

Contents

Abridged Preface to First Edition	v
Preface to Second Edition	xi
0 Introduction	1
0.1 What Is this Book About?	1
0.2 Some Terminology	2
0.3 How Might Programs Fail?	3
0.4 A Way Forward	10
0.5 On Mathematics	12
0.6 Linking Paradigms	13
0.7 Problem Solving	15
0.8 The Book Plan	22
Part A: Preliminaries	29
1 The Technical Background	31
1.0 Introduction	31
1.1 Functions, Relations and Specifications	35
1.1.1 Summary of Features	49
1.1.2 Guidelines for Specifications	50
1.2 Equational Reasoning and Types	51
1.3 The Origin and Application of Rules	55
1.4 Data Types	61
1.4.1 A Glimpse at the Integers	61
1.4.2 Logical Types	66
1.4.2.1 The Boolean Type, \mathbb{B}	66
1.4.2.2 Implication and Deduction	72
1.4.2.3 Boolean Quantifiers	76
1.4.2.4 Extended (3-valued) Logic	78
1.4.3 Sets	91
1.4.4 Integers	96
1.4.4.1 Inequalities	99
1.4.5 Bags	101
1.4.6 Lists	103

1.4.7	Records and n -tuples	107
1.4.8	Union Types	109
1.4.9	Sub-types and Sub-ranges	110
1.4.10	Type Transfer Functions and Casts	111
1.4.11	Data Types and Transformations	114
1.4.12	On Quantification	116
1.5	Applying Unfold/Fold Transformations	118
2	On Programming	125
2.0	Overview	126
2.1	Procedural Programming	127
2.2	‘Good’ Programming	130
2.3	Structuring and (control) Flowcharts	131
2.4	PDL Overview	134
2.4.1	“Let” and “Where”	138
2.4.2	Scope and Parameters	139
2.5	Comments and Assertions	139
2.6	Verification of Procedural Programs	146
2.6.1	Sequencing	147
2.6.2	Alternation	149
2.6.3	Iteration	150
2.7	Program Derivation	154
Part B: Fundamentals	159
3	Algorithm Extraction	161
3.0	Overview	162
3.1	On Converging Recursion	164
3.2	Design Tactics	169
3.2.1	Checking Perceived Answers	172
3.2.2	Problem Reduction	175
3.2.3	Problem Decomposition	182
3.2.3.1	Structural Splitting	185
3.2.3.2	Predicated Splitting	201
3.2.3.3	Mixed Strategies	201
3.2.3.4	Domain Partitioning	202
3.2.4	The Use of Analogy	203
3.3	‘Eureka’ Processes	206
	Summary	221
4	Recursion Removal	223
4.1	Tail Recursion	225
4.2	Associative Recursion	238

4.3	Up and Down Iteration	249
4.4	Speeding up Iteratons	257
4.5	Recursive Procedures	262
	Summary	265
5	Quantifications	267
5.0	Overview	268
5.1	Defining Composite Values	268
5.2	Derived Composite Values	270
5.2.1	1-place Functions	270
5.2.2	2-place Functions	272
5.3	Application to Program Development	277
5.3.1	1-place Functions	278
5.3.2	2-place Functions	280
5.3.3	An Extended Example: The Factorial Function	282
5.4	Some Rules for Quantifications	291
5.4.1	General Rules	292
5.4.2	Special Rules for Logical Quantifiers	298
	Summary	300
6	Refinement and Re-use	301
6.1	Operational Refinement	302
6.1.1	On Correctness	302
6.1.2	Some Properties of Design Refinement	307
6.1.3	An Alternative View	309
6.2	Re-using Designs	310
	Conclusion	313
	Part C: Developments	315
7	Sorting	317
7.1	Specification and Initial Discussion	317
7.2	Initial Designs	323
7.2.1	Problem Reduction	323
7.2.2	Structural Splitting	326
7.2.3	Predicated Splitting (Partitioning)	333
7.3	Complete Designs	341
7.3.1	Exchange Sorts	341
7.3.2	Merge Sorts	347
7.3.2.1	The Basic Merge Sort	347
7.3.3	Partition Sorts	348
7.3.3.1	Simple Partition Sort	350
7.4	A Quick Design	352

8	Data Refinement	357
8.1	On 'Internal' Data Types	358
8.2	Changing Data Types	358
8.3	Where to next?	370
9	Sorting Revisited	375
9.1	Exchange Sorts	375
9.2	Merge Sorts	383
9.2.1	Variants of the Merge Sort	384
9.3	Partition Sorts	390
10	Failures and Fixes	409
10.1	Inadequate Pre-Conditions	410
10.2	Failures in Structural Splitting	411
10.2.1	Loss of Vital Information	412
11	Further Examples	417
11.1	The 2-D Convex Hull	418
11.2	Topological Sort	424
11.2.1	Experimentation	425
11.2.2	A Proper Formulation	433
11.3	Some 'Extremal' Problems	439
12	On Interactive Software	455
12.1	Specifications Involving Change	457
12.1.1	Specifications of Input/Output	457
12.1.2	Conventional Communications	463
12.1.3	The Enabling of Computations	466
12.2	Pertaining to (Software) Systems	466
12.2.1	System Requirements	467
12.2.2	Specifying Systems	469
Appendix	Transformation Digest	473
A.0	Re-write Rule Conventions	473
A.1	Data Manipulation Rules	473
A.1.1	The Type \mathbb{B}	475
A.1.2	Extended Logic and Conditional Expressions	477
A.1.3	Integers	479
A.1.4	Sets	480
A.1.5	Bags	482
A.1.6	Lists	483
A.1.7	Common Conversion Functions	485
A.1.8	Quantifier Rules	486

Contents

xxi

A.2	Quantifier Properties	490
A.3	'Not Occurs in'	491
A.4	On PDL Structure	492
	A.4.1 Scope and Parameters	494
A.5	PDL Transformation Rules	495
Bibliography		501
Index		503



<http://www.springer.com/978-1-85233-820-6>

Constructing Correct Software

Cooke, D.J.

2005, XXI, 509 p. 100 illus., Softcover

ISBN: 978-1-85233-820-6