

Contents

1	Mathematics in Civilization	1
1.1	Introduction	1
1.2	The Babylonians	3
1.3	The Egyptians	6
1.4	The Greeks	8
1.5	The Romans	16
1.6	Islamic Influence	19
1.7	Chinese and Indian Mathematics	20
1.8	Review Questions	21
1.9	Summary	21
2	Sets, Relations and Functions	23
2.1	Introduction	23
2.2	Set Theory	24
2.2.1	Set Theoretical Operations	26
2.2.2	Properties of Set Theoretical Operations	28
2.2.3	Russell's Paradox	29
2.3	Relations	30
2.3.1	Reflexive, Symmetric and Transitive Relations	32
2.3.2	Composition of Relations	34
2.3.3	Binary Relations	35
2.4	Functions	36
2.5	Review Questions	40
2.6	Summary	41
3	Logic	43
3.1	Introduction	43
3.2	Propositional Logic	45
3.2.1	Truth Tables	47
3.2.2	Properties of Propositional Calculus	49
3.2.3	Proof in Propositional Calculus	50
3.2.4	Applications of Propositional Calculus	54
3.2.5	Limitations of Propositional Calculus	55

3.3	Predicate Calculus	55
3.3.1	Formalisation of Predicate Calculus	58
3.3.2	Interpretation and Valuation Functions	59
3.3.3	Properties of Predicate Calculus	60
3.3.4	Applications of Predicate Calculus	60
3.4	Undefined Values	61
3.4.1	Logic of Partial Functions	62
3.4.2	Parnas Logic	63
3.4.3	Dijkstra and Undefinedness	65
3.5	Other Logics	66
3.6	Tools for Logic	68
3.7	Review Questions	69
3.8	Summary	69
4	Software Engineering	71
4.1	Introduction	71
4.2	What is Software Engineering?	73
4.3	Early Software Engineering	78
4.4	Software Engineering Mathematics	81
4.5	Formal Methods	82
4.6	Software Inspections and Testing	83
4.7	Process Maturity Models	85
4.8	Review Questions	86
4.9	Summary	86
5	Formal Methods	89
5.1	Introduction	89
5.2	Why Should We Use Formal Methods?	91
5.3	Applications of Formal Methods	92
5.4	Tools for Formal Methods	93
5.5	Approaches to Formal Methods	94
5.5.1	Model-Oriented Approach	94
5.5.2	Axiomatic Approach	95
5.6	Proof and Formal Methods	95
5.7	The Future of Formal Methods	96
5.8	The Vienna Development Method	97
5.9	VDM [♣] , the Irish School of Vienna Development Method (VDM)	98
5.10	The Z Specification Language	99
5.11	The B-Method	100
5.12	Predicate Transformers and Weakest Pre-Conditions	101
5.13	The Process Calculi	102
5.14	Finite State Machines	103
5.15	The Parnas Way	104
5.16	Usability of Formal Methods	105
5.16.1	Why Are Formal Methods Difficult?	105
5.16.2	Characteristics of a Usable Formal Method	106

5.17	Review Questions	107
5.18	Summary	107
6	Z Formal Specification Language	109
6.1	Introduction	109
6.2	Sets	111
6.3	Relations	112
6.4	Functions	114
6.5	Sequences	115
6.6	Bags	116
6.7	Schemas and Schema Composition	117
6.8	Reification and Decomposition	120
6.9	Proof in Z	121
6.10	Review Questions	121
6.11	Summary	122
7	Number Theory	123
7.1	Introduction	123
7.2	Elementary Number Theory	125
7.3	Prime Number Theory	129
7.3.1	Greatest Common Divisors (GCD)	131
7.3.2	Least Common Multiple (LCM)	132
7.3.3	Euclid's Algorithm	132
7.3.4	Distribution of Primes	134
7.4	Theory of Congruences	137
7.5	Review Questions	140
7.6	Summary	140
8	Cryptography	141
8.1	Introduction	141
8.2	Breaking the Enigma Codes	143
8.3	Cryptographic Systems	145
8.4	Symmetric Key Systems	146
8.5	Public Key Systems	150
8.5.1	RSA Public Key Cryptosystem	152
8.5.2	Digital Signatures	153
8.6	Review Questions	154
8.7	Summary	154
9	Coding Theory	155
9.1	Introduction	155
9.2	Mathematical Foundations	156
9.2.1	Groups	156
9.2.2	Rings	157
9.2.3	Fields	158
9.2.4	Vector Spaces	159

9.3	Simple Channel Code	161
9.4	Block Codes	162
9.4.1	Error Detection and Correction	163
9.5	Linear Block Codes	164
9.5.1	Parity-Check Matrix	166
9.5.2	Binary Hamming Code	167
9.5.3	Binary Parity-Check Code	168
9.6	Miscellaneous Codes in Use	168
9.7	Review Questions	169
9.8	Summary	169
10	Language Theory and Semantics	171
10.1	Introduction	171
10.2	Alphabets and Words	172
10.3	Grammars	173
10.3.1	Backus Naur Form	174
10.3.2	Parse Trees and Derivations	176
10.4	Programming Language Semantics	178
10.4.1	Axiomatic Semantics	179
10.4.2	Operational Semantics	180
10.4.3	Denotational Semantics	181
10.5	Lambda Calculus	182
10.6	Lattices and Order	184
10.6.1	Partially Ordered Sets	184
10.6.2	Lattices	186
10.6.3	Complete Partial Orders	186
10.6.4	Recursion	187
10.7	Review Questions	189
10.8	Summary	189
11	Computability and Decidability	191
11.1	Introduction	191
11.2	Formalism	192
11.3	Decidability	194
11.4	Computability	196
11.5	Computational Complexity	199
11.6	Review Questions	199
11.7	Summary	200
12	Probability, Statistics and Software Reliability	201
12.1	Introduction	201
12.2	Probability Theory	202
12.2.1	Laws of Probability	203
12.2.2	Random Variables	204
12.3	Statistics	207

12.3.1 Abuse of Statistics	207
12.3.2 Statistical Sampling	207
12.3.3 Averages in a Sample	208
12.3.4 Variance and Standard Deviation	209
12.3.5 Bell-shaped (Normal) Distribution	210
12.3.6 Frequency Tables, Histograms and Pie Charts	212
12.3.7 Hypothesis Testing	213
12.4 Software Reliability	214
12.4.1 Software Reliability and Defects	215
12.4.2 Cleanroom Methodology	217
12.4.3 Software Reliability Models	218
12.5 Review Questions	220
12.6 Summary	220
13 Matrix Theory	223
13.1 Introduction	223
13.1.1 2×2 Matrices	224
13.2 Matrix Operations	227
13.3 Determinants	228
13.4 Eigenvectors and Eigenvalues	230
13.5 Gaussian Elimination	231
13.6 Review Questions	232
13.7 Summary	233
14 Complex Numbers and Quaternions	235
14.1 Introduction	235
14.2 Complex Numbers	236
14.3 Quaternions	240
14.3.1 Quaternion Algebra	242
14.3.2 Quaternions and Rotations	245
14.4 Review Questions	246
14.5 Summary	246
15 Calculus	247
15.1 Introduction	247
15.2 Differentiation	250
15.2.1 Rules of Differentiation	252
15.3 Integration	254
15.3.1 Definite Integrals	255
15.3.2 Fundamental Theorems of Integral Calculus	257
15.4 Numerical Analysis	258
15.5 Fourier Series	261
15.6 The Laplace Transform	262
15.7 Differential Equations	263
15.8 Review Questions	264
15.9 Summary	264

16 Graph Theory	267
16.1 Introduction	267
16.2 Undirected Graphs	268
16.2.1 Hamiltonian Paths	272
16.3 Trees	273
16.3.1 Binary Trees	273
16.4 Graph Algorithms	274
16.5 Review Questions	274
16.6 Summary	274
References	277
Glossary	281
Index	283

Mathematics in Computing

An Accessible Guide to Historical, Foundational and
Application Contexts

O'Regan, G.

2013, XX, 288 p., Hardcover

ISBN: 978-1-4471-4533-2