<table>
<thead>
<tr>
<th><strong>Title:</strong></th>
<th><em>Specification and Verification I</em></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lecturer:</strong></td>
<td>Mike Gordon</td>
</tr>
<tr>
<td><strong>Class:</strong></td>
<td>Computer Science Tripos, Part II</td>
</tr>
<tr>
<td><strong>Duration:</strong></td>
<td>Twelve lectures</td>
</tr>
</tbody>
</table>
Specification and Verification I

Mike Gordon

Overview
These lecture notes are for the course entitled Specification and Verification I. Some of the material is derived from previously published sources.1

Chapters 1–4 introduce classical ideas of specification and proof of programs due to Floyd and Hoare. Chapter 5 is an introduction to program refinement using an approach due to Paul Curzon. Chapter 6 presents higher order logic and Chapter 7 explains how Floyd-Hoare logic can be embedded in higher order logic.

The course presents classical ideas on the specification and verification of software. Although much of the material is old – see the dates on some of the cited references – it is still a key foundation for current research.2

This course is a prerequisite for the Part II course entitled Specification and Verification II, which makes extensive use of higher order logic (see Chapter 6) for specifying and verifying hardware.

Learning Guide
These notes contain all the material that will be covered in the course. It should thus not be necessary to consult any textbooks etc.

The copies of transparencies give the contents of the lectures. However note that I sometimes end up going faster or slower than expected so, for example, material shown in Lecture n might actually get covered in Lecture n+1 or Lecture n−1.

The examination questions will be based on material in the lectures. Thus if I end up not covering some topic in the lectures, then I would not expect to set an examination question on it.

This course has been fairly stable for several years, so past exam questions are a reasonable guide to the sort of thing I will set this year.

Acknowledgement
Paul Curzon made many improvements, extensions and corrections to these notes.

---


2See www.dcs.qmul.ac.uk/~ohearn/localreasoning.html for a current research thread.
Contents

1 Program Specification 7
  1.1 Introduction ............................................. 7
  1.2 A little programming language .......................... 7
    1.2.1 Assignments ........................................ 8
    1.2.2 Array assignments .................................. 8
    1.2.3 Sequences .......................................... 9
    1.2.4 Blocks ............................................. 9
    1.2.5 One-armed conditionals .............................. 9
    1.2.6 Two-armed conditionals ............................... 9
    1.2.7 WHILE-commands .................................. 10
    1.2.8 FOR-commands ..................................... 10
    1.2.9 Summary of syntax .................................. 10
  1.3 Hoare's notation ........................................ 11
  1.4 Some examples .......................................... 12
  1.5 Terms and statements ................................... 14

2 Floyd-Hoare Logic 17
  2.1 Axioms and rules of Floyd-Hoare logic .................. 18
    2.1.1 The assignment axiom ................................ 19
    2.1.2 Precondition strengthening .......................... 21
    2.1.3 Postcondition weakening .............................. 22
    2.1.4 Specification conjunction and disjunction ........... 22
    2.1.5 The sequencing rule .................................. 23
    2.1.6 The derived sequencing rule .......................... 24
    2.1.7 The block rule ...................................... 24
    2.1.8 The derived block rule ................................ 25
    2.1.9 The conditional rules ................................ 26
    2.1.10 The WHILE-rule ...................................... 28
    2.1.11 The FOR-rule ....................................... 29
    2.1.12 Arrays ............................................ 34
  2.2 Soundness and completeness ............................... 37
  2.3 Some exercises .......................................... 38
3 Mechanizing Program Verification 47
  3.1 Overview 47
  3.2 Verification conditions 49
  3.3 Annotation 50
  3.4 Verification condition generation 51
  3.5 Justification of verification conditions 58

4 Total Correctness 63
  4.1 Axioms and rules for non-looping commands 63
  4.2 Derived rule for total correctness of non-looping commands 65
  4.3 The termination of assignments 65
  4.4 WHILE-rule for total correctness 66
  4.5 Termination specifications 67
  4.6 Verification conditions for termination 67
  4.7 Verification condition generation 68

5 Program Refinement 75
  5.1 Introduction 75
  5.2 Refinement laws 76
  5.3 An example 79
  5.4 General remarks 80

6 Higher Order Logic 81
  6.1 Terms 83
    6.1.1 Variables and constants 83
    6.1.2 Function applications 83
    6.1.3 Lambda-terms 83
  6.2 Types 84
    6.2.1 Type variables and polymorphism 86
  6.3 Special Syntactic Forms 86
    6.3.1 Infixes 87
    6.3.2 Binders 87
    6.3.3 Pairs and tuples 88
    6.3.4 Lists 89
    6.3.5 Conditionals 89
    6.3.6 Hilbert’s ε-operator 89
  6.4 Definitions 91
  6.5 Peano’s axioms 91
    6.5.1 Primitive recursion 92
    6.5.2 Arithmetic 93
    6.5.3 Lists 94
7 Deriving Floyd-Hoare Logic

7.1 Semantic embedding ........................................... 97
7.2 A simple imperative programming language ...................... 98
  7.2.1 Axioms and rules of Hoare logic .......................... 99
7.3 Semantics in logic ............................................. 100
  7.3.1 Semantics of commands .................................... 102
  7.3.2 Semantics of partial correctness specifications .......... 104
7.4 Floyd-Hoare logic as higher order logic ......................... 105
  7.4.1 Derivation of the SKIP-axiom .............................. 106
  7.4.2 Derivation of precondition strengthening ................ 106
  7.4.3 Derivation of postcondition weakening .................... 107
  7.4.4 Derivation of the sequencing rule ......................... 107
  7.4.5 Derivation of the IF-rule .................................. 107
  7.4.6 Derivation of the WHILE-rule ............................. 107
  7.4.7 Derivation of the assignment axiom ....................... 108
7.5 Termination and total correctness ................................ 109
  7.5.1 Derived rules for total correctness ....................... 110
7.6 Other programming logic constructs ............................ 111
  7.6.1 VDM-style specifications ................................. 111
  7.6.2 Dijkstra’s weakest preconditions ......................... 114
  7.6.3 Dynamic logic ........................................... 117

Bibliography
Chapter 1

Program Specification

A simple programming language containing assignments, conditionals, blocks, WHILE-commands and FOR-commands is introduced. This language is then used to illustrate Hoare’s notation for specifying the partial correctness of programs. Hoare’s notation uses predicate calculus to express conditions on the values of program variables. A fragment of predicate calculus is introduced and illustrated with examples.

1.1 Introduction

In order to prove mathematically the correctness of a program one must first specify what it means for it to be correct. In this chapter a notation for specifying the desired behaviour of imperative programs is described. This notation is due to C.A.R. Hoare.

Executing an imperative program has the effect of changing the state, i.e. the values of program variables\(^1\). To use such a program, one first establishes an initial state by setting the values of some variables to values of interest. One then executes the program. This transforms the initial state into a final one. One then inspects (using print commands etc.) the values of variables in the final state to get the desired results. For example, to compute the result of dividing \(y\) into \(x\) one might load \(x\) and \(y\) into program variables \(X\) and \(Y\), respectively. One might then execute a suitable program (see Example 7 in Section 1.4) to transform the initial state into a final state in which the variables \(Q\) and \(R\) hold the quotient and remainder, respectively.

The programming language used in these notes is described in the next section.

1.2 A little programming language

Programs are built out of commands like assignments, conditionals etc. The terms ‘program’ and ‘command’ are really synonymous; the former will only be used for commands representing complete algorithms. Here the term ‘statement’ is used

\(^1\)For languages more complex than those described here, the state may consist of other things besides the values of variables [16].
for conditions on program variables that occur in correctness specifications (see Section 1.3). There is a potential for confusion here because some writers use this word for commands (as in ‘for-statement’ [21]).

We now describe the *syntax* (i.e. form) and *semantics* (i.e. meaning) of the various commands in our little programming language. The following conventions are used:

1. The symbols $V, V_1, \ldots, V_n$ stand for arbitrary variables. Examples of particular variables are $X, R, Q$ etc.
2. The symbols $E, E_1, \ldots, E_n$ stand for arbitrary expressions (or terms). These are things like $x + 1$, $\sqrt{2}$ etc. which denote values (usually numbers).
3. The symbols $S, S_1, \ldots, S_n$ stand for arbitrary statements. These are conditions like $x < y$, $x^2 = 1$ etc. which are either true or false.
4. The symbols $C, C_1, \ldots, C_n$ stand for arbitrary commands of our programming language; these are described in the rest of this section.

Terms and statements are described in more detail in Section 1.5.

### 1.2.1 Assignments

**Syntax:** $V := E$

**Semantics:** The state is changed by assigning the value of the term $E$ to the variable $V$.

**Example:** $X := X + 1$

This adds one to the value of the variable $X$.

### 1.2.2 Array assignments

**Syntax:** $V(E_1) := E_2$

**Semantics:** The state is changed by assigning the value of the term $E_2$ to the $E_1$th component of the array variable $V$.

**Example:** $A(X+1) := A(X) + 2$

If the value of $X$ is $n$ then the value stored in the $n+1$th component of $A$ becomes the value of the $n$th component of $A$ plus 2.
1.2.3 Sequences

Syntax: $C_1; \cdots; C_n$

Semantics: The commands $C_1, \cdots, C_n$ are executed in that order.

Example: $R := X; \ X := Y; \ Y := R$

The values of $X$ and $Y$ are swapped using $R$ as a temporary variable. This command has the side effect of changing the value of the variable $R$ to the old value of the variable $X$.

1.2.4 Blocks

Syntax: \begin{verbatim} BEGIN VAR V_1; \cdots VAR V_n; C END \end{verbatim}

Semantics: The command $C$ is executed, and then the values of $V_1, \cdots, V_n$ are restored to the values they had before the block was entered. The initial values of $V_1, \cdots, V_n$ inside the block are unspecified.

Example: \begin{verbatim} BEGIN VAR R; \ R := X; \ X := Y; \ Y := R END \end{verbatim}

The values of $X$ and $Y$ are swapped using $R$ as a temporary variable. This command does not have a side effect on the variable $R$.

1.2.5 One-armed conditionals

Syntax: $\text{IF } S \text{ THEN } C$

Semantics: If the statement $S$ is true in the current state, then $C$ is executed. If $S$ is false, then nothing is done.

Example: $\text{IF } \neg(X=0) \text{ THEN } R := Y \div X$

If the value $X$ is not zero, then $R$ is assigned the result of dividing the value of $Y$ by the value of $X$.

1.2.6 Two-armed conditionals

Syntax: $\text{IF } S \text{ THEN } C_1 \text{ ELSE } C_2$

Semantics: If the statement $S$ is true in the current state, then $C_1$ is executed. If $S$ is false, then $C_2$ is executed.

Example: $\text{IF } X < Y \text{ THEN } \text{MAX} := Y \text{ ELSE } \text{MAX} := X$

The value of the variable $\text{MAX}$ it set to the maximum of the values of $X$ and $Y$. 
1.2.7  **WHILE**-commands  

**Syntax:**  `WHILE S DO C`  

**Semantics:** If the statement `S` is true in the current state, then `C` is executed and the **WHILE**-command is then repeated. If `S` is false, then nothing is done. Thus `C` is repeatedly executed until the value of `S` becomes false. If `S` never becomes false, then the execution of the command never terminates.  

**Example:**  `WHILE ¬(X=0) DO X:= X-2`  

If the value of `X` is non-zero, then its value is decreased by 2 and then the process is repeated. This **WHILE**-command will terminate (with `X` having value 0) if the value of `X` is an even non-negative number. In all other states it will not terminate.  

1.2.8  **FOR**-commands  

**Syntax:**  `FOR V:=E₁ UNTIL E₂ DO C`  

**Semantics:** If the values of terms `E₁` and `E₂` are positive numbers `e₁` and `e₂` respectively, and if `e₁ ≤ e₂`, then `C` is executed `(e₂−e₁)+1` times with the variable `V` taking on the sequence of values `e₁, e₁+1, . . . , e₂` in succession. For any other values, the **FOR**-command has no effect. A more precise description of this semantics is given in Section 2.1.11.  

**Example:**  `FOR N:=1 UNTIL M DO X:=X+N`  

If the value of the variable `M` is `m` and `m ≥ 1`, then the command `X:=X+N` is repeatedly executed with `N` taking the sequence of values `1, . . . , m`. If `m < 1` then the **FOR**-command does nothing.  

1.2.9  **Summary of syntax**  

The syntax of our little language can be summarized with the following specification in BNF notation\(^2\)  

\[
<\text{command}> ::= <\text{variable}> : = <\text{term}> \\
| <\text{variable}>(<\text{term}>): = <\text{term}> \\
| <\text{command}>; . . . ; <\text{command}> \\
| \text{BEGIN} VAR <\text{variable}>; . . . VAR <\text{variable}>; <\text{command}> \text{ END} \\
| \text{IF} <\text{statement}> \text{ THEN} <\text{command}> \\
| \text{IF} <\text{statement}> \text{ THEN} <\text{command}> \text{ ELSE} <\text{command}> \\
| \text{WHILE} <\text{statement}> \text{ DO} <\text{command}> \\
| \text{FOR} <\text{variable}> : = <\text{term}> \text{ UNTIL} <\text{term}> \text{ DO} <\text{command}> \\
\]

\(^2\)BNF stands for Backus-Naur form; it is a well-known notation for specifying syntax.
Note that:

- Variables, terms and statements are as described in Section 1.5.
- Only declarations of the form ‘VAR <variable>’ are needed. The types of variables need not be declared (unlike in Pascal).
- Sequences $C_1; \ldots C_n$ are valid commands; they are equivalent to `BEGIN $C_1; \ldots C_n$ END` (i.e. blocks without any local variables).
- The BNF syntax is ambiguous: it does not specify, for example, whether `IF $S_1$ THEN IF $S_2$ THEN $C_1$ ELSE $C_2$` means

\[
\text{IF } S_1 \text{ THEN (IF } S_2 \text{ THEN } C_1 \text{ ELSE } C_2) \]

or

\[
\text{IF } S_1 \text{ THEN (IF } S_2 \text{ THEN } C_1 \text{ ELSE } C_2) \]

We will clarify, whenever necessary, using brackets.

1.3 Hoare’s notation

In a seminal paper [20] C.A.R. Hoare introduced the following notation for specifying what a program does\(^3\):

\[
\{P\} \ C \ \{Q\}
\]

where:

- $C$ is a program from the programming language whose programs are being specified (the language in Section 1.2 in our case).
- $P$ and $Q$ are conditions on the program variables used in $C$.

Conditions on program variables will be written using standard mathematical notations together with logical operators like $\land$ (‘and’), $\lor$ (‘or’), $\neg$ (‘not’) and $\Rightarrow$ (‘implies’). These are described further in Section 1.5.

We say $\{P\} \ C \ \{Q\}$ is true, if whenever $C$ is executed in a state satisfying $P$ and if the execution of $C$ terminates, then the state in which $C$’s execution terminates satisfies $Q$.

**Example:** $\{X = 1\} \ X := X + 1 \ \{X = 2\}$. Here $P$ is the condition that the value of $X$ is $1$, $Q$ is the condition that the value of $X$ is $2$ and $C$ is the assignment command $X := X + 1$ (i.e. ‘$X$ becomes $X+1$’). $\{X = 1\} \ X := X + 1 \ \{X = 2\}$ is clearly true. □

\(^3\)Actually, Hoare’s original notation was $P \{C\} \ Q$ not $\{P\} \ C \ \{Q\}$, but the latter form is now more widely used.
Chapter 1. Program Specification

An expression \( \{ P \} C \{ Q \} \) is called a partial correctness specification; \( P \) is called its precondition and \( Q \) its postcondition.

These specifications are ‘partial’ because for \( \{ P \} C \{ Q \} \) to be true it is not necessary for the execution of \( C \) to terminate when started in a state satisfying \( P \). It is only required that if the execution terminates, then \( Q \) holds.

A stronger kind of specification is a total correctness specification. There is no standard notation for such specifications. We shall use \( [P] C [Q] \).

A total correctness specification \( [P] C [Q] \) is true if and only if the following conditions apply:

(i) Whenever \( C \) is executed in a state satisfying \( P \), then the execution of \( C \) terminates.

(ii) After termination \( Q \) holds.

The relationship between partial and total correctness can be informally expressed by the equation:

\[
\text{Total correctness} = \text{Termination} + \text{Partial correctness}.
\]

Total correctness is what we are ultimately interested in, but it is usually easier to prove it by establishing partial correctness and termination separately.

Termination is often straightforward to establish, but there are some well-known examples where it is not. For example, no one knows whether the program below terminates for all values of \( X \):

\[
\text{WHILE } X > 1 \text{ DO } \\
\quad \text{IF ODD}(X) \text{ THEN } X := (3 \times X) + 1 \text{ ELSE } X := \text{X DIV 2}
\]

(The expression \( \text{X DIV 2} \) evaluates to the result of rounding down \( \text{X}/2 \) to a whole number.)

Exercise 1
Write a specification which is true if and only if the program above terminates.

1.4 Some examples

The examples below illustrate various aspects of partial correctness specification.

In Examples 5, 6 and 7 below, \( T \) (for ‘true’) is the condition that is always true. In Examples 3, 4 and 7, \( \wedge \) is the logical operator ‘and’, i.e. if \( P_1 \) and \( P_2 \) are conditions, then \( P_1 \wedge P_2 \) is the condition that is true whenever both \( P_1 \) and \( P_2 \) hold.

1. \( \{ X = 1 \} \text{ Y:=X} \{ Y = 1 \} \)

---

\( ^4 \)This example is taken from Exercise 2 on page 17 of Reynolds’s book [38].
1.4. Some examples

This says that if the command \( Y := X \) is executed in a state satisfying the condition \( X = 1 \) (i.e. a state in which the value of \( X \) is 1), then, if the execution terminates (which it does), then the condition \( Y = 1 \) will hold. Clearly this specification is true.

2. \{ \( X = 1 \) \} \( Y := X \) \{ \( Y = 2 \) \}

This says that if the execution of \( Y := X \) terminates when started in a state satisfying \( X = 1 \), then \( Y = 2 \) will hold. This is clearly false.

3. \{ \( x \land y \) \} \( \{ \begin{align*} &R := X; \\ &X := Y; \\ &Y := R \end{align*} \} \{ \( x \land y \) \}

This says that if the execution of \( \{ \begin{align*} &R := X; \\ &X := Y; \\ &Y := R \end{align*} \} \) terminates (which it does), then the values of \( X \) and \( Y \) are exchanged. The variables \( x \) and \( y \), which don’t occur in the command and are used to name the initial values of program variables \( X \) and \( Y \), are called auxiliary variables (or ghost variables).

4. \{ \( x \land y \) \} \( \{ \begin{align*} &X := Y; \\ &Y := X \end{align*} \} \{ \( x \land y \) \}

This says that \( \{ \begin{align*} &X := Y; \\ &Y := X \end{align*} \} \) exchanges the values of \( X \) and \( Y \). This is not true.

5. \{ \( T \) \} \( C \) \{ \( Q \) \}

This says that whenever \( C \) halts, \( Q \) holds.

6. \{ \( P \) \} \( C \) \{ \( T \) \}

This specification is true for every condition \( P \) and every command \( C \) (because \( T \) is always true).

7. \{ \( T \) \}
\begin{align*}
\{ \begin{align*}
&R := X; \\
&Q := 0; \\
&\text{WHILE } Y \leq R \text{ DO} \\
&\quad \begin{align*} &R := R - Y; \\ &Q := Q + 1 \end{align*} \\
&\text{END} \\
&R < Y \land X = R + (Y \times Q) \}
\end{align*}
\end{align*}

This is \( \{ \( T \) \} \{ R < Y \land X = R + (Y \times Q) \} \) where \( C \) is the command indicated by the braces above. The specification is true if whenever the execution of \( C \) halts, then \( Q \) is quotient and \( R \) is the remainder resulting from dividing \( Y \) into \( X \). It is true (even if \( X \) is initially negative!).

In this example a program variable \( Q \) is used. This should not be confused with the \( Q \) used in 5 above. The program variable \( Q \) (notice the font) ranges over numbers, whereas the postcondition \( Q \) (notice the font) ranges over statements. In general, we use typewriter font for particular program variables and italic font for variables ranging over statements. Although this subtle use of fonts might appear confusing at first, once you get the hang of things the difference between the two
kinds of ‘Q’ will be clear (indeed you should be able to disambiguate things from context without even having to look at the font).

Exercise 2
Let $C$ be as in Example 7 above. Find a condition $P$ such that:

$$[P] \quad [R < Y \land X = R + (Y \times Q)]$$

is true. □

Exercise 3
When is $[T] \quad C \quad [T]$ true? □

Exercise 4
Write a partial correctness specification which is true if and only if the command $C$ has the effect of multiplying the values of $X$ and $Y$ and storing the result in $X$. □

Exercise 5
Write a specification which is true if the execution of $C$ always halts when execution is started in a state satisfying $P$. □

1.5 Terms and statements

The notation used here for expressing pre- and postconditions is based on first-order logic. This will only be briefly reviewed here as readers are assumed to be familiar with it. 5

The following are examples of atomic statements.

$T, \quad F, \quad X = 1, \quad R < Y, \quad X = R + (Y \times Q)$

Statements are either true or false. The statement $T$ is always true and the statement $F$ is always false. The statement $X = 1$ is true if the value of $X$ is equal to 1. The statement $R < Y$ is true if the value of $R$ is less than the value of $Y$. The statement $X = R + (Y \times Q)$ is true if the value of $X$ is equal to the sum of the value of $R$ with the product of $Y$ and $Q$.

Statements are built out of terms like:

$X, \quad 1, \quad R, \quad Y, \quad R + (Y \times Q), \quad Y \times Q$

Terms denote values such as numbers and strings, unlike statements which are either true or false. Some terms, like 1 and $4 + 5$, denote a fixed value, whilst other terms contain variables like $X, \ Y, \ Z$ etc. whose value can vary. We will use conventional mathematical notation for terms, as illustrated by the examples below:

5See the IB course Logic and Proof.
1.5. Terms and statements

\[ X, \; Y, \; Z, \]
\[ 1, \; 2, \; 325, \]
\[ -X, \; -(X+1), \; (X \times Y)+Z, \]
\[ \sqrt{(1+X^2)}, \; X!, \; \sin(X), \; \text{rem}(X,Y) \]

T and F are atomic statements that are always true and false respectively. Other atomic statements are built from terms using predicates. Here are some more examples:

\[ \text{ODD}(X), \; \text{PRIME}(3), \; X = 1, \; (X+1)^2 \geq X^2 \]

ODD and PRIME are examples of predicates and = and ≥ are examples of infixed predicates. The expressions X, 1, 3, X+1, (X+1)^2, X^2 are examples of terms.

**Compound statements** are built up from atomic statements using the following logical operators:

\[ \neg \quad \text{(not)} \]
\[ \land \quad \text{(and)} \]
\[ \lor \quad \text{(or)} \]
\[ \Rightarrow \quad \text{(implies)} \]
\[ \iff \quad \text{(if and only if)} \]

The single arrow → is commonly used for implication instead of \( \Rightarrow \). We use \( \Rightarrow \) to avoid possible confusion with the use of → for \( \lambda \)-conversion in Part II.

Suppose \( P \) and \( Q \) are statements, then:

- \( \neg P \) is true if \( P \) is false, and false if \( P \) is true.
- \( P \land Q \) is true whenever both \( P \) and \( Q \) are true.
- \( P \lor Q \) is true if either \( P \) or \( Q \) (or both) are true.
- \( P \Rightarrow Q \) is true if whenever \( P \) is true, then \( Q \) is true also. By convention we regard \( P \Rightarrow Q \) as being true if \( P \) is false. In fact, it is common to regard \( P \Rightarrow Q \) as equivalent to \( \neg P \lor Q \); however, some philosophers called intuitionists disagree with this treatment of implication.
- \( P \Leftrightarrow Q \) is true if \( P \) and \( Q \) are either both true or both false. In fact \( P \Leftrightarrow Q \) is equivalent to \( (P \Rightarrow Q) \land (Q \Rightarrow P) \).

Examples of statements built using the connectives are:

\[ \text{ODD}(X) \lor \text{EVEN}(X) \quad X \text{ is odd or even.} \]
\[ \neg (\text{PRIME}(X) \Rightarrow \text{ODD}(X)) \quad \text{It is not the case that if } X \text{ is prime, then } X \text{ is odd.} \]
\[ X \leq Y \Rightarrow X \leq Y^2 \quad \text{If } X \text{ is less than or equal to } Y, \text{ then } X \text{ is less than or equal to } Y^2. \]
To reduce the need for brackets it is assumed that $\neg$ is more binding than $\land$ and $\lor$, which in turn are more binding than $\Rightarrow$ and $\Leftrightarrow$. For example:

$$\neg P \land Q \quad \text{is equivalent to} \quad (\neg P) \land Q$$

$$P \land Q \Rightarrow R \quad \text{is equivalent to} \quad (P \land Q) \Rightarrow R$$

$$P \land Q \Leftrightarrow \neg R \lor S \quad \text{is equivalent to} \quad (P \land Q) \Leftrightarrow ((\neg R) \lor S)$$
Chapter 2

Floyd-Hoare Logic

The idea of formal proof is discussed. Floyd-Hoare logic is then introduced as a method for reasoning formally about programs.

In the last chapter three kinds of expressions that could be true or false were introduced:

(i) Partial correctness specifications \( \{P\} C \{Q\} \).

(ii) Total correctness specifications \([P] C [Q]\).

(iii) Statements of mathematics (e.g. \((X + 1)^2 = X^2 + 2 \times X + 1\)).

It is assumed that the reader knows how to prove simple mathematical statements like the one in (iii) above. Here, for example, is a proof of this fact.

1. \((X + 1)^2 = (X + 1) \times (X + 1)\) Definition of \(\cdot^2\).
2. \((X + 1) \times (X + 1) = (X + 1) \times X + (X + 1) \times 1\) Left distributive law of \(\times\) over \(+\).
3. \((X + 1)^2 = (X + 1) \times X + (X + 1) \times 1\) Substituting line 2 into line 1.
4. \((X + 1) \times 1 = X + 1\) Identity law for \(1\).
5. \((X + 1) \times X = X \times X + 1 \times X\) Right distributive law of \(\times\) over \(+\).
6. \((X + 1)^2 = X \times X + 1 \times X + X + 1\) Substituting lines 4 and 5 into line 3.
7. \(1 \times X = X\) Identity law for \(1\).
8. \((X + 1)^2 = X \times X + X + 1\) Substituting line 7 into line 6.
9. \(X \times X = X^2\) Definition of \(\cdot^2\).
10. \(X + X = 2 \times X\) \(2=1+1\), distributive law.
11. \((X + 1)^2 = X^2 + 2 \times X + 1\) Substituting lines 9 and 10 into line 8.

This proof consists of a sequence of lines, each of which is an instance of an axiom (like the definition of \(\cdot^2\)) or follows from previous lines by a rule of inference (like the substitution of equals for equals). The statement occurring on the last line of a proof is the statement proved by it (thus \((X + 1)^2 = X^2 + 2 \times X + 1\) is proved by the proof above).

To construct formal proofs of partial correctness specifications axioms and rules of inference are needed. This is what Floyd-Hoare logic provides. The formulation of the deductive system is due to Hoare [20], but some of the underlying ideas originated with Floyd [11].
A proof in Floyd-Hoare logic is a sequence of lines, each of which is either an axiom of the logic or follows from earlier lines by a rule of inference of the logic.

The reason for constructing formal proofs is to try to ensure that only sound methods of deduction are used. With sound axioms and rules of inference, one can be confident that the conclusions are true. On the other hand, if any axioms or rules of inference are unsound then it may be possible to deduce false conclusions; for example\(^1\)

1. \(\sqrt{-1} \times -1 = \sqrt{-1} \times -1\) Reflexivity of =.
2. \(\sqrt{-1} \times -1 = (\sqrt{-1}) \times (\sqrt{-1})\) Distributive law of \(\sqrt{\cdot}\) over \(\times\).
3. \(\sqrt{-1} \times -1 = (\sqrt{-1})^2\) Definition of \(\sqrt{\cdot}\).
4. \(\sqrt{-1} \times -1 = -1\) definition of \(\sqrt{\cdot}\).
5. \(\sqrt{1} = -1\) As \(-1 \times -1 = 1\).
6. \(1 = -1\) As \(\sqrt{1} = 1\).

A formal proof makes explicit what axioms and rules of inference are used to arrive at a conclusion. It is quite easy to come up with plausible rules for reasoning about programs that are actually unsound (some examples for FOR-commands can be found in Section 2.1.11). Proofs of correctness of computer programs are often very intricate and formal methods are needed to ensure that they are valid. It is thus important to make fully explicit the reasoning principles being used, so that their soundness can be analysed.

Exercise 6
Find the flaw in the ‘proof’ of \(1 = -1\) above. \(\square\)

For some applications, correctness is especially important. Examples include life-critical systems such as nuclear reactor controllers, car braking systems, fly-by-wire aircraft and software controlled medical equipment. At the time of writing, there is a legal action in progress resulting from the death of several people due to radiation overdoses by a cancer treatment machine that had a software bug \([25]\). Formal proof of correctness provides a way of establishing the absence of bugs when exhaustive testing is impossible (as it almost always is).

The Floyd-Hoare deductive system for reasoning about programs will be explained and illustrated, but the mathematical analysis of the soundness and completeness of the system is only briefly discussed (see Section 2.2).

### 2.1 Axioms and rules of Floyd-Hoare logic

As discussed at the beginning of this chapter, a formal proof of a statement is a sequence of lines ending with the statement and such that each line is either an instance of an axiom or follows from previous lines by a rule of inference. If \(S\) is a statement (of either ordinary mathematics or Floyd-Hoare logic) then we write \(\vdash S\) to mean that \(S\) has a proof. The statements that have proofs are called theorems.

\(^1\)This example was shown to me by Sylva Cohn.
As discussed earlier, in these notes only the axioms and rules of inference for Floyd-Hoare logic are described; we will thus simply assert \( \vdash S \) if \( S \) is a theorem of mathematics without giving any formal justification. Of course, to achieve complete rigour such assertions must be proved, but for details of how to do this the reader will have to consult the later chapters on first order and higher order logic.

The axioms of Floyd-Hoare logic are specified below by schemas which can be instantiated to get particular partial correctness specifications. The inference rules of Floyd-Hoare logic will be specified with a notation of the form:

\[
\vdash S_1, \ldots, \vdash S_n \therefore \vdash S
\]

This means the conclusion \( \vdash S \) may be deduced from the hypotheses \( \vdash S_1, \ldots, \vdash S_n \). The hypotheses can either all be theorems of Floyd-Hoare logic (as in the sequencing rule below), or a mixture of theorems of Floyd-Hoare logic and theorems of mathematics (as in the rule of preconditioning strengthening described in Section 2.1.2).

### 2.1.1 The assignment axiom

The assignment axiom represents the fact that the value of a variable \( V \) after executing an assignment command \( V := E \) equals the value of the expression \( E \) in the state before executing it. To formalize this, observe that if a statement \( P \) is to be true after the assignment, then the statement obtained by substituting \( E \) for \( V \) in \( P \) must be true before executing it.

In order to say this formally, define \( P[E/V] \) to mean the result of replacing all occurrences of \( V \) in \( P \) by \( E \). Read \( P[E/V] \) as ‘\( P \) with \( E \) for \( V \)’. For example,

\[
(X + 1 > X)[Y+Z/X] = ((Y+Z)+1 > Y+Z)
\]

The way to remember this notation is to remember the ‘cancellation law’

\[
V[E/V] = E
\]

which is analogous to the cancellation property of fractions

\[
v \times (e/v) = e
\]

---

**The assignment axiom**

\[
\vdash \{P[E/V]\} \ V := E \{P\}
\]

Where \( V \) is any variable, \( E \) is any expression, \( P \) is any statement and the notation \( P[E/V] \) denotes the result of substituting the term \( E \) for all occurrences of the variable \( V \) in the statement \( P \).
Instances of the assignment axiom are:

1. \( \vdash \{Y = 2\} \ X := 2 \ \{Y = X\} \)
2. \( \vdash \{X + 1 = n + 1\} \ X := X + 1 \ \{X = n + 1\} \)
3. \( \vdash \{E = E\} \ X := E \ \{X = E\} \) (if \(X\) does not occur in \(E\)).

Many people feel the assignment axiom is ‘backwards’ from what they would expect. Two common erroneous intuitions are that it should be as follows:

(i) \( \vdash \{P\} \ V := E \ \{P[V/E]\} \).

Where the notation \(P[V/E]\) denotes the result of substituting \(V\) for \(E\) in \(P\).

This has the clearly false consequence that \( \vdash \{X=0\} \ X := 1 \ \{X=0\} \), since the \((X=0)[X/1]\) is equal to \((X=0)\) as \(1\) doesn’t occur in \((X=0)\).

(ii) \( \vdash \{P\} \ V := E \ \{P[E/V]\} \).

This has the clearly false consequence \( \vdash \{X=0\} \ X := 1 \ \{1=0\} \) which follows by taking \(P\) to be \(X=0\), \(V\) to be \(X\) and \(E\) to be \(1\).

The fact that it is easy to have wrong intuitions about the assignment axiom shows that it is important to have rigorous means of establishing the validity of axioms and rules. We will not go into this topic here aside from remarking that it is possible to give a formal semantics of our little programming language and then to prove that the axioms and rules of inference of Floyd-Hoare logic are sound. Of course, this process will only increase our confidence in the axioms and rules to the extent that we believe the correctness of the formal semantics. The simple assignment axiom above is not valid for ‘real’ programming languages. For example, work by G. Ligler [27] shows that it can fail to hold in six different ways for the language Algol 60.

One way that our little programming language differs from real languages is that the evaluation of expressions on the right of assignment commands cannot ‘side effect’ the state. The validity of the assignment axiom depends on this property.

To see this, suppose that our language were extended so that it contained the ‘block expression’

\[
\text{BEGIN } Y := 1; \ 2 \ \text{END}
\]

This expression, \(E\) say, has value \(2\), but its evaluation also ‘side effects’ the variable \(Y\) by storing \(1\) in it. If the assignment axiom applied to expressions like \(E\), then it could be used to deduce:

\[
\vdash \{Y=0\} \ X := \text{BEGIN } Y := 1; \ 2 \ \text{END} \ \{Y=0\}
\]

(since \((Y=0)[E/X] = (Y=0)\) as \(X\) does not occur in \((Y=0)\)). This is clearly false, as after the assignment \(Y\) will have the value \(1\).
2.1. Axioms and rules of Floyd-Hoare logic

Floyd-Hoare logic can be extended to cope with arrays so that, for example, the correctness of inplace sorting programs can be verified. However, it is not as straightforward as one might expect to do this. The main problem is that the assignment axiom does not apply to array assignments of the form \( A(E_1) := E_2 \) (where \( A \) is an array variable and \( E_1 \) and \( E_2 \) are expressions).

One might think that the assignment axiom in could be generalized to
\[
\vdash \{ P[E_2/A(E_1)] \} \ A(E_1) := E_2 \ \{ P \}
\]
where \( 'P[E_2/A(E_1)]' \) denotes the result of substituting \( E_2 \) for all occurrences of \( A(E_1) \) throughout \( P \). Alas, this does not work. Consider the following case:
\[
P ≡ 'A(Y)=0', \quad E_1 ≡ 'X', \quad E_2 ≡ '1'
\]
Since \( A(X) \) does not occur in \( P \), it follows that \( P[1/A(X)] = P \), and hence the generalized axiom yields
\[
\vdash \{ A(Y)=0 \} \ A(X):=1 \ \{ A(Y)=0 \}
\]
This specification is clearly false if \( X=Y \). To avoid this, the array assignment axiom must take into account the possibility that changes to \( A(X) \) may also change \( A(Y), A(Z), \ldots \) (since \( X \) might equal \( Y, Z, \ldots \)). This is discussed further in Section 2.1.12.

2.1.2 Precondition strengthening

The next rule of Floyd-Hoare logic enables the preconditions of (i) and (ii) on page 20 to be simplified. Recall that
\[
\vdash S_1, \ldots , \vdash S_n\quad \vdash S
\]
means that \( \vdash S \) can be deduced from \( \vdash S_1, \ldots , \vdash S_n \).

Using this notation, the rule of precondition strengthening is

\[
\begin{align*}
\text{Precondition strengthening} & \\
\vdash P \Rightarrow P' & \quad \vdash \{P'\} C \{Q\} & \quad \vdash \{P\} C \{Q\}
\end{align*}
\]

Examples

1. From the arithmetic fact \( \vdash X+n \Rightarrow X+1=n+1 \), and 2 on page 20 it follows by precondition strengthening that
\[
\vdash \{ X = n \} \ X := X + 1 \ \{ X = n + 1 \}.
\]
The variable \( n \) is an example of an auxiliary (or ghost) variable. As described earlier (see page 13), auxiliary variables are variables occurring in a partial correctness
specification \( \{P\} C \{Q\} \) which do not occur in the command \( C \). Such variables are used to relate values in the state before and after \( C \) is executed. For example, the specification above says that if the value of \( X \) is \( n \), then after executing the assignment \( X:=X+1 \) its value will be \( n+1 \).

2. From the logical truth \( \vdash T \Rightarrow (E=E) \), and 3 on page 20 one can deduce that if \( X \) is not in \( E \) then:

\[
\vdash \{T\} X:=E \{X=E\}
\]

\( \square \)

### 2.1.3 Postcondition weakening

Just as the previous rule allows the precondition of a partial correctness specification to be strengthened, the following one allows us to weaken the postcondition.

**Postcondition weakening**

\[
\begin{align*}
\vdash \{P\} C \{Q\}', & \quad \vdash Q' \Rightarrow Q \\
\vdash \{P\} C \{Q\}
\end{align*}
\]

**Example:** Here is a little formal proof.

1. \( \vdash \{R=X \land 0=0\} Q:=0 \{R=X \land Q=0\} \) By the assignment axiom.
2. \( \vdash R=X \Rightarrow R=X \land 0=0 \) By pure logic.
3. \( \vdash \{R=X\} Q=0 \{R=X \land Q=0\} \) By precondition strengthening.
4. \( \vdash R=X \land Q=0 \Rightarrow R=X+(Y \times Q) \) By laws of arithmetic.
5. \( \vdash \{R=X\} Q:=0 \{R=X+(Y \times Q)\} \) By postcondition weakening.

\( \square \)

The rules precondition strengthening and postcondition weakening are sometimes called the *rules of consequence*.

### 2.1.4 Specification conjunction and disjunction

The following two rules provide a method of combining different specifications about the same command.
2.1. Axioms and rules of Floyd-Hoare logic

Specification conjunction

\[ \frac{\vdash \{ P_1 \} C \{ Q_1 \}, \quad \vdash \{ P_2 \} C \{ Q_2 \} \quad \vdash \{ P_1 \land P_2 \} C \{ Q_1 \land Q_2 \} \]

Specification disjunction

\[ \frac{\vdash \{ P_1 \} C \{ Q_1 \}, \quad \vdash \{ P_2 \} C \{ Q_2 \} \quad \vdash \{ P_1 \lor P_2 \} C \{ Q_1 \lor Q_2 \} \]

These rules are useful for splitting a proof into independent bits. For example, they enable \( \vdash \{ P \} C \{ Q_1 \land Q_2 \} \) to be proved by proving separately that both \( \vdash \{ P \} C \{ Q_1 \} \) and \( \vdash \{ P \} C \{ Q_2 \} \).

The rest of the rules allow the deduction of properties of compound commands from properties of their components.

2.1.5 The sequencing rule

The next rule enables a partial correctness specification for a sequence \( C_1; C_2 \) to be derived from specifications for \( C_1 \) and \( C_2 \).

The sequencing rule

\[ \frac{\vdash \{ P \} C_1 \{ Q \}, \quad \vdash \{ Q \} C_2 \{ R \} \quad \vdash \{ P \} C_1; C_2 \{ R \} \]

Example: By the assignment axiom:

(i) \( \vdash \{ X=x \land Y=y \} \ R:=X \ \{ R=x \land Y=y \} \)

(ii) \( \vdash \{ R=x \land Y=y \} \ X:=Y \ \{ R=x \land X=y \} \)

(iii) \( \vdash \{ R=x \land X=y \} \ Y:=R \ \{ Y=x \land X=y \} \)

Hence by (i), (ii) and the sequencing rule

(iv) \( \vdash \{ X=x \land Y=y \} \ R:=X; \ X:=Y \ \{ R=x \land X=y \} \)

Hence by (iv) and (iii) and the sequencing rule

(v) \( \vdash \{ X=x \land Y=y \} \ R:=X; \ X:=Y; \ Y:=R \ \{ Y=x \land X=y \} \)
2.1.6 The derived sequencing rule

The following rule is derivable from the sequencing and consequence rules.

\[
\begin{align*}
\therefore & P \\
& \{P_1, C_1, Q_1\} \quad \{Q_1 \Rightarrow P_2\} \\
& \{P_2, C_2, Q_2\} \quad \{Q_2 \Rightarrow P_3\} \\
& \cdots \\
& \{P_n, C_n, Q_n\} \quad \{Q_n \Rightarrow P\} \\
\therefore & \{P\} C_1; \cdots; C_n; \{Q\}
\end{align*}
\]

The derived sequencing rule enables (v) in the previous example to be deduced directly from (i), (ii) and (iii) in one step.

2.1.7 The block rule

The block rule is like the sequencing rule, but it also takes care of local variables.

\[
\begin{align*}
\therefore & \{P\} C \{Q\} \\
\therefore & \{P\} \text{BEGIN VAR } V_1; \cdots; \text{VAR } V_n; \text{END } \{Q\}
\end{align*}
\]

where none of the variables \(V_1, \ldots, V_n\) occur in \(P\) or \(Q\).

The syntactic condition that none of the variables \(V_1, \ldots, V_n\) occur in \(P\) or \(Q\) is an example of a side condition. It is a syntactic condition that must hold whenever the rule is used. Without this condition the rule is invalid; this is illustrated in the example below.

Note that the block rule is regarded as including the case when there are no local variables (the ‘\(n = 0\)’ case).

**Example:** From \(\therefore \{X=x \land Y=y\} R:=X; X:=Y; Y:=R \{Y=x \land X=y\}\) (see page 23) it follows by the block rule that

\(\therefore \{X=x \land Y=y\} \text{BEGIN VAR } R; R:=X; X:=Y; Y:=R \text{ END } \{Y=x \land X=y\}\)

since \(R\) does not occur in \(X=x \land Y=y\) or \(X=y \land Y=x\). Notice that from

\(\therefore \{X=x \land Y=y\} R:=X; X:=Y \{R=x \land X=y\}\)

one cannot deduce
2.1. Axioms and rules of Floyd-Hoare logic

\[ \vdash \{ X=x \wedge Y=y \} \text{~BEGIN~} R := X; X := Y \text{~END~} \{ R=x \wedge X=y \} \]

since \( R \) occurs in \( \{ R=x \wedge X=y \} \). This is as required, because assignments to local variables of blocks should not be felt outside the block body. Notice, however, that it is possible to deduce:

\[ \vdash \{ X=x \wedge Y=y \} \text{~BEGIN~} R := X; X := Y \text{~END~} \{ R=x \wedge X=y \}. \]

This is correct because \( R \) is no longer a local variable. □

The following exercise addresses the question of whether one can show that changes to local variables inside a block are invisible outside it.

**Exercise 7**

Consider the specification

\[ \{ X=x \} \text{~BEGIN~} X := 1 \text{~END~} \{ X=x \} \]

Can this be deduced from the rules given so far?

(i) If so, give a proof of it.

(ii) If not, explain why not and suggest additional rules and/or axioms to enable it to be deduced.

\[ \square \]

### 2.1.8 The derived block rule

From the derived sequencing rule and the block rule the following rule for blocks can be derived.

**The derived block rule**

\[ \begin{array}{c}
\vdash P \\
\vdash \{ P_1 \} C_1 \{ Q_1 \} \\
\vdash \{ P_2 \} C_2 \{ Q_2 \} \\
\vdots \\
\vdash \{ P_n \} C_n \{ Q_n \} \\
\vdash Q_n \Rightarrow Q \\
\vdash \{ P \} \text{~BEGIN~} V_1; \ldots; V_m; C_1; \ldots; C_n \{ Q \}
\end{array} \]

where none of the variables \( V_1, \ldots, V_m \) occur in \( P \) or \( Q \).

Using this rule, it can be deduced *in one step* from (i), (ii) and (iii) on page 23 that:

\[ \vdash \{ X=x \wedge Y=y \} \text{~BEGIN~} R := X; X := Y; Y := R \text{~END~} \{ Y=x \wedge X=y \} \]
Exercise 8
Is the following specification true?
\[ \{ X=x \land Y=y \} X:=X+Y; Y:=X-Y; X:=X-Y \{ Y=x \land X=y \} \]
If so, prove it. If not, give the circumstances in which it fails. □

Exercise 9
Show \[ \{ X=R+(Y \times Q) \} \text{ BEGIN } R:=R-Y; Q:=Q+1 \text{ END } \{ X=R+(Y \times Q) \} \]
□

2.1.9 The conditional rules
There are two kinds of conditional commands: one-armed conditionals and two-armed conditionals. There are thus two rules for conditionals.

The conditional rules

\[
\begin{align*}
\vdash & \quad \{ P \land S \} \ C \ \{ Q \}, \quad \vdash \quad P \land \neg S \Rightarrow Q \\
\vdash & \quad \{ P \} \text{ IF } S \text{ THEN } C \ \{ Q \} \\
\vdash & \quad \{ P \land S \} \ C_1 \ \{ Q \}, \quad \vdash \quad P \land \neg S \quad C_2 \ \{ Q \} \\
\vdash & \quad \{ P \} \text{ IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \ \{ Q \}
\end{align*}
\]

Example: Suppose we are given that

(i) \[ \vdash X \geq Y \Rightarrow \max(X,Y) = X \]

(ii) \[ \vdash Y \geq X \Rightarrow \max(X,Y) = Y \]

Then by the conditional rules (and others) it follows that

\[ \vdash \{ T \} \text{ IF } X \geq Y \text{ THEN } MAX:=X \text{ ELSE } MAX:=Y \ \{ \max=\max(X,Y) \} \]

□

Exercise 10
Give a detailed formal proof that the specification in the previous example follows from hypotheses (i) and (ii). □

Exercise 11
Devise an axiom and/or rule of inference for a command \text{SKIP} that has no effect. Show that if \text{IF } S \text{ THEN } C \text{ is regarded as an abbreviation for } \text{IF } S \text{ THEN } C \text{ ELSE } \text{SKIP}, then the rule for one-armed conditionals is derivable from the rule for two-armed conditionals and your axiom/rule for \text{SKIP}. □
Exercise 12
Suppose we add to our little programming language commands of the form:

\[
\text{CASE } E \text{ OF BEGIN } C_1; \ldots ; C_n \text{ END}
\]

These are evaluated as follows:

(i) First $E$ is evaluated to get a value $x$.

(ii) If $x$ is not a number between 1 and $n$, then the CASE-command has no effect.

(iii) If $x = i$ where $1 \leq i \leq n$, then command $C_i$ is executed.

Why is the following rule for CASE-commands wrong?

\[
\frac{\vdash \{P \land E = 1\} C_1 \{Q\}, \ldots , \vdash \{P \land E = n\} C_n \{Q\}}{\vdash \{P\} \text{ CASE } E \text{ OF BEGIN } C_1; \ldots ; C_n \text{ END } \{Q\}}
\]

*Hint:* Consider the case when $P$ is ‘$X = 0$’, $E$ is ‘$X$’, $C_1$ is ‘$Y := 0$’ and $Q$ is ‘$Y = 0$’.

\[\square\]

Exercise 13
Devise a proof rule for the CASE-commands in the previous exercise and use it to show:

\[
\vdash \{1 \leq X \land X \leq 3\}
\]

CASE $X$ OF
BEGIN
\begin{align*}
Y &:= X-1; \\
Y &:= X-2; \\
Y &:= X-3
\end{align*}
END
\{Y=0\}

\[\square\]

Exercise 14
Show that if $\vdash \{P \land S\} C_1 \{Q\}$ and $\vdash \{P \land \neg S\} C_2 \{Q\}$, then it is possible to deduce:

\[
\vdash \{P\} \text{ IF } S \text{ THEN } C_1 \text{ ELSE IF } \neg S \text{ THEN } C_2 \{Q\}.
\]

\[\square\]
2.1.10 The **WHILE**-rule

If \( \vdash \{ P \land S \} \{ C \} \{ P \} \), we say: \( P \) is an *invariant* of \( C \) whenever \( S \) holds. The **WHILE**-rule says that if \( P \) is an invariant of the body of a **WHILE**-command whenever the test condition holds, then \( P \) is an invariant of the whole **WHILE**-command. In other words, if executing \( C \) once preserves the truth of \( P \), then executing \( C \) any number of times also preserves the truth of \( P \).

The **WHILE**-rule also expresses the fact that after a **WHILE**-command has terminated, the test must be false (otherwise, it wouldn’t have terminated).

### The **WHILE**-rule

\[
\begin{align*}
\vdash & \{ P \land S \} \{ C \} \{ P \} \\
\vdash & \{ P \} \text{ WHILE } S \text{ DO } \{ C \} \{ P \land \neg S \}
\end{align*}
\]

**Example:** By Exercise 9 on page 26

\[\vdash \{ X=R+(Y \times Q) \} \text{ BEGIN } R:=R-Y; \; Q:=Q+1 \text{ END } \{ X=R+(Y \times Q) \}\]

Hence by precondition strengthening

\[\vdash \{ X=R+(Y \times Q) \land Y \leq R \} \text{ BEGIN } R:=R-Y; \; Q:=Q+1 \text{ END } \{ X=R+(Y \times Q) \}\]

Hence by the **WHILE**-rule (with \( P = 'X=R+(Y \times Q)' \))

1. \( \vdash \{ X=R+(Y \times Q) \} \) 
   \[\text{WHILE } Y \leq R \text{ DO} \]
   \[\text{BEGIN } R:=R-Y; \; Q:=Q+1 \text{ END} \]
   \[\{ X=R+(Y \times Q) \land \neg (Y \leq R) \}\]
   It is easy to deduce that

2. \( \vdash \{ T \} \; R:=X; \; Q:=0 \; \{ X=R+(Y \times Q) \}\)

Hence by (i) and (ii), the sequencing rule and postcondition weakening

\[\vdash \{ T \} \]
\[R:=X; \]
\[Q:=0; \]
\[\text{WHILE } Y \leq R \text{ DO} \]
\[\text{BEGIN } R:=R-Y; \; Q:=Q+1 \text{ END} \]
\[\{ R<Y \land X=R+(Y \times Q) \}\]

\( \square \)

With the exception of the **WHILE**-rule, all the axioms and rules described so far are sound for total correctness as well as partial correctness. This is because the only commands in our little language that might not terminate are **WHILE**-commands. Consider now the following proof:
2.1. Axioms and rules of Floyd-Hoare logic

1. \[ {\{ T \} \} \vdash X := 0 \{ T \} \]  (assignment axiom)
2. \[ {\{ T \land T \} \} \vdash X := 0 \{ T \} \]  (precondition strengthening)
3. \[ {\{ T \} \} \vdash \text{WHILE } T \text{ DO } X := 0 \{ T \land \neg T \} \]  (2 and the WHILE-rule)

If the WHILE-rule were true for total correctness, then the proof above would show that:

\[ \vdash [T] \text{WHILE } T \text{ DO } X := 0 [T \land \neg T] \]

but this is clearly false since WHILE T DO X:=0 does not terminate, and even if it did then T \land \neg T could not hold in the resulting state.

Extending Floyd-Hoare logic to deal with termination is quite tricky. One approach can be found in Dijkstra [10].

2.1.11 The FOR-rule

It is quite hard to capture accurately the intended semantics of FOR-commands in Floyd-Hoare logic. Axioms and rules are given here that appear to be sound, but they are not necessarily complete (see Section 2.2). An early reference on the logic of FOR-commands is Hoare’s 1972 paper [21]; a comprehensive treatment can be found in Reynolds [38].

The intention here in presenting the FOR-rule is to show that Floyd-Hoare logic can get very tricky. All the other axioms and rules were quite straightforward and may have given a false sense of simplicity: it is very difficult to give adequate rules for anything other than very simple programming constructs. This is an important incentive for using simple languages.

One problem with FOR-commands is that there are many subtly different versions of them. Thus before describing the FOR-rule, the intended semantics of FOR-commands must be described carefully. In these notes, the semantics of

\[ \text{FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \]

is as follows:

(i) The expressions \( E_1 \) and \( E_2 \) are evaluated once to get values \( e_1 \) and \( e_2 \), respectively.

(ii) If either \( e_1 \) or \( e_2 \) is not a number, or if \( e_1 > e_2 \), then nothing is done.

(iii) If \( e_1 \leq e_2 \) the FOR-command is equivalent to:

\[
\begin{align*}
\text{BEGIN} & \text{ VAR } V; \\
& V := e_1; C; V := e_1+1; C; \ldots; V := e_2; C \\
\text{END}
\end{align*}
\]

i.e. \( C \) is executed \((e_2-e_1)+1\) times with \( V \) taking on the sequence of values \( e_1, e_1+1, \ldots, e_2 \) in succession. Note that this description is not rigorous: ‘\( e_1 \)’ and ‘\( e_2 \)’ have been used both as numbers and as expressions of our little language; the semantics of FOR-commands should be clear despite this.
FOR-rules in different languages can differ in subtle ways from the one here. For example, the expressions $E_1$ and $E_2$ could be evaluated at each iteration and the controlled variable $V$ could be treated as global rather than local. Note that with the semantics presented here, FOR-commands cannot go into infinite loops (unless, of course, they contain non-terminating WHILE-commands).

To see how the FOR-rule works, suppose that

$$\vdash \{P\} \ {C} \ \{P[V+1/V]\}$$

Suppose also that $C$ does not contain any assignments to the variable $V$. If this is the case, then it is intuitively clear (and can be rigorously proved) that

$$\vdash \{(V = v)\} \ {C} \ \{(V = v)\}$$

hence by specification conjunction

$$\vdash \{P \land (V = v)\} \ {C} \ \{P[V+1/V] \land (V = v)\}$$

Now consider a sequence $V := v; \ C$. By Example 2 on page 22,

$$\vdash \{P[v/V]\} \ V := v \ \{P \land (V = v)\}$$

Hence by the sequencing rule

$$\vdash \{P[v/V]\} \ V := v; \ C \ \{P[V+1/V] \land (V = v)\}$$

Now it is a truth of logic alone that

$$\vdash P[V+1/V] \land (V = v) \Rightarrow P[v+1/V]$$

hence by postcondition weakening

$$\vdash \{P[v/V]\} \ V := v; \ C \ \{P[v+1/V]\}$$

Taking $v$ to be $e_1, e_1+1, \ldots, e_2$ and using the derived sequencing rule we can thus deduce

$$\{P[e_1/V]\} \ V := e_1; \ C; \ V := e_1+1; \ldots; \ V := e_2; \ C \ \{P[e_2/V]\}$$

This suggests that a FOR-rule could be:

$$\vdash \{P\} \ {C} \ \{P[V+1/V]\} \ \{P[E_1/V]\} \ \{P[E_2+1/V]\}$$

Unfortunately, this rule is unsound. To see this, first note that:

1. $\vdash \{Y+1=Y+1\} \ \{X:=Y+1\}$ (assignment axiom)
2. $\vdash \{T\} \ X := Y+1 \ \{X=Y+1\}$ (1 and precondition strengthening)
3. $\vdash X = Y \Rightarrow T$ (logic: ‘anything implies true’)
4. $\vdash \{X=Y\} \ X := Y+1 \ \{X=Y+1\}$ (2 and precondition strengthening)
Thus if \( P \) is ‘\( x = y \)’ then:

\[
\vdash \{ P \} \; x := y + 1 \; \{ P[y+1/y] \}
\]

and so by the \textsc{for}-rule above, if we take \( V \) to be \( y \), \( E_1 \) to be 3 and \( E_2 \) to be 1, then

\[
\vdash \{ \begin{array}{c} x = 3 \\ P[3/y] \end{array} \} \; \textsc{for} \; y := 3 \; \text{until} \; 1 \; \text{do} \; x := y + 1 \; \{ \begin{array}{c} x = 2 \\ P[1+1/y] \end{array} \}
\]

This is clearly false: it was specified that if the value of \( E_1 \) were greater than the value of \( E_2 \) then the \textsc{for}-command should have no effect, but in this example it changes the value of \( x \) from 3 to 2.

To solve this problem, the \textsc{for}-rule can be modified to

\[
\vdash \{ P \} \; C \; \{ P[V+1/V] \}
\]

\[
\vdash \{ P[E_1/V] \; \land \; E_1 \leq E_2 \} \; \textsc{for} \; V := E_1 \; \text{until} \; E_2 \; \text{do} \; C \; \{ P[E_2+1/V] \}
\]

If this rule is used on the example above all that can be deduced is

\[
\vdash \{ x = 3 \; \land \; 3 \leq 1 \} \; \textsc{for} \; y := 3 \; \text{until} \; 1 \; \text{do} \; x := y + 1 \; \{ x = 2 \}
\]

never true!

This conclusion is harmless since it only asserts that \( x \) will be changed if the \textsc{for}-command is executed in an impossible starting state.

Unfortunately, there is still a bug in our \textsc{for}-rule. Suppose we take \( P \) to be ‘\( y = 1 \)’, then it is straightforward to show that:

\[
\vdash \{ y = 1 \} \; y := y - 1 \; \{ y + 1 = 1 \}
\]

so by our latest \textsc{for}-rule

\[
\vdash \{ \begin{array}{c} 1 = 1 \\ P[1/y] \end{array} \} \; \textsc{for} \; y := 1 \; \text{until} \; y := y - 1 \; \{ \begin{array}{c} 2 = 1 \\ P[1+1/y] \end{array} \}
\]

Whatever the command does, it doesn’t lead to a state in which \( 2 = 1 \). The problem is that the body of the \textsc{for}-command modifies the controlled variable. It is not surprising that this causes problems, since it was explicitly assumed that the body didn’t modify the controlled variable when we motivated the \textsc{for}-rule. It turns out that problems also arise if any variables in the expressions \( E_1 \) and \( E_2 \) (which specify the upper and lower bounds) are modified. For example, taking \( P \) to be \( z = y \), then it is straightforward to show

\[
\vdash \{ z = y \} \; z := z + 1 \; \{ z + 1 = 1 \}
\]

hence the rule allows us the following to be derived:

\[
\vdash \{ \begin{array}{c} z = 1 \\ P[1/y] \end{array} \} \; \textsc{for} \; y := 1 \; \text{until} \; z := z + 1 \; \{ \begin{array}{c} z = z + 1 \\ P[z+1/y] \end{array} \}
\]
This is clearly wrong as one can never have \( Z = Z + 1 \) (subtracting \( Z \) from both sides would give \( 0 = 1 \)). One might think that this is not a problem because the \texttt{FOR}-command would never terminate. In some languages this might be the case, but the semantics of our language were carefully defined in such a way that \texttt{FOR}-commands always terminate (see the beginning of this section).

To rule out the problems that arise when the controlled variable or variables in the bounds expressions, are changed by the body, we simply impose a side condition on the rule that stipulates that the rule cannot be used in these situations. The final rule is thus:

\[
\begin{align*}
\text{The FOR-rule} \\
\vdash & \{ P \land (E_1 \leq V) \land (V \leq E_2) \} \ C \ \{ P[V+1/V] \} \\
\vdash & \{ P[E_1/V] \land (E_1 \leq E_2) \} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \ \{ P[E_2+1/V] \}
\end{align*}
\]

where neither \( V \), nor any variable occurring in \( E_1 \) or \( E_2 \), is assigned to in the command \( C \).

This rule does not enable anything to be deduced about \texttt{FOR}-commands whose body assigns to variables in the bounds expressions. This precludes such assignments being used if commands are to be reasoned about. The strategy of only defining rules of inference for non-tricky uses of constructs helps ensure that programs are written in a perspicuous manner. It is possible to devise a rule that does cope with assignments to variables in bounds expressions, but it is not clear whether it is a good idea to have such a rule.

\textbf{The FOR-axiom}

To cover the case when \( E_2 < E_1 \), we need the FOR-axiom below.

\[
\begin{align*}
\text{The FOR-axiom} \\
\vdash & \{ P \land (E_2 < E_1) \} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \ \{ P \}
\end{align*}
\]

This says that when \( E_2 \) is less than \( E_1 \) the \texttt{FOR}-command has no effect.

\textbf{Example:} By the assignment axiom and precondition strengthening

\[
\begin{align*}
\vdash & \{ X = ((N-1) \times N) \text{ DIV } 2 \} \ X := X+N \ \{ X = (N \times (N+1)) \text{ DIV } 2 \}
\end{align*}
\]

Strengthening the precondition of this again yields

\[
\begin{align*}
\vdash & \{ (X = ((N-1) \times N) \text{ DIV } 2) \land (1 \leq N) \land (N \leq M) \} \ X := X+N \ \{ X = (N \times (N+1)) \text{ DIV } 2 \}
\end{align*}
\]
Hence by the FOR-rule
\[ \vdash \{ X=((1-1)\times1) \div (1\leq M) \} \]
\[ \text{FOR } N:=1 \text{ UNTIL } M \text{ DO } X:=X+N \]
\[ \{ X=(M\times(M+1)) \div 2 \} \]
Hence
\[ \vdash \{ X=0 \} \land (1\leq M) \text{ FOR } N:=1 \text{ UNTIL } M \text{ DO } X:=X+N \{ X=(M\times(M+1)) \div 2 \} \]
\[ \square \]

Note that if
(i) \[ \vdash \{ P \} C \{ P[V+1/V] \}, \text{ or} \]
(ii) \[ \vdash \{ P \land (E_1 \leq V) \} C \{ P[V+1/V] \}, \text{ or} \]
(iii) \[ \vdash \{ P \land (V \leq E_2) \} C \{ P[V+1/V] \} \]
then by precondition strengthening one can infer
\[ \vdash \{ P \land (E_1 \leq V) \land (V \leq E_2) \} C \{ P[V+1/V] \} \]

**Exercise 15**
Show that
\[ \vdash \{ M\geq1 \} \]
\[ \text{BEGIN} \]
\[ X:=0; \]
\[ \text{FOR } N:=1 \text{ UNTIL } M \text{ DO } X:=X+N \]
\[ \text{END} \]
\[ \{ X=(M\times(M+1)) \div 2 \} \]
\[ \square \]

**Exercise 16**
Justify the following alternative FOR-rule suggested by Bob Tennent:

<table>
<thead>
<tr>
<th>Alternative FOR-rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ \vdash { P[V-1/V] \land (E_1 \leq V) \land (V \leq E_2) } C { P } ]</td>
</tr>
<tr>
<td>[ \vdash { P[E_1-1/V] \land (E_1-1\leq E_2) } \text{ FOR } V:=E_1 \text{ UNTIL } E_2 \text{ DO } C { P[E_2/V] } ]</td>
</tr>
</tbody>
</table>

where neither \( V \), nor any variable occurring in \( E_1 \) or \( E_2 \), is assigned to in the command \( C \).

The advantage of this rule is that the “special case” of executing the loop body 0 times can normally be handled without use of the FOR-axiom. Justify this claim.

\[ \square \]
2.1.12 Arrays

At the end of Section 2.1.1 it is shown that the naive array assignment axiom
\[ \{ P[E_2/A(E_1)] \} \quad A(E_1) := E_2 \quad \{ P \} \]
does not work, because of the possibility that changes to \( A(X) \) may also change \( A(Y), A(Z), \ldots \) (since \( X \) might equal \( Y, Z, \ldots \)).

The solution, due to Hoare, is to treat an array assignment
\[ A(E_1) := E_2 \]
as an ordinary assignment
\[ A := A\{ E_1 \leftarrow E_2 \} \]
where the term \( A\{ E_1 \leftarrow E_2 \} \) denotes an array identical to \( A \), except that the \( E_1 \)-th component is changed to have the value \( E_2 \).

Thus an array assignment is just a special case of an ordinary variable assignment.

The array assignment axiom
\[ \{ P[A\{ E_1 \leftarrow E_2 \} / A] \} \quad A(E_1) := E_2 \quad \{ P \} \]

Where \( A \) is an array variable, \( E_1 \) is an integer valued expression, \( P \) is any statement and the notation \( A\{ E_1 \leftarrow E_2 \} \) denotes the array identical to \( A \), except that the value at \( E_1 \) is \( E_2 \).

In order to reason about arrays, the following axioms, which define the meaning of the notation \( A\{ E_1 \leftarrow E_2 \} \), are needed.

The array axioms
\[ A\{ E_1 \leftarrow E_2 \}(E_1) = E_2 \]

\[ E_1 \neq E_3 \Rightarrow \quad \vdash A\{ E_1 \leftarrow E_2 \}(E_3) = A(E_3) \]

Example: We show
\[ \{ A(X)=x \land A(Y)=y \} \]
BEGIN
\[ \text{VAR } R; \]
\[ R := A(X); \]
\[ A(X) := A(Y); \]
\[ A(Y) := R \]
END
\[ \{ A(X)=y \land A(Y)=x \} \]
2.1. Axioms and rules of Floyd-Hoare logic

Working backwards using the array assignment axiom:

\[ \vdash \{ A \{ Y \leftarrow R \} \{ X \leftarrow A(Y) \} \} \{ Y \leftarrow R \} \{ X \leftarrow A(Y) \} \]
\[ A(Y) := R \]
\[ \{ A(X) = y \land A(Y) = x \} \]

By precondition strengthening using \( \vdash A \{ Y \leftarrow R \} \{ Y = R \} \)

\[ \vdash \{ A \{ Y \leftarrow R \} \{ X \leftarrow A(Y) \} \} \{ Y \leftarrow R \} \{ X \leftarrow A(Y) \} \]
\[ A(Y) := R \]
\[ \{ A(X) = y \land A(Y) = x \} \]

Continuing backwards

\[ \vdash \{ A \{ X \leftarrow A(Y) \} \{ Y \leftarrow R \} \{ X \leftarrow A(Y) \} \} \{ Y \leftarrow R \} \{ X \leftarrow A(Y) \} \]
\[ A(Y) := A(Y) \]
\[ \{ A(X) = y \land A(Y) = x \} \]

Hence by the derived sequencing rule:

\[ \vdash \{ A \{ A(Y) \} \{ Y \leftarrow R \} \{ X \leftarrow A(Y) \} \} \{ X \leftarrow A(Y) \} \]
\[ R := A(Y) ; A(X) := A(Y) ; A(Y) := R \]
\[ \{ A(X) = y \land A(Y) = x \} \]

By the array axioms (considering the cases \( X = Y \) and \( X \neq Y \) separately), it follows that:

\[ \vdash A \{ A(Y) \} \{ Y \leftarrow R \} \{ X \leftarrow A(Y) \} \{ X \leftarrow A(Y) \} = A(Y) \]

Hence:

\[ \vdash \{ A(Y) = y \land A(X) = x \} \]
\[ R := A(X) ; A(X) := A(Y) ; A(Y) := R \]
\[ \{ A(X) = y \land A(Y) = x \} \]

The desired result follows from the block rule. □

**Exercise 17**

Show

\[ \vdash \{ A(X) = x \land A(Y) = y \land X \neq Y \} \]
\[ A(X) := A(X) + A(Y) ; \]
\[ A(Y) := A(X) - A(Y) ; \]
\[ A(X) := A(X) - A(Y) \]
\[ \{ A(X) = y \land A(Y) = x \} \]

Why is the precondition \( X \neq Y \) necessary? □
Example: Suppose $c_{\text{sort}}$ is a command that is intended to sort the first $n$ elements of an array. To specify this formally, let $\text{SORTED}(A, n)$ mean that:

$$A(1) \leq A(2) \leq \ldots \leq A(n)$$

A first attempt to specify that $c_{\text{sort}}$ sorts is:

$$\{1 \leq N\} \ c_{\text{sort}} \ \{\text{SORTED}(A, N)\}$$

This is not enough, however, because $\text{SORTED}(A, N)$ can be achieved by simply zeroing the first $N$ elements of $A$.

Exercise 18
Prove

$$\vdash \{1 \leq N\} \ \{\text{SORTED}(A, N)\}$$

It is necessary to require that the sorted array is a rearrangement, or permutation, of the original array.

To formalize this, let $\text{PERM}(A, A', N)$ mean that $A(1), A(2), \ldots, A(n)$ is a rearrangement of $A'(1), A'(2), \ldots, A'(n)$.

An improved specification that $c_{\text{sort}}$ sorts is then

$$\{1 \leq N \land A=a\} \ c_{\text{sort}} \ \{\text{SORTED}(A, N) \land \text{PERM}(A, a, N)\}$$

However, this still is not correct.²

Exercise 19
Prove

$$\vdash \{1 \leq N\} \ \{\text{SORTED}(A, N) \land \text{PERM}(A, a, N)\}$$

It is necessary to say explicitly that $N$ is unchanged also. A correct specification is thus:

$$\{1 \leq N \land A=a \land N=n\} \ c_{\text{sort}} \ \{\text{SORTED}(A, N) \land \text{PERM}(A, a, N) \land N=n\}$$

²Thanks to an anonymous member of the 1990 class “Proving Programs Correct” for pointing this out to me.
2.2 Soundness and completeness

It is clear from the discussion of the FOR-rule in Section 2.1.11 that it is not always straightforward to devise correct rules of inference. As discussed at the beginning of Chapter 2, it is very important that the axioms and rules be sound. There are two approaches to ensure this:

(i) Define the language by the axioms and rules of the logic.

(ii) Prove that the logic fits the language.

Approach (i) is called axiomatic semantics. The idea is to define the semantics of the language by requiring that it make the axioms and rules of inference true. It is then up to implementers to ensure that the logic matches the language. One snag with this approach is that most existing languages have already been defined in some other way (usually by informal and ambiguous natural language statements). An example of a language defined axiomatically is Euclid [29]. The other snag with axiomatic semantics is that it is known to be impossible to devise complete Floyd-Hoare logics for certain constructs (this is discussed further below). It could be argued that this is not a snag at all but an advantage, because it forces programming languages to be made logically tractable. I have some sympathy for this latter view; it is clearly not the position taken by the designers of Ada.

Approach (ii) requires that the axioms and rules of the logic be proved valid. To do this, a mathematical model of states is constructed and then a function, Meaning say, is defined which takes an arbitrary command $C$ to a function $\text{Meaning}(C)$ from states to states. Thus $\text{Meaning}(C)(s)$ denotes the state resulting from executing command $C$ in state $s$. The specification $\{P\}C\{Q\}$ is then defined to be true if whenever $P$ is true in a state $s$ and $\text{Meaning}(C)(s) = s'$ then $Q$ is true in state $s'$. It is then possible to attempt to prove rigorously that all the axioms are true and that the rules of inference lead from true premisses to true conclusions. Actually carrying out this proof is likely to be quite tedious, especially if the programming language is at all complicated, and there are various technical details which require care (e.g. defining Meaning to correctly model non-termination). The precise formulation of such soundness proofs is not covered here, but details can be found in the text by Loeckx and Sieber [28].

Even if we are sure that our logic is sound, how can we be sure that every true specification can be proved? It might be the case that for some particular $P$, $Q$ and $C$ the specification $\{P\}C\{Q\}$ was true, but the rules of our logic were too weak to prove it (see Exercise 7 on page 25 for an example). A logic is said to be complete if every true statement in it is provable. There are various subtle technical problems in formulating precisely what it means for a Floyd-Hoare logic to be complete. For example, it is necessary to distinguish incompleteness arising due to incompleteness in the assertion language (e.g. arithmetic) from incompleteness
due to inadequate axioms and rules for programming language constructs. The
completeness of a Floyd-Hoare logic must thus be defined independently of that of
its assertion language. Good introductions to this area can be found in Loeckx and
Sieber [28] and Clarke’s paper [9]. Clarke’s paper also contains a discussion of his
important results showing the impossibility of giving complete inference systems
for certain combinations of programming language constructs. For example, he
proves that it is impossible to give a sound and complete system for any language
combining procedures as parameters of procedure calls, recursion, static scopes,
global variables and internal procedures as parameters of procedure calls. These
features are found in Algol 60, which thus cannot have a sound and complete Floyd-
Hoare logic.

2.3 Some exercises

The exercises in this section have been taken from various sources, including Alagić

Exercise 20

The exponentiation function $exp$ satisfies:

\[
\begin{align*}
exp(m, 0) &= 1 \\
exp(m, n+1) &= m \times exp(m, n)
\end{align*}
\]

Devise a command $C$ that uses repeated multiplication to achieve the following
partial correctness specification:

$$\{ X = x \land Y = y \land Y \geq 0 \} \ C \ \{ Z = \exp(x, y) \land X = x \land Y = y \}$$

Prove that your command $C$ meets this specification. □

Exercise 21

Show that:

$$\vdash \{ M \geq 0 \}
\begin{align*}
& \text{BEGIN} \\
& \quad X := 0; \\
& \quad \text{FOR } N := 1 \text{ UNTIL } M \text{ DO } X := X + N \\
& \text{END} \\
& \{ X = \frac{(M \times (M+1))}{2} \}
\end{align*}
$$

\textit{Hint:} Compare precondition with that of Exercise 15 on Page 33. □

Exercise 22

Deduce:

$$\vdash \{ S = (x \times y) - (X \times Y) \}
\begin{align*}
& \text{WHILE } \neg \text{ODD}(X) \text{ DO} \\
& \quad \text{BEGIN } Y := 2 \times Y; \ X := X \text{ DIV } 2 \text{ END} \\
& \{ S = (x \times y) - (X \times Y) \land \text{ODD}(X) \}
\end{align*}
$$

□
Exercise 23

Deduce:

\[ \{ S = (x \times y) - (X \times Y) \} \]

\[ \text{WHILE } \neg (X=0) \text{ DO} \]

BEGIN

\[ \text{WHILE } \neg \text{ODD}(X) \text{ DO} \]

BEGIN

\[ Y := 2 \times Y; \quad X := X \div 2 \]

\[ S := S + Y; \quad X := X - 1 \]

END

END

\{ S = x \times y \}

\[ \square \]

Exercise 24

Deduce:

\[ \{ X = x \wedge Y = y \} \]

BEGIN

\[ S := 0; \]

\[ \text{WHILE } \neg (X=0) \text{ DO} \]

BEGIN

\[ \text{WHILE } \neg \text{ODD}(X) \text{ DO} \]

BEGIN

\[ Y := 2 \times Y; \quad X := X \div 2 \]

\[ S := S + Y; \quad X := X - 1 \]

END

END

\{ S = x \times y \}

\[ \square \]

Exercise 25

Prove the following invariant property.

\[ \{ S = (x-X) \times y \wedge Y = y \} \]

BEGIN

VAR R;

\[ R := 0; \]

\[ \text{WHILE } \neg (R=Y) \text{ DO} \]

BEGIN

\[ S := S + 1; \quad R := R + 1 \]

\[ X := X - 1 \]

END

\{ S = (x-X) \times y \}

\text{Hint: Show that } S = (x-X) \times y + R \text{ is an invariant for } S := S + 1; \quad R := R + 1. \quad \square \]

Exercise 26

Deduce:
\[
\vdash \{ X = x \land Y = y \}
\]
BEGIN
\[
S := 0;
WHILE \neg (X = 0) DO
BEGIN
VAR R;
R := 0;
WHILE \neg (R = Y) DO
BEGIN
S := S + 1; R := R + 1
END
X := X - 1
END
\]
\[
\{ S = x \times y \}
\]

Exercise 27
Using \( P \times X^n = x^n \) as an invariant, deduce:

\[
\vdash \{ X = x \land N = n \}
\]
BEGIN
\[
P := 1;
WHILE \neg (N = 0) DO
BEGIN
\quad IF ODD(N) THEN P := P \times X;
\quad N := N \text{ DIV } 2;
\quad X := X \times X
END
\]
\[
\{ P = x^n \}
\]

Exercise 28
Prove that the command

BEGIN
\[
Z := 0;
WHILE \neg (X = 0) DO
BEGIN
\quad IF ODD(X) THEN Z := Z + Y;
\quad Y := Y \times 2;
\quad X := X \text{ DIV } 2
END
\]
computes the product of the initial values of \( X \) and \( Y \) and leaves the result in \( Z \).

Exercise 29
Prove that the command
BEGIN
Z:=1;
WHILE N>0 DO
BEGIN
IF ODD(N) THEN Z:=Z×X;
N:=N DIV 2;
X:=X×X
END
END
assigns $x^n$ to $Z$, where $x$ and $n$ are the initial values of $X$ and $N$ respectively and we assume $n \geq 0$. ☐

Exercise 30
Devise a proof rule for a command

\[
\text{REPEAT command UNTIL statement}
\]

The meaning of \text{REPEAT C UNTIL S} is that $C$ is executed and then $S$ is tested; if the result is true, then nothing more is done, otherwise the whole \text{REPEAT} command is repeated. Thus \text{REPEAT C UNTIL S} is equivalent to $C; \text{WHILE } \neg S \text{ DO } C$. ☐

Exercise 31
Use your \text{REPEAT} rule to deduce:

\[
\vdash \{ S = C+R \land R<Y \}
\]

\[
\text{REPEAT}
\begin{align*}
\text{BEGIN} & \ S:=S+1; \ R:=R+1 \ 
\text{UNTIL} & \ R=Y; \\
& \ \{ S = C+Y \}
\end{align*}
\]

☐

Exercise 32
Use your \text{REPEAT} rule to deduce:

\[
\vdash \{ X=x \land Y=y \}
\]

\[
\text{BEGIN}
\begin{align*}
S:=0; \\
\text{REPEAT} \\
& \ R:=0; \\
& \ \text{REPEAT}
\begin{align*}
& \ \text{BEGIN} \ S:=S+1; \ R:=R+1 \ 
\text{UNTIL} & \ R=Y; \\
& \ X:=X-1 \ 
\text{END} \\
& \ \text{UNTIL} X=0
\end{align*}
\end{align*}
\]

\[
\{ S = x \times y \}
\]

☐

Exercise 33
Assume $\text{gcd}(X,Y)$ satisfies:
\( \vdash (X > Y) \Rightarrow \text{gcd}(X, Y) = \text{gcd}(X - Y, Y) \)
\( \vdash \text{gcd}(X, Y) = \text{gcd}(Y, X) \)
\( \vdash \text{gcd}(X, X) = X \)

Prove:
\( \vdash \{(A > 0) \land (B > 0) \land (\text{gcd}(A, B) = \text{gcd}(X, Y))\} \)
\( \text{WHILE } A > B \text{ DO } A := A - B; \)
\( \text{WHILE } B > A \text{ DO } B := B - A \)
\( \{0 < B \land (B \leq A) \land (\text{gcd}(A, B) = \text{gcd}(X, Y))\} \)

Hence, or otherwise, use your rule for REPEAT commands to prove:
\( \vdash \{A = a \land B = b\} \)
\( \text{REPEAT} \)
\( \text{BEGIN} \)
\( \text{WHILE } A > B \text{ DO } A := A - B; \)
\( \text{WHILE } B > A \text{ DO } B := B - A \)
\( \text{END} \)
\( \text{UNTIL } A = B \)
\( \{A = B \land A = \text{gcd}(a, b)\} \)

\( \Box \)

**Exercise 34**
Prove:
\( \vdash \{N \geq 1\} \)
\( \text{BEGIN} \)
\( \text{PROD} = 0; \)
\( \text{FOR } X := 1 \text{ UNTIL } N \text{ DO } \text{PROD} := \text{PROD} + M \)
\( \text{END} \)
\( \{\text{PROD} = M \times N\} \)

\( \Box \)

**Exercise 35**
Prove:
\( \vdash \{X > 0 \land Y > 0\} \)
\( \text{BEGIN} \)
\( S := 0; \)
\( \text{FOR } I := 1 \text{ UNTIL } X \text{ DO } \)
\( \text{FOR } J := 1 \text{ UNTIL } Y \text{ DO } \)
\( S := S + 1 \)
\( \text{END} \)
\( \{S = X \times Y\} \)

\( \Box \)

**Exercise 36**
In some programming languages (e.g. ALGOLW) the following specification would be true:
\( \vdash \{Y = 3\} \)
\( \text{FOR } I := 1 \text{ UNTIL } Y \text{ DO } Y := Y + 1 \)
\( \{Y = 6\} \)
Explain why this cannot be deduced using the FOR-rule given on page 32. Design a more general FOR-rule, and use it to prove the above specification.

Exercise 37
(Hard!) Prove:

\[ \vdash \{1 \leq N \land A=a \land N=n\} \]
\[ \text{FOR } I:=1 \text{ UNTIL } N \text{ DO} \]
\[ \text{FOR } J:=I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IF } A(I)>A(J) \]
\[ \text{THEN BEGIN} \]
\[ \text{VAR } R; \]
\[ R := A(I); \]
\[ A(I) := A(J); \]
\[ A(J) := R \]
\[ \text{END} \]
\[ \{\text{SORTED}(A,N) \land \text{PERM}(A,a,N) \land N=n\} \]

Outline solution

Warning: although I believe the outline proof below to be sound, I have not yet fully checked all the details and so there may be errors and omissions.

We outline a proof that:

\[ \vdash \{1 \leq N \land A=a \land N=n\} \]
\[ \text{FOR } I:=1 \text{ UNTIL } N \text{ DO} \]
\[ \text{FOR } J:=I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IF } A(I)>A(J) \]
\[ \text{THEN BEGIN} \]
\[ \text{VAR } R; \]
\[ R := A(I); \]
\[ A(I) := A(J); \]
\[ A(J) := R \]
\[ \text{END} \]
\[ \{\text{SORTED}(A,N) \land \text{PERM}(A,a,N) \land N=n\} \]

Let IFSWAP(A,I,J) abbreviate the command:

\[ \text{IF } A(I)>A(J) \]
\[ \text{THEN BEGIN} \]
\[ \text{VAR } R; \]
\[ R := A(I); \]
\[ A(I) := A(J); \]
\[ A(J) := R \]
\[ \text{END} \]

Then what has to be proved is:

\[ \vdash \{1 \leq N \land A=a \land N=n\} \]
\[ \text{FOR } I:=1 \text{ UNTIL } N \text{ DO} \]
\[ \text{FOR } J:=I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IFSWAP}(A,I,J) \]
\[ \{\text{SORTED}(A,N) \land \text{PERM}(A,a,N) \land N=n\} \]
By specification conjunction it is sufficient to prove.

\[ \vdash \{1 \leq N\} \]

\[ \text{FOR } I := 1 \text{ UNTIL } N \text{ DO} \]

\[ \text{FOR } J := I + 1 \text{ UNTIL } N \text{ DO} \]

\[ \text{IFS}W\text{AP}(A, I, J) \]

\{\text{SORTED}(A, N)\} \]

and

\[ \vdash \{1 \leq N \land A = a\} \]

\[ \text{FOR } I := 1 \text{ UNTIL } N \text{ DO} \]

\[ \text{FOR } J := I + 1 \text{ UNTIL } N \text{ DO} \]

\[ \text{IFS}W\text{AP}(A, I, J) \]

\{\text{PERM}(A, a, N)\} \]

and

\[ \vdash \{N = n\} \]

\[ \text{FOR } I := 1 \text{ UNTIL } N \text{ DO} \]

\[ \text{FOR } J := I + 1 \text{ UNTIL } N \text{ DO} \]

\[ \text{IFS}W\text{AP}(A, I, J) \]

\{N = n\} \]

The proof of the second and third of these are easy. For the second, it is necessary to use properties of the predicate \text{PERM} such as the following:

\[ \vdash \text{PERM}(A, A, N) \]

\[ \vdash \text{PERM}(A, A', N) \land 1 \leq I \leq N \land 1 \leq J \leq N \Rightarrow \]

\[ \text{PERM}(A, A'\{I \leftarrow A'(J)}\{J \leftarrow A'(I)}\}, N) \]

Using these properties one can show that swapping two elements in an array preserves permutation, i.e.

\[ \vdash \{\text{PERM}(A, a, N) \land 1 \leq I \land I \leq N\} \]

\[ \text{IFS}W\text{AP}(A, I, J) \]

\{\text{PERM}(A, a, N)\} \]

Using the \text{FOR}-rule twice on this specification, followed by precondition strengthening with \text{PERM} using the first property above, establishes that the sorting command only permutes the array. To show that it sorts the array into ascending order is more complicated.

Notice that each inner \text{FOR} loop results in the minimum element in \(A(I), \ldots, A(N)\) being placed at position \(I\). To formulate this formally, define \text{MIN}(A, I, J) to mean that if \(1 \leq I \leq J\) then \(A(I)\) is less than or equal to each of \(A(I + 1), \ldots, A(J - 1)\). It is intuitively clear that \text{MIN} has the properties:

\[ \vdash \text{MIN}(A, I, J) \land A(I) \leq A(J) \Rightarrow \text{MIN}(A, I, J + 1) \]

\[ \vdash \text{MIN}(A, I, J) \land A(I) \geq A(J) \Rightarrow \text{MIN}(A\{I \leftarrow A(J)}\{J \leftarrow A(I)}\}, I, J + 1) \]

Using these properties it is straightforward to prove:

\[ \vdash \{\text{MIN}(A, I, J)\} \text{IFS}W\text{AP}(A, I, J) \{\text{MIN}(A, I, J + 1)\} \]

and hence by the \text{FOR}-rule
\[ \forall \{ 1 \leq N \land \text{MIN}(A, I, I+1) \} \]
\[ \text{FOR } J := I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IFS\textsc{wap}}(A, I, J) \]
\[ \{ \text{MIN}(A, I, N) \} \]

and hence, since \( \vdash \text{MIN}(A, I, I+1) \), it follows by precondition strengthening that:
\[ \vdash \{ 1 \leq N \} \]
\[ \text{FOR } J := I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IFS\textsc{wap}}(A, I, J) \]
\[ \{ \text{MIN}(A, I, N) \} \]

Using various properties of \text{MIN} and \text{SORTED} one can also show that
\[ \vdash \{ \text{SORTED}(A, I-1) \land \text{MIN}(A, I-1, N+1) \land I \leq J \} \]
\[ \text{IFS\textsc{wap}}(A, I, J) \]
\[ \vdash \{ \text{SORTED}(A, I-1) \land \text{MIN}(A, I-1, N+1) \} \]

and hence by the \text{FOR}-rule
\[ \vdash \{ \text{SORTED}(A, I-1) \land \text{MIN}(A, I-1, N+1) \land I \leq I+1 \} \]
\[ \text{FOR } J := I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IFS\textsc{wap}}(A, I, J) \]
\[ \vdash \{ \text{SORTED}(A, I-1) \land \text{MIN}(A, I-1, N+1) \} \]

which simplifies, by precondition strengthening and postcondition weakening, to:
\[ \vdash \{ \text{SORTED}(A, I-1) \land \text{MIN}(A, I-1, N+1) \} \]
\[ \text{FOR } J := I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IFS\textsc{wap}}(A, I, J) \]
\[ \vdash \{ \text{SORTED}(A, I-1) \} \]

hence by specification conjunction (using a previously proved result):
\[ \vdash \{ \text{SORTED}(A, I-1) \land \text{MIN}(A, I-1, N+1) \land 1 \leq N \} \]
\[ \text{FOR } J := I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IFS\textsc{wap}}(A, I, J) \]
\[ \vdash \{ \text{SORTED}(A, I-1) \land \text{MIN}(A, I, N) \} \]

hence by postcondition weakening
\[ \vdash \{ \text{SORTED}(A, I-1) \land \text{MIN}(A, I-1, N+1) \land 1 \leq N \} \]
\[ \text{FOR } J := I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IFS\textsc{wap}}(A, I, J) \]
\[ \vdash \{ \text{SORTED}(A, I) \} \]

hence by the \text{FOR}-rule (noticing that \text{SORTED}(A, I) is equivalent to \text{SORTED}(A, (I+1)-1))
\[ \vdash \{ \text{SORTED}(A, 1-1) \land \text{MIN}(A, 1-1, N+1) \land 1 \leq N \} \]
\[ \text{FOR } I := 1 \text{ UNTIL } N \text{ DO} \]
\[ \text{FOR } J := I+1 \text{ UNTIL } N \text{ DO} \]
\[ \text{IFS\textsc{wap}}(A, I, J) \]
\[ \vdash \{ \text{SORTED}(A, (N+1)-1) \} \]

which simplifies to the desired result using \( 1-1 = 0 \) and properties of \text{SORTED} and \text{MIN}. 
Mechanizing Program Verification

The architecture of a simple program verifier is described. Its operation is justified with respect to the rules of Floyd-Hoare logic.

After doing only a few exercises, the following two things will be painfully clear:

(i) Proofs are typically long and boring (even if the program being verified is quite simple).

(ii) There are lots of fiddly little details to get right, many of which are trivial (e.g. proving \( \vdash (R = X \land Q = 0) \Rightarrow (X = R + Y \times Q) \)).

Many attempts have been made (and are still being made) to automate proof of correctness by designing systems to do the boring and tricky bits of generating formal proofs in Floyd-Hoare logic. Unfortunately logicians have shown that it is impossible in principle to design a decision procedure to decide automatically the truth or falsehood of an arbitrary mathematical statement [13]. However, this does not mean that one cannot have procedures that will prove many useful theorems. The non-existence of a general decision procedure merely shows that one cannot hope to prove everything automatically. In practice, it is quite possible to build a system that will mechanize many of the boring and routine aspects of verification. This chapter describes one commonly taken approach to doing this.

Although it is impossible to decide automatically the truth or falsity of arbitrary statements, it is possible to check whether an arbitrary formal proof is valid. This consists in checking that the results occurring on each line of the proof are indeed either axioms or consequences of previous lines. Since proofs of correctness of programs are typically very long and boring, they often contain mistakes when generated manually. It is thus useful to check proofs mechanically, even if they can only be generated with human assistance.

3.1 Overview

In the previous chapter it was shown how to prove \( \{P\}C\{Q\} \) by proving properties of the components of \( C \) and then putting these together (with the appropriate proof rule) to get the desired property of \( C \) itself. For example, to prove \( \vdash \{P\}C_1;C_2\{Q\} \)
first prove \( \vdash \{P\}C_1\{R\} \) and \( \vdash \{R\}C_2\{Q\} \) (for suitable \( R \)), and then deduce \( \vdash \{P\}C_1;C_2\{Q\} \) by the sequencing rule.

This process is called \textit{forward proof} because one moves forward from axioms via rules to conclusions. In practice, it is more natural to work backwards: starting from the goal of showing \( \{P\}C\{Q\} \) one generates subgoals, subsubgoals etc. until the problem is solved. For example, suppose one wants to show:

\[
\{x=x \land y=y\} \quad R:=X; \quad X:=Y; \quad Y:=R \quad \{y=x \land x=y\}
\]

then by the assignment axiom and sequencing rule it is sufficient to show the subgoal

\[
\{x=x \land y=y\} \quad R:=X; \quad X:=Y \quad \{y=x \land x=y\}
\]

(because \( \vdash \{y=x \land x=y\} \quad Y:=R \quad \{y=x \land x=y\} \)). By a similar argument this subgoal can be reduced to

\[
\{x=x \land y=y\} \quad R:=X \quad \{y=x \land x=y\}
\]

which clearly follows from the assignment axiom.

This chapter describes how such a \textit{goal oriented} method of proof can be formalized.

The verification system described here can be viewed as a proof checker that also provides some help with generating proofs. The following diagram gives an overview of the system.
The system takes as input a partial correctness specification annotated with mathematical statements describing relationships between variables. From the annotated specification the system generates a set of purely mathematical statements, called verification conditions (or vc’s). In Section 3.5 it is shown that if these verification conditions are provable, then the original specification can be deduced from the axioms and rules of Floyd-Hoare logic.

The verification conditions are passed to a theorem prover program which attempts to prove them automatically; if it fails, advice is sought from the user. We will concentrate on those aspects pertaining to Floyd-Hoare logic and say very little about theorem proving here.

The aim of much current research is to build systems which reduce the role of the slow and expensive human expert to a minimum. This can be achieved by:

- reducing the number and complexity of the annotations required, and
- increasing the power of the theorem prover.

The next section explains how verification conditions work. In Section 3.5 their use is justified in terms of the axioms and rules of Floyd-Hoare logic. Besides being the basis for mechanical verification systems, verification conditions are a useful way of doing proofs by hand.

### 3.2 Verification conditions

The following sections describe how a goal oriented proof style can be formalized. To prove a goal $\{P\}C\{Q\}$, three things must be done. These will be explained in detail later, but here is a quick overview:

(i) The program $C$ is annotated by inserting into it statements (often called assertions) expressing conditions that are meant to hold at various intermediate points. This step is tricky and needs intelligence and a good understanding of how the program works. Automating it is a problem of artificial intelligence.

(ii) A set of logic statements called verification conditions (vc’s for short) is then generated from the annotated specification. This process is purely mechanical and easily done by a program.

(iii) The verification conditions are proved. Automating this is also a problem of artificial intelligence.

It will be shown that if one can prove all the verification conditions generated from $\{P\}C\{Q\}$ (where $C$ is suitably annotated), then $\vdash \{P\}C\{Q\}$.

Since verification conditions are just mathematical statements, one can think of step 2 above as the ‘compilation’, or translation, of a verification problem into a conventional mathematical problem.
The following example will give a preliminary feel for the use of verification conditions.

Suppose the goal is to prove (see the example on page 28)

\[
\begin{align*}
\{ & T \} \\
& \text{BEGIN} \\
& \quad R := X; \\
& \quad Q := 0; \\
& \quad \text{WHILE } Y \leq R \text{ DO} \\
& \quad \quad \text{BEGIN } R := R - Y; \quad Q := Q + 1 \quad \text{END} \\
& \text{END} \\
\{ & X = R + Y \times Q \land R < Y \}
\end{align*}
\]

This first step ((i) above) is to insert annotations. A suitable annotated specification is:

\[
\begin{align*}
\{ & T \} \\
& \text{BEGIN} \\
& \quad R := X; \\
& \quad Q := 0; \quad \{ R=\text{X} \land Q=\text{0} \} \quad \leftarrow \text{P}_1 \\
& \quad \text{WHILE } Y \leq R \text{ DO} \quad \{ X = R + Y \times Q \} \quad \leftarrow \text{P}_2 \\
& \quad \quad \text{BEGIN } R := R - Y; \quad Q := Q + 1 \quad \text{END} \\
& \text{END} \\
\{ & X = R + Y \times Q \land R < Y \}
\end{align*}
\]

The annotations \(\text{P}_1\) and \(\text{P}_2\) state conditions which are intended to hold whenever control reaches them. Control only reaches the point at which \(\text{P}_1\) is placed once, but it reaches \(\text{P}_2\) each time the \text{WHILE} body is executed and whenever this happens \(\text{P}_2\) (i.e. \(X=R+Y\times Q\)) holds, even though the values of \(R\) and \(Q\) vary. \(\text{P}_2\) is an invariant of the \text{WHILE}-command.

The second step ((ii) above), which has yet to be explained, will generate the following four verification conditions:

(i) \(T \Rightarrow (X=X \land 0=0)\)

(ii) \((R=X \land Q=0) \Rightarrow (X = R+(Y\times Q))\)

(iii) \((X = R+(Y\times Q)) \land Y \leq R \Rightarrow (X = (R-Y)+(Y\times(Q+1)))\)

(iv) \((X = R+(Y\times Q)) \land \neg(Y \leq R) \Rightarrow (X = R+(Y\times Q) \land R < Y)\)

Notice that these are statements of arithmetic; the constructs of our programming language have been ‘compiled away’.

The third step ((iii) above) consists in proving these four verification conditions. These are all well within the capabilities of modern automatic theorem provers.

### 3.3 Annotation

An annotated command is a command with statements (called \textit{assertions}) embedded within it. A command is said to be properly annotated if statements have been inserted at the following places:

...
(i) Before each command $C_i$ (where $i > 1$) in a sequence $C_1; C_2; \ldots ; C_n$ which is not an assignment command,

(ii) After the word **DO** in **WHILE** and **FOR** commands.

Intuitively, the inserted assertions should express the conditions one expects to hold whenever control reaches the point at which the assertion occurs.

A properly annotated specification is a specification $\{P\}C\{Q\}$ where $C$ is a properly annotated command.

**Example:** To be properly annotated, assertions should be at points $\mathfrak{1}$ and $\mathfrak{2}$ of the specification below:

\[
\{X=n\}
\]
BEGIN
  \[
  Y:=1; \quad \mathfrak{1}
  \]
  WHILE $X\neq 0$ DO $\mathfrak{2}$
    BEGIN $Y:=Y\times X; \; X:=X-1$ END
  END
\{X=0 \land Y=n!\}

Suitable statements would be:

- at $\mathfrak{1}$: $\{Y = 1 \land X = n\}
- at $\mathfrak{2}$: $\{Y\times X! = n!\}$

The verification conditions generated from an annotated specification $\{P\}C\{Q\}$ are described by considering the various possibilities for $C$ in turn. This process is justified in Section 3.5 by showing that $\vdash \{P\}C\{Q\}$ if all the verification conditions can be proved.

### 3.4 Verification condition generation

In this section a procedure is described for generating verification conditions for an annotated partial correctness specification $\{P\}C\{Q\}$. This procedure is **recursive** on $C$. 
Assignment commands

The single verification condition generated by

\[ \{ P \} \ V := E \ \{ Q \} \]

is

\[ P \Rightarrow Q[E/V] \]

The single verification condition generated by

\[ \{ P \} \ A(E_1) := E_2 \ \{ Q \} \]

is

\[ P \Rightarrow Q[A \{ E_1 \leftarrow E_2 \}] / A \]

Example: The verification condition for

\[ \{ X=0 \} \ X := X+1 \ \{ X=1 \} \]

is

\[ X=0 \Rightarrow (X+1)=1 \]

(which is clearly true).

Verifications for array assignments are obtained by treating \( A(E_1):=E_2 \) as the ordinary assignment \( A := A \{ E_1 \leftarrow E_2 \} \) as discussed in Section 2.1.12.

One-armed conditional

The verification conditions generated by

\[ \{ P \} \ \text{IF} \ S \ \text{THEN} \ C \ \{ Q \} \]

are

(i) \( (P \land \neg S) \Rightarrow Q \)

(ii) the verification conditions generated by

\[ \{ P \land S \} \ C \ \{ Q \} \]

Example: The verification conditions for

\[ \{ T \} \ \text{IF} \ X < 0 \ \text{THEN} \ X := -X \ \{ X \geq 0 \} \]

are \( T \land \neg (X < 0) \Rightarrow X \geq 0 \) together with the verification conditions for \( \{ T \land (X < 0) \} \ X := -X \ \{ X \geq 0 \} \), i.e. \( T \land (X < 0) \Rightarrow -X \geq 0 \). The two vc’s are thus:
(i) $T \land \neg (X<0) \Rightarrow X \geq 0$

(ii) $T \land (X<0) \Rightarrow -X \geq 0$

These are equivalent to $X \geq 0 \Rightarrow X \geq 0$ and $X < 0 \Rightarrow -X \geq 0$, respectively, which are both clearly true. □

**Two-armed conditional**

The verification conditions generated from

$$\{P\} \text{ IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \{Q\}$$

are

(i) the verification conditions generated by

$$\{P \land S\} \ C_1 \{Q\}$$

(ii) the verification conditions generated by

$$\{P \land \neg S\} \ C_2 \{Q\}$$

**Exercise 38**

What are the verification conditions for the following specification?

$$\{T\} \text{ IF } X \geq Y \text{ THEN } \text{MAX}:=X \text{ ELSE } \text{MAX}:=Y \{\text{MAX} = \text{max}(X,Y)\}$$

Do they follow from the assumptions about $\text{max}(X,Y)$ given in the example on page 26? □

If $C_1; \ldots; C_n$ is properly annotated, then (see page 50) it must be of one of the two forms:

1. $C_1; \ldots; C_{n-1}; \{R\} C_n$, or

2. $C_1; \ldots; C_{n-1}; V := E$.

where, in both cases, $C_1; \ldots; C_{n-1}$ is a properly annotated command.
Sequences

1. The verification conditions generated by

\{ P \} C_1; \ldots; C_{n-1}; \{ R \} C_n \{ Q \}

(where \( C_n \) is not an assignment) are:

(a) the verification conditions generated by

\{ P \} C_1; \ldots; C_{n-1} \{ R \}

(b) the verification conditions generated by

\{ R \} C_n \{ Q \}

2. The verification conditions generated by

\{ P \} C_1; \ldots; C_{n-1}; V := E \{ Q \}

are the verification conditions generated by

\{ P \} C_1; \ldots; C_{n-1} \{ Q[E/V] \}

Example: The verification conditions generated from

\{ X=x \land Y=y \} \ R:=X; \ X:=Y; \ Y:=R \{ X=y \land Y=x \}

are those generated by

\{ X=x \land Y=y \} \ R:=X; \ X:=Y \{ (X=y \land Y=x)[R/Y] \}

which, after doing the substitution, simplifies to

\{ X=x \land Y=y \} \ R:=X; \ X:=Y \{ X=y \land R=x \}

The verification conditions generated by this are those generated by

\{ X=x \land Y=y \} \ R:=X \{ (X=x \land R=x)[Y/X] \}

which, after doing the substitution, simplifies to

\{ X=x \land Y=y \} \ R:=X \{ Y=y \land R=x \}.

The only verification condition generated by this is

X=x \land Y=y \Rightarrow (Y=y \land R=x)[X/R]

which, after doing the substitution, simplifies to

X=x \land Y=y \Rightarrow Y=y \land X=x
which is obviously true. □

The procedure for generating verification conditions from blocks involves checking the syntactic condition that the local variables of the block do not occur in the precondition or postcondition. The need for this is clear from the side condition in the block rule (see page 24); this will be explained in more detail when the procedure for generating verification conditions is justified in Section 3.5.

### Blocks

The verification conditions generated by

\[
\{P\} \text{BEGIN \text{VAR}} \ V_1; \ldots; \text{VAR} \ V_n; \text{C END} \ \{Q\}
\]

are

(i) the verification conditions generated by \(\{P\} C \{Q\}\), and

(ii) the syntactic condition that none of \(V_1, \ldots, V_n\) occur in either \(P\) or \(Q\).

**Example:** The verification conditions for

\[
\{X=x \land Y=y\} \text{BEGIN \text{VAR} R; R:=X; X:=Y; Y:=R END} \ \{X=y \land Y=x\}
\]

are those generated by \(\{X=x \land Y=y\} \text{R:=X; X:=Y; Y:=R} \ \{X=y \land Y=x\}\) (since \(R\) does not occur in \(\{X=x \land Y=y\}\) or \(\{X=y \land Y=x\}\)). See the previous example for the verification conditions generated by this. □

**Exercise 39**

What are the verification conditions for the following specification?

\[
\{X = R+(Y \times Q)\} \text{BEGIN \text{R:=R-Y; Q:=Q+1 END} \ \{X = R+(Y \times Q)\}}
\]

□

**Exercise 40**

What are the verification conditions for the following specification?

\[
\{X=x\} \text{BEGIN \text{VAR X; X:=1 END} \ \{X=x\}}
\]

Relate your answer to this exercise to your answer to Exercise 7 on page 25. □

A correctly annotated specification of a **WHILE**-command has the form

\[
\{P\} \text{WHILE S DO } \{R\} \text{ C } \{Q\}
\]

Following the usage on page 28, the annotation \(R\) is called an invariant.
WHILE-commands

The verification conditions generated from

\{P\} WHILE S DO \{R\} C \{Q\}

are

(i) \( P \Rightarrow R \)
(ii) \( R \land \neg S \Rightarrow Q \)
(iii) the verification conditions generated by \( \{R \land S\} C\{R\} \).

Example: The verification conditions for

\{R=X \land Q=0\}
WHILE Y\leq R DO \{X=R+Y\times Q\}
BEGIN R:=R-Y; Q:=Q+1 END
\{X = R+(Y\times Q) \land R<Y\}

are:

(i) \( R=X \land Q=0 \Rightarrow (X = R+(Y\times Q)) \)
(ii) \( X = R+Y\times Q \land \neg(Y\leq R) \Rightarrow (X = R+(Y\times Q) \land R<Y) \)

Together with the verification condition for

\{X = R+(Y\times Q) \land (Y\leq R)\}
BEGIN R:=R-Y; Q:=Q+1 END
\{X=R+(Y\times Q)\}

which (see Exercise 39) consists of the single condition

(iii) \( X = R+(Y\times Q) \land (Y\leq R) \Rightarrow X = (R-Y)+(Y\times(Q+1)) \)

The WHILE-command specification is thus true if (i), (ii) and (iii) hold, i.e.

\[\vdash \{R=X \land Q=0\}\]
WHILE Y\leq R DO
BEGIN R:=R-Y; Q:=Q+1 END
\{X = R+(Y\times Q) \land R<Y\}

if

\[\vdash R=X \land Q=0 \Rightarrow (X = R+(Y\times Q))\]

and

\[\vdash X = R+(Y\times Q) \land \neg(Y\leq R) \Rightarrow (X = R+(Y\times Q) \land R<Y)\]

and

\[\vdash X = R+(Y\times Q) \land (Y\leq R) \Rightarrow X = (R-Y)+(Y\times(Q+1))\]
Exercise 41

What are the verification conditions generated by the annotated program for computing $n!$ (the factorial of $n$) given in the example on page 51?

A correctly annotated specification of a FOR-command has the form

$$\{P\} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } \{R\} \text{ C } \{Q\}$$

FOR-commands

The verification conditions generated from

$$\{P\} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } \{R\} \text{ C } \{Q\}$$

are

(i) $P \Rightarrow R[E_1/V]$

(ii) $R[E_2+1/V] \Rightarrow Q$

(iii) $P \land E_2 < E_1 \Rightarrow Q$

(iv) the verification conditions generated by

$$\{R \land E_1 \leq V \land V \leq E_2\} \text{ C } \{R[V+1/V]\}$$

(v) the syntactic condition that neither $V$, nor any variable occurring in $E_1$ or $E_2$, is assigned to inside $C$.

Example: The verification conditions generated by

$$\{X=0 \land 1 \leq M\} \text{ FOR } N := 1 \text{ UNTIL } M \text{ DO } \{X=((N-1)\times N) \text{ DIV } 2\} \text{ X}:=X+N$$

$$X = (M\times(M+1)) \text{ DIV } 2$$

are

(i) $X=0 \land 1 \leq M \Rightarrow X=((1-1)\times 1) \text{ DIV } 2$

(ii) $X = (((M+1)-1) \times (M+1)) \text{ DIV } 2 \Rightarrow X = (M\times(M+1)) \text{ DIV } 2$

(iii) $X=0 \land 1 \leq M \land M<1 \Rightarrow X = (M\times(M+1)) \text{ DIV } 2$

(iv) The verification condition generated by

$$\{X = ((N-1)\times N) \text{ DIV } 2 \land 1 \leq N \land N \leq M\}$$

$$X:=X+N$$

$$\{X = (((N+1)-1) \times (N+1)) \text{ DIV } 2\}$$

which, after some simplification, is

$$X = ((N-1) \times N) \text{ DIV } 2 \land 1 \leq N \land N \leq M \Rightarrow X+N = (N \times (N+1)) \text{ DIV } 2$$
which is true since
\[
\frac{(N - 1) \times N}{2} + N = \frac{2N + (N - 1) \times N}{2}
\]
\[
= \frac{2N + N^2 - N}{2}
\]
\[
= \frac{N + N^2}{2}
\]
\[
= \frac{N \times (N + 1)}{2}
\]

(Exercise: justify this calculation in the light of the fact that
\[(x + y) \div z \neq (x \div z) + (y \div z)\]
as is easily seen by taking \(x, y\) and \(z\) to be 3, 5 and 8, respectively.)

(v) Neither \(N\) or \(M\) is assigned to in \(X:=X+N\)

\[\square\]

### 3.5 Justification of verification conditions

It will be shown in this section that an annotated specification \(\{P\}C\{Q\}\) is provable in Floyd-Hoare logic (i.e. \(\vdash \{P\}C\{Q\}\)) if the verification conditions generated by it are provable. This shows that the verification conditions are *sufficient*, but not that they are necessary. In fact, the verification conditions are the weakest sufficient conditions, but we will neither make this more precise nor go into details here. An in-depth study of preconditions can be found in Dijkstra’s book [10].

It is easy to show (see the exercise below) that the verification conditions are not necessary, i.e. that the verification conditions for \(\{P\}C\{Q\}\) not being provable doesn’t imply that \(\vdash \{P\}C\{Q\}\) cannot be deduced.

**Exercise 42**

Show that

(i) The verification conditions from the annotated specification

\[
\{T\} \text{ WHILE } F \text{ DO } \{F\} \text{ X:=0 } \{T\}
\]

are not provable.

(ii) \(\vdash \{T\} \text{ WHILE } F \text{ DO } X:=0 \{T\}\)

\[\square\]
3.5. Justification of verification conditions

The argument that the verification conditions are sufficient will be by induction on the structure of $C$. Such inductive arguments have two parts. First, it is shown that the result holds for assignment commands. Second, it is shown that when $C$ is not an assignment command, then if the result holds for the constituent commands of $C$ (this is called the induction hypothesis), then it holds also for $C$. The first of these parts is called the basis of the induction and the second is called the step. From the basis and the step it follows that the result holds for all commands.

**Assignments**

The only verification condition for $\{P\}V := E\{Q\}$ is $P \Rightarrow Q[E/V]$. If this is provable, then as $\vdash \{Q[E/V]\}V := E\{Q\}$ (by the assignment axiom on page 19) it follows by precondition strengthening (page 21) that $\vdash \{P\}V := E\{Q\}$.

**One-armed conditionals**

If the verification conditions for $\{P\}$ IF $S$ THEN $C$ $\{Q\}$ are provable, then $\vdash P \wedge \neg S \Rightarrow Q$ and all the verification conditions for $\{P \wedge S\} C \{Q\}$ are provable. Hence by the induction hypothesis $\vdash \{P \wedge S\} C \{Q\}$ and hence by the one-armed conditional rule (page 26) it follows that $\vdash \{P\}$ IF $S$ THEN $C \{Q\}$.

**Two-armed conditionals**

If the verification conditions for $\{P\}$ IF $S$ THEN $C_1$ ELSE $C_2$ $\{Q\}$ are provable, then the verification conditions for both $\{P \wedge S\} C_1 \{Q\}$ and $\{P \wedge \neg S\} C_2 \{Q\}$ are provable. By the induction hypothesis we can assume that $\vdash \{P \wedge S\} C_1 \{Q\}$ and $\vdash \{P \wedge \neg S\} C_2 \{Q\}$. Hence by the two-armed conditional rule (page 26) $\vdash \{P\}$ IF $S$ THEN $C_1$ ELSE $C_2$ $\{Q\}$.

**Sequences**

There are two cases to consider:

1. If the verification conditions for $\{P\} C_1; \ldots; C_{n-1} ; \{R\} C_n \{Q\}$ are provable, then the verification conditions for $\{P\} C_1; \ldots; C_{n-1} \{R\}$ and $\{R\} C_n \{Q\}$ must both be provable and hence by induction we have $\vdash \{P\} C_1; \ldots; C_{n-1} \{R\}$ and $\vdash \{R\} C_n \{Q\}$. Hence by the sequencing rule (page 23) $\vdash \{P\} C_1; \ldots; C_{n-1} ; C_n \{Q\}$.

2. If the verification conditions for $\{P\} C_1; \ldots; C_{n-1} ; V := E \{Q\}$ are provable, then it must be the case that the verification conditions for $\{P\} C_1; \ldots; C_{n-1} \{Q[E/V]\}$ are also provable and hence by induction we have $\vdash \{P\} C_1; \ldots; C_{n-1} \{Q[E/V]\}$. It then follows by the assignment axiom that $\vdash \{Q[E/V]\} V := E \{Q\}$, hence by the sequencing rule $\vdash \{P\} C_1; \ldots; C_{n-1} ; V := E\{Q\}$. 


Blocks

If the verification conditions for \( \{ P \} \text{BEGIN} \text{VAR} V_1; \ldots; \text{VAR} V_n; C \text{END} \{ Q \} \) are provable, then the verification conditions for \( \{ P \} C \{ Q \} \) are provable and \( V_1, \ldots, V_n \) do not occur in \( P \) or \( Q \). By induction \( \vdash \{ P \} C \{ Q \} \) hence by the block rule (page 24) \( \vdash \{ P \} \text{BEGIN} \text{VAR} V_1; \ldots; \text{VAR} V_n; C \text{END} \{ Q \} \).

WHILE\-commands

If the verification conditions for \( \{ P \} \text{WHILE} S \text{DO} \{ R \} C \{ Q \} \) are provable, then

\[
\vdash P \Rightarrow R, \quad \vdash (R \land \lnot S) \Rightarrow Q
\]

and the verification conditions for \( \{ R \land S \} C \{ R \} \) are provable. By induction \( \vdash \{ R \land S \} C \{ R \} \), hence by the WHILE\-rule (page 28) \( \vdash \{ R \} \text{WHILE} S \text{DO} C \{ R \land \lnot S \} \), hence by the consequence rules (see page 22) \( \vdash \{ P \} \text{WHILE} S \text{DO} C \{ Q \} \).

FOR\-commands

Finally, if the verification conditions for

\[
\{ P \} \text{FOR} V := E_1 \text{UNTIL} E_2 \text{DO} \{ R \} C \{ Q \}
\]

are provable, then

(i) \( \vdash P \Rightarrow R[E_1/V] \)

(ii) \( \vdash R[E_2 + 1/V] \Rightarrow Q \)

(iii) \( \vdash P \land E_2 < E_1 \Rightarrow Q \)

(iv) The verification conditions for

\[
\{ R \land E_1 \leq V \land V \leq E_2 \} C \{ R[V + 1/V] \}
\]

are provable.

(v) Neither \( V \), nor any variable in \( E_1 \) or \( E_2 \), is assigned to in \( C \).

By induction \( \vdash \{ R \land E_1 \leq V \land V \leq E_2 \} C \{ R[V + 1/V] \} \), hence by the FOR\-rule

\( \vdash \{ R[E_1/V] \land E_1 \leq E_2 \} \text{FOR} V := E_1 \text{UNTIL} E_2 \text{DO} C \{ R[E_2 + 1/V] \} \)

hence by (i), (ii) and the consequence rules

(vi) \( \vdash \{ P \land E_1 \leq E_2 \} \text{FOR} V := E_1 \text{UNTIL} E_2 \text{DO} C \{ Q \} \).

Now by the FOR\-axiom (see page 32) with \( P \) instantiated to \( P \land E_2 < E_1 \), followed by Precondition Strengthening (to eliminate the repeated \( E_2 < E_1 \)):

\( \vdash \{ P \land E_2 < E_1 \} \text{FOR} V := E_1 \text{UNTIL} E_2 \text{DO} C \{ P \land E_2 < E_1 \} \),

hence by the consequence rules and (iii)
\[ \vdash \{ P \land E_2 < E_1 \} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \{ Q \}. \]

Combining this last specification with (vi) using specification disjunction (page 22) yields

\[ \vdash \{ P \land E_2 < E_1 \} \lor \{ P \land E_1 \leq E_2 \} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \{ Q \lor Q \} \]

Now \( \vdash Q \lor Q \Rightarrow Q \) and

\[ \vdash (P \land E_2 < E_1) \lor (P \land E_1 \leq E_2) \iff P \land (E_2 < E_1 \lor E_1 \leq E_2) \]

but \( \vdash E_2 < E_1 \lor E_1 \leq E_2 \), hence

\[ \vdash P \Rightarrow (P \land E_2 < E_1) \lor (P \land E_1 \leq E_2) \]

and so one can conclude:

\[ \vdash \{ P \} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \{ Q \} \]

Thus the verification conditions for the \texttt{FOR}-command are sufficient.

**Exercise 43**
Annotate the specifications in Exercises 21 to 29 (they start on page 38) and then generate the corresponding verification conditions. $\Box$

**Exercise 44**
Devise verification conditions for commands of the form

\[ \text{REPEAT } C \text{ UNTIL } S \]

(See Exercise 30, page 41.) $\Box$

**Exercise 45**
Do Exercises 31–35 using verification conditions. $\Box$

**Exercise 46**
With the rules given, can one prove by induction on the structure of $C$ that if no variable occurring in $P$ is assigned to in $C$, then \( \vdash \{ P \} \ C \{ P \}? \) $\Box$

**Exercise 47**
Consider the following alternative scheme, due to Silas Brown, for generating VCs from annotated \texttt{WHILE}-commands.
### WHILE-commands

Alternative verification conditions generated from

\[
\{P\} \text{WHILE} S \text{DO} \{R\} \text{C} \{Q\}
\]

are

(i) \(P \land S \Rightarrow R\)

(ii) \(P \land \neg S \Rightarrow Q\)

(iii) the verification conditions generated by \(\{R\} \text{C}\{(Q \land \neg S) \lor (R \land S)\}\).

Either justify these VCs, or find a counterexample. \(\square\)
The axioms and rules of Floyd-Hoare logic are extended to total correctness. Verification conditions for total correctness specifications are given.

In Section 1.3 the notation $[P] C [Q]$ was introduced for the total correctness specification that $C$ halts in a state satisfying $Q$ whenever it is executed in a state satisfying $P$. At the end of the section describing the \texttt{WHILE}-rule (Section 2.1.10), it is shown that the rule is not valid for total correctness specifications. This is because \texttt{WHILE}-commands may introduce non-termination. None of the other commands can introduce non-termination, and thus the rules of Floyd-Hoare logic can be used.

4.1 Axioms and rules for non-looping commands

Repeating curly brackets by square ones results in the following axioms and rules.

**Assignment axiom for total correctness**

$$\vdash [P[E/V]] V := E [P]$$

**Precondition strengthening for total correctness**

$$\vdash P \Rightarrow P', \quad \vdash [P'] C [Q]$$

$$\vdash [P] C [Q]$$

**Postcondition weakening for total correctness**

$$\vdash [P] C [Q'], \quad \vdash Q' \Rightarrow Q$$

$$\vdash [P] C [Q]$$

**Specification conjunction for total correctness**

$$\vdash [P_1] C [Q_1], \quad \vdash [P_2] C [Q_2]$$

$$\vdash [P_1 \land P_2] C [Q_1 \land Q_2]$$

**Specification disjunction for total correctness**
\[
\vdash [P_1] C [Q_1], \quad \vdash [P_2] C [Q_2] \\
\vdash [P_1 \lor P_2] C [Q_1 \lor Q_2]
\]

Sequencing rule for total correctness

\[
\vdash [P] C_1 [Q], \quad \vdash [Q] C_2 [R] \\
\vdash [P] C_1; C_2 [R]
\]

Derived sequencing rule for total correctness

\[
\vdash P \Rightarrow P_1 \\
\vdash [P_1] C_1 [Q_1] \quad \vdash Q_1 \Rightarrow P_2 \\
\vdash [P_2] C_2 [Q_2] \quad \vdash Q_2 \Rightarrow P_3 \\
\vdots \\
\vdash [P_n] C_n [Q_n] \quad \vdash Q_n \Rightarrow Q \\
\vdash [P] C_1; \ldots; C_n [Q]
\]

Block rule for total correctness

\[
\vdash [P] C [Q] \\
\vdash [P] \text{BEGIN VAR } V_1; \ldots; \text{VAR } V_n; C \text{ END } [Q]
\]

Where none of the variables \(V_1, \ldots, V_n\) occur in \(P\) or \(Q\).

Derived block rule for total correctness

\[
\vdash P \Rightarrow P_1 \\
\vdash [P_1] C_1 [Q_1] \quad \vdash Q_1 \Rightarrow P_2 \\
\vdash [P_2] C_2 [Q_2] \quad \vdash Q_2 \Rightarrow P_3 \\
\vdots \\
\vdash [P_n] C_n [Q_n] \quad \vdash Q_n \Rightarrow Q \\
\vdash [P] \text{BEGIN VAR } V_1; \ldots; \text{VAR } V_n; C_1; \ldots; C_n [Q]
\]

Where none of the variables \(V_1, \ldots, V_n\) occur in \(P\) or \(Q\).

Conditional rules for total correctness

\[
\vdash [P \land S] C [Q], \quad \vdash P \land \lnot S \Rightarrow Q \\
\vdash [P] \text{IF } S \text{ THEN } C \text{ END } [Q]
\]

\[
\vdash [P \land S] C_1 [Q], \quad \vdash [P \land \lnot S] C_2 [Q] \\
\vdash [P] \text{IF } S \text{ THEN } C_1 \text{ ELSE } C_2 [Q]
\]

FOR-axiom and rule for total correctness

\[
\vdash [P \land (E_1 \leq V) \land (V \leq E_2)] C [P[V+1/V]] \\
\vdash [P[E_1/V] \land (E_1 \leq E_2)] \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C [P[E_2+1/V]]
\]
4.2 Derived rule for total correctness of non-looping commands

Where neither $V$, nor any variable occurring in $E_1$ or $E_2$, is assigned to in the command $C$.

$$ \vdash [P \land (E_2 < E_1)] \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } C \{P\} $$

4.2 Derived rule for total correctness of non-looping commands

The rules just given are formally identical to the corresponding rules of Floyd-Hoare logic, except that they have $[ \text{ and } ]$ instead of $\{ \text{ and } \}$. It is thus clear that the following is a valid derived rule.

$$ \vdash \{P\} C \{Q\} $$

If $C$ contains no WHILE-commands.

4.3 The termination of assignments

Note that the assignment axiom for total correctness states that assignment commands always terminate, which implicitly assumes that all function applications in expressions terminate. This might not be the case if functions could be defined recursively. For example, consider the assignment: $X := \text{fact}(-1)$, where $\text{fact}(n)$ is defined recursively by:

$$ \text{fact}(n) = \text{if } n = 0 \text{ then } 1 \text{ else } n \times \text{fact}(n-1) $$

It is also assumed that erroneous expressions like $1/0$ do not cause problems. Most programming languages will cause an error stop when division by zero is encountered. However, in our logic it follows that:

$$ \vdash \{T\} X := 1/0 \{X = 1/0\} $$

i.e. the assignment $X := 1/0$ always halts in a state in which the condition $X = 1/0$ holds. This assumes that $1/0$ denotes some value that $X$ can have. There are two possibilities:

(i) $1/0$ denotes some number;

(ii) $1/0$ denotes some kind of ‘error value’.

It seems at first sight that adopting (ii) is the most natural choice. However, this makes it tricky to see what arithmetical laws should hold. For example, is $(1/0) \times 0$ equal to $0$ or to some ‘error value’? If the latter, then it is no longer the case that $n \times 0 = 0$ is a valid general law of arithmetic? It is possible to make everything
work with undefined and/or error values, but the resultant theory is a bit messy. We shall assume here that arithmetic expressions always denote numbers, but in some cases exactly what the number is will be not fully specified. For example, we will assume that $m/n$ denotes a number for any $m$ and $n$, but the only property of “/” that will be assumed is:

$$\neg(n = 0) \Rightarrow (m/n) \times n = m$$

It is not possible to deduce anything about $m/0$ from this, in particular it is not possible to deduce $(m/0) \times 0 = 0$. In fact, sometimes it may be assumed that numbers are integers. In this case, the defining property of “/” is:

$$\neg(n = 0) \land p \times n = m \Rightarrow (m/n) = p$$

4.4 WHILE-rule for total correctness

WHILE-commands are the only commands in our little language that can cause non-termination, they are thus the only kind of command with a non-trivial termination rule. The idea behind the WHILE-rule for total correctness is that to prove WHILE $S$ DO $C$ terminates one must show that some non-negative quantity decreases on each iteration of $C$. This decreasing quantity is called a variant. In the rule below, the variant is $E$, and the fact that it decreases is specified with an auxiliary variable $n$. An extra hypothesis, $\vdash P \land S \Rightarrow E \geq 0$, ensures the variant is non-negative.

```
WHILE-rule for total correctness

\[ \vdash [P \land S \land (E = n)] C [P \land (E < n)], \quad \vdash P \land S \Rightarrow E \geq 0 \]
\[ \vdash [P] \textbf{WHILE} S \textbf{DO} C [P \land \neg S] \]
```

where $E$ is an integer-valued expression and $n$ is an auxiliary variable not occurring in $P$, $C$, $S$ or $E$.

Example: We show:

$$\vdash [Y > 0] \textbf{WHILE} Y \leq R \textbf{DO} \text{ BEGIN } R := R - Y; \ Q := Q + 1 \text{ END } [T]$$

Take

\[
\begin{align*}
P &= Y > 0 \\
S &= Y \leq R \\
E &= R \\
C &= \text{ BEGIN } R := R - Y \ Q := Q + 1 \text{ END }
\end{align*}
\]

We want to show $\vdash [P] \textbf{WHILE} S \textbf{DO} C [T]$. By the WHILE-rule for total correctness it is sufficient to show:
4.5 Termination specifications

(i) \(\vdash [P \land S \land (E = n)] \rightarrow [P \land (E < n)]\)

(ii) \(\vdash P \land S \Rightarrow E \geq 0\)

The first of these, (i), can be proved by establishing

\[\vdash \{P \land S \land (E = n)\} \rightarrow \{P \land (E < n)\}\]

and then using the total correctness rule for non-looping commands. The verification condition for this partial correctness specification is:

\[Y > 0 \land Y \leq R \land R = n \Rightarrow (Y > 0 \land R < n)[Q+1/Q][R-Y/R]\]

i.e.

\[Y > 0 \land Y \leq R \land R = n \Rightarrow Y > 0 \land R-Y < n\]

which follows from the laws of arithmetic.

The second subgoal, (ii), is just \(\vdash Y > 0 \land Y \leq R \Rightarrow R \geq 0\), which follows from the laws of arithmetic. □

4.5 Termination specifications

As already discussed in Section 1.3, the relation between partial and total correctness is informally given by the equation:

Total correctness = Termination + Partial correctness.

This informal equation above can now be represented by the following two formal rules of inferences.

\[
\frac{\vdash \{P\} \rightarrow \{Q\}, \quad \vdash [P] \rightarrow [T]}{\vdash [P] \rightarrow [T]}\\
\frac{\vdash [P] \rightarrow [Q]}{\vdash \{P\} \rightarrow \{Q\}, \quad \vdash [P] \rightarrow [T]}
\]

Exercise 48
Think about whether these two rules derivable from the other rules? □

4.6 Verification conditions for termination

The idea of verification conditions is easily extended to deal with total correctness.

To generate verification conditions for `WHILE`-commands, it is necessary to add a variant as an annotation in addition to an invariant. No other extra annotations are needed for total correctness. We assume this is added directly after the invariant,
surrounded by square brackets. A correctly annotated total correctness specification of a \texttt{WHILE}-command thus has the form

\[ [P] \text{WHILE } S \text{ DO } \{R\} [E] C [Q] \]

where $R$ is the invariant and $E$ the variant. Note that the variant is intended to be a non-negative expression that decreases each time around the \texttt{WHILE} loop. The other annotations, which are enclosed in curly brackets, are meant to be conditions that are true whenever control reaches them. The use of square brackets around variant annotations is meant to be suggestive of this difference.

The rules for generating verification conditions from total correctness specifications are now given in the same format as the rules for generating partial correctness verification conditions given in Section 3.4.

### 4.7 Verification condition generation

**Assignment commands**

The single verification condition generated by

\[ [P] V := E [Q] \]

is

\[ P \Rightarrow Q[E/V] \]

**Example:** The verification condition for

\[ [X=0] X := X+1 [X=1] \]

is

\[ X=0 \Rightarrow (X+1)=1 \]

This is the same as for partial correctness. □

**One-armed conditional**

The verification conditions generated by

\[ [P] \text{IF } S \text{ THEN } C [Q] \]

are

(i) \( (P \land \neg S) \Rightarrow Q \)

(ii) the verifications generated by \([P \land S] C [Q]\)
Example: The verification conditions for

\[ T \text{ IF } X < 0 \text{ THEN } X := -X \ [X \geq 0] \]

are \( T \land \neg(X < 0) \Rightarrow X \geq 0 \) together with the verification conditions for
\[ T \land (X < 0) \ X := -X \ [X \geq 0], \] i.e. \( T \land (X < 0) \Rightarrow -X \geq 0 \). The two verification conditions are thus: \( T \land \neg(X > 0) \Rightarrow X \geq 0 \) and \( T \land (X < 0) \Rightarrow -X \geq 0 \). These are both clearly true. □

Two-armed conditional

The verification conditions generated from

\[ [P] \text{ IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \ [Q] \]

are

(i) the verification conditions generated by \([P \land S] \ C_1 \ [Q]\)

(ii) the verifications generated by \([P \land \neg S] \ C_2 \ [Q]\)

Exercise 49

What are the verification conditions for the following specification?

\[ T \text{ IF } X \geq Y \text{ THEN } \text{MAX} := X \ \text{ELSE} \ \text{MAX} := Y \ [\text{MAX} = \max(X, Y)] \]

□

If \( C_1; \ldots; C_n \) is properly annotated, then (see page 50) it must be of one of the two forms:

1. \( C_1; \ldots; C_{n-1}; \{R\}C_n, \) or

2. \( C_1; \ldots; C_{n-1}; V := E. \)

where, in both cases, \( C_1; \ldots; C_{n-1} \) is a properly annotated command.
Sequences

1. The verification conditions generated by

\[ [P] \ C_1; \ldots; C_{n-1}; \{R\} C_n \ [Q] \]

(where \( C_n \) is not an assignment) are:

(a) the verification conditions generated by

\[ [P] \ C_1; \ldots; C_{n-1} \ [R] \]

(b) the verification conditions generated by

\[ [R] \ C_n \ [Q] \]

2. The verification conditions generated by

\[ [P] \ C_1; \ldots; C_{n-1}; V := E \ [Q] \]

are the verification conditions generated by

\[ [P] \ C_1; \ldots; C_{n-1} \ [Q[E/V]] \]

Example: The verification conditions generated from

\[ [X=x \ \land \ Y=y] \ R := X; \ X := Y; \ Y := R \ [X=y \ \land \ Y=x] \]

are those generated by

\[ [X=x \ \land \ Y=y] \ R := X; \ X := Y \ [(X=y \ \land \ Y=x) [R/Y]] \]

which, after doing the substitution, simplifies to

\[ [X=x \ \land \ Y=y] \ R := X; \ X := Y \ [X=y \ \land \ R=x] \]

The verification conditions generated by this are those generated by

\[ [X=x \ \land \ Y=y] \ R := X \ [(X=y \ \land \ R=x) [Y/X]] \]

which, after doing the substitution, simplifies to

\[ [X=x \ \land \ Y=y] \ R := X \ [Y=y \ \land \ R=x] . \]

The only verification condition generated by this is

\[ X=x \ \land \ Y=y \ \Rightarrow \ Y=y \ \land \ R=x \]

which, after doing the substitution, simplifies to

\[ X=x \ \land \ Y=y \ \Rightarrow \ Y=y \ \land \ X=x \]
which is obviously true. □

Blocks

The verification conditions generated by

\[ [P] \text{BEGIN VAR } V_1; \ldots ; \text{VAR } V_n; C \text{ END } [Q] \]

are

(i) the verification conditions generated by \([P] \ C \ [Q] \), and

(ii) the syntactic condition that none of \(V_1, \ldots, V_n\) occur in either \(P\) or \(Q\).

Example: The verification conditions for

\[ [X=x \land Y=y] \text{BEGIN VAR } R; R:=X; X:=Y; Y:=R \text{ END } [X=y \land Y=x] \]

are those generated by \([X=x \land Y=y] \ R:=X; X:=Y; Y:=R \ [X=y \land Y=x] \) (since \(R\) does not occur in \([X=x \land Y=y]\) or \([X=y \land Y=x]\)). See the previous example for the verification conditions generated by this. □

A correctly annotated specification of a WHILE-command has the form

\[ [P] \text{WHILE } S \text{ DO } \{R\}[E] \ C \ [Q] \]

while-commands

The verification conditions generated from

\[ [P] \text{WHILE } S \text{ DO } \{R\}[E] \ C \ [Q] \]

are

(i) \(P \Rightarrow R\)

(ii) \(R \land \neg S \Rightarrow Q\)

(iii) \(R \land S \Rightarrow E \geq 0\)

(iv) the verification conditions generated by

\[ [R \land S \land (E = n)] \ C[R \land (E < n)] \]

where \(n\) is an auxiliary variable not occurring in \(P, C, S, R, E\) or \(Q\).

Example: The verification conditions for

\[ [R=X \land Q=0] \]

\[ \text{WHILE } Y \leq R \text{ DO } \{X=R+Y \times Q\}[R] \]

\[ \text{BEGIN } R:=R-Y; Q=Q+1 \text{ END} \]

\[ [X = R+(Y \times Q) \land R < Y] \]
are:

(i) \( R = X \land Q = 0 \Rightarrow (X = R + (Y \times Q)) \)

(ii) \( X = R + Y \times Q \land \neg (Y \leq R) \Rightarrow (X = R + (Y \times Q) \land R < Y) \)

(iii) \( X = R + Y \times Q \land Y \leq R \Rightarrow R \geq 0 \)

together with the verification condition for

\[
[X = R + (Y \times Q) \land (Y \leq R) \land (R = n)]
\begin{align*}
\text{BEGIN } & R := R - Y; \quad Q := Q + 1 \quad \text{END} \\
\text{[}X = R + (Y \times Q) \land (R < n)\text{]} 
\] \]

which (exercise for the reader) consists of the single condition

(iv) \( X = R + (Y \times Q) \land (Y \leq R) \land (R = n) \Rightarrow X = (R - Y) + (Y \times (Q + 1)) \land ((R - Y) < n) \)

But this isn’t true (take \( Y = 0 \))! □

**Exercise 50**

Explain why one would not expect to be able to prove the verification conditions of the last example. Change the specification and annotations so that provable verifications are generated. □

A correctly annotated specification of a FOR-command has the form

\[
\{P\} \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } \{R\} \text{ C } \{Q\}
\]

**FOR-commands**

The verification conditions generated from

\[
[P] \text{ FOR } V := E_1 \text{ UNTIL } E_2 \text{ DO } \{R\} \text{ C } [Q]
\]

are

(i) \( P \Rightarrow R[E_1/V] \)

(ii) \( R[E_2 + 1/V] \Rightarrow Q \)

(iii) \( P \land E_2 < E_1 \Rightarrow Q \)

(iv) the verification conditions generated by

\[
[R \land E_1 \leq V \land V \leq E_2] \text{ C } [R[V + 1/V]]
\]

(v) the syntactic condition that neither \( V \), nor any variable occurring in \( E_1 \) or \( E_2 \), is assigned to inside \( C \).

**Example:** The verification conditions generated by
4.7 Verification condition generation

\[X=0 \land 1 \leq M\]
\[
\text{FOR } N:=1 \text{ UNTIL } M \text{ DO } \{X=\((N-1)\times N) \text{ DIV } 2\} \quad X:=X+N
\]
\[
X = (M\times(M+1)) \text{ DIV } 2
\]

are

(i) \(X=0 \land 1 \leq M \Rightarrow X=\((1-1)\times1) \text{ DIV } 2\)

(ii) \(X = (((M+1)-1)\times(M+1)) \text{ DIV } 2 \Rightarrow X = (M\times(M+1)) \text{ DIV } 2\)

(iii) \(X=0 \land 1 \leq M \land M<1 \Rightarrow X = (M\times(M+1)) \text{ DIV } 2\)

(iv) The verification condition generated by
\[
\begin{align*}
[X = ((N-1)\times N) \text{ DIV } 2 \land 1 \leq N \land N \leq M] \\
X:=X+N \\
[X = (((N+1)-1)\times(N+1)) \text{ DIV } 2]
\end{align*}
\]

(v) The syntactic condition that neither \(N\) or \(M\) is assigned to in \(X:=X+N\).

These verification conditionss are proved in the example on page 57. \(\square\)

We leave it as an exercise for the reader to extend the argument given in Section 3.5 to a justification of the total correctness verification conditions.
Chapter 5

Program Refinement

Floyd-Hoare Logic is a method of proving that existing programs meet their specifications. It can also be used as a basis for ‘refining’ specifications to programs – i.e. as the basis for a programming methodology.

5.1 Introduction

The task of a programmer can be viewed as taking a specification consisting of a precondition $P$ and postcondition $Q$ and then coming up with a command $C$ such that $\vdash [P] C [Q]$.

Theories of refinement present rules for ‘calculating’ programs $C$ from specification $P$ and $Q$. A key idea, due to Ralph Back [3] of Finland (and subsequently rediscovered by both Joseph Morris [35] and Carroll Morgan [34]), is to introduce a new class of programming constructs, called specifications. These play the same syntactic role as commands, but are not directly executable though they are guaranteed to achieve a given postcondition from a given precondition. The resulting generalized programming language contains pure specifications, pure code and mixtures of the two. Such languages are called wide spectrum languages.

The approach taken here follows the style of refinement developed by Morgan, but is founded on Floyd-Hoare logic, rather than on Dijkstra’s theory of weakest preconditions (see Section 7.6.2). This foundation is a bit more concrete and syntactical than the traditional one: a specification is identified with its set of possible implementations and refinement is represented as manipulations on sets of ordinary commands. This approach aims to convey the ‘look and feel’ of (Morgan style) refinement using the notational and conceptual ingredients introduced in the preceding chapters.

The notation $[P, Q]$ will be used for specifications, and thus:

$$[P, Q] = \{ C \mid \vdash [P] C [Q] \}$$

The process of refinement will then consist of a sequence of steps that make systematic design decisions to narrow down the sets of possible implementations until

---

1The approach to refinement described here is due to Paul Curzon. Mark Staples and Joakim Von Wright provided some feedback on an early draft, which I have incorporated.
a unique implementation is reached. Thus a refinement of a specification \( S \) to an implementation \( C \) has the form:

\[
S \supseteq S_1 \supseteq S_2 \cdots \supseteq S_n \supseteq \{ C \}
\]

The initial specification \( S \) has the form \([P, Q]\) and each intermediate specification \( S_i \) is obtained from its predecessor \( S_{i-1} \) by the application of a refinement law.

In the literature \( S \supseteq S' \) is normally written \( S \subseteq S' \). The use of “\( \supseteq \)” here, instead of the more abstract “\( \subseteq \)”, reflects the concrete interpretation of refinement as the narrowing down of sets of implementations.

### 5.2 Refinement laws

The refinement laws are derived from the axioms and rules of Floyd-Hoare Logic. In order to state these laws, the usual notation for commands is extended to sets of commands as follows (\( C, C_1, C_2 \) etc. range over sets of commands):

\[
C_1; \cdots ; C_n = \{ C_1; \cdots ; C_n \mid C_1 \in C_1 \land \cdots \land C_n \in C_n \}
\]

\[
\text{BEGIN} \text{VAR} V_1; \cdots \text{VAR} V_n; \text{END} = \{ \text{BEGIN} \text{VAR} V_1; \cdots \text{VAR} V_n; \text{END} \mid C \in C \}
\]

\[
\text{IF} S \text{THEN} C = \{ \text{IF} S \text{THEN} C \mid C \in C \}
\]

\[
\text{IF} S \text{THEN} C_1 \text{ELSE} C_2 = \{ \text{IF} S \text{THEN} C_1 \text{ELSE} C_2 \mid C_1 \in C_1 \land C_2 \in C_2 \}
\]

\[
\text{WHILE} S \text{DO} C = \{ \text{WHILE} S \text{DO} C \mid C \in C \}
\]

This notation for sets of commands can be viewed as constituting a wide spectrum language.

Note that such sets of commands are monotonic with respect to refinement (i.e. inclusion). If \( C \supseteq C', C_1 \supseteq C_1', \ldots, C_n \supseteq C_n' \), then:

\[
C_1; \cdots ; C_n \supseteq C_1'; \cdots ; C_n'
\]

\[
\text{BEGIN} \text{VAR} V_1; \cdots \text{VAR} V_n; \text{END} \supseteq \text{BEGIN} \text{VAR} V_1; \cdots \text{VAR} V_n; C' \text{END}
\]

\[
\text{IF} S \text{THEN} C \supseteq \text{IF} S \text{THEN} C'
\]

\[
\text{IF} S \text{THEN} C_1 \text{ELSE} C_2 \supseteq \text{IF} S \text{THEN} C_1' \text{ELSE} C_2'
\]

\[
\text{WHILE} S \text{DO} C \supseteq \text{WHILE} S \text{DO} C'
\]

This monotonicity shows that a command can be refined by separately refining its constituents.

The following 'laws' follow directly from the definitions above and the axioms and rules of Floyd-Hoare logic.
5.2. Refinement laws

The Skip Law
\[ [P, P] \supseteq \{\text{SKIP}\} \]

Derivation
\[ C \in \{\text{SKIP}\} \]
\[ \iff C = \text{SKIP} \]
\[ \Rightarrow \vdash [P] \ C \ [P] \quad \text{(Skip Axiom)} \]
\[ \Rightarrow C \in [P, P] \quad \text{(Definition of \([P, P]\))} \]

The Assignment Law
\[ [P[E/V], P] \supseteq \{V := E\} \]

Derivation
\[ C \in \{V := E\} \]
\[ \iff C = V := E \]
\[ \Rightarrow \vdash [P[E/V]] \ C \ [P] \quad \text{(Assignment Axiom)} \]
\[ \Rightarrow C \in [P[E/V], P] \quad \text{(Definition of \([P[E/V], P]\))} \]

Derived Assignment Law
\[ [P, Q] \supseteq \{V := E\} \]

provided \( \vdash P \Rightarrow Q[E/V] \)

Precondition Weakening
\[ [P, Q] \supseteq [R, Q] \]

provided \( \vdash P \Rightarrow R \)

Derivation
\[ C \in [R, Q] \]
\[ \iff \vdash [R] \ C \ [Q] \quad \text{(Definition of \([R, Q]\))} \]
\[ \Rightarrow \vdash [P] \ C \ [Q] \quad \text{(Precondition Strengthening \& \( \vdash P \Rightarrow R \))} \]
\[ \Rightarrow C \in [P, Q] \quad \text{(Definition of \([P, Q]\))} \]
Postcondition Strengthening

\[ [P, Q] \supseteq [P, R] \]
provided \( \vdash R \Rightarrow Q \)

Derivation

\[ C \in [P, R] \]
\( \iff \vdash [P] \ C \ [R] \quad \text{(Definition of } [R, Q]) \]
\( \Rightarrow \vdash [P] \ C \ [Q] \quad \text{(Postcondition Weakening & } \vdash R \Rightarrow Q) \)
\( \iff C \in [P, Q] \quad \text{(Definition of } [P, Q]) \]

The Sequencing Law

\[ [P, Q] \supseteq [P, R] ; [R, Q] \]

Derivation

\( C \in [P, R] ; [R, Q] \)
\( \iff C \in \{ C_1 ; C_2 \mid C_1 \in [P, R] \land C_2 \in [R, Q] \} \quad \text{(Definition of } C_1 ; C_2) \)
\( \iff C \in \{ C_1 ; C_2 \mid \vdash [P] C_1 [R] \land \vdash [R] C_2 [Q] \} \quad \text{(Definition of } [P, R] \text{ and } [R, Q]) \)
\( \Rightarrow C \in \{ C_1 ; C_2 \mid \vdash [P] C_1 ; C_2 [Q] \} \quad \text{(Sequencing Rule)} \)
\( \iff C \in [P, Q] \quad \text{(Definition of } [P, Q]) \)

The Block Law

\[ [P, Q] \supseteq \begin{array}{l}
\text{BEGIN VAR } V ; [P, Q] \text{ END}
\end{array} \]
where \( V \) does not occur in \( P \) or \( Q \)

Derivation

\( C \in \begin{array}{l}
\text{BEGIN VAR } V ; [P, Q] \text{ END}
\end{array} \)
\( \iff C \in \{ \begin{array}{l}
\text{BEGIN VAR } V ; C' \text{ END} | C' \in [P, Q] \end{array} \} \quad \text{(Definition of-BEGIN VAR } V ; C \text{ END)} \)
\( \iff C \in \{ \begin{array}{l}
C' \in [P, Q] \mid \vdash [P] C' [Q] \end{array} \} \quad \text{(Definition of } [P, Q]) \)
\( \Rightarrow C \in \{ \begin{array}{l}
\text{BEGIN VAR } V ; C' \text{ END} | \vdash [P] \text{ BEGIN VAR } V ; C' \text{ END} [Q] \end{array} \} \quad \text{(Block Rule & } V \text{ not in } P \text{ or } Q) \)
\( \iff \vdash [P] C [Q] \quad \text{(Definition of } [P, Q]) \)

The One-armed Conditional Law

\[ [P, Q] \supseteq \text{IF } S \text{ THEN } [P \land S, Q] \]
provided \( \vdash P \land \neg S \Rightarrow Q \)
Derivation

\[ C \in \text{IF } S \text{ THEN } [P \land S, \ Q] \]
\[ \equiv \ C \in \{ \text{IF } S \text{ THEN } C' \mid C' \in [P \land S, \ Q] \} \] (Definition of \text{IF } S \text{ THEN } C)
\[ \equiv \ C \in \{ \text{IF } S \text{ THEN } C' \mid \vdash [P \land S] C' [Q] \} \] (Definition of \([P \land S, \ Q]\))
\[ \equiv \ C \in \{ \text{IF } S \text{ THEN } C' \mid \vdash [P] \text{ IF } S \text{ THEN } C' [Q] \} \] (One-armed Conditional Rule & \(\vdash P \land \neg S \Rightarrow Q\))
\[ \equiv \ C \in [P, Q] \] (Definition of \([P, Q]\))

5.3 An example

The Two-armed Conditional Law

\([P, Q] \supset \text{IF } S \text{ THEN } [P \land S, \ Q] \text{ ELSE } [P \land \neg S, \ Q]\)

Derivation

\[ C \in \text{IF } S \text{ THEN } [P \land S, \ Q] \text{ ELSE } [P \land \neg S, \ Q] \]
\[ \equiv \ C \in \{ \text{IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \mid \]
\[ C_1 \in [P \land S, \ Q] \text{ & } C_2 \in [P \land \neg S, \ Q] \} \] (Definition of \text{IF } S \text{ THEN } C_1 \text{ ELSE } C_2)
\[ \equiv \ C \in \{ \text{IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \mid \]
\[ \vdash [P \land S] C_1 [Q] \text{ & } \vdash [P \land \neg S] C_2 [Q] \} \] (Definition of \([P \land S, \ Q] \& [P \land \neg S, \ Q]\))
\[ \equiv \ C \in \{ \text{IF } S \text{ THEN } C_1 \text{ ELSE } C_2 \mid \]
\[ \vdash [P] \text{ IF } S \text{ THEN } C_1 \text{ ELSE } C_2 [Q] \} \] (Two-armed Conditional Rule)
\[ \equiv \ C \in [P, Q] \] (Definition of \([P, Q]\))

The While Law

\([P, P \land \neg S] \supset \text{WHILE } S \text{ DO } [P \land S \land (E=n), \ P \land (E<n)] \]

provided \(\vdash P \land S \Rightarrow E \geq 0\)

where \(E\) is an integer-valued expression and \(n\) is an identifier not occurring in \(P, S\) or \(E\).

Derivation

\[ C \in \text{WHILE } S \text{ DO } [P \land S \land (E=n), \ P \land (E<n)] \]
\[ \equiv \ C \in \{ \text{WHILE } S \text{ DO } C' \mid \]
\[ C' \in [P \land S \land (E=n), \ P \land (E<n)] \} \] (Definition of \text{WHILE } S \text{ DO } C)
\[ \equiv \ C \in \{ \text{WHILE } S \text{ DO } C' \mid \]
\[ \vdash [P \land S \land (E=n)] C' [P \land (E<n)] \} \] (Definition of \([P \land S \land (E=n), \ P \land (E<n)]\))
\[ \equiv \ C \in \{ \text{WHILE } S \text{ DO } C' \mid \]
\[ \vdash [P] \text{ WHILE } S \text{ DO } C' [P \land \neg S] \} \] (While Rule & \(\vdash P \land S \Rightarrow E \geq 0\))
\[ \equiv \ C \in [P, P \land \neg S] \] (Definition of \([P, P \land \neg S]\))

5.3 An example

The notation \([P_1, P_2, P_3, \cdots, P_{n-1}, P_n]\) will be used to abbreviate:

\([P_1, P_2] \mid [P_2, P_3] \mid \cdots \mid [P_{n-1}, P_n]\)

The brackets around fully refined specifications of the form \(\{C\}\) will be omitted – e.g. if \(C\) is a set of commands, then \(R := X \ ; C\) abbreviates \(R := X \ ; C\).
The familiar division program can be ‘calculated’ by the following refinement of the specification: \[ Y > 0, \; X = R + (Y \times Q) \land R \leq Y \]

Let \( I \) stand for the invariant \( X = R + (Y \times Q) \). In the refinement that follows, the comments in curley brackets after the symbol “\( \supseteq \)” indicate the refinement law used for the step.

\[
\begin{align*}
Y > 0, \; I \land R \leq Y & \supseteq (\text{Sequencing}) \\
Y > 0, \; R = X \land Y > 0, \; I \land R \leq Y & \supseteq (\text{Assignment}) \\
R := X; \; [R = X \land Y > 0, \; I \land R \leq Y] & \supseteq (\text{Sequencing}) \\
R := X; \; [R = X \land Y > 0, \; R = X \land Y > 0 \land Q = 0, \; I \land R \leq Y] & \supseteq (\text{Assignment}) \\
(R := X) \quad ; \quad Q := 0; \; [R = X \land Y > 0 \land Q = 0, \; I \land R \leq Y] & \supseteq (\text{Precondition Weakening}) \\
(R := X) \quad ; \quad Q := 0; \; [I \land Y > 0, \; I \land R \leq Y] & \supseteq (\text{Postcondition Strengthening}) \\
R := X; \; Q := 0; \; [I \land Y > 0, \; I \land Y > 0 \land \neg (Y \leq R)] & \supseteq (\text{While}) \\
R := X; \; Q := 0; \; \text{WHILE} \; Y \leq R \; \text{DO} \; [I \land Y > 0 \land Y \leq R \land R = n, \; I \land Y > 0 \land R < n] & \supseteq (\text{Sequencing}) \\
R := X; \; Q := 0; \; \text{WHILE} \; Y \leq R \; \text{DO} \; [I \land Y > 0 \land Y \leq R \land R = n, \; X = (R - Y) + (Y \times Q) \land Y > 0 \land (R - Y) < n, \; I \land Y > 0 \land R < n] & \supseteq (\text{Derived Assignment}) \\
R := X; \; Q := 0; \; \text{WHILE} \; Y \leq R \; \text{DO} \; [I \land Y > 0 \land Y \leq R \land R = n, \; X = (R - Y) + (Y \times Q) \land Y > 0 \land (R - Y) < n] & \supseteq (\text{Derived Assignment}) \\
R := X; \; Q := 0; \; \text{WHILE} \; Y \leq R \; \text{DO} \; Q := Q + 1; \; R := R - Y & \supseteq (\text{While})
\end{align*}
\]

5.4 General remarks

The ‘Morgan style of refinement’ illustrated here provides laws for systematically introducing structure with the aim of eventually getting rid of specification statements. This style has been accused of being “programming in the microscopic”.

The ‘Back style’ is less rigidly top-down and provides a more flexible (but maybe also more chaotic) program development framework. It also emphasises and supports transformations that distribute control (e.g. going from sequential to parallel programs). General algebraic laws not specifically involving specification statements are used, for example:

\[ C = \text{IF } S \text{ THEN } C \text{ ELSE } C \]

which can be used both to introduce and eliminate conditionals.

Both styles of refinement include large-scale transformations (data refinement and superposition) where a refinement step actually is a much larger change than a simple IF or WHILE introduction. However, this will not be covered here.
Chapter 6

Higher Order Logic

Higher order logic generalises first order logic by supporting \(\lambda\)-notation and allowing variables to range over functions and predicates. To preserve consistency it is typed. Various programming logics can be embedded in higher order logic.

Higher order predicate calculus (also called “higher order logic” and “simple type theory”) uses the familiar notation of first order logic.

- “\(P(x)\)” means “\(x\) has property \(P\),”
- “\(\neg t\)” means “not \(t\),”
- “\(t_1 \land t_2\)” means “\(t_1\) and \(t_2\),”
- “\(t_1 \lor t_2\)” means “\(t_1\) or \(t_2\),”
- “\(t_1 \Rightarrow t_2\)” means “\(t_1\) implies \(t_2\),”
- “\(\forall x. t[x]\)” means “for all \(x\) it is the case that \(t[x]\),”
- “\(\exists x. t[x]\)” means “for some \(x\) it is the case that \(t[x]\),”
- “\(\exists! x. t[x]\)” means “there is a unique \(x\) such that \(t[x]\).”

The difference is that in higher order logic, statements (or formulae) are regarded as boolean valued terms, i.e. terms whose value is one of the two truth values (or booleans) \(T\) or \(F\). In the phrases just listed, \(t\), \(t_1\) and \(t_2\) stand for arbitrary boolean terms, and \(t[x]\) stands for some boolean term containing the variable \(x\).

The structure of terms in higher order logic is more general that in the first order case. There are four kinds of terms; these will be explained in detail later, but here is a quick overview:

1. **Variables.** These are sequences of letters or digits beginning with a letter. For example: \(x, y, P\).
2. **Constants.** Constants stand for fixed values. They will be distinguished from variables by being either mathematical characters or strings in sans serif font. Examples of constants are: \(T, F\) (the truth-values), \(0, 1, 2, \ldots\) (numbers), \(+, \times\), (arithmetical operators) \(<, \leq\) (arithmetical predicates).
3. **Function applications.** These have the general form \( t_1 \, t_2 \) where \( t_1 \) and \( t_2 \) are terms, an example is \( P \, 0 \). Brackets can be inserted around terms to increase readability or to enforce grouping, thus \( P \, 0 \) is equivalent to \( P(0) \). Binary function constants can be infixed. Thus one can write \( t_1 + t_2 \) instead of \(+ \, t_1 \, t_2\).

4. **Lambda-terms.** These denote functions and have the form \( \lambda x. \, t \) (where \( x \) is a variable and \( t \) a term). For example, \( \lambda n. \, n + 1 \) denotes the successor function.

The various kinds of statements are just terms in higher order logic. For example, \( \neg t \) is just the application of the constant \( \neg \) to the term \( t \) and \( t_1 \Rightarrow t_2 \) is just the infixed application of the binary constant \( \Rightarrow \) to argument terms \( t_1 \) and \( t_2 \).

The representation of quantifiers as terms is less straightforward, because of bound variables. In higher order logic, there is only a single variable binding mechanism: \( \lambda \)-abstraction. The quantifiers \( \forall \) and \( \exists \) are regarded as constants and the quantifications \( \forall x. \, t \) and \( \exists x. \, t \) are ‘user friendly syntax’ for the terms \( \forall (\lambda x. \, t) \) and \( \exists (\lambda x. \, t) \). Such constants are called *binders*.

**Example:** \( \forall n. \, P(n) \Rightarrow P(n + 1) \) is written instead of \( \forall (\lambda n. \, \Rightarrow (P(n))(P(+ \, n \, 1))) \)

Higher order logic generalizes first order logic by allowing *higher order* variables — i.e. variables ranging over functions and predicates. For example, the induction axiom for natural numbers can be written as:

\[
\forall P. \, P(0) \land (\forall n. \, P(n) \Rightarrow P(n + 1)) \Rightarrow \forall n. \, P(n)
\]

and the legitimacy of simple recursive definitions (the Peano-Lawvere Axiom [30]) can be expressed by:

\[
\forall n_0. \, \forall f. \, \exists s. \, (s(0) = n_0) \land (\forall n. \, s(n + 1) = f(s(n)))
\]

Sentences like these are not allowed in first order logic: in the first example above \( P \) ranges over predicates; in the second example \( f \) and \( s \) range over functions.

An example that will be central to the next chapter is the representation of partial correctness specifications in higher order logic. This is done by defining a predicate (i.e. a function whose result is a truth value) \( \text{Spec} \) by:

\[
\text{Spec}(p, c, q) = \forall s_1 \, s_2. \, p \, s_1 \land c(s_1, s_2) \Rightarrow q \, s_2
\]

\( \text{Spec} \) is a predicate on triples \( (p, c, q) \) where \( p \) and \( q \) are unary predicates and \( c \) is a binary predicate. To represent command sequencing we can define a constant \( \text{Seq} \) by:

\[
\text{Seq}(c_1, c_2)(s_1, s_2) = \exists s. \, c_1(s_1, s) \land c_2(s, s_2)
\]
The sequencing rule in Hoare logic can be stated directly in higher order logic as:

\[ \forall p \ q \ r \ c_1 \ c_2, \ Spec(p, c_1, q) \land Spec(q, c_2, r) \Rightarrow Spec(p, Seq(c_1, c_2), r) \]

These examples, which will be fully explained in the next chapter, make essential use of higher order variables; they can’t be expressed in first-order logic.

6.1 Terms

The four kinds of terms in the higher order logic are variables, constants, applications (of a function to an argument) and abstractions (also called \( \lambda \)-terms). These are described in detail below.

6.1.1 Variables and constants

Variables and constants stand for values. Variables will normally be strings of letters and digits starting with a letter. They will be written in italics. Constants can either be strings of letters and digits starting with a letter but they will be written in sans serif font. In addition, there are some special non-alphanumeric symbols for the constants representing logical operators; these include: the equals sign (=), the equivalence symbol (\( \equiv \)), the negation symbol (\( \neg \)), the conjunction symbol (\( \land \)), the disjunction symbol (\( \lor \)), the implication symbol (\( \Rightarrow \)), the universal quantifier (\( \forall \)), the existential quantifier (\( \exists \)), the unique existence quantifier (\( \exists! \)) and Hilbert’s epsilon symbol (\( \varepsilon \)). Other allowed constant symbols are the pairing symbol (comma: \( , \)), the numerals 0, 1, 2 etc., the arithmetic functions +, \( - \), \( \times \) and \( / \), and the arithmetic relations \( < \), \( > \), \( \leq \) and \( \geq \).

6.1.2 Function applications

Terms of the form \( t_1(t_2) \) are called applications or combinations. The subterm \( t_1 \) is called the operator (or rator) and the term \( t_2 \) is called the operand (or rand or argument). The result of such a function application can itself be a function and thus terms like \( (t_1(t_2))(t_3) \) are allowed. Functions that take functions as arguments or return functions as results are called higher order.

To save writing brackets, function applications can be written as \( f \ x \) instead of \( f(x) \). More generally we adopt the usual convention that \( t_1 \ t_2 \ t_3 \ \ldots \ t_n \) abbreviates \( ( \ldots (t_1 t_2) t_3) \ldots t_n \) i.e. application associates to the left.

6.1.3 Lambda-terms

The version of higher order logic presented here\(^1\) provides lambda-terms (also called \( \lambda \)-terms or abstractions) for denoting functions. Such a term has the form \( \lambda x. t \)

\(^1\)The version of higher order logic presented here is based on ‘Simple Type Theory’ which was invented by the logician Alonzo Church in 1940 [8].
(where $t$ is a term) and denotes the function $f$ defined by:

$$f(x) = t$$

For example, $\lambda n. \cos(\sin(n))$ denotes the function $f$ such that:

$$f(n) = \cos(\sin(n))$$

thus: $f(1) = \cos(\sin(1))$, $f(2) = \cos(\sin(2))$ etc. The variable $x$ and term $t$ are called respectively the bound variable and body of the $\lambda$-expression $\lambda x. t$. An occurrence of the bound variable in the body is called a bound occurrence. If an occurrence is not bound it is called free.

### 6.2 Types

The increased expressive power gained by allowing higher order variables is dangerous. Consider the predicate $P$ defined by:

$$P x = \neg(x x)$$

from this definition it follows that:

$$P P = \neg(P P)$$

which is a version of Russell’s paradox. Russell invented a method for preventing such inconsistencies based on the use of types [18]. The formulation used here is a simplification of Russell’s type system due to Church [8] with extensions developed by Milner [15]. It is very similar to the type system of the ML programming language.

Types are expressions that denote sets of values, they are either atomic or compound. Examples of atomic types are:

- $\text{bool}$, $\text{ind}$, $\text{num}$, $\text{real}$

these denote the sets of booleans, individuals, natural numbers and real numbers respectively. Compound types are built from atomic types (or other compound types) using type operators. For example, if $\sigma$, $\sigma_1$ and $\sigma_2$ are types then so are:

$$\sigma \text{ list}, \sigma_1 \rightarrow \sigma_2, \sigma_1 \times \sigma_2$$

where $\text{list}$ is a unary type operator and $\rightarrow$ and $\times$ are an infixed binary type operators. The type $\sigma \text{ list}$ denotes the set of lists of values of type $\sigma$, the type $\sigma_1 \rightarrow \sigma_2$ denotes the set of functions with domain denoted by $\sigma_1$ and range denoted by $\sigma_2$ and the type $\sigma_1 \times \sigma_2$ denotes the Cartesian product type of pairs whose first component has type $\sigma_1$ and second component has type $\sigma_2$ (see Section 6.3.3). In general, compound types are expressions of the form:

$$(\sigma_1, \ldots, \sigma_n) \text{ op}$$
where \( \text{op} \) is a type operator and \( \sigma_1, \ldots, \sigma_n \) are types. If the operator has only one argument then the brackets can be omitted (hence \( \sigma \text{ list} \)); the types \( \sigma_1 \rightarrow \sigma_2 \) and \( \sigma_1 \times \sigma_2 \) are \textit{ad hoc} abbreviations for \( (\sigma_1, \sigma_2) \text{fun} \) and \( (\sigma_1, \sigma_2) \text{prod} \), respectively. We will use lower case slanted identifiers for particular types, and greek letters (mostly \( \sigma \)) to range over arbitrary types.

Terms of higher order logic must be \textit{well-typed} in the sense that each subterm can be assigned a type 'in a consistent way'. More precisely, it must be possible to assign a type to each subterm such that both 1 and 2 below hold.

1. For every subterm of the form \( t_1 t_2 \) there are types \( \sigma \) and \( \sigma' \) such that:
   - \( t_1 \) is assigned \( \sigma' \rightarrow \sigma \)
   - \( t_2 \) is assigned \( \sigma' \)
   - \( t_1 t_2 \) is assigned the type \( \sigma \).

2. Every subterm of the form \( \lambda x. \ t \) is assigned a type \( \sigma_1 \rightarrow \sigma_2 \) where:
   - \( x \) is assigned \( \sigma_1 \)
   - \( t \) is assigned \( \sigma_2 \).

Variables with the same name can be assigned different types, but then they are regarded as different variables.

Writing \( t: \sigma \) indicates that a term \( t \) has type \( \sigma \). Thus \( x: \sigma_1 \) is the same variable as \( x: \sigma_2 \) if and only if \( \sigma_1 = \sigma_2 \). In Church’s original notation \( t: \sigma \) would be written \( t_{\sigma} \).

In some formulations of higher-order logic, the types of variables have to be written down explicitly. For example, \( \lambda x. \cos(\sin(x)) \) would not be allowed in Church’s system, instead one would have to write:

\[
\lambda x_{\text{real}}. \cos_{\text{real}} \rightarrow_{\text{real}} \sin_{\text{real}} \rightarrow_{\text{real}} \langle x_{\text{real}} \rangle
\]

We allow the types of variables to be omitted if they can be inferred from the context. There is an algorithm, due to Robin Milner [33], for doing such type inference.

We adopt the standard conventions that \( \sigma_1 \rightarrow \sigma_2 \rightarrow \sigma_3 \rightarrow \cdots \rightarrow \sigma_n \rightarrow \sigma \) is an abbreviation for \( \sigma_1 \rightarrow (\sigma_2 \rightarrow (\sigma_3 \rightarrow (\cdots (\sigma_n \rightarrow \sigma) \cdots))) \) i.e. \( \rightarrow \) associates to the right. This convention blends well with the left associativity of function application, because if \( f \) has type \( \sigma_1 \rightarrow \cdots \rightarrow \sigma_n \rightarrow \sigma \) and \( t_1, \ldots, t_n \) have types \( \sigma_1, \ldots, \sigma_n \) respectively, then \( f t_1 \cdots t_n \) is a well-typed term of type \( \sigma \). We also assume \( \times \) is more tightly binding than \( \rightarrow \); for example, \( \text{state} \times \text{state} \rightarrow \text{bool} \) means \( (\text{state} \times \text{state}) \rightarrow \text{bool} \). The notation \( \lambda x_1 x_2 \cdots x_n. \ t \) abbreviates \( \lambda x_1. \lambda x_2. \cdots \lambda x_n. \ t \). The scope of the \( . \) after a \( \lambda \) extends as far to the right as possible. Thus, for example, \( \lambda b. \ b = \lambda x. \ T \) means \( \lambda b. \ (b = (\lambda x. \ T)) \) not \( (\lambda b. \ b) = (\lambda x. \ T) \).
6.2.1 Type variables and polymorphism

Consider the function \texttt{twice} defined by:

\[
\texttt{twice} = \lambda f. \lambda x. f(f(x))
\]

If \( f \) is a function then \( \texttt{twice}(f) \), the result of applying \texttt{twice} to \( f \), is the function \( \lambda x. f(f(x)) \); \texttt{twice} is thus a function-returning function, i.e. it is higher order. For example, if \( \sin \) is a trigonometric function with type \( \text{real} \rightarrow \text{real} \), then \( \texttt{twice} (\sin) \) is \( \lambda x. \sin(\sin(x)) \) which is the function taking the \( \sin \) of the \( \sin \) of its argument, a function of type \( \text{real} \rightarrow \text{real} \), and if \( \texttt{not} \) is a boolean function with type \( \text{bool} \rightarrow \text{bool} \), then \( \texttt{twice} (\texttt{not}) \) is \( \lambda x. \texttt{not} (\texttt{not}(x)) \) which is the function taking the double negation of its argument, a function of type \( \text{bool} \rightarrow \text{bool} \). What then is the type of the function \( \texttt{twice} \)? Since \( \texttt{twice}(\sin) \) has type \( \text{real} \rightarrow \text{real} \) it would appear that \( \texttt{twice} \) has the type \( (\text{real} \rightarrow \text{real}) \rightarrow (\text{real} \rightarrow \text{real}) \). However, since \( \texttt{twice}(\texttt{not}) \) has type \( \text{bool} \rightarrow \text{bool} \) it would also appear that \( \texttt{twice} \) has the type \( (\text{bool} \rightarrow \text{bool}) \rightarrow (\text{bool} \rightarrow \text{bool}) \). Thus \( \texttt{twice} \) would appear to have two different types. In Church’s Simple Type Theory this would not be allowed and we would have to define two functions, \( \texttt{twice}_{\text{real} \rightarrow \text{real}} \rightarrow (\text{real} \rightarrow \text{real}) \) and \( \texttt{twice}_{\text{bool} \rightarrow \text{bool}} \rightarrow (\text{bool} \rightarrow \text{bool}) \) say. In the version of higher order used here, type variables are used to overcome this messiness; for example, if \( \alpha \) is a type variable then \( \texttt{twice} \) can be given the type \( (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha) \) and it behaves as though it has all instances of this that can be obtained by replacing \( \alpha \) by a type. Types containing type variables are called \textit{polymorphic}, ones not containing variables are \textit{monomorphic}. We shall call a term polymorphic or monomorphic if its type is polymorphic or monomorphic respectively. We will use \( \alpha, \beta, \gamma \) etc. for type variables. This use of type variables is an extension of Church’s simple type theory. It is due to Robin Milner and was developed by him for a special purpose logic called \texttt{PPLAMBDA}[15].

An \textit{instance} of a type \( \sigma \) is a type obtained by replacing zero or more type variables in \( \sigma \) by types. Here are some instances of \( (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha) \):

\[
(\text{real} \rightarrow \text{real}) \rightarrow (\text{real} \rightarrow \text{real}) \\
(\text{bool} \rightarrow \text{bool}) \rightarrow (\text{bool} \rightarrow \text{bool}) \\
((\alpha \rightarrow \text{bool}) \rightarrow (\alpha \rightarrow \text{bool})) \rightarrow ((\alpha \rightarrow \text{bool}) \rightarrow (\alpha \rightarrow \text{bool}))
\]

In these examples \( \alpha \) has been replaced by \( \text{real}, \text{bool} \) and \( \alpha \rightarrow \text{bool} \) respectively. The only instances of monomorphic types are themselves.

All constants are assumed to have a fixed type. If this type is polymorphic then for the purposes of type checking the constant behaves as though it is assigned every instance of the type. For example, if \( \texttt{twice} \) had type \( (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha) \), then the terms \( \texttt{twice}(\sin) \) and \( \texttt{twice}(\texttt{not}) \) would be well-typed.

6.3 Special Syntactic Forms

Certain applications are conventionally written in special ways, for example:
• $t_1 + t_2$ is written $t_1 + t_2$

• $t_1, t_2$ is written $(t_1, t_2)$

• $\forall (\lambda x. t)$ is written $\forall x. t$

Constants can have a special syntactic status to support such forms. For example, $+$ and $\cdot$ are examples of infixes and $\forall$ is an example of a binder. Some other ad hoc syntactic forms are also allowed, these are explained below.

### 6.3.1 Infixes

Constants with types of the form $\sigma_1 \to \sigma_2 \to \sigma_3$ can be infixes. If $f$ is an infixed constant then applications are written as $t_1 f t_2$ rather than as $f t_1 t_2$. Standard examples of infixes are the arithmetic functions $+$, $\times$ etc. Whether a constant is an infix or not has no logical significance, it is merely syntactic.

Examples of infixes are the following constants:

- $\land : \text{bool} \to \text{bool} \to \text{bool}$ (Conjunction - i.e. “and”)
- $\lor : \text{bool} \to \text{bool} \to \text{bool}$ (Disjunction - i.e. “or”)
- $\Rightarrow : \text{bool} \to \text{bool} \to \text{bool}$ (Implication - i.e. “implies”)
- $\equiv : \text{bool} \to \text{bool} \to \text{bool}$ (Equivalence - i.e. “if and only if”)

Equality is also an infixed constant; it is polymorphic:

- $= : \alpha \to \alpha \to \text{bool}$

Equivalence ($\equiv$) is equality ($=$) restricted to booleans. The constants $\land$, $\lor$, $\Rightarrow$, $\equiv$ and $=$ are all infixes.

### 6.3.2 Binders

It is sometimes more readable to write $f x. t$ instead of $f(\lambda x. t)$. For example, the quantifiers $\forall$ and $\exists$ are polymorphic constants:

- $\forall : (\alpha \to \text{bool}) \to \text{bool}$
- $\exists : (\alpha \to \text{bool}) \to \text{bool}$

The idea is that if $P : \sigma \to \text{bool}$, then $\forall(P)$ is true if $P(x)$ is true for all $x$ and $\exists(P)$ is true if $P(x)$ is true for some $x$. Instead of writing $\forall(\lambda x. t)$ and $\exists(\lambda x. t)$ it is nice to be able to use the more conventional forms $\forall x. t$ and $\exists x. t$.

Any constant $f$ with a type of the form $(\sigma_1 \to \sigma_2) \to \sigma_3$ can be a binder, so that instead of writing:

$$f(\lambda x_1. f(\lambda x_2. \cdots f(\lambda x_n. t) \cdots))$$

one writes:

$$f \; x_1 \cdots \; x_n. \; t$$
As with infixes, the binder status of a constant is purely syntactic.

Recall the statement of mathematical induction:

\[ \forall P. P(0) \land (\forall n. P(n) \Rightarrow P(n+1)) \Rightarrow \forall n. P(n) \]

This is a term of type bool. Without using infix and binder notation it would be much less readable, namely:

\[ \forall(\lambda P. \Rightarrow(\land(\lambda 0. \Rightarrow(\forall n. \Rightarrow(\lambda n. P(n))(P(n+1)))))))(\forall(\lambda n. P(n))) \]

The quantifiers \( \forall \) and \( \exists \) need not be primitive; they can be defined in terms of more primitive notions. We will not, however, go into this here.

### 6.3.3 Pairs and tuples

A function of \( n \) arguments can be represented as a higher order function of 1 argument that returns a function of \( n-1 \) arguments. Thus \( \lambda m. \lambda n. m^2 + n^2 \) represents the 2 argument function that sums the squares of its arguments. Functions of this form are called curried. An alternative way of representing multiple argument functions is as single argument functions taking tuples as arguments. To handle tuples a binary type operator \( \text{prod} \) is used. If \( t_1: \sigma_1 \) and \( t_2: \sigma_2 \) then the term \( (t_1, t_2) \) has type \( (\sigma_1, \sigma_2)\text{prod} \) and denotes the pair of values. The type \( (\sigma_1, \sigma_2)\text{prod} \) can also be written as \( \sigma_1 \times \sigma_2 \). Another representation of the sum-squares function would be as a constant, \( \text{sumsq} \) say, of type \( (\text{num} \times \text{num}) \rightarrow \text{num} \) defined by:

\[ \text{sumsq}(m, n) = m^2 + n^2 \]

A term of the form \( (t_1, t_2) \) is equivalent to the term \( , t_1 t_2 \) where \( , \) is a polymorphic infixed constant of type \( \alpha \rightarrow \beta \rightarrow (\alpha \times \beta) \). Instead of having tuples as primitive, they will be treated as iterated pairs. Thus the term:

\[ (t_1, t_2, \ldots, t_{n-1}, t_n) \]

is an abbreviation for:

\[ (t_1, (t_2, \ldots, (t_{n-1}, t_n) \ldots)) \]

i.e. \( , \) associates to the right. To match this, the infixed type operator \( \times \) also associates to the right so that if \( t_1: \sigma_1, \ldots, t_n: \sigma_n \) then:

\[ (t_1, \ldots, t_n) : \sigma_1 \times \cdots \times \sigma_n \]

The type operator \( \text{prod} \) can be defined in terms of \( \text{fun} \) and thus pairing need not be primitive. We shall not go into this here.
6.3.4 Lists

To represent lists, types of the form $\sigma$ list are used, together with constants Nil and Cons of types $\alpha$ list and $\alpha \to (\alpha$ list)$\to(\alpha$ list) respectively. A term with type $\sigma$ list denotes a list of values all of type $\sigma$. Nil is the empty list; $[]$ is an alternative form of Nil and $[t_1; \ldots; t_n]$ as an alternative form for $\text{Cons} \ t_1 (\text{Cons} \ t_2 \cdots (\text{Cons} \ t_n \text{Nil}) \cdots)$.

The difference between lists and tuples is:

1. Different lists of a given type can contain different numbers of elements, but all tuples of a given type contain exactly the same numbers of elements.

2. The elements of a list must all have the same type but elements of tuples can have different types.

6.3.5 Conditionals

The constant Cond is defined so that $\text{Cond} \ t \ t_1 \ t_2$ means “if $t$ then $t_1$ else $t_2$”. The special syntax $(t \to t_1 \mid t_2)$ is provided for such terms. The original conditional notation due to McCarthy used “,” instead of “|”.

6.3.6 Hilbert’s $\varepsilon$-operator

If $t[x]$ is a boolean term containing a free variable $x$ of type $\sigma$, then the Hilbert-term $\varepsilon x. \ t[x]$ denotes some value of type $\sigma$, $a$ say, such that $t[a]$ is true. For example, the term $\varepsilon n. \ n < 10$ denotes some unspecified number less than 10 and the term $\varepsilon n. \ (n^2 = 25) \land (n \geq 0)$ denotes 5.

If there is no $a$ of type $\sigma$ such that $t[a]$ is true then $\varepsilon x. \ t[x]$ denotes a fixed but unspecified value of type $\sigma$. For example, $\varepsilon n. \neg (n = n)$ denotes an unspecified number. The logical axiom

$$\vdash \forall P. \ P x \Rightarrow P(\varepsilon P)$$

which is called SELECT AX, defines the meaning of $\varepsilon$. This axiom is equivalent to:

$$\vdash \forall P. \ (\exists x. \ P x) \Rightarrow P(\varepsilon P)$$

It must be admitted that the $\varepsilon$-operator looks rather suspicious. For a thorough discussion of it see [26]. It is useful for naming things one knows to exist but have no name. For example, the Peano-Lawvere axiom asserts that given a number $n_0$ and a function $f: \text{num} \to \text{num}$, there exists a unique sequence $s$ defined recursively by:

$$(s(0) = n_0) \land (\forall n. \ s(n + 1) = f(s(n)))$$

Using the $\varepsilon$-operator we can define a function, Rec say, that returns $s$ when given the pair $(n_0, f)$ as an argument:

$$\text{Rec}(n_0, f) = \varepsilon s. \ (s(0) = n_0) \land (\forall n. \ s(n + 1) = f(s(n)))$$
\( \text{Rec}(n_0, f) \) denotes the unique sequence whose existence is asserted by the Peano-Lawvere Axiom. It follows from this axiom that:

\[
(\text{Rec}(n_0, f)0 = n_0) \land (\forall n. \text{Rec}(n_0, f)(n + 1) = f(\text{Rec}(n_0, f)n))
\]

Many things that are normally primitive can be defined using the \( \varepsilon \)-operator. For example, the conditional term \( \text{Cond} t t_1 t_2 \) (meaning “if \( t \) then \( t_1 \) else \( t_2 \)”) can be defined by:

\[
\text{Cond} t t_1 t_2 = \varepsilon x. ((t = T) \Rightarrow (x = t_1)) \land ((t = F) \Rightarrow (x = t_2))
\]

One can use the \( \varepsilon \)-operator to simulate \( \lambda \)-abstraction: if the variable \( f \) does not occur in the term \( t \), then the function \( \lambda x. t \) is equivalent to \( \varepsilon f. \forall x. f(x) = t \) (“the function \( f \) such that \( f(x) = t \) for all \( x \)”). This idea can be used to create functional abstractions that cannot be expressed with simple \( \lambda \)-terms. For example, the factorial function is denoted by:

\[
\varepsilon f. \forall n. (f(0) = 1) \land (f(n + 1) = (n + 1) \times f(n))
\]

Terms like this can be used to simulate the kind of pattern matching mechanisms found in programming languages like ML.

The inclusion of \( \varepsilon \)-terms in the logic ‘builds in’ the Axiom of Choice [18]. In Set Theory, the Axiom of Choice states that if \( S \) is a family of sets then there exists a function, \( \text{Choose} \) say, such that for each non-empty \( X \in S \) we have \( \text{Choose}(X) \in X \). As sets are not primitive in higher order logic, we must reformulate \( \text{Choose} \) to act on the characteristic functions of sets rather than sets themselves. The characteristic function of a set \( X \) is the function \( f_X \) with range \( \{T, F\} \) defined by \( f_X(x) = T \) if and only if \( x \in X \). If \( P \) is any function with range \( \{T, F\} \), we call \( P \) non-empty if for some \( x \) it is the case that \( P(x) = T \) (so \( f_X \) is non-empty if and only if \( X \) is non-empty). The higher order logic version of the Axiom of Choice asserts that there exists a function, \( \text{Select} \) say, such that if \( P \) is a non-empty function with range \( \{T, F\} \) then \( P(\text{Select}(P)) = T \). Intuitively \( \text{Select} \) \( P \) is just \( \text{Choose}\{x \mid P(x) = T\} \).

Hilbert’s \( \varepsilon \)-operator is a binder that denotes \( \text{Select} \). More precisely \( \varepsilon \) is a binder with type \( (\alpha \rightarrow \text{bool}) \rightarrow \alpha \) which is interpreted so that if \( P \) has type \( \sigma \rightarrow \text{bool} \) then:

- \( \varepsilon(P) \) denotes some fixed (but unknown) value \( x \) such that \( P(x) = T \) if such a value exists;

- if no such value exists (i.e. \( P(x) = F \) for all \( x \)) then \( \varepsilon(P) \) denotes some unspecified value in the set denoted by \( \sigma \).

Having \( \varepsilon \)-terms forces every type to be non-empty because the term \( \varepsilon x:\sigma.T \) always denotes a member of \( \sigma \).
6.4 Definitions

Definitions are axioms of the form $\vdash c = t$ where $c$ is a new constant and $t$ is a closed term\(^2\) (i.e. a term without any free variables) that doesn’t contain $c$. Such a definition just introduces the constant $c$ as an abbreviation for the term $t$. The requirement that $c$ may not occur in $t$ prevents definitions from being recursive, this is to rule out inconsistent ‘definitions’ like $\vdash c = c + 1$. A function definition:

$$\vdash f = \lambda x_1 \cdots x_n. t$$

can be written as:

$$\vdash f x_1 \cdots x_n = t$$

For example, the definition of $\text{Seq}$ given in Section 7.3 below is:

$$\vdash \text{Seq} = \lambda (C_1, C_2). \lambda (s_1, s_2). \exists s. C_1(s_1, s) \land C_2(s, s_2)$$

which is logically equivalent to:

$$\vdash \text{Seq}(C_1, C_2)(s_1, s_2) = \exists s. C_1(s_1, s) \land C_2(s, s_2)$$

Definitions have the property that adding a new definition to the set of existing ones cannot introduce any new inconsistencies. As was shown by Russell and Whitehead [18], with suitable definitions, all of classical mathematics can be constructed from logic together with the assumption that there are infinitely many individuals (the Axiom of Infinity). It is thus not necessary to postulate axioms other than definitions.

6.5 Peano’s axioms

The natural numbers are defined by introducing a type $\text{num}$ and constants $0 : \text{num}$ and $\text{Suc} : \text{num} \rightarrow \text{num}$ and then postulating Peano’s Axioms\(^3\). These axioms are:

1. There is a number $0$.
2. There is a function $\text{Suc}$ called the successor function such that if $n$ is a number then $\text{Suc} n$ is a number.
3. $0$ is not the successor of any number.
4. If two numbers have the same successor then they are equal.
5. If a property holds of $0$ and if whenever it holds of a number then it also holds of the successor of the number, then the property holds of all numbers. This postulate is called Mathematical Induction.

\(^2\)It is also necessary to require that all type variables occurring in the types of subterms of $t$ also occur in the type of $c$, but this technicality is glossed over here.

\(^3\)In fact, the type $\text{num}$ and constants $0$ and $\text{Suc}$ can be defined in higher order logic and Peano’s axioms then proved as theorems (given the Axiom of Infinity). We will not go into this here; in particular, we will not describe how types are defined.
The first two postulates hold because $0: \text{num}$ and $\text{Suc}: \text{num} \rightarrow \text{num}$. The following axiom formalizes the third postulate:

$$\vdash \forall m. \neg (\text{Suc } m = 0)$$

The forth postulate is:

$$\vdash \forall n. (\text{Suc } m = \text{Suc } n) \Rightarrow (m = n)$$

The fifth postulate, Mathematical Induction, is higher order:

$$\vdash \forall P: \text{num} \rightarrow \text{bool}. P 0 \land (\forall m. P m \Rightarrow P(\text{Suc } m)) \Rightarrow \forall m. P m$$

The numerals 1, 2, 3 etc. are defined by:

$$\vdash 1 = \text{Suc } 0$$
$$\vdash 2 = \text{Suc}(\text{Suc } 0)$$
$$\vdash 3 = \text{Suc}(\text{Suc}(\text{Suc } 0))$$

Because $\text{Suc}$ is one-to-one these denote an infinite set of distinct values of type $\text{num}$.

### 6.5.1 Primitive recursion

The usual theorems of arithmetic can be derived from Peano’s postulates. The first step in doing this is to provide a mechanism for defining functions recursively. For example, the usual ‘definition’ of $+$ is:

$$\vdash 0 + m = m$$
$$\vdash (\text{Suc } m) + n = \text{Suc}(m + n)$$

Unfortunately this isn’t a definition. In order to convert such recursion equations into definitions we need the Primitive Recursion Theorem:

$$\vdash \forall x: \alpha. \forall f: \alpha \rightarrow \text{num} \rightarrow \alpha. \exists \text{fun}: \text{num} \rightarrow \alpha. (\text{fun } 0 = x) \land (\forall m. \text{fun}($$ \text{Suc } m$$) = f(\text{fun } m)m)$$

The proof of this theorem from Peano’s postulates is quite complicated and is omitted. To show that the Primitive Recursion Theorem solves the problem of defining $+$ one specializes it by taking $x$ to be $\lambda n. n$ and $f$ to be $\lambda f’: x’. \lambda n. \text{Suc}(f’ n)$, this yields:

$$\vdash \exists \text{fun}. (\text{fun } 0 = (\lambda n. n)) \land (\forall m. \text{fun}(\text{Suc } m) = (\lambda f’ x’. \lambda n. \text{Suc}(f’ n))(\text{fun } m)m)$$
which is equivalent to:

\[ \exists \text{fun. } (\text{fun } 0 \ n = n) \land \\ \quad (\text{fun}(\text{Suc } m)n = \text{Suc}(\text{fun } m \ n)) \]

Thus, if we define + by:

\[ + = \exists \text{fun. } (\forall m. (\text{fun } 0 \ n = n) \land \\ \quad (\text{fun}(\text{Suc } m)n = \text{Suc}(\text{fun } m \ n))) \]

then it follows from the axiom for the \( \varepsilon \)-operator that:

\[ 0 + n = n \]
\[ (\text{Suc } m) + n = \text{Suc}(m + n) \]

as desired.

The method just used to define + generalizes to any primitive recursive definition. Such a definition has the form:

\[
\begin{align*}
\text{fun } 0 \ x_1 \cdots x_n &= f_1 \ x_1 \cdots x_n \\
\text{fun} (\text{Suc } m) \ x_1 \cdots x_n &= f_2 (\text{fun } m \ x_1 \cdots x_n) \ m \ x_1 \cdots x_n
\end{align*}
\]

where \( \text{fun} \) is the function being defined and \( f_1 \) and \( f_2 \) are given functions. To define a \( \text{fun} \) satisfying these equations we first define:

\[ \triangleright \text{Prim}_\text{Rec} = \lambda x. \exists \text{fun. } (\text{fun } 0 = x) \land \\ \quad (\forall m. \text{fun}(\text{Suc } m) = f(\text{fun } m) m) \]

It then follows by the axiom for the \( \varepsilon \)-operator and the Primitive Recursion Theorem that:

\[ \triangleright \text{Prim}_\text{Rec} \ x \ f \ 0 = x \]
\[ \triangleright \text{Prim}_\text{Rec} \ x \ f \ (\text{Suc } m) = f (\text{Prim}_\text{Rec} \ x \ f \ m) \ m \]

A function \( \text{fun} \) satisfying the primitive recursive equations above can thus be defined by:

\[ \triangleright \text{fun} = \text{Prim}_\text{Rec} \ f_1 (\lambda f \ m \ x_1 \cdots x_n. \ f_2 (f \ x_1 \cdots x_n) \ m \ x_1 \cdots x_n) \]

An example of a primitive recursion in this form is the definition of +:

\[ \triangleright + = \text{Prim}_\text{Rec} (\lambda x_1. \ x_1) (\lambda f \ m \ x_1. \ \text{Suc}(f \ x_1)) \]

### 6.5.2 Arithmetic

Standard arithmetic functions and relations can easily be defined. These include the primitive recursive infixes +, −, × and > which are defined:

\[ \triangleright (0 + n = n) \land ((\text{Suc } m) + n = \text{Suc}(m + n)) \]
The division function is an infix / defined by:
\[ m / n = \exists x. m = n \times x \]
This satisfies:
\[ \exists x. m = n \times x \vdash m = n \times (m/n) \]
The arithmetic relation > is defined by primitive recursion above. The other relations are defined without recursion by:
\[ m < n = (n > m) \]
\[ m \leq n = (m < n) \lor (m = n) \]
\[ m \geq n = (m > n) \lor (m = n) \]

The various laws of arithmetic can be deduced from these definitions, together with Peano’s axioms and axioms and rules of inference of predicate calculus.

6.5.3 Lists

Values of type \( \sigma \) list are finite lists of values of type \( \sigma \). The two standard list processing functions:
\[
\text{Nil} : \alpha \text{ list} \\
\text{Cons} : \alpha \rightarrow (\alpha \text{ list}) \rightarrow (\alpha \text{ list})
\]
satisfy the the following primitive recursion theorem for lists:
\[
\vdash \forall x: \beta. \forall f: \beta \rightarrow (\alpha \text{ list}) \rightarrow \beta. \exists ! \text{fun}: (\alpha \text{ list}) \rightarrow \beta.
\]
\[
(fun \text{ Nil} = x) \land \\
(\forall h t. fun(\text{Cons} h t) = f(fun t)h t)
\]
This theorem, which can be proved from suitable definitions of Cons, Nil and the type operator list (not given here), serves as the only ‘axiom’ for lists. It can be used to define the additional list processing functions:
\[
\text{Hd} : (\alpha \text{ list}) \rightarrow \alpha \\
\text{Tl} : (\alpha \text{ list}) \rightarrow (\alpha \text{ list}) \\
\text{Null} : (\alpha \text{ list}) \rightarrow \text{bool}
\]

\footnote{In fact, in the formal development of numbers, < is usually defined using a higher order trick before primitive recursion has been established.}
The definitions of these functions (which are left as an exercise for the reader) ensure that they have the usual properties, namely:

\[ \vdash \text{Null} \text{Nil} \]
\[ \vdash \forall x \ l. \neg(\text{Null}(\text{Cons} \ x \ l)) \]
\[ \vdash \forall x \ l. \text{Hd}(\text{Cons} \ x \ l) = x \]
\[ \vdash \forall x \ l. \text{Tl}(\text{Cons} \ x \ l) = l \]
\[ \vdash \forall l. \neg(\text{Null} \ l) \Rightarrow \text{Cons}(\text{Hd} \ l)(\text{Tl} \ l) = l \]

In addition we want lists to have the following property, which is analogous to induction for numbers:

\[ \vdash \forall P. (P \text{Nil}) \land (\forall l. (P \text{Cons} \ x \ l) \Rightarrow \forall x. P(\text{Cons} \ x \ l)) \Rightarrow \forall l. P \ l \]

This property follows directly from the uniqueness part of the primitive recursion theorem for lists given above.

The following alternative notation for lists is allowed: the empty list \text{Nil} can be written as \([\ ]\) and a list of the form \text{Cons} \ t_1(\text{Cons} \ t_2 \cdots (\text{Cons} \ t_n \text{Nil}) \cdots) can be written as \([t_1; \cdots; t_n]\).

6.6 Semantics

In this section we give a very informal sketch of the intended set-theoretic semantics of higher order logic.

The essential idea is that types denote sets and terms denote members of these sets. Only well-typed terms are considered meaningful. If term \(t\) has type \(\sigma\) then \(t\) should denote a member of the set denoted by \(\sigma\).

The meaning of a type depends on the interpretation of the type variables (as sets) that it contains. A type \(\sigma\) containing type variables \(\alpha_1, \ldots, \alpha_m\) denotes a function from \(m\)-tuples of sets to sets, such a function is not itself a set but is a class. For example, the type \(\alpha \to \alpha\) denotes the ‘class function’ that maps a set \(X\) to the set of functions from \(X\) to \(X\) (i.e. \(\alpha \to \alpha\) denotes \(X \mapsto \{f \mid f : X \to X\}\)).

Polymorphic constants are interpreted as functions of the interpretations of the type variables in their type. For example, the standard meaning of the constant \(I : \alpha \to \alpha\) is the function that maps a set \(X\) (the interpretation of \(\alpha\)) to the identity function on \(X\).

The meaning of a term depends on the interpretation of the constants, free variables and type variables in it. The interpretation of a term \(t\) with type variables \(\alpha_1, \ldots, \alpha_m\) and free variables \(x_1: \sigma_1, \ldots, x_n: \sigma_n\) is a function from \(m+n\)-tuples of sets to sets. More specifically, it is a function from tuples \((X_1, \ldots, X_m, v_1, \ldots, v_n)\) where each \(X_i\) is a set and each \(v_i\) is a member of the interpretation of \(\sigma_i\) (where \(\sigma_i\) is interpreted with respect to the interpretation of \(\alpha_1, \ldots, \alpha_m\) as \(X_1, \ldots, X_m\)). For example, the interpretation of \((\lambda x: \alpha. \ x) \ y\) with respect to the tuple \((X, v)\) is
v, where X is the interpretation of α and v ∈ X is the interpretation of y (i.e. the term \((\lambda x: \alpha. \ x) \ y\) denotes \((X, v) \mapsto v\)).

Type variables are regarded as implicitly universally quantified at the outermost level. Thus a theorem \(\vdash (\lambda x: \alpha. \ x) \ y = y\) asserts that with respect to every interpretation of α as a (non-empty) set X the interpretation of \(\lambda x: \alpha. \ x\) is a function which when applied to the interpretation, v say, of y yields v.
Chapter 7

Deriving Floyd-Hoare Logic

It is shown how Floyd-Hoare logic can be derived in higher order logic. This involves (i) defining the meaning of commands with suitable semantic definitions, (ii) regarding correctness specifications as notations for certain statements in higher order logic, and (iii) showing that these statements obey the laws of Floyd-Hoare logic. A number of alternative program specification methods are briefly discussed.

7.1 Semantic embedding

Specialized languages and logics can often be represented in higher order logic by the method of semantic embedding. To illustrate this consider the propositional language:

\[
\text{wff ::= True \mid N \ wff \mid C \ wff \ wff \mid D \ wff \ wff}
\]

One approach to embedding this little language, called deep embedding, is to represent \textit{wff}s \textit{inside} the host logic (higher order logic in this example) by values of some type, \textit{wff} say, and then define \textit{in the host logic} a semantic function, \(\mathcal{M}\) say, by recursion:

\[
\begin{align*}
\mathcal{M}(\text{True}) &= T \\
\mathcal{M}(\text{N w}) &= \neg \mathcal{M}(w) \\
\mathcal{M}(\text{C w}_1 w_2) &= \mathcal{M}(w_1) \land \mathcal{M}(w_2) \\
\mathcal{M}(\text{D w}_1 w_2) &= \mathcal{M}(w_1) \lor \mathcal{M}(w_2)
\end{align*}
\]

Here \(\mathcal{M}\) is a constant of higher order logic of type \textit{wff} \(\rightarrow\) \textit{bool}.

Another approach, called shallow embedding, is to set up notational conventions for translating \textit{wff}s into host logic terms. Suppose \([w]\) is the translation of \(w\) into higher order logic. The operation \(w \mapsto [w]\) is not defined ‘inside’ the host logic, but corresponds to an informal set of ‘parsing and pretty-printing’ conventions. Let \(\rightsquigarrow\) mean “is translated by notational conventions to”, then with shallow embedding:

\[
\begin{align*}
[\text{True}] &\rightsquigarrow "T" \\
[N \ w] &\rightsquigarrow "\neg" \rightsquigarrow [w] \\
[C \ w_1 w_2] &\rightsquigarrow [w_1] \rightsquigarrow "\land" \rightsquigarrow [w_2] \\
[D \ w_1 w_2] &\rightsquigarrow [w_1] \rightsquigarrow "\lor" \rightsquigarrow [w_2]
\end{align*}
\]
Deep and shallow embedding are really two ends of a spectrum. At intermediate points of this spectrum some aspects of the semantics would be formalized inside the host logic and others as informal notational conventions.

The advantage of deep embedding is that theorems about the embedded language can be proved. For example:

$$\forall w_1 w_2 \in \text{wff}. \mathcal{M}(Cw_1w_2) = \mathcal{M}(\text{ND}Nw_1\text{N}w_2)$$

It formalizes more of the embedding, but also requires a host logic expressive enough to accommodate this formalization.

With shallow embedding only theorems in the embedded language are provable. In the example above, quantification over \textit{wff}s is not expressible. There is less in the logic, and hence the embedding is less demanding on it and so it is often easier to support complex notations.

In the rest of this chapter, shallow embeddings of Hoare specifications will be described, together with an outline of how the axioms and rules of Floyd-Hoare logic can be derived.

### 7.2 A simple imperative programming language

We will only consider a subset of our little programming language; in particular, \texttt{FOR}-commands and arrays are omitted. Instead of having separate one and two-armed conditionals, we will instead just have two-armed conditionals together with a \texttt{SKIP}-command. The syntax of this subset is specified by the BNF given below. In this specification, the variable \(N\) ranges over the \textit{numerals} 0, 1, 2 etc, the variable \(V\) ranges over \textit{program variables} \(X, Y, Z\) etc, the variables \(E, E_1, E_2\) etc. range over \textit{integer expressions}, the variables \(B, B_1, B_2\) etc. range over \textit{boolean expressions} and the variables \(C, C_1, C_2\) etc. range over \textit{commands}.

\[
\begin{align*}
E & ::= \quad N \mid V \mid E_1 + E_2 \mid E_1 - E_2 \mid E_1 \times E_2 \mid \ldots \\
B & ::= \quad E_1 = E_2 \mid E_1 \leq E_2 \mid \ldots \\
C & ::= \quad \text{SKIP} \\
& \quad \mid V ::= E \\
& \quad \mid C_1 ; C_2 \\
& \quad \mid \text{IF } B \text{ THEN } C_1 \text{ ELSE } C_2 \\
& \quad \mid \text{WHILE } B \text{ DO } C
\end{align*}
\]

A formal semantics of \{\(P\)\} \(C\) \{\(Q\)\} in higher order logic will be given later.

---

1To distinguish program variables from logical variables, the convention is adopted here that the former are upper case and the latter are lower case. The need for such a convention is explained in Section 7.3.
7.2. A simple imperative programming language

7.2.1 Axioms and rules of Hoare logic

Here are the axioms and rules of Floyd-Hoare logic for the language used in this chapter. These are minor variants of the ones given earlier. We write \( \vdash \{ P \} C \{ Q \} \) if \( \{ P \} C \{ Q \} \) is either an instance of one of the axiom schemes A1 or A2 below, or can be deduced by a sequence of applications of the rules R1, R2, R3, R4 or R5 below from such instances. We write \( \vdash P \), where \( P \) is a formula of predicate logic, if \( P \) can be deduced from the laws of logic and arithmetic.

If \( \vdash P \), where \( P \) is a formula of predicate calculus or arithmetic, then we say ‘\( \vdash P \) is a theorem of pure logic’; if \( \vdash \{ P \} C \{ Q \} \) we say ‘\( \vdash \{ P \} C \{ Q \} \) is a theorem of Hoare logic’.

**A1: the SKIP-axiom.** For any formula \( P \):

\[ \vdash \{ P \} \text{SKIP} \{ P \} \]

**A2: the assignment-axiom.** For any formula \( P \), program variable \( V \) and integer expression \( E \):

\[ \vdash \{ P[E/V] \} V := E \{ P \} \]

where \( P[E/V] \) denotes the result of substituting \( E \) for all free occurrences of \( V \) in \( P \) (and free variables are renamed, if necessary, to avoid capture).

Rules R1 to R5 below are stated in standard notation: the hypotheses of the rule above a horizontal line and the conclusion below it. For example, R1 states that if \( \vdash P' \Rightarrow P \) is a theorem of pure logic and \( \vdash \{ P \} C \{ Q \} \) is a theorem of Hoare logic, then \( \vdash \{ P' \} C \{ Q \} \) can be deduced by R1.

**R1: the rule of precondition strengthening.** For any formulae \( P, P' \) and \( Q \), and command \( C \):

\[ \vdash P' \Rightarrow P \quad \vdash \{ P \} C \{ Q \} \]

\[ \vdash \{ P' \} C \{ Q \} \]

**R2: the rule of postcondition weakening.** For any formulae \( P, Q \) and \( Q' \), and command \( C \):

\[ \vdash \{ P \} C \{ Q \} \quad \vdash Q \Rightarrow Q' \]

\[ \vdash \{ P \} C \{ Q' \} \]

Notice that in R1 and R2, one hypothesis is a theorem of ordinary logic whereas the other hypothesis is a theorem of Hoare logic. This shows that proofs in Hoare logic may require subproofs in pure logic; more will be said about the implications of this later.
R3: the sequencing rule. For any formulae $P$, $Q$ and $R$, and commands $C_1$ and $C_2$:  

$$
\frac{\vdash \{P\} C_1 \{Q\} \quad \vdash \{Q\} C_2 \{R\}}{\vdash \{P\} C_1; C_2 \{R\}}$

R4: the IF-rule. For any formulae $P$, $Q$ and $B$, and commands $C_1$ and $C_2$:  

$$
\frac{\vdash \{P \land B\} C_1 \{Q\} \quad \vdash \{P \land \neg B\} C_2 \{Q\}}{\vdash \{P\} \text{ IF } B \text{ THEN } C_1 \text{ ELSE } C_2 \{Q\}}$

Notice that in this rule (and also in R5 below) it is assumed that $B$ is both a boolean expression of the programming language and a formula of predicate logic. We shall only assume that the boolean expressions of the language are a subset of those in predicate logic. This assumption is reasonable since we are the designers of our example language and can design the language so that it is true; it would not be reasonable if we were claiming to provide a logic for reasoning about an existing language like Pascal. One consequence of this assumption is that the semantics of boolean expressions must be the usual logical semantics. We could not, for example, have ‘sequential’ boolean operators in which the boolean expression $T \lor (1/0 = 0)$ evaluates to $T$, but $(1/0 = 0) \lor T$ causes an error (due to division by 0).

R5: the WHILE-rule. For any formulae $P$ and $B$, and command $C$:  

$$
\frac{\vdash \{P \land B\} C \{P\}}{\vdash \{P\} \text{ WHILE } B \text{ DO } C \{P \land \neg B\}}$

A formula $P$ such that $\vdash \{P \land B\} C \{P\}$ is called an invariant of $C$ for $B$.

7.3 Semantics in logic

The traditional denotation of a command $C$ is a function, $\text{Meaning}(C)$ say, from machine states to machine states. The idea is:  

$$
\text{Meaning}(C)(s) = \text{‘the state resulting from executing } C \text{ in state } s\text{’}
$$

Since WHILE-commands need not terminate, the functions denoted by commands will be partial. For example, for any state $s$ and command $C$

$$
\text{Meaning(\text{WHILE } T \text{ DO } C)}(s)
$$

will be undefined. Since functions in conventional predicate calculus are total, we cannot use them as command denotations. Instead we will take the meaning of commands to be predicates on pairs of states $(s_1, s_2)$; the idea being that if $C$ denotes $c$ then:

$$
c(s_1, s_2) \equiv (\text{Meaning}(C)(s_1) = s_2)
$$
### 7.3. Semantics in logic

#### i.e.

\[ c(s_1, s_2) = \begin{cases} 
  T & \text{if executing } C \text{ in state } s_1 \text{ results in state } s_2 \\
  F & \text{otherwise}
\end{cases} \]

If \( c_{\text{WHILE}} \) is the predicate denoted by \( \text{WHILE } T \text{ DO } C \), we will simply have:

\[ \forall s_1 s_2. c_{\text{WHILE}}(s_1, s_2) = F \]

Formally, the type \textit{state} of states that we use is defined by:

\[ \text{state} = \text{string} \to \text{num} \]

The notation ‘\( XYZ \)’ will be used for the string consisting of the three characters \( X, Y \) and \( Z \); thus ‘\( XYZ \)’ : \textit{string}. A state \( s \) in which the strings ‘\( X \)’, ‘\( Y \)’ and ‘\( Z \)’ are bound to 1, 2 and 3 respectively, and all other strings are bound to 0, is defined by:

\[ s = \lambda x. (x = 'X' \to 1 | (x = 'Y' \to 2 | (x = 'Z' \to 3 | 0))) \]

If \( e, b \) and \( c \) are the denotations of \( E, B \) and \( C \) respectively, then:

\[ e : \text{state} \to \text{num} \]
\[ b : \text{state} \to \text{bool} \]
\[ c : \text{state} \times \text{state} \to \text{bool} \]

For example, the denotation of \( X + 1 \) would be \( \lambda s. s'X' + 1 \) and the denotation of \( (X + Y) > 10 \) would be \( \lambda s. (s'X' + s'Y') > 10 \).

It is convenient to introduce the notations \( \llbracket E \rrbracket \) and \( \llbracket B \rrbracket \) for the logic terms representing the denotations of \( E \) and \( B \). For example:

\[ \llbracket X + 1 \rrbracket = \lambda s. s'X' + 1 \]
\[ \llbracket (X + Y) > 10 \rrbracket = \lambda s. (s'X' + s'Y') > 10 \]

Note that \( \llbracket E \rrbracket \) and \( \llbracket B \rrbracket \) are terms, i.e., syntactic objects.

Sometimes it is necessary for pre and postconditions to contain logical variables that are not program variables. An example is:

\[ \{ X = x \land Y = y \} \ Z := X ; \ X := Y ; \ Y := Z \{ X = y \land Y = x \} \]

Here \( x \) and \( y \) are logical variables whereas \( X \) and \( Y \) (and \( Z \)) are program variables. The formulae representing the correct semantics of the pre and post conditions of this specification are:

\[ \llbracket X = x \land Y = y \rrbracket = \lambda s. s'X' = x \land s'Y' = y \]
\[ \llbracket X = y \land Y = x \rrbracket = \lambda s. s'X' = y \land s'Y' = x \]

The convention adopted here is that upper case variables are program variables and lower case variables are logical variables (as in the example just given). In our little programming language the only data type is numbers, hence program variables will have type \textit{num}. The definition of \( \llbracket \cdots \rrbracket \) can now be stated more precisely: if
$T[X_1, \ldots, X_n]$ is a term of higher order logic whose upper case free variables of type \textit{num} are $X_1, \ldots, X_n$ then

$$[[T[X_1, \ldots, X_n]]] = \lambda s. T[s^\prime X_1^\prime, \ldots, s^\prime X_n^\prime]$$

In other words if $T$ is a term of type $\sigma$ then the term $[[T]]$ of type $\text{state} \rightarrow \sigma$ is obtained as follows:

(i) Each free upper case variable $V$ of type $\text{num}$ is replaced by the term $s^\prime V^\prime$, where $s$ is a variable of type $\text{state}$ not occurring in $P$.

(ii) The result of (i) is prefixed by $\lambda s.$.

### 7.3.1 Semantics of commands

To represent the semantics of our little programming language, predicates in higher order logic that correspond to the five kinds of commands are defined. For each command $C$, a term $[[C]]$ of type $\text{state} \times \text{state} \rightarrow \text{bool}$ is defined as follows:

1. $[[\text{SKIP}]] = \text{Skip}$
   where the constant $\text{Skip}$ is defined by:
   $$\text{Skip}(s_1, s_2) = (s_1 = s_2)$$

2. $[[V := E]] = \text{Assign}(V^\prime, [[E]])$
   where the constant $\text{Assign}$ is defined by:
   $$\text{Assign}(v, e)(s_1, s_2) = (s_2 = \text{Bnd}(e, v, s_1))$$
   where:
   $$\text{Bnd}(e, v, s) = \lambda x. (x = v \rightarrow e \ s \mid s \ x)$$

3. $[[C_1; C_2]] = \text{Seq}([[C_1]], [[C_2]])$
   where the constant $\text{Seq}$ is defined by:
   $$\text{Seq}(c_1, c_2)(s_1, s_2) = \exists s. c_1(s_1, s) \land c_2(s, s_2)$$

4. $[[\text{IF } B \text{ THEN } C_1 \text{ ELSE } C_2]] = \text{If}([[B]], [[C_1]], [[C_2]])$
   where the constant $\text{If}$ is defined by:
   $$\text{If}(b, c_1, c_2)(s_1, s_2) = (b \ s_1 \rightarrow c_1(s_1, s_2) \mid c_2(s_1, s_2))$$

5. $[[\text{WHILE } B \text{ DO } C]] = \text{While}([[B]], [[C]])$
   where the constant $\text{While}$ is defined by:
   $$\text{While}(b, c)(s_1, s_2) = \exists n. \text{Iter}(n)(b, c)(s_1, s_2)$$
where $\text{Iter}(n)$ is defined by primitive recursion as follows:

\[
\begin{align*}
\text{Iter}(0)(b, c)(s_1, s_2) &= F \\
\text{Iter}(n+1)(b, c)(s_1, s_2) &= \text{if}(b, \text{Seq}(c, \text{Iter}(n)(b, c)), \text{Skip})(s_1, s_2)
\end{align*}
\]

**Example**

\[
\begin{align*}
R &:= X; \\
Q &:= 0; \\
\text{WHILE} \ Y \leq R \\
\text{DO} \ (R := R - Y; \ Q := Q + 1)
\end{align*}
\]

denotes:

\[
\text{Seq} \\
\text{Seq} \\
\text{Seq}
\]

Expanding the $\cdots$s results in:

\[
\text{Seq} \\
\text{Seq} \\
\text{Seq}
\]

It might appear that by representing the meaning of commands with relations, we can give a semantics to nondeterministic constructs. For example, if $C_1 \parallel C_2$ is the nondeterministic choice ‘either do $C_1$ or do $C_2$’, then one might think that a satisfactory semantics would be given by:

\[
[C_1 \parallel C_2] = \text{Choose}([C_1], [C_2])
\]

where the constant $\text{Choose}$ is defined by:

\[
\text{Choose}(c_1, c_2)(s_1, s_2) = c_1(s_1, s_2) \lor c_2(s_1, s_2)
\]

Unfortunately this semantics has some undesirable properties. For example, if $c_{\text{WHILE}}$ is the predicate denoted by the non-terminating command $\text{WHILE} \ T \ \text{DO} \ \text{SKIP}$, then

\[
\forall s_1 s_2. c_{\text{WHILE}}(s_1, s_2) = F
\]
and hence, because \( \forall t. t \lor F = t \), it follows that:

\[
\text{SKIP} \parallel \text{c\textsubscript{WHILE}} = \text{SKIP}
\]

Thus the command that does nothing is equivalent to a command that \textit{either} does nothing or loops! It is well known how to distinguish guaranteed termination from possible termination [36]; the example above shows that the relational semantics used here does not do it. This problem will appear again in connection with Dijkstra’s theory of weakest preconditions in Section 7.6.2.

7.3.2 Semantics of partial correctness specifications

A partial correctness specification \( \{P\} C \{Q\} \) denotes:

\[
\forall s_1 s_2. [P] s_1 \land [C](s_1, s_2) \Rightarrow [Q] s_2
\]

To abbreviate this formula, define a constant \( \text{Spec} \) by:

\[
\text{Spec}(p, c, q) = \forall s_1 s_2. p s_1 \land c(s_1, s_2) \Rightarrow q s_2
\]

Note that the denotation of pre and postconditions \( P \) and \( Q \) are not just the logical formulae themselves, but are \( [P] \) and \( [Q] \). For example, in the specification \( \{X = 1\} C \{Q\} \), the precondition \( X = 1 \) asserts that the value of the string ‘\( X \)’ in the initial state is 1. The precondition thus denotes \( [P] \), i.e. \( \lambda s. s'X' = 1 \). Thus:

\[
\{X = 1\} X := X + 1 \{X = 2\}
\]

denotes

\[
\text{Spec}([X = 1], \text{Assign}('X', [X + 1]), [X = 2])
\]

i.e.

\[
\text{Spec}((\lambda s. s'X' = 1), \text{Assign}('X', \lambda s. s'X' + 1), \lambda s. s'X' = 2)
\]

Example

In the specification below, \( x \) and \( y \) are logical variables whereas \( X \) and \( Y \) (and \( Z \)) are program variables.

\[
\{X = x \land Y = y\} Z := X; X := Y; Y := Z \{X = y \land Y = x\}
\]

The semantics of this is thus represented by the term:

\[
\text{Spec}([X = x \land Y = y],
\text{Seq}((\text{Assign}('Z', [X]),
\text{Seq}(\text{Assign}('X', [Y]), \text{Assign}('Y', [Z]))),
[X = y \land Y = x])
\]

which abbreviates:

\[
\text{Spec}((\lambda s. s'X' = x \land s'Y' = y),
\text{Seq}((\text{Assign}('Z', \lambda s. s'X'),
\text{Seq}(\text{Assign}('X', \lambda s. s'Y'), \text{Assign}('Y', \lambda s. s'Z'))),
\lambda s. s'X' = y \land s'Y' = x)
\]
7.4 Floyd-Hoare logic as higher order logic

Floyd-Hoare logic can be embedded in higher order logic simply by regarding the concrete syntax given in Section 7.2 as an abbreviation for the corresponding semantic formulae described in Section 7.3. For example:

\{X = x\} X := X + 1 \{X = x + 1\}

can be interpreted as abbreviating:

Spec(\([X = x]\), Assign(\(\cdot X^c; [X + 1]\)), \([X = x + 1]\))

i.e.

Spec((\(\lambda s. s^c X^c = x\)), Assign(\(\cdot X^c, \lambda s. s^c X^c + 1\)), \(\lambda s. s^c X^c = x + 1\))

The translation between the syntactic ‘surface structure’ and the semantic ‘deep structure’ is straightforward; it can easily be mechanized with a simple parser and pretty-printer.

If partial correctness specifications are interpreted this way then, as shown in the rest of this section, the axioms and rules of Hoare logic become derived rules of higher order logic.

The first step in this derivation is to prove the following seven theorems from the definitions of the constants Spec, Skip, Assign, Bnd, Seq, If, While and Iter.

H1. \(\vdash \forall p. \text{Spec}(p, \text{Skip}, p)\)

H2. \(\vdash \forall p v e. \text{Spec}(\(\lambda s. p(Bnd(e, v, s))\), Assign(v, e), p)\)

H3. \(\vdash \forall p p' q c. (\forall s. p' s \Rightarrow p s) \land \text{Spec}(p, c, q) \Rightarrow \text{Spec}(p', c, q)\)

H4. \(\vdash \forall p q q' c. \text{Spec}(p, c, q) \land (\forall s. q s \Rightarrow q' s) \Rightarrow \text{Spec}(p, c, q')\)

H5. \(\vdash \forall p q r c_1 c_2. \text{Spec}(p, c_1, q) \land \text{Spec}(q, c_2, r) \Rightarrow \text{Spec}(p, \text{Seq}(c_1, c_2), r)\)

H6. \(\vdash \forall p q c_1 c_2 b. \text{Spec}((\lambda s. p s \land b s), c_1, q) \land \text{Spec}((\lambda s. p s \land \neg(b s)), c_2, q) \Rightarrow \text{Spec}(p, \text{If}(b, c_1, c_2), q)\)

H7. \(\vdash \forall p c b. \text{Spec}((\lambda s. p s \land b s), c, p) \Rightarrow \text{Spec}(p, \text{While}(b, c), (\lambda s. p s \land \neg(b s)))\)

The proofs of H1 to H7 are rather tedious (and are omitted). All the axioms and rules of Hoare logic, except for the assignment axiom, can be implemented in a uniform way from H1 – H7. The derivation of the assignment axiom from H2, although straightforward, is a bit messy; it is thus explained last (in Section 7.4.7).
7.4.1 Derivation of the SKIP-axiom

To derive the SKIP-axiom it must be shown for arbitrary $P$ that:

$$\vdash \{P\} \text{SKIP} \{P\}$$

which abbreviates:

$$\vdash \text{Spec}([P], \text{Skip}, [P])$$

This follows by specializing $p$ to $[P]$ in H1.

7.4.2 Derivation of precondition strengthening

To derive the rule of precondition strengthening it must be shown that for arbitrary $P, P', C$ and $Q$ that:

$$\vdash P' \Rightarrow P \quad \vdash \{P\} \ C \ \{Q\}$$

Expanding abbreviations converts this to:

$$\vdash P' \Rightarrow P \quad \vdash \text{Spec}([P], [C], [Q])$$

$$\vdash \text{Spec}([P'], [C], [Q])$$

Specializing H3 yields:

$$\vdash (\forall s. [P'] s \Rightarrow [P] s) \land \text{Spec}([P], [C], [Q]) \Rightarrow \text{Spec}([P'], [C], [Q])$$

The rule of precondition strengthening will follow if $\vdash \forall s. [P'] s \Rightarrow [P] s$ can be deduced from $\vdash P' \Rightarrow P$. To see that this is indeed the case, let us make explicit the program variables $X_1, \ldots, X_n$ occurring in $P$ and $P'$ by writing $P[X_1, \ldots, X_n]$ and $P'[X_1, \ldots, X_n]$. Then $\vdash P' \Rightarrow P$ becomes

$$\vdash P'[X_1, \ldots, X_n] \Rightarrow P[X_1, \ldots, X_n]$$

Since $X_1, \ldots, X_n$ are free variables in this theorem, they are implicitly universally quantified, and hence each $X_i$ can be instantiated to $s^i X_i$ to get:

$$\vdash P'[s^i X_1, \ldots, s^i X_n] \Rightarrow P[s^i X_1, \ldots, s^i X_n]$$

Generalizing on the free variable $s$ yields:

$$\vdash \forall s. P'[s^i X_1, \ldots, s^i X_n] \Rightarrow P[s^i X_1, \ldots, s^i X_n]$$

which is equivalent (by $\beta$-reduction) to

$$\vdash \forall s. (\lambda s. P'[s^i X_1, \ldots, s^i X_n]) s \Rightarrow (\lambda s. P[s^i X_1, \ldots, s^i X_n]) s$$

i.e.

$$\vdash \forall s. [P'[X_1, \ldots, X_n]] s \Rightarrow [P[X_1, \ldots, X_n]] s$$
7.4.3 Derivation of postcondition weakening

To derive the rule of postcondition weakening, it must be shown that for arbitrary \( P, C \), and \( Q \) and \( Q' \) that:

\[
\vdash \{ P \} C \{ Q \} \quad \vdash Q \Rightarrow Q'
\]

The derivation of this from H4 is similar to the derivation of precondition strengthening from H3.

7.4.4 Derivation of the sequencing rule

To derive the sequencing rule, it must be shown that for arbitrary \( P, C_1, R, C_2 \) and \( Q \) that:

\[
\vdash \{ P \} C_1 \{ Q \} \quad \vdash \{ Q \} C_2 \{ R \}
\]

\[
\vdash \{ P \} C_1 ; C_2 \{ R \}
\]

Expanding the abbreviations yields:

\[
\vdash \text{Spec}([P], [C_1], [Q]) \quad \vdash \text{Spec}([Q], [C_2], [R])
\]

\[
\vdash \text{Spec}([P], \text{Seq}([C_1], [C_2]), [R])
\]

The validity of this rule follows directly from H5.

7.4.5 Derivation of the IF-rule

To derive the IF-rule, it must be shown that for arbitrary \( P, B, C_1, C_2 \) and \( Q \) that:

\[
\vdash \{ P \land B \} C_1 \{ Q \} \quad \vdash \{ P \land \neg B \} C_2 \{ Q \}
\]

\[
\vdash \{ P \} \text{IF } B \text{ THEN } C_1 \text{ ELSE } C_2 \{ Q \}
\]

Expanding abbreviations yields:

\[
\vdash \text{Spec}([P \land B], [C_1], [Q]) \quad \vdash \text{Spec}([P \land \neg B], [C_2], [Q])
\]

\[
\vdash \text{Spec}([P], \text{If}(B, C_1, C_2), [Q])
\]

This follows from H6 in a similar fashion to the way precondition strengthening follows from H3.

7.4.6 Derivation of the WHILE-rule

To derive the WHILE-rule, it must be shown that for arbitrary \( P, B \) and \( C \) that:

\[
\vdash \{ P \land B \} C \{ P \}
\]

\[
\vdash \{ P \} \text{WHILE } B \text{ DO } C \{ P \land \neg B \}
\]

Expanding abbreviations yields:

\[
\vdash \text{Spec}([P \land B], [C], [P])
\]

\[
\vdash \text{Spec}([P], \text{While}(B, C), [P \land \neg B])
\]

This follows from H7.
7.4.7 Derivation of the assignment axiom

To derive the assignment axiom, it must be shown that for arbitrary $P$, $E$ and $V$:

$$\vdash \{ P[E/V] \} \ V := E \{ P \}$$

This abbreviates:

$$\vdash \text{Spec}([P[E/V]], \text{Assign}(V, [E]), [P])$$

By H2:

$$\vdash \forall x e. \text{Spec}((\lambda s. \, p(\text{Bnd}(e, s, x, s))), \text{Assign}(x, e), p)$$

Specializing $p$, $x$ and $e$ to $[P]$, $V$ and $[E]$ yields:

$$\vdash \text{Spec}((\lambda s. \, [P](\text{Bnd}([E]s, V, s))), \text{Assign}(V, [E]), [P])$$

Thus, to derive the assignment axiom it must be shown that:

$$\vdash [P[E/V]] = \lambda s. \, [P](\text{Bnd}([E]s, V, s))$$

To see why this holds, let us make explicit the free program variables in $P$ and $E$ by writing $P[V, X_1, \ldots, X_n]$ and $E[V, X_1, \ldots, X_n]$, where $X_1, \ldots, X_n$ are the free program variables that are not equal to $V$. Then, for example, $P[1, \ldots, n]$ would denote the result of substituting $1, \ldots, n$ for $X_1, \ldots, X_n$ in $P$ respectively. The equation above thus becomes:

$$[P[V, X_1, \ldots, X_n][E[V, X_1, \ldots, X_n]/V]] = \lambda s. \, [P[V, X_1, \ldots, X_n]](\text{Bnd}([E[V, X_1, \ldots, X_n]]s, V, s))$$

Performing the substitution in the left hand side yields:

$$[P[E[V, X_1, \ldots, X_n], X_1, \ldots, X_n]] = \lambda s. \, [P[V, X_1, \ldots, X_n]](\text{Bnd}([E[V, X_1, \ldots, X_n]]s, V, s))$$

Replacing expressions of the form $[P[\cdots]]$ by their meaning yields:

$$\lambda s. \, P[E[s'V, s'X_1\ldots, s'X_n], s'X_1\ldots, s'X_n'] = \lambda s. \, P[s'V, s'X_1\ldots, s'X_n'](\text{Bnd}([E[V, X_1, \ldots, X_n]]s, V, s))$$

Performing a $\beta$-reduction on the right hand side, and then simplifying with the following easily derived properties of $\text{Bnd}$ (the second of which assumes $V \neq X_i$):

$$\vdash \text{Bnd}([E[V, X_1, \ldots, X_n]]s, V, s) \equiv [E[V, X_1, \ldots, X_n]]s$$

$$\vdash \text{Bnd}([E[V, X_1, \ldots, X_n]]s, V, s) \equiv s \ X_i$$

results in:

$$\lambda s. \, P[E[s'V, s'X_1\ldots, s'X_n'], s'X_1\ldots, s'X_n'] = \lambda s. \, P[[E[V, X_1, \ldots, X_n]]s, s'X_1\ldots, s'X_n']$$
which is true since:

\[[E[V, X_1, \ldots, X_n]]s = E[s'V', s'X_1', \ldots, s'X_n']\]

Although this derivation might appear tricky at first sight, it is straightforward and easily mechanized.

It is tempting to try to formulate the assignment axiom as a theorem of higher order logic looking something like:

\[\forall p e v. \text{Spec}(p[e/v], \text{Assign}(v, e, p))\]

Unfortunately, the expression \(p[e/v]\) does not make sense when \(p\) is a variable. \(P[E/V]\) is a meta notation and consequently the assignment axiom can only be stated as a meta theorem. This elementary point is nevertheless quite subtle. In order to prove the assignment axiom as a theorem within higher order logic it would be necessary to have types in the logic corresponding to formulae, variables and terms. One could then prove something like:

\[\forall P E V. \text{Spec} (\text{Truth(Subst(P, E, V))}, \text{Assign(V, Value E)}, \text{Truth P})\]

It is clear that working out the details of this would be lots of work. This sort of embedding of a subset of a logic within itself has been explored in the context of the Boyer-Moore theorem prover [6].

### 7.5 Termination and total correctness

Hoare logic is usually presented as a self-contained calculus. However, if it is regarded as a derived logic, as it is here, then it’s easy to add extensions and modifications without fear of introducing unsoundness. To illustrate this, we will sketch how termination assertions can be added, and how these can be used to prove total correctness.

A **termination assertion** is a formula \(\text{Halts}([P], [C])\), where the constant \(\text{Halts}\) is defined by:

\[\text{Halts}(p, c) = \forall s_1. p s_1 \Rightarrow \exists s_2. c(s_1, s_2)\]

Notice that this says that \(c\) ‘halts’ under precondition \(p\) if there is some final state for each initial state satisfying \(p\). For example, although \(\text{WHILE T DO SKIP}\) does not terminate, the definition above suggests that \((\text{WHILE T DO SKIP}) \parallel \text{SKIP}\) does, since:

\[\vdash \text{Halts}([T], \text{Choose}([\text{WHILE T DO SKIP}], [\text{SKIP}]))\]

(\(\parallel\) and \text{Choose} are described in Section 7.3). The meaning of \(\text{Halts}([P], [C])\) is ‘some computation of \(C\) starting from a state satisfying \(P\) terminates’ this is quite different from ‘every computation of \(C\) starting from a state satisfying \(P\) terminates’. The latter stronger kind of termination requires a more complex kind of semantics for its
formalization (e.g. one using powerdomains [36]). If commands are deterministic, then termination is adequately formalized by $\text{Halts}$. It is intuitively clear that the relations denoted by commands in our little language (*not including $\parallel$*) are partial functions. If $\text{Det}$ is defined by:

$$\text{Det } c = \forall s s_1 s_2. c(s, s_1) \land c(s, s_2) \Rightarrow (s_1 = s_2)$$

then for any command $C$ it can be proved that $\vdash \text{Det } [C]$. This fact will be needed to show that the formalization of weakest preconditions in Section 7.6.2 is correct.

The informal equation

$$\text{Total correctness} = \text{Termination} + \text{Partial correctness.}$$

can be implemented by defining:

$$\text{Total}_\text{Spec}(p, c, q) = \text{Halts}(p, c) \land \text{Spec}(p, c, q)$$

Then $[P] C [Q]$ is represented by $\text{Total}_\text{Spec}([P], [C], [Q])$.

From the definition of $\text{Halts}$ it is straightforward to prove the following theorems:

T1. $\vdash \forall p. \text{Halts}(p, \text{Skip})$

T2. $\vdash \forall p v e. \text{Halts}(p, \text{Assign}(v, e))$

T3. $\vdash \forall p p' c. (\forall s. p' s \Rightarrow p s) \land \text{Halts}(p, c) \Rightarrow \text{Halts}(p', c)$

T4. $\vdash \forall p c_1 c_2 q. \text{Halts}(p, c_1) \land \text{Spec}(p, c_1, q) \land \text{Halts}(q, c_2) \Rightarrow \text{Halts}(p, \text{Seq}(c_1, c_2))$

T5. $\vdash \forall p c_1 c_2 b. \text{Halts}(p, c_1) \land \text{Halts}(p, c_2) \Rightarrow \text{Halts}(p, \text{If}(b, c_1, c_2))$

T6. $\vdash \forall p b c x. (\forall n. \text{Spec}((\lambda s. p s \land b s \land (s x = n)), c, (\lambda s. p s \land s x < n))) \land \text{Halts}((\lambda s. p s \land b s), c) \Rightarrow \text{Halts}(p, \text{While}(b, c))$

T6 shows that if $x$ is a *variant*, i.e. a variable whose value decreases each time ‘around the loop’ ($n$ is assumed to be of natural number type, i.e. $n \geq 0$), then the $\text{WHILE}$-command halts.

### 7.5.1 Derived rules for total correctness

Using T1 – T6 above and H1 – H7 of Section 7.4, it is straightforward to apply the methods described in Section 7.4 to implement the derived rules for total correctness shown below. These are identical to the corresponding rules for partial correctness except for having ‘[’ and ‘]’ instead of ‘{’ and ‘}’ respectively.

$$\vdash [P] \text{SKIP } [P]$$

$$\vdash P' \Rightarrow P \vdash [P] C [Q]$$

$$\vdash [P'] C [Q]$$
7.6. Other programming logic constructs

The total correctness rule for \texttt{WHILE}-commands needs a stronger hypothesis than the corresponding one for partial correctness. This is to ensure that the command terminates. For this purpose, a variant is needed in addition to an invariant.

\[
\vdash [P \land B \land (N = n)] C [P \land (N < n)]
\]

\[
\vdash [P] \text{WHILE } B \text{ DO } C [P \land \neg B]
\]

Notice that since

\[
\text{Total} \_{\text{Spec}}(p, c, q) = \text{Halts}(p, c) \land \text{Spec}(p, c, q)
\]

it is clear that the following rule is valid

\[
\vdash [P] C [Q]
\]

The converse to this is only valid if \( C \) contains no \texttt{WHILE}-commands. We thus have the derived rule:

\[
\vdash \{P\} C \{Q\}
\]

if \( C \) contains no \texttt{WHILE}-commands.

7.6 Other programming logic constructs

In this section, three variants on Hoare logic are described.

(i) VDM-style specifications.

(ii) Weakest preconditions.

(iii) Dynamic logic.

7.6.1 VDM-style specifications

The Vienna Development Method (VDM) \cite{VDM}) is a formal method for program development which uses a variation on Hoare-style specifications. The VDM notation reduces the need for auxiliary logical variables by providing a way of referring to the initial values of variables in postconditions. For example, the following Hoare-style partial correctness specification:

\[
\{X = x \land Y = y\} R := X; \ X := Y; \ Y := R \{Y = x \land X = y\}
\]
could be written in a VDM-style as:

\{ T \} \ R := X \ ; \ X := Y \ ; \ Y := R \ \{ Y = \overleftarrow{X} \ \land \ X = \overleftarrow{Y} \}

where \overleftarrow{X} and \overleftarrow{Y} denote the values X and Y had before the three assignments were executed. More generally,

\{ P[X_1, \ldots, X_n] \} \ C \ \{ Q[X_1, \ldots, X_n, \overleftarrow{X_1}, \ldots, \overleftarrow{X_n}] \}

can be thought of as an abbreviation for

\{ P[X_1, \ldots, X_n] \ \land \ X_1 = \overleftarrow{X_1} \ \land \ \ldots \ \land \ X_n = \overleftarrow{X_n} \} \\
C \\
{ Q[X_1, \ldots, X_n, \overleftarrow{X_1}, \ldots, \overleftarrow{X_n}] } \\

where \overleftarrow{X_1}, \ldots, \overleftarrow{X_n} are distinct logical variables not occurring in \ C.

Although the meaning of individual VDM specifications is clear, it is not so easy to see what the correct Hoare-like rules of inference are. For example, the sequencing rule must somehow support the deduction of

\{ T \} \ X := X + 1 ; \ X := X + 1 \ \{ X = \overleftarrow{X} + 2 \}

from

\{ T \} \ X := X + 1 \ \{ X = \overleftarrow{X} + 1 \}

There is another semantics of VDM specifications, which Jones attributes to Peter Aczel [24]. This semantics avoids the need for hidden logical variables and also makes it easy to see what the correct rules of inference are. The idea is to regard the postcondition as a binary relation on the initial and final states. This can be formalized by regarding

\{ P[X_1, \ldots, X_n] \} \ C \ \{ Q[X_1, \ldots, X_n, \overleftarrow{X_1}, \ldots, \overleftarrow{X_n}] \}

as an abbreviation for

\text{VDM\_Spec}([P[X_1, \ldots, X_n]], [C], [Q[X_1, \ldots, X_n, \overleftarrow{X_1}, \ldots, \overleftarrow{X_n}]]_2) \\

where \text{VDM\_Spec} is defined by:

\text{VDM\_Spec}(p, c, r) = \forall s_1 \ s_2. \ p \ s_1 \ \land \ c(s_1, s_2) \ \Rightarrow \ r(s_1, s_2)

and the notation \([ \ldots ]_2\) is defined by:

\[ Q[X_1, \ldots, X_n, \overleftarrow{X_1}, \ldots, \overleftarrow{X_n}]_2 = \lambda(s_1, s_2). \ Q[s_2^{X_1}, \ldots, s_2^{X_n}, s_1^{X_1}, \ldots, s_1^{X_n}] \]

The sequencing rule now corresponds to the theorem:
7.6. Other programming logic constructs

\[ \vdash \forall p_1 \ p_2 \ r_1 \ r_2 \ c_1 \ c_2. \]
\[ \text{VDM\_Spec}(p_1, \ c_1, \ \lambda(s_1, s_2). \ p_2 \ s_2 \land r_1(s_1, s_2)) \land \]
\[ \text{VDM\_Spec}(p_2, \ c_2, \ r_2) \Rightarrow \]
\[ \text{VDM\_Spec}(p_1, \ \text{Seq}(c_1, c_2), \ \text{Seq}(r_1, r_2)) \]

Example

If \( \{ T \} \ X := X + 1 \ {\{ X = \overset{\rightarrow}{X} + 1 \}} \) is interpreted as:
\[ \text{VDM\_Spec}([T], \ [X := X + 1], \ [X = \overset{\rightarrow}{X} + 1]_2) \]
which (since \( \vdash \forall x. \ T \land x = x \)) implies:
\[ \text{VDM\_Spec}([T], \ [X := X + 1], \ \lambda(s_1, s_2). \ [T] s_2 \land [X = \overset{\rightarrow}{X} + 1]_2(s_1, s_2) \]
and hence it follows by the sequencing theorem above that:
\[ \text{VDM\_Spec}([T], \ [X := X + 1; \ X := X + 1], \ \text{Seq}([X = \overset{\rightarrow}{X} + 1]_2, \ [X = \overset{\rightarrow}{X} + 1]_2)) \]

By the definition of \text{Seq} in Section 7.3:
\[ \text{Seq}([X = \overset{\rightarrow}{X} + 1]_2, \ [X = \overset{\rightarrow}{X} + 1]_2)(s_1, s_2) \]
\[ = \exists s. \ [X = \overset{\rightarrow}{X} + 1]_2(s_1, s) \land [X = \overset{\rightarrow}{X} + 1]_2(s, s_2) \]
\[ = \exists s. (\lambda(s_1, s_2). \ s_2 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 1)(s_1, s) \land (\lambda(s_1, s_2). \ s_2 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 1)(s_2, s_2) \]
\[ = \exists s. (s_1 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 1) \land (s_2 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 1) \]
\[ = \exists s. (s_1 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 1) \land (s_2 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 2) \]
\[ = \exists s. s_1 \overset{\rightarrow}{X}^i + 1) \land (s_2 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 2) \]
\[ = T \land (s_2 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 2) \]
\[ = (s_2 \overset{\rightarrow}{X}^i = s_1 \overset{\rightarrow}{X}^i + 2) \]
\[ = [X = \overset{\rightarrow}{X} + 1]_2(s_1, s_2) \]

Hence:

\[ \vdash \{ T \} \ X := X + 1; \ X := X + 1 \ {\{ X = \overset{\rightarrow}{X} + 2 \}} \]

\( \square \)

An elegant application of treating postconditions as binary relations is Aczel's version of the \text{WHILE}-rule [24]:

\[ \vdash \{ P \land B \} C \{ P \land R \} \]
\[ \vdash \{ P \} \text{WHILE} B \text{DO} C \{ P \land \lnot B \land R^* \} \]

Where \( R^* \) is the reflexive closure of \( R \) defined by
\[ R^*(s_1, s_2) = \exists n. \ R^n(s_1, s_2) \]

and \( R^n \) is definable in higher order logic by the following primitive recursion:
\[ R^0 = \lambda(s_1, s_2). \ (s_1 = s_2) \]
\[ R^{n+1} = \text{Seq}(R, R^n) \]

Aczel pointed out that his version of the \text{WHILE}-rule can be converted into a rule of total correctness simply by requiring \( R \) to be transitive and well-founded:
114 Chapter 7. Deriving Floyd-Hoare Logic

\[\frac{\vdash [P \land B] \ C \ [P \land R]}{\vdash \ Transitive \ R} \frac{\vdash \ Well\_Founded \ R}{\vdash [P] \ WHILE \ B \ DO \ C \ [P \land \neg B \land R']}
\]

where:

Transitive \( r = \forall s_1 \ s_2 \ s_3. \ r(s_1, s_2) \land r(s_2, s_3) \Rightarrow r(s_1, s_3) \)

Well\_Founded \( r = \neg \exists f : \text{num} \rightarrow \text{state}. \ \forall n. \ r(f(n), f(n+1)) \)

Notice how it is straightforward to define notions like Transitive and Well\_Founded in higher order logic; these cannot be defined in first order logic.

7.6.2 Dijkstra’s weakest preconditions

Dijkstra’s theory of weakest preconditions, like VDM, is primarily a theory of rigorous program construction rather than a theory of post hoc verification. As will be shown, it is straightforward to define weakest preconditions for deterministic programs in higher order logic\(^2\).

In his book [10], Dijkstra introduced both ‘weakest liberal preconditions’ (wlp) and ‘weakest preconditions’ (wp); the former for partial correctness and the latter for total correctness. The idea is that if \( C \) is a command and \( Q \) a predicate, then:

- \( \text{wlp}(C, Q) = 'The weakest predicate \( P \) such that \( \{P\}Q\{Q\}' \)
- \( \text{wp}(C, Q) = 'The weakest predicate \( P \) such that \([P]\ Q\ [Q]\)' \)

Before defining these notions formally, it is necessary to first define the general notion of the ‘weakest predicate’ satisfying a condition. If \( p \) and \( q \) are predicates on states (i.e. have type \( \text{state} \rightarrow \text{bool} \)), then define \( p \leftarrow q \) to mean \( p \) is weaker (i.e. ‘less constraining’) than \( q \), in the sense that everything satisfying \( q \) also satisfies \( p \). Formally:

\[p \leftarrow q = \forall s. \ q s \Rightarrow p s\]

The weakest predicate satisfying a condition can be given a general definition using Hilbert’s \( \varepsilon \)-operator.

\[\text{Weakest} \ P = \varepsilon p. \ P \ p \land \forall p'. \ P \ p' \Rightarrow (p \leftarrow p')\]

Dijkstra’s two kinds of weakest preconditions can be defined by:

\[\text{wlp}(c, q) = \text{Weakest}(\lambda p. \ \text{Spec}(p, c, q))\]
\[\text{wp}(c, q) = \text{Weakest}(\lambda p. \ \text{Total\_Spec}(p, c, q))\]

These definitions seem to formalize the intuitive notions described by Dijkstra, but are cumbersome to work with. The theorems shown below are easy consequences of the definitions above, and are much more convenient to use in formal proofs.

\(^2\)Dijkstra’s semantics of nondeterministic programs can also be formalized in higher order logic, but not using the simple methods described in this paper (see the end of Section 7.3.1).
\[ \vdash \text{wlp}(c, q) = \lambda s. \forall s'. \ c(s, s') \Rightarrow q' \]
\[ \vdash \text{wp}(c, q) = \lambda s. (\exists s'. \ c(s, s')) \land \forall s'. \ c(s, s') \Rightarrow q' \]

The relationship between Hoare’s notation and weakest preconditions is given by:

\[ \vdash \text{Spec}(p, c, q) = \forall s. \ p \ s \Rightarrow \text{wlp}(c, q) \ s \]
\[ \vdash \text{Total} \text{Spec}(p, c, q) = \forall s. \ p \ s \Rightarrow \text{wp}(c, q) \ s \]

The statement of the last two theorems, as well as other results below, can be improved if ‘big’ versions of the logical operators \( \land, \lor, \Rightarrow \) and constants \( \top, \bot \) are introduced which are ‘lifted’ to predicates. These are defined in the table below, together with the operator \( \models \) which tests whether a predicate is always true. These lifted predicates will also be useful in connection with dynamic logic.

<table>
<thead>
<tr>
<th>Operators on predicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p \land q ) = ( \lambda s. \ p \ s \land q \ s )</td>
</tr>
<tr>
<td>( p \lor q ) = ( \lambda s. \ p \ s \lor q \ s )</td>
</tr>
<tr>
<td>( p \Rightarrow q ) = ( \lambda s. \ p \ s \Rightarrow q \ s )</td>
</tr>
<tr>
<td>( \lnot p ) = ( \lambda s. \ \lnot p \ s )</td>
</tr>
<tr>
<td>( \top ) = ( \lambda s. \ \top )</td>
</tr>
<tr>
<td>( \bot ) = ( \lambda s. \ \bot )</td>
</tr>
<tr>
<td>( \models p ) = ( \forall s. \ p \ s )</td>
</tr>
</tbody>
</table>

The last two theorems can now be reformulated more elegantly as:

\[ \vdash \text{Spec}(p, c, q) = \models p \Rightarrow \text{wlp}(c, q) \]
\[ \vdash \text{Total} \text{Spec}(p, c, q) = \models p \Rightarrow \text{wp}(c, q) \]

In Dijkstra’s book, various properties of weakest preconditions are stated as axioms, for example:

**Property 1.** \( \vdash \forall c. \models \text{wp}(c, \bot) = \bot \)

**Property 2.** \( \vdash \forall q r c. \models (q \Rightarrow r) \Rightarrow (\text{wp}(c, q) \Rightarrow \text{wp}(c, r)) \)

**Property 3.** \( \vdash \forall q r c. \models \text{wp}(c, q) \land \text{wp}(c, r) = \text{wp}(c, q \land r) \)

**Property 4.** \( \vdash \forall q r c. \models \text{wp}(c, q) \lor \text{wp}(c, r) \Rightarrow \text{wp}(c, q \lor r) \)

**Property 4’.** \( \vdash \forall q r c. \text{Det } c \Rightarrow \models \text{wp}(c, q) \lor \text{wp}(c, r) = \text{wp}(c, q \lor r) \)
These all follow easily from the definition of \( \text{wp} \) given above (\( \text{Det} \) is the determinacy predicate defined in Section 7.5). It is also straightforward to derive analogous properties of weakest liberal preconditions:

\[
\begin{align*}
\vdash \forall c. \ | = \ wp(c, F) = \lambda s. \neg \exists s'. c(s, s') \\
\vdash \forall q r c. \ | = (q \Rightarrow r) \Rightarrow (wp(c, q) \Rightarrow wp(c, r)) \\
\vdash \forall q r c. \ | = wp(c, q) \land wp(c, r) = wp(c, q \land r) \\
\vdash \forall q r c. \ | = wp(c, q) \lor wp(c, r) = wp(c, q \lor r) \\
\vdash \forall q r c. \ Det c \Rightarrow | = wp(c, q) \lor wp(c, r) = wp(c, q \lor r)
\end{align*}
\]

Many of the properties of programming constructs given in Dijkstra’s book [10] are straightforward to verify for the constructs of our little language. For example:

\[
\begin{align*}
\vdash wp([\text{SKIP}], q) = q \\
\vdash wp([\text{SKIP}], q) = q \\
\vdash wp([V := E], q) = \lambda s. q(Bnd([E]s) \ 'V' s) \\
\vdash wp([V := E], q) = \lambda s. q(Bnd([E]s) \ 'V' s) \\
\vdash wp([\text{IF } B \text{ THEN } C_1 \text{ ELSE } C_2], q) = \lambda s. ([B]s \rightarrow wp([C_1], q)s \ | wp([C_2], q)s) \\
\vdash wp([\text{IF } B \text{ THEN } C_1 \text{ ELSE } C_2], q) = \lambda s. ([B]s \rightarrow wp([C_1], q)s \ | wp([C_2], q)s)
\end{align*}
\]

The inadequacy of the relational model reveals itself when we try to derive Dijkstra’s \( \text{wp} \)-law for sequences. This law is:

\[
wp([C_1 ; C_2], q) = wp([C_1], wp([C_2], q))
\]

which is not true with our semantics. For example, taking:

\[
\begin{align*}
s_1 &= \lambda x. 0 \\
s_2 &= \lambda x. 1 \\
c_1(s_1, s_2) &= (s_1 = s_1) \lor (s_2 = s_2) \\
c_2(s_1, s_2) &= (s_1 = s_1) \land (s_2 = s_2)
\end{align*}
\]

results in:

\[
wp(\text{Seq}(c_1, c_2), T) = T
\]

but

\[
wp(c_1, wp(c_2, T)) = F
\]

The best that can be proved using the relational semantics is the following:
As discussed in Section 7.3.1, the problem lies in the definition of Halts. For partial correctness there is no problem; the following sequencing law for weakest liberal preconditions can be proved from the relational semantics.

\[ \vdash \text{Det } [C_1] \Rightarrow \wp([C_1; C_2], q) = \wp([C_1], \wp([C_2], q)) \]

With relational semantics, the wp-law for WHILE-commands also requires a determinacy assumption:

\[ \vdash \text{Det } c \Rightarrow \wp([\text{WHILE } B \text{ DO } C], q) s = \exists n. \text{Iter}_w p n [B] [C] q s \]

where

\[
\begin{align*}
\text{iter}_w p 0 b c q & = \neg b \land q \\
\text{iter}_w p (n+1) b c q & = b \land \wp(c, \text{iter}_w p n b c q)
\end{align*}
\]

However, the wlp-law for WHILE-commands does not require a determinacy assumption:

\[ \vdash \text{wlp}([\text{WHILE } B \text{ DO } C], q) s = \forall n. \text{Iter}_w l p n [B] [C] q s \]

where

\[
\begin{align*}
\text{iter}_l w p 0 b c q & = \neg b \Rightarrow q \\
\text{iter}_l w p (n+1) b c q & = b \Rightarrow \text{wlp}(c, \text{iter}_w l p n b c q)
\end{align*}
\]

### 7.6.3 Dynamic logic

Dynamic logic is a programming logic which emphasizes an analogy between Hoare logic and modal logic; it was invented by V.R. Pratt based on an idea of R.C. Moore [37, 14]. In dynamic logic, states of computation are thought of as possible worlds, and if a command \( C \) transforms an initial state \( s \) to a final state \( s' \) then \( s' \) is thought of as accessible from \( s \) (the preceding phrases in italics are standard concepts from modal logic).

Modal logic is characterized by having formulae \( \Box q \) and \( \Diamond q \) with the following interpretations.

- \( \Box q \) is true in \( s \) if \( q \) is true in all states accessible from \( s \).
- \( \Diamond q \) is true in \( s \) if \( \neg \Box \neg q \) is true in \( s \).

Instead of a single \( \Box \) and \( \Diamond \), dynamic logic has operators \([C]\) and \(<C>\) for each command \( C \). These can be defined on the relation \( c \) denoted by \( C \) as follows:

\[
\begin{align*}
[c] q & = \lambda s. \forall s'. c(s, s') \Rightarrow q s' \\
<c> q & = \neg([c] (\neg q))
\end{align*}
\]
where \( \neg \) is negation lifted to predicates (see preceding section).

A typical theorem of dynamic logic is:

\[
\vdash \forall c, q. \text{Det } c \Rightarrow [\langle c \rangle q] = [c]q
\]

This is a version of the modal logic principle that says that if the accessibility relation is functional then \( \Diamond q \Rightarrow \Box q \) [14].

From the definitions of \([c]q\) and \(\langle c \rangle q\) it can be easily deduced that:

\[
\vdash (\models [c]q) = \text{Spec}(T, c, q)
\]

\[
\vdash \text{Det } c \Rightarrow ([\langle c \rangle q] = \text{Total Spec}(T, c, q))
\]

\[
\vdash \text{Spec}(p, c, q) = (\models p \Rightarrow [c]q)
\]

\[
\vdash \text{Det } c \Rightarrow (\text{Total Spec}(p, c, q) = (\models p \Rightarrow \langle c \rangle q))
\]

Where \(\models, \Rightarrow\) and \(T\) were defined in the preceding section. Using these relationships, theorems of dynamic logic can be converted to theorems of Hoare logic (and vice versa).

Dynamic logic is closely related to weakest preconditions as follows:

\[
\vdash \text{wp}(c, q) = [c]q
\]

\[
\vdash \text{Det } c \Rightarrow (\text{wp}(c, q) = \langle c \rangle q)
\]

These theorems can be used to translate results from one system to the other.
Bibliography


