
Contents

1	Software Engineering	1
1.1	Introduction	1
1.2	What Is Software Engineering?	4
1.3	Challenges in Software Engineering	6
1.4	Software Processes and Life cycles.	8
1.4.1	Waterfall Life cycle	9
1.4.2	Spiral Life cycles.	10
1.4.3	Rational Unified Process	11
1.4.4	Agile Development	12
1.5	Activities in Waterfall Life cycle	14
1.5.1	Business Requirements Definition	15
1.5.2	Specification of System Requirements	16
1.5.3	Design	16
1.5.4	Implementation	17
1.5.5	Software Testing	18
1.5.6	Support and Maintenance	19
1.6	Software Inspections.	20
1.7	Software Project Management.	21
1.8	CMMI Maturity Model.	22
1.9	Formal Methods	23
1.10	Review Questions.	24
1.11	Summary	24
	References.	25
2	Software Reliability and Dependability	27
2.1	Introduction	27
2.2	Software Reliability	28
2.2.1	Software Reliability and Defects	29
2.2.2	Cleanroom Methodology	31
2.2.3	Software Reliability Models.	32
2.3	Dependability	35
2.4	Computer Security	37
2.5	System Availability.	38

2.6	Safety Critical Systems	38
2.7	Review Questions	39
2.8	Summary	40
	References.	40
3	Overview of Formal Methods.	41
3.1	Introduction	41
3.2	Why Should We Use Formal Methods?	43
3.3	Industrial Applications of Formal Methods.	45
3.4	Industrial Tools for Formal Methods	46
3.5	Approaches to Formal Methods	47
	3.5.1 Model-Oriented Approach	47
	3.5.2 Axiomatic Approach	49
3.6	Proof and Formal Methods	49
3.7	Mathematics in Software Engineering.	50
3.8	The Vienna Development Method	51
3.9	VDM ⁺ , the Irish School of VDM.	52
3.10	The Z Specification Language.	54
3.11	The <i>B</i> -Method.	55
3.12	Predicate Transformers and Weakest Preconditions.	56
3.13	The Process Calculi	56
3.14	Finite-State Machines	57
3.15	The Parnas Way	58
3.16	Model Checking	59
3.17	Usability of Formal Methods	60
3.18	Review Questions	61
3.19	Summary	61
	References.	62
4	Sets, Relations and Functions.	65
4.1	Introduction	65
4.2	Set Theory	66
	4.2.1 Set Theoretical Operations.	68
	4.2.2 Properties of Set Theoretical Operations	71
	4.2.3 Russell's Paradox	72
	4.2.4 Computer Representation of Sets.	73
4.3	Relations.	74
	4.3.1 Reflexive, Symmetric and Transitive Relations	75
	4.3.2 Composition of Relations	78
	4.3.3 Binary Relations	79
	4.3.4 Applications of Relations.	80
4.4	Functions	82
4.5	Application of Functions.	87
	4.5.1 Miranda Functional Programming Language	88

4.6	Review Questions	90
4.7	Summary	91
	References.	92
5	A Short History of Logic	93
5.1	Introduction	93
5.2	Syllogistic Logic	94
5.3	Paradoxes and Fallacies	96
5.4	Stoic Logic	98
5.5	Boole’s Symbolic Logic	99
	5.5.1 Switching Circuits and Boolean Algebra	102
5.6	Application of Symbolic Logic to Digital Computing	104
5.7	Frege.	105
5.8	Review Questions	107
5.9	Summary	107
	References.	108
6	Propositional and Predicate Logic	109
6.1	Introduction	109
6.2	Propositional Logic	110
	6.2.1 Truth Tables	112
	6.2.2 Properties of Propositional Calculus	114
	6.2.3 Proof in Propositional Calculus	116
	6.2.4 Semantic Tableaux in Propositional Logic	118
	6.2.5 Natural Deduction	121
	6.2.6 Sketch of Formalization of Propositional Calculus	121
	6.2.7 Applications of Propositional Calculus	123
	6.2.8 Limitations of Propositional Calculus	125
6.3	Predicate Calculus.	125
	6.3.1 Sketch of Formalization of Predicate Calculus.	127
	6.3.2 Interpretation and Valuation Functions	129
	6.3.3 Properties of Predicate Calculus.	130
	6.3.4 Applications of Predicate Calculus	130
	6.3.5 Semantic Tableaux in Predicate Calculus.	131
6.4	Review Questions	134
6.5	Summary	134
	References.	135
7	Advanced Topics in Logic.	137
7.1	Introduction	137
7.2	Fuzzy Logic	138
7.3	Temporal Logic	139
7.4	Intuitionist Logic.	141
7.5	Undefined Values	143

7.5.1	Logic of Partial Functions	143
7.5.2	Parnas Logic	145
7.5.3	Dijkstra and Undefinedness	146
7.6	Logic and AI	148
7.7	Theorem Provers for Logic	151
7.8	Review Questions	153
7.9	Summary	153
	References.	154
8	Z Formal Specification Language.	155
8.1	Introduction	155
8.2	Sets.	158
8.3	Relations.	159
8.4	Functions	161
8.5	Sequences.	162
8.6	Bags	163
8.7	Schemas and Schema Composition.	164
8.8	Reification and Decomposition	167
8.9	Proof in Z.	168
8.10	Industrial Applications of Z	169
8.11	Review Questions.	170
8.12	Summary	170
	References.	171
9	Vienna Development Method	173
9.1	Introduction	173
9.2	Sets.	176
9.3	Sequences.	178
9.4	Maps.	179
9.5	Logic of Partial Functions in VDM	180
9.6	Data Types and Data Invariants	181
9.7	Specification in VDM.	182
9.8	Refinement in VDM.	183
9.9	Industrial Applications of VDM	184
9.10	Review Questions.	185
9.11	Summary	185
	References.	186
10	Irish School of VDM.	187
10.1	Introduction	187
10.2	Mathematical Structures and Their Morphisms	189
10.3	Models and Modelling	191
10.4	Sets.	192
10.5	Relations and Functions	194
10.6	Sequences.	196

10.7	Indexed Structures	197
10.8	Specifications and Proofs	198
10.9	Refinement in Irish VDM	200
10.10	Review Questions	202
10.11	Summary	203
	References.	204
11	Unified Modelling Language.	205
11.1	Introduction	205
11.2	Overview of UML	206
11.3	UML Diagrams.	208
11.4	Object Constraint Language	214
11.5	Industrial Tools for UML	215
11.6	Rational Unified Process.	215
11.7	Review Questions	217
11.8	Summary	218
	References.	218
12	Dijkstra, Hoare and Parnas	219
12.1	Introduction	219
12.2	Calculus of Weakest Preconditions	224
	12.2.1 Properties of WP	226
	12.2.2 WP of Commands	226
	12.2.3 Formal Program Development with WP	230
12.3	Axiomatic Definition of Programming Languages	231
12.4	Tabular Expressions	236
12.5	Review Questions	240
12.6	Summary	241
	Reference	241
13	Automata Theory	243
13.1	Introduction	243
13.2	Finite-State Machines	244
13.3	Pushdown Automata.	247
13.4	Turing Machines.	249
13.5	Review Questions	251
13.6	Summary	251
	References.	252
14	Model Checking.	253
14.1	Introduction	253
14.2	Modelling Concurrent Systems	257
14.3	Linear Temporal Logic	258
14.4	Computational Tree Logic	259
14.5	Tools for Model Checking	260

14.6	Industrial Applications of Model Checking	260
14.7	Review Questions	261
14.8	Summary	261
	References	262
15	The Nature of Theorem Proving	263
15.1	Introduction	263
15.2	Early Automation of Proof	265
15.3	Interactive Theorem Provers	267
15.4	A Selection of Theorem Provers	269
15.5	Review Questions	269
15.6	Summary	269
	Reference	271
16	Probability and Statistics	273
16.1	Introduction	273
16.2	Probability Theory	274
	16.2.1 Laws of Probability	275
	16.2.2 Random Variables	276
16.3	Statistics	279
	16.3.1 Abuse of Statistics	280
	16.3.2 Statistical Sampling	280
	16.3.3 Averages in a Sample	281
	16.3.4 Variance and Standard Deviation	282
	16.3.5 Bell-Shaped (Normal) Distribution	283
	16.3.6 Frequency Tables, Histograms and Pie Charts	285
	16.3.7 Hypothesis Testing	287
16.4	Review Questions	288
16.5	Summary	289
	References	289
17	Industrial Tools for Formal Methods	291
17.1	Introduction	291
17.2	Tools for Z	292
17.3	Tools for VDM	293
17.4	Tools for B	294
17.5	Tools for UML	295
17.6	Tools for Model Checking	296
17.7	Tools for Theorem Provers	297
17.8	Review Questions	298
17.9	Summary	298
	References	299

18	Technology Transfer to Industry	301
18.1	Introduction	301
18.2	Formal Methods and Industry	302
18.3	Usability of Formal Methods	304
18.3.1	Why Are Formal Methods Difficult?	305
18.3.2	Characteristics of a Usable Formal Method	305
18.4	Pilot of Formal Methods	307
18.4.1	Technology Transfer of Formal Methods	307
18.5	Review Questions	308
18.6	Summary	308
	References	309
19	Epilogue	311
19.1	The Future of Formal Methods	314
20	Erratum to: Concise Guide to Formal Methods	E1
	Gerard O'Regan	
	Glossary	315
	Index	319



<http://www.springer.com/978-3-319-64020-4>

Concise Guide to Formal Methods

Theory, Fundamentals and Industry Applications

O'Regan, G.

2017, XXVI, 322 p. 81 illus., 56 illus. in color., Softcover

ISBN: 978-3-319-64020-4