

Contents

Preface	XVII
List of Contributors	XIX
I Classical Information Theory	1
1 Classical Information Theory and Classical Error Correction (<i>M. Grassl</i>)	3
1.1 Introduction	3
1.2 Basics of Classical Information Theory	3
1.2.1 Abstract communication system	3
1.2.2 The discrete noiseless channel	4
1.2.3 The discrete noisy channel	6
1.3 Linear Block Codes	9
1.3.1 Repetition code	9
1.3.2 Finite fields	11
1.3.3 Generator and parity check matrix	12
1.3.4 Hamming codes	14
1.4 Further Aspects	15
References	16
2 Computational Complexity (<i>S. Mertens</i>)	17
2.1 Basics	17
2.2 Algorithms and Time Complexity	19
2.3 Tractable Trails: The Class P	20
2.4 Intractable Itineraries: The class NP	21
2.4.1 Coloring graphs	25
2.4.2 Logical truth	26
2.5 Reductions and NP -completeness	27
2.6 P vs. NP	29
2.7 Optimization	31
2.8 Complexity Zoo	34
References	35

II	Foundation of Quantum Information Theory	37
3	Discrete Quantum States versus Continuous Variables	
	<i>(J. Eisert)</i>	39
3.1	Introduction	39
3.2	Finite-dimensional quantum systems	40
	3.2.1 Quantum states	40
	3.2.2 Quantum operations	41
3.3	Continuous-variables	43
	3.3.1 Phase space	43
	3.3.2 Gaussian states	45
	3.3.3 Gaussian unitaries	46
	3.3.4 Gaussian channels	47
	3.3.5 Gaussian measurements	49
	3.3.6 Non-Gaussian operations	51
	References	52
4	Approximate Quantum Cloning	
	<i>(D. Bruß and C. Macchiavello)</i>	53
4.1	Introduction	53
4.2	The No-Cloning Theorem	53
4.3	State-Dependent Cloning	54
4.4	Phase Covariant Cloning	62
4.5	Universal Cloning	63
	4.5.1 The case of qubits	63
	4.5.2 Higher dimensions	66
	4.5.3 Entanglement structure	67
4.6	Asymmetric Cloning	67
4.7	Probabilistic Cloning	68
4.8	Experimental Quantum Cloning	68
4.9	Summary and Outlook	69
	References	70
5	Channels and Maps	
	<i>(M. Keyl and R. F. Werner)</i>	73
5.1	Introduction	73
5.2	Completely Positive Maps	73
5.3	The Jamiolkowski Isomorphism	76
5.4	The Stinespring Dilation Theorem	78
5.5	Classical Systems as a Special Case	82
5.6	Examples	83
	5.6.1 The ideal quantum channel	83
	5.6.2 The depolarizing channel	83
	5.6.3 Entanglement breaking channels	84
	5.6.4 Covariant channels	84
	References	86

6 Quantum Algorithms

(*J. Kempe*)

	87
6.1 Introduction	87
6.2 Precursors	88
6.2.1 Deutsch’s algorithm	89
6.2.2 Deutsch–Josza algorithm	90
6.2.3 Simon’s algorithm	92
6.3 Shor’s Factoring Algorithm	93
6.3.1 Reduction from factoring to period finding	93
6.3.2 Implementation of the QFT	94
6.3.3 Shor’s algorithm for period finding	95
6.4 Grover’s Algorithm	96
6.5 Other Algorithms	97
6.5.1 The hidden subgroup problem	97
6.5.2 Search algorithms	98
6.5.3 Other algorithms	99
6.6 Recent Developments	99
6.6.1 Quantum walks	99
6.6.2 Adiabatic quantum algorithms	100
References	102

7 Quantum Error Correction

(*M. Grassl*)

	105
7.1 Introduction	105
7.2 Quantum Channels	105
7.3 Using Classical Error-Correcting Codes	109
7.3.1 Negative results: the quantum repetition code	109
7.3.2 Positive results: a simple three-qubit code	110
7.3.3 Shor’s nine-qubit code	112
7.3.4 Steane’s seven-qubit code and CSS codes	114
7.3.5 The five-qubit code and stabilizer codes	116
7.4 Further Aspects	118
References	119

III Theory of Entanglement

8 The Separability versus Entanglement Problem

(*A. Sen(De), U. Sen, M. Lewenstein, and A. Sanpera*)

	123
8.1 Introduction	123
8.2 Bipartite Pure States: Schmidt Decomposition	123
8.3 Bipartite Mixed States: Separable and Entangled States	124
8.4 Operational Entanglement Criteria	125
8.4.1 Partial transposition	125
8.4.2 Majorization	127

8.5	Nonoperational Entanglement Criteria	128
8.5.1	Entanglement witnesses	128
8.5.2	Positive maps	131
8.6	Bell Inequalities	135
8.7	Classification of Bipartite States with Respect to Quantum Dense Coding	138
8.7.1	The Holevo bound	139
8.7.2	Capacity of quantum dense coding	140
8.8	Further Reading: Multipartite States	142
	References	143
9	Entanglement Theory with Continuous Variables	
	<i>(P. van Loock)</i>	147
9.1	Introduction	147
9.2	Phase-Space Description	149
9.3	Entanglement of Gaussian States	149
9.3.1	Gaussian states	150
9.3.2	Gaussian operations	151
9.3.3	Pure entangled Gaussian states	152
9.3.4	Mixed entangled Gaussian states and inseparability criteria	154
9.4	More on Gaussian Entanglement	157
	References	159
10	Entanglement Measures	
	<i>(M. B. Plenio and S. S. Virmani)</i>	161
10.1	Introduction	161
10.2	Manipulation of Single Systems	163
10.3	Manipulation in the Asymptotic Limit	164
10.4	Postulates for Axiomatic Entanglement Measures: Uniqueness and Extremality Theorems	166
10.5	Examples of Axiomatic Entanglement Measures	169
	References	174
11	Purification and Distillation	
	<i>(W. Dür and H.-J. Briegel)</i>	177
11.1	Introduction	177
11.2	Pure States	179
11.2.1	Bipartite systems	179
11.2.2	Multipartite systems	180
11.3	Distillability and Bound Entanglement in Bipartite Systems	181
11.3.1	Distillable entanglement and yield	181
11.3.2	Criteria for entanglement distillation	182
11.4	Bipartite Entanglement Distillation Protocols	184
11.4.1	Filtering protocol	184
11.4.2	Recurrence protocols	185
11.4.3	$N \rightarrow M$ protocols, hashing, and breeding	190

- 11.5 Distillability and Bound Entanglement in Multipartite systems 192
 - 11.5.1 *n*-party distillability 192
 - 11.5.2 *m*-party distillability with respect to coarser partitions 192
 - 11.5.3 Bound entanglement in multipartite systems 193
- 11.6 Entanglement Purification Protocols in Multipartite Systems 193
 - 11.6.1 Graph states 194
 - 11.6.2 Recurrence protocol 194
 - 11.6.3 Hashing protocol 196
 - 11.6.4 Entanglement purification of nonstabilizer states 197
- 11.7 Distillability with Noisy Apparatus 197
 - 11.7.1 Distillable entanglement and yield 197
 - 11.7.2 Error model 198
 - 11.7.3 Bipartite recurrence protocols 199
 - 11.7.4 Multipartite recurrence protocols 200
 - 11.7.5 Hashing protocols 201
- 11.8 Applications of Entanglement Purification 202
 - 11.8.1 Quantum communication and cryptography 202
 - 11.8.2 Secure state distribution 203
 - 11.8.3 Quantum error correction 203
 - 11.8.4 Quantum computation 204
- 11.9 Summary and Conclusions 205
 - References 206

12 Bound Entanglement

(Paweł Horodecki)

209

- 12.1 Introduction 209
- 12.2 Distillation of Quantum Entanglement: Repetition 209
 - 12.2.1 Bipartite entanglement distillation 209
 - 12.2.2 Multipartite entanglement distillation 212
- 12.3 Bound Entanglement—Bipartite Case 213
 - 12.3.1 Bound entanglement—the phenomenon 213
 - 12.3.2 Bound entanglement and entanglement measures.
 - Asymptotic irreversibility 215
 - 12.3.3 Which states are bound entangled ? 216
 - 12.3.4 Applications in single copy case 219
 - 12.3.5 Applications in asymptotic regime 221
- 12.4 Bound Entanglement: Multipartite Case 225
 - 12.4.1 Which multipartite states are bound entangled? 225
 - 12.4.2 Activation effects 227
 - 12.4.3 Remote quantum information concentration 228
 - 12.4.4 Violation of Bell inequalities and communication complexity
 - reduction 228
 - 12.4.5 Feedback to classical theory: multipartite bound information and its
 - activation 229
 - 12.4.6 Bound entanglement and multiparty quantum channels 230

12.5	Further Reading: Continuous Variables	230
	References	231
13	Multiparticle Entanglement	
	<i>(J. Eisert and D. Gross)</i>	237
13.1	Introduction	237
13.2	Pure States	238
	13.2.1 Classifying entanglement of single specimens	238
	13.2.2 Asymptotic manipulation of multiparticle quantum states	241
13.3	Mixed States	243
	13.3.1 Classifying mixed state entanglement	243
	13.3.2 Methods of detection	245
13.4	Quantifying Multiparticle Entanglement	246
13.5	Stabilizer States and Graph States	247
13.6	Applications of Multiparticle Entangled States	249
	References	250
IV	Quantum Communication	253
14	Quantum Teleportation	
	<i>(L. C. Dávila Romero and N. Korolkova)</i>	255
14.1	Introduction	255
	14.1.1 Setting up the problem and the role of entanglement	255
	14.1.2 A template for quantum teleportation	257
	14.1.3 Efficiency and fidelity	259
14.2	Experimental Realization	260
	14.2.1 The first quantum teleportation experiment	261
	14.2.2 Further experiments	262
14.3	Continuous Variables—Concept and Extension	263
	References	268
15	Theory of Quantum Key Distribution (QKD)	
	<i>(N. Lütkenhaus)</i>	271
15.1	Introduction	271
15.2	Classical Background to QKD	271
15.3	Ideal QKD	272
15.4	Idealized QKD in noisy environment	275
15.5	Realistic QKD in noisy and lossy environment	277
15.6	Improved Schemes	280
15.7	Improvements in Public Discussion	282
15.8	Conclusion	283
	References	283

16 Quantum Communication Experiments with Discrete Variables	285
<i>(H. Weinfurter)</i>	
16.1 Aunt Martha	285
16.2 Quantum Cryptography	286
16.2.1 Faint pulse QKD	286
16.2.2 Entanglement-Based QKD—Single Photon QKD	290
16.3 Entanglement-Based Quantum Communication	292
16.3.1 Quantum Dense Coding	292
16.3.2 Error Correction	293
16.4 Conclusion	295
References	295
17 Continuous Variable Quantum Communication	297
<i>(U. L. Andersen and G. Leuchs)</i>	
17.1 Introduction	297
17.2 Continuous Variable Quantum Systems	297
17.3 Tools for State Manipulation	300
17.3.1 Gaussian transformations	300
17.3.2 Homodyne detection and feed forward	303
17.3.3 Non-Gaussian transformations	303
17.4 Quantum Communication Protocols	304
17.4.1 Quantum dense coding	305
17.4.2 Quantum key distribution	306
17.4.3 Long distance communication	308
References	310
V Quantum Computing: Concepts	313
18 Requirements for a Quantum Computer	315
<i>(A. Ekert and A. Kay)</i>	
18.1 Classical World of Bits and Probabilities	315
18.1.1 Parallel composition = tensor products	318
18.1.2 Sequential composition = matrix products	319
18.2 Logically Impossible Operations?	320
18.3 Quantum World of Probability Amplitudes	323
18.4 Interference Revisited	326
18.5 Tools of the Trade	328
18.5.1 Quantum states	328
18.5.2 Unitary operations	331
18.5.3 Quantum measurements	334
18.6 Composite Systems	335
18.6.1 Density operators	340
18.7 Quantum Circuits	341
18.7.1 Economy of resources	342

18.7.2	Computations	344
18.8	Summary	346
19	Probabilistic Quantum Computation and Linear Optical Realizations	
	<i>(N. Lütkenhaus)</i>	349
19.1	Introduction	349
19.2	Gottesman/Chuang Trick	349
19.3	Optical Background	351
19.3.1	Optical qubits	351
19.3.2	Linear Optics Framework	352
19.4	Knill–Laflamme–Milburn (KLM) scheme	353
19.4.1	Extension of Gottesman–Chuang trick	353
19.4.2	Implementation with linear optics	355
19.4.3	Offline probabilistic gates	356
	References	358
20	One-way Quantum Computation	
	<i>(D.E. Browne and H.J. Briegel)</i>	359
20.1	Introduction	359
20.1.1	Cluster states and graph states	360
20.1.2	Single-qubit measurements and rotations	360
20.2	Simple examples	361
20.2.1	Connecting one-way patterns - arbitrary single-qubit operations	362
20.2.2	Graph states as a resource	364
20.2.3	Two-qubit gates	364
20.2.4	Cluster-state quantum computing	364
20.3	Beyond quantum circuit simulation	365
20.3.1	Stabilizer formalism	365
20.3.2	A logical Heisenberg picture	366
20.3.3	Dynamical variables on a stabilizer sub-space	367
20.3.4	One-way patterns in the stabilizer formalism	368
20.3.5	Pauli measurements	368
20.3.6	Pauli measurements and the Clifford group	370
20.3.7	Non-Pauli measurements	371
20.3.8	Diagonal unitaries	371
20.3.9	Gate patterns beyond the standard network model –CD-decomposition	373
20.4	Implementations	374
20.4.1	Optical lattices	374
20.4.2	Linear optics and cavity QED	375
20.5	Recent developments	376
20.6	Outlook	376
	References	378

21 Holonomic Quantum Computation	381
<i>(A.C.M. Carollo and Vlatko Vedral)</i>	
21.1 Geometric Phase and Holonomy	381
21.1.1 Adiabatic implementation of holonomies	382
21.2 Application to Quantum Computation	384
21.2.1 Example	385
References	386
VI Quantum Computing: Implementations	389
22 Quantum Computing with Cold Ions and Atoms: Theory	391
<i>(D. Jaksch, J.J. García-Ripoll, J.I. Cirac, and Peter Zoller)</i>	
22.1 Introduction	391
22.2 Trapped Ions	391
22.2.1 Motional degrees of freedom	392
22.2.2 Internal degrees of freedom and atom–laser interaction	393
22.2.3 Lamb–Dicke limit and sideband transitions	393
22.2.4 Single-qubit operations and state measurement	394
22.2.5 The gate Cirac–Zoller ’95	395
22.2.6 Optimal gates based on quantum control	397
22.3 Trapped Neutral Atoms	401
22.3.1 Optical lattices	401
22.3.2 The (Bose) Hubbard Hamiltonian	406
22.3.3 Loading schemes	408
22.3.4 Quantum computing in optical lattices	408
References	420
23 Quantum Computing Experiments with Cold Trapped Ions	423
<i>(F. Schmidt-Kaler)</i>	
23.1 Introduction	423
23.2 Paul Traps	425
23.2.1 Stability diagram of dynamic trapping	426
23.2.2 3D confinement in a linear Paul trap	427
23.3 Ion crystals and their normal modes	428
23.3.1 Lagrangian of the ion motion in the trap	428
23.3.2 Eigenmodes	430
23.4 Ion–light interaction	432
23.5 Levels and Transitions for Typical Qubit Candidates	433
23.6 Various Two-Qubit Gates	434
23.6.1 The Cirac and Zoller scheme 1995	434
23.6.2 Experimental realization of the Cirac and Zoller gate	435
23.6.3 The Sørensen and Mølmer scheme	436
23.6.4 The Jonathan, Plenio, and Knight scheme	439
23.6.5 Geometric phase shift gates	440

23.6.6	The Mintert and Wunderlich gate proposal	442
23.6.7	Gate proposals based on the interaction of ions with a common optical mode	442
23.7	Teleportation	443
23.8	Segmented Traps and Future Directions	444
	References	447
24	Quantum Computing with Solid State Systems	
	<i>(G. Burkard and D. Loss)</i>	451
24.1	Introduction	451
24.2	Concepts	452
24.2.1	The exchange coupling	452
24.2.2	Anisotropic exchange	454
24.2.3	Universal QC with the exchange coupling	456
24.2.4	Adiabaticity	458
24.3	Electron Spin Qubits	458
24.3.1	Quantum dots	459
24.3.2	Exchange in laterally coupled QDs	459
24.3.3	Semiconductor microcavities	466
24.3.4	Decoherence	467
24.4	Superconducting Qubits	469
24.4.1	Regimes of operation	469
24.4.2	Decoherence, visibility, and leakage	470
	References	478
25	Quantum Computing Implemented via Optimal Control: Theory and Application to Spin and Pseudo-Spin Systems	
	<i>(T. Schulte-Herbrüggen, A. K. Spörl, R. Marx, N. Khaneja, J. M. Myers, A. F. Fahmy, and S. J. Glaser)</i>	481
25.1	Introduction	481
25.2	From Controllable Spin Systems to Suitable Molecules	483
25.2.1	Reachability and controllability	483
25.2.2	Molecular hardware for quantum computation	483
25.3	Scalability	485
25.3.1	Scaling problem with pseudo-pure states	485
25.3.2	Approaching pure states	485
25.3.3	Scalable quantum computing on thermal ensembles	486
25.4	Control Theory for Spin- and Pseudo-Spin Systems	487
25.5	Applied Quantum Control	492
25.5.1	Regime of fast local controls: the NMR limit	492
25.5.2	Regime of finite local controls: beyond NMR	494
25.6	Conclusions	495
25.6.1	Ensemble quantum computing	495
25.6.2	From gate-complexity to time-complexity by optimal control	495
25.6.3	Beyond NMR spin systems	496
	References	498

VII Transfer of Quantum Information Between Different Types of Implementations	503
26 Quantum Repeater	
<i>(W. Dür, H.-J. Briegel, and P. Zoller)</i>	505
26.1 Introduction	505
26.2 Concept of the quantum repeater	507
26.2.1 Entanglement purification	507
26.2.2 Connection of elementary pairs	507
26.2.3 Nested purification loops	508
26.2.4 Resources	509
26.3 Proposals for Experimental Realization	511
26.3.1 Photons and cavities	512
26.3.2 Atomic ensembles	512
26.3.3 Quantum dots	512
26.4 Summary and Conclusions	513
References	513
27 Quantum Interface Between Light and Atomic Ensembles	
<i>(E. S. Polzik and J. Fiurášek)</i>	515
27.1 Introduction	515
27.2 Off-Resonant Interaction of Light with Atomic Ensemble	516
27.3 Entanglement of Two Atomic Clouds	524
27.4 Quantum Memory for Light	526
27.5 Multiple Passage Protocols	528
27.6 Atoms-light teleportation and entanglement swapping	531
27.7 Quantum Cloning into Atomic Memory	532
27.8 Summary	534
References	534
28 Cavity Quantum Electrodynamics: Quantum Information Processing with Atoms and Photons	
<i>(J.-M. Raimond and G. Rempe)</i>	537
28.1 Introduction	537
28.2 Microwave Cavity Quantum Electrodynamics	538
28.3 Optical Cavity Quantum Electrodynamics	543
28.4 Conclusions and Outlook	549
References	550
29 Quantum Electrodynamics of a Qubit	
<i>(G. Alber and G. M. Nikolopoulos)</i>	555
29.1 Quantum Electrodynamics of a Qubit in a Spherical Cavity	556
29.1.1 The model	556
29.1.2 Mode structure of the free radiation field in a spherical cavity	558
29.1.3 Dynamics of spontaneous photon emission	559

29.2	Suppression of Radiative Decay of a Qubit in a Photonic Crystal	564
29.2.1	Photonic crystals and associated density of states	564
29.2.2	“Photon + atom” bound states	566
29.2.3	Beyond the two-level approximation	567
29.2.4	Exercises	568
	References	570
VIII	Towards Quantum Technology Applications	573
30	Quantum Interferometry	
	<i>(O. Glöckl, U. L. Andersen, and G. Leuchs)</i>	575
30.1	Introduction	575
30.2	The Interferometer	576
30.2.1	Sensitivity	577
30.3	Interferometer with Coherent States of Light	579
30.3.1	Geometrical visualization	579
30.4	Interferometer with Squeezed States of Light	581
30.4.1	Interferometer operating with a coherent state and a squeezed vacuum state	581
30.4.2	Interferometer operating with two bright squeezed states	584
30.4.3	Interferometer operating with a bright squeezed state and a squeezed vacuum state	585
30.5	Summary and Discussion	587
	References	589
31	Quantum Imaging	
	<i>(C. Fabre and N. Treps)</i>	591
31.1	Introduction	591
31.2	The Quantum Laser Pointer	592
31.3	Manipulation of Spatial Quantum Noise	593
31.3.1	Observation of pure spatial quantum correlations in parametric down conversion	594
31.3.2	Noiseless image parametric amplification	595
31.4	Two-Photon Imaging	595
31.5	Other Topics in Quantum Imaging	597
31.6	Conclusion and Perspectives	598
	References	598
Index		601