Proofs and Proof Outlines for Partial Correctness

Part 1: Full Proofs and Proof Outlines of Partial Correctness
CS 536: Science of Programming, Fall 2021

A. Why

• A formal proof lets us write out in detail the reasons for believing that something is valid.

B. Objectives

At the end of this activity assignment you should be able to

• Write and check formal proofs of partial correctness.
• Translate between full formal proofs and full proof outlines

C. Problems

Formal Proofs

1. The formal Hilbert-style proof below is incomplete; fill in the missing rule names (and line references, where needed).

    1. $T \rightarrow 0 \geq 0 \wedge 1 = 2\text{^}0$ ___________
    2. $\{0 \geq 0 \wedge 1 = 2\text{^}0\}\ k := 0\ \{k \geq 0 \wedge 1 = 2\text{^}k\}$ ___________
    3. $\{T\}\ k := 0\ \{k \geq 0 \wedge 1 = 2\text{^}k\}$ ___________
    4. $\{k \geq 0 \wedge 1 = 2\text{^}k\}\ x := 1\ \{k \geq 0 \wedge x = 2\text{^}k\}$ ___________
    5. $\{T\}\ k := 0;\ x := 1\ \{k \geq 0 \wedge x = 2\text{^}k\}$ ___________

    Here's an alternate version of the proof that uses forward assignments:

    1. $\{T\}\ k := 0\ \{k = 0\}$ ___________
    2. $\{k = 0\}\ x := 1\ \{k = 0 \wedge x = 1\}$ ___________
    3. $\{T\}\ k := 0;\ x := 1\ \{k = 0 \wedge x = 1\}$ ___________
    4. $k = 0 \wedge x = 1 \rightarrow k \geq 0 \wedge x = 2\text{^}k$ ___________
    5. $\{T\}\ k := 0;\ x := 1\ \{k \geq 0 \wedge x = 2\text{^}k\}$ ___________

2. Repeat Problem 1 on the incomplete proof below.

    1. $\{-x = abs(x)\}\ y := -x\ \{y = abs(x)\}$ ___________
    2. $y = x \wedge x < 0 \rightarrow -x = abs(x)$ ___________
    3. $\{y = x \wedge x < 0\}\ y := -x\ \{y = abs(x)\}$ ___________
    4. $\{y = abs(x)\}\ skip\ \{y = abs(x)\}$ ___________
    5. $y = x \wedge x \geq 0 \rightarrow y = abs(x)$ ___________

6. $\{ y = x \wedge x \geq 0 \}$ *skip* $\{ y = abs(x) \}$ __________
7. $\{ y = x \}$ *if* $x < 0$ *then* $y := -x$ *fi* $\{ y = abs(x) \}$ __________

3. Repeat Problem 1 on the incomplete proof below.

   Below, let $W \equiv$ *while* $j > 0$ *do* $j := j-1;\ s := s+j$ *od* [and $p \equiv 0 \leq j \leq n \wedge s = sum(j, n)$ added 10/19]

   1. $\{ p[n/s] \}\ s := n\ \{ p \}$ assignment (backwards)
   2. $\{ p[n/s][n/j] \}\ j := n\ \{ p[n/s] \}$ assignment (backwards)
   3. $\{ p[n/s] \}\ j := n;\ s := n\ \{ p \}$ sequence 2, 1
   4. $n \geq 0 \rightarrow p[n/s][n/j]$ predicate logic
   5. $\{ n \geq 0 \}\ j := n;\ s := n\ \{ p \}$ precondition strength. 4, 3
   6. $\{ p \wedge j > 0 \}\ j := j-1\ \{ p1 \}$ assignment (forwards)

      where $p_1 \equiv p[j_0/j] \wedge j = j_0-1$
   7. $\{ p_1 \}\ s := s+j\ \{ p_2 \}$ assignment (forwards)

      where $p_2 \equiv p_1[s_0/s] \wedge s = s_0+j$
   8. $\{ p \wedge j > 0 \}\ j := j-1;\ s := s+j\ \{ p_2 \}$ sequence 6, 7
   9. $p_2 \rightarrow p$ predicate logic
   10. $\{ p \wedge j > 0 \}\ j := j-1;\ s := s+j\ \{ p \}$ postcondition weak. 8, 9
   11. $\{ inv\ p \}\ W\ \{ p \wedge j \leq 0 \}$ while 10
   12. $\{ n \geq 0 \}\ j := n;\ s := n\ \{ inv\ p \}\ W\ \{ p \wedge j \leq 0 \}$ sequence 5, 11
   13. $p \wedge j \leq 0 \rightarrow s = sum(0, n)$ predicate logic
   14. $\{ n \geq 0 \}\ j := n;\ s := n\ \{ inv\ p \}\ W\ \{ s = sum(0, n) \}$ postcondition weak. 12, 13

Full Proof Outlines

For Problems 1–3, you are given a full proof outline; write a corresponding Hilbert-style proof of partial correctness from it. There are multiple right answers.

1. $\{ T \}\ \{ 0 \geq 0 \wedge 1 = 2\hat{\ }0 \}\ k := 0;\ \{ k \geq 0 \wedge 1 = 2\hat{\ }k \}\ x := 1\ \{ k \geq 0 \wedge x = 2\hat{\ }k \}$

2a. $\{ y = x \}$ *if* $x < 0$ *then*

   $\{ y = x \wedge x < 0 \}\ \{ -x = abs(x) \}\ y := -x\ \{ y = abs(x) \}$

else

   $\{ y = x \wedge x \geq 0 \}\ \{ y = abs(x) \}$ *skip* $\{ y = abs(x) \}$

fi $\{ y = abs(x) \}$

2b. $\{y = x\}$ *if* $x < 0$ *then*

$\{y = x \wedge x < 0\}$ $y := -x$ $\{y_0 = x \wedge x < 0 \wedge y = -x\}$

else

$\{y = x \wedge x \geq 0\}$ *skip* $\{y = x \wedge x \geq 0\}$

fi $\{(y_0 = x \wedge x < 0 \wedge y = -x) \vee (y = x \wedge x \geq 0)\}$ $\{y = abs(x)\}$

2c. $\{y = x\}$ $\{(x < 0 \rightarrow -x = abs(x)) \wedge (x \geq 0 \rightarrow y = abs(x))\}$

if $x < 0$ *then*

$\{-x = abs(x)\}$ $y := -x$ $\{y = abs(x)\}$

else

$\{y = abs(x)\}$ *skip* $\{y = abs(x)\}$

fi $\{y = abs(x)\}$

3. Hint: Use *sp* for the two loop initialization assignments.

$\{n \geq 0\}$ $j := n;$ $\{n \geq 0 \wedge j = n\}$ $s := n;$ $\{n \geq 0 \wedge j = n \wedge s = n\}$

$\{$*inv* $p \equiv 0 \leq j \leq n \wedge s = sum(j, n)\}$

while $j > 0$ *do*

$\{p \wedge j > 0\}$ $\{p[s+j/s][j-1/j]\}$ $j := j-1$

$\{p[s+j/s]\}$ $s := s+j$ $\{p\}$

od

$\{p \wedge j \leq 0\}$ $\{s = sum(0, n)\}$

Solution to Practice 16 (Formal Proofs and Full Proof Outlines

1. Proof:

1.	$T \rightarrow 0 \geq 0 \wedge 1 = 2^\wedge 0$	predicate logic
2.	$\{0 \geq 0 \wedge 1 = 2^\wedge 0\}\ k := 0\ \{k \geq 0 \wedge 1 = 2^\wedge k\}$	assignment (backward)
3.	$\{T\}\ k := 0\ \{k \geq 0 \wedge 1 = 2^\wedge k\}$	precondition strengthening 1, 2
4.	$\{k \geq 0 \wedge 1 = 2^\wedge k\}\ x := 1\ \{k \geq 0 \wedge x = 2^\wedge k\}$	assignment (backward)
5.	$\{T\}\ k := 0;\ x := 1\ \{k \geq 0 \wedge x = 2^\wedge k\}$	sequence 3, 4
	[Alternate version]	
1.	$\{T\}\ k := 0\ \{k = 0\}$	assignment (forward)
2.	$\{k = 0\}\ x := 1\ \{k = 0 \wedge x = 1\}$	assignment (forward)
3.	$\{T\}\ k := 0;\ x := 1\ \{k = 0 \wedge x = 1\}$	sequence 1, 2
4.	$k = 0 \wedge x = 1 \rightarrow k \geq 0 \wedge x = 2^\wedge k$	predicate logic
5.	$\{T\}\ k := 0;\ x := 1\ \{k \geq 0 \wedge x = 2^\wedge k\}$	postcondition weakening 3, 4

2. Proof:

1.	$\{-x = abs(x)\}\ y := -x\ \{y = abs(x)\}$	assignment (backward)
2.	$y = x \wedge x < 0 \rightarrow -x = abs(x)$	predicate logic
3.	$\{y = x \wedge x < 0\}\ y := -x\ \{y = abs(x)\}$	precondition strength. 2, 1
4.	$\{y = abs(x)\}\ skip\ \{y = abs(x)\}$	skip
5.	$y = x \wedge x \geq 0 \rightarrow y = abs(x)\}$	predicate logic
6.	$\{y = x \wedge x \geq 0\}\ skip\ \{y = abs(x)\}$	precondition strength. 5, 4
7.	$\{y = x\}\ if\ x < 0\ then\ y := -x\ fi\ \{y = abs(x)\}$	conditional 3, 6

3. Below, $W \equiv while\ j > 0\ do\ j := j-1;\ s := s+j\ od$

1.	$\{n \geq 0\}\ j := n\ \{n \geq 0 \wedge j = n\}$	assignment (forward)
2.	$\{n \geq 0 \wedge j = n\}\ s := n\ \{n \geq 0 \wedge j = n \wedge s = n\}$	assignment (forward)
3.	$\{n \geq 0\}\ j := n;\ s := n\ \{n \geq 0 \wedge j = n \wedge s = n\}$	sequence 1, 2
4.	$n \geq 0 \wedge j = n \wedge s = n \rightarrow p$	predicate logic
5.	$\{n \geq 0\}\ j := n;\ s := n\ \{p\}$	postcondition weak. 3, 4
6.	$\{p[s+j/s]\}\ s := s+j\ \{p\}$	assignment (backwards)
7.	$\{p[s+j/s][j-1/j]\}\ j := j-1\ \{p[s+j/s]\}$	assignment (backwards)
8.	$p \wedge j > 0 \rightarrow p[s+j/s][j-1/j]$	predicate logic
9.	$\{p \wedge j > 0\}\ j := j-1\ \{p[s+j/s]\}$	precondition strength. 8, 7
10.	$\{p \wedge j > 0\}\ j := j-1;\ s := s+j\ \{p\}$	sequence 9, 6
11.	$\{inv\ p\}\ W\ \{p \wedge j \leq 0\}$	while 10
12.	$p \wedge j \leq 0 \rightarrow s = sum(0, n)$	predicate logic
13.	$\{inv\ p\}\ W\ \{s = sum(0, n)\}$	postcondition weak. 12, 11
14.	$\{n \geq 0\}\ j := n;\ s := n;\ \{inv\ p\}\ W\ \{s = sum(0, n)\}$	sequence 5, 13

Full Proof Outlines (Solution)

1. (Full outline to proof):

1.	$T \to 0 \geq 0 \wedge 1 = 2\hat{}0$	predicate logic
2.	$\{0 \geq 0 \wedge 1 = 2\hat{}0\}\ k := 0;\ \{k \geq 0 \wedge 1 = 2\hat{}k\}$	assignment (backwards)
3.	$\{T\}\ k := 0;\ \{k \geq 0 \wedge 1 = 2\hat{}k\}$	precondition strength. 1, 2
4.	$\{k \geq 0 \wedge 1 = 2\hat{}k\}\ x := 1\ \{k \geq 0 \wedge x = 2\hat{}k\}$	assignment (backwards)
5.	$\{T\}\ k := 0;\ x := 1\ \{k \geq 0 \wedge x = 2\hat{}k\}$	sequence 3, 4

2a. (Full outline to proof):

1.	$\{-x = abs(x)\}\ y := -x\ \{y = abs(x)\}$	assignment (backwards)
2.	$y = x \wedge x < 0 \to -x = abs(x)$	predicate logic
3.	$\{y = x \wedge x < 0\}\ y := -x\ \{y = abs(x)\}$	precondition strength. 2, 1
4.	$\{y = abs(x)\}\ skip\ \{y = abs(x)\}$	skip
5.	$y = x \wedge x \geq 0 \to y = abs(x)\}$	predicate logic
6.	$\{y = x \wedge x \geq 0\}\ skip\ \{y = abs(x)\}$	precondition strength. 5, 4
7.	$\{y = x\}\ if\ x < 0\ then\ y := -x\ fi\ \{y = abs(x)\}$	conditional 3, 6

2b. (Full outline to proof):

1.	$\{y = x \wedge x < 0\}\ y := -x\ \{y_0 = x \wedge x < 0 \wedge y = -x\}$	assignment (forward)
2.	$\{y = x \wedge x \geq 0\}\ skip\ \{y = x \wedge x \geq 0\}$	skip
3.	$\{y = x\}\ if\ x < 0\ then\ y := -x\ fi$ $\{(y_0 = x \wedge x < 0 \wedge y = -x) \vee (y = x \wedge x \geq 0)\}$	conditional 1, 2
4.	$(y_0 = x \wedge x < 0 \wedge y = -x) \vee (y = x \wedge x \geq 0) \to y = abs(x)$	predicate logic
5.	$\{y = x\}\ if\ x < 0\ then\ y := -x\ fi\ \{y = abs(x)\}$	postcondition weak., 3, 4

2c. (Full outline to proof):

1.	$\{-x = abs(x)\}\ y := -x\ \{y = abs(x)\}$	assignment (backwards)
2.	$\{y = abs(x)\}\ skip\ \{y = abs(x)\}$	skip
3.	$\{p\}\ if\ x < 0\ then\ y := -x\ fi\ \{y = abs(x)\}$ where $p \equiv (x < 0 \to -x = abs(x)) \wedge (x \geq 0 \to y = abs(x))$	conditional 1, 2
4.	$y = x \to p$	predicate Logic
5.	$\{y = x\}\ if\ x < 0\ then\ y := -x\ fi\ \{y = abs(x)\}$	precondition strength. 4, 3

3. Below, let $W \equiv while\ k > 0\ do\ k := k–1;\ s := s+k\ od$

1.	$\{ n \ge 0\}\ k := n\ \{ n \ge 0 \wedge k = n \}$	assignment (forward)
2.	$\{ n \ge 0 \wedge k = n \}\ s := n\ \{ n \ge 0 \wedge k = n \wedge s = n \}$	assignment (forward)
3.	$\{ n \ge 0\}\ k := n;\ s := n\ \{ n \ge 0 \wedge k = n \wedge s = n \}$	sequence 1, 2
4.	$n \ge 0 \wedge k = n \wedge s = n \rightarrow p$	predicate logic
5.	$\{ n \ge 0\}\ k := n;\ s := n\ \{ p \}$	postcondition weak. 3, 4
6.	$\{ p[s+k/s] \}\ s := s+k\ \{ p \}$	assignment (backwards)
7.	$\{ p[s+k/s][k–1/k] \}\ k := k–1\ \{ p[s+k/s] \}$	assignment (backwards)
8.	$p \wedge k > 0 \rightarrow p[s+k/s][k–1/k]$	predicate logic
9.	$\{ p \wedge k > 0\}\ k := k–1\ \{ p[s+k/s] \}$	precondition strength. 8, 7
10.	$\{ p \wedge k > 0\}\ k := k–1;\ s := s+k\ \{ p \}$	sequence 9, 6
11.	$\{inv\ p \}\ W\ \{ p \wedge k \le 0\}$	while 10
12.	$p \wedge k \le 0 \rightarrow s = sum(0, n)$	predicate logic
13.	$\{inv\ p \}\ W\ \{s = sum(0, n) \}$	postcondition weak. 12, 11
14.	$\{ n \ge 0\}\ k := n;\ s := n;\ W\ \{s = sum(0, n) \}$	sequence 5, 13