

Contents

1	Invitation to Quantum Information Science	1
1.1	From Classical Information Science to Quantum Information Science	1
1.2	Further Expansion of Quantum Information Science	4
1.3	Feedback from Quantum Information Science to Physics	6
1.4	Toward Realization of Quantum Information Processing	8
1.5	Organization of This Book	9
	References	12
2	Quantum Mechanics for Qubit Systems	13
2.1	Preliminary	13
2.2	Preparation	15
2.2.1	Conceptual Preparation: Physical System, State, Measurement of Physical Quantity	15
2.2.2	Notational Preparation: Dirac Notation	16
2.3	Qubit Systems	20
2.3.1	A Qubit System	21
2.3.2	Time Evolution in Qubit System	24
2.3.3	Composition of Qubit Systems: n -Qubit Systems	28
	References	34
3	Foundations on Quantum Computing	37
3.1	What is Computation?	37
3.2	Mathematical Notation for Information Science	40
3.3	Classical Circuit Model	41
3.4	Quantum Circuit Model	45
	References	53
4	Quantum Algorithms	55
4.1	Introduction	55
4.2	Deutsch–Jozsa Algorithm	56

4.3	Grover's Algorithm	59
4.3.1	Construction of Grover's Algorithm	59
4.3.2	Analysis of Success Probability	62
4.3.3	Generalization: Multiple Solutions	64
4.4	Shor's Algorithm.	66
4.4.1	Quantum Algorithm for Period Finding	66
4.4.2	Quantum Algorithm for Factorization	70
4.4.3	Quantum Algorithm for Discrete Logarithm.	72
4.5	Other Quantum Algorithms.	73
	References	73
5	Foundations of Quantum Mechanics and Quantum Information Theory	75
5.1	Introduction	75
5.1.1	Postulates and Preconditions.	76
5.1.2	Hilbert Space and Linear Operators.	77
5.1.3	Dirac Notation II	78
5.2	Postulates for Quantum Mechanics	80
5.2.1	Quantum States, and Measurements of Physical Quantities	81
5.2.2	Time Evolution.	88
5.2.3	Composite Systems	89
5.2.4	Comment on the Measurement Process: State-Changes due to Measurements	91
5.3	Reformulation of Quantum Mechanics	93
5.3.1	General Class of Quantum States	93
5.3.2	General Class of Measurements	107
5.3.3	General Class of Time Evolutions.	115
5.3.4	General Class of Measurement Processes.	119
	References	125
6	Information Quantities in Quantum Systems.	127
6.1	Introduction	127
6.2	Information Quantities in Classical Systems	128
6.2.1	Shannon Entropy	128
6.2.2	Entropy and Typical Sequence	130
6.2.3	Joint Entropy and Conditional Entropy	134
6.2.4	Conditional Probability and Classical Channel	135
6.2.5	Divergence.	136
6.2.6	f -Divergence	138
6.2.7	Mutual Information	141
6.2.8	Concavity and Subadditivity of the Entropy	143
6.2.9	Fano Inequality.	144

6.3	Information Quantities in Quantum Systems	145
6.3.1	Von Neumann Entropy	145
6.3.2	Quantum Relative Entropy	147
6.3.3	Mutual Information in Quantum Systems	149
6.3.4	Concavity and Subadditivity of the von Neumann Entropy	152
6.3.5	Trace Distance	153
6.3.6	Fidelity and Uhlmann's Theorem	155
6.3.7	Properties of Fidelity	158
6.3.8	Entanglement Fidelity	162
	References	165
7	Quantum Entanglement	167
7.1	Introduction	167
7.2	Basic Concepts of Entanglement	168
7.2.1	Quantum and Classical Correlation	168
7.2.2	Product State and Maximally Entangled State	169
7.2.3	Quantum Teleportation	171
7.2.4	Superdense Coding	173
7.3	Quantifying Entanglement	174
7.3.1	Local Operations and Classical Communication (LOCC)	174
7.3.2	Basic Unit of Entanglement	176
7.3.3	Entanglement Concentration	177
7.3.4	Quantum Data Compression	180
7.3.5	Entanglement Dilution	183
7.3.6	Amount of Entanglement	185
7.4	Multipartite Entanglement	186
7.4.1	GHZ and W State	186
7.4.2	Stochastic LOCC	187
7.4.3	Classification of Multipartite Entanglement	188
7.5	Mixed-State Entanglement	190
7.5.1	Entanglement Criteria	190
7.5.2	LOCC on Mixed States	194
7.5.3	Entanglement Measure	196
7.5.4	Entanglement of Formation	197
7.5.5	Relative Entropy of Entanglement	199
7.5.6	Relationship among Entanglement Measures	200
7.5.7	Entanglement Monotone	202
	References	202
8	Classical-Quantum Channel Coding	205
8.1	Introduction	205
8.2	Quantum Hypothesis Testing	206

8.2.1	Problem of Quantum Hypothesis Testing	206
8.2.2	Trace Inequality for Quantum Hypothesis Testing.	208
8.2.3	Asymptotic Theory of Quantum Hypothesis Testing	210
8.2.4	Properties of Relative Rényi Entropy.	213
8.3	Classical-Quantum Channel Coding.	216
8.3.1	Message Transmission Over Quantum Channels	216
8.3.2	Proof of the C-Q Channel Coding Theorem (Converse Part).	219
8.3.3	Proof of the C-Q Channel Coding Theorem (Direct Part).	223
	References	228
9	Quantum Error Correction and Quantum Cryptography	231
9.1	Introduction	231
9.2	Algebraic Error Correction in the Classical System	232
9.2.1	Formulation	232
9.2.2	Evaluation of Error Probability Under Code Ensemble.	236
9.2.3	Examples of Code Ensemble	239
9.2.4	Asymptotic Theory	241
9.2.5	Error Correction with Confidentiality	242
9.3	Quantum Error Correcting Code	246
9.3.1	Pauli Channel	246
9.3.2	Stabilizer Code	247
9.3.3	CSS Code	250
9.3.4	Asymptotic Theory	254
9.4	Application to Quantum Secret Communication	255
9.4.1	Channel to the Environment System	255
9.4.2	Leaked Information Without Privacy Amplification	256
9.4.3	Leaked Information with Privacy Amplification	260
9.5	Application to Quantum Cryptography (Quantum Key Distribution).	264
	References	268
	Appendix A: Foundations of Linear Algebra and Basic Mathematics	269
	Appendix B: Solution for Exercises	305
	Index	327