ≤ z ≤ 3)} = { -3 ≤ x - 2 ≤ 3 } = {-1 ≤ x ≤ 5}
    z = x - 2;
      { wp("else",(-9 ≤ x ≤ -5) ∨ (-1 ≤ x ≤ 5)} = { -3 ≤ z ≤ 3 }
} else {
      { wp("if (x ≤ -5) ",-9 ≤ x ≤ -3)} = { (-9 ≤ x ≤ -5) ∨ (-1 ≤ x ≤ 1) }
   if (x <= -5) {
         { wp("z = x + 6",-3 ≤ z ≤ 3)} = { -9 ≤ x ≤ -3 }
      z = x + 6;
         { wp("else",-1 ≤ x ≤ 1)} = { -3 ≤ z ≤ 3 }
   } else {
         { wp("3 * x", -3 ≤ z ≤ 3)} = { -3 ≤ 3x ≤ 3 } = {-1 ≤ x ≤ 1}
      z = 3 * x;
         { wp("}", -3 ≤ z ≤ 3)} = { -3 ≤ z ≤ 3 }
   }
      { wp("}", -3 ≤ z ≤ 3)} = { -3 ≤ z ≤ 3 }
}
{ -3 ≤ z ≤ 3 }
```

(5) { wp("x = y / 2", x > -1)} = { y > -2 }

```
x = y / 2;
   { wp("z = x + 1", x ≠ 0.5 ∧ z > 0)} = { x > -1 }
z = x + 1;
{ x ≠ 0.5 ∧ z > 0}
```

Problem 6 (10 pts., 1 pt. each condition, 1 pt. sufficient/insufficient): Verifying Correctness

For each block of code, fill in all the conditions, then use them to state whether the precondition is sufficient to guarantee the postcondition. If the precondition is insufficient, explain why.

Hint: Use backward reasoning to find the weakest precondition that guarantees the postcondition and see if the given precondition is strong enough to guarantee the postcondition. In other words, is the given precondition not stronger than the weakest precondition?

Copy all code to your answer file and fill in the blanks. Answers must be expressed in the format `wp("code", condition) = precondition`. Show all work. Assume all referenced variables are defined as integers.

(1) { x < 2 }

```
    { wp("z = x - z", x > 3)} = { x > 3}
z = x - z;
    { wp("w = x - 1", w > 2)} = { x > 3}
w = x - 1;
    { wp("z = w - 1", z > 1)} = { w > 2}
z = w - 1;
{z > 1}
```

Sufficient or Insufficient: `Insufficient because the precondition value of x is too small to satisfy the post condition, as x would need to be greater than or equal to 4 at least but it less than 2.`

(2) { x = y ∧ y > 0 ∨ y ≠ x ∧ x ≥ 0 }

```
    { wp("if (x < y)", x < y + 1 ∧ x ≥ 1)} = { (x < y -1 ∧ x ≥1) ∨ (x > y ∧ y
> 0}
if (x < y) {
      { wp("x--", x < y ∧ x ≥ 0)} = { x < y + 1 ∧ x ≥ 1}
   x--;
      { wp("else", y > 0)} = { x < y ∧ x ≥ 0}
} else {
      { wp("x = y / 2", x < y ∧ x ≥ 0)} = { y > 0}
   x = y / 2;
      { wp("}", x < y ∧ x ≥ 0)} = { x < y ∧ x ≥ 0}
}
{ x < y ∧ x ≥ 0}
```

Sufficient or Insufficient: `Insufficient because when x < y and y > 0 the post condition will not be satisfied.`