CSE 331 Spring 2022 HW1

General rules:

- For logical operators, you may use words (e.g., "or") or any standard symbols (e.g., "V").
- Assume that
  - all numbers are integers
  - integer overflow will never occur
  - integer division rounds toward zero (as in Java)
- Simplify but **do not weaken** (i.e., change the set of described states) in your assertions.
- Wherever possible, rewrite your assertions to only refer to the current state of variables rather than using subscripts.

1. **Forward reasoning with assignment statements.** Find the strongest postcondition for each sequence using forward reasoning, writing the appropriate assertion in each blank space. The first assertion in part (a) is supplied as an example.

   a. {{ }}
   x = 5;
   {{ x = 5 }}
   y = 4 * x;
   {{ $x=5$ and $y=10x$ }}
   z = y / 5;
   {{ $x=5$ and $y=4x$ and $z=y/5$ }}
   y = x – z;
   {{ $x=5$ and $y=\frac{1}{5}x$ and $z=x-y$ }}

   b. {{ $0 \le x < 100$ }}
   y = x;
   {{ $0 \le x < 100$ and $y=x$ }}
   z = y – 2;
   {{ $0 \le x < 100$ and $y=x$ and $z=y-2$ }}
   x = y – z;
   {{ $0 \le x+z < 100$ and $y=x+z$ and $z=y-2$ }}

   c. {{ $0 \le x < 50$ }}
   x = x + 50;
   {{ $50 \le x < 100$ }}
   x = x / 10;
   {{ $5 \le x < 10$ }}
   x = 10 – x;
   {{ $0 < x \le 5$ }}

2. **Backward reasoning with assignment statements.** Find the weakest precondition for each sequence using backward reasoning, writing the appropriate assertion in each blank space.

a. {{ $-1 \leq x \leq 4$ }}
x = x * 3;
{{ $-3 \leq x \leq 12$ }}
y = 4 + x;
{{ $1 \leq y \leq 16$ }}

b. {{ $x \geq 2$ }}
y = 6 – x;
{{ $y \leq 2x$ }}
x = x * 2;
{{ $y \leq x$ }}

c. {{ $6 \leq x \leq 22$ }} (be careful!)
x = x / 2;
{{ $3 \leq x \leq 11$ }}
y = x – 3;
{{ $0 \leq y \leq 8$ }}

d. {{ $2 \leq w \leq \sqrt{}$ }}
z = v – 2;
{{ $2 \leq w \leq 2+z$ }}
x = 2w – 4;
{{ $0 \leq x \leq 2z$ }}
y = 2*z;
{{ $0 \leq x$ and $x \leq y$ }}

3. **Forward reasoning with if/else statements.** Find the strongest postcondition for the following conditional statement using forward reasoning, inserting the appropriate assertion in each blank.

a. {{ $0 \le x \le 40$ }}

if (x <= 20)

{{ $0 \le x \le 20$ }}

y = 3;

{{ $0 \le x \le 20$ and $y = 3$ }}

else

{{ $20 < x \le 60$ }}

y = 2;

{{ $20 < x \le 60$ and $y = 2$ }}

{{ $(0 \le x \le 20$ and $y = 3)$ or $(20 < x \le 60$ and $y = 2)$ }}

b. {{ }}

if (x >= 1)

{{ $x \ge 1$ }}

x = 3 * x;

{{ $x \ge 3$ }}

else

{{ $x < 1$ }}

x = x + 1;

{{ $x < 2$ }}

{{ $x < 2$ or $x \ge 3$ }}

4. **Backward reasoning with if/else statements.** Find the weakest precondition for the following conditional statement using backward reasoning, inserting the appropriate assertion in each blank.

a. {{ $0 \le x \le 24$ }}
if (x >= 10)
{{ $4 \le x \le 24$ }}
y = x – 4;
{{ $0 \le y \le 20$ }}
else
{{ $0 \le x \le 10$ }}
y = 2 * x;
{{ $0 \le y \le 20$ }}
{{ 0 ≤ y ≤ 20 }}

b. {{ $\forall x$ }}
if (x >= 0)
{{ $x \ge 1$ }}
x = -x;
{{ $x \le 1$ }}
else
{{ $x < 0$ }}
x = x + 1;
{{ $x < 1$ }}
{{ x < 1 }}

5. **Hoare triples.** State whether each Hoare triple is valid. If it is invalid, give a counterexample.

a. {{ $1 \le x < 100$ }}
x = x - 1;
{{ $0 \le x \le 100$ }}

Valid

b. {{ x = 89 }}
y = x - 34;
{{ x = 89 }}

Valid

c. {{ $x = 2y$ and $0 \le y \le 100$ }}
if (x > 100)
x = x / 2;
else
x = x + 50;
{{ x > 50 }}

Invalid y=0 and x=2y

d. {{ $x = 2y + z$ and $0 \le z \le 1$ }}
if (z == 0)
x = x / 2;
else
x = (x – 1) / 2;
{{ x = y }}

Valid

6. **Weakest conditions.** Circle the weakest condition in each list.

a.	{{ x < 0 }}	{{ x < 3 }}	{{ x < 5 }}
b.	{{ b != 5 }}	{{ |b| != 5 }}	{{ b < 0 }}
c.	{{ x > 1 and y > x }}	{{ x > 1 or y > 1 }}	{{ x > 1 or y > x }}
d.	{{ x > 1 and y > x }}	{{ x > 1 and y > 1 }}	{{ x > 1 and (if y > x, then y > 1) }}

7. **Verifying correctness.** For each block of code, fill in the intermediate assertions in the direction indicated by the arrows. Finally, state whether the code is correct (i.e., whether *all* triples are valid).

a. {{ 3 ≤ x }}
↓ y = x + 4;
{{ x≥3 and y = x+4 }}
↓ x = 2*x;
{{ x≥6 and y = ½x+4 }}
y = y + x;
{{ 14 ≤ y }} Incorrect

b. {{ x < 3 }}
y = 3 * x;
{{ 6x-9<y }}
↑ x = x * 6;
{{ x-9<y }}
↑ z = x – 9;
{{ z < y }} Correct!

c. {{ x ≤ 100 }}
↓ **if** (y > x)
{{ y>x and x≤100 }}
x = y – x;
{{ x≥1 }}
else
{{ y≤x≤100 }}
x = y / x; (be careful!)
{{ x≥1 }}
↑
{{ 1 ≤ x }} Incorrect!

8. **Verifying correctness of loops.** Fill in the missing assertions by reasoning in the direction indicated by the arrows. Then, in the places where two assertions appear next to each other with no code between (see the "?"s), provide an explanation of why the top assertion implies the bottom one.

   Note: You may use "n" as a short hand for "A.length".

```
{{ Pre: }} (i.e., nothing is assumed other than A is not null, which is an implicit constraint)
int find(int[] A, int val) {
  {{ n>0 }}
↓ int i = 0;
  {{ i=0 <n }}
? A[-1] represents nothing. hence we have A[i-1] != val
  {{ Inv: A[0] != val, A[1] != val, …, A[i-1] != val }}
  while (i != A.length) {
↓
    {{ A[0] !=val, A[1] !=val, ··· A[i-1] !=val, i!=n }}
↓   if (A[i] == val) {
      {{ A[0] !=val, A[1]!=val, ··· A[i-1]!=val, A[i] = val, }} i!=n
?     From above we know that A[i]=val and i!=n
      {{ Post: A[i] = val }}
      return i;
    } else {
↓     {{ A[0] !=val, A[1] != val, ···, A[i] != val, i!=n }}
?       above is tighter than below, so above can lead to below
      {{ A[0] !=val, A[1] != val, ···, A[i] !=val }}
↑   }
    {{ A[0] != val, ···· A[i] != val, }}
↑   i = i + 1;
    {{ A[0] != val, ···, A[i-1] != val }}
↑
  }
↓
  {{ A[0] != val, A[1] != val, …, A[i-1] != val and i = A.length }}
? plug in i=n and can get the post
  {{ Post: A[0] != val, A[1] != val, …, A[n-1] != val }}
  return -1;
}
```

9. **More loop correctness.** Fill in the missing assertions by reasoning in the direction indicated by the arrows. Then, in the places where two assertions appear next to each other with no code between (see the "?"s), provide an explanation of why the top assertion implies the bottom one.

   Notation: You may use "n" as a short-hand for "A.length".

```
{{ Pre: 0 < n }}
float evalPoly(float[] A, float v) {
↓ int i = A.length - 1;
  {{ n>0 and i=n-1 }}
↓ int j = 0;
  {{ n>0 and j>=0 and i=n-1 }}
↓ float val = A[i];
  {{ n>0 and j=0 and i=n-1 and val=A[i] }}
? plug in and get i+j = n-1+0=n-1.
  val = A[i]
  {{ Inv: val = A[i] + A[i+1] v + … + A[n-1] v^j and i + j = n – 1 }}
  while (j != A.length - 1) {
↓
    {{ val = A[i] + A[i+1] v + … + A[n-1] v^j and i+j=n-1 and j!=n-1 }}
↓   j = j + 1;
    {{ val = A[i] + A[i+1] v + … + A[n-1] v^(j-1) and i+j=n and j!=n }}
↓   i = i - 1;
    {{ val = A[i+1] + A[i+2] v + … + A[n-1] v^(j-1) and i+j=n-1 and j!=n
? the above is tighter than below, hence above can lead to below
    {{ val = A[i+1] + A[i+2] v + … + A[n-1] v^(j-1) and i+j=n-1 }}
↑   val = val * v + A[i];
    {{ val = A[i] + A[i+1] v + … + A[n-1] v^j and i+j=n-1 }}
↑
  }
↓
  {{ val = A[i] + A[i+1] v + … + A[n-1] v^j and i+j = n-1 and j=n-1 }}
? i+j=n-1 and j=n-1 => i=0. plug in i and j into the expression of val
  val = A[0] + A[1] v + … + A[n-1] v^(n-1)
  {{ Post: val = A[0] + A[1] v + A[2] v^2 + … + A[n-1] v^(n-1) }}
  return val;
}
```