Proof Rules and Proofs for Correctness Triples

Part 2: Conditional and Iterative Statements

CS 536: Science of Programming, Fall 2022

A. Why

- We can't generally prove that correctness triples are valid using truth tables.
- We need inference rules for compound statements such as conditional and iterative.

B. Objectives

At the end of this topic you should be able to

- Use the rules of inference for ***if-else, if-then, if-fi,*** and ***while*** statements.
- Describe how loop invariants work.

C. Problems

Use the Hilbert style (the two-column vertical format) to display rules.

1. Give the instance of the conditional rule we need to combine $\{x = y \wedge x < 0\}\ y := -x\ \{y \geq 0\}$ and $\{x = y \wedge x \geq 0\}$ ***skip*** $\{y \geq 0\}$.
2. Our goal is to find p such that $\{p\}$ ***if*** $b[M] < x$ ***then*** $L := M$ ***else*** $R := M$ ***fi*** $\{L < R\}$ is provable, using *wp*.
   a. Calculate $wp(L := M, L < R)$ and $wp(R := M, L < R)$.
   b. Let $p \equiv$ the *wp* of the ***if-fi*** and show the instance of the conditional rule that you get when you use part (a) to build the triples.
3. If we want to use the loop rule to prove $\{$***inv*** $x = 2\text{^}k\}$ ***while*** $k \neq n$ ***do*** $x := x+x;\ k := k+1$ ***od*** $\{q\}$
   a. What can we use for q?
   b. What triple do we need to prove about the loop body? Show the rule instance.
4. Study the triple $\{x = X/2\text{^}k \wedge x > 1\}\ x := x/2\ ;\ k := k+1\ \{x = X/2\text{^}k\}$.
   a. Write out a formal proof of the triple that uses *wp* on both assignments.
   b. Write out a second formal proof of the triple, but this time use *sp* on both assignments.
   c. Let $W \equiv$ ***while*** $x > 1$ ***do*** $x := x/2\ ;\ k := k+1$ od. Write out a formal proof of

      $\{x = X\}\ k := 0\ \{$***inv*** $x = X\ /\ 2\text{^}k\}\ W\ \{k = log_2\ X\}$[1]

      For the proof of the loop body, just refer to Part (a) or (b) above (doesn't matter which)

      $\{x = X/2\text{^}k \wedge x > 1\}\ x := x/2\ ;\ k := k+1\ \{x = X/2\text{^}k\}$ *See part a*

---

[1] We're using integer division with truncation, so we're calculating an integer logarithm. E.g. $log_2\ 3 = 1$.

Solution to Practice 15 (Proof Rules and Proofs, pt. 2)

1. (Conditional rule)

   One way to combine $\{x = y \wedge x < 0\}\ y := -x\ \{y \geq 0\}$ and $\{x = y \wedge x \geq 0\}$ ***skip*** $\{y \geq 0\}$ is to use an ***if-then*** statement $\{x = y\}$ ***if*** $x < 0$ ***then*** $y := -x$ ***fi*** $\{y \geq 0\}$ (which contains an implicit ***else skip***)

   1. $\{x = y \wedge x < 0\}\ y := -x\ \{y \geq 0\}$
   2. $\{x = y \wedge x \geq 0\}$ ***skip*** $\{y \geq 0\}$
   3. $\{x = y\}$ ***if*** $x < 0$ ***then*** $y := -x$ ***else skip fi*** $\{y \geq 0\}$ — *conditional 1, 2*

The other way to combine them is to make the ***skip*** the true branch (this would be pretty weird).

   4. $\{x = y\}$ ***if*** $x < 0$ ***then*** $y := -x$ ***else skip fi*** $\{y \geq 0\}$ — *conditional 2, 1*

2. (Prove $\{p\}$ ***if*** $b[M] < x$ ***then*** $L := M$ ***else*** $R := M$ ***fi*** $\{L < R\}$ using *wp*)

   a. $wp(L := M, L < R) \equiv M < R$ and $wp(R := M, L < R) \equiv L < M$.

   b. The rule instance is

   1. $\{L < M\}\ R := M\ \{L < R\}$
   2. $\{M < R\}\ L := M\ \{L < R\}$
   3. $\{p\}$ ***if*** $b[M] < x$ ***then*** $L := M$ ***else*** $R := M$ ***fi*** $\{L < R\}$ — *conditional 1, 2*

      where $p \equiv (b[M] < x \rightarrow M < R) \wedge (b[M] \geq x \rightarrow L < M)$

   (Technical note: If $M = (L+R)/2$, then we need $R \geq L+2$ to establish p.)

3. (Powers of 2 loop)

   a. The loop postcondition is $q \equiv x = 2\text{^}k \wedge k = n$ (the invariant and the negation of the test).

   b. The triple we need for the loop body is $\{x = 2\text{^}k \wedge k \neq n\}\ x := x+x;\ k := k+1\ \{x = 2\text{^}k\}$ (If the invariant and loop test are true, then the loop body re-establishes the invariant.) The rule instance is

   1. $\{x = 2\text{^}k \wedge k \neq n\}\ x := x+x;\ k := k+1\ \{2\text{^}k\}$
   2. $\{$***inv*** $x = 2\text{^}k\}$ ***while*** $k \neq n$ ***do*** $x := x+x;\ k := k+1$ ***od***

      $\{x = 2\text{^}k \wedge k = n\}$ — *loop 1*

4. (Integer $\log_2$ calculation)

   a. (Using *wp*) An alternative proof forms the sequence and then does precondition str.

   1. $\{x = X/2\text{^}(k+1)\}\ k := k+1\ \{x = X/2\text{^}k\}$ — *(backward) assignment*
   2. $\{x/2 = X/2\text{^}(k+1)\}\ x := x/2\ \{x = X/2\text{^}(k+1)\}$ — *(backward) assignment*
   3. $x = X/2\text{^}k \wedge x > 1 \rightarrow x/2 = X/2\text{^}(k+1)$ — *predicate logic*
   4. $\{x = X/2\text{^}k \wedge x > 1\}\ x := x/2\ \{x = X/2\text{^}(k+1)\}$ — *precondition str. 3, 2*
   5. $\{x = X/2\text{^}k \wedge x > 1\}\ x := x/2\ ;\ k := k+1\ \{x = X/2\text{^}k\}$ — *sequence 4, 1*

b. (Using *sp*) An alternative proof forms the sequence and then does precondition str.

1.	$\{x = X/2\text{^}k \wedge x > 1\}\ x := x/2\ \{q_1\}$	(forward) assignment
	where $q_1 \equiv x_0 = X/2\text{^}k \wedge x_0 > 1 \wedge x = x_0/2$	
2.	$\{q_1\}\ k := k+1\ \{q_2\}$	(forward) assignment
	where $q_2 \equiv x_0 = X/2\text{^}k_0 \wedge x_0 > 1 \wedge x = x_0/2 \wedge k = k_0+1$	
3.	$\{x = X/2\text{^}k \wedge x > 1\}\ x := x/2\ ;\ k := k+1\ \{q_2\}$	sequence 1, 2
4.	$q_2 \rightarrow x = X/2\text{^}k$	predicate logic
5.	$\{x = X/2\text{^}k \wedge x > 1\}\ x := x/2\ ;\ k := k+1\ \{x = X/2\text{^}k\}$	postcondition weakening 3, 4

c. (Proof of entire loop)

1.	$\{x = X\}\ k := 0\ \{x = X \wedge k = 0\}$	(forward) assignment
2.	$x = X \wedge k = 0 \rightarrow x = X / 2\text{^}k$	predicate logic
3.	$\{x = X\}\ k := 0\ \{x = X / 2\text{^}k\}$	postcondition weakening 2, 1
4.	$\{x = X/2\text{^}k \wedge x > 1\}\ x := x/2\ ;\ k := k+1\ \{x = X/2\text{^}k\}$	See part a or b
5.	$\{\textbf{inv}\ x = X / 2\text{^}k\}\ W\ \{x = X / 2\text{^}k \wedge k \le 1\}$	loop 4
	where $W \equiv$ ***while*** $x > 1$ ***do*** $x := x/2\ ;\ k := k+1$ ***od***	
6.	$x = X / 2\text{^}k \wedge x \le 1 \rightarrow k = \log_2 X$	predicate logic
7.	$\{\textbf{inv}\ x = X / 2\text{^}k\}\ W\ \{k = \log_2 X\}$	postcondition weakening 5, 6
8.	$\{x = X\}\ k := 0;\ \{\textbf{inv}\ x = X / 2\text{^}k\}\ W\ \{k = \log_2 X\}$	sequence 3, 7

