

# Correctness Triples

## CS 536 Activity 7, Mon Feb 1, 2012

### A. Why

- Correctness triples are how we write a program with its specification.
- Proof rules for correctness triples will show us how to reason about programs and their specifications.

### B. Objectives

- At the end of today you should
- Be able to explain the intuitive meaning of a correctness triple.
- Be able to show that an assignment triple is correct using the backward assignment rule.

### C. Questions

For Questions 1 – 4, use the triple  $\{\text{true}\} y := x*x \{y > x\}$

1. This triple is not valid: Find one or more states in which it isn't satisfied.
2. Suggest a fix to the triple that involves changing only the precondition.
3. Suggest a fix to the triple that involves changing only the program.
4. Suggest a fix to the triple that involves changing only the postcondition.
5. If you didn't already, give the most precise postcondition possible for this program.

6. Find a precondition such that  $\{\text{???}\} x := (x+1) / 2 \{x \geq 0\}$ .

7. Find a precondition such that  $\{\text{???}\} y := 2*y \{2*y < z\}$

### D. Solution

1. The state where  $x = 1$

There exist many answers to questions 2 – 4

2.  $\{x > 1\} y := x*x \{y > x\}$  [exist lots of answers:  $x < -1$ , false]

3.  $\{\text{true}\} \text{if } x > 1 \text{ then } y := x*x \text{ else } y := x+1 \text{ fi } \{y > x\}$

4.  $\{\text{true}\} y := x*x \{y \geq x\}$

5.  $\{\text{true}\} y := x*x \{y = x^2\}$

6.  $\{(x+1)/2 \geq 0\} x := (x+1) / 2 \{x \geq 0\}$  [exist lots of answers]

7.  $\{2*(2*y) < z\} y := 2*y \{2*y < z\}$