Grassroots Series

David Lightfoot

Formal Specification Using Z

Contents

	Preface to the Second Edition	xi
Chapter 1	**Introduction**	**1**
1.1	Who this book is for	1
1.2	The need for formal specification	1
1.3	The role of mathematics	2
1.4	Current use of mathematics	3
1.5	The specification language Z	4
1.6	Textual aspects of the Z notation	4
	Exercises	5
Chapter 2	**Sets**	**7**
2.1	Types	7
2.2	The built-in type Integer	7
2.3	Basic types	9
2.4	Free types	9
2.5	Declaring variables	9
2.6	Single value from a type	10
2.7	Set values	10
2.8	The empty set	10
2.9	Singleton set	11
2.10	Ranges of integers	11
2.11	Operators	11
2.12	Disjoint sets	17
2.13	Partition	18
2.14	Summary of notation	18
	Exercises	19
Chapter 3	**Using sets to describe a system – a simple example**	**21**
3.1	Introduction	21
3.2	State-based approach	21
3.3	The state	22
3.4	Initialisation operation	22
3.5	Operations	22
3.6	Enquiries	24

3.7	Conclusion	25
	Exercises	25
Chapter 4	**Logic**	**27**
4.1	Introduction	27
4.2	Propositional calculus	27
4.3	Operators	27
4.4	De Morgan's laws	29
4.5	Demonstrating laws	29
4.6	Using laws	30
4.7	Example proof – exclusive-or	30
4.8	Laws about logical operators	31
4.9	Summary of notation	32
	Exercises	32
Chapter 5	**The example extended**	**35**
5.1	Full definition of boarding operation	35
5.2	A better way	36
	Exercises	36
Chapter 6	**Schemas**	**37**
6.1	Schemas	37
6.2	Schema calculus	39
6.3	Decoration of input and output variables	42
6.4	Simple example of schema with input and output	42
6.5	Example of schemas with input	42
6.6	Further operations on schemas	47
6.7	Overall structure of a Z specification document	49
6.8	Summary of notation	50
	Exercises	52
Chapter 7	**Examples of Z specification documents**	**55**
7.1	Introduction	55
7.2	The types	55
7.3	The state	55
7.4	Initialisation operation	56
7.5	Operations	56
7.6	Enquiry operations	57
7.7	Dealing with errors	58
7.8	Example of schemas: Student Programme of Modules	59
	Exercises	63

Chapter 8 Predicates and quantifiers 65

8.1 Introduction 65
8.2 Quantifiers 65
8.3 Set comprehension 67
8.4 Relationship between logic and set theory 68
8.5 Summary of notation 69
Exercises 69

Chapter 9 Relations 71

9.1 A relation is a set 71
9.2 Cartesian product 71
9.3 Relations 72
9.4 Declaring a relation 72
9.5 Maplets 73
9.6 Membership 73
9.7 Infix relations 73
9.8 Domain and range 74
9.9 Relational image 75
9.10 Constant value for a relation 75
9.11 Example of a relation 76
9.12 Restriction 77
9.13 Example of restriction 78
9.14 Composition 79
9.15 Example 80
9.16 Transitive closure 80
9.17 Identity relation 81
9.18 Reflexive transitive closure 81
9.19 Inverse of a relation 81
9.20 Examples 81
9.21 Summary of notation 82
Exercises 83

Chapter 10 Functions 87

10.1 A function is a relation 87
10.2 Function application 88
10.3 Partial and total functions 88
10.4 Other classes of functions 89
10.5 Constant functions 90
10.6 Overriding 91
10.7 Example from business – stock control 92

10.8 Example from data processing 93
10.9 Summary of notation 96
Exercises 96

Chapter 11 A seat allocation system **99**

11.1 Introduction 99
11.2 The types 99
11.3 The state 99
11.4 Initialisation operation 99
11.5 Operations 100
11.6 Enquiry operations 100
11.7 Dealing with errors 101
Exercises 102

Chapter 12 Sequences **103**

12.1 A sequence is a function 103
12.2 Sequence constructors 103
12.3 Sequence operators 104
12.4 Example of using sequences – stack 107
12.5 Example of using sequences – an air route 109
12.6 Sequences with no duplicates permitted 110
12.7 Example of using sequences – files in Pascal 110
12.8 Summary of notation 112
Exercises 113

Chapter 13 An example of sequences – the aircraft example again **115**

13.1 Introduction 115
13.2 The state 115
13.3 Initialisation operation 116
13.4 Operations 116
13.5 Enquiry operations 117
13.6 Dealing with errors 117
13.7 Implementation 117
Exercises 118

Chapter 14 Extending a specification **119**

14.1 Limitations of specifications given so far 119
14.2 The type of a flight 119
14.3 A function to a function 119
14.4 The state 120

14.5 Initialisation operation 121
14.6 Operations 121
14.7 Enquiry operations 122
14.8 Error conditions 123
14.9 Conclusions 123
Exercises 123

Chapter 15 Hints on creating specifications 125

15.1 Introduction 125
15.2 Types 125
15.3 Relationships 126
15.4 The state 126
15.5 Initialisation operation 126
15.6 Operations 126
15.7 Enquiry operations 126
15.8 In case of severe difficulty 127

Chapter 16 Example specifications 129

16.1 The Airport example 129
16.2 The types 129
16.3 The state 129
16.4 The initialisation operation 130
16.5 The operations 130
16.6 Handling errors 131
16.7 Error-handling operations 131
16.8 Fully specified operations 133
16.9 The operations 133
16.10 The Library example 133
16.11 Types 134
16.12 State 134
16.13 Initialisation operation 134
16.14 Operations 134
16.15 Extension 1: Limit on number of books out 137
16.16 The state 137
16.17 The initialisation operation 137
16.18 Operations 138
16.19 Extension 2: Books out for a limited period 139
16.20 Types 139
16.21 The state 139
16.22 Initialisation operation 139
16.23 Operations 140

16.24 Extension 3: Reservations 142
16.25 Types 142
16.26 The state 142
16.27 Initialisation operation 143
16.28 Operations 143

Appendix 1: Collected notation 145
Appendix 2: Solutions to exercises 151
Index 163