

---

# HW 12 – Hoare Logic

CS 421 – Spring 2008

Revision 1.1

**Assigned** Thursday, April 24, 2008

**Due** Tuesday, April 29, in class

**Extension** None

---

## 1 Change Log

1.1 Corrected program for problem 3.

1.0 Initial Release.

1. Consider this program:

```
P:  q := 0; r := 0; a := 1;
    while (a <= x) {
      if (r = y-1)
        then { q := q+1; r := 0; }
      else { r := r+1; }
      a := a + 1;
    }
```

The correctness assertion for this program is

$$x > 0 \ \& \ y > 0 \ \{ P \} \ 0 \leq r < y \ \& \ x = qy + r$$

(a) Give the loop invariant  $I$  for the loop. Remember that the conjunction  $I \ \& \ \neg(a \leq x)$  must imply the post-condition of the correctness formula just given.

(b) Prove the loop terminates: Provide an integer-valued function  $f(q, r, a, x, y)$  whose value is always greater than or equal to zero, and prove that its value decreases at every iteration.

2. Consider this program:

```
P:  x := x0; y := y0;
    while (x != y) {
      if (x < y)
        then y := y-x;
      else x := x-y;
    }
```

The correctness assertion for this program is

$$x_0 > 0 \ \& \ y_0 > 0 \ \{ P \} \ x = \text{gcd}(x_0, y_0)$$

As for problem 1, do the following: (a) provide the loop invariant for the loop; (b) prove the loop terminates by providing a function  $f(x_0, y_0, x, y)$  whose value is a natural number and proving that the value of the function is decreased by executing the body of the loop.

3. The assignment rule does not apply directly to array computations (see problem 5). However, the other rules do, including the while rule. The correctness assertion for this program:

```
P:  i := 0; max := 0;
    while (i < n) {
      if (a[i] > max)
        then max := a[i];

      i := i + 1;
    }
```

is

$$\forall 0 \leq i < n. a[i] \geq 0 \{P\} \forall 0 \leq i < n. a[i] \leq \max \ \& \ \exists 0 \leq i < n. \max = a[i]$$

Again, answer parts (a) and (b) given in the previous questions.

4. Give a rule of inference for the if-then statement. That is, fill in the hypotheses for this rule:

---

$$P \{ \text{if } (b) \text{ then } S \} Q$$

5. (Extra credit) We noted above that the assignment rule does not apply when array assignment is allowed. Give an assertion  $P$  and assignment  $x := e$ , where  $x$  could be an array reference and  $e$  could contain array references, such that

$$P[e/x] \{x := e\} P$$

is false.