# *Proof Rules and Proofs for Correctness Triples*

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

## *CS 536: Science of Programming, Fall 2021*

### ***A.*** *Why*

- We can't generally prove that correctness triples are valid using truth tables.
- We need proof axioms for atomic statements (*skip* and assignment) and inference rules for compound statements like sequencing.
- In addition, we have inference rules that let us manipulate preconditions and postconditions.

### ***B.*** *Objectives*

At the end of this practice activity you should

- Be able to match a statement and its conditions to its proof rule.

### ***C.*** *Problems*

Use the vertical format to display rule instances. Below, ^ means exponentiation.

1. Consider the triples $\{p_1\}\ x := x+x\ \{p_2\}$ and $\{p_2\}\ k := k+1\ \{x = 2\hat{}k\}$ where $p_1$ and $p_2$ are unknown.
   a. Find values for $p_1$ and $p_2$ that make the triples provable. *(*Hint: Use *wp.)*
   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 $x = 2\hat{}k$.

*[Q1 parts d – f added 10/17]*

   d. Let's strengthen the precondition of $x := x+x$ to be $x = 2\hat{}k$ before the use of sequence. What is the proof now?
   e. Now try using *sp* on the two assignments instead of *wp*, plus weakening the postcondition after forming the sequence. What is the proof now?
   f. Say we continue using *sp* but weaken the postcondition of each assignment (to simplify it) before forming the sequence. What is the proof now?

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

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

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.)

c. Now give a proof for $\{T\}\ k := 1;\ x := e\ \{x = 2\text{^}k\}$ that uses *sp* on each assignment and weakens the final postcondition to $x = 2\text{^}k$. What value do you want for $e$?

3. The goal is to derive a proof rule with an extended version of the sequence rule:

| | | |
|---|---|---|
| 1. | $\{p\}\ S_1\ \{q\}$ | antecedent 1 |
| 2. | $q \to q'$ | antecedent 2 |
| 3. | $\{q'\}\ S_2\ \{r\}$ | antecedent 3 |
| 4. | $\{p\}\ S_1;\ S_2\ \{r\}$ | extended sequence 1, 2, 3 |

We can do this by taking this framework and adding proof lines to get us from lines 1 – 3 to 4. There are a couple of ways to do this; show one of them.

## *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. $\{x = 2\hat{}k\}\ x := x+x;\ k := k+1\ \{x = 2\hat{}k\}$ consequence 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. $\{x = 2\hat{}k\}\ x := x+x\ \{x = 2\hat{}(k+1)\}$ consequence 3, 2
   5. $\{x = 2\hat{}k\}\ x := x+x;\ k := k+1\ \{x = 2\hat{}k\}$ sequence 2, 1

   e. If we use *sp* on the assignments and weaken the postcondition of the sequence, we get:

   1. $\{x = 2\hat{}k\}\ x := x+x\ \{x_0 = 2\hat{}k \wedge x = x_0+x_0\}$ assignment (forward)
   2. $\{x_0 = 2\hat{}k \wedge x = x_0+x_0\}\ k := k+1\ \{q_0\}$ assignment (forward)
      where $q_0 \equiv x_0 = 2\hat{}k_0 \wedge x = x_0+x_0 \wedge k = k_0+1$
   3. $\{x = 2\hat{}k\}\ x := x+x;\ k := k+1\ \{q_0\}$ sequence 2, 1
   4. $q_0 \rightarrow x = 2\hat{}k$ predicate logic
   5. $\{x = 2\hat{}k\}\ x := x+x;\ k := k+1\ \{x = 2\hat{}k\}$ consequence 3, 4

   f. If we use *sp* but weaken the postconditions as we go, we get:

   1. $\{x = 2\hat{}k\}\ x := x+x\ \{x_0 = 2\hat{}k \wedge x = x_0+x_0\}$ assignment (forward)
   2. $x_0 = 2\hat{}k \wedge x = x_0+x_0 \rightarrow x/2 = 2\hat{}k$ predicate logic
   3. $\{x = 2\hat{}k\}\ x := x+x\ \{x/2 = 2\hat{}k\}$ consequence1, 2
   4. $\{x/2 = 2\hat{}k\}\ k := k+1\ \{x/2 = 2\hat{}k_0 \wedge k = k_0+1\}$ assignment (forward)
   5. $x/2 = 2\hat{}k_0 \wedge k = k_0+1 \rightarrow x = 2\hat{}k$ predicate logic
   6. $\{x/2 = 2\hat{}k\}\ k := k+1\ \{x = 2\hat{}k\}$ consequence 4, 5
   7. $\{x = 2\hat{}k\}\ x := x+x;\ k := k+1\ \{x = 2\hat{}k\}$ sequence 3, 6

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

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

| | | |
|---|---|---|
| 1. | $\{e = 2\text{^}k\}\ x := e\ \{x = 2\text{^}k)$ | assignment (backward) |
| 2. | $\{e = 2\text{^}0\}\ k := 0\ \{e = 2\text{^}k\}$ | assignment (backward) |
| 3. | $\{e = 2\text{^}0\}\ k := 0;\ x := e\ \{x = 2\text{^}k)$ | sequence 2, 1 |
| 4. | $T \to e = 2\text{^}0$ | predicate logic |
| 5. | $\{T\}\ k := 0;\ x := e\ \{x = 2\text{^}k)$ | consequence 4, 3 |

   We can use $e \equiv 1$.

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

| | | |
|---|---|---|
| 1. | $\{x = 2\text{^}0\}\ k := 0\ \{x = 2\text{^}k)$ | assignment (backward) |
| 2. | $\{e = 2\text{^}0\}\ x := e\ \{x = 2\text{^}0\}$ | assignment (backward) |
| 3. | $\{e = 2\text{^}0\}\ x := e;\ k := 0\ \{x = 2\text{^}k)$ | sequence 2, 1 |
| 4. | $T \to e = 2\text{^}0$ | predicate logic |
| 5. | $\{T\}\ k := 0;\ x := e\ \{x = 2\text{^}k)$ | consequence 4, 3 |

   Again, $e \equiv 1$.

   c. (Prove $\{T\}\ k := 1;\ x := e\ \{x = 2\text{^}k\}$ using *sp* and ending with postcondition weakening.)

| | | |
|---|---|---|
| 1. | $\{T\}\ k := 1\ \{k = 1\}$ | assignment (forward) |
| 2. | $\{k = 1\}\ x := e\ \{k = 1 \wedge x = e\}$ | assignment (forward) |
| 3. | $\{T\}\ k := 1;\ x := e\ \{k = 1 \wedge x = e\}$ | sequence 1, 2 |
| 4. | $k = 1 \wedge x = e \to x = 2\text{^}k$ | predicate logic |
| 5. | $\{T\}\ k := 1;\ x := e\ \{x = 2\text{^}k\}$ | consequence 3, 4 |

   This time, $e = 2$, since we need $x = 2\text{^}k \equiv 2 = 2\text{^}1$.

   d. (Prove $\{T\}\ k := 1;\ x := e\ \{x = 2\text{^}k\}$ using *sp* on first assignment, *wp* on second.)

| | | |
|---|---|---|
| 1. | $\{T\}\ k := 1\ \{k = 1\}$ | assignment (forward) |
| 2. | $\{e = 2\text{^}k\}\ x := e\ \{x = 2\text{^}k\}$ | assignment (backward) |
| 3. | $k = 1 \to e = 2\text{^}k$ | predicate logic |
| 4. | $\{e = 2\text{^}k\}\ x := e\ \{x = 2\text{^}k\}$ | consequence 3, 2 |
| 5. | $\{T\}\ k := 1;\ x := e\ \{x = 2\text{^}k\}$ | sequence 1, 4 |

3. (Derived proof rule for antecedents $\{p\}\ S_1\ \{q\}$, $q \to q'$, $\{q'\}\ S_2\ \{r\}$ and consequent $\{p\}\ S_1;\ S_2\ \{r\}$.)
   Below, we weaken the postcondition of antecedent 1 and then use sequence with antecedent 3.
   (A symmetric proof uses precondition strengthening on antecedent 3 and then uses sequence with antecedent 1.)

| | | |
|---|---|---|
| 1. | $\{p\}\ S_1\ \{q\}$ | antecedent 1 |
| 2. | $q \to q'$ | antecedent 2 |
| 3. | $\{p\}\ S_1\ \{q'\}$ | postcond. weak. 1, 3 |
| 4. | $\{q'\}\ S_2\ \{r\}$ | antecedent 3 |
| 5. | $\{p\}\ S_1;\ S_2\ \{r\}$ | sequence 4, 3 |