Proof Outlines for Partial Correctness

Part 1: Full Proof Outlines of Partial Correctness

CS 536: Science of Programming, Fall 2022

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

1. Form the full outline for the proof below. (It's an alternative to Example 1 in the notes.)

1.	$\{T\}\ k := 0\ \{k = 0\}$	*assignment (forward)*
2.	$\{k = 0\}\ x := 1\ \{k = 0 \wedge x = 1\}$	*assignment (forward)*
3.	$k = 0 \wedge x = 1 \rightarrow k \ge 0 \wedge x = 2\hat{\ }k$	*predicate logic*
4.	$\{k = 0\}\ x := 1\ \{k \ge 0 \wedge x = 2\hat{\ }k\}$	*postcondition weakening 2, 3*
5.	$\{T\}\ k := 0;\ x := 1\ \{k \ge 0 \wedge x = 2\hat{\ }k\}$	*sequence 1, 4*

2. Let $W \equiv$ ***while*** $k > 0$ ***do*** $k := k-1;\ s := s+k$ ***od.*** Take the partial proof below and give the full proof outline for it.

1.	$\{n \ge 0\}\ k := n\ \{n \ge 0 \wedge k = n\}$	__________
2.	$\{n \ge 0 \wedge k = n\}\ s := n\ \{n \ge 0 \wedge k = n \wedge s = n\}$	__________
3.	$\{n \ge 0\}\ k := n;\ s := n\ \{n \ge 0 \wedge k = n \wedge s = n\}$	__________
4.	$n \ge 0 \wedge k = n \wedge s = n \rightarrow p$	__________
5.	$\{n \ge 0\}\ k := n;\ s := n\ \{p\}$	__________
6.	$\{p[s+k/s]\}\ s := s+k\ \{p\}$	__________
7.	$\{p[s+k/s][k-1/k]\}\ k := k-1\ \{p[s+k/s]\}$	__________
8.	$p \wedge k > 0 \rightarrow p[s+k/s][k-1/k]$	__________
9.	$\{p \wedge k > 0\}\ k := k-1\ \{p[s+k/s]\}$	__________
10.	$\{p \wedge k > 0\}\ k := k-1;\ s := s+k\ \{p\}$	__________
11.	$\{$**inv** $p\}\ W\ \{p \wedge k \le 0\}$	__________
12.	$p \wedge k \le 0 \rightarrow s = sum(0, n)$	__________
13.	$\{$**inv** $p\}\ W\ \{s = sum(0, n)\}$	__________
14.	$\{n \ge 0\}\ k := n;\ s := n;$	__________
15.	$\{$**inv** $p\}\ W\ \{s = sum(0, n)\}$	__________

For Problems 3–5, you are given a full proof outline; write a corresponding proof of partial correctness from it. There are multiple right answers.

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

4a.. $\{y = x\}$ ***if*** $x < 0$ ***then***

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

else

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

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

4b. $\{y = x\}$ ***if*** $x < 0$ ***then***

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

else

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

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

4c. $\{y = x\}\ \{(x < 0 \rightarrow -x = abs(x)) \land (x \geq 0 \rightarrow y = abs(x))\}$

if $x < 0$ ***then***

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

else

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

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

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

$\{n \geq 0\}\ k := n;\ \{n \geq 0 \land k = n\}\ s := n;\ \{n \geq 0 \land k = n \land s = n\}$

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

while $k > 0$ ***do***

$\{p \land k > 0\}\ \{p[s+k/s][k-1/k]\}\ k := k-1;$

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

od

$\{p \land k \leq 0\}\ \{s = sum(0, n)\}$

Solution to Practice 16 (Full Proof Outlines

Solution

1. (Full outline from formal proof.)

   $\{T\}\ k := 0;\ x := 1\ \{k = 0 \wedge x = 1\}\ \{k \geq 0 \wedge x = 2\text{^}k\}$

2. (Full outline from formal proof.) where $W \equiv$ ***while*** $k > 0$ ***do*** $k{:=}\ k-1;\ s{:=}\ s+k$ ***od.***

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

   $\{$ ***inv*** $p\}$ ***while*** $k > 0$ ***do***

   $\quad\{p \wedge k > 0\}$

   $\quad\{p[s{+}k/s][k{-}1/k]\}\ k{:=}\ k-1$

   $\quad\{p[s{+}k/s]\};\ s{:=}\ s+k$

   $\{p\}$

   od

   $\{p \wedge k \leq 0\}$

   $\{s = sum(0, n)$

3. (Full outline to proof):

1.	$T \rightarrow 0 \geq 0 \wedge 1 = 2\text{^}0$	*predicate logic*
2.	$\{0 \geq 0 \wedge 1 = 2\text{^}0\}\ k := 0;\ \{k \geq 0 \wedge 1 = 2\text{^}k\}$	*assignment (backwards)*
3.	$\{T\}\ k := 0;\ \{k \geq 0 \wedge 1 = 2\text{^}k\}$	*precondition strengthen. 1, 2*
4.	$\{k \geq 0 \wedge 1 = 2\text{^}k\}\ x := 1\ \{k \geq 0 \wedge x = 2\text{^}k\}$	*assignment (backwards)*
5.	$\{T\}\ k := 0;\ x := 1\ \{k \geq 0 \wedge x = 2\text{^}k\}$	*sequence 3, 4*

4a. (Full outline to proof):

1.	$\{-x = abs(x)\}\ y := -x\ \{y = abs(x)\}$	*assignment (backwards)*
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*

4b. (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.	$(y_0 = x \wedge x < 0 \wedge y = -x) \vee (y = x \wedge x \geq 0) \rightarrow y = abs(x)$	*predicate logic*
5.	$\{y = x\}$ ***if*** $x < 0$ ***then*** $y := -x$ ***fi*** $\{y = abs(x)\}$	*postcondition weak., 3, 4*

© James Sasaki, 2022

*4c. (Full ou*tline 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* $\{y = abs(x)\}$ — *conditional 1, 2*
   where $p \equiv (x < 0 \rightarrow -x = abs(x)) \wedge (x \geq 0 \rightarrow y = abs(x))$
4. $y = x \rightarrow p$ — *predicate Logic*
5. $\{y = x\}$ ***if*** $x < 0$ ***then*** $y := -x$ *fi* $\{y = abs(x)\}$ — *precondition strength. 4, 3*

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

1. $\{n \geq 0\}\ k := n\ \{n \geq 0 \wedge k = n\}$ — *assignment (forward)*
2. $\{n \geq 0 \wedge k = n\}\ s := n\ \{n \geq 0 \wedge k = n \wedge s = n\}$ — *assignment (forward)*
3. $\{n \geq 0\}\ k := n;\ s := n\ \{n \geq 0 \wedge k = n \wedge s = n\}$ — *sequence 1, 2*
4. $n \geq 0 \wedge k = n \wedge s = n \rightarrow p$ — *predicate logic*
5. $\{n \geq 0\}\ k := n;\ s := n\ \{p\}$ — *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*** $p\}\ W\ \{p \wedge k \leq 0\}$ — *while 10*
12. $p \wedge k \leq 0 \rightarrow s = sum(0, n)$ — *predicate logic*
13. $\{$***inv*** $p\}\ W\ \{s = sum(0, n)\}$ — *postcondition weak. 12, 11*
14. $\{n \geq 0\}\ k := n;\ s := n;\ W\ \{s = sum(0, n)\}$ — *sequence 5, 13*

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

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

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

while $k > 0$ ***do***

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

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

od

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

 © James Sasaki, 2022