Program Correctness (Section 8.1)

Program Correctness (for imperative programs)

- A theory of program correctness needs wffs, axioms, and inference rules. The 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* with respect to (wrt) precondition P and postcondition Q.

Assignment Axiom

- The Assignment Axiom (AA) is: $\{P(x/t)\}\ x := t\ \{P\}$.
- *Example:* $\{x = 4\}\ x := x - 1\ \{x = 3\}$
- Consequence Rules are
  - $\frac{P \to R \text{ and } \{R\}S\{Q\}}{\{P\}S\{Q\}}$
  - $\frac{\{P\}S\{T\} \text{ and } T \to Q}{\{P\}S\{Q\}}$

Example Proof

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

1.	$\{x < 4\}x := x - 1\{x < 3\}$	AA
2.	$\quad x < 3$	P [for $(x < 3) \to (x < 4)$]
3.	$\quad x < 4$	2,T
4.	$(x < 3) \to (x < 4)$	2,3,CP
5.	$\{x < 3\}x := x - 1\{x < 3\}$	1,4,Consequence. QED

Another Correctness Proof

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

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

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

Example proof

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

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. $\quad x < 2$	P [for $(x < 2) \rightarrow (2x - 3 < 1)$]
5. $\quad 2x < 4$	4,T
6. $\quad 2x - 3 < 1$	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 Rules

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

If proof

Prove the correctness of $\{x > 0\}\textbf{if } x > 1 \textbf{ then } x := x - 1\{x > 0\}$

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

QED

While rule

- $\dfrac{\{P \wedge C\} S \{P\}}{\{P\} \textbf{while } C \textbf{ do } S \{P \wedge \neg C\}}$
- P is called a *loop invariant*

Additional issues

Two additional issues that the book investigates are: arrays and array indices, and loop termination.

Section 8.2

This section is about Higher-Order Logic. This allows us to, for example, quantify over predicates, rather than just variables. We won't study this idea.