
Contents

1	Introduction	1
1.1	Why is Mathematics Useful?	1
1.2	Formal Methods in Software Development	3
1.3	Formal Methods and Object-orientation	6
1.4	Z ⁺⁺	8
1.5	VDM ⁺⁺	11
1.6	Adding Formality to Diagrammatic Methods	12
1.7	Problems in Object-oriented Development	13
2	The Software Development Process	15
2.1	Formal Object-oriented Development	15
2.2	Example Development: Shapes and Points	19
2.3	The Layered Development Paradigm	30
2.4	Development Example in VDM ⁺⁺	35
3	From Analysis to Formal Specification	44
3.1	Formalisation of Object Models	45
3.2	Aggregation	52
3.3	Alternative Approaches	56
3.4	Formalisation of Dynamic Models	58
3.5	The Booch Method	73
3.6	Specification Construction Principles	75
3.7	Animation	79
4	Specification Notations and Techniques	84
4.1	Attributes and Data Structures	85
4.2	Operations	92
4.3	Inheritance	111
4.4	Subtyping	113
4.5	Class Composition	120
4.6	Object Identity	122

CONTENTS

4.7	Dynamic Behaviour	126
4.8	Complex Data Types	132
4.9	VDM++	134
5	Design and Refinement	137
5.1	Design Approaches	137
5.2	Refinement	146
5.3	Subtyping, Composition and Refinement	167
5.4	VDM++	173
6	Proof Methods and Techniques	176
6.1	Safety Reasoning – Monitor and Gate	176
6.2	Liveness Reasoning – Dining Philosophers	180
6.3	Internal Consistency Proofs	182
6.4	Refinement and Subtyping Proofs	183
6.5	Object Identity	207
6.6	Reasoning About Concurrent Object Execution	212
6.7	Synchronisation Refinement Proofs	214
6.8	General Refinement Proof Techniques	218
7	Concurrent and Real-time Behaviour	219
7.1	Extended Harel Statecharts	219
7.2	Specifying Reactive System Properties	236
8	Implementation and Code Generation	257
8.1	Translation into Procedural Languages	257
8.2	Introducing Concurrency in Implementations	276
8.3	Implementation Case Study: Personnel System	278
8.4	Testing	281
9	Case Studies	286
9.1	Invoice System	286
9.2	Expedited Data Queue	297
9.3	Fire Control	299
9.4	Specification of Reactive Systems	303
9.5	Mine Pump Control	305
A	Appendix: Z++	332
A.1	Mathematical Notation	332
A.2	Z Notation	336
A.3	Z++ Specification Notation	337
A.4	Z++/RTL Logic	347

B Appendix: VDM⁺⁺	365
B.1 VDM ⁺⁺ Mathematical Notation	365
B.2 VDM ⁺⁺ Specification Notation	368
B.3 The VDM ⁺⁺ Model of Concurrency	372
B.4 The Semantics of Procedural Statements	374
B.5 Tool Support	380
B.6 Syntax Summary of VDM ⁺⁺	383
 C Exercise Answers	 388
 D Task Analysis	 415