Correctness ("Hoare") Triples, v 1.1

Part 2: Sequencing, Assignment, Strengthening, and Weakening

CS 536: Science of Programming, Fall 2021

A. Why

- To specify a program's correctness, we need to know its precondition and postcondition (what should be true before and after executing it).
- The semantics of a verified program combines its program semantics rule with the state-oriented semantics of its specification predicates.
- To connect correctness triples in sequence, we need to weaken and strengthen conditions.

B. Objectives

At the end of today you should be able to

- Differentiate between different annotations for the same program.
- Determine whether two correctness triples can be joined and to give the result of joining.
- Reason "backwards" about assignment statements.
- Connect correctness triples in sequence by weakening and strengthening intermediate conditions

C. Problems

For all these problems, assume we're working over \( \mathbb{Z} \). There may be more than one correct answer; any right answer will do.

1. Find a state \( \sigma \) such that \( \sigma \not\models \{T\} y := x*x*x \{y > 4*x\} \). I.e., give a state in which the triple is unsatisfied — this proves that the triple is invalid.

2. Find the weakest precondition \( p \) that makes \( \models \{p\} y := x*x*x \{y > 4*x\} \) valid.

3. Find the strongest postcondition \( q \) such that \( \{T\} y := x; \text{if } x \geq 0 \text{ then } x := x*x \text{ fi } \{q\} \) is valid. (We want \( q \) to be satisfied by as many end states as possible.)

4. Fill in the missing code to make \( \{T\} \text{ if } ??? \text{ then } y := ??? \text{ else } y := x*x \text{ fi } \{y > 2*x\} \) valid. (There's no unique right answer.)

* Note if \( p \) is a weakest precondition, then so is anything logically equivalent to \( p \), so "the" weakest precondition is a bit of a misnomer. The same goes for "the" strongest postcondition.
For Problems 5 and 6, use the backward assignment rule discussed in the notes.

5a. Find the most general precondition $p$ such that $\{p\} x := (x+1)^y \{x \geq f(y)\}$ is valid.

5b. Using $p$, now find the most general precondition $q$ such that $\{q\} y := y+2 \{p\}$ is valid. (Note parts (a) and (b) together make $\{q\} y := y+2; x := (x+1)^y \{x \geq f(y)\}$ valid.)

6. Repeat Problem 5 using $\{p\} x := x^x \{x > 15\}$ and $\{q\} x := x+1 \{p\}$. 