
Contents

1	Mathematics in Civilization	1
1.1	Introduction	1
1.2	The Babylonians	4
1.3	The Egyptians	6
1.4	The Greeks	8
1.5	The Romans	17
1.6	Islamic Influence	19
1.7	Chinese and Indian Mathematics	22
1.8	Review Questions	23
1.9	Summary	23
	References	24
2	Sets, Relations and Functions	25
2.1	Introduction	25
2.2	Set Theory	26
2.2.1	Set Theoretical Operations	28
2.2.2	Properties of Set Theoretical Operations	31
2.2.3	Russell's Paradox	32
2.2.4	Computer Representation of Sets	33
2.3	Relations	34
2.3.1	Reflexive, Symmetric and Transitive Relations	35
2.3.2	Composition of Relations	37
2.3.3	Binary Relations	39
2.3.4	Applications of Relations	40
2.4	Functions	41
2.5	Application of Functions	46
2.6	Review Questions	49
2.7	Summary	50
	References	51
3	Number Theory	53
3.1	Introduction	53
3.2	Elementary Number Theory	55
3.3	Prime Number Theory	59

3.3.1	Greatest Common Divisors (GCD)	61
3.3.2	Least Common Multiple (LCM)	62
3.3.3	Euclid's Algorithm	63
3.3.4	Distribution of Primes	65
3.4	Theory of Congruences.	67
3.5	Binary System and Computer Representation of Numbers	71
3.6	Review Questions	73
3.7	Summary	74
	References.	74
4	Mathematical Induction and Recursion	75
4.1	Introduction	75
4.2	Strong Induction	78
4.3	Recursion	80
4.4	Structural Induction.	82
4.5	Review Questions	83
4.6	Summary	83
	Reference	84
5	Sequences, Series and Permutations and Combinations	85
5.1	Introduction	85
5.2	Sequences and Series	86
5.3	Arithmetic and Geometric Sequences	87
5.4	Arithmetic and Geometric Series	88
5.5	Simple and Compound Interest.	89
5.6	Time Value of Money and Annuities	91
5.7	Permutations and Combinations	92
5.8	Review Questions	96
5.9	Summary	97
6	Algebra	99
6.1	Introduction	99
6.2	Simple and Simultaneous Equations	100
6.3	Quadratic Equations	103
6.4	Indices and Logarithms.	106
6.5	Horner's Method for Polynomials.	108
6.6	Abstract Algebra.	109
6.6.1	Monoids and Groups	109
6.6.2	Rings	111
6.6.3	Fields.	112
6.6.4	Vector Spaces	113
6.7	Review Questions	115
6.8	Summary	116
	Reference	116

7	Automata Theory	117
7.1	Introduction	117
7.2	Finite-State Machines	118
7.3	Pushdown Automata	121
7.4	Turing Machines	123
7.5	Review Questions	125
7.6	Summary	125
	Reference	126
8	Matrix Theory	127
8.1	Introduction	127
8.2	Two \times Two Matrices	129
8.3	Matrix Operations	131
8.4	Determinants	133
8.5	Eigen Vectors and Values	135
8.6	Gaussian Elimination	136
8.7	Review Questions	138
8.8	Summary	138
	Reference	139
9	Graph Theory	141
9.1	Introduction	141
9.2	Undirected Graphs	143
9.2.1	Hamiltonian Paths	147
9.3	Trees	148
9.3.1	Binary Trees	149
9.4	Graph Algorithms	150
9.5	Graph Colouring and Four-Colour Problem	150
9.6	Review Questions	152
9.7	Summary	152
	References	153
10	Cryptography	155
10.1	Introduction	155
10.2	Breaking the Enigma Codes	157
10.3	Cryptographic Systems	160
10.4	Symmetric Key Systems	161
10.5	Public Key Systems	165
10.5.1	RSA Public Key Cryptosystem	167
10.5.2	Digital Signatures	168
10.6	Review Questions	169
10.7	Summary	169
	References	170

11	Coding Theory	171
11.1	Introduction	171
11.2	Mathematical Foundations	172
11.3	Simple Channel Code	173
11.4	Block Codes	174
11.4.1	Error Detection and Correction	176
11.5	Linear Block Codes	177
11.5.1	Parity Check Matrix	179
11.5.2	Binary Hamming Code	180
11.5.3	Binary Parity-Check Code	181
11.6	Miscellaneous Codes in Use	182
11.7	Review Questions	182
11.8	Summary	183
	References	183
12	Language Theory and Semantics	185
12.1	Introduction	185
12.2	Alphabets and Words	186
12.3	Grammars	187
12.3.1	Backus Naur Form	189
12.3.2	Parse Trees and Derivations	191
12.4	Programming Language Semantics	192
12.4.1	Axiomatic Semantics	193
12.4.2	Operational Semantics	195
12.4.3	Denotational Semantics	196
12.5	Lambda Calculus	197
12.6	Lattices and Order	199
12.6.1	Partially Ordered Sets	199
12.6.2	Lattices	201
12.6.3	Complete Partial Orders	202
12.6.4	Recursion	203
12.7	Review Questions	205
12.8	Summary	205
	References	206
13	Computability and Decidability	207
13.1	Introduction	207
13.2	Logicism and Formalism	208
13.3	Decidability	210
13.4	Computability	212
13.5	Computational Complexity	216
13.6	Review Questions	216
13.7	Summary	217
	Reference	218

14	A Short History of Logic	219
14.1	Introduction	219
14.2	Syllogistic Logic	220
14.3	Paradoxes and Fallacies	222
14.4	Stoic Logic	223
14.5	Boole's Symbolic Logic	225
14.5.1	Switching Circuits and Boolean Algebra	227
14.6	Application of Symbolic Logic to Digital Computing	229
14.7	Frege	230
14.8	Review Questions	231
14.9	Summary	232
	References	233
15	Propositional and Predicate Logic	235
15.1	Introduction	235
15.2	Propositional Logic	236
15.2.1	Truth Tables	238
15.2.2	Properties of Propositional Calculus	240
15.2.3	Proof in Propositional Calculus	242
15.2.4	Semantic Tableaux in Propositional Logic	244
15.2.5	Natural Deduction	246
15.2.6	Sketch of Formalization of Propositional Calculus	248
15.2.7	Applications of Propositional Calculus	248
15.2.8	Limitations of Propositional Calculus	250
15.3	Predicate Calculus	250
15.3.1	Sketch of Formalization of Predicate Calculus	253
15.3.2	Interpretation and Valuation Functions	255
15.3.3	Properties of Predicate Calculus	256
15.3.4	Applications of Predicate Calculus	256
15.3.5	Semantic Tableaux in Predicate Calculus	257
15.4	Review Questions	259
15.5	Summary	260
	References	261
16	Advanced Topics in Logic	263
16.1	Introduction	263
16.2	Fuzzy Logic	264
16.3	Temporal Logic	265
16.4	Intuitionist Logic	267
16.5	Undefined Values	269
16.5.1	Logic of Partial Functions	269
16.5.2	Parnas Logic	271
16.5.3	Dijkstra and Undefinedness	272
16.6	Logic and AI	274
16.7	Theorem Provers for Logic	278

16.8	Review Questions	279
16.9	Summary	280
	References.	280
17	Software Engineering Mathematics	283
17.1	Introduction	283
17.2	What Is Software Engineering?.	285
17.3	Early Software Engineering Mathematics	290
17.4	Mathematics in Software Engineering.	293
17.5	Software Inspections and Testing	294
17.6	Process Maturity Models.	295
17.7	Review Questions.	296
17.8	Summary	296
	References.	297
18	Formal Methods	299
18.1	Introduction	299
18.2	Why Should We Use Formal Methods?	302
18.3	Applications of Formal Methods.	303
18.4	Tools for Formal Methods	303
18.5	Approaches to Formal Methods	304
	18.5.1 Model-Oriented Approach	304
	18.5.2 Axiomatic Approach	305
18.6	Proof and Formal Methods	306
18.7	The Future of Formal Methods.	307
18.8	The Vienna Development Method	307
18.9	VDM ⁺ , the Irish School of VDM.	309
18.10	The Z Specification Language.	310
18.11	The B Method.	311
18.12	Predicate Transformers and Weakest Preconditions.	312
18.13	The Process Calculi	312
18.14	The Parnas Way	313
18.15	Usability of Formal Methods	314
18.16	Review Questions.	316
18.17	Summary	317
	References.	317
19	Z Formal Specification Language.	319
19.1	Introduction	319
19.2	Sets.	322
19.3	Relations.	323
19.4	Functions	325
19.5	Sequences	326
19.6	Bags	327
19.7	Schemas and Schema Composition.	328
19.8	Reification and Decomposition	331

19.9	Proof in Z.	332
19.10	Review Questions.	333
19.11	Summary	333
	Reference	334
20	Probability, Statistics and Applications	335
20.1	Introduction	335
20.2	Probability Theory	336
	20.2.1 Laws of Probability	337
	20.2.2 Random Variables	338
20.3	Statistics	342
	20.3.1 Abuse of Statistics	342
	20.3.2 Statistical Sampling	342
	20.3.3 Averages in a Sample	344
	20.3.4 Variance and Standard Deviation.	344
	20.3.5 Bell-Shaped (Normal) Distribution	345
	20.3.6 Frequency Tables, Histograms and Pie Charts.	347
	20.3.7 Hypothesis Testing	348
20.4	Software Reliability	350
	20.4.1 Software Reliability and Defects	351
	20.4.2 Cleanroom Methodology	353
	20.4.3 Software Reliability Models.	353
20.5	Queuing Theory	356
20.6	Review Questions.	358
20.7	Summary	359
	References.	360
	Glossary	361
	Index	365

<http://www.springer.com/978-3-319-44560-1>

Guide to Discrete Mathematics

An Accessible Introduction to the History, Theory, Logic
and Applications

O'Regan, G.

2016, XXI, 368 p. 117 illus., Hardcover

ISBN: 978-3-319-44560-1