

Contents

Preface IX

Introduction 1

1	Boolean Algebra	5
1.1	Boolean Functions of One Variable	5
1.2	Boolean Functions of Two Variables	6
1.3	Boolean Functions of n Variables	8
1.3.1	The Minterm Expansion	9
1.3.2	The Maxterm Expansion	9
1.3.3	The Reed–Muller Expansion	10
1.3.4	The Minimal ESOP Expansion	11
1.4	Linear Functions	11
1.5	Affine Linear Functions	12
1.6	Monotonic Functions	13
1.7	Boolean Derivative	13
1.8	Boolean Decompositions	14
1.9	Exercises for Chapter 1	15
2	Group Theory	17
2.1	Introduction	17
2.2	Permutation Groups	19
2.3	Matrix Groups	21
2.4	Group Generators	22
2.5	Subgroups	23
2.6	Young Subgroups	23
2.7	Sylow p -Subgroups	24
2.8	Cyclic Subgroups	25
2.9	Closing Remarks	25
2.10	Exercises for Chapter 2	26
3	Reversible Computing	29
3.1	Introduction	29
3.2	Reversible Circuits	32
3.3	Conservative Circuits	33

3.4	Monotonic Circuits	34
3.5	Linear Circuits	34
3.6	Affine Linear Circuits	36
3.7	Exchange Gates	37
3.8	SWAP Gates	39
3.9	Affine Exchange Gates	39
3.10	Control Gates	42
3.11	Sylow Circuits	47
3.12	Gate Cost and Logic Depth	49
3.13	Methods of Synthesis	51
3.14	Cosets	52
3.15	Double Cosets	55
3.16	The Synthesis Algorithm	57
3.16.1	Basic Idea of the Algorithm	58
3.16.2	Working Out the Algorithm	60
3.16.3	Results	61
3.17	Variable Ordering	64
3.18	Templates	65
3.19	The Linear Synthesis Algorithm	69
3.20	Preset Bits and Garbage Bits	72
3.20.1	Duplicating Circuit	72
3.20.2	Controlled NOT	73
3.20.3	An Application: the Majority Circuit	74
3.21	Another Application: the Full Adder	77
3.22	Avoiding Garbage	80
3.23	Exercises for Chapter 3	82
4	Low-power Computing	85
4.1	Entropy	85
4.2	Permutation Matrices	88
4.3	Landauer's Theorem	89
4.4	Thermodynamics	90
4.5	An Application: Prototype Chips	93
4.6	Switch Cost	101
4.7	Moore's Law	103
4.8	Quasi-adiabatic Addressing	105
4.9	Exercises for Chapter 4	110
5	Analog Computing	113
5.1	Computing with Real Numbers	113
5.2	Synthesis	115
5.3	An Application: the Color Transform	117
5.4	About Determinants	119
5.5	LIFT Gates versus SCALE Gates	120
5.6	Conclusion	122
5.7	Computations with Complex Numbers	123

5.8	An Application: the Fourier Transform	124
5.9	Nonlinear Computations	126
5.10	Exercises for Chapter 5	130
6	Computing in Modulo 2^b	131
6.1	Addition in Modulo 2^b	131
6.2	Multiplication by a Constant	135
6.3	Scaling by -1	136
6.4	Scaling by $1/2$ or by 2	137
6.5	Lifting	139
6.6	Exercises for Chapter 6	141
7	Quantum Computing	143
7.1	Doubly Stochastic Matrices	143
7.2	Unitary Matrices	144
7.3	Entropy in the Quantum World	147
7.4	Entanglement	148
7.5	Control Circuits and Control Gates	149
7.6	Synthesis	151
7.7	Decomposition	152
7.8	Discussion	154
7.9	Bottom-Up and Top-Down	156
7.10	Bottom-Up Approach	157
7.10.1	One-(Qu)bit Calculations	157
7.10.2	Two-(Qu)bit Calculations	159
7.10.3	Three- and Multi-(Qu)bit Calculations	161
7.11	Top-Down Approach	162
7.12	An Application: the Quantum Fourier Transform	163
7.13	Nonlinear Computations	166
7.14	Exercises for Chapter 7	167
8	Reversible Programming Languages	169
8.1	The if-then-else Structure	170
8.2	The do-until Structure	175
8.3	Exercises for Chapter 8	177
Appendix A The Number of Linear Reversible Circuits		181
Appendix B Bounds for the q-Factorial		183
Appendix C A Theorem about Universal Reversible Gates		185
C.1	Universality in Conventional Logic Circuits	185
C.2	Preliminary Concepts	186
C.3	No-Fan-Out Theorem and Its Consequences	187
C.4	Final Theorem	190
C.5	Discussion	191
C.6	Exercises for Appendix C	192

Appendix D Synthesis Efficiency	193
D.1 Exercises for Appendix D	195
Appendix E Birkhoff's Theorem	197
E.1 Exercises for Appendix E	201
Appendix F Microentropy and Macroentropy	205
F.1 Exercises for Appendix F	207
Appendix G Computing the Successive Powers of a Matrix	209
G.1 Exercises for Appendix G	210
Post Scriptum	211
References	213
Solutions to the Exercises	223
Index	247