
Contents

1	Introduction	1
1.1	Software Life Cycle	2
1.2	The Problem	4
1.3	Formal Methods	5
1.3.1	What Are Formal Methods	5
1.3.2	Some Commonly Used Formal Methods	7
1.3.3	Challenges to Formal Methods	9
1.4	Formal Engineering Methods	10
1.5	What Is SOFL	13
1.6	A Little History of SOFL	16
1.7	Comparison with Related Work	17
1.8	Exercises	19
2	Propositional Logic	21
2.1	Propositions	21
2.2	Operators	22
2.3	Conjunction	23
2.4	Disjunction	24
2.5	Negation	24
2.6	Implication	25
2.7	Equivalence	25
2.8	Tautology, Contradiction, and Contingency	26
2.9	Normal Forms	27
2.10	Sequent	27
2.11	Proof	28
2.11.1	Inference Rules	28
2.11.2	Rules for Conjunction	29
2.11.3	Rules for Disjunction	29
2.11.4	Rules for Negation	30
2.11.5	Rules for Implication	30

2.11.6	Rules for Equivalence	30
2.11.7	Properties of Propositional Expressions	31
2.12	Exercises	34
3	Predicate Logic	37
3.1	Predicates	37
3.2	Quantifiers	40
3.2.1	The Universal Quantifier	40
3.2.2	The Existential Quantifier	41
3.2.3	Quantified Expressions with Multiple Bound Variables .	42
3.2.4	Multiple Quantifiers	43
3.2.5	de Morgan's Laws	43
3.3	Substitution	44
3.4	Proof in Predicate Logic	46
3.4.1	Introduction and Elimination of Existential Quantifiers.	46
3.4.2	Introduction and Elimination of Universal Quantifiers .	46
3.5	Validity and Satisfaction	47
3.6	Treatment of Partial Predicates	48
3.7	Formal Specification with Predicates	50
3.8	Exercises	50
4	The Module	53
4.1	Module for Abstraction	53
4.2	Condition Data Flow Diagrams	55
4.3	Processes	56
4.4	Data Flows	68
4.5	Data Stores	71
4.6	Convention for Names	79
4.7	Conditional Structures	79
4.8	Merging and Separating Structures	81
4.9	Diverging Structures	84
4.10	Renaming Structure	86
4.11	Connecting Structures	87
4.12	Important Issues on CDFDs	88
4.12.1	Starting Processes	89
4.12.2	Starting Nodes	90
4.12.3	Terminating Processes	90
4.12.4	Terminating Nodes	91
4.12.5	Enabling and Executing a CDFD	91
4.12.6	Restriction on Parallel Processes	92
4.12.7	Disconnected CDFDs	94
4.12.8	External Processes	96
4.13	Associating CDFD with a Module	97
4.14	How to Write Comments	104
4.15	A Module for the ATM	104

4.16	Compound Expressions	107
4.16.1	The if-then-else Expression	107
4.16.2	The let Expression	108
4.16.3	The case Expression	109
4.16.4	Reference to Pre and Postconditions	110
4.17	Function Definitions	111
4.17.1	Explicit and Implicit Specifications	111
4.17.2	Recursive Functions	113
4.18	Exercises	114
5	Hierarchical CDFDs and Modules	117
5.1	Process Decomposition	117
5.2	Handling Stores in Decomposition	123
5.3	Input and Output Data Flows	124
5.4	The Correctness of Decomposition	127
5.5	Scope	129
5.6	Exercises	132
6	Explicit Specifications	133
6.1	The Structure of an Explicit Specification	133
6.2	Assignment Statement	134
6.3	Sequential Statements	135
6.4	Conditional Statements	135
6.5	Multiple Choice Statements	136
6.6	The Block Statement	137
6.7	The While Statement	137
6.8	Method Invocation	138
6.9	Input and Output Statements	139
6.10	Example	139
6.11	Exercises	141
7	Basic Data Types	143
7.1	The Numeric Types	143
7.2	The Character Type	145
7.3	The Enumeration Types	146
7.4	The Boolean Type	147
7.5	An Example	148
7.6	Exercises	148
8	The Set Types	151
8.1	What Is a Set	151
8.2	Set Type Declaration	152
8.3	Constructors and Operators on Sets	153
8.3.1	Constructors	153
8.3.2	Operators	154

8.4	Specification with Set Types	160
8.5	Exercises	162
9	The Sequence and String Types	165
9.1	What Is a Sequence	165
9.2	Sequence Type Declarations	166
9.3	Constructors and Operators on Sequences	167
9.3.1	Constructors	167
9.3.2	Operators	169
9.4	Specifications Using Sequences	174
9.4.1	Input and Output Module	174
9.4.2	Membership Management System	175
9.5	Exercises	176
10	The Composite and Product Types	179
10.1	Composite Types	179
10.1.1	Constructing a Composite Type	179
10.1.2	Fields Inheritance	181
10.1.3	Constructor	182
10.1.4	Operators	182
10.1.5	Comparison	184
10.2	Product Types	184
10.3	An Example of Specification	186
10.4	Exercises	188
11	The Map Types	191
11.1	What Is a Map	191
11.2	The Type Constructor	192
11.3	Operators	193
11.3.1	Constructors	193
11.3.2	Operators	194
11.4	Specification Using a Map	199
11.5	Exercises	201
12	The Union Types	203
12.1	Union Type Declaration	203
12.2	A Special Union Type	204
12.3	Is Function	205
12.4	A Specification with a Union Type	205
12.5	Exercises	206
13	Classes	209
13.1	Classes and Objects	209
13.1.1	Class Definition	210
13.1.2	Objects	213
13.1.3	Identity of Objects	214

13.2	Reference and Access Control	214
13.3	The Reference of a Current Object	216
13.4	Inheritance	217
13.4.1	What Is Inheritance	217
13.4.2	Superclasses and Subclasses	218
13.4.3	Constructor	220
13.4.4	Method Overloading	220
13.4.5	Method Overriding	221
13.4.6	Garbage Collection	222
13.5	Polymorphism	222
13.6	Generic Classes	224
13.7	An Example of Class Hierarchy	226
13.8	Example of Using Objects in Modules	229
13.9	Exercises	232
14	The Software Development Process	235
14.1	Software Process Using SOFL	235
14.2	Requirements Analysis	236
14.2.1	The Informal Specification	237
14.2.2	The Semi-formal Specification	239
14.3	Abstract Design	243
14.4	Evolution	252
14.5	Detailed Design	252
14.5.1	Transformation from Implicit to Explicit Specifications	253
14.5.2	Transformation from Structured to Object-Oriented Specifications	255
14.6	Program	257
14.7	Validation and Verification	258
14.8	Adapting the Process to Specific Applications	259
14.9	Exercises	260
15	Approaches to Constructing Specifications	261
15.1	The Top-Down Approach	261
15.1.1	The CFD-Module-First Strategy	262
15.1.2	The CFD-Hierarchy-First Strategy	263
15.1.3	The Modules and Classes	264
15.2	The Middle-out Approach	265
15.3	Comparison of the Approaches	267
15.4	Exercises	268
16	A Case Study – Modeling an ATM	269
16.1	Informal User Requirements Specification	270
16.2	Semi-formal Functional Specification	273
16.3	Formal Abstract Design Specification	279
16.4	Formal Detailed Design Specification	287

16.5	Summary	300
16.6	Exercises	301
17	Rigorous Review	303
17.1	The Principle of Rigorous Review	303
17.2	Properties	305
17.2.1	Internal Consistency of a Process	305
17.2.2	Invariant-Conformance Consistency	307
17.2.3	Satisfiability	308
17.2.4	Internal Consistency of CDFD	309
17.3	Review Task Tree	310
17.3.1	Review Task Tree Notation	310
17.3.2	Minimal Cut Sets	312
17.3.3	Review Evaluation	313
17.4	Property Review	314
17.4.1	Review of Consistency Between Process and Invariant	314
17.4.2	Process Consistency Review	316
17.4.3	Review of Process Satisfiability	317
17.4.4	Review of Internal Consistency of CDFD	317
17.5	Constructive and Critical Review	319
17.6	Important Points	320
17.7	Exercises	321
18	Specification Testing	323
18.1	The Process of Testing	323
18.2	Unit Testing	325
18.2.1	Process Testing	326
18.2.2	Invariant Testing	332
18.3	Criteria for Test Case Generation	335
18.4	Integration Testing	338
18.4.1	Testing Sequential Constructs	339
18.4.2	Testing Conditional Constructs	341
18.4.3	Testing Decompositions	343
18.5	Exercises	346
19	Transformation from Designs to Programs	349
19.1	Transformation of Data Types	350
19.2	Transformation of Modules and Classes	351
19.3	Transformation of Processes	357
19.3.1	Transformation of Single-Port Processes	357
19.3.2	Transformation of Multiple-Port Processes	360
19.4	Transformation of CDFD	362
19.5	Exercises	369

20	Intelligent Software Engineering Environment	371
20.1	Software Engineering Environment	371
20.2	Intelligent Software Engineering Environment	373
20.3	Ways to Build an ISEE	375
20.3.1	Domain-Driven Approach	375
20.3.2	Method-Driven Approach	375
20.3.3	Combination of Both	376
20.4	ISEE and Formalization	376
20.5	ISEE for SOFL	377
20.5.1	Support for Requirements Analysis	377
20.5.2	Support for Abstract Design	378
20.5.3	Support for Refinement	378
20.5.4	Support for Verification and Validation	379
20.5.5	Support for Transformation	379
20.5.6	Support for Program Testing	379
20.5.7	Support for System Modification	380
20.5.8	Support for Process Management	380
20.6	Exercises	381
	References	383
A	Syntax of SOFL	391
A.1	Specifications	391
A.2	Modules	392
A.3	Processes	392
A.4	Functions	394
A.5	Classes	394
A.6	Types	395
A.7	Expressions	396
A.8	Ordinary Expressions	396
A.8.1	Compound Expressions	396
A.8.2	Unary Expressions	397
A.8.3	Binary Expressions	397
A.8.4	Apply Expressions	397
A.8.5	Basic Expressions	399
A.8.6	Constants	399
A.8.7	Simple Variables	400
A.8.8	Special Keywords	400
A.8.9	Set Expressions	400
A.8.10	Sequence Expressions	400
A.8.11	Map Expressions	401
A.8.12	Composite Expressions	401
A.8.13	Product Expressions	401

XXII Contents

A.9 Predicate Expressions	401
A.9.1 Boolean Variables	401
A.9.2 Relational Expressions	401
A.9.3 Conjunction	402
A.9.4 Disjunction	402
A.9.5 Implication	402
A.9.6 Equivalence	402
A.9.7 Negation	402
A.9.8 Quantified Expressions	402
A.10 Identifiers	403
A.11 Character	403
A.12 Comments	403
Index	405