Proof Rules and Proofs

CS 536: Science of Programming, Spring 2023

Due Wed Mar 22, 11:59 pm

2023-03-09 due date updated

A. Why?

- To prove validity of correctness triples, we use a proof system with axioms for atomic statements and rules of inference for compound statements.

B. Outcomes

After this homework, you should be able to

- Verify and generate instances of the partial correctness proof rules.

C. Problems [60 points total]

Lectures 14 - 15: Proof Rules and Proofs, parts 1 & 2

For all the problems, if you define something using substitution notation (e.g., defining p' using "where $p' \equiv q'[e/v]$"), be sure to show the result of the substitution somewhere. Intermediate calculations that you write out might be worth partial credit.

Note the names used in one problem have no connection to the same names in other problems. (E.g., p_1 in Problem 1 is unrelated to p_1 in Problem 2.) Exception: Explicit connection can be made but they refer only to the given names. (E.g., if Problem 2 said "Let p_1 be as in Problem 1", then p_2 in Problems 1 and 2 are unrelated.)

You can use the looser sense of ≡ from lecture.

Small changes to the rule names are ok (assignment backward" vs "backward assignment", "while loop" or "loop", etc.)

1. [24 = 8 * 3 points] Let $p \equiv x = 2\,\hat{}\,k \wedge k \le n$. Complete the proof of correctness below by calculating p_1, p_2, and p_3 and the rule references $R_1 - R_5$. For the assignments, include whether it's backward or forward. Include line references (if any) with the rule name. Hint: For p_1, look at the loop rule; that will lead you to p_2, which leads to p_3.

1.	$\{p_1\}\ x := x * 2\ \{p_2\}$	R_1
2.	$\{p_2\}\ k := k + 1\ \{p_3\}$	R_2
3.	$\{p_1\}\ x := x * 2 ; k := k + 1\ \{p_3\}$	R_3
4.	$p_3 \rightarrow p$	predicate logic
5.	$\{p_1\}\ x := x * 2 ; k := k + 1\ \{p\}$	R_4
6.	$\{\textbf{inv}\ p\}\ \textbf{while}\ k < n\ \textbf{do}\ x := x * 2 ; k := k + 1\ \textbf{od}\ \{p \wedge k \ge n\}$	R_5

 © James Sasaki, 2023

2. [36 = 12 * 3 points] Let $IF \equiv$ ***if*** $even(x)$ then $y := 2 * y;\ x := x/2$ ***else*** $r := r + y;\ x := x - 1$ ***fi*** and let $q \equiv r = X * Y - x * y$. Complete the proof of correctness below for $\{q\}\ IF\ \{q\}$ by calculating $q_1 - q_6$ and $R_1 - R_6$. Hint: For q_1 and q_6, see how they are used in the if-else rule (see lines 5, 9, and 10).

1.	$\{q_1\}\ r := r + y\ \{q_2\}$	assignment (forward)
2.	$\{q_2\}\ x := x - 1\ \{q_3\}$	R_1
3.	$q_3 \rightarrow q$	predicate logic
4.	$\{q_2\}\ x := x - 1\ \{q\}$	R_2
5.	$\{q_1\}\ r := r + y;\ x := x - 1\ \{q\}$	sequence 1, 4
6.	$\{q_4\}\ x := x/2\ \{q\}$	R_3
7.	$\{q_5\}\ y := 2 * y\ \{q_4\}$	R_4
8.	$q_6 \rightarrow q_5$	predicate logic
9.	$\{q_6\}\ y := 2 * y\ \{q_4\}$	R_5
10.	$\{q_6\}\ y := 2 * y;\ x := x/2\ \{q\}$	sequence 9, 6
11.	$\{q\}\ IF\ \{q\}$	R_6

 © James Sasaki, 2023