Proof Rules and Proofs for Correctness Triples

Part 1: Axioms, Sequencing, and Auxiliary Rules, v.10/17

CS 536: Science of Programming, Fall 2021

Try the below using some of the different proof methods we've studied (proof trees, Hilbert-style, proof outlines). Below, ^ means exponentiation.

1. Consider the triples $\{p_1\}\ x := x+x\ \{p_2\}$ and $\{p_2\}\ k := k+1\ \{x = 2\text{^}k\}$ where p_1 and p_2 are unknown.

    a. Find values for p_1 and p_2 that make the triples provable.

    b. What do you get if you combine the triples using the sequence rule? Show the complete proof. (I.e., include the rules for the two assignments.)

    c. Add lines to the proof so that the sequence has precondition $x = 2\text{^}k$.

[Q1 parts d – f added 10/17]

    d. Let's strengthen the precondition of $x := x+x$ to be $x = 2\text{^}k$ before the use of sequence. What is the proof now?

[Q2 part a modified parts b & c added, Q3 added 10/17]

2. Say we want to prove $\{T\}\ k := 0; x := e\ \{x = 2\text{^}k\}$.

    a. Give a proof that calculates p and q for the triples $\{p\}\ k := 0\ \{q\}$ and $\{q\}\ x := e\ \{x = 2\text{^}k\}$, forms the sequence, and strengthens the initial precondition to T. Also, suggest a value for e.

    b. Repeat, but on the sequence $\{T\}\ x := e; k := 0\ \{x = 2\text{^}k\}$. (No change to e is needed.)

Solution to Practice 14 (Proof Rules and Proofs, pt.1)

1. *(*Preconditions for $x = 2\hat{}k$ postcondition*)*

   a. $p_2 \equiv wp(k := k+1, x = 2\hat{}k) \equiv x = 2\hat{}(k+1)$.
   $p_1 \equiv wp(x := x+x, p_2) \equiv wp(x := x+x, x = 2\hat{}(k+1)) \equiv x+x = 2\hat{}(k+1)$.

   b. The full proof is:

1.	$\{x = 2\hat{}(k+1)\}\ k := k+1\ \{x = 2\hat{}k\}$	assignment (backward)
2.	$\{x+x = 2\hat{}(k+1)\}\ x := x+x\ \{x = 2\hat{}(k+1)\}$	assignment (backward)
3.	$\{x+x = 2\hat{}(k+1)\}\ x := x+x;\ k := k+1\ \{x = 2\hat{}k\}$	sequence 2, 1

   c. To make the precondition $x = 2\hat{}k$, we have to strengthen the precondition of line 3. We need a predicate logic obligation and a strengthening step:

4.	$x = 2\hat{}k \rightarrow x+x = 2\hat{}(k+1)$	predicate logic
5.	$\{x = 2\hat{}k\}\ x := x+x;\ k := k+1\ \{x = 2\hat{}k\}$	precond. strength. 4, 3

   d. We need to reorder the proof lines to strengthen the precondition of $x := x+x$ before combining it with $k := k+1$:

1.	$\{x = 2\hat{}(k+1)\}\ k := k+1\ \{x = 2\hat{}k\}$	assignment (backward)
2.	$\{x+x = 2\hat{}(k+1)\}\ x := x+x\ \{x = 2\hat{}(k+1)\}$	assignment (backward)
3.	$x = 2\hat{}k \rightarrow x+x = 2\hat{}(k+1)$	predicate logic
4.	$\{x = 2\hat{}k\}\ x := x+x\ \{x = 2\hat{}(k+1)\}$	precond. strength. 3, 2
5.	$\{x = 2\hat{}k\}\ x := x+x;\ k := k+1\ \{x = 2\hat{}k\}$	sequence 2, 1

2. (Proofs of $\{T\}\ k := 0;\ x := e\ \{x = 2\hat{}k\}$.)

   a. (Use *wp* twice, form the sequence, and strengthen the precondition to T.)

1.	$\{e = 2\hat{}k\}\ x := e\ \{x = 2\hat{}k)$	assignment (backward)
2.	$\{e = 2\hat{}0\}\ k := 0\ \{e = 2\hat{}k\}$	assignment (backward)
3.	$\{e = 2\hat{}0\}\ k := 0;\ x := e\ \{x = 2\hat{}k)$	sequence 2, 1
4.	$T \rightarrow e = 2\hat{}0$	predicate logic
5.	$\{T\}\ k := 0;\ x := e\ \{x = 2\hat{}k)$	precond. strength. 4, 3

   We can use $e \equiv 1$.

b. (Prove *{T} x := e; k := 0 {x = 2^k}* in the same way, with no change to *e*.)

1.	*{x = 2^0} k := 0 {x = 2^k)*	assignment (backward)
2.	*{e = 2^0} x := e {x = 2^0}*	assignment (backward)
3.	*{e = 2^0} x := e; k := 0 {x = 2^k)*	sequence 2, 1
4.	$T \rightarrow e = 2^0$	predicate logic
5.	*{T} k := 0; x := e {x = 2^k)*	precond. strength. 4, 3

Again, $e \equiv 1$.