

Contents

Introduction to the Tenth Anniversary Edition	<i>page xvii</i>
Afterword to the Tenth Anniversary Edition	xix
Preface	xxi
Acknowledgements	xxvii
Nomenclature and notation	xxix
Part I Fundamental concepts	1
1 Introduction and overview	1
1.1 Global perspectives	1
1.1.1 History of quantum computation and quantum information	2
1.1.2 Future directions	12
1.2 Quantum bits	13
1.2.1 Multiple qubits	16
1.3 Quantum computation	17
1.3.1 Single qubit gates	17
1.3.2 Multiple qubit gates	20
1.3.3 Measurements in bases other than the computational basis	22
1.3.4 Quantum circuits	22
1.3.5 Qubit copying circuit?	24
1.3.6 Example: Bell states	25
1.3.7 Example: quantum teleportation	26
1.4 Quantum algorithms	28
1.4.1 Classical computations on a quantum computer	29
1.4.2 Quantum parallelism	30
1.4.3 Deutsch's algorithm	32
1.4.4 The Deutsch–Jozsa algorithm	34
1.4.5 Quantum algorithms summarized	36
1.5 Experimental quantum information processing	42
1.5.1 The Stern–Gerlach experiment	43
1.5.2 Prospects for practical quantum information processing	46
1.6 Quantum information	50
1.6.1 Quantum information theory: example problems	52
1.6.2 Quantum information in a wider context	58

2 Introduction to quantum mechanics	60
2.1 Linear algebra	61
2.1.1 Bases and linear independence	62
2.1.2 Linear operators and matrices	63
2.1.3 The Pauli matrices	65
2.1.4 Inner products	65
2.1.5 Eigenvectors and eigenvalues	68
2.1.6 Adjoints and Hermitian operators	69
2.1.7 Tensor products	71
2.1.8 Operator functions	75
2.1.9 The commutator and anti-commutator	76
2.1.10 The polar and singular value decompositions	78
2.2 The postulates of quantum mechanics	80
2.2.1 State space	80
2.2.2 Evolution	81
2.2.3 Quantum measurement	84
2.2.4 Distinguishing quantum states	86
2.2.5 Projective measurements	87
2.2.6 POVM measurements	90
2.2.7 Phase	93
2.2.8 Composite systems	93
2.2.9 Quantum mechanics: a global view	96
2.3 Application: superdense coding	97
2.4 The density operator	98
2.4.1 Ensembles of quantum states	99
2.4.2 General properties of the density operator	101
2.4.3 The reduced density operator	105
2.5 The Schmidt decomposition and purifications	109
2.6 EPR and the Bell inequality	111
3 Introduction to computer science	120
3.1 Models for computation	122
3.1.1 Turing machines	122
3.1.2 Circuits	129
3.2 The analysis of computational problems	135
3.2.1 How to quantify computational resources	136
3.2.2 Computational complexity	138
3.2.3 Decision problems and the complexity classes P and NP	141
3.2.4 A plethora of complexity classes	150
3.2.5 Energy and computation	153
3.3 Perspectives on computer science	161
Part II Quantum computation	171
4 Quantum circuits	171
4.1 Quantum algorithms	172
4.2 Single qubit operations	174

	<i>Contents</i>	xi
4.3 Controlled operations		177
4.4 Measurement		185
4.5 Universal quantum gates		188
4.5.1 Two-level unitary gates are universal		189
4.5.2 Single qubit and CNOT gates are universal		191
4.5.3 A discrete set of universal operations		194
4.5.4 Approximating arbitrary unitary gates is generically hard		198
4.5.5 Quantum computational complexity		200
4.6 Summary of the quantum circuit model of computation		202
4.7 Simulation of quantum systems		204
4.7.1 Simulation in action		204
4.7.2 The quantum simulation algorithm		206
4.7.3 An illustrative example		209
4.7.4 Perspectives on quantum simulation		211
5 The quantum Fourier transform and its applications		216
5.1 The quantum Fourier transform		217
5.2 Phase estimation		221
5.2.1 Performance and requirements		223
5.3 Applications: order-finding and factoring		226
5.3.1 Application: order-finding		226
5.3.2 Application: factoring		232
5.4 General applications of the quantum Fourier transform		234
5.4.1 Period-finding		236
5.4.2 Discrete logarithms		238
5.4.3 The hidden subgroup problem		240
5.4.4 Other quantum algorithms?		242
6 Quantum search algorithms		248
6.1 The quantum search algorithm		248
6.1.1 The oracle		248
6.1.2 The procedure		250
6.1.3 Geometric visualization		252
6.1.4 Performance		253
6.2 Quantum search as a quantum simulation		255
6.3 Quantum counting		261
6.4 Speeding up the solution of NP-complete problems		263
6.5 Quantum search of an unstructured database		265
6.6 Optimality of the search algorithm		269
6.7 Black box algorithm limits		271
7 Quantum computers: physical realization		277
7.1 Guiding principles		277
7.2 Conditions for quantum computation		279
7.2.1 Representation of quantum information		279
7.2.2 Performance of unitary transformations		281

xii	<i>Contents</i>	
	7.2.3 Preparation of fiducial initial states	281
	7.2.4 Measurement of output result	282
	7.3 Harmonic oscillator quantum computer	283
	7.3.1 Physical apparatus	283
	7.3.2 The Hamiltonian	284
	7.3.3 Quantum computation	286
	7.3.4 Drawbacks	286
	7.4 Optical photon quantum computer	287
	7.4.1 Physical apparatus	287
	7.4.2 Quantum computation	290
	7.4.3 Drawbacks	296
	7.5 Optical cavity quantum electrodynamics	297
	7.5.1 Physical apparatus	298
	7.5.2 The Hamiltonian	300
	7.5.3 Single-photon single-atom absorption and refraction	303
	7.5.4 Quantum computation	306
	7.6 Ion traps	309
	7.6.1 Physical apparatus	309
	7.6.2 The Hamiltonian	317
	7.6.3 Quantum computation	319
	7.6.4 Experiment	321
	7.7 Nuclear magnetic resonance	324
	7.7.1 Physical apparatus	325
	7.7.2 The Hamiltonian	326
	7.7.3 Quantum computation	331
	7.7.4 Experiment	336
	7.8 Other implementation schemes	343
	Part III Quantum information	353
	8 Quantum noise and quantum operations	353
	8.1 Classical noise and Markov processes	354
	8.2 Quantum operations	356
	8.2.1 Overview	356
	8.2.2 Environments and quantum operations	357
	8.2.3 Operator-sum representation	360
	8.2.4 Axiomatic approach to quantum operations	366
	8.3 Examples of quantum noise and quantum operations	373
	8.3.1 Trace and partial trace	374
	8.3.2 Geometric picture of single qubit quantum operations	374
	8.3.3 Bit flip and phase flip channels	376
	8.3.4 Depolarizing channel	378
	8.3.5 Amplitude damping	380
	8.3.6 Phase damping	383

	<i>Contents</i>	xiii
8.4 Applications of quantum operations	386	
8.4.1 Master equations	386	
8.4.2 Quantum process tomography	389	
8.5 Limitations of the quantum operations formalism	394	
9 Distance measures for quantum information	399	
9.1 Distance measures for classical information	399	
9.2 How close are two quantum states?	403	
9.2.1 Trace distance	403	
9.2.2 Fidelity	409	
9.2.3 Relationships between distance measures	415	
9.3 How well does a quantum channel preserve information?	416	
10 Quantum error-correction	425	
10.1 Introduction	426	
10.1.1 The three qubit bit flip code	427	
10.1.2 Three qubit phase flip code	430	
10.2 The Shor code	432	
10.3 Theory of quantum error-correction	435	
10.3.1 Discretization of the errors	438	
10.3.2 Independent error models	441	
10.3.3 Degenerate codes	444	
10.3.4 The quantum Hamming bound	444	
10.4 Constructing quantum codes	445	
10.4.1 Classical linear codes	445	
10.4.2 Calderbank–Shor–Steane codes	450	
10.5 Stabilizer codes	453	
10.5.1 The stabilizer formalism	454	
10.5.2 Unitary gates and the stabilizer formalism	459	
10.5.3 Measurement in the stabilizer formalism	463	
10.5.4 The Gottesman–Knill theorem	464	
10.5.5 Stabilizer code constructions	464	
10.5.6 Examples	467	
10.5.7 Standard form for a stabilizer code	470	
10.5.8 Quantum circuits for encoding, decoding, and correction	472	
10.6 Fault-tolerant quantum computation	474	
10.6.1 Fault-tolerance: the big picture	475	
10.6.2 Fault-tolerant quantum logic	482	
10.6.3 Fault-tolerant measurement	489	
10.6.4 Elements of resilient quantum computation	493	
11 Entropy and information	500	
11.1 Shannon entropy	500	
11.2 Basic properties of entropy	502	
11.2.1 The binary entropy	502	
11.2.2 The relative entropy	504	

11.2.3	Conditional entropy and mutual information	505
11.2.4	The data processing inequality	509
11.3	Von Neumann entropy	510
11.3.1	Quantum relative entropy	511
11.3.2	Basic properties of entropy	513
11.3.3	Measurements and entropy	514
11.3.4	Subadditivity	515
11.3.5	Concavity of the entropy	516
11.3.6	The entropy of a mixture of quantum states	518
11.4	Strong subadditivity	519
11.4.1	Proof of strong subadditivity	519
11.4.2	Strong subadditivity: elementary applications	522
12	Quantum information theory	528
12.1	Distinguishing quantum states and the accessible information	529
12.1.1	The Holevo bound	531
12.1.2	Example applications of the Holevo bound	534
12.2	Data compression	536
12.2.1	Shannon's noiseless channel coding theorem	537
12.2.2	Schumacher's quantum noiseless channel coding theorem	542
12.3	Classical information over noisy quantum channels	546
12.3.1	Communication over noisy classical channels	548
12.3.2	Communication over noisy quantum channels	554
12.4	Quantum information over noisy quantum channels	561
12.4.1	Entropy exchange and the quantum Fano inequality	561
12.4.2	The quantum data processing inequality	564
12.4.3	Quantum Singleton bound	568
12.4.4	Quantum error-correction, refrigeration and Maxwell's demon	569
12.5	Entanglement as a physical resource	571
12.5.1	Transforming bi-partite pure state entanglement	573
12.5.2	Entanglement distillation and dilution	578
12.5.3	Entanglement distillation and quantum error-correction	580
12.6	Quantum cryptography	582
12.6.1	Private key cryptography	582
12.6.2	Privacy amplification and information reconciliation	584
12.6.3	Quantum key distribution	586
12.6.4	Privacy and coherent information	592
12.6.5	The security of quantum key distribution	593
	Appendices	608
	Appendix 1: Notes on basic probability theory	608
	Appendix 2: Group theory	610
A2.1	Basic definitions	610
A2.1.1	Generators	611
A2.1.2	Cyclic groups	611
A2.1.3	Cosets	612

Cambridge University Press

978-1-107-00217-3 - Quantum Computation and Quantum Information, 10th Anniversary Edition

Michael A. Nielsen and Isaac L. Chuang

Table of Contents

[More information](#)

	<i>Contents</i>	xv
A2.2 Representations		612
A2.2.1 Equivalence and reducibility		612
A2.2.2 Orthogonality		613
A2.2.3 The regular representation		614
A2.3 Fourier transforms		615
Appendix 3: The Solovay–Kitaev theorem		617
Appendix 4: Number theory		625
A4.1 Fundamentals		625
A4.2 Modular arithmetic and Euclid’s algorithm		626
A4.3 Reduction of factoring to order-finding		633
A4.4 Continued fractions		635
Appendix 5: Public key cryptography and the RSA cryptosystem		640
Appendix 6: Proof of Lieb’s theorem		645
Bibliography		649
Index		665