

Section 8.2 Program Correctness (for imperative programs)

A theory of program correctness needs wffs, axioms, and inference rules.

Wffs (called Hoare triples) are of the form

$$\{P\} S \{Q\}$$

Where S is a program statement and P (a *precondition*) and Q (a *postcondition*) are logical statements about the variables of S .

Semantics: The meaning of $\{P\} S \{Q\}$ is the truth value of the statement:

If P is true before S executes, then Q is true after S halts.

Note that it is assumed that S halts. If $\{P\} S \{Q\}$ is true, then S is said to be *correct* wrt to precondition P and postcondition Q .

Assignment Axiom (AA): $\{P(x/t)\} x := t \{P\}$.

Example. $\{x = 4\} x := x - 1 \{x = 3\}$.

Example. $\{x < 4\} x := x - 1 \{x < 3\}$.

Inference Rules

Consequence Rule:

$$\frac{P \rightarrow R \text{ and } \{R\} S \{Q\}}{\therefore \{P\} S \{Q\}} \quad \text{and} \quad \frac{\{P\} S \{T\} \text{ and } T \rightarrow Q}{\therefore \{P\} S \{Q\}}$$

Example. Prove the correctness of $\{x < 3\} x := x - 1 \{x < 3\}$.

Proof:	1.	$\{x < 4\} x := x - 1 \{x < 3\}$	AA
	2.	$x < 3$	P
	3.	$x < 4$	2, T
	4.	$(x < 3) \rightarrow (x < 4)$	2, 3, CP
	5.	$\{x < 3\} x := x - 1 \{x < 3\}$	1, 4, Consequence. QED.

Example/Quiz. Prove the correctness of $\{\exists x (y = 2x)\} y := y + 3 \{\exists x (y = 2x + 1)\}$.

Proof:

1.	$\{\exists x (y + 3 = 2x + 1)\} y := y + 3 \{\exists x (y = 2x + 1)\}$	AA
2.	$\exists x (y = 2x)$	P
3.	$y = 2c$	2, EI
4.	$(y = 2c) \rightarrow (y + 3 = 2c + 3)$	EE, where $f(x) = x + 3$
5.	$y + 3 = 2c + 3$	3, 4, MP
6.	$y + 3 = 2(c + 1) + 1$	5, T
7.	$\exists x (y + 3 = 2x + 1)$	6, EG
8.	$\exists x (y = 2x) \rightarrow \exists x (y + 3 = 2x + 1)$	2, 7, CP
9.	$\{\exists x (y = 2x)\} y := y + 3 \{\exists x (y = 2x + 1)\}$	1, 8, Consequence

QED.

Composition Rule:
$$\frac{\{P\} S_1 \{Q\} \text{ and } \{Q\} S_2 \{R\}}{\therefore \{P\} S_1 ; S_2 \{R\}}$$

Example/Quiz. Prove the correctness of $\{x < 2\} y := 2x; x := y - 3 \{x < 1\}$.

Proof:

1.	$\{y - 3 < 1\} x := y - 3 \{x < 1\}$	AA
2.	$\{2x - 3 < 1\} y := 2x \{y - 3 < 1\}$	AA
3.	$\{2x - 3 < 1\} y := 2x; x := y - 3 \{x < 1\}$	1, 2, Composition
4.	$x < 2$	P
5.	$2x < 4$	4, T
6.	$2x - 3 < 1$	5, T
7.	$(x < 2) \rightarrow (2x - 3 < 1)$	4, 6, CP
8.	$\{x < 2\} y := 2x; x := y - 3 \{x < 1\}$	3, 7, Consequence

QED.

If-Then Rule:
$$\frac{\{P \wedge C\} S \{Q\} \text{ and } P \wedge \neg C \rightarrow Q}{\therefore \{P\} \text{ if } C \text{ then } S \{Q\}}$$

Example/Quiz. Prove the correctness of $\{x > 0\}$ **if** $x > 1$ **then** $x := x - 1$ $\{x > 0\}$.

Proof:

1.	$\{x - 1 > 0\} x := x - 1 \{x > 0\}$	AA
2.	$(x > 0) \wedge (x > 1)$	P
3.	$x > 1$	2, Simp
4.	$x - 1 > 0$	3, T
5.	$(x > 0) \wedge (x > 1) \rightarrow (x - 1 > 0)$	2, 4, CP
6.	$\{(x > 0) \wedge (x > 1)\} x := x - 1 \{x > 0\}$	1, 5, Consequence
7.	$(x > 0) \wedge \neg(x > 1)$	P
8.	$x > 0$	7, Simp
9.	$(x > 0) \wedge \neg(x > 1) \rightarrow (x > 0)$	7, 8, CP
10.	$\{x > 0\}$ if $x > 1$ then $x := x - 1$ $\{x > 0\}$	6, 9, If-Then

QED.

If-Then-Else Rule:
$$\frac{\{P \wedge C\} S_1 \{Q\} \text{ and } \{P \wedge \neg C\} S_2 \{Q\}}{\therefore \{P\} \text{ if } C \text{ then } S_1 \text{ else } S_2 \{Q\}}$$

Example/Quiz. Prove the correctness of $\{\text{true}\}$ **if** $x < y$ **then** $z := x$ **else** $z := y$ $\{(z \leq x) \wedge (z \leq y)\}$.

Proof: By the if-then-else rule it suffices to prove the correctness of the two statements,

1. $\{\text{true} \wedge (x < y)\} z := x \{(z \leq x) \wedge (z \leq y)\}$.
2. $\{\text{true} \wedge \neg(x < y)\} z := y \{(z \leq x) \wedge (z \leq y)\}$.

While Rule:
$$\frac{\{P \wedge C\} S \{P\}}{\therefore \{P\} \text{ while } C \text{ do } S \{P \wedge \neg C\}} \quad (P \text{ is called a } \textit{loop invariant})$$

Example/Quiz. Prove the correctness of the following wff, where $\text{int}(x)$ means x is an integer.

$\{ \text{int}(x) \wedge (x > 0) \}$
while $\text{even}(x)$ **do** $x := x/2$
 $\{ \text{int}(x) \wedge (x > 0) \wedge \text{odd}(x) \}$.

This wff matches the conclusion of the while rule, where

$P = \text{int}(x) \wedge (x > 0)$, $C = \text{even}(x)$, and $S = "x := x/2"$

So by the while rule the wff will be correct if we can prove the correctness of

$\{P \wedge C\} x := x/2 \{P\}$.

Proof:	1.	$\{ \text{int}(x/2) \wedge (x/2 > 0) \} x := x/2 \{ \text{int}(x) \wedge (x > 0) \}$	AA
	2.	$\text{int}(x) \wedge (x > 0) \wedge \text{even}(x)$	P (This is $P \wedge C$)
	3.	$x > 0$	2, Simp
	4.	$x/2 > 0$	3, T
	5.	$\text{int}(x) \wedge \text{even}(x)$	2, Simp
	6.	$\text{int}(x) \wedge \text{even}(x) \rightarrow \text{int}(x/2)$	T
	7.	$\text{int}(x/2)$	5, 6, MP
	8.	$\text{int}(x/2) \wedge (x/2 > 0)$	4, 7, Conj
	9.	$\text{int}(x) \wedge (x > 0) \wedge \text{even}(x) \rightarrow \text{int}(x/2) \wedge (x/2 > 0)$	2, 8, CP
	10.	(Statement to be proved)	1, 9, Consequence

QED.

Example (Discovering a loop invariant). Given two integers $x \leq y$, the sum

$$x + (x + 1) + \dots + y$$

can be calculated by the formula $(x + y) (y - x + 1)/2$. The sum can also be calculated by the following program (for those who don't know the formula):

$$\{\text{int}(x) \wedge \text{int}(y) \wedge (x \leq y)\} = \{A\}$$

$s := x;$

$i := x;$

while $i < y$ **do**

$i := i + 1;$

$s := s + i$

od

$$\{s = (x + y) (y - x + 1)/2\} = \{B\}$$

To prove the correctness of this program wrt A and B we need to find a loop invariant P for the while-statement. Then we need to prove the following three statements:

- $\{A\} s := x; i := x \{P\}$
- $\{P\} \text{ while } i < y \text{ do } i := i + 1; s := s + i \text{ od } \{P \wedge \neg (i < y)\}$
- $P \wedge \neg (i < y) \rightarrow B$

Notice that P should be a statement involving the variables i , s , x , and y . Why?

After some trial and error, a candidate for P appears to be the statement

$$(s = (x + i)(i - x + 1)/2) \wedge (i \leq y).$$

Quiz (On your time). Prove the correctness of the program.

Array Assignment

Suppose we try to prove the correctness of the following wff.

$$\{(i = j) \wedge (a[i] = 1)\} a[i] := 2 \{a[j] = 2\}.$$

If we start the proof by using AA, we obtain $\{a[j] = 2\} a[i] := 2 \{a[j] = 2\}$.

Now we might try to use the consequence rule. But the following wff is false.

$$(i = j) \wedge (a[i] = 1) \rightarrow a[j] = 2.$$

So AA can't be used to prove correctness for array assignment. We need a new axiom.

Array Assignment Axiom (AAA): $\{P\} a[i] := t \{Q\}$, where P is obtained from Q by:

- Replace all occurrences of $a[i]$ in Q by t .
- Replace all occurrences of $a[j]$ in Q by “if $j = i$ then t else $a[j]$ ”.
- *Restriction:* An expression $a[\dots]$ may not occur in the expressions i and j .

Note: (if A then B else C) $\equiv (A \rightarrow B) \wedge (\neg A \rightarrow C)$. So we can write

$$(\text{if } j = i \text{ then } t \text{ else } a[j]) \equiv ((i = j) \rightarrow t) \wedge ((i \neq j) \rightarrow a[j]).$$

Example. Prove the correctness of $\{(i = j) \wedge (a[i] = 1)\} a[i] := 2 \{a[j] = 2\}$.

<i>Proof:</i>	1. $\{(\text{if } j = i \text{ then } 2 \text{ else } a[j]) = 2\} a[i] := 2 \{a[j] = 2\}$	AAA
	2. $(i = j) \wedge (a[i] = 1)$	P
	3. $i = j$	2, Simp
	4. $(i = j) \rightarrow (2 = 2)$	EA, T (trivial)
	5. $(i \neq j) \rightarrow (a[j] = 2)$	3, Add, T , (or vacuous)
	6. $((i = j) \rightarrow (2 = 2)) \wedge ((i \neq j) \rightarrow (a[j] = 2))$	4, 5, Conj
	7. $(\text{if } j = i \text{ then } 2 \text{ else } a[j]) = 2$	6, T
	8. $(i = j) \wedge (a[i] = 1) \rightarrow ((\text{if } j = i \text{ then } 2 \text{ else } a[j]) = 2)$	2, 7, CP
	QED	1, 8, Consequence.

Example (The Restriction is Needed). Consider the wff

$$\{(a[1] = 1) \wedge (a[2] = 1)\} a[a[1]] := 2 \{a[a[1]] = 2\}.$$

This wff is not correct because $a[a[1]] = 1$ after execution of the assignment statement. But if we used AAA without regard to the restriction, we would obtain

$$\{2 = 2\} a[a[1]] := 2 \{a[a[1]] = 2\}.$$

Now we can apply the consequence rule to the following trivially true statement.

$$(a[1] = 1) \wedge (a[2] = 1) \rightarrow (2 = 2).$$

So we would conclude, falsely, that the wff is correct.

- *Satisfying the Restriction*

Replace $a[a[k]] := t$ with $i := a[k]; a[i] := t$.

Replace $a[a[k]] = t$ with $\exists x ((x = a[k]) \wedge (a[x] = t))$.

Example (Revisited). Attempt to prove the correctness of the following wff.

$$\{(a[1] = 1) \wedge (a[2] = 1)\} i := a[1]; a[i] := 2 \{\exists x ((x = a[1]) \wedge (a[x] = 2))\}.$$

Proof Attempt: Apply AAA to $a[i] := 2$ and the postcondition to obtain

$$\{\exists x [(x = (\text{if } 1 = i \text{ then } 2 \text{ else } a[1])) \wedge ((\text{if } x = i \text{ then } 2 \text{ else } a[x]) = 2)]\}$$

Now apply AA to $i := a[1]$ and the above condition to obtain

$$\{\exists x [(x = (\text{if } 1 = a[1] \text{ then } 2 \text{ else } a[1])) \wedge ((\text{if } x = a[1] \text{ then } 2 \text{ else } a[x]) = 2)]\}$$

What next? To use the consequence rule we need to show that $(a[1] = 1) \wedge (a[2] = 1) \rightarrow P$, where P is the preceding precondition. But this is an INVALID statement. If we assume it is valid, then from the premise $(a[1] = 1) \wedge (a[2] = 1)$ we can use MP, EI, and equality axioms to conclude that $a[2] = 2$, which contradicts $a[2] = 1$.

Termination of Loops

The correctness of $\{P\} S \{Q\}$ assumes that S terminates. So we have to prove termination to have *total correctness*.

The *state* of a computation at some point in time is the tuple of variable values at the point.

Idea for proving a loop terminates: Find a well-founded set $\langle W, < \rangle$ and associate the state of the i th iteration of the loop with an element $x_i \in W$ such that

$$x_1 > x_2 > x_3 > \dots$$

Since W is well-founded, the chain stops. Therefore the loop terminates.

Termination Condition. Given the following while-program with loop invariant P .

$\{P\}$ **while** C **do** S $\{P \wedge \neg C\}$.

To prove that the program terminates perform the following actions, where s is the state before S executes and t is the state after S executes.

Find a well-founded set $\langle W, < \rangle$.

Find an expression $f(\dots)$ of the program variables.

Prove: $P \wedge C \rightarrow (f(s) \in W) \wedge (f(t) \in W) \wedge (f(s) > f(t))$.

Example. Show that the following program terminates, where $\text{int}(x)$ means x is an integer.

$\{\text{int}(x) \wedge (x > 0)\}$ **while** $\text{even}(x)$ **do** $x := x/2$ $\{\text{int}(x) \wedge (x > 0) \wedge \text{odd}(x)\}$.

Proof: Let $s = (x)$. Then $t = (x/2)$. Choose the well-founded set $\langle \mathbf{N}, < \rangle$. Let $f(x) = x$.

Assume $\text{int}(x) \wedge (x > 0) \wedge \text{even}(x)$. Then $x \in \mathbf{N}$, $x > 0$ and $x = 2k$ for some $k \in \mathbf{N}$ with $k > 0$.

So $f(s) = f(x) = x \in \mathbf{N}$ and $f(t) = f(x/2) = x/2 = k \in \mathbf{N}$ and $f(s) = x = 2k > k = f(t)$.

Therefore, the program terminates. QED.

Example. The following program terminates, where $q(x)$ means x is a rational number.

$\{q(x) \wedge q(y)\}$
while $x < y$ **do** $x := x + 1; y := y + 1/2$ **od**
 $\{q(x) \wedge q(y) \wedge (x \geq y)\}$.

Proof: Let $s = (x, y)$. Then $t = (x + 1, y + 1/2)$. Choose the well-founded set $\langle \mathbf{N}, < \rangle$. Now try out some possible definitions of f :

(1) $f(x, y) = y - x$. Is this OK?

NO. Let $x = 1/2$ and $y = 2$. Then $f(s) = f(x, y) = f(1/2, 2) = 2 - 1/2 = 3/2 \notin \mathbf{N}$.

(2) $f(x, y) = \lfloor y - x \rfloor$. Is this OK?

NO. Let $x = 1/2$ and $y = 1$. Then $f(s) = f(1/2, 1) = \lfloor 1 - 1/2 \rfloor = \lfloor 1/2 \rfloor = 0 \in \mathbf{N}$.

Also $f(t) = f(x + 1, y + 1/2) = f(3/2, 3/2) = \lfloor 3/2 - 3/2 \rfloor = \lfloor 0 \rfloor = 0 \in \mathbf{N}$. But $f(s) = f(t)$.

(3) $f(x, y) = \lceil y - x \rceil$. Is this OK?

Quiz. Why is the answer NO?

Answer: Let $x = 1$ and $y = 2$. Then $f(s) = f(x, y) = f(1, 2) = \lceil 2 - 1 \rceil = \lceil 1 \rceil = 1 \in \mathbf{N}$.

Also $f(t) = f(x + 1, y + 1/2) = f(2, 5/2) = \lceil 5/2 - 2 \rceil = \lceil 1/2 \rceil = 1 \in \mathbf{N}$. But $f(s) = f(t)$.

Quiz: Prove termination with $f(x, y) = \lceil 2(y - x) \rceil$.

Proof: Assume $q(x) \wedge q(y) \wedge (x < y)$. Then $f(s) = f(x, y) = \lceil 2(y - x) \rceil = \lceil 2y - 2x \rceil \geq 1$.

We also have $f(t) = f(x + 1, y + 1/2) = \lceil 2((y + 1/2) - (x + 1)) \rceil = \lceil 2y - 2x - 1 \rceil \geq 0$.

So $f(s) \in \mathbf{N}$, $f(t) \in \mathbf{N}$, and $f(s) = \lceil 2y - 2x \rceil > \lceil 2y - 2x - 1 \rceil = f(t)$.

Therefore the program terminates. QED.

Example. The following program terminates, where $q(x)$ means x is a rational number.

$\{q(x) \wedge q(y) \wedge (y > 0)\}$
while $x > y$ **do** $x := x - y$ **od**
 $\{q(x) \wedge q(y) \wedge (y > 0) \wedge (x \leq y)\}$

Proof: Let $s = (x, y)$. Then $t = (x - y, y)$. Choose the well-founded set $\langle \mathbf{N}, < \rangle$.

Quiz: Show that each of the following possible definitions of f do not work.

(1) $f(x, y) = x - y$.

NO. Let $x = 1/2$ and $y = 1/4$. Then $f(s) = f(1/2, 1/4) = 1/2 - 1/4 = 1/4 \notin \mathbf{N}$.

(2) $f(x, y) = \lceil x - y \rceil$.

NO. Let $x = 1/2$ and $y = 1/8$. Then $f(s) = f(1/2, 1/8) = \lceil 1/2 - 1/8 \rceil = \lceil 3/8 \rceil = 1 \in \mathbf{N}$.

Also, $f(t) = f(1/2 - 1/8, 1/8) = \lceil 3/8 - 1/8 \rceil = \lceil 1/4 \rceil = 1 \in \mathbf{N}$. But $f(s) = f(t)$.

(3) $f(x, y) = \lceil x \rceil$.

NO. Let $x = 1/2$ and $y = 1/4$. Then $f(s) = f(1/2, 1/4) = \lceil 1/2 \rceil = 1 \in \mathbf{N}$.

Also, $f(t) = f(1/2 - 1/4, 1/4) = f(1/4, 1/4) = \lceil 1/4 \rceil = 1 \in \mathbf{N}$. But $f(s) = f(t)$.

Quiz: Prove termination with $f(x, y) = \lceil x/y \rceil$.

Proof: Assume $q(x) \wedge q(y) \wedge (y > 0) \wedge (x > y)$. Then $x/y > 1$. Calculate $f(s)$ and $f(t)$.

$f(s) = f(x, y) = \lceil x/y \rceil \in \mathbf{N}$ and $\lceil x/y \rceil \geq 2$ because $x/y > 1$.

$f(t) = f(x - y, y) = \lceil (x - y)/y \rceil = \lceil (x/y) - 1 \rceil = \lceil x/y \rceil - 1 \in \mathbf{N}$ because $\lceil x/y \rceil \geq 2$.

Also, we have $f(s) = \lceil x/y \rceil > \lceil x/y \rceil - 1 = f(t)$. So the program terminates. QED.