Alternative proof styles and proof outlines

Farzaneh Derakhshan
based on material by Stefan Muller and Jim Sasaki

CS 536: Science of Programming, Fall 2023
Lecture 10

In Lecture 9, we learned about building proof trees to show the provability of partial correctness triples. Proof trees are useful in understanding the basics of Hoare logic, establishing its metatheory (for example, soundness and (in-)completeness), and automating the proof-making process. However, building proofs manually using proof trees becomes increasingly difficult when the program becomes more complex. In this lecture, we learn two alternative methods to display proofs of partial correctness triples.

1 Hilbert-style proofs

Example 0. In Lecture 9 we built a proof tree for the triple $\vdash \{x = a \wedge y = b\}\ z{:=}x; x{:=}y; y{:=}z\ \{x = b \wedge y = a\}$ as fillows:

$$\dfrac{\dfrac{}{\{x = a \wedge y = b\}\ z := x\ \{z = a \wedge y = b\}}\ (\mathrm{A}) \quad \dfrac{\dfrac{}{\{z = a \wedge y = b\}\ x := y\ \{z = a \wedge x = b\}}\ (\mathrm{A}) \quad \dfrac{}{\{z = a \wedge x = b\}\ y := z\ \{x = b \wedge y = a\}}\ (\mathrm{A})}{\{z = a \wedge y = b\}\ x := y; y := z\ \{x = b \wedge y = a\}}\ (\mathrm{S})}{\{x = a \wedge y = b\}\ z := x; x := y; y := z\ \{x = b \wedge y = a\}}\ (\mathrm{S})$$

Even for this small program, I couldn't quite fit the proof tree within the margins of a letter-sized paper. Therefore, we need an alternative way of presenting the proofs. In this section, we introduce an alternative style of presenting proofs, called Hilbert-style proofs [1].

To build a Hilbert-style proof, we list the nodes of the proof tree. Each line in the list is either an axiom (skip or assign axioms) or can be derived by the application of an inference rule (if, sequence, or consequence rules) on the previous lines.

Example 1. Here is the Hilbert-style proof for the proof tree built in Example 0:

(1)	$\{x = a \wedge y = b\}\ z := x\ \{z = a \wedge y = b\}$	**Assign**
(2)	$\{z = a \wedge y = b\}\ x := y\ \{z = a \wedge x = b\}$	**Assign**
(3)	$\{z = a \wedge x = b\}\ y := z\ \{x = b \wedge y = a\}$	**Assign**
(4)	$\{z = a \wedge y = b\}\ x := y; y := z\ \{x = b \wedge y = a\}$	**Sequence 2, 3**
(5)	$\{x = a \wedge y = b\}\ z := x; x := y; y := z\ \{x = b \wedge y = a\}$	**Sequence 1, 4**

Example 2. The following is a Hilbert-style proof for the triple $\vdash \{T\}\ x{:=}1; \mathsf{if}\ x > 0\ \mathsf{then}\ z := 1\ \mathsf{else}\ z := 0\ \mathsf{fi}\ \{z = 1\}$:

(1)	$\{1 = 1\}\ x := 1\ \{x = 1\}$	**Assign**
(2)	$\{T\}\ x := 1\ \{x > 0\}$	**Consequence 1**
(3)	$\{1 = 1\}\ z := 1\ \{z = 1\}$	**Assign**
(4)	$\{x > 0 \wedge x > 0\}\ z := 1\ \{z = 1\}$	**Consequence 3**
(5)	$\{F\}\ z := 0\ \{F\}$	**Assign**
(6)	$\{x > 0 \wedge \neg\, x > 0\}\ z := 0\ \{z = 1\}$	**Consequence 5**
(7)	$\{x > 0\}\ \mathsf{if}\ x > 0\ \mathsf{then}\ z := 1\ \mathsf{else}\ z := 0\ \mathsf{fi}\ \{z = 1\}$	**If 4, 6**
(8)	$\{T\}\ x := 1; \mathsf{if}\ x > 0\ \mathsf{then}\ z := 1\ \mathsf{else}\ z := 0\ \mathsf{fi}\ \{z = 1\}$	**Seq 2, 7**

[1] Hilbert-style proofs are attributed to Hilbert, a highly influential logicians with a crucial role in creating mathematical logic and proof theory.

Example 3. The following is a Hilbert-style proof for the triple

$$\vdash \{T\} \text{ if } x > 0 \text{ then } y := 1 \text{ else } y := 2 \text{ fi}; \text{if } y > 0 \text{ then } z := 1 \text{ else } z := 0 \text{ fi } \{z = 1\} :$$

(1)	$\{1 > 0\}\ y := 1\ \{y > 0\}$	**Assign**
(2)	$\{2 > 0\}\ y := 2\ \{y > 0\}$	**Assign**
(3)	$\{T \wedge x > 0\}\ y := 1\ \{y > 0\}$	**Consequence 1**
(4)	$\{T \wedge \neg\, x > 0\}\ y := 2\ \{y > 0\}$	**Consequence 2**
(5)	$\{T\}$ if $x > 0$ then $y := 1$ else $y := 2$ fi $\{y > 0\}$	**If 3, 4**
(6)	$\{1 = 1\}\ z := 1\ \{z = 1\}$	**Assign**
(7)	$\{y > 0 \wedge y > 0\}\ z := 1\ \{z = 1\}$	**Consequence 6**
(8)	$\{F\}\ z := 0\ \{F\}$	**Assign**
(9)	$\{y > 0 \wedge \neg\, y > 0\}\ z := 0\ \{z = 1\}$	**Consequence 8**
(10)	$\{y > 0\}$ if $y > 0$ then $z := 1$ else $z := 0$ fi $\{z = 1\}$	**If 7, 9**
(11)	$\{T\}$ if $x > 0$ then $y := 1$ else $y := 2$ fi; if $y > 0$ then $z := 1$ else $z := 0$ fi $\{z = 1\}$	**Seq 5, 10**

2 Proof outlines

A proof outline is a way to summarize the information that one would need to generate a full formal proof by annotating the program. To create a proof outline, we start by annotating each program statement with its preconditions and postconditions. Precondition strengthening and postcondition weakening using the consequence rule are also included in the outline. Example 4 presents a proof outline for the proof presented in Example 1.

Example 4.

$$\begin{array}{ll} & \{x = a \wedge y = b\} \\ z := x; & \{z = a \wedge y = b\} \\ x := y; & \{z = a \wedge x = b\} \\ y := z & \{x = b \wedge y = a\} \end{array}$$

Example 5 presents a proof outline for the proof presented in Example 2.

Example 5.

$$\begin{array}{ll} & \{T\} \Rightarrow \{1 = 1\} \\ x := 1 & \{x = 1\} \Rightarrow \{x > 0\} \\ \text{if } x > 0 \text{ then} & \{x > 0 \wedge x > 0\} \Rightarrow \{1 = 1\} \\ \ z := 1 & \{z = 1\} \\ \text{else} & \{x \geq 0 \wedge \neg\, x \geq 0\} \Rightarrow \{F\} \\ \ z := 1; & \{F\} \Rightarrow \{z = 1\} \\ \text{fi} & \{z = 1\} \end{array}$$

Exercise 1. Convert the Hilbert-style proof in Example 3 to a proof outline.

A proof outline does not stand for a unique proof. For example, the proof outline in Example 4 corresponds to proofs in both Examples 1 and 6. Example 6 swaps lines 1 and 2 in Example 6.

Example 6.

(1)	$\{z = a \wedge y = b\}\, x := y\, \{z = a \wedge x = b\}$	**Assign**
(2)	$\{x = a \wedge y = b\}\, z := x\, \{z = a \wedge y = b\}$	**Assign**
(3)	$\{z = a \wedge x = b\}\, y := z\, \{x = b \wedge y = a\}$	**Assign**
(4)	$\{z = a \wedge y = b\}\, x := y; y := z\, \{x = b \wedge y = a\}$	**Sequence 1, 3**
(5)	$\{x = a \wedge y = b\}\, z := x; x := y; y := z\, \{x = b \wedge y = a\}$	**Sequence 2, 4**

Aside from permuting line orderings, the timing of precondition strengthening and postcondition weakening may not be unique. For example, the proof outline in Example 5 corresponds to proofs in both Examples 2 and 7.

Example 7.

(1)	$\{1 = 1\}\ x := 1\ \{x = 1\}$	**Assign**
(2)	$\{1 = 1\}\ z := 1\ \{z = 1\}$	**Assign**
(3)	$\{F\}\ z := 0\ \{F\}$	**Assign**
(4)	$\{x > 0 \wedge x > 0\}\ z := 1\ \{z = 1\}$	**Consequence 2**
(5)	$\{T\}\ x := 1\ \{x > 0\}$	**Consequence 1**
(6)	$\{x > 0 \wedge \neg\, x > 0\}\ z := 0\ \{z = 1\}$	**Consequence 3**
(7)	$\{x > 0\}$ if $x > 0$ then $z := 1$ else $z := 0$ fi $\{z = 1\}$	**If 4, 6**
(8)	$\{T\}\ x := 1;$ if $x > 0$ then $z := 1$ else $z := 0$ fi $\{z = 1\}$	**Seq 5, 7**