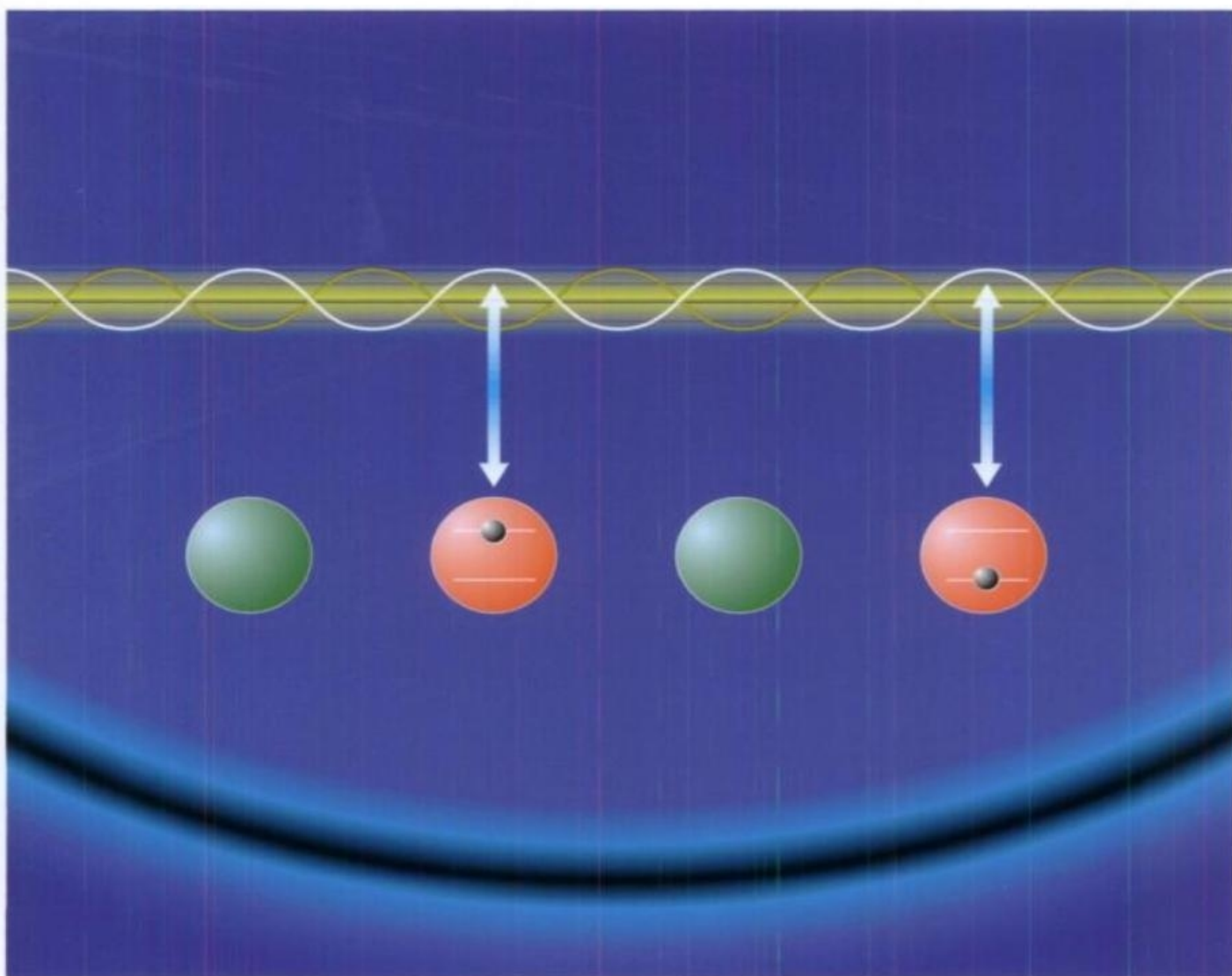


Edited by
Dagmar Bruß and Gerd Leuchs

 WILEY-VCH

Lectures on Quantum Information



Lectures on Quantum Information

Edited by

Dagmar Bruß and Gerd Leuchs

1807–2007 Knowledge for Generations

Each generation has its unique needs and aspirations. When Charles Wiley first opened his small printing shop in lower Manhattan in 1807, it was a generation of boundless potential searching for an identity. And we were there, helping to define a new American literary tradition. Over half a century later, in the midst of the Second Industrial Revolution, it was a generation focused on building the future. Once again, we were there, supplying the critical scientific, technical, and engineering knowledge that helped frame the world. Throughout the 20th Century, and into the new millennium, nations began to reach out beyond their own borders and a new international community was born. Wiley was there, expanding its operations around the world to enable a global exchange of ideas, opinions, and know-how.

For 200 years, Wiley has been an integral part of each generation's journey, enabling the flow of information and understanding necessary to meet their needs and fulfill their aspirations. Today, bold new technologies are changing the way we live and learn. Wiley will be there, providing you the must-have knowledge you need to imagine new worlds, new possibilities, and new opportunities.

Generations come and go, but you can always count on Wiley to provide you the knowledge you need, when and where you need it!



William J. Pesce
President and Chief Executive Officer



Peter Booth Wiley
Chairman of the Board

Lectures on Quantum Information

Edited by
Dagmar Bruß and Gerd Leuchs



WILEY-VCH Verlag GmbH & Co. KGaA

The Editors

Prof. Dr. Dagmar Bruß

Heinrich-Heine-Universität Düsseldorf
Inst. f. Theoret. Physik III
Universitätsstr. 1
40225 Düsseldorf

Prof. Dr. Gerd Leuchs

Institut für Optik, Information und Photonik
Universität Erlangen - Nürnberg
Günther-Scharowsky-Str. 1
91058 Erlangen

Cover

Peter Hesse, Berlin

All books published by Wiley-VCH are carefully produced. Nevertheless, authors, editors, and publisher do not warrant the information contained in these books, including this book, to be free of errors. Readers are advised to keep in mind that statements, data, illustrations, procedural details or other items may inadvertently be inaccurate.

Library of Congress Card No.:

applied for

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.d-db.de>.

© 2007 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

All rights reserved (including those of translation into other languages). No part of this book may be reproduced in any form – by photoprinting, microfilm, or any other means – nor transmitted or translated into a machine language without written permission from the publishers. Registered names, trademarks, etc. used in this book, even when not specifically marked as such, are not to be considered unprotected by law.

Printing betz-druck GmbH, Darmstadt

Binding Litges & Dopf Buchbinderei GmbH, Heppenheim

Printed in the Federal Republic of Germany
Printed on acid-free paper

ISBN 978-3-527-40527-5

Contents

Preface	XVII
List of Contributors	XIX
I Classical Information Theory	1
1 Classical Information Theory and Classical Error Correction	3
(M. Grassl)	
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	17
(S. Mertens)	
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	39
	<i>(J. Eisert)</i>	
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	53
	<i>(D. Bruß and C. Macchiavello)</i>	
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	73
	<i>(M. Keyl and R. F. Werner)</i>	
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**121****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

<i>(H. Weinfurter)</i>	285
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

<i>(U. L. Andersen and G. Leuchs)</i>	297
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**

<i>(A. Ekert and A. Kay)</i>	315
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*(A.C.M. Carollo and Vlatko Vedral)* **381**

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***(D. Jaksch, J.J. García-Ripoll, J.I. Cirac, and Peter Zoller)* **391**

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*(F. Schmidt-Kaler)* **423**

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 Mölmer 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

(W. Dür, H.-J. Briegel, and P. Zoller) **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

(E. S. Polzik and J. Fiurášek) **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

(J.-M. Raimond and G. Rempe) **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

(G. Alber and G. M. Nikolopoulos) **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 575 (*O. Glöckl, U. L. Andersen, and G. Leuchs*)

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 591 (*C. Fabre and N. Treps*)

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

Preface

Quantum information processing and quantum communication has developed into a very active field in the last decade. A number of countries devote sizeable funding to the topic and several books were already published in the field. Why yet another book? We think that the answer is obvious: this book is special. The starting point was a week-long summer school on quantum computing and related topics, funded by the Heraeus Foundation and held in 2000 in the Physikzentrum at Bad Honnef near Bonn, Germany. It was at the time when quantum information in Germany was picking up momentum. About 80 students enjoyed the exciting and stimulating atmosphere, studying the modern topic in the old mansion. The barrel vault basement had sufficient supplies of beer and wine to fuel night long discussions of some hard-liners on the topics of the day: Can one really do quantum computation with NMR although the density matrix is separable? Are there many algorithms for which a quantum computer, once it is built, will outcompete standard Turing machine type computers? The classical Toffoli gate can copy one input channel to two output channels, a perfect cloner; what is the corresponding operation for the quantum version of the Toffoli gate? Can one be sure that factorization is as hard and complex a problem as security agents like to make us believe? Are the coherent states of light, emitted by standard lasers, “quantum” enough to be a worth while resource for quantum communication?

This special, very enjoyable, and fruitful school atmosphere triggered a process which ultimately led to putting together this book to which most of the lecturers have contributed a section. We approached a few additional distinguished colleagues and they also agreed to provide a section. During the school it had turned out that one of the participants had detailed knowledge about a topic that was not covered by the lecturers, and he was talked into giving an improvised lecture which turned out to be a great success. This lecture is also included. Each of the lectures is self-contained and written in a tutorial style, at the same time providing insight into today’s hot topics in quantum information. We hope that this book covers an unusually wide spectrum of quantum information themes, and that the reader may benefit from its diversity and variety.

In all the excitement there is also sadness. Last year Thomas Beth, one of the prominent lecturers at the school and always in the midst of the most intense discussions, lost his brave fight against cancer and died much too young. Friends and foes concede that he deserves the credit for pioneering quantum information in Germany. After studying mathematics and medicine and receiving a chair in computer sciences he may have been burning the candle from both ends. Thomas Beth achieved so much and yet could not sit still in view of the many things out there to discover. We miss him and dedicate this book to his memory.

Dagmar Bruß and Gerd Leuchs

Düsseldorf and Erlangen, May 2006

List of Contributors

Gernot Alber *Chap. 29*

Institut für Angewandte Physik
Technische Universität Darmstadt
64289 Darmstadt
Germany
gernot.alber@physik.tu-darmstadt.de

Ulrik L. Andersen *Chap. 17, 30*

Institut für Optik, Information und Photonik
Max-Planck Forschungsgruppe
Universität Erlangen-Nürnberg
Günther-Scharowsky-Str. 1
91058 Erlangen
Germany
andersen@kerr.physik.uni-erlangen.de

Hans-J. Briegel *Chap. 11, 20, 26*

Institute for Theoretical Physics
University of Innsbruck
Technikerstr. 25
6020 Innsbruck
Austria
hans.briegel@uibk.ac.at

Daniel E. Browne *Chap. 20*

Departments of Materials and Physics
Oxford University
Parks Road
Oxford OX1 3PH
UK
daniel.browne@merton.ox.ac.uk

Dagmar Bruß *Chap. 4*

Institut für Theoretische Physik III
Heinrich-Heine-Universität Düsseldorf
Universitätsstr. 1
40225 Düsseldorf
Germany
bruss@thphy.uni-duesseldorf.de

Guido Burkard *Chap. 24*

Department of Physics and Astronomy
University of Basel
Klingelbergstr. 82
4056 Basel
Switzerland
Guido.Burkard@unibas.ch

Angelo C. M. Carollo *Chap. 21*

Centre for Quantum Computation Department
of Applied Mathematics and Theoretical Physics
(DAMTP)
University of Cambridge
Wilberforce Road
Cambridge CB3 0WA
UK
Angelo.Carollo@uibk.ac.at

J. Ignazio Cirac *Chap. 22*

Max-Planck-Institut für Quantenoptik
Hans-Kopfermann-Str. 1
85748 Garching
Germany
Ignacio.Cirac@mpq.mpg.de

Luciana C. Dávila Romero *Chap. 14*

School of Physics and Astronomy
University of St Andrews
North Haugh
ST. Andrews KY16 9SS
UK
lcdr@st-andrews.ac.uk

Wolfgang Dür *Chap. 11, 26*

Institut für Theoretische Physik
Universität Innsbruck
Technikerstr. 25
6020 Innsbruck
Austria
wolfgang.duer@uibk.ac.at

Jens Eisert *Chap. 3, 13*

Blackett Laboratory
Imperial College London
London SW7 2BW
UK
j.eisert@imperial.ac.uk

Artur Ekert *Chap. 18*

Department of Applied Mathematics and Theoretical Physics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WA
UK
artur.ekert@qubit.org

Claude Fabre *Chap. 31*

Laboratoire Kastler Brossel
University Pierre et Marie Curie
Campus Jussieu, Case 74
75252 Paris Cedex 05
France
fabre@spectro.jussieu.fr

Amr F. Fahmy *Chap. 25*

Biological Chemistry and Molecular Pharmacology
Harvard Medical School
240 Longwood Avenue
Boston, MA 02115
USA
amr_fahmy@hms.harvard.edu

Jaromír Fiurásek *Chap. 27*

Department of Optics
Palacký University
17, listopadu 50
77200 Olomouc
Czech Republic
fiurasek@optics.upol.cz

Juan José García-Ripoll *Chap. 22*

Max-Planck-Institut für Quantenoptik
Hans-Kopfermann-Str. 1
85748 Garching
Germany
Juan.Ripoll@mpq.mpg.de

Steffen J. Glaser *Chap. 25*

Department Chemie
Technische Universität München
Lichtenbergstr. 4
85747 Garching
Germany
glaser@ch.tum.de

Oliver Glöckl *Chap. 30*

Institut für Optik, Information und Photonik
Max-Planck Forschungsgruppe
Universität Erlangen-Nürnberg
Günther-Scharowsky-Str. 1
91058 Erlangen
Germany
oliver.gloeckl@anu.edu.au

Markus Grassl *Chap. 1, 7*

Institut für Algorithmen und Kognitive Systeme
(IAKS)
Fakultät für Informatik
Universität Karlsruhe (TH)
Postfach 6980
76128 Karlsruhe
Germany
grassl@ira.uka.de

David Gross *Chap. 13*

Institute of Physics
University of Potsdam
14469 Potsdam
Germany
davis.gross@imperial.ac.uk

Pawel Horodecki *Chap. 12*

Technical University of Gdansk
ul. Narutowicza 11/12
80-952 Gdansk Wrzeszcz
Poland
pawel@mifgate.mif.pg.gda.pl

D. Jaksch *Chap. 22*

Clarendon Laboratory
University of Oxford
Parks Road
Oxford OX1 3PU
UK
Dieter.Jaksch@physics.ox.ac.uk

Alastair Kay *Chap. 18*

Department of Applied Mathematics and Theoretical Physics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WA
UK
a.s.kay@damtp.cam.ac.uk

Julia Kempe *Chap. 6*

CNRS-LRI UMR 8623
Université de Paris-Sud
91405 Orsay
France
kempe@lri.fr

Michael Keyl *Chap. 5*

QUIT Group of the INFN
Unità di Pavia, Dipartimento di Fisica "A. Volta"
Via Bassi 6
27100 Pavia
Italy
M.Keyl@tu-bs.de

Navin Khaneja *Chap. 25*

Division of Engineering and Applied Sciences
Harvard University
33, Oxford Street
Cambridge, MA
USA
navin@hrl.harvard.edu

Natalia Korolkova *Chap. 14*

School of Physics and Astronomy
University of St Andrews
North Haugh
ST. Andrews KY16 9SS
UK
nvk@st-andrews.ac.uk

Gerd Leuchs *Chap. 17, 30*

Institut für Optik
Information und Photonik
Max-Planck Forschungsgruppe
Universität Erlangen-Nürnberg
Günther-Scharowsky-Str. 1
91058 Erlangen
Germany
leuchs@physik.uni-erlangen.de

Maciej Lewenstein Chap. 8

ICREA and ICFO-Institut de Ciències Fotòniques
Mediterranean Technology Park
08860 Castelldefels, Barcelona
Spain
Maciej.Lewenstein@icfo.es

Daniel Loss Chap. 24

Department of Physics and Astronomy
University of Basel
Klingelbergstr. 82
4056 Basel
Switzerland
Daniel.Loss@unibas.ch

Norbert Lütkenhaus Chap. 19

University of Waterloo
200 University Avenue W.
Waterloo, ON N2L 3G1
Canada
nlutkenhaus@iqc.ca

Chiara Macchiavello Chap. 4

QUIT Group of the INFN
Unità di Pavia
Dipartimento di Fisica “A. Volta”
Via Bassi 6
27100 Pavia
Italy
chiara@unipv.it

Raimund Marx Chap. 25

Department Chemie
Technische Universität München
Lichtenbergstr. 4
85747 Garching
Germany
Raimund.Marx@ch.tum.de

Stephan Mertens Chap. 2

Institut für Theoretische Physik
Otto-von-Guericke-Universität Magdeburg
Postfach 4120
39016 Magdeburg
Germany
Stephan.Mertens@Physik.Uni-Magdeburg.DE

John M. Myers Chap. 25

Harvard University
Gordon McKay Laboratory
Division of Engineering and Applied Sciences
Cambridge, MA 02138
USA
myers@deas.harvard.edu

Georgios M. Nikolopoulos Chap. 29

Institut für Angewandte Physik
Technische Universität Darmstadt
64289 Darmstadt
Germany
nikolg@physik.tu-darmstadt.de

Martin B. Plenio Chap. 10

QOLS, Blackett Laboratory
Imperial College London
Prince Consort Road
London SW7 2BW
UK
m.plenio@imperial.ac.uk

Eugene S. Polzik Chap. 27

QUANTOP, Niels Bohr Institute
Copenhagen University
Blegdamsvej 17
2100 København
Denmark
polzik@phys.au.dk

Jean-Michel Raimond Chap. 28

Laboratoire Kastler Brossel
Département de Physique
Ecole Normale Supérieure
24 rue Lhomond
75005 Paris
France
jmr@physique.ens.fr

Gerhard Rempe Chap. 28

Max-Planck Institute for Quantum Optics
Hans-Kopfermann-Str. 1
85748 Garching
Germany
Gerhard.Rempe@mpq.mpg.de

Anna Sanpera *Chap. 8*

ICREA and Grup de Física Teòrica
 Universitat Autònoma de Barcelona
 08193 Bellaterra
 Spain
 sanpera@ifae.es

Ferdinand Schmidt-Kaler *Chap. 23*

Universität Ulm
 Abteilung Quanteninformationsverarbeitung
 Albert-Einstein-Allee 11
 89069 Ulm
 Germany
 ferdinand.schmidt-kaler@uni-ulm.de

Thomas Schulte-Herbrüggen *Chap. 25*

Department Chemie
 Technische Universität München
 Lichtenbergstr. 4
 85747 Garching
 Germany
 tosh@ch.tum.de

Aditi Sen(De) *Chap. 8*

ICFO-Institut de Ciències Fotòniques
 Mediterranean Technology Park
 08860 Castelldefels, Barcelona
 Spain
 Aditi.Sen@icfo.es

Ujjwal Sen *Chap. 8*

ICFO-Institut de Ciències Fotòniques
 Mediterranean Technology Park
 08860 Castelldefels, Barcelona
 Spain
 Ujjwal.Sen@icfo.es

A. K. Spörl *Chap. 25*

Department Chemie
 Technische Universität München
 Lichtenbergstr. 4
 85747 Garching
 Germany
 spoerl@ch.tum.de

Nicolas Treps *Chap. 31*

Laboratoire Kastler Brossel
 University Pierre et Marie Curie
 Campus Jussieu, Case 74
 75252 Paris Cedex 05
 France
 nicolas.treps@spectro.jussieu.fr

Peter van Loock *Chap. 9*

Quantum Information Science Group
 National Institute of Informatics (NII)
 2-1-2 Hitotsubashi
 Chiyodaku
 Tokyo 101-8430
 Japan
 vanloock@nii.ac.jp

Vlatko Vedral *Chap. 21*

School of Physics and Astronomy
 University of Leeds
 Leeds LS2 JT
 UK
 v.vedral@leeds.ac.uk

Shashank S. Virmani *Chap. 10*

Institute for Mathematical Sciences
 Imperial College London
 Exhibition Road
 London SW7 2BW
 UK
 s.virmani@imperial.ac.uk

Harald Weinfurter *Chap. 16*

Physics Department
 Ludwig-Maximilians University
 Schellingstr. 4/III
 80799 Munich
 Germany
 harald.weinfurter@physik.uni-muenchen.de

Reinhard F. Werner *Chap. 5*

Institut für Mathematische Physik der Techni-
schen Universität Braunschweig
Mendelssohnstr. 3
38106 Braunschweig
Germany
r.werner@tu-bs.de

Peter Zoller *Chap. 22, 26*

Institute for Theoretical Physics
University of Innsbruck
Technikerstr. 25
6020 Innsbruck
Austria
peter.zoller@uibk.ac.at

Part I
Classical Information Theory

1 Classical Information Theory and Classical Error Correction

Markus Grassl

1.1 Introduction

Information theory establishes a framework for any kind of communication and information processing. It allows us to derive bounds on the complexity or costs of tasks such as storing information using the minimal amount of space or sending data over a noisy channel. It provides means to quantify information. So one may ask, “How much does someone know about what somebody else knows?”—a question which is important in cryptographic context. Before studying the new aspects that quantum mechanics adds to information theory in later chapters, we will have a brief look at the basics of classical information theory in the next section.

While information theory provides an answer to the question how fast one can send information over a noisy channel, it usually does not give a constructive solution to this task. This is a problem error correction deals with. In Section 1.3 we give a short introduction to linear blocks codes, laying ground for the discussion of error-correcting codes for quantum systems in Chapter 7.

1.2 Basics of Classical Information Theory

1.2.1 Abstract communication system

The foundations of information theory have been laid by Claude Shannon in his landmark paper “A Mathematical Theory of Communication” [Sha48]. In that paper, Shannon introduces the basic mathematical concepts for communication systems and proves two fundamental *coding theorems*. Here we mainly follow his approach.

The first important observation of Shannon is that although the process of communication is intended to transfer a message with some meaning, the design of a communication system can abstract from any meaning:

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of com-

munication are irrelevant to the engineering problem. The significant aspect is that the actual message is *one selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

Additionally, we can to some extent abstract from the physical channel that is used to transmit the message. For this, we introduce a *transmitter* and a *receiver* that convert the messages into some physical signal and vice versa. The general layout of such a communication system is illustrated in Fig. 1.1. Given a channel and an information source, the basic problem is

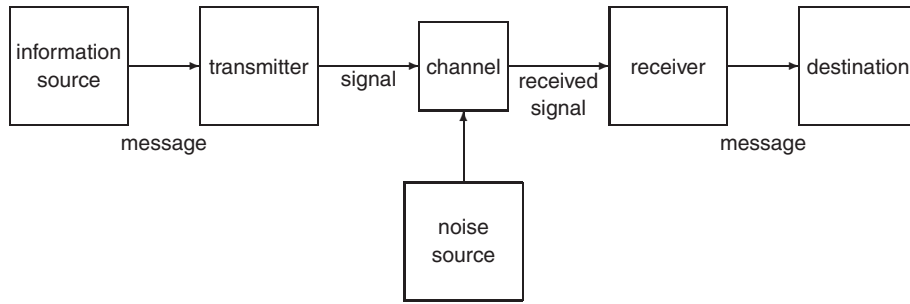


Figure 1.1. Schematic diagram of a general communication system.

to transmit the messages produced by the information source through the channel as efficient and as reliable as possible. Efficient means that we can send as much information as possible per use of the channel, and reliable means that, despite the disturbance due to the noise added by the channel, the original message is (with high probability) reproduced by the receiver. Shannon has shown that one can treat the two problems separately. First we will consider a *noiseless channel* which transmits every input perfectly, and then we will deal with *noisy channels*. For simplicity, we will consider only *discrete channels* here, i.e., both the input and the output of the channel, as well as those of the transmitter and receiver, are symbols of a finite discrete set.

1.2.2 The discrete noiseless channel

For a channel that transmits its inputs perfectly, the goal in the design of a communication system is to maximize its efficiency, i.e., the amount of information that can be sent through the channel per time. Usually it is assumed that for each channel input the transmission takes the same amount of time. Then we want to maximize the throughput per channel use. Otherwise, we first have to consider how many symbols we can send through the channel per time. Following [Sha48], we define

Definition 1.1 (capacity of a discrete noiseless channel) The capacity C of a discrete channel is given by

$$C = \lim_{T \rightarrow \infty} \frac{\log_2 N(T)}{T},$$

where $N(T)$ is the number of allowed signals of duration T .

If we use the symbols $x_1, \dots, x_n$ with durations $t_1, \dots, t_n$, then we get the recursive equation

$$N(t) = N(t - t_1) + (t - t_2) + \dots + N(t - t_n),$$

as we can partition the sequences of duration t by, say, the last symbol. For large t , $N(t)$ tends to X_0^t where X_0 is the largest real solution of the characteristic equation

$$X^{-t_1} + X^{-t_2} + \dots + X^{-t_n} = 1. \quad (1.1)$$

Summarizing, we get

Lemma 1.1 *The capacity of a discrete noiseless channel with symbols $x_1, \dots, x_n$ with durations $t_1, \dots, t_n$ is*

$$C = \log_2 X_0,$$

where X_0 is the largest real solution of (1.1).

In order to maximize the efficiency of the communication system, we additionally need a measure for the amount of information that is produced by the source. Recall that we abstract from the meaning of a message, i.e., a single message does not provide any information. Instead, we always consider a set of possible symbols, and each of the symbols will occur with some probability. The less frequent a symbol, the more surprising is its occurrence and hence it bears more information. The amount of information of a source is described as follows:

Definition 1.2 (Shannon entropy) Let a source S emit the symbols $x_1, \dots, x_n$ with probabilities $p(x_1), \dots, p(x_n)$. Then the *Shannon entropy* of the source is given by

$$H(S) = - \sum_{i=1}^n p(x_i) \log_2 p(x_i).$$

In this definition we have assumed that the symbols are emitted independently, i.e., the probability of receiving a sequence $x_{i_1} x_{i_2} \dots x_{i_m}$ of length m is given by

$$p(x_{i_1} x_{i_2} \dots x_{i_m}) = p(x_{i_1}) p(x_{i_2}) \dots p(x_{i_m}).$$

If there are some correlations between the symbols, the entropy of the source decreases when the original symbols are combined to new symbols. This is a consequence of the fact that the entropy is maximal when all probabilities are equal. As an example we may consider any natural language. The entropy depends on whether we consider the single-letter entropy, the pairs or triples of letters, whole words, or even sentences. Of course, the entropy does also depend on the language itself.

From now on, we fix the alphabet of the information source and assume that there are no correlations between the symbols. A very important concept in information theory is that of ε -typical words.

Theorem 1.1 (ε -typical words) *Let $\mathcal{S}$ be a source with entropy $H(\mathcal{S})$. Given any $\varepsilon > 0$ and $\delta > 0$, we can find an N_0 such that the sequences of any length $N \geq N_0$ fall into two classes:*

1. *A set whose total probability is less than ε .*
2. *The remainder, all of whose members have probability p satisfying the inequality*

$$\left| \frac{-\log_2 p}{N} - H(\mathcal{S}) \right| < \delta.$$

Asymptotically, this means that a sequence either occurs with negligible probability, i.e., is nontypical, or it is a so-called ε -typical word, which are approximately equally distributed.

Fixing the length N one can order the sequences by decreasing probability. For $0 < q < 1$, we define $n(q)$ as the minimum number of sequences of length N that accumulate a total probability q . Shannon has shown that in the limit of large N , this fraction is independent of q :

Theorem 1.2

$$\lim_{N \rightarrow \infty} \frac{\log_2 n(q)}{N} = H(\mathcal{S}) \quad \text{for} \quad 0 < q < 1.$$

The quantity $\log_2 n(q)$ can be interpreted as the number of bits that are required to describe a sequence when considering only the most probable sequences with total probability q . From Theorem 1.1 we get that even for the finite length N , almost all words can be described in this way. The bounds for sending arbitrary sequences through the channel are given by Shannon's first fundamental coding theorem:

Theorem 1.3 (noiseless coding theorem) *Given a source with entropy H (in bits per symbol) and a channel with capacity C (in bits per second), it is possible to encode the output of the source in such a way as to transmit at the average rate $\frac{C}{H} - \varepsilon$ symbols per second over the channel where $\varepsilon > 0$ is arbitrarily small.*

Conversely, it is not possible to transmit at an average rate greater than $\frac{C}{H}$.

The small defect ε compared to the maximal achievable transmission speed is due to the small extra information that is needed to encode the nontypical words of the source. An efficient scheme for encoding the output of the source is e.g. the so-called *Huffman coding* [Huf52]. In view of Theorem 1.1, one can also ignore the nontypical words which have a negligible total probability ε in the encoding, resulting in a small error (*lossy data compression*).

1.2.3 The discrete noisy channel

A discrete noisy channel maps an input symbol x_i from the (finite) input alphabet $\mathcal{X}$ to an output symbol y_j from the output alphabet $\mathcal{Y}$. A common assumption is that the channel is memoryless, i.e., the probability of observing a symbol y_j depends only on the last channel input x_i and nothing else. The size of the input and output alphabet need not be the same, as depicted in Fig. 1.2. Given the channel output y_j , the task for the receiver is to determine the most likely input x_i to the channel. For this we consider how much information the channel output provides about the channel input. First we define some general quantities for pairs of random variables (see, e.g., [CT91]).

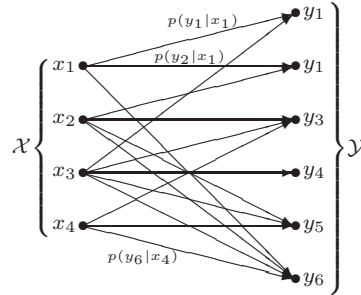


Figure 1.2. Schematic representation of a discrete memoryless channel. Arrows correspond to transitions with nonzero probability $p(y_j|x_i)$.

Definition 1.3 (joint entropy) The *joint entropy* $H(X, Y)$ of a pair of discrete random variables X and Y with joint distribution $p(x, y)$ is defined as

$$H(X, Y) = - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log_2 p(x, y).$$

For the joint entropy, we consider the channel input and the channel output together as one symbol.

Definition 1.4 (conditional entropy) The *conditional entropy* $H(Y|X)$ of a pair of discrete random variables X and Y with joint distribution $p(x, y)$ is defined as

$$\begin{aligned} H(Y|X) &= \sum_{x \in \mathcal{X}} p(x) H(Y|X = x) \\ &= - \sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|x) \log_2 p(y|x) \\ &= - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log_2 p(y|x). \end{aligned}$$

The conditional entropy is a measure for the information that we additionally get when considering both X and Y together, and not only X . This is reflected by the following *chain rule* (see [CT91, Theorem 2.2.1]).

Theorem 1.4 (chain rule)

$$H(X, Y) = H(X) + H(Y|X).$$

Another important quantity in information theory is the *mutual information*.

Definition 1.5 (mutual information) The *mutual information* $I(X; Y)$ of a pair of discrete random variables X and Y is defined as

$$I(X; Y) = H(X) + H(Y) - H(X, Y).$$

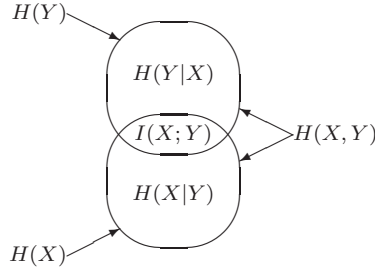


Figure 1.3. Relationship between entropy and mutual information.

The relationship between entropy and mutual information is illustrated in Fig. 1.3. From Theorem 1.4 we get the following equivalent expressions for the mutual information:

$$\begin{aligned} I(X; Y) &= H(X) + H(Y) - H(X, Y) \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X). \end{aligned}$$

With this preparation, we are ready to define the capacity of a noisy discrete memoryless channel.

Definition 1.6 (capacity of a noisy discrete memoryless channel) The capacity of a discrete memoryless channel with joint input–output distribution $p(x, y)$ is defined as

$$C := \max_{p(x)} I(X; Y) = \max_{p(x)} (H(X) - H(X|Y)),$$

where the maximum is taken over all possible input distributions.

The justification of this definition is provided by Shannon’s second fundamental coding theorem.

Theorem 1.5 (noisy coding theorem) *Let $\mathcal{S}$ be a source with entropy $H(\mathcal{S})$ and let a discrete memoryless channel have the capacity C . If $H(\mathcal{S}) < C$, then there exists an encoding scheme such that the output of the source can be transmitted over the channel with an arbitrarily small frequency of errors.*

For the proof of this theorem, one considers a particular set of encoding schemes and then averages the frequency of errors. This average can be made arbitrarily small, implying that at least one of the encoding schemes must have a negligible error probability.

Before we turn our attention to the explicit construction of error-correcting codes, we consider a particular interesting channel.

Example 1.1 (binary symmetric channel (BSC)) The BSC maps the input symbols $\{0, 1\}$ to the output symbols $\{0, 1\}$. With probability $1 - p$, the symbol is transmitted correctly; with probability p the output symbol is flipped (see Fig. 1.4).

For the capacity of the BSC, we compute

$$\begin{aligned}
 I(X; Y) &= H(Y) - H(Y|X) \\
 &= H(Y) - \sum p(x)H(Y|X = x) \\
 &= H(Y) - \sum p(x)H(p) \\
 &= H(Y) - H(p) \\
 &\leq 1 - H(p).
 \end{aligned} \tag{1.2}$$

Here we have used the *binary entropy function* $H(p)$ defined as

$$H(p) := -p \log_2 p - (1 - p) \log_2 (1 - p).$$

The last inequality follows from the fact that the entropy of the binary variable Y is at most 1. From (1.2) it follows that the capacity of a BSC is at most $1 - H(p)$, and if the input distribution is uniform, this maximal capacity is achieved.

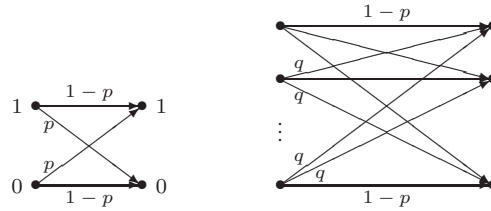


Figure 1.4. The binary symmetric channel (BSC) and its generalization, the uniform symmetric channel (USC). Each symbol is transmitted correctly with probability $1 - p$. In case of an error, each of the other symbols is equally likely.

The generalization of the BSC to more than one input symbol is shown in Fig. 1.4. Again, a symbol is transmitted correctly with probability $1 - p$. If an error occurs, each of the, say, $m - 1$ other symbols is equally likely, i.e., it occurs with probability $q = p/(m - 1)$. These types of channels are extremal in the sense that the transition probabilities only depend on whether a symbol is transmitted correctly or not. Hence an incorrect symbol bears minimal information about the input symbol. Any deviation from this symmetry results in an increased capacity.

1.3 Linear Block Codes

1.3.1 Repetition code

When sending information over a noisy channel, on the highest level of abstraction we distinguish only the cases whether a symbol is transmitted correctly or not. Then the difference between the input sequence and the output sequence is measured by the *Hamming distance*.

Definition 1.7 (Hamming distance/weight) The *Hamming distance* between two sequences $\mathbf{x} = (x_1 \dots x_n)$ and $\mathbf{y} = (y_1 \dots y_n)$ is the number of positions where $\mathbf{x}$ and $\mathbf{y}$ differ, i.e.,

$$d_{\text{Hamming}}(\mathbf{x}, \mathbf{y}) := |\{i : 1 \leq i \leq n \mid x_i \neq y_i\}|.$$

If the alphabet contains a special symbol 0, we can also define the *Hamming weight* of a sequence which equals the number of nonzero positions.

In order to be able to correct errors, we use only a subset of all possible sequences. In particular, we may take a subset of all possible sequences of length n .

Definition 1.8 (block code) A *block code* $\mathcal{B}$ of length n is a subset of all possible sequences of length n over an alphabet $\mathcal{A}$, i.e., $\mathcal{B} \subseteq \mathcal{A}^n$. The *rate* of the code is

$$R = \frac{\log |\mathcal{B}|}{\log |\mathcal{A}^n|} = \frac{\log |\mathcal{B}|}{n \log |\mathcal{A}|},$$

i.e., the average number of symbols encoded by a codeword.

The simplest code that can be used to detect or correct errors is the *repetition code*. A repetition code with rate $1/2$ transmits every symbol twice. At the receiver, the two symbols are compared, and if they differ, an error is detected. Using this code over a channel with error probability p , the probability of an undetected error is p^2 . Sending more than two copies of each symbol, we can decrease the probability of an undetected error even more. But at the same time, the rate of the code decreases since the number of codewords remains fixed while the length of the code increases.

A repetition code can not only be used to detect errors, but also to correct errors. For this, we send three copies of each symbols, i.e., we have a repetition code with rate $1/3$. At the receiver, the three symbols are compared. If at most one symbol is wrong, the two error-free symbols agree and we assume that the corresponding symbol is correct. Again, increasing the number of copies sent increases the number of errors that can be corrected. For the general situation, we consider the distance between two words of the block code $\mathcal{B}$.

Definition 1.9 (minimum distance) The *minimum distance* of a block code $\mathcal{B}$ is the minimum number of positions in which two distinct codewords differ, i.e.

$$d_{\min}(\mathcal{B}) := \min\{d_{\text{Hamming}}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{B} \mid \mathbf{x} \neq \mathbf{y}\}.$$

The error-correcting ability of a code is related to its minimum distance.

Theorem 1.6 Let $\mathcal{B}$ be a block code with minimum Hamming distance d . Then one can either detect any error that acts on no more than d positions or correct any error that acts on no more than $\lfloor (d-1)/2 \rfloor$ positions.

Proof. From the definition of the minimum distance of the code $\mathcal{B}$ it follows that at least d positions have to be changed in order to transform one codeword into another. Hence any error acting on less than $d-1$ positions can be detected. If strictly less than $d/2$ positions are changed, there will be a unique codeword which is closest in the Hamming distance. Hence up to $\lfloor (d-1)/2 \rfloor$ errors can be corrected. The situation is illustrated in Fig. 1.5. $\square$

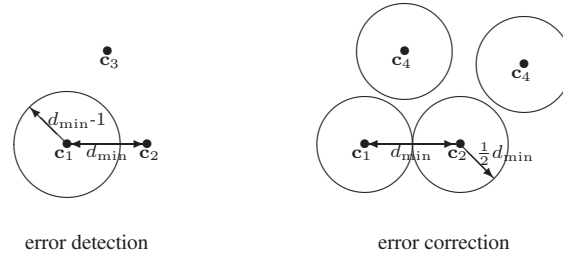


Figure 1.5. Geometry of the codewords. Any sphere of radius $d_{\min} - 1$ around a codeword contains exactly one codeword. The spheres of radius $\lfloor (d_{\min} - 1)/2 \rfloor$ are disjoint.

1.3.2 Finite fields

For a general block code $\mathcal{B}$ over an alphabet $\mathcal{A}$, we have to make a list of all codewords, i.e., the description of the code is proportional to its size. In order to get a more efficient description—and thereby more efficient algorithms for encoding and decoding—we impose some additional structure. In particular, we require that the elements of the alphabet have the algebraic structure of a field, i.e., we can add, subtract, and multiply any two elements, and every nonzero element has an inverse. First we consider a finite field whose size is a prime number.

Proposition 1.1 (prime field) *The integers modulo a prime number p form a finite field $\mathbb{F}_p$ with p elements.*

Proof. It is clear that the modulo operation is a ring homomorphism, i.e., it is compatible with addition, subtraction, and multiplication. It remains to show that any nonzero element has a multiplicative inverse. As p is a prime number, for any nonzero element b we have $\gcd(p, b) = 1$. By the extended Euclidean algorithm (see Table 1.1), there exist integers s and t such that $1 = \gcd(p, b) = sp + tb$. Hence we get $tb = 1 \pmod{p}$, i.e. t is the multiplicative inverse of b modulo p . $\square$

The smallest field is the binary field $\mathbb{F}_2$ which has only two elements 0 and 1. Note that the integers modulo a composite number do not form a field as some nonzero elements do not have a multiplicative inverse. For example, for the integers modulo 4 we have $2 \cdot 2 = 0 \pmod{4}$.

In order to construct a field whose size is not a prime number, one uses the following construction.

Proposition 1.2 (extension field) *Let $\mathbb{F}_p$ be a finite field with p elements, p prime. If $f(X) \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree m , then the polynomials in $\mathbb{F}_p[X]$ modulo $f(X)$ form a finite field $\mathbb{F}_q$ with $q = p^m$ elements.*

Proof. The remainder of the division by the polynomial $f(X)$ of degree m can be any polynomial of degree strictly less than m . Hence we obtain p^m different elements. Again addition, subtraction, and multiplication of two elements are performed over the polynomial ring and the result is reduced modulo $f(X)$. For the computation of the multiplicative inverse, we use the extended Euclidean algorithms of Table 1.1. The condition that $f(X)$ is an irreducible

Table 1.1. The extended Euclidean algorithm (see [AHU74]).

```

EUCLID( $a_0, a_1$ )
 $s_0 \leftarrow 1; t_0 \leftarrow 0;$ 
 $s_1 \leftarrow 0; t_1 \leftarrow 1;$ 
 $i \leftarrow 1;$ 
while  $a_i$  does not divide  $a_{i-1}$  do
   $q \leftarrow a_{i-1} \text{ div } a_i;$ 
   $a_{i+1} \leftarrow a_{i-1} - qa_i;$ 
   $s_{i+1} \leftarrow s_{i-1} - qs_i;$ 
   $t_{i+1} \leftarrow t_{i-1} - qt_i;$ 
   $i \leftarrow i + 1;$ 
end while
return  $a_i, s_i, t_i;$ 
end

```

polynomial implies that $f(X)$ cannot be written as the product of two nonconstant polynomials. So again, for any nonzero element $b(X)$ we have $\gcd(b(X), p(X)) = 1$. $\square$

It can be shown that for any prime number p and for any positive integer m there exists an irreducible polynomial of degree p over $\mathbb{F}_p$, i.e., for any prime power $q = p^m$, there exists a finite field of that size. Furthermore, it can be shown that any finite field can be obtained by the construction of Proposition 1.2. Hence we get (see, e.g., [Jun93])

Theorem 1.7 *A finite field of size s exists if and only if s is a prime power, i.e., $s = p^m$ for some prime number p and some positive integer m .*

Example 1.2 The polynomial $f(X) = X^2 + X + 1$ has no zero over the integers modulo 2 and is hence irreducible. The resulting field $\mathbb{F}_4 = \mathbb{F}_2[X]/(f(X))$ has four elements $\{0, 1, X, X+1\}$ which may also be denoted as $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ where ω is a root of $f(X)$, i.e., $\omega^2 + \omega + 1 = 0$.

Example 1.3 The polynomial $f(X) = X^2 + 1$ has no zero over the integers modulo 3 and is hence irreducible. The resulting field $\mathbb{F}_9 = \mathbb{F}_3[X]/(f(X))$ has nine elements $\{0, 1, 2, X, X+1, X+2, 2X, 2X+1, 2X+2\}$. Note that here the powers of a root α of $f(X)$ do not generate all nonzero elements as $\alpha^2 = -1$ and hence $\alpha^4 = 1$. Instead we may use the powers of the element $\beta = \alpha + 1$.

1.3.3 Generator and parity check matrix

In order to get a more efficient description of a block code $\mathcal{B}$ of length n we consider only codes whose alphabet is a finite field $\mathbb{F}_q$. Furthermore, we require that the code $\mathcal{C}$ forms a linear vector space over the field $\mathbb{F}_q$, i.e.,

$$\forall \mathbf{x}, \mathbf{y} \in \mathcal{B} \forall \alpha, \beta \in \mathbb{F} : \alpha \mathbf{x} + \beta \mathbf{y} \in \mathcal{B}.$$

This implies that the code has q^k elements for some k , $0 \leq k \leq n$. We will use the notation $\mathcal{B} = [n, k]_q$. Instead of listing all q^k elements, it is sufficient to specify a basis of k linear

independent vectors in $\mathbb{F}_q^n$. Alternatively, the linear space $\mathcal{B}$ can be given as the solution of $n - k$ linearly independent homogeneous equations.

Definition 1.10 (generator matrix/parity check matrix) A *generator matrix* of a linear code $\mathcal{B} = [n, k]_q$ over the field $\mathbb{F}_q$ is a matrix G with k rows and n columns of full rank whose row-span is the code.

A *parity check matrix* of a linear code $\mathcal{B} = [n, k]_q$ is a matrix H with $n - k$ rows and n columns of full rank whose row null-space is the code.

The generator matrix with $k \times n$ entries provides a compact description of a code with q^k elements. Moreover, encoding of information sequences $\mathbf{i} \in \mathbb{F}_q^k$ of length k corresponds to the linear map given by G , i.e.,

$$\mathbf{i} \mapsto \mathbf{c} := \mathbf{i}G.$$

The parity check matrix H can be used to check whether a vector lies in the code.

Proposition 1.3 (error syndrome) *Let H be a parity check matrix of a linear code $\mathcal{B} = [n, k]_q$. Then a vector $\mathbf{v} \in \mathbb{F}_q^n$ is a codeword if and only if the error syndrome $\mathbf{s}$ given by*

$$\mathbf{s} := \mathbf{v}H^t$$

is zero. Moreover, the syndrome $\mathbf{s}$ depends only on the error.

Proof. The code $\mathcal{B}$ is the row null-space of H , i.e., for any codeword $\mathbf{c} \in \mathcal{B}$ we get $\mathbf{c}H^t = \mathbf{0}$. If $\mathbf{v}$ is a codeword with errors, we can always write $\mathbf{v} = \mathbf{c} + \mathbf{e}$, where $\mathbf{v}$ is a codeword and $\mathbf{e}$ corresponds to the error. Then we compute

$$\mathbf{s} = \mathbf{v}H^t = (\mathbf{c} + \mathbf{e})H^t = \mathbf{c}H^t + \mathbf{e}H^t = \mathbf{e}H^t.$$

□

The reason for defining the parity check matrix H as a matrix with n columns and $n - k$ rows and not as its transpose is motivated by the following.

Proposition 1.4 (dual code) *Let $\mathcal{B} = [n, k]_q$ be a linear code over the finite field $\mathbb{F}_q$. Then the dual code $\mathcal{B}^\perp$ is a code of length n and dimension $n - k$ given by*

$$\mathcal{B}^\perp = \{\mathbf{v} : \mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{v} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{B}\}.$$

Here $\mathbf{v} \cdot \mathbf{c} = \sum_{i=1}^n v_i c_i$ denotes the Euclidean inner product on $\mathbb{F}_q^n$. If G is a generator matrix and H a parity check matrix for $\mathcal{B}$, then G is a parity check matrix and H is a generator matrix for $\mathcal{B}^\perp$.

As we have seen in Theorem 1.6, the minimum distance of a code is a criterion for its error-correcting ability. For linear codes, the minimum distance equals the minimum Hamming weight of the nonzero codewords as

$$d_{\text{Hamming}}(\mathbf{x}, \mathbf{y}) = d_{\text{Hamming}}(\mathbf{x} - \mathbf{y}, \mathbf{y} - \mathbf{y}) = d_{\text{Hamming}}(\mathbf{x} - \mathbf{y}, \mathbf{0}) = \text{wgt}_{\text{Hamming}}(\mathbf{x} - \mathbf{y}).$$

The minimum Hamming weight of a linear code can be computed using the parity check matrix.

Proposition 1.5 *If any $d-1$ columns in the parity check matrix H of a linear code are linearly independent, then the minimum distance of the code is at least d .*

Proof. Assume that we have a nonzero codeword $\mathbf{c}$ with Hamming weight $d-1$, i.e. there are $d-1$ nonzero positions $i_1, \dots, i_{d-1}$ in $\mathbf{c}$. From $\mathbf{c}H^t = \mathbf{0}$ it follows that $c_{i_1}h^{(i_1)} + \dots + c_{i_{d-1}}h^{(i_{d-1})} = \mathbf{0}$, where $h^{(i)}$ denotes the i th column of H . This contradicts the fact that any $d-1$ columns in H are linearly independent. $\square$

1.3.4 Hamming codes

The last proposition can be used to construct codes. For a single-error-correcting code, we require $d \geq 3$. This implies that any two columns in H have to be linearly independent, i.e., no column is a scalar multiple of another column. If we fix the redundancy $m = n - k$, it is possible to find $(q^m - 1)/(q - 1)$ vectors with this properties which can be combined to a parity check matrix H . This construction gives the following class of single-error-correcting codes (see [Ham86, MS77])

Proposition 1.6 (Hamming code) *The m th Hamming code over $\mathbb{F}_q$ is a linear code of length $n = (q^m - 1)/(q - 1)$ and dimension $k = (q^m - 1)/(q - 1) - m$. The parity check matrix H is formed by all normalized nonzero vectors of length m , i.e., the first nonzero coordinate of the vectors is 1. The minimum distance of the code is 3.*

For binary Hamming codes, the parity check matrix H consists of all $2^m - 1$ nonzero vectors of length m . If we order those columns in such a way that the i th column equals the binary expansion $\text{bin}(i)$ of i , error correction is particularly easy. If $\mathbf{e}$ is an error of weight 1, then the syndrome $\mathbf{s} = \mathbf{e}H^t$ equals the i th column of H and hence the binary expansion of i . Therefore, the syndrome directly provides the position of the error.

Example 1.4 The third binary Hamming code has parameters $[7, 4, 3]$. The parity check matrix is

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

For an error at the fifth position, we have $\mathbf{e} = (0, 0, 0, 0, 1, 0, 0)$ and $\mathbf{s} = \mathbf{e}H = (1, 0, 1) = \text{bin}(5)$.

Usually, a received vector will be decoded as the codeword which is closest in the Hamming distance. In general, decoding an arbitrary linear binary code is an NP hard problem [BMvT78]. More precisely, it was shown that it is an NP complete problem to decide whether there is a vector $\mathbf{e} \in \mathbb{F}_2^n$ which corresponds to a given syndrome $\mathbf{s} \in \mathbb{F}_2^k$ and whose Hamming weight is at most w . Hence we cannot expect to have an efficient general algorithm for decoding.

Instead, by exhaustive search we can precompute an error vector of minimal Hamming weight corresponding to each syndrome. For this, we first arrange all codewords as the first row of an array, where the all-zero codeword is the first element. Among the remaining vectors of length n , we pick a vector $\mathbf{e}_1$ with minimal Hamming weight. This vector is the first element of the next row in our array. The remaining entries of this row are obtained by

adding the vector $\mathbf{e}_1$ to the corresponding codeword in the first row. This guarantees that all elements of a row correspond to the same syndrome. We proceed until all q^n vectors have been arranged into an array with q^{n-k} rows and q^k columns, the so-called *standard array*. The elements in the first column of the standard array are called *coset leaders*, having minimal Hamming weight among all vectors in a row. Table 1.2 shows the standard array of a binary code $\mathcal{B} = [7, 3, 4]$ which is the dual of the Hamming code of Example 1.4. Actually, the code $\mathcal{B}$ is a subcode of the Hamming code. In the first row, 16 codewords are listed. For the next seven rows, the coset leader is the unique vector of Hamming weight 1 in each coset, reflecting the fact that the code can correct a single error. For the next seven rows, the coset leader has weight 2, but each coset contains three vectors of weight 2. Hence decoding succeeds only in one out of three cases. In the final row, we have even seven vectors of weight 3.

Table 1.2. Standard array for decoding the code $\mathcal{B} = [7, 3, 4]$, the dual of a binary Hamming code.

0000000	0001111	0110011	0111100	1010101	1011010	1100110	1101001
0000001	0001110	0110010	0111101	1010100	1011011	1100111	1101000
0000010	0001101	0110001	0111110	1010111	1011000	1100100	1101011
0000100	0001011	0110111	0111000	1010001	1011110	1100010	1101101
0001000	0000111	0111011	0110100	1011101	1010010	1101110	1100001
0010000	0011111	0100011	0101100	1000101	1001010	1110110	1111001
0100000	0101111	0010011	0011100	1110101	1111010	1000110	1001001
1000000	1001111	1110011	1111100	0010101	0011010	0100110	0101001
0110000	0111111	0000011	0001100	1100101	1101010	1010110	1011001
1000001	1001110	1110010	1111101	0010100	0011011	0100111	0101000
1000010	1001101	1110001	1111110	0010111	0011000	0100100	0101011
1000100	1001011	1110111	1111000	0010001	0011110	0100010	0101101
1001000	1000111	1111011	1110100	0011101	0010010	0101110	0100001
1010000	1011111	1100011	1101100	0000101	0001010	0110110	0111001
1100000	1101111	1010011	1011100	0110101	0111010	0000110	0001001
1110000	1111111	1000011	1001100	0100101	0101010	0010110	0011001

1.4 Further Aspects

We have seen that the Hamming code is a code for which the correction of errors is rather simple, but it can only correct a single error. On the other hand, using an arbitrary linear code, the problem of error correction is NP complete. But luckily, there are other families of error-correcting codes for which efficient algorithms exist to correct at least all errors of bounded weight. More about these codes can be found in any textbook on coding theory or the book by MacWilliams and Sloane [MS77], which is an excellent reference for the theory of error-correcting codes.

References

- [AHU74] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison Wesley, Reading, MA, 1974.
- [BMvT78] Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.
- [CT91] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, New York, 1991.
- [Ham86] Richard W. Hamming. *Coding and Information Theory*. Prentice-Hall, Englewood Cliffs, NJ, 1986.
- [Huf52] David A. Huffman. A method for the construction of minimum-redundancy codes. *Proceedings of the Institute of Radio Engineers*, 40:1098–1101, 1952.
- [Jun93] Dieter Jungnickel. *Finite Fields: Structure and Arithmetics*. BI-Wissenschaftsverlag, Mannheim, 1993.
- [MS77] Florence J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.
- [Sha48] Claude E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, 623–656, July, October 1948. Online available at <http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html>.

2 Computational Complexity

Stephan Mertens

To most people who are not theoretical computer scientists, the theory of computational complexity—one of the great intellectual achievements of the twentieth century—is simply a meaningless jumble of capital letters.

Scott Aaronson [2]

2.1 Basics

The branch of theoretical computer science known as computational complexity is concerned with classifying problems according to the computational resources required to solve them. Informally, a problem A is computationally more complex than a problem B if the solution of A requires more resources than the solution of B . This informal idea can be turned into a formal theory that touches the very foundations of science (What can be calculated? What can be proven?) as well as practical problems (optimization, cryptography, etc.). This chapter can only provide a short exposition, too short to do justice to the richness and beauty of the theory of computational complexity, but hopefully inspiring enough to wet your appetite for more. For a real understanding of the subject you should consult one of the excellent textbooks written by computer scientists [10, 19, 24], or, if you prefer a book written from a physicist's point of view, you may like [18].

The theory of computational complexity is a mathematical theory, with precise formal definitions, theorems, and proofs. Here we will adopt a largely informal point of view. Let us start with a brief discussion on the building blocks of the theory: problems, solutions, and resources.

Problems. Theoretical computer scientists think of a “problem” as an *infinite family* of problems. Each particular member of this family is called an *instance* of the problem. Let us illustrate this by an example that dates back into the 18th century, where in the city of Königsberg (now Kaliningrad) seven bridges crossed the river Pregel and its two arms (Fig. 2.1). A popular puzzle of the time asked if it was possible to walk through the city crossing each of the bridges exactly once. In theoretical computer science, the “puzzle of the Königsberg bridges” is not considered a problem, but an instance. The corresponding *problem* is this:

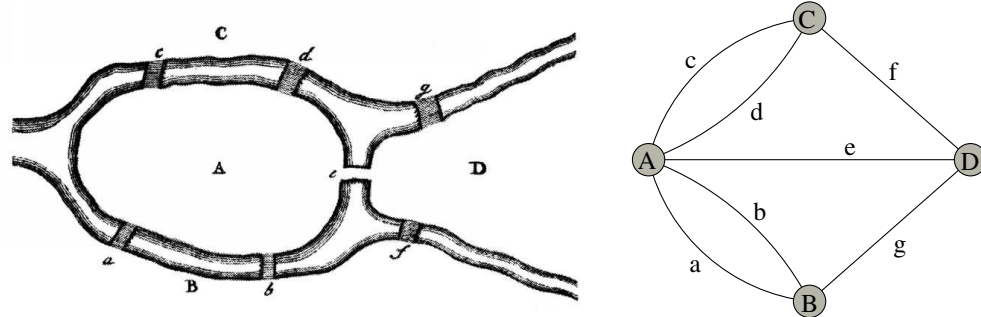


Figure 2.1. The seven bridges of Königsberg, as drawn in Euler's paper from 1736 [8] (left) and represented as a graph (right). In the graph, the riverbanks and islands are condensed to points (vertices), and each of the bridges is drawn as a line (edge).

EULERIAN PATH

Input: A graph G

Question: Does there exist a path on G that traverses each edge exactly once?

This generalization qualifies as a problem in theoretical computer science since it asks a question on arbitrary graphs, i.e., on an infinite set of inputs. It was Leonhard Euler who solved the Königsberg bridges puzzle for general graphs and, en passant, started what is now known as graph theory. In honor of Euler, the problem and the path bear his name. In theoretical computer science, a problem is to a lesser extent something that needs to be solved, but an object of mathematical study. We underline this view by writing problem names in elegant small capitals.

Solutions. To a computer scientist, a solution is an *algorithm* that accepts an instance of a problem as input and returns the correct answer as output. While the notion of an algorithm can be defined precisely, we will settle for an intuitive definition: namely, a series of elementary computation steps which, if carried out, will produce the desired output. You can think of an algorithm as a computer program written in your favorite programming language. The main point here is that an algorithm has to work on *every* instance of the problem to qualify as a solution. This includes those *worst case* instances that give the algorithm a hard time.

Resource consumption. The main resources are *time* (number of elementary steps) and *space* (size of memory). All we can measure (or calculate) is the time (or the space) that a particular algorithm uses to solve the problem, and the intrinsic time complexity of a problem is defined by the most time-efficient algorithm for that problem. Unfortunately, for the vast majority of problems we do not know the most efficient algorithm. But every algorithm we do know gives an *upper bound* for the complexity of a problem. The theory of computational complexity is to a large extent a theory of upper bounds. As we will see in the next section, even the definition of an algorithmic bound requires some care.

2.2 Algorithms and Time Complexity

The running time of an algorithm depends on the problem's size and on the specific instance. Sorting 1000 numbers takes longer than sorting 10 numbers, and some algorithms run faster if the input data are partially sorted already. To minimize the dependence on the specific instance we consider the *worst case time complexity* $T(n)$,

$$T(n) = \max_{|x|=n} t(x), \quad (2.1)$$

where $t(x)$ is the running time of the algorithm for input data x and the maximum is taken over all problem instances of size n . The worst case time is an upper bound for the observable running time, which harmonizes with the fact that an algorithm gives an upper bound for the intrinsic complexity of a problem.

A measure of time complexity should be based on a unit of time that is independent of the clock rate of a specific CPU. Such a unit is provided by the time it takes to perform an elementary operation like the addition of two integer numbers. Measuring the time in this unit means counting the number of elementary operations executed by your algorithm. This number in turn depends strongly on the implementation details of the algorithm—smart programmers and optimizing compilers will try to reduce it. Therefore, we will not consider the precise number $T(n)$ of elementary operations but only the asymptotic behavior of $T(n)$ for large values of n as denoted by the Landau symbols $\mathcal{O}$ and Θ :

- We say $T(n)$ is of order at most $g(n)$ and write $T(n) = \mathcal{O}(g(n))$ if there exist positive constants c and n_0 such that $T(n) \leq cg(n)$ for all $n \geq n_0$.
- We say $T(n)$ is of order $g(n)$ and write $T(n) = \Theta(g(n))$ if there exist positive constants c_1, c_2 , and n_0 such that $c_1g(n) \leq T(n) \leq c_2g(n)$ for all $n \geq n_0$.

Let us apply this measure of complexity to an elementary problem: How fast can you multiply? The algorithm we learned at school takes time $T(n) = \Theta(n^2)$ to multiply two n -bit integers. This algorithm is so natural that it is hard to believe that one can do better, but in fact one can.

The idea is to solve the problem recursively by splitting x and y into high-order and low-order terms. First, write

$$x = 2^{n/2}a + b, \quad y = 2^{n/2}c + d$$

where a, b, c, d are $n/2$ -bit integers. If we write out x in binary, then a and b are just the first and second halves of its binary digit sequence, respectively, and similarly for y . Then

$$xy = 2^n ac + 2^{n/2}(ad + bc) + bd. \quad (2.2)$$

The grade-school method of adding two n -digit numbers takes just $\Theta(n)$ time, and, if we operate in binary, it is easy to multiply a number by 2^n or $2^{n/2}$ simply by shifting it to the left. The hard part of (2.2) then consists of four multiplications of $n/2$ -digit numbers, and this gives the recurrence

$$T(n) = 4T(n/2) + \Theta(n).$$

Unfortunately, the solution to this recurrence is still $T(n) = \Theta(n^2)$. So, we need another idea.

The key observation is that we do not actually need four multiplications. Specifically, we do not need ad and bc separately; we only need their sum. Now

$$(a + b)(c + d) = ac + bd + (ad + bc). \quad (2.3)$$

Therefore, if we calculate ac , bd , and $(a + b)(c + d)$, we can compute $ad + bc$ by subtracting the first two of these from the third. This changes our recurrence to

$$T(n) = 3T(n/2) + \Theta(n), \quad (2.4)$$

which yields $T(n) = \Theta(n^{\log_2 3})$, or roughly $T(n) = \Theta(n^{1.58})$.

This *divide-and-conquer* algorithm reduces our upper bound on the intrinsic time complexity of multiplication: before, we knew that this complexity was $\mathcal{O}(n^2)$, and now this is sharpened to $\mathcal{O}(n^{1.58})$. In fact, this algorithm can be improved even further to $\mathcal{O}(n^{1+\epsilon})$ for ϵ arbitrarily small [23]. Thus multiplication is considerably less complex than the grade-school algorithm would suggest.

2.3 Tractable Trails: The Class P

Let us return to the problem from the first section. What is the time complexity of EULERIAN PATH? One possible algorithm is an exhaustive (and exhausting) search through all possible paths in a graph, but the intractability of this approach was already noticed by Euler. More than 200 years before the advent of computers he wrote, “The particular problem of the seven bridges of Königsberg could be solved by carefully tabulating all possible paths, thereby ascertaining by inspection which of them, if any, met the requirement. This method of solution, however, is too tedious and too difficult because of the large number of possible combinations, and in other problems where many more bridges are involved it could not be used at all” (cited from [17]). Euler was of course referring to the manual labor in creating an exhaustive list of all possible tours. Today this task can be given to a computer which will generate and check all tours across the seven bridges in a blink, but Euler’s remark is still valid and aims right at the heart of theoretical computer science. Euler addresses the *scaling* of this approach with the size of the problem. In a graph with many bridges, you have more choices at each node, and these numbers multiply. This leads to an exponential growth of the number of possible tours with the number of edges. The resulting table will soon get too long to be exhaustively searched by even the fastest computer in the world. Solving the “Venice bridges puzzle” (ca. 400 bridges) by exhaustive search would surely overstrain all present day computers. But Euler proposed an ingenious shortcut that allows us to solve problems much bigger than that.

Euler noticed that in a path that visits each edge exactly once you must leave each vertex on the way via an edge different from the edge that has taken you there. In other words, the degree of the vertex (that is the number of edges adjacent to the vertex) must be even, except for the vertices where the path starts and ends. This is obviously a necessary condition, but Euler noticed that it is also sufficient

Theorem 2.1 *A connected graph contains an Eulerian path if and only if the number of vertices with odd degree is 0 or 2. If it is zero, the Eulerian path is closed (a cycle). If it is 2, the Eulerian path starts and ends at the odd-degree vertices.*

Euler's theorem allows us to devise an efficient algorithm for EULERIAN PATH: loop over all vertices of the graph and count the number of odd-degree vertices. If this number exceeds 2, return "no," otherwise return "yes." The precise scaling of the running time depends on the data structure we used to store the graph, but in any case it scales polynomially in the size of the graph.

The enormous difference between exponential and polynomial scaling is obvious. An exponential algorithm means a hard limit for the accessible problem size. Suppose that with your current equipment you can solve a problem of size n just within your schedule. If your algorithm has complexity $\Theta(2^n)$, a problem of size $n + 1$ will need twice the time, pushing you definitely off schedule. The increase in time caused by a $\Theta(n)$ or $\Theta(n^2)$ algorithm, on the other hand, is far less dramatic and can easily be compensated for by upgrading your hardware. You might argue that a $\Theta(n^{100})$ algorithm outperforms a $\Theta(2^n)$ algorithm only for problem sizes that will never occur in your application. A polynomial algorithm for a problem usually goes hand in hand with a mathematical *insight* into the problem which lets you find a polynomial algorithm with a small degree, typically $\Theta(n^k)$ with $k = 1, 2$, or 3 . Polynomial algorithms with $k > 4$ are rare and arise in rather esoteric problems.

This brings us to our first complexity class. Given a function $f(n)$, $\text{TIME}(f(n))$ denotes the class of problems for which an algorithm exists that solves problems of size n in time $\mathcal{O}(f(n))$. Then the class P (for polynomial time) is defined as

$$P = \bigcup_{k \geq 0} \text{TIME}(n^k). \quad (2.5)$$

In other words, P is the set of problems for which there exists some constant k such that there exists an algorithm that solves the problem in time $\mathcal{O}(n^k)$. Conversely, a problem is outside P if *no algorithm exists* which solves it in polynomial time; for instance, if the most efficient algorithm takes exponential time $2^{\varepsilon n}$ for some $\varepsilon > 0$.

For complexity theorists, P is not so much about tractability as it is about whether or not we possess a mathematical insight into a problem's structure. It is trivial to observe that EULERIAN PATH can be solved in exponential time by exhaustive search, but there is something special about EULERIAN PATH that yields a polynomial-time algorithm. When we ask whether a problem is in P or not, we are no longer just computer users who want to know whether we can finish a calculation in time to graduate: we are theorists who seek a deep understanding of why some problems are qualitatively easier, or harder, than others.

Thanks to Euler's insight, EULERIAN PATH is a tractable problem. The burghers of Königsberg on the other hand had to learn from Euler, that they would never find a walk through their hometown crossing each of the seven bridges exactly once.

2.4 Intractable Itineraries: The class NP

Our next problem is associated with the mathematician and Astronomer Royal of Ireland, Sir William Rowan Hamilton. In the year 1859, Hamilton put on the market a new puzzle called the Icosian game (Fig. 2.2). Its generalization is known as *Hamiltonian path*

HAMILTONIAN PATH

Input: A graph G

Question: Does there exist a path on G that traverses each vertex exactly once?

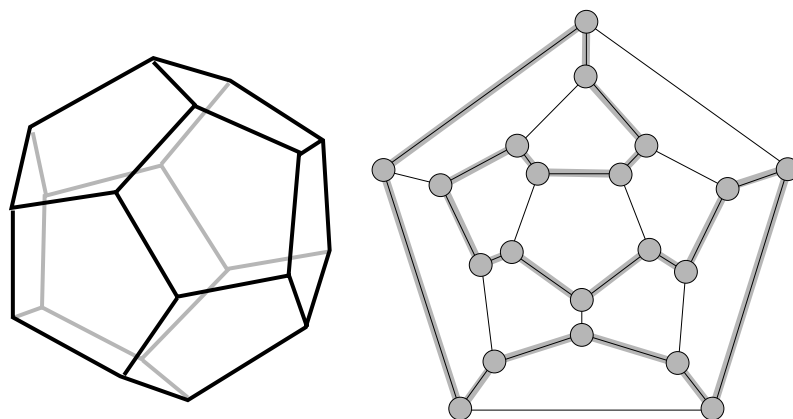


Figure 2.2. Sir Hamilton's Icosian game: Find a route along the edges of the dodecahedron (left), passing each corner exactly once and returning to the starting corner. A solution is indicated (shaded edges) in the planar graph that is isomorphic to the dodecahedron (right).

There is a certain similarity between EULERIAN PATH and HAMILTONIAN PATH. In the former we must pass each edge once—in the latter, each vertex once. Both are decision problems, i.e., problems with answer “yes” or “no,” and both problems can be solved by exhaustive search which for both problems would take exponential time. Despite this resemblance the two problems represent entirely different degrees of difficulty. The available mathematical insights into HAMILTONIAN PATH provide us neither with a polynomial algorithm nor with a proof that such an algorithm is impossible. HAMILTONIAN PATH is intractable, and nobody knows why.

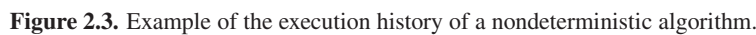
The situation is well described by the proverbial needle in a haystack scenario. It is hard (exponential) to find the needle in a haystack although we can easily (polynomially) tell a needle from a blade of hay. The only source of difficulty is the large size of the search space. This feature is shared by many important problems and it will be the base of our next complexity class. The “needle in a haystack” class is called **NP** for *nondeterministic polynomial*:

Definition 2.1 A decision problem is in NP if and only if it can be solved in nondeterministic polynomial time.

What is nondeterministic time? This is the time consumed by a nondeterministic algorithm, which is like an ordinary algorithm, except that it may use one additional, very powerful instruction:

goto both label 1, label 2

This instruction splits the computation into two parallel processes, one continuing from each of the instructions indicated by “label 1” and “label 2.” By encountering more and



There are two peculiarities in the definition of NP: First, NP contains only decision problems. This allows us to divide each problem into “yes” and “no” instances. Second, polynomial time is required only for the “yes” branch of a nondeterministic algorithm (if there is any). This asymmetry between “yes” and “no” reflects the asymmetry between the “there is” and “for all” quantifiers in decision problems: a graph G is a “yes” instance of HAMILTONIAN PATH, if *there is* at least one Hamiltonian path in G . For a “no” instance, *all* cycles in G have to be non-Hamiltonian.

There is a second, equivalent definition of **NP**, based on the notion of a *succinct certificate*. A certificate is a proof. If you claim that a graph G has a Hamiltonian path, you can proof

your claim by providing a Hamiltonian path, and I can verify your proof in polynomial time. A certificate is succinct if its size is bounded by a polynomial in the size of the problem. The second definition then reads

Definition 2.2 A decision problem P is in NP if and only if for every “yes” instance of P there exists a *succinct certificate* that can be verified in polynomial time.

The equivalence of both definitions can easily be shown [13]. The idea is that a succinct certificate can be used to deterministically select the branch in a nondeterministic algorithm that leads to a “yes” output.

The definition based on nondeterministic algorithms reveals the key feature of the class NP more clearly, but the second definition is more useful for proving that a decision problem is in NP. As an example consider

COMPOSITENESS

Input: A positive integer N
 Question: Are there integer numbers $p > 1$ and $q > 1$ such that $N = pq$?

A certificate of a “yes” instance N of COMPOSITENESS is a factorization $N = pq$. It is succinct, because the number of bits in p and q is less than or equal to the number of bits in N , and it can be verified in quadratic time (or even faster, see above) by multiplication. Hence COMPOSITENESS $\in$ NP.

Most decision problems ask for the existence of an object with a given property, like a cycle which is Hamiltonian or a factorization with integer factors. In these cases, the desired object may serve as a succinct certificate. For some problems this does not work, however, like for

PRIMALITY

Input: A positive integer N
 Question: Is N prime?

PRIMALITY is the negation or complement of COMPOSITENESS: the “yes” instances of the former are the “no” instances of the latter and vice versa. A succinct certificate for PRIMALITY is by no means obvious. In fact, for many decision problems in NP no succinct certificate is known for the complement, i.e., it is not known whether the complement is also in NP. An example is HAMILTONIAN PATH: there is no proof of “non-Hamiltonicity” that can be verified in polynomial time. This brings us to our next complexity class:

Definition 2.3 A decision problem is in coNP if and only if its complement is in NP.

From COMPOSITENESS $\in$ NP we get PRIMALITY $\in$ coNP, but is PRIMALITY $\in$ NP? In fact it is, a succinct certificate can be constructed using Fermat’s Theorem [20]. Euler’s theorem can be used to prove the presence as well as the absence of an Eulerian path, hence EULERIAN PATH $\in$ NP $\cap$ coNP. This is generally true for all problems in P: the trace of the polynomial algorithm is a succinct certificate for both “yes” and “no” instances. Hence we have

$$P \subseteq NP \cap \text{coNP}. \quad (2.6)$$

The class NP is populated by many important problems. Let us discuss two of the most prominent members of the class.

2.4.1 Coloring graphs

Imagine we wish to arrange talks in a conference in such a way that no participant will be forced to miss a talk he or she would like to hear. Assuming a good supply of lecture rooms enabling us to hold as many parallel talks as we like, can we finish the program within k time slots? This problem can be formulated in terms of graphs: Let G be a graph whose vertices are the talks and in which two talks are adjacent (joined by an edge) if and only if there is a participant wishing to attend both. Your task is to assign one of the k time slots to each vertex in such a way that adjacent vertices have different time slots. The common formulation of this problem uses colors instead of time slots:

k -COLORING

Input: $G = (V, E)$ and a positive integer k .

Question: Is there a coloring of the vertices of G using at most k different colors such that no two adjacent vertices have the same color?

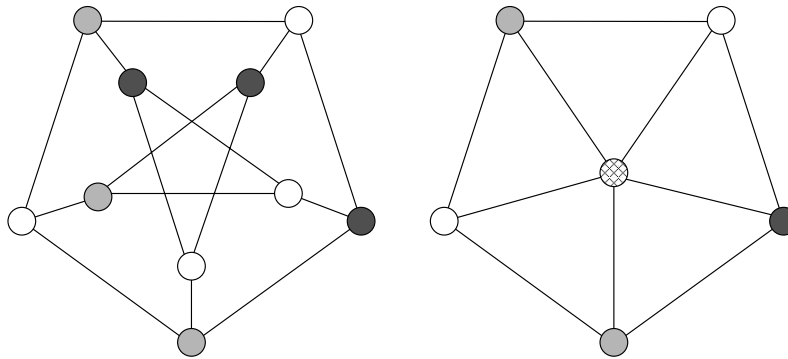


Figure 2.4. The Petersen graph (left) with a proper 3-coloring. The cart-wheel graph (right) cannot be colored with less than four colors.

Despite its colorful terminology, k -COLORING is a serious problem with a wide range of applications. It arises naturally whenever one is trying to allocate resources in the presence of conflicts, like in our conference example. Another example is the assignment of frequencies to wireless communication devices. We would like to assign one of k frequencies to each of n devices. If two devices are sufficiently close to each other they need to use different frequencies to prevent interference. This problem is equivalent to k -COLORING on the graph that has the communication devices as vertices, and an edge for each pair of devices that is close enough to interfere.

If a graph can be colored with less than k colors, the proper coloring is a proof of this fact that can be checked in polynomial time; hence k -COLORING $\in$ NP. For very few colors, the

problem is tractable:

$$1\text{-COLORING} \in P \quad 2\text{-COLORING} \in P. \quad (2.7)$$

Finding a polynomial algorithm for this cases is left as an exercise. For three or more colors, no polynomial algorithm is known, and exhaustive search through all possible colorings seems to be unavoidable.

2.4.2 Logical truth

We close this section with a decision problem that is not from graph theory but from Boolean logic. A Boolean variable x can take the value 0 (false) or 1 (true). Boolean variables can be combined in *clauses* using the Boolean operators

- NOT $\neg$ (negation): the clause $\overline{x}$ is true ($\overline{x} = 1$) if and only if x is false ($x = 0$).
- AND $\wedge$ (conjunction): the clause $x_1 \wedge x_2$ is true ($x_1 \wedge x_2 = 1$) if and only if both variables are true: $x_1 = 1$ and $x_2 = 1$
- OR $\vee$ (disjunction): the clause $x_1 \vee x_2$ is true ($x_1 \vee x_2 = 1$) if and only if at least one of the variables is true: $x_1 = 1$ or $x_2 = 1$.

A variable x or its negation $\overline{x}$ is called a *literal*. Different clauses can be combined to yield complex Boolean formulas, e.g.

$$\Phi_1(x_1, x_2, x_3) = (x_1 \vee \overline{x_2} \vee x_3) \wedge (x_2 \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2) \wedge (\overline{x_1} \vee \overline{x_3}). \quad (2.8)$$

A Boolean formula evaluates to either 1 or 0, depending on the assignment of the Boolean variables. In the above example $\Phi_1 = 1$ for $x_1 = 1, x_2 = 1, x_3 = 0$ and $\Phi_1 = 0$ for $x_1 = x_2 = x_3 = 1$. A formula Φ is called *satisfiable* if there is at least one assignment of the variables such that the formula is true. Φ_1 is satisfiable, but

$$\Phi_2(x_1, x_2) = (\overline{x_1} \vee x_2) \wedge \overline{x_2} \wedge x_1 \quad (2.9)$$

is not satisfiable.

Every Boolean formula can be written in a *conjunctive normal form* (CNF), i.e., as a set of clauses C_k combined exclusively with the AND operator,

$$\Phi = C_1 \wedge C_2 \wedge \cdots \wedge C_m, \quad (2.10)$$

where the literals in each clause are combined exclusively with the OR operator. The examples Φ_1 and Φ_2 are both written in CNF. Each clause can be considered as a constraint on the variables, and satisfying a formula means satisfying a set of (possibly conflicting) constraints simultaneously. Therefore

SAT (SATISFIABILITY)

Input: A Boolean formula $\Phi(x_1, \dots, x_n)$ in CNF.
 Question: Is Φ satisfiable?

can be considered as a prototype of a constraint satisfaction problem [14]. Obviously the evaluation of a Boolean formula for a given assignment of variables can be done in polynomial time; hence $\text{SAT} \in \text{NP}$. The same is true for the special variant of SAT where one fixes the number of literals per clause:

 k -SAT

Input: A Boolean formula Φ in CNF with k literals per clause
 Question: Is Φ satisfiable?

Again polynomial algorithms are known for $k = 1$ and $k = 2$ [4], but general SAT and k -SAT for $k > 2$ seem to be intractable.

2.5 Reductions and NP-completeness

So far, all the intractable problems seem to be isolated islands in the map of complexity. In fact, they are tightly connected by a device called polynomial reduction, which lets us bound the computational complexity of one problem to the computational complexity of another.

We will illustrate this point by showing that general SAT cannot be harder than 3-SAT. We write

$$\text{SAT} \leq 3\text{-SAT}, \quad (2.11)$$

which means that the computational complexity of SAT cannot exceed that of 3-SAT. In other words, if someone finds a polynomial algorithm for 3-SAT, this would immediately imply a polynomial algorithm for SAT. To prove (2.11) we need to map a general SAT-formula Φ to a 3-SAT-formula Φ' such that Φ is satisfiable if and only if Φ' is satisfiable. The map proceeds clause by clause. Let C be a clause in Φ . If C has three literals, it becomes a clause of Φ' . If C has less than three literals, we fill it up by repeating literals: $(l_1 \vee l_2) \mapsto (l_1 \vee l_2 \vee l_2)$ etc., and copy the augmented clause into Φ' . If C has more than three literals, $C = l_1 \vee l_2 \vee \dots \vee l_p$ with $(p > 3)$, we introduce $p - 3$ new variables $y_1, y_2, \dots, y_{p-3}$ and form the 3-SAT-formula

$$C' = (l_1 \vee l_2 \vee y_1) \wedge (\bar{y}_1 \vee l_3 \vee y_2) \wedge (\bar{y}_2 \vee l_4 \vee y_3) \wedge \dots \wedge (\bar{y}_{p-3} \vee l_{p-2} \vee l_p).$$

Now assume that C is satisfied. This means that at least one of the literals l_i is true. If we set $y_j = 1$ for $j < i - 1$ and $y_j = 0$ for $j \geq i - 1$, all clauses in C' are satisfied. Now assume that C' is satisfied and all literals l_i are 0. The first clause in C' forces y_1 to be 1, the second clause then forces y_2 to be 1, and so on, but this chain reaction leaves the last clause unsatisfied. Hence C' is satisfiable if at least one of the literals l_i is 1, which in turn implies satisfaction for C . Hence we have proven $C \Leftrightarrow C'$, and we add C' to Φ' . Obviously this map from Φ to Φ' can be done in polynomial time; hence a polynomial time algorithm for 3-SAT could be used as a “subroutine” for a polynomial time algorithm for SAT. This proves (2.11).

Since k -SAT is a special case of SAT, we have $k\text{-SAT} \leq \text{SAT}$ and by transitivity

$$k\text{-SAT} \leq 3\text{-SAT}. \quad (2.12)$$

By a more complicated reduction one can prove that

$$k\text{-COLORING} \leq 3\text{-COLORING}. \quad (2.13)$$

Equations (2.12) and (2.13) are reductions from a class of problems to one special member ($k = 3$) of that class, but there are also reductions between problems that do not seem a priori to be related to each other, like

$$3\text{-SAT} \leq 3\text{-COLORING} \quad (2.14)$$

$$3\text{-COLORING} \leq 3\text{-HAMILTONIAN PATH}. \quad (2.15)$$

To prove (2.14), one has to construct a graph $G(\Phi)$ for a 3-SAT formula Φ such that G is 3-colorable if and only if Φ is satisfiable, and this construction must not take more than polynomial time. For (2.15) one needs to map a graph G in polynomial time to a graph G' such that G is 3-colorable if and only if G' has a Hamiltonian path. Reductions like these can be tricky [10, 18, 19, 24], but they reveal an astounding structure within NP. Imagine that after decades of research someone discovers a polynomial time algorithm for HAMILTONIAN PATH. Then the reductions (2.11)–(2.15) immediately imply polynomial time algorithms for k -COLORING and SAT. And this is only part of the story. Stephen Cook [6] revealed polynomial reducibility's true scope in 1971 when he proved the following theorem:

Theorem 2.2 *All problems in NP are polynomially reducible to SAT:*

$$\forall P \in \text{NP} : P \leq \text{SAT} \quad (2.16)$$

This theorem means that

- no problem in NP is harder than SAT, or SAT is among the hardest problems in NP.
- a polynomial algorithm for SAT would imply a polynomial algorithm for *every* problem in NP, that is, it would imply $P = \text{NP}$.

It seems as if SAT is very special, but according to transitivity and Eqs. (2.11)–(2.15) it can be replaced by 3-SAT, 3-COLORING or HAMILTONIAN PATH. These problems form a new complexity class:

Definition 2.4 A problem P is called NP-complete if $P \in \text{NP}$ and $Q \leq P$ for all $Q \in \text{NP}$

The class of NP-complete problems collects the hardest problems in NP. If any of them has an efficient algorithm, then *every* problem in NP can be solved efficiently, i.e., $P = \text{NP}$. Since Cook proved his theorem, many problems have been shown to be NP-complete. A comprehensive, up-to-date list of hundreds of NP-complete problems can be found in the web [7].

2.6 P vs. NP

At this point we will pause for a moment and review what we have achieved. We have defined the class NP whose members represent “needle in a haystack” type of problems. For some of these problems we know a shortcut to locate the needle without actually searching through the haystack. These problems form the subclass P . For other problems we know that a similar shortcut for one of them would immediately imply shortcuts for all other problems and hence $P = NP$. This is extremely unlikely, however, considering the futile efforts of many brilliant people to find polynomial time algorithms for the hundreds of NP -complete problems. The general belief is that $P \neq NP$. Note that to prove $P \neq NP$ it would suffice to prove the nonexistence of a polynomial time algorithm for a *single* problem from NP . This would imply the nonexistence of efficient algorithms for all NP -complete problems. As long as such a proof is missing,

$$P \stackrel{?}{\neq} NP \quad (2.17)$$

represents the most famous open conjecture in theoretical computer science. It is one of the seven *millenium problems* named by the Clay Mathematics Institute, and its solution will be awarded with one million US dollar [12].

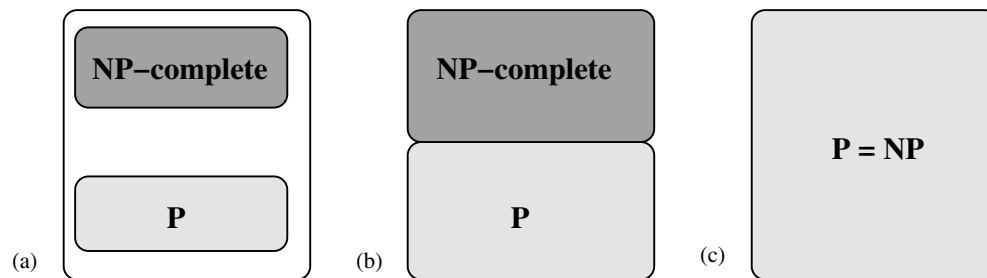


Figure 2.5. Three tentative maps of NP . We can rule out (b), and it is very likely (but not sure) that (a) is the correct map.

Usually a problem from NP is either found to be in P (by a mathematical insight and a corresponding polynomial time algorithm), or it is classified as NP -complete (by reducing another NP -complete problem to it). Every now and then, however, a problem in NP resists classification in P or NP -complete. COMPOSITENESS and PRIMALITY for example have been proven to be in P only very recently [3]. The related problem of factorizing an integer into its prime factors can be formulated as a decision problem $\in NP$:

FACTORIZATION

Input: Integer numbers N and M
 Question: Does N have a nontrivial factor smaller than M ?

Note that the conventional version of the integer factorization problem (find a nontrivial factor) can be solved in polynomial time if and only if FACTORIZATION $\in P$. This follows

from the fact that $\mathcal{O}(\log N)$ instances of FACTORIZATION with properly chosen thresholds M (bisection method) are sufficient to find a nontrivial factor of N . Despite many efforts, no polynomial time algorithm for FACTORIZATION has been found. On the other hand there is no proof that FACTORIZATION is NP-complete, and the general belief is that it is not. FACTORIZATION seems to live in the gap between P and NP-complete. The following theorem [15] guarantees that this gap is populated unless $P = NP$:

Theorem 2.3 *If $P \neq NP$, then there exist NP problems which are neither in P nor are they NP-complete.*

This theorem rules out one of three tentative maps of NP (Fig. 2.5). Another problem that—according to our present knowledge—lives in the gap between P and NP-complete is this:

GRAPH ISOMORPHISM

Input: Two graphs G and G'
 Question: Are G and G' isomorphic?

Two graphs are isomorphic if and only if there is a one-to-one mapping from the nodes of one graph to the nodes of the other graph that preserves adjacency and nonadjacency.

Both FACTORIZATION and GRAPH ISOMORPHISM are problems of considerable practical as well as theoretical importance. If you discover a polynomial time algorithm for one of them, you will get invitations to many conferences, but you will not shatter the world of computational complexity. The true challenge is to find a polynomial time algorithm for an NP-complete problem such as SAT or HAMILTONIAN PATH. The consequences of $P = NP$ would be far greater than better algorithms for practical problems.

Firstly, cryptography, as we know would not exist. Modern cryptography relies on the idea of a *one-way function*: a function (encryption) which is in P, but whose inverse (decryption) is not. For instance, RSA cryptography [22] relies on the fact that multiplying two numbers is easy, but factoring seems to be hard. However, it is easy to see that finding the inverse of a polynomial-time function is in NP. Therefore, if $P = NP$ there are no one-way functions, and we can break *any* polynomial-time encryption scheme. To break the RSA method in particular, however, you “only” need $\text{FACTORIZATION} \in P$.

Secondly, and most profoundly, if $P = NP$ then mathematics would no longer be the same. Consider a problem of finding proofs for the most difficult and elusive mathematical problems. Finding proofs is hard, but *checking* them is not, as long as they are carefully written in a formal language. Indeed, checking a formal proof is just a matter of making sure that each line follows from the previous ones according to the axioms we are working with. The time it takes to do this is clearly polynomial as a function of the length of the proof, so the following problem is in P:

PROOF CHECKING

Input: A set of axioms A , a statement S , and a proof P
 Question: Is P a valid proof of S with axioms A ?

Then the following decision problem is in NP:

PROOF EXISTENCE

Input: A set of axioms A , a statement S , and an integer ℓ given in unary
 Question: Does S have a proof of length ℓ or less?

Now suppose that $P = NP$. Then you can take your favorite unsolved mathematical problem—the Riemann hypothesis, the Goldbach conjecture, you name it—and use your polynomial-time algorithm for PROOF EXISTENCE to search for proofs of less than, say, a million lines. The point is that no proof constructed by a human will be longer than a million lines anyway, so if no such proof exists, we have no hope of finding it. In fact, a polynomial algorithm for PROOF EXISTENCE can be used to design a polynomial algorithm that actually outputs the proof (if there is one). If $P = NP$, mathematics could be done by a computer. This solution of the P vs. NP millennium problem would probably allow you to solve the other six millennium problems, too, and this, in turn, would get you far more than just invitations to conferences.

2.7 Optimization

So far we have classified decision problems. This was mainly for technical reasons, and the notions of polynomial reductions and completeness apply to other problems as well. The most prominent problems are from combinatorial optimization. Here the task is not to find the needle in a haystack, but the shortest (or longest) blade of hay.

As an example consider the following problem from network design. You have a business with several offices and you want to lease phone lines to connect them up with each other. The phone company charges different amounts of money to connect different pairs of cities, and your task is to select a set of lines that connects all your offices with a minimum total cost.

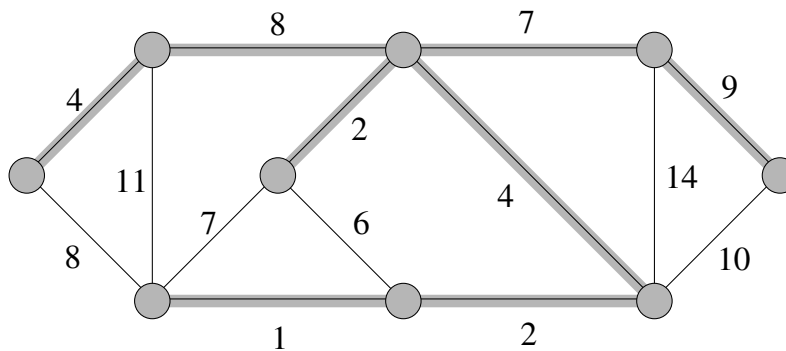


Figure 2.6. A weighted graph and its minimum spanning tree (colored edges).

In mathematical terms the cities and the lines between them form the vertices V and edges E of a weighted graph $G = (V, E)$, the weight of an edge being the leasing costs of the corresponding phone line. Your task is to find a subgraph that connects all vertices in the graph, i.e., a spanning subgraph, and whose edges have minimum total weight. Your subgraph

should not contain cycles, since you can always remove an edge from a cycle keeping all nodes connected and reducing the cost. A graph without cycles is a tree, so what you are looking for is a *minimum spanning tree* in a weighted graph (Fig. 2.6).

MST (MINIMUM SPANNING TREE)

Input: A weighted graph $G = (V, E)$ with non-negative weights
 Question: A tree $T \subseteq G$ with minimum total weight.

How do you find a minimum spanning tree? A naive approach is to generate all possible trees with n vertices and keep the one with minimal weight. The enumeration of all trees can be done using Prüfer codes [5], but Cayley's formula tells us that there are n^{n-2} different trees with n vertices. Already for $n = 100$ there are more trees than atoms in the observable universe! Hence exhaustive enumeration is prohibitive for all but the smallest trees. The mathematical insight that turns MST into a tractable problem is this:

Theorem 2.4 *Let $U \subset V$ be any subset of the vertices of $G = (V, E)$, and let e be the edge with the smallest weight of all edges connecting U and $V - U$. Then e is part of the minimum spanning tree.*

Proof. (by contradiction) Suppose T is a minimum spanning tree not containing e . Let $e = (u, v)$ with $u \in U$ and $v \in V - U$. Then because T is a spanning tree it contains a unique path from u to v , which together with e forms a cycle in G . This path has to include another edge f connecting U and $V - U$. Now $T + e - f$ is another spanning tree with less total weight than T . So T was not a minimum spanning tree. $\square$

The theorem allows us to grow a minimum spanning tree edge by edge, using Prim's algorithm, for example:

```
Prim( $G$ )
Input: weighted graph  $G(V, E)$ 
Output: minimum spanning tree  $T \subseteq G$ 
begin
  Let  $T$  be a single vertex  $v$  from  $G$ 
  while  $T$  has less than  $n$  vertices
    find the minimum edge connecting  $T$  to  $G - T$ 
    add it to  $T$ 
  end
end
```

The precise time complexity of Prim's algorithm depends on the data structure used to organize the edges, but in any case $\mathcal{O}(n^2 \log n)$ is an upper bound. (see [9] for faster algorithms). Equipped with such a polynomial algorithm you can find minimum spanning trees with thousands of nodes within seconds on a personal computer. Compare this to exhaustive search! According to our definition, MST is a tractable problem.

Encouraged by the efficient algorithm for MST we will now investigate a similar problem. Your task is to plan an itinerary for a traveling salesman who must visit n cities. You are given

a map with all cities and the distances between them. In what order should the salesman visit the cities to minimize the total distance he has to travel? You number the cities arbitrarily and write down the distance matrix (d_{ij}) , where d_{ij} denotes the distance between city number i and city number j . A tour is given by a *cyclic permutation* $\pi : [1 \dots n] \mapsto [1 \dots n]$, where $\pi(i)$ denotes the successor of city i , and your problem can be defined as:

TSP (TRAVELING SALESMAN PROBLEM)

Input: An $n \times n$ distance matrix with elements $d_{ij} \geq 0$.
 Question: A cyclic permutation π that minimizes $c_n(\pi) = \sum_{i=1}^n d_{i\pi(i)}$

TSP is probably the most famous optimization problem, and there exists a vast literature specially devoted to it, see [11, 16, 21] and references therein. It is not very difficult to find good solutions, even to large problems, but how can we find the *best* solution for a given instance? There are $(n-1)!$ cyclic permutations. The length of a single tour can be calculated in time $\mathcal{O}(n)$; hence exhaustive search has complexity $\mathcal{O}(n!)$. Again this approach is limited to very small instances. Is there a mathematical insight that provides us with a shortcut to the optimum solution, like for MST? Nobody knows! Despite the efforts of many brilliant people, no polynomial algorithm for TSP has been found. The situation reminds us of the futile efforts to find efficient algorithms for NP-complete problems, and in fact, TSP (like many other hard optimization problems) is closely related to NP-complete decision problems. We will discuss this relation in general terms.

The general instance of an optimization problem is a pair (F, c) , where F is the set of feasible solutions and c is a cost function $c : F \rightarrow \mathbb{R}$. We consider only *combinatorial optimization* where the set F is countable. A combinatorial optimization problem P comes in three different flavors:

1. *The optimization problem $P(O)$* : Find the *feasible solution* $f^* \in F$ that minimizes the cost function.
2. *The evaluation problem $P(E)$* : Find the *cost* $c^* = c(f^*)$ of the minimum solution.
3. *The decision problem $P(D)$* : Given a bound $B \in \mathbb{R}$, is there a feasible solution $f \in F$ such that $c(f) \leq B$?

Under the assumption that the cost function c can be evaluated in polynomial time, it is straightforward to write down polynomial reductions that establish

$$P(D) \leq P(E) \leq P(O). \quad (2.18)$$

If the decision variant of an optimization problem is NP-complete, there is no efficient algorithm for the optimization problem at all—unless $P = NP$.

How does this help us with the TSP? Well, the decision variant of TSP is NP-complete, as can be seen by the following reduction from HAMILTONIAN PATH. Let G be the graph that we want to check for a Hamiltonian path and let $V = (v_1, \dots, v_n)$ denote the vertices and $E \subseteq V \times V$ the edges of G . We define the $n \times n$ distance matrix

$$d_{ij} = \begin{cases} 1 & (v_i, v_j) \in E \\ 2 & (v_i, v_j) \notin E \end{cases}. \quad (2.19)$$

Then $G = (V, E)$ has a Hamiltonian path if and only if there is a tour for our salesman of distance strictly less than $n+2$. If we could check the latter in polynomial time, we would have a polynomial algorithm for HAMILTONIAN PATH, and hence a proof for $P = NP$. Problems like the TSP that are not members of NP but whose polynomial solvability would imply $P = NP$ are called NP-hard.

Now that we have shown TSP to be NP-hard, we know that a polynomial time algorithm for TSP is rather unlikely to exist, and we better concentrate on polynomial algorithms that yield a good, but not necessarily the best tour.

What about the reverse direction? If we know that the decision variant of an optimization problem is in P, does this imply a polynomial algorithm for the optimization or evaluation variant? For that we need to prove the reversal of Eq. (2.18),

$$P(O) \leq P(E) \leq P(D). \quad (2.20)$$

$P(E) \leq P(D)$ can be shown to hold if the cost of the optimum solution's cost is an integer with logarithm bounded by a polynomial in the size of the input. The corresponding polynomial reduction evaluates the optimal cost c^* by asking the question "Is $c^* \leq B$?" for a sequence of values B that approaches c^* , similar to the bisection method to find the zeros of a function.

There is no general method to prove $P(O) \leq P(E)$, but a strategy that often works can be demonstrated for the TSP: Let c^* be the known solution of TSP(E). Replace an arbitrary entry d_{ij} of the distance matrix with a value $c > c^*$ and solve TSP(E) with this modified distance matrix. If the length of the optimum tour is not affected by this modification, the link ij does not belong to the optimal tour. Repeating this procedure for different links one can reconstruct the optimum tour with a polynomial number of calls to a TSP(E) solver, hence $TSP(O) \leq TSP(E)$. In that sense $P = NP$ would also imply efficient algorithms for the TSP and many other hard optimization problems.

2.8 Complexity Zoo

At the time of writing the complexity zoo [1] houses 443 complexity classes. We have discussed (or at least briefly mentioned) only five: P, NP, co-NP, NP-complete and NP-hard. Apparently we have seen only the tip of the iceberg! Some of the other 438 classes refer to *space* rather than time complexity, others classify problems that are neither decision nor optimization problems, like *counting problems*: how many blades of the hay of length X are in this haystack? The most interesting classes, however, are based on different (more powerful?) models of computation, most notably randomized algorithms and, of course, quantum computing. As you will learn in Julia Kempe's lecture on quantum algorithms, there is a quantum algorithm that solves FACTORIZATION in polynomial time, but as you have learned in this lecture this is only a very small step toward the holy grail of computational complexity: a polynomial time quantum algorithm for an NP-complete problem.

References

- [1] Scott Aaronson and Greg Kuperberg. Complexity zoo, http://qwiki.caltech.edu/wiki/Complexity_Zoo.
- [2] Scott Joel Aaronson, *Limits on Efficient Computations in the Physical World*, PhD thesis, University of California, Berkeley, 2004 (quant-ph/0412143).
- [3] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P., *Annals of Mathematics*, 160(2):781–793, 2004.
- [4] Bengt Aspvall, Michael F. Plass, and Robert Endre Tarjan, A linear-time algorithm for testing the truth of certain quantified boolean formulas, *Information Processing Letters*, 8(3):121–123, 1979.
- [5] Béla Bollobás, *Modern Graph Theory*, volume 184 of *Graduate Texts in Mathematics*, Springer, Berlin, 1998.
- [6] Stephen Cook, The complexity of theorem proving procedures, In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, pages 151–158, 1971.
- [7] Pierluigi Crescenzi and Viggo Kann, A compendium of NP optimization problems, <http://www.nada.kth.se/~viggo/wwwcompendium>.
- [8] L. Euler, Solutio problematis ad geometriam situs pertinentis, *Comm. Acad. Sci. Imper. Petropol.*, 8:128–140, 1736.
- [9] H.N. Gabow, Z. Galil, T.H. Spencer, and R.E. Tarjan, Efficient algorithms for finding minimum spanning trees in undirected and directed graphs, *Combinatorica*, 6:109–122, 1986.
- [10] Michael R. Garey and David S. Johnson, *Computers and Intractability. A Guide to the Theory of NP-Completeness*, Freeman, New York, 1979.
- [11] Martin Grötschel and Manfred W. Padberg, Die optimierte Odyssee, *Spektrum der Wissenschaft*, 4:76–85, 1999. See also <http://www.spektrum.de/odyssee.html>.
- [12] Clay Mathematics Institute, Millenium problems, <http://www.claymath.org/millennium>.
- [13] D.S. Johnson and C.H. Papadimitriou, Computational complexity, In E.L. Lawler, J.K. Lenstra, A.H.G. Rinnoy Kan, and D.B. Shmoys, editors, *The Traveling Salesman Problem*, Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley, New York, 1985, pages 37–85.
- [14] Vipin Kumar, Algorithms for Constraint Satisfaction Problems: A Survey, *AI Magazine*, 13(1):32–44, 1992. available at <ftp://ftp.cs.umn.edu/dept/users/kumar/csp-aimagazine.ps>.
- [15] R.E. Ladner, On the structure of polynomial time reducibility, *Journal of the ACM*, 22:155–171, 1975.
- [16] E.L. Lawler, J.K. Lenstra, A.H.G. Rinnoy Kan, and D.B. Shmoys, editors, *The Traveling Salesman Problem*, Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley, New York, 1985.
- [17] Harry R. Lewis and Christos H. Papadimitriou, The efficiency of algorithms, *Scientific American*, pages 96–109, 1 1978.
- [18] Stephan Mertens and Cris Moore, *The Nature of Computation*, Oxford University Press, Oxford, 2007.

- [19] Christos H. Papadimitriou, *Computational Complexity*, Addison-Wesley, Reading, MA, 1994.
- [20] V.R. Pratt, Every prime has a succinct certificate, *SIAM J. Comput.*, 4:214–220, 1975.
- [21] Gerhard Reinelt, *The Travelling Salesman. Computational Solutions for TSP Applications*, volume 840 of *Lecture Notes in Computer Science*, Springer-, Berlin, Heidelberg, New York, 1994.
- [22] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Comm. ACM*, 21:120–126, 1978.
- [23] A. Schönhage and V. Strassen, Schnelle Multiplikation grosser Zahlen, *Computing*, 7:281–292, 1971.
- [24] Ingo Wegener, *Complexity Theory*. Springer-Verlag, Berlin, Heidelberg, New York, 2005.

Part II

Foundation of Quantum Information Theory

3 Discrete Quantum States versus Continuous Variables

Jens Eisert

3.1 Introduction

Much of the theory of quantum information science has originally been developed in the realm of quantum bits and trits, so for finite-dimensional quantum systems. The closest analog of the classical bit is the state of the two-level quantum system, and indeed, quite a lot of intuition of classical information theory carries over to the quantum domain [1, 2]. Yet, needless to say, many quantum systems do not fall under this category of being finite dimensional, the familiar simple quantum mechanical harmonic oscillator being an example. Such an oscillator may be realized as a field mode of light or as the vibrational degree of freedom of an ion in a trap. Also, the collective spin of atomic samples can to a good approximation be described as a quantum system of this type. Not very long ago it became clear that such infinite-dimensional quantum systems are also very attractive candidates for quantum information processing, both from a theoretical and from an experimental perspective [3–6].

This early chapter is mainly aiming at “setting the coordinates”, introducing elementary notions of states and operations. We will briefly have a look at the situation in the finite-dimensional case. We will then move on to a description of states and operations in the case of infinite-dimensional quantum systems. Questions of entanglement or protocols as for quantum key distribution are deliberately left out and will be dealt with in detail in later chapters.

Such infinite-dimensional (bosonic) quantum systems have canonical coordinates corresponding to position and momentum. These observables do not have eigenvalues, but a continuous spectrum; hence the term “continuous-variable systems” has been coined to describe the situation. At first one might be led to think that the discussion of states, of quantum operations, and of quantum information processing as such is overburdened with technicalities of infinite-dimensional Hilbert spaces. Indeed, a number of subtle points alien to the finite-dimensional setting arise: for example, without an additional constraint, the entropy and also the degree of entanglement for that matter are typically almost everywhere infinite. Most of these technicalities can yet be tamed, with the help of natural constraints to the mean energy or other linear constraints [7, 8].

A large number of protocols and many properties of quantum states and their manipulation, however, can be grasped in terms that avoid these technicalities rightaway: this is due to the fact that many states that occur in the context of quantum information science can be described in a simple manner in terms of their moments. These Gaussian or quasifree states will be quite in the center of attention in later subsections of this chapter. Finally, we will see that this

language has even something to say when we are not dealing with Gaussian states, but with a class of non-Gaussian states that plays a central role in quantum optical systems.

3.2 Finite-dimensional quantum systems

3.2.1 Quantum states

States embody all information about the preparation of a quantum system that has potential consequences for later statistical measurements. *States* correspond to density operators ρ satisfying [2, 3]

$$\rho \geq 0, \quad \text{tr}[\rho] = 1, \quad \rho = \rho^\dagger.$$

Expectation values of measurements of observables A are given by $\langle A \rangle_\rho = \text{tr}[A\rho]$. So density operators can be thought of defining the linear positive normalized map mapping observables onto their expectation values. Finite-dimensional quantum systems such as two-level or spin systems are equipped with a finite-dimensional Hilbert space $\mathcal{H}$. In a basis $\{|0\rangle, \dots, |d\rangle\}$, any state ρ can be represented as

$$\rho = \sum_{i,j=1}^d \rho_{i,j} |i\rangle\langle j|.$$

The set of all density operators is typically referred to as *state space*.

The state space for a single *qubit* is particularly transparent: it can be represented as the unit ball in $\mathbb{R}^3$, the *Bloch ball*. The Hilbert space of a qubit is spanned by $\{|0\rangle, |1\rangle\}$. In terms of this basis, a state can be written as

$$\rho = \frac{1}{2} (\mathbb{I}_2 + x_1 X + x_2 Y + x_3 Z),$$

where X , Y , and Z denote the Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

So states of single qubits are characterized by vectors $(x_1, x_2, x_3) \in \mathbb{R}^3$ taken from the unit ball, so by *Bloch vectors*.

In general, the state space of a d -dimensional quantum system is a $(d^2 - 1)$ -dimensional convex set: if ρ_1 and ρ_2 are legitimate quantum states, then the convex combination $\lambda\rho_1 + (1 - \lambda)\rho_2$ with $\lambda \in [0, 1]$ is also a quantum state. Such a procedure reflects *mixing* of two quantum states. Convex sets have extreme points, so elements that are no convex combinations of two different elements of the set. The extreme points of state space are the *pure quantum states*. This can be represented as vectors in Hilbert space,

$$|\psi\rangle = \sum_{i=1}^d c_i |i\rangle,$$

$c_1, \dots, c_d \in \mathbb{C}$. State space is convex, but not a simplex: so there are typically infinitely many different representations of states

$$\rho = \sum_{i=1}^K p_i |\psi_i\rangle\langle\psi_i|$$

in terms of pure states, where $(p_1, \dots, p_K)$ is a probability distribution. This innocent-looking fact is at the root of the technicalities in mixed-state entanglement theory: even the very definition of separability or classical correlations refers to the notion of a convex combination of products. Meaning, there must exist a decomposition in terms of extreme points such that each of the terms corresponds to a product, or—in other words—that a state is contained in the convex hull of product states.

Let us end this subsection with a remark on the composition of quantum systems, which is of key relevance when talking about entanglement. The composition of quantum systems is incorporated in the state concept via the *tensor product*: the Hilbert space of a composite system consisting of parts with Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ is defined to be $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. The basis of $\mathcal{H}$ can then identified to be

$$\{|i\rangle \otimes |j\rangle : i = 1, \dots, d_1; j = 1, \dots, d_2\},$$

where $\{|1\rangle, \dots, |d_1\rangle\}$ and $\{|1\rangle, \dots, |d_2\rangle\}$ are bases of $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively.

3.2.2 Quantum operations

A *quantum operation* or a *quantum channel* reflects any processing of quantum information, or any way a state can be manipulated by an actual physical device. When grasping the notion of a quantum operation, two approaches appear to be particularly natural: on the one hand, one may list the elementary operations that are known from any textbook on quantum mechanics, and conceive a general quantum operation as a concatenation of these ingredients. On the other hand, in an axiomatic approach one may formulate certain minimal requirements any meaningful quantum operation has to fulfill in order to fit into the framework of the statistical interpretation of quantum mechanics. Fortunately, the two approaches coincide in the sense that they give rise to the same concept of a quantum operation. We only touch upon this issue, as this will be discussed in great detail in the chapter on quantum channels. To start with the former approach, any quantum operation

$$\rho \longmapsto T(\rho)$$

can be thought of being a consequence of the application of the following elementary operations:

- *Unitary dynamics*: Time evolution according to Schrödinger dynamics gives rise to a unitary operation

$$\rho \longmapsto U\rho U^\dagger.$$

- *Composition of systems*: For states ω , this is

$$\rho \longmapsto \rho \otimes \omega.$$

This is the composition with an uncorrelated additional system.

- *Partial traces*: This amounts to

$$\rho \longmapsto \text{tr}_E[\rho]$$

in a composite quantum system.

- *Von-Neumann measurements*: This is a measurement associated with a set of orthogonal projections, $\pi_1, \dots, \pi_K$.

Now, to mention the latter approach, any quantum operation T consistent with the statistical interpretation of quantum mechanics must certainly be linear and positive: density operators must be mapped onto density operators. Trace preservation of the map incorporates that the trace of the density operator remains to be given by unity.

However, perhaps surprisingly, mere positivity of the map T is not enough: it could well be that the map is applied to a part of a composite quantum system which has previously been prepared in an entangled state. Needless to say, the image under this map must again correspond to a legitimate density operator. This means that we have to require that

$$T \otimes \mathbb{I}_n$$

is positive for all $n \in \mathbb{N}$. It may at first not appear very intuitive that this is a stronger requirement as mere positivity, referred to as *complete positivity*. The good news is that these conditions are already enough to specify the class of maps that correspond to physical quantum operations, being identical to the above sketched class of concatenated maps. So obviously, quantum channels are completely positive maps. They can be cast into the general form

$$\rho \longmapsto T(\rho) = \sum_{i=1}^K A_i \rho A_i^\dagger.$$

Trace preservation is reflected as $\sum_{i=1}^K A_i^\dagger A_i = \mathbb{I}$. If they are unital, they satisfy $\sum_{i=1}^K A_i A_i^\dagger = \mathbb{I}$. In turn, any such completely positive map can be formulated as a dilation of the form

$$T(\rho) = \text{tr}_E[U(\rho \otimes \rho_E)U^\dagger],$$

where U is a unitary acting in $\mathcal{H}$ and the Hilbert space $\mathcal{H}_E$ of an “environment.” So any channel can be thought of as resulting from an interaction with an additional quantum system, so a system one does not have complete access to.

3.3 Continuous-variables

So much about finite-dimensional quantum systems. What can we say now if the system is an infinite-dimensional quantum system [4–6], such as a system consisting of field modes of light [9–12] or collective spin degrees of freedom [13, 14]? As mentioned before, the term “infinite-dimensional quantum system” refers to the fact that the underlying Hilbert space $\mathcal{H}$ is infinite dimensional. The prototypical example of such a system is a single mode, so a single *quantum harmonic oscillator*. Its canonical coordinates of position and momentum are

$$X = (a + a^\dagger)/\sqrt{2}, \quad P = -i(a - a^\dagger)/\sqrt{2},$$

here expressed in terms of creation and annihilation operators. A basis of its Hilbert space which is dense is given by the set of *number state vectors*

$$\{|n\rangle : n \in \mathbb{N}\}.$$

For such infinite-dimensional systems with a finite number of degrees of freedom, the state concept of density operators is just the same as before—except that we have to require that the density operators are of trace class. Needless to say, the carrier of a state does not have to be finite. For example, the familiar *coherent state*—so important in quantum optics—has the state vector

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad (3.1)$$

$\alpha \in \mathbb{C}$, satisfying $a|\alpha\rangle = \alpha|\alpha\rangle$.

3.3.1 Phase space

The physics of N canonical (bosonic) degrees of freedom—or modes for that matter—is that of N harmonic oscillators. Such a quantum system is described in a *phase space*. The phase space of a system of N degrees of freedom is $\mathbb{R}^{2N}$, equipped with an anti-symmetric bilinear form [3, 6, 15, 16]. The latter originates from the canonical commutation relations between the canonical coordinates. Writing the canonical coordinates as $(R_1, \dots, R_{2N}) = (X_1, P_1, \dots, X_N, P_N)$, the *canonical commutation relations* can be expressed as

$$[R_k, R_l] = i\sigma_{k,l}\mathbb{I},$$

where the skew-symmetric $2N \times 2N$ -matrix σ is given by

$$\sigma = \bigoplus_{i=1}^N \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

This matrix is block diagonal, as observables of different degrees of freedom certainly commute with each other. Here, units have been chosen such that $\hbar = 1$. The commutation

relations are those of position and momentum, although, needless to say, this should not be taken too literal: these coordinates correspond, for example, to the quadratures of field modes of light.

A convenient tool for a description of states in phase space is the *displacement operator*—or, depending on the scientific community, *Weyl operator*. Defined as

$$W_\xi = e^{i\xi^T \sigma R}$$

for $\xi \in \mathbb{R}^{2N}$, it is straightforward to see that this operator indeed generates translations in phase space. For a single degree of freedom this displacement operator becomes

$$W_{(x,p)} = e^{ixP_1 - ipX_1}.$$

The canonical commutation relations manifest themselves for Weyl operators as $W_\xi W_\eta = e^{-i\xi^T \sigma \eta} W_{\xi+\eta}$.

Equivalent to referring to a state, i.e., a density operator, one can specify the state of a system with canonical coordinates by means of a suitable function in phase space. In the literature one finds a plethora of such phase space functions, each of which equipped with a certain physical interpretation. One of them is the *characteristic function* [6, 17, 18]. It is defined as the expectation value of the Weyl operator, so as

$$\chi(\xi) = \text{tr}[W_\xi \rho].$$

This is generally a complex-valued function in phase space. It uniquely defines the quantum state, which can be reobtained via $\rho = \int d^{2N} \xi \chi(\xi) W_\xi^\dagger / (2\pi)^N$. The characteristic function is the Fourier transform of the *Wigner function*, so familiar in quantum optics,

$$\mathcal{W}_\rho(\xi) = \frac{1}{(2\pi)^N} \int d^{2N} \eta e^{i\xi^T \sigma \eta} \chi(\eta).$$

The Wigner function is a real-valued function in phase space. It is normalized, in that for a single mode the integral over phase space delivers the value 1. Yet, it is in general not a probability distribution, and it can take negative values.

One of the useful properties is the so-called *overlap property* [17, 18]. If we define the Wigner function of the operators A_1 and A_2 as the Fourier transforms of $\xi \mapsto \text{tr}[A_1 W_\xi]$ and $\xi \mapsto \text{tr}[A_2 W_\xi]$, respectively, and denote them with $\mathcal{W}_{A_1}$ and $\mathcal{W}_{A_2}$, we have that

$$\text{tr}[A_1 A_2] = (2\pi)^N \int d^{2N} \xi \mathcal{W}_{A_1}(\xi) \mathcal{W}_{A_2}(\xi).$$

This can straightforwardly be used to determine moments of canonical coordinates. For example, assume that we know the Wigner function. How can we determine from it the first moment of the position observable? This is easily found to be

$$\langle X \rangle_\rho = \int_{-\infty}^{\infty} dx dp x \mathcal{W}_\rho(x, p).$$

Similarly, the expectation value of the momentum operator is obtained as

$$\langle P \rangle_\rho = \int_{-\infty}^{\infty} dx dp p \mathcal{W}_\rho(x, p).$$

Needless to say, similar expressions can be found for integration along any direction in phase space.

Often, it is also convenient to describe states in terms of their moments [3, 6]. The *first moments* are the expectation values of the canonical coordinates, so $d_k = \langle R_k \rangle_\rho = \text{tr}[R_k \rho]$. The *second moments*, in turn, can be embodied in the real symmetric $2N \times 2N$ -matrix γ , the entries of which are given by

$$\gamma_{j,k} = 2\text{Re}(\langle (R_j - d_j)(R_k - d_k) \rangle_\rho),$$

$j, k = 1, \dots, N$. This matrix is typically referred to as the covariance matrix of the state. Similarly, higher moments can be defined.

3.3.2 Gaussian states

As mentioned before, Gaussian states play a central role in continuous-variable systems, so in quantum systems with canonical coordinates. *Quantum states* of a system consisting of N degrees of freedom are called Gaussian (or also *quasifree*) if its characteristic function is a Gaussian function in phase space [3, 5, 6, 16], that is, if χ takes the form

$$\chi(\rho) = \exp(i\xi^T \sigma d - \xi^T \sigma^T \gamma \sigma \xi / 4)$$

As Gaussians are defined by their first and second moments, so are Gaussian states. The vector d and the matrix γ can then be identified as the displacement and covariance matrix in the above sense.

What states are now Gaussian in this sense? *Coherent states* with state vectors as in Eq. (3.1) constitute important examples of Gaussian states, having a covariance matrix $\gamma = \mathbb{I}_2$: Coherent states are nothing but vacuum states, displaced in phase space. The covariance matrix of a *squeezed vacuum state* is given by $\gamma = \text{diag}(d, 1/d)$ for $d > 0$ (and rotations thereof), $-\log d$ being its squeezing parameter. Thermal or Gibbs states are also Gaussian states, which can in the number basis expressed as

$$\rho = \sum_{n=0}^{\infty} \frac{1}{\bar{n} + 1} \left(\frac{\bar{n}}{\bar{n} + 1} \right)^n |n\rangle \langle n|,$$

where $\bar{n} = (e^\beta - 1)^{-1}$ is the mean photon number of the thermal state of inverse temperature $\beta > 0$. These states are mixed, with covariance matrix

$$\gamma = (2\bar{n} + 1)\mathbb{I}_2.$$

3.3.3 Gaussian unitaries

The significance of the Gaussian states, needless to say, stems in part from the significance of Gaussian operations. Gaussian unitaries are generated by Hamiltonians which are at most quadratic in the canonical coordinates: such Hamiltonians, yet, are ubiquitous in physics [6]. So a Gaussian unitary operation is of the form

$$\rho \mapsto U\rho U^\dagger, \quad U = \exp\left(\frac{i}{2} \sum_{k,l} H_{k,l} R_k R_l\right),$$

H being real and symmetric, corresponding to a bosonic quadratic Hamiltonian. Such unitaries correspond to a representation of the symplectic group $Sp(2N, \mathbb{R})$. It is formed by those real matrices for which

$$S\sigma S^T = \sigma.$$

In other words, these transformations are the familiar transformations from one legitimate set of canonical coordinates to another. In turn, the connection from S to the Hamiltonian is determined by $S = e^{H\sigma}$. It is convenient to keep track of the action of Gaussian unitaries on the level of second moments [5, 6, 15, 16], i.e., covariance matrices, as

$$\gamma \mapsto S\gamma S^T.$$

Those Gaussian unitaries that are energy preserving are typically called *passive*. In the optical context, such unitaries preserve the total photon number. Beam splitters of some transmittivity t and phase shifts, for example, have this property. They correspond—in the convention chosen in this chapter—to

$$\begin{aligned} S_{\text{BS}} &= \begin{pmatrix} \sqrt{t}\mathbb{I}_2 & \sqrt{1-t}\mathbb{I}_2 \\ -\sqrt{1-t}\mathbb{I}_2 & \sqrt{t}\mathbb{I}_2 \end{pmatrix}, & t \in [0, 1], \\ S_{\text{PS}} &= \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix}, & \phi \in [0, 2\pi). \end{aligned}$$

Whether a transformation is passive or not can easily be read off from the matrix S : the matrices S corresponding to passive operations are exactly those that are orthogonal, $S \in SO(N)$. These transformations again form a group, $Sp(2N, \mathbb{R}) \cap O(2N)$. This group is a representation of $U(N)$, which is a property that can conveniently be exploited when assessing quantum information tasks that are assessable using passive optics (see, e.g., Ref. [19]).

Active transformations, in contrast, do not preserve the total photon number. Operations that induce squeezing in optical systems are such active transformations. The most prominent example is a unitary that squeezes the quantum state of a single mode,

$$U = \exp\left(\frac{x}{2}(a^2 - (a^\dagger)^2)\right),$$

the number $x > 0$ characterizing the strength of the squeezing. We find that

$$S = \text{diag}(e^{-x}, e^x);$$

this matrix in turn determines the transformation on the level of covariance matrices.

It seems a right moment to get back to the constraint that any covariance matrix actually has to satisfy. Is any real symmetric $2N \times 2N$ -matrix a legitimate covariance matrix? The answer can only be “no”; the *Heisenberg uncertainty principle* constrains the second moments of any quantum state. The Heisenberg uncertainty principle may be expressed as the semidefinite constraint

$$\gamma + i\sigma \geq 0. \quad (3.2)$$

In turn, for any real symmetric matrix there exists a state ρ having these second moments [3,6].

That this is indeed nothing but the familiar Heisenberg uncertainty principle can be seen as follows: For any covariance matrix γ of a system with N degrees of freedom, there exists an $S \in Sp(2N, \mathbb{R})$ such that

$$S\gamma S^T = \bigoplus_{i=1}^N s_i \mathbb{I}_2. \quad (3.3)$$

The numbers $s_1, \dots, s_N$ can be identified to be given by the positive part of the spectrum of $i\sigma\gamma$. This is the *normal mode decomposition*, resulting from the familiar procedure of decoupling a coupled system of harmonic oscillators. The covariance matrix of Eq. (3.3) is then the covariance matrix of a system of N uncoupled modes, each of which is in a thermal state of mean “photon number” $\bar{n}_i = (s_i - 1)/2$ [15, 16]. Now, having this in mind, we can reduce (3.2) to a single-mode problem, for a covariance matrix of the form $\gamma = \text{diag}(s, s)$. For the covariance matrix of one of these uncoupled modes, in turn, the Heisenberg uncertainty principle becomes

$$\Delta X \Delta P \geq 1/2,$$

where $\Delta X = \langle (X - \langle X \rangle_\rho)^2 \rangle_\rho$ and $\Delta P = \langle (P - \langle P \rangle_\rho)^2 \rangle_\rho$.

This normal mode decomposition is a very helpful tool when evaluating any quantity dependent on quantum states that is unitarily invariant. For example, to calculate the (*Von Neumann*) entropy $S(\rho) = -\text{tr}[\rho \log \rho]$ of a Gaussian state becomes a straightforward enterprise, once the problem is reduced to a single-mode problem using this Williamson normal form.

Finally, in this subsection, let us note that Gaussian states can be characterized by entropic expressions: Namely, Gaussian states are those quantum states for fixed first and second moments that have the *largest entropy*. Quite surprisingly, it is not at all technically involved to show that this is the case. If σ is any quantum state having the same first and second moments as the Gaussian state ρ , then

$$S(\rho) - S(\sigma) = S(\rho, \sigma) + \text{tr}[(\sigma - \rho) \log \rho],$$

the first symbol on the right-hand side denoting the quantum relative entropy. This argument shows that in fact, Gaussians have the largest Von-Neumann entropy. This may be regarded as a manifestation of the *Jaynes minimal information principle*.

3.3.4 Gaussian channels

A more general class of Gaussian operations is given by the *Gaussian channels* [20–22]. Such Gaussian channels play a quite central role in quantum information with continuous variables.

Most prominently, they are models for optical fibers as noisy or lossy transmission lines. A Gaussian channel is again of the form

$$\rho' = T(\rho) = \text{tr}_E[U(\rho \otimes \rho_E)U^\dagger], \quad (3.4)$$

where now U is a Gaussian unitary and ρ_E is a Gaussian state of some number of degrees of freedom. Such channels arise whenever one encounters a coupling which is at most quadratic in the canonical coordinates, to some external degrees of freedom, in turn governed by some bosonic quadratic Hamiltonian. Needless to say, such a situation is quite ubiquitous. Whenever one encounters, say, a weak coupling of canonical degrees of freedom to a some bosonic heat bath, it gives rise to a Gaussian channel in this sense.

How can such channels now concisely be described? Since they map Gaussian states onto Gaussian states, they are—up to displacements—completely characterized by their action on second moments. This action can be cast into the form

$$\gamma \mapsto \gamma' = F^T \gamma F + G, \quad (3.5)$$

where G is a real symmetric $2N \times 2N$ -matrix, and F is an arbitrary real $2N \times 2N$ -matrix [20, 21]. On the level of Weyl or displacement operators, this can be grasped as $W_\xi \mapsto W_{F\xi} \exp(-\xi^T G \xi / 2)$.

In more physical terms, the matrix X may be said, roughly speaking, to determine the amplification or attenuation part of the channel. The matrix Y originates from the “quantum noise induced by the coupling with the environment.” Not every pair of matrices F and G result in a legitimate quantum channel: from complete positivity we have that

$$G + i\sigma - iF^T \sigma F \geq 0. \quad (3.6)$$

This inequality sign originates again from the Heisenberg uncertainty principle. Eqs. (3.5) and (3.6) specify the most general Gaussian quantum channel as given by Eq. (3.4).

An important example of such Gaussian channels in practice is the *lossy channel*. This channel does what the name indicates: it loses photons. It can be modeled by a beam splitter of transmittivity $t \in [0, 1]$ with an empty port in which the vacuum is coupled in. In the above language, this becomes

$$F = \sqrt{t}\mathbb{I}_2, \quad G = (t - 1)\mathbb{I}_2.$$

Then, the channel that induces *classical Gaussian noise* is a Gaussian quantum channel [23, 24]. This channel can be conceived as resulting from random displacements in phase space with a Gaussian weight,

$$T(\rho) = \frac{1}{4\pi \det[G]^{1/2}} \int d^2\xi W_\xi \rho W_\xi^\dagger e^{-i\xi^T G^{-1} \xi},$$

which is reflected as a map

$$\gamma \mapsto \gamma' = \gamma + G,$$

with a positive matrix G . This classical noise channel can also be realized as a lossy channel, followed by an amplification, which is identical to the lossy channel, yet with $t > 1$.

In this language, one can also conveniently read off how well an impossible operation can be approximated in a way that induces minimal noise. For example, optical *phase conjugation* is an impossible operation, in that there is no device that perfectly performs this operation with perfect fidelity. This would correspond to a channel of the above form with

$$F = \text{diag}(1, -1).$$

However, if we allow for $G = (2, 2)$, then the map $\gamma \mapsto F^T \gamma F + G$ corresponds to a channel, so a legitimate completely positive map. One may say—which can also be made more precise in terms of a figure of merit—that for Gaussian states far away from minimum uncertainty, this additional offset Y hardly matters. Close to minimal uncertainty, this additional noise leads to a significant deviation from actual phase conjugation.

Then, how well can *Gaussian quantum cloning* be implemented? The answer to this question depends, needless to say, on the figure of merit. Natural choices would be the joint fidelity of the output with respect to two specimens of the input, or the single clone fidelity. However, if we ask which symmetric Gaussian channel approximates the perfect cloner inducing minimal noise, then the answer will take us only a single line. We fix F to be identical to

$$F = \begin{pmatrix} \mathbb{I}_2 & \mathbb{I}_2 \\ 0 & 0 \end{pmatrix};$$

then $G = \mathbb{I}_4/2$ is a minimal solution of (3.6). This can be conceived as an optimal cloner inducing minimal noise [25]. Indeed, it turns out that this channel is identical to the optimal $1 \rightarrow 2$ -cloner when the joint fidelity is taken as the figure of merit [26]. So when judging clones by means of their joint fidelity, a Gaussian channel amounts indeed to the optimal cloner for Gaussian states, which is by no means obvious. Interestingly, it turns out that when one judges single clones (by means of the single-copy fidelity), the optimal cloner is no longer Gaussian [27].

3.3.5 Gaussian measurements

If we project parts of a system in a Gaussian state onto a Gaussian state of a single mode, how do we describe the resulting Gaussian state? This is nothing but a non-trace-preserving channel. In practice, this occurs in a dichotomic measurement associated with Kraus operators

$$K_0 = |0\rangle\langle 0|, \quad K_1 = \sum_{n=1}^{\infty} |n\rangle\langle n|.$$

A perfect avalanche photodiode could be described by a measurement of this type: K_0 corresponds to the outcome that no photon has been detected, K_1 to the one in which photons have been detected, although there is no finer resolution concerning the number of photons. Imperfect detectors may be conveniently and accurately described by means of a lossy channel, followed by a measurement of this type.

In a system consisting of $N + 1$ modes in a Gaussian state ρ , what would be the covariance matrix of

$$\rho' = \frac{\text{tr}_{N+1}[\langle 0|\rho|0\rangle]}{\text{tr}[\langle 0|\rho|0\rangle]}?$$

The covariance matrix of ρ can be written as

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix},$$

where A is a $2N \times 2N$ -matrix and B is a 2×2 -matrix. It turns out that the covariance matrix of the resulting (unmeasured) N modes is given by [28]

$$\gamma' = A - C(B + \mathbb{I}_2)^{-1}C^T.$$

This expression can be identified as a Schur complement of the matrix $\gamma + 0_N \oplus \mathbb{I}_2$. This formula provides a very useful description of the resulting state after a vacuum projection, without the need of actually determining the resulting quantum state explicitly.

In turn, a homodyne detection leads to a covariance matrix of the form [28]

$$\gamma' = A - C(\pi B \pi)^{-1}C^T,$$

where π is a 2×2 -matrix of rank 1. The inverse has then to be understood as the pseudo inverse. The most general Gaussian operation, including Gaussian measurements, resulting from the concatenation of the above elementary operations [28–30], gives rise to a transformation on the level of covariance matrices

$$\gamma \mapsto \gamma' = \tilde{\Gamma}_1 - \tilde{\Gamma}_{1,2}(\tilde{\Gamma}_2 + \gamma)^{-1}\tilde{\Gamma}_{1,2}^T.$$

Here, Γ is by itself a covariance matrix on $2N$ modes,

$$\Gamma = \begin{pmatrix} \Gamma_1 & \Gamma_{1,2} \\ \Gamma_{1,2}^T & \Gamma_2 \end{pmatrix},$$

and $\tilde{\Gamma} = P\Gamma P$, where

$$P = \mathbb{I}_{2N} \oplus \mathbb{I}_N \oplus (-\mathbb{I}_N)$$

is the covariance matrix of the partial transposition of the Gaussian state described by Γ . This is the transformation law for any completely positive map that maps Gaussian states onto Gaussian states. This approach can be understood in terms of the isomorphism between completely positive maps and positive operators [29–31]. If one asks a question what operations are accessible in the Gaussian setting, this is a natural starting point.

3.3.6 Non-Gaussian operations

It might appear ridiculous to think that the formalism of Gaussian states and Gaussian operations has anything to contribute once we leave the strict framework of the Gaussian setting. After all, with general quantum operations, the reduced description in terms of first and second moments becomes inappropriate.¹ However, for the probably most important Gaussian operation from the quantum optical perspective, this language is still valuable.

This measurement again corresponds to a dichotomic measurement distinguishing the absence or presence of photons, as realized with perfect avalanche photon detectors. In contrast to the case of the outcome associated with $K_0 = |0\rangle\langle 0|$, the outcome of $K_1 = \sum_{n=1}^{\infty} |n\rangle\langle n|$ does not correspond to a Gaussian operation. Yet, it is clear how one can describe the state ρ after such a measurement in mode labeled $N+1$ —corresponding to a “click” in the detector—of an entangled of N modes:

$$\rho = \text{tr}_{N+1}[\rho - \langle 0|\rho|0\rangle].$$

This is not a convex combination of Gaussian states, but nevertheless a sum of two Gaussians, each of which can be characterized by its moments. So in a network consisting of only Gaussian unitaries and k such yes–no detectors, the resulting state will at most be a sum of 2^k contributions, each of which has a description in terms of first and second moments, as can be obtained from the above Schur complements.

An important measurement of this type is the one where one “subtracts a photon.” Here, in one of the ports of a beam splitter the input of a single mode is fed in, into the other vacuum, such that the second moments transformation becomes

$$\gamma \longmapsto S_{\text{BS}}(\gamma \oplus \mathbb{I}_2)S_{\text{BS}}^T.$$

Then, one postselects on the outcomes corresponding to K_1 , to a “clicking” detector. For the values of $t \in [0, 1]$ close to 1, one can, to an arbitrarily good approximation (in trace-norm), realize a transformation

$$\rho \longmapsto \rho' = a\rho a^\dagger$$

at the expense that the respective outcome becomes very unlikely. Hence, this procedure amounts to essentially applying an annihilation operator to the state. Such photon subtractions have been realized experimentally to prepare non-Gaussian states [12]. They form, for example, the starting point of distillation procedures with continuous-variable systems [32] or for ways to violate Bell’s inequalities using homodyne detectors [33].

¹To start with, as an interesting exercise, one can pose the question whether non-Gaussian operations, meaning general completely positive maps, allow for transformations of Gaussian states that are not accessible with Gaussian operations. It turns out that this is indeed the case. For example, in the bipartite setting, there are pure Gaussian states that are accessible starting from pure Gaussian states under non-Gaussian operations, which are inaccessible in the Gaussian framework [31].

References

- [1] I.L. Chuang and M.A. Nielsen, *Quantum information and computation* (Cambridge University Press, Cambridge, 2000).
- [2] R.F. Werner, *Quantum information theory—an invitation*, in *Quantum information—an introduction to basic theoretical concepts and experiments* (Springer, Heidelberg, 2000).
- [3] A.S. Holevo, *Probabilistic and statistical aspects of quantum theory* (North Holland, Amsterdam, 1982).
- [4] S.L. Braunstein and P. van Loock, *Rev. Mod. Phys.* **77**, 513 (2005).
- [5] J. Eisert and M.B. Plenio, *Int. J. Quant. Inf.* **1**, 479 (2003).
- [6] J.I. Cirac, J. Eisert, G. Giedke, M. Lewenstein, M.B. Plenio, R.F. Werner, and M.M. Wolf, textbook in preparation.
- [7] J. Eisert, C. Simon, and M.B. Plenio, *J. Phys. A: Math. Gen.* **35**, 3911 (2002).
- [8] M.E. Shirokov, Preprint, quant-ph/0408009, 2004.
- [9] Ch. Silberhorn, P.K. Lam, O. Weiss, F. Koenig, N. Korolkova, and G. Leuchs, *Phys. Rev. Lett.* **86**, 4267 (2001).
- [10] W.P. Bowen, R. Schnabel, P.K. Lam, and T.C. Ralph, *Phys. Rev. A* **69**, 012304 (2004).
- [11] L.A. Wu, H.J. Kimble, J.L. Hall, and H. Wu, *Phys. Rev. Lett.* **57**, 2520 (1986).
- [12] J. Wenger, R. Tualle-Brouiri, and P. Grangier, *Phys. Rev. Lett.* **92**, 153601 (2004).
- [13] J. Sherson, K. Mølmer, *Phys. Rev. A* **71**, 033813 (2005).
- [14] A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, *Science* **282**, 706 (1998).
- [15] R. Simon, E.C.G. Sudarshan, and N. Mukunda, *Phys. Rev. A* **36**, 3868 (1987).
- [16] Arvind, B. Dutta, N. Mukunda, and R. Simon, *Pramana* **45**, 471 (1995).
- [17] W. Schleich, *Quantum optics in phase space* (Wiley-VCH, Weinheim, 2001).
- [18] D.F. Walls and G.J. Milburn, *Quantum optics* (Springer, Berlin, 1994).
- [19] M.M. Wolf, J. Eisert, and M.B. Plenio, *Phys. Rev. Lett.* **90**, 047904 (2003).
- [20] J. Eisert and M.M. Wolf, Preprint, quant-ph/0505151, 2005.
- [21] B. Demoen, P. Vanheuverzwijn, and A. Verbeure, *Rep. Math. Phys.* **15**, 27 (1979).
- [22] A. Holevo and R.F. Werner, *Phys. Rev. A* **63**, 032312 (2001).
- [23] J. Harrington and J. Preskill, *Phys. Rev. A* **64**, 062301 (2001).
- [24] V. Giovannetti, S. Lloyd, L. Maccone, and P.W. Shor, *Phys. Rev. Lett.* **91**, 047901 (2003).
- [25] G. Lindblad, *J. Phys. A: Math. Gen.* **33**, 5059 (2000).
- [26] N.J. Cerf, A. Ipe, and X. Rottenberg, *Phys. Rev. Lett.* **85**, 1754 (2000).
- [27] N.J. Cerf, O. Krueger, P. Navez, R.F. Werner, and M.M. Wolf, *Phys. Rev. Lett.* **95**, 070501 (2005).
- [28] J. Eisert, S. Scheel, and M.B. Plenio, *Phys. Rev. Lett.* **89**, 137903 (2002).
- [29] J. Fiurasek, *Phys. Rev. Lett.* **89**, 137904 (2002).
- [30] G. Giedke and J.I. Cirac, *Phys. Rev. A* **66**, 032316 (2002).
- [31] G. Giedke, J. Eisert, J.I. Cirac, and M.B. Plenio, *Quant. Inf. Comp.* **3**, 211 (2003).
- [32] J. Eisert, D.E. Browne, S. Scheel, and M.B. Plenio, *Ann. Phys. (NY)* **311**, 431 (2004).
- [33] R. Garcia-Patron Sanchez, J. Fiurasek, N.J. Cerf, J. Wenger, R. Tualle-Brouiri, and Ph. Grangier, *Phys. Rev. Lett.* **93**, 130409 (2004).

4 Approximate Quantum Cloning

Dagmar Bruß and Chiara Macchiavello

4.1 Introduction

Perfect cloning of quantum states that are *a priori* unknown is forbidden by the laws of quantum mechanics [1–3]. Perfect cloning is only possible when the input states belong to a known set of orthogonal states. For example, the controlled-NOT quantum gate [4], which operates as follows on two qubits (two-level systems)

$$|x_1\rangle|x_2\rangle \rightarrow |x_1\rangle|x_1 \oplus x_2\rangle, \quad (4.1)$$

where $\oplus$ denotes addition modulo 2 and $|x_i\rangle \in \{|0\rangle, |1\rangle\}$ represent basis states for each qubit, implements a perfect cloning transformation for qubits, when the second qubit is initially prepared in state $|0\rangle$ (the first qubit is the one to be cloned and is initially in one of the two orthogonal states $|0\rangle$ or $|1\rangle$). The requirement that the input state belongs to a known class of orthogonal states is quite restrictive. It is intuitive to expect that by relaxing the conditions on the class of allowed input states, perfect cloning can be approximated with a decreasing efficiency.

In this chapter we describe approximate cloning transformations for different sets of input states and analyze the corresponding optimal qualities in terms of the fidelity. In Section 4.2 we review the no-cloning theorem. In Section 4.3 we analyze the smallest nontrivial class of input states, namely the set of two nonorthogonal states, and then consider the case of two pairs of orthogonal states. In Section 4.4 we consider another interesting set of input states, namely the one of all possible states lying on the equator of the Bloch sphere. In Section 4.5 we describe the least restrictive case, where the input states of the qubits are completely unknown, and report the optimal fidelities for the case of qubits and then for systems with arbitrary finite dimension. We review the fidelities of the various processes and show how the fidelity increases by restricting the class of inputs. In Section 4.6 we drop the constraint that all copies should have identical output density matrices, and study asymmetric cloning. In Section 4.7 we discuss probabilistic cloning, where perfect copies can be created with a certain probability. Before concluding, we finally briefly report on experimental quantum cloning in Section 4.8.

4.2 The No-Cloning Theorem

The no-cloning theorem states that it is not possible to perfectly clone an unknown quantum state, or a state drawn from a set of two (or more) nonorthogonal states [1–3]. The theorem

can be easily proved by contradiction. Let us assume that such an ideal cloner exists. It can be described by a unitary operator U_c that acts on the global system of the initial copy, in a pure state $|\psi\rangle$, a blank copy on which the state will be cloned, in an initially arbitrary state $|0\rangle$, and, in general, an auxiliary system (ancilla) whose dimension is not specified, initially in a state $|A\rangle$. Note that all the states that we consider are normalized. Assuming that ideal cloning is possible for two nonorthogonal input states $|\psi\rangle$ and $|\phi\rangle$, the cloning transformation would lead to

$$\begin{aligned} U_c(|\psi\rangle|0\rangle|A\rangle) &= |\psi\rangle|\psi\rangle|A_\psi\rangle, \\ U_c(|\phi\rangle|0\rangle|A\rangle) &= |\phi\rangle|\phi\rangle|A_\phi\rangle, \end{aligned} \quad (4.2)$$

where $|A_\psi\rangle$ and $|A_\phi\rangle$ represent the output states of the ancilla and $|\langle A_\psi|A_\phi\rangle| \leq 1$. Since the cloning transformation U_c is unitary, it preserves the scalar product. The scalar product $\langle\psi|\phi\rangle$ of the two possible inputs in the above expressions must then be equal to the corresponding scalar product between the outputs, i.e., $\langle\psi|\phi\rangle^2 \langle A_\psi|A_\phi\rangle$. Since the two possible input states are assumed to be nonorthogonal the above relation leads to

$$\langle\psi|\phi\rangle = \frac{1}{\langle A_\psi|A_\phi\rangle}, \quad (4.3)$$

which clearly can never be satisfied, unless in the trivial case $\langle\psi|\phi\rangle = 1$. Thus, U_c does not exist. All cloning transformations presented in the following sections are therefore *approximate* cloning transformations, the optimal quality of which depends on the scenario.

Another reason for the impossibility of perfect quantum cloning is the impossibility of superluminal signalling: assume the situation where Alice and Bob are distant and share a maximally entangled state, e.g., the singlet state for two qubits. Alice measures her qubit and encodes one bit of information into whether her measurement is in the x - or the z -basis. If Bob possessed a perfect cloner, he could make many perfect copies of his qubit (after Alice's measurement) and measure half of them in the x -basis, half of them in the z -basis. In the case where his basis coincides with Alice's, all measurement outcomes are identical; in the other case half of his results are 0, half of them 1. The speed of information transfer would just depend on the speed of the cloner, and if Alice and Bob were far enough from each other they could communicate with superluminal speed. Note that the impossibility of superluminal signaling does not only arise in a relativistic theory, but also in quantum mechanics, due to linearity of any physical transformation (CP-map) [5].

4.3 State-Dependent Cloning

In this section we study approximate cloning transformations for a set of two nonorthogonal input states, parametrized as follows:

$$\begin{aligned} |a\rangle &= \cos\theta|0\rangle + \sin\theta|1\rangle, \\ |b\rangle &= \sin\theta|0\rangle + \cos\theta|1\rangle, \end{aligned} \quad (4.4)$$

where $\theta \in [0, \pi/4]$. This set of two input states can equivalently be specified by means of their scalar product $S = \langle a|b\rangle = \sin 2\theta$.

We will derive here a lower bound for the fidelity of an optimal $N \rightarrow M$ cloning transformation that operates on N input states of the form $|x\rangle^{\otimes N}$, with $x = a, b$. This analysis was performed in [6] for $N = 1$ and $M = 2$, and later generalized in [7] for any values of N and M . The resulting transformation is called the state-dependent cloner, because its form depends explicitly on the set of initial states, namely on the parameter θ .

We will consider a unitary operator V_{NM} acting on the Hilbert space of M qubits and define the final states $|\alpha_{NM}\rangle$ and $|\beta_{NM}\rangle$ as

$$|\alpha_{NM}\rangle = V_{NM}(|a\rangle^{\otimes N} \otimes |0\rangle^{\otimes M-N}), \quad (4.5)$$

$$|\beta_{NM}\rangle = V_{NM}(|b\rangle^{\otimes N} \otimes |0\rangle^{\otimes M-N}). \quad (4.6)$$

Unitarity gives the following constraint on the scalar product of the final states:

$$\langle\alpha_{NM}|\beta_{NM}\rangle = (\langle a|b\rangle)^N = S^N. \quad (4.7)$$

Note that this ansatz does not describe the most general cloning transformation, because we have not included an auxiliary system. Therefore the fidelities derived below will be lower bounds on the optimal cloning fidelity.

As a convenient criterion for optimality of the cloning transformation, we maximize the average global fidelity $F_g(N, M)$ of both final states $|\alpha_{NM}\rangle$ and $|\beta_{NM}\rangle$ with respect to the perfectly cloned states $|a^M\rangle \equiv |a\rangle^{\otimes M}$ and $|b^M\rangle \equiv |b\rangle^{\otimes M}$. The average global fidelity is defined formally as

$$F_g(N, M) = \frac{1}{2} (|\langle\alpha_{NM}|a^M\rangle|^2 + |\langle\beta_{NM}|b^M\rangle|^2). \quad (4.8)$$

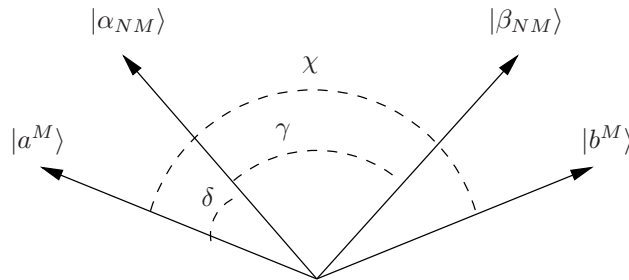


Figure 4.1. Vectors and angles for cloning of two nonorthogonal states. See the text for the notation.

It can be easily shown [6] that the above fidelity is maximized when the states $|\alpha_{NM}\rangle$ and $|\beta_{NM}\rangle$ lie in the two-dimensional space $\mathcal{H}_{a^M, b^M}$, which is spanned by the vectors $\{|a^M\rangle, |b^M\rangle\}$. We will now maximize explicitly the value of the global fidelity (4.8). We can think about it in a geometrical way and define χ , δ and γ as the “angles” between the vectors $|a^M\rangle$ and $|b^M\rangle$, $|a^M\rangle$ and $|\alpha_{NM}\rangle$, $|\alpha_{NM}\rangle$ and $|\beta_{NM}\rangle$ respectively, as illustrated in

Fig. 4.1. The global fidelity (4.8) then takes the form

$$F_g(N, M) = \frac{1}{2} (\cos^2 \delta + \cos^2(\chi - \gamma - \delta)) \quad (4.9)$$

and is thus maximized when the angle between $|a^M\rangle$ and $|\alpha_{NM}\rangle$ is equal to the angle between $|b^M\rangle$ and $|\beta_{NM}\rangle$, i.e., $\delta = \frac{1}{2}(\chi - \gamma)$. The optimal situation thus corresponds to the maximal symmetry in the disposition of the vectors. This symmetry guarantees that the fidelity is the same for both input states $|a^N\rangle$ and $|b^N\rangle$. By inserting the explicit definitions of the angles $\chi = \arccos(S^M)$ and $\gamma = \arccos(S^N)$ —note that due to $M > N$ we have $\chi > \gamma$ —the optimal global fidelity then takes the form

$$F_g^{\text{opt}}(N, M) = \frac{1}{2} (1 + S^{N+M} + \sqrt{1 - S^{2N}} \sqrt{1 - S^{2M}}). \quad (4.10)$$

We will now derive the explicit expression of a different figure of merit, namely the single-copy fidelity $F_{\text{sd}}(N, M)$ of each output copy with respect to the initial state. We first write the output states as

$$\begin{aligned} |\alpha_{NM}\rangle &= (A + B)|a^M\rangle + (A - B)|b^M\rangle \\ |\beta_{NM}\rangle &= (A - B)|a^M\rangle + (A + B)|b^M\rangle, \end{aligned} \quad (4.11)$$

where

$$A = \frac{1}{2} \sqrt{\frac{1 + S^N}{1 + S^M}}, \quad B = \frac{1}{2} \sqrt{\frac{1 - S^N}{1 - S^M}}. \quad (4.12)$$

From the above equations the reduced density operator ρ_α corresponding to one of the M output copies can be easily derived (note that the global states of the M copies $|\alpha_{NM}\rangle$ and $|\beta_{NM}\rangle$ belong to the symmetric subspace, i.e., the space spanned by all states which are invariant under any permutation of the constituent subsystems; therefore, each output copy is described by the same reduced density operator):

$$\rho_\alpha = (A + B)^2 |a\rangle\langle a| + (A - B)^2 |b\rangle\langle b| + (A^2 - B^2) S^{M-1} (|a\rangle\langle b| + |b\rangle\langle a|). \quad (4.13)$$

The fidelity is then calculated as

$$\begin{aligned} F_{\text{sd}}(N, M) &= \langle a | \rho_\alpha | a \rangle \\ &= A^2(1 + S^2 + 2S^M) + B^2(1 + S^2 - 2S^M) + 2AB(1 - S^2). \end{aligned} \quad (4.14)$$

As mentioned above, note that by the symmetry of the transformation the fidelity of the output state ρ_β with respect to the input $|b\rangle$ leads to the same result.

Note that the single-copy fidelities for the cloner of nonorthogonal states (4.14) are just a lower bound. Actually, in order to find the optimal state-dependent cloner to be compared with the phase covariant and universal ones, the fidelity $F_{\text{sd}}(N, M)$ should be maximized explicitly, and in general additional auxiliary systems interacting with the M qubits should be considered in the definition of the cloning transformation V_{NM} . In [6] it was shown that for the $1 \rightarrow 2$ case the maximization of $F_{\text{sd}}(1, 2)$ leads to a different cloning transformation than the one considered here, where the global fidelity is maximized. However, the value of the

resulting optimal fidelity is only slightly different from the fidelity reported in Eq. (4.14) for $N = 1$ and $M = 2$, which was first derived in [6] and reads explicitly

$$F_{\text{sd}}(1, 2) = \frac{1}{2} \left[1 + \frac{1 - S^2}{\sqrt{1 + S^2}} + \frac{S^2(1 + S)}{1 + S^2} \right]. \quad (4.15)$$

As an illustration, we also report here the explicit form of the bound (4.14) for the fidelity corresponding to the case of the $1 \rightarrow 3$ cloner

$$F_{\text{sd}}(1, 3) = \frac{1}{4} \left[2S^3 \left(\frac{1 + S}{1 + S^3} - \frac{1 - S}{1 - S^3} \right) + (1 + S^2) \left(\frac{1 + S}{1 + S^3} + \frac{1 - S}{1 - S^3} \right) + 2(1 - S^2) \sqrt{\frac{1 - S^2}{1 - S^6}} \right]. \quad (4.16)$$

In Fig. 4.2 we show the fidelities for the $1 \rightarrow 2$ and $1 \rightarrow 3$ cloners as functions of the parameter θ . The dashed curve corresponds to $F_{\text{sd}}(1, 2)$, the full curve to $F_{\text{sd}}(1, 3)$. As expected, the values of the fidelity are always much higher than $F_{\text{pc}}^{\text{opt}}(1, 2) = (\sqrt{2} + 1)/(2\sqrt{2}) \approx 0.854$ and $F_{\text{u}}^{\text{opt}}(1, 2) = 5/6 \approx 0.833$ for the $1 \rightarrow 2$ optimal phase covariant and universal cloners, respectively, and than $F_{\text{pc}}^{\text{opt}}(1, 3) = (7 + 2\sqrt{3})/[2(2\sqrt{3} + 3)] \approx 0.809$ and $F_{\text{u}}^{\text{opt}}(1, 3) = 7/9 \approx 0.778$, see Sections 4.4 and 4.5.

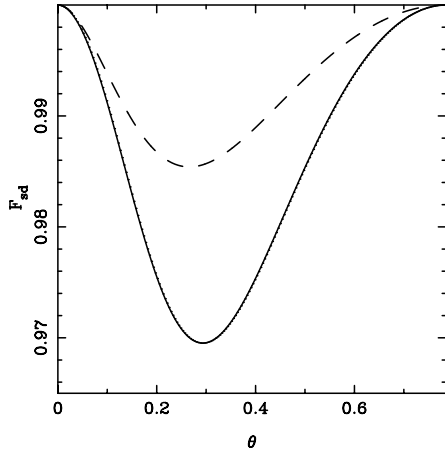


Figure 4.2. Fidelity for each output copy of the state-dependent cloner as a function of the parameter θ . The dashed curve refers to the $1 \rightarrow 2$ cloner (Eq. (4.15)), while the full curve corresponds to the $1 \rightarrow 3$ cloner (Eq. (4.16)).

We can describe the state of each qubit in terms of its Bloch vector representation

$$\rho = \frac{1}{2} (\mathbb{1} + \vec{s} \cdot \vec{\sigma}) , \quad (4.17)$$

where $\mathbb{1}$ is the 2×2 identity matrix, $\vec{s}$ is the Bloch vector (with unit length for pure states) and σ_i are the Pauli matrices. The length of the output Bloch vector can then be easily calculated.

For example, in the $1 \rightarrow 2$ case it takes the form

$$|\vec{s}(1, 2)| = \sqrt{\frac{S^2(1+S)^2}{(1+S^2)^2} + \frac{1-S^2}{1+S^2}}. \quad (4.18)$$

It can be seen that, different from the phase covariant and universal cases which will be analyzed in the next sections, in state-dependent cloning the Bloch vector of the input states is not simply shrunk along the direction of the input Bloch vector, but is also rotated in the Bloch sphere.

We now slightly enlarge the class of possible input states and consider an ensemble that consists of two pairs of orthogonal states for a two-dimensional quantum system [8]. These four states can be parametrized in the Bloch sphere representation with a single parameter in the following way. The four Bloch vectors $\vec{m}_i$ for the states $|\psi_i\rangle$ with

$$|\psi_i\rangle\langle\psi_i| = \frac{1}{2}(\mathbb{1} + \vec{m}_i \cdot \vec{\sigma}) \quad i = 1, \dots, 4, \quad (4.19)$$

where $\mathbb{1}$ is the identity operator and σ_i with $i = x, y, z$ are the Pauli matrices, are given by

$$\begin{aligned} \vec{m}_1 &= \begin{pmatrix} \sin \varphi \\ 0 \\ \cos \varphi \end{pmatrix}, \quad \vec{m}_2 = \begin{pmatrix} -\sin \varphi \\ 0 \\ \cos \varphi \end{pmatrix}, \\ \vec{m}_3 &= \begin{pmatrix} -\sin \varphi \\ 0 \\ -\cos \varphi \end{pmatrix}, \quad \vec{m}_4 = \begin{pmatrix} \sin \varphi \\ 0 \\ -\cos \varphi \end{pmatrix}. \end{aligned} \quad (4.20)$$

In this representation the four vectors are lying in the x, z -plane, and each of them includes an angle $\pm\varphi$ or $\pm(\pi - \varphi)$ with the z -axis, see Fig. 4.3. The two pairs of orthogonal states are given by $\{|\psi_1\rangle, |\psi_3\rangle\}$ and $\{|\psi_2\rangle, |\psi_4\rangle\}$.

We could also parametrize the states $|\psi_i\rangle$ with the real parameters α and β with $\alpha^2 + \beta^2 = 1$:

$$\begin{aligned} |\psi_1\rangle &= \alpha|0\rangle + \beta|1\rangle, & |\psi_2\rangle &= \alpha|0\rangle - \beta|1\rangle, \\ |\psi_3\rangle &= \beta|0\rangle - \alpha|1\rangle, & |\psi_4\rangle &= \beta|0\rangle + \alpha|1\rangle, \end{aligned} \quad (4.21)$$

where the relation between the parameters α and φ is given by

$$\alpha = \cos \frac{\varphi}{2}. \quad (4.22)$$

We study the case of the $1 \rightarrow 2$ cloning and consider the most general cloning transformation as a unitary operation acting on the input, a prescribed blank qubit, and an auxiliary system, initially in an arbitrary state $|X\rangle$. In order to derive the optimal cloning transformation, due to linearity it is sufficient to define its action on the basis states of the input, namely

$$\begin{aligned} U|0\rangle|0\rangle|X\rangle &= a|00\rangle|A\rangle + b(|01\rangle + |10\rangle)|B\rangle + c|11\rangle|C\rangle, \\ U|1\rangle|0\rangle|X\rangle &= \tilde{a}|11\rangle|\tilde{A}\rangle + \tilde{b}(|10\rangle + |01\rangle)|\tilde{B}\rangle + \tilde{c}|00\rangle|\tilde{C}\rangle, \end{aligned} \quad (4.23)$$

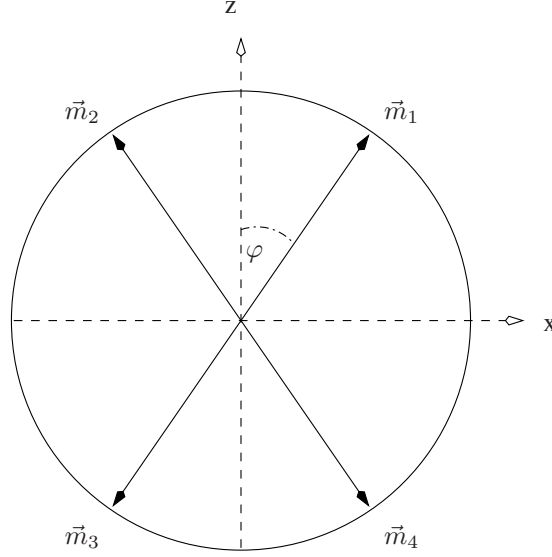


Figure 4.3. Geometrical disposition of two pairs of orthogonal states.

where the coefficients $a, b, c, \tilde{a}, \tilde{b}, \tilde{c}$ can be taken real and positive by including possible phases into the ancilla states. The above form for the cloning transformation guarantees that the two output copies are described by the same reduced density operator. We study cloning transformations that lead to the same efficiency for the four states $|\psi_i\rangle$. Since the four states are transformed into one another by renaming the basis states, i.e., $|0\rangle \leftrightarrow |1\rangle$, the cloning transformation will be invariant under the exchange of $|0\rangle$ and $|1\rangle$. This condition leads to $a = \tilde{a}, b = \tilde{b}, c = \tilde{c}$. Moreover, unitarity of the cloning transformation U dictates the condition

$$a^2 + 2b^2 + c^2 = 1. \quad (4.24)$$

We will now optimize the fidelity F of each output copy with respect to the input state $F = \langle \psi_i | \rho_i | \psi_i \rangle$, where $\rho_i = \text{Tr}[U|\psi_i\rangle\langle\psi_i|U^\dagger]$ and the trace is performed over the auxiliary system and one of the output copies. With our symmetric way to parametrize the states we can easily derive the fidelity for the four input states, as we just have to calculate the fidelity once and can then use symmetry arguments in order to find the explicit form of the other three cases, e.g., we can replace β by $-\beta$ to go from the fidelity for $|\psi_1\rangle$ to the fidelity for $|\psi_2\rangle$. We require the fidelities for the four input states to be equal. This condition leads to

$$F = a^2(\alpha^4 + \beta^4) + 2c^2\alpha^2\beta^2 + b^2 + \alpha^2\beta^2 \left[ab \cdot 2 \text{Re}(\langle A|\tilde{B}\rangle + \langle B|\tilde{A}\rangle) + bc \cdot 2 \text{Re}(\langle B|\tilde{C}\rangle + \langle C|\tilde{B}\rangle) \right]. \quad (4.25)$$

Independently of the coefficients a, b, c the fidelity will be maximal for the following choice of scalar products between the auxiliary states:

$$\begin{aligned}\langle A|\tilde{B}\rangle &= 1 = \langle B|\tilde{A}\rangle, \\ \langle B|\tilde{C}\rangle &= 1 = \langle C|\tilde{B}\rangle,\end{aligned}\tag{4.26}$$

which can be reached with a two-dimensional ancilla and, e.g., the choice

$$\begin{aligned}|A\rangle &= |0\rangle, \quad |B\rangle = |1\rangle, \quad |C\rangle = |0\rangle, \\ |\tilde{A}\rangle &= |1\rangle, \quad |\tilde{B}\rangle = |0\rangle, \quad |\tilde{C}\rangle = |1\rangle.\end{aligned}\tag{4.27}$$

Inserting this into Eq. (4.25) we arrive at

$$F = \frac{1}{2} + \frac{1}{2}(a^2 - c^2) \cos^2 \varphi + b(a + c) \sin^2 \varphi.\tag{4.28}$$

The optimal cloning transformation corresponds to the maximum value of the fidelity (4.28), together with the constraint (4.24) due to unitarity.

Using the method of Lagrange multipliers we thus have to solve the system of equations

$$\begin{aligned}a \cos^2 \varphi + b \sin^2 \varphi &= 2a\lambda, \\ (a + c) \sin^2 \varphi &= 4b\lambda, \\ -c \cos^2 \varphi + b \sin^2 \varphi &= 2c\lambda, \\ a^2 + 2b^2 + c^2 &= 1,\end{aligned}\tag{4.29}$$

where λ is the Lagrange multiplier. The solution for the coefficients a, b and c turns out to be

$$\begin{aligned}a &= \frac{1}{2}(1 + \cos^2 \varphi \sqrt{\frac{1}{\sin^4 \varphi + \cos^4 \varphi}}), \\ b &= \frac{1}{2} \sin^2 \varphi \sqrt{\frac{1}{\sin^4 \varphi + \cos^4 \varphi}}, \\ c &= \frac{1}{2}(1 - \cos^2 \varphi \sqrt{\frac{1}{\sin^4 \varphi + \cos^4 \varphi}}).\end{aligned}\tag{4.30}$$

Inserting this into Eq. (4.28) leads to the optimal fidelity

$$F^{\text{opt}} = \frac{1}{2}(1 + \sqrt{\sin^4 \varphi + \cos^4 \varphi}).\tag{4.31}$$

The explicit form of the resulting optimal cloning transformation is found immediately by inserting Eqs. (4.30) and (4.27) into Eq. (4.23).

In Fig. 4.4 we plot F^{opt} as a function of the angle φ . The figure demonstrates that the cloning task is performed in the worst way for the two pairs being maximally spread, i.e., in the case $\varphi = \pi/4$.

We point out the following geometrical description of the cloning transformation. For states with a Bloch vector lying on the x - z plane of the Bloch sphere, namely states given by the density operator $\rho = \frac{1}{2}(\mathbb{1} + m_x \sigma_x + m_z \sigma_z)$, we can describe the cloning transformation (4.23) in terms of two shrinking factors η_x for the x -component of the Bloch vector, and η_z for its z -component, such that the output state of each copy takes the form

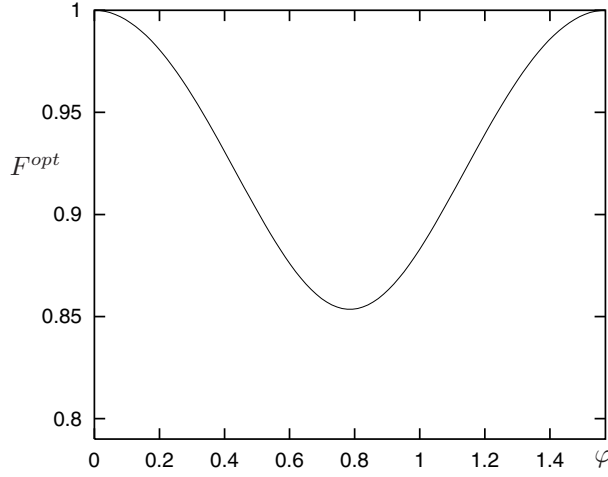


Figure 4.4. Optimal fidelity for cloning two pairs of orthogonal states, as a function of φ .

$\rho_{\text{out}} = \frac{1}{2}(\mathbf{1} + \eta_x m_x \sigma_x + \eta_z m_z \sigma_z)$. The explicit expression for the two shrinking factors with our choice of ancillas (4.27) is given by

$$\begin{aligned}\eta_x &= 2b(a+c), \\ \eta_z &= a^2 - c^2.\end{aligned}\tag{4.32}$$

In the case of the optimal transformation, according to Eq. (4.30), the shrinking factors depend only on the value of φ :

$$\begin{aligned}\eta_x &= \sin^2 \varphi \sqrt{\frac{1}{\sin^4 \varphi + \cos^4 \varphi}}, \\ \eta_z &= \cos^2 \varphi \sqrt{\frac{1}{\sin^4 \varphi + \cos^4 \varphi}}.\end{aligned}\tag{4.33}$$

According to the symmetry of the input ensemble (4.20) that we used to perform the optimization the shrinking factors are related as $\eta_x(\varphi) = \eta_z(\pi/2 - \varphi)$. Furthermore, the identity $\eta_x^2 + \eta_z^2 = 1$ holds. The shrinking factors become equal for $\varphi = \pi/4$, namely $\eta_x(\pi/4) = \eta_z(\pi/4) = 1/\sqrt{2}$. Note that this case turns out to coincide with the optimal $1 \rightarrow 2$ phase covariant cloner, which will be discussed in the following section.

4.4 Phase Covariant Cloning

In this section we extend the set of input states to a continuous one, and consider states of the form

$$|\psi_\phi\rangle = \frac{1}{\sqrt{2}} [|0\rangle + e^{i\phi} |1\rangle] , \quad (4.34)$$

where $\phi \in [0, 2\pi)$. Note that this class of states corresponds to a Bloch vector lying on the x - y plane in the Bloch sphere representation. We are interested in cloning transformations that treat each input state belonging to this class in the same way, namely whose quality does not depend on the value of the phase ϕ . This requirement corresponds to imposing the following phase covariant condition on the operation of the cloning map C_{NM} :

$$U_\varphi \rho^{out} U_\varphi^\dagger = Tr_{M-1} [C_{NM}(U_\varphi^N |\psi_\phi\rangle\langle\psi_\phi| U_\varphi^{\dagger N})] \quad (4.35)$$

for all input states $|\psi_\phi\rangle$ and for all unitary phase shift operators $U_\varphi = \exp(i\varphi) |1\rangle\langle 1|$, where $\varphi \in [0, 2\pi)$. In the above equation Tr_{M-1} denotes the trace operation over all the output copies except one. Cloning transformations satisfying the above condition will be called phase covariant.

It can be shown [9] that phase covariant cloning transformations for input states $|\psi_\phi\rangle$ correspond to a shrinking of the Bloch vector by a factor $\eta_{pc}(N, M)$ (in this case $\eta_{pc}(N, M)$ represents the shrinking in the x - y plane of the Bloch representation). The simplest case of $N = 1$ and $M = 2$ was reported for the first time in [9] and corresponds to the optimal transformation for two pairs of orthogonal states, derived in Section 4.3, for $\varphi = \pi/4$. We point out that this transformation turns out to coincide with the optimal eavesdropping strategy in the BB84 scheme [10].

The case of general N and M was studied in [11, 12]. The derivation is very involved and will not be reported here. In [11] a cloning transformation from an arbitrary number of input copies N to an arbitrary number M of output copies was presented, and was proved to be optimal only for $N = 1$. The optimal maps for the case $N \rightarrow M$ with equal parity of N and M (i.e., N and M are either both even or both odd) were derived in [12]. There is not a unique expression for the optimal single-copy fidelity as a function of N and M . For the $1 \rightarrow M$ case the optimal phase covariant fidelity is given by [12]

$$F_{pcc} = \frac{1}{2} \left(1 + \frac{M+1}{2M} \right) \quad \text{for odd } M , \quad (4.36)$$

$$F_{pcc} = \frac{1}{2} \left(1 + \frac{\sqrt{M(M+2)}}{2M} \right) \quad \text{for even } M . \quad (4.37)$$

Moreover, when N and M have the same parity the fidelity takes the form

$$F_{pcc} = \frac{1}{2} + \frac{1}{M2^N} \sum_{j=0}^{N-1} \sqrt{C(N, j)C(N, j+1)} \sqrt{\left[\frac{(M+N)}{2} - j \right] \left[\frac{(M-N)}{2} + j + 1 \right]} , \quad (4.38)$$

where $C(n, m)$ is the binomial coefficient $C(n, m) \equiv n!/(m!(n-m)!)$. It is interesting to note that, in contrast to the universal case where the optimal maps are the same for optimization of the global or single particle fidelity [13], in the phase covariant case the solutions are in general different [12].

It is possible to extend the definition of phase covariant cloning to higher dimensional systems with finite dimension d , by optimizing the cloning transformations on “equatorial” states

$$|\psi(\{\phi_j\})\rangle = \frac{1}{\sqrt{d}}(|0\rangle + e^{i\phi_1}|1\rangle + e^{i\phi_2}|2\rangle + \dots + e^{i\phi_{d-1}}|d-1\rangle), \quad (4.39)$$

where the ϕ_j ’s are independent phases in the interval $[0, 2\pi)$. The optimal fidelity for the $1 \rightarrow 2$ case is given by [14]

$$F_{\text{d,pcc}}^{\text{opt}} = \frac{1}{d} + \frac{1}{4d} \left(d - 2 + \sqrt{d^2 + 4d - 4} \right). \quad (4.40)$$

The general $N \rightarrow M$ case was analyzed in [15], where explicit simple solutions were obtained for a number of output copies given by $M = kd + N$, with k the positive integer. In this case the optimal fidelity takes the explicit form

$$F_{\text{d,pcc}}^{\text{opt}} = \frac{1}{d} + \frac{1}{Md^{N+1}} \sum_{\{n_j\}} \sum_{i \neq j} \frac{N!}{n_0! \dots n_i! \dots n_j! \dots} \sqrt{\frac{(n_i + k + 1)(n_j + k + 1)}{(n_i + 1)(n_j + 1)}}. \quad (4.41)$$

In the above summation n_j represent d indices that have to fulfill the constraint $\sum_{j=0}^{d-1} n_j = N - 1$. The interesting aspect of these cloning transformations is that they can be achieved “economically,” without the need of auxiliary systems in addition to the M output copies [15].

4.5 Universal Cloning

4.5.1 The case of qubits

We now consider the least restrictive set of pure input states, namely the one corresponding to the whole two-dimensional Hilbert space of a qubit. We will investigate universal cloning transformations, namely transformations whose quality does not depend on the input state. As a figure of merit we use the single-copy fidelity $F_u = \langle \psi | \rho_{\text{out}} | \psi \rangle$.

Universal $N \rightarrow M$ quantum cloning is a unitary transformation acting on an extended input which contains N original qubits all in the same unknown pure state $|\psi\rangle$, $M - N$ “blank” qubits and K auxiliary systems, and leading to M output clones. The “blanks” and the auxiliary systems are initially in some prescribed quantum state. In order to guarantee that the M output qubits have the same reduced density operator ρ_{out} (symmetry condition) we require that the output state of the M copies is supported on the symmetric subspace. When requiring that all input states must be treated in the same way (universality condition) it has been shown [6] that the reduced density operator ρ_{out} , describing the state of each of the M output qubits, is related to the input state, characterized by the Bloch vector $\vec{s}$, via the transformation

$$\rho_{\text{out}} = \frac{1}{2}(\mathbb{1} + \eta_u(N, M)\vec{s} \cdot \vec{\sigma}), \quad (4.42)$$

namely the Bloch vector is just shortened by a shrinking factor $\eta_u(N, M)$. Note that the shrinking factor is simply related to the single-copy fidelity F_u as

$$F_u(N, M) = (1 + \eta_u(N, M))/2. \quad (4.43)$$

In order to optimize the fidelity $F_u(N, M)$, or equivalently the shrinking factor $\eta_u(N, M)$, of an $N \rightarrow M$ universal cloning transformation we follow the approach of [16], relating universal cloning to state estimation. The aim of state estimation is to find a measurement which leads to the best possible estimation of the *a priori* unknown quantum state $|\psi\rangle$. The most general measurement is a positive operator valued measure (POVM), namely a set of positive operators $\{P_\mu\}$, such that $\sum_\mu P_\mu = \mathbf{1}$. Suppose that we have at our disposal N copies of the state $|\psi\rangle$. The outcome of each instance of the measurement provides, with probability $p_\mu(\psi) = \text{Tr}(P_\mu |\psi\rangle\langle\psi|^{\otimes N})$, the “candidate” $|\psi_\mu\rangle$ for $|\psi\rangle$. We can calculate the fidelity $F_{\text{est}}(N)$ of state estimation by averaging over the outcomes of the measurement as follows:

$$F_{\text{est}}(N) = \sum_\mu p_\mu(\psi) |\langle\psi|\psi_\mu\rangle|^2 = \langle\psi|\rho_{\text{est}}|\psi\rangle, \quad (4.44)$$

where $\rho_{\text{est}} = \sum_\mu p_\mu(\psi) |\psi_\mu\rangle\langle\psi_\mu|$ represents the reconstructed density operator corresponding to the state $|\psi\rangle$. For a universal state estimating procedure the fidelity must not depend on $|\psi\rangle$; thus the reconstructed density operator ρ_{est} can also be written as in Eq. (4.42), with shrinking factor $\eta_{\text{est}}(N)$. It has been shown in [17] that the optimal fidelity $F_{\text{est}}^{\text{opt}}(N)$ for the state estimation of N pure qubits has the form

$$F_{\text{est}}^{\text{opt}}(N) = \frac{N+1}{N+2}, \quad (4.45)$$

corresponding to the optimal shrinking factor

$$\eta_{\text{est}}^{\text{opt}}(N) = N/(N+2). \quad (4.46)$$

We now want to show a connection between optimal universal cloning and optimal universal state estimation, given by the equality

$$F_{\text{est}}^{\text{opt}}(N) = F_u^{\text{opt}}(N, \infty). \quad (4.47)$$

To prove it, we first consider a measurement procedure performed on N copies which is composed of an optimal $N \rightarrow L$ cloning process and a subsequent universal measurement on the L output copies. This concept is illustrated in Fig. 4.5. The total procedure can be regarded as a possible state estimation method. Since the state ρ_L of the L output copies of the optimal universal cloner is supported on the symmetric subspace, it can be conveniently decomposed as [18]

$$\rho_L = \sum_i \gamma_i (|\psi_i\rangle\langle\psi_i|)^{\otimes L}, \quad (4.48)$$

where the coefficients γ_i add up to one ($\sum_i \gamma_i = 1$), but are not necessarily positive. After performing the optimal universal measurement on the L outputs of the cloner we can calculate the average fidelity of the total estimation process due to linearity of the measurement

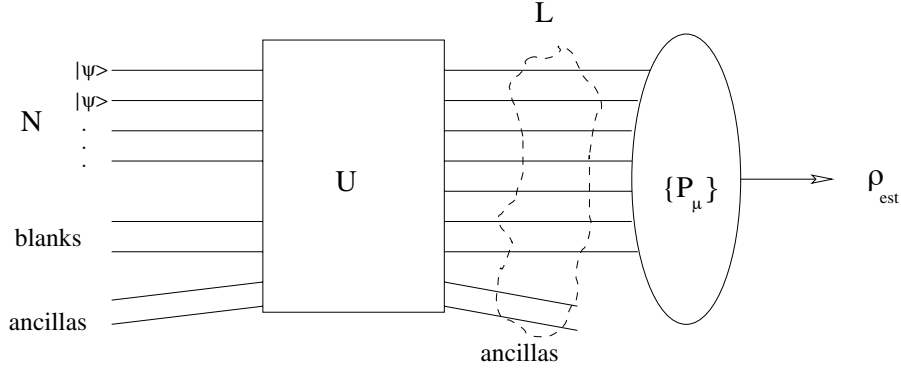


Figure 4.5. Concatenation of an $N \rightarrow L$ cloner with a state estimation of the L copies. The output of the cloner is entangled (as indicated by the dashed line).

procedure as follows:

$$F_{\text{total}}(N, L) = \sum_i \gamma_i \sum_{\mu} p_{\mu}(\psi_i) |\langle \psi_i | \psi_{\mu} \rangle|^2 \quad (4.49)$$

$$= \sum_i \gamma_i \text{Tr} \{ [\eta_{\text{est}}^{\text{opt}}(L) |\psi_i\rangle\langle\psi_i| + (1 - \eta_{\text{est}}^{\text{opt}}(L)) \frac{1}{2} \mathbb{1}] |\psi\rangle\langle\psi| \} , \quad (4.50)$$

where we explicitly exploited the universality of state estimation from Eq. (4.49) to Eq. (4.50). In the limit $L \rightarrow \infty$ we have $\eta_{\text{est}}^{\text{opt}}(\infty) = 1$. Remembering that at the output of the $N \rightarrow L$ cloner $\sum_i \gamma_i |\psi_i\rangle\langle\psi_i| = \eta_{\text{u}}^{\text{opt}}(N, L) |\psi\rangle\langle\psi| + \mathbb{1}(1 - \eta_{\text{u}}^{\text{opt}}(N, L))/2$, the average estimation fidelity in the limit $L \rightarrow \infty$ can be written as

$$\begin{aligned} \lim_{L \rightarrow \infty} F_{\text{total}}(N, L) &= \text{Tr} \{ [\eta_{\text{u}}^{\text{opt}}(N, \infty) |\psi\rangle\langle\psi| + (1 - \eta_{\text{u}}^{\text{opt}}(N, \infty)) \frac{1}{2} \mathbb{1}] |\psi\rangle\langle\psi| \} \\ &= \frac{1}{2} [1 + \eta_{\text{u}}^{\text{opt}}(N, \infty)] . \end{aligned} \quad (4.51)$$

This fidelity cannot be higher than the one for the optimal state estimation performed directly on N pure inputs; thus we conclude

$$F_{\text{u}}^{\text{opt}}(N, \infty) \leq F_{\text{est}}^{\text{opt}}(N) . \quad (4.52)$$

We can derive the opposite inequality by noticing that after performing a universal measurement procedure on N identically prepared input copies $|\psi\rangle$, we can prepare a state of L systems, supported on the symmetric subspace, where each system has the same reduced density operator, given by ρ_{est} . As mentioned above, a universal cloning process generates outputs that are supported on the symmetric subspace. Therefore, the above method of performing state estimation followed by preparation of a symmetric state can be viewed as a universal cloning process and thus it cannot lead to a higher fidelity than the optimal $N \rightarrow L$ cloning transformation. Therefore we find the inequality

$$F_{\text{est}}^{\text{opt}}(N) \leq F_{\text{u}}^{\text{opt}}(N, L) , \quad (4.53)$$

which holds for any value of L , in particular for $L \rightarrow \infty$. The above inequality, together with Eq. (4.52), leads to equality (4.47).

An interesting property of universal cloning transformations is that the shrinking factors of universal cloning machines multiply [16], namely the shrinking factor of a universal $N \rightarrow L$ cloner composed of a sequence of an $N \rightarrow M$ cloner followed by an $M \rightarrow L$ cloner is the product of the two shrinking factors: $\eta_u(N, L) = \eta_u(N, M) \cdot \eta_u(M, L)$. Moreover, since a sequence of an $N \rightarrow M$ and an $M \rightarrow \infty$ universal cloner cannot perform better than the optimal $N \rightarrow \infty$ universal cloner, we can write the following upper bound for an $N \rightarrow M$ cloner:

$$\eta_u(N, M) \leq \frac{\eta_u^{\text{opt}}(N, \infty)}{\eta_u^{\text{opt}}(M, \infty)} = \frac{N(M+2)}{M(N+2)}, \quad (4.54)$$

where we have used Eqs. (4.46), (4.47) and (4.43) on the right-hand side. The corresponding fidelity reads

$$F_u(N, M) \leq \frac{M + N + MN}{M(N+2)}. \quad (4.55)$$

The above bound is achieved by the cloning transformations proposed in [19] for $N = 1$ and $M = 2$, and in [20] for arbitrary values of N and M . The explicit optimal $1 \rightarrow 2$ transformation for universal cloning of qubits, suggested by Bužek and Hillery [19], reads

$$\begin{aligned} U |0\rangle|0\rangle|A\rangle &= \sqrt{\frac{2}{3}}|00\rangle|0\rangle + \sqrt{\frac{1}{6}}(|01\rangle + |10\rangle)|1\rangle, \\ U |1\rangle|0\rangle|A\rangle &= \sqrt{\frac{2}{3}}|11\rangle|1\rangle + \sqrt{\frac{1}{6}}(|01\rangle + |10\rangle)|0\rangle. \end{aligned} \quad (4.56)$$

Here, one still has the freedom of a unitary transformation of the output ancilla states.

4.5.2 Higher dimensions

The optimal $N \rightarrow M$ cloning transformation for pure states in arbitrary finite dimension d was derived in [18]. The corresponding optimal single copy fidelity is given by

$$F_u^{\text{opt}}(N, M) = \frac{M - N + N(M+d)}{M(N+d)}, \quad (4.57)$$

which generalizes the optimal fidelity derived in Eq. (4.55) to an arbitrary finite dimension.

Subsequently explicit unitary realizations of the above transformations were shown in [21]. It is interesting to note that the link (4.47) between optimal universal cloning and optimal universal state estimation can be proved in a very similar way also in the case of higher dimensional systems [22], thus leading to the following explicit evaluation of the optimal fidelity for state estimation of N identical states in dimension d ,

$$F_{\text{est}}^{\text{opt}}(N; d) = \frac{N+1}{N+d}. \quad (4.58)$$

4.5.3 Entanglement structure

In Eq. (4.56) the output of a universal $1 \rightarrow 2$ cloner for qubits was given. It is clear that the output state is entangled. In [23] the entanglement structure for the output of a cloner was studied. For the simple case of a $1 \rightarrow 2$ cloner it was shown that the three-qubit output is an entangled state from the W -class (see Chapter on multipartite entanglement on p. 237). By considering the concurrence, which is a good measure of entanglement for two-qubit subsystems, see chapter on multipartite entanglement on p. 237, it was also shown that the entanglement between clone and ancilla is higher than between the clones.

For the case $N = 1$ and general M it is straightforward to derive an explicit expression for the concurrence between two clones or one clone and one ancilla, by calculating the according reduced density matrices and using their symmetry properties, as derived in [24]. The concurrence between two clones is found to be

$$C_{cc}(1, M) = 2 \max \left(\frac{1}{6} - \frac{\sqrt{(3M+2)(M-2)}}{6M}, 0 \right). \quad (4.59)$$

As we can see, the entanglement between two clones surprisingly vanishes for $M \geq 3$. The concurrence between one clone and one ancilla can be calculated as

$$C_{ca}(1, M) = \frac{1}{3} \left(\frac{M+2}{M} - \sqrt{\frac{M-2}{M}} \right). \quad (4.60)$$

This expression is nonzero for all finite M , i.e., there is always entanglement between a clone and an ancilla, unless $M \rightarrow \infty$.

Generalizing these results to the $N \rightarrow M$ cloner for qubits, one can again calculate the concurrence between two clones. Again, the entanglement between two clones does not only vanish for $M \rightarrow \infty$, but already for finite M , namely for $M = N + 2$. The entanglement between one clone and one ancilla, however, has different properties: the concurrence is nonzero for any finite M , and only vanishes in the limit $M \rightarrow \infty$.

It is also possible to study multipartite entanglement in the cloning output. An interesting example is the $N \rightarrow N + 2$ qubit cloner, for which no bipartite entanglement between the clones exists, as mentioned above. However, by studying the reduced density matrix of three clones, which consists of a mixture of projectors onto W -states and a certain product state, it was shown [23] that there does exist genuine tripartite entanglement of the W -type between three clones.

4.6 Asymmetric Cloning

So far we have always assumed symmetry for the output copies, i.e., all reduced one-particle output density matrices of the cloner were supposed to be identical. If one gives up this requirement, one can study asymmetric quantum cloning. For the universal $1 \rightarrow 2$ cloner it was shown in [25] for qubits, and in [26] for d -dimensional systems, that there exists a tradeoff for the quality of the copies: Increasing the fidelity of one copy requires to decrease

the fidelity of the other copy. The resulting no-cloning inequality reads

$$(1 - F_1) + \frac{2}{d} \sqrt{(1 - F_1)(1 - F_2)} + (1 - F_2) \geq \frac{d - 1}{d}, \quad (4.61)$$

where F_i denotes the fidelity of copy i . Note that this bound is tight. For the symmetric case $F_1 = F_2$ this bound reduces to the upper bound given in Eq. (4.57) for $N = 1, M = 2$. This concept has been generalized in [27] to the case of N identical inputs and a number M_A of output copies having the same fidelity, while M_B outputs all have some different fidelity. For the scenario of asymmetric phase covariant $1 \rightarrow 2$ cloning in d dimensions, similar inequalities have been derived in [28].

Asymmetric cloning is closely related to security issues in quantum cryptography (see p. 349): the eavesdropper can use an asymmetric cloner in order to win partial information about the state sent from Alice to Bob, by keeping one copy and sending on the second one. In all protocols where the optimal eavesdropping strategy (*optimal* in the sense of maximizing Eve's mutual information with Alice for a fixed disturbance) is known, it turns out that the optimal eavesdropping strategy is equivalent to optimal asymmetric cloning [29, 30]. However, at the moment there does not exist a proof whether this equivalence holds in general for all protocols.

4.7 Probabilistic Cloning

In the previous sections we have always considered deterministic quantum cloning, i.e., the case where the cloning machine consists of a unitary operation only. The different concept of probabilistic quantum cloning [31] allows for a unitary operation plus measurement. By selecting a certain measurement result one may arrive at perfect clones, however with a success probability of less than 1. It was shown in [31] that the states chosen from a set $S = \{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ can be probabilistically cloned if and only if the $|\psi_i\rangle$ are linearly independent. In this case a unitary transformation of the following form exists:

$$U|\psi_i\rangle|0\rangle|A\rangle = \sqrt{p_i}|\psi_i\rangle|\psi_i\rangle|A_0\rangle + \sum_{j=1}^n c_{ij}|\Phi_j\rangle|A_j\rangle, \quad (4.62)$$

with $i = 1, 2, \dots, n$ and $\langle A_k|A_l\rangle = \delta_{kl}$ for $k, l = 0, 1, \dots, n$. Measuring the ancilla state in the basis $\{|A_k\rangle\}$ then leads with probability p_i to the desired clones $|\psi_i\rangle|\psi_i\rangle$.

The most simple example is given by an input set of only two states, namely $S = \{|\psi_1\rangle, |\psi_2\rangle\}$. Here, the success probabilities have to obey the inequality [31]

$$\frac{1}{2}(p_1 + p_2) \leq \frac{1}{1 + |\langle\psi_1|\psi_2\rangle|}. \quad (4.63)$$

In the more general case of n input states one arrives at bounds for the according success probabilities by solving a certain series of inequalities.

4.8 Experimental Quantum Cloning

The first explicit idea of how to implement an approximate cloning transformation in an experiment was suggested in [32], where it was shown that optimal universal quantum cloning

can be realized via stimulated emission in certain three-level systems, e.g., atoms in a cavity. These three-level systems have a ground state and two degenerate excited levels, connected to the ground state by two orthogonal modes of the electromagnetic field, a_1 and a_2 . The aim is to clone general superposition states $(\alpha a_1^\dagger + \beta a_2^\dagger)|0\rangle$, via stimulated emission. Another experimental possibility is based on stimulated parametric down-conversion. The latter proposal was used for an experimental demonstration of an optimal universal $1 \rightarrow 2$ cloning process [33]. A quality of the clones that is close to the optimal value of $F_{\text{th}} = 5/6 = 0.833$ was reached, namely $F_{\text{ex}} = 0.81 \pm 0.01$. The interaction Hamiltonian for parametric down-conversion reads

$$H = \kappa(a_v^\dagger b_h^\dagger - a_h^\dagger b_v^\dagger) + h.c., \quad (4.64)$$

where κ is a coupling constant, and $a_v^\dagger(a_h^\dagger)$ is the creation operator for a vertically (horizontally) polarized photon in spatial mode a , and analogously for $b_{v,h}^\dagger$. This Hamiltonian is invariant under joint identical polarization transformations in modes a and b , thus ensuring universality of the cloning process.

Polarized photons have been used in [34] to realize optimal universal quantum cloning, and in [35] to demonstrate optimal $1 \rightarrow 3$ phase covariant cloning.

A completely different idea was realized in [36], where a nuclear magnetic resonance (NMR) experiment (see p. 297) with three qubits was used to implement the approximate $1 \rightarrow 2$ cloner via the network that was derived in [37] (in a slightly modified version). The universality was tested explicitly by studying 312 input states, covering the Bloch sphere. Recently, also phase covariant cloning [38] and state-dependent cloning [39] have been implemented with NMR techniques.

Another physical system in which quantum cloning could be implemented is cavity QED [40]. Recently, it has been shown [41] that optimal phase covariant cloning can be achieved in a spin network with a certain XY Hamiltonian. This method is more robust against noise than the network approach [37].

4.9 Summary and Outlook

In this contribution we have reviewed approximate quantum cloning transformations for various scenarios. Here, we have only discussed cloning for finite-dimensional systems. Optimal cloning of continuous variable systems has also been studied in the literature, mainly for Gaussian cloning transformations [42], but is beyond the scope of this chapter.

The topic of approximate quantum cloning is mainly of fundamental interest: e.g., limits on the cloning fidelity imply limits on the security in quantum cryptography. Thus we have learned about differences between classical and quantum information processing by studying cloning. It is interesting to ask whether a cloning process be used as a tool in quantum information processing. In [43] it has been shown that quantum information distribution can improve the performance of certain quantum computation tasks. This distribution can be naturally implemented with different types of quantum cloning procedures: the information content of the input state is spread over the output state.

As a generalization of the concept of quantum cloning of pure input states one can consider the case of mixed input states. Here one arrives at the so-called no-broadcasting theorem [44],

which states that it is impossible to create from one mixed state, drawn from a set of two noncommuting density operators, an N -party output state, where each single-copy density operator is equal to the input. Recent developments in this direction [45] have shown that the no-broadcasting theorem does not hold if we increase the number of input copies ($N > 3$).

Exercises

1. *No-cloning theorem and linearity*
Show that perfect cloning of a set of linearly dependent states cannot be achieved by any linear transformation.
2. *Phase covariant cloning*
Derive the optimal phase covariant $1 \rightarrow 2$ cloning transformation for qubits. (Hint: start from the ansatz in Eq. (4.23) and impose that states from a great circle of the Bloch sphere, i.e., states of the form given in Eq. (4.34), are cloned with the same fidelity.)
3. *Entanglement structure of universal cloning*
 - (a) Derive the concurrence between two clones, i.e., formula (4.59), and between one clone and one ancilla, i.e., formula (4.60), for the universal $1 \rightarrow M$ cloner for qubits. (Hint: use the concurrence for certain symmetric density matrices as derived in [24].)
 - (b) Show that the total output state of the universal $1 \rightarrow 2$ cloner belongs to the W-class. (Hint: consider the tangle. See chapter on multipartite entanglement on p. 237).

References

- [1] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982).
- [2] D. Dieks, *Phys. Lett. A* **92**, 271 (1982).
- [3] H. P. Yuen, *Phys. Lett. A* **113** 405 (1986).
- [4] A. Barenco *et al.*, *Phys. Rev. Lett.* **74**, 4083 (1995).
- [5] D. Bruß, G. M. D'Ariano, C. Macchiavello, M. F. Sacchi, *Phys. Rev. A* **62**, 62302 (2000).
- [6] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, *Phys. Rev. A* **57**, 2368 (1998).
- [7] C. Macchiavello, *J. Optics B* **2**, 144 (2000).
- [8] D. Bruß and C. Macchiavello, *J. Phys. A: Math. Gen.* **34**, 1 (2001).
- [9] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, *Phys. Rev. A* **62**, 12302 (2000).
- [10] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, *Phys. Rev. A* **56**, 1163 (1997).
- [11] H. Fan *et al.*, *Phys. Rev. A* **65**, 012304 (2002).
- [12] G.M. D'Ariano and C. Macchiavello, *Phys. Rev. A* **67**, 042306 (2003).
- [13] M. Keyl and R. Werner, *J. Math. Phys.* **40**, 3283 (1999).
- [14] H. Fan, H. Imai, K. Matsumoto, and X.-B. Wang, *Phys. Rev. A* **67**, 022317 (2003).

- [15] F. Buscemi, G.M. D'Ariano, and C. Macchiavello, Phys. Rev. A **71**, 042327 (2005).
- [16] D. Bruß, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).
- [17] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
- [18] R. Werner, Phys. Rev. A **58**, 1827 (1998).
- [19] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
- [20] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
- [21] S. Alberverio and S.M. Fei, Eur. Phys. J. B **14**, 669 (2000).
- [22] D. Bruß and C. Macchiavello, Phys. Lett. A **253**, 249 (1999).
- [23] D. Bruß and C. Macchiavello, Found. Phys. **33**, 1617 (2003).
- [24] K. O'Connor and W. Wootters, Phys. Rev. A **63**, 052302 (2001).
- [25] N. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
- [26] N. Cerf, J. Mod. Opt. **47**, 187 (2000).
- [27] S. Iblisdir, A. Acin, N. Gisin, J. Fiurasek, R. Filip, and N. Cerf, *Preprint quant-ph/0411179*.
- [28] L.-P. Lamoureux and N. Cerf, Quant. Info. Comput. **5**, 32 (2005).
- [29] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
- [30] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
- [31] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
- [32] C. Simon, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **84**, 2993 (2000).
- [33] A. Lamas-Linares, C. Simon, J. Howell, and D. Bouwmeester, Science **296**, 712 (2002).
- [34] F. De Martini, D. Pelliccia and F. Sciarrino, Phys. Rev. Lett. **92**, 067901 (2004); F. Sciarrino, C. Sias, M. Ricci, and F. De Martini, Phys. Lett. A **323**, 34 (2004).
- [35] F. Sciarrino and F. De Martini, *Preprint quant-ph/0412041*.
- [36] H. Cummins et al., Phys. Rev. Lett. **88**, 187901 (2002).
- [37] V. Bužek, S. Braunstein, M. Hillery, and D. Bruß, Phys. Rev. A **56**, 3446 (1997).
- [38] J. Du et al., *Preprint quant-ph/0311010*.
- [39] J. Du et al., Phys. Rev. Lett. **94**, 040505 (2005).
- [40] P. Milman, H. Ollivier, and J. M. Raimond, *Preprint quant-ph/0207039*.
- [41] G. De Chiara, R. Fazio, C. Macchiavello, S. Montangero, and G. M. Palma, Phys. Rev. A **70**, 062308 (2004).
- [42] N. Cerf, in *Quantum Information with Continuous Variables*, Ed. S. L. Braunstein and A. K. Pati (Kluwer, Dordrecht, 2002).
- [43] E. Galvao and L. Hardy, Phys. Rev. A **62**, 022301 (2000).
- [44] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
- [45] G. M. D'Ariano, C. Macchiavello, and P. Perinotti, *Preprint quant-ph/0506251*.

5 Channels and Maps

Michael Keyl and Reinhard F. Werner

5.1 Introduction

Consider a typical quantum system like a string of ions in a trap. To “process” the quantum information they carry we generally have to perform many steps of a quite different nature. Typical examples are free time evolution (including unwanted but unavoidable interactions with the environment), controlled time evolution (e.g., the application of a “quantum gate” in a quantum computer), preparations, and measurements. The purpose of this chapter is to provide a unified framework for the description of all these different operations.

5.2 Completely Positive Maps

The basic idea is to interpret each processing step as a *channel* which transforms the system’s initial state ρ_{in} into the output state ρ_{out} the system attains, after the processing is finished. Occasionally, we will represent this picture graphically as in Fig. 5.1. To get a mathematical description consider the two Hilbert spaces $\mathcal{H}$, $\mathcal{H}'$ (subsequently called the “initial” and the “target” Hilbert space) with (finite) dimensions¹ d and d' and the algebras $\mathcal{B}(\mathcal{H})$ respectively $\mathcal{B}(\mathcal{H}')$ of (bounded) operators on them. Input and output states are described by density operators on $\mathcal{H}$ and $\mathcal{H}'$ which we denote by ρ_{in} and ρ_{out} again. Using this notation, we can regard a channel as a map T which transforms the input state ρ_{in} to the output state $T(\rho_{\text{in}}) = \rho_{\text{out}}$.

Each physically reasonable operation should respect the mixing of states, i.e., if $\rho_{\text{in}}^{(j)}$, $j = 1, 2$, are transformed to $\rho_{\text{out}}^{(j)}$, the mixture $\rho_{\text{in}} = \lambda \rho_{\text{in}}^{(1)} + (1 - \lambda) \rho_{\text{in}}^{(2)}$, $0 < \lambda < 1$, is mapped to $\rho_{\text{out}} = \lambda \rho_{\text{out}}^{(1)} + (1 - \lambda) \rho_{\text{out}}^{(2)}$. This implies that T can be extended to a *linear map*

$$T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}'),$$

and since T maps density matrices to density matrices it must be *positive*

$$T(A^* A) \geq 0 \quad \forall A \in \mathcal{B}(\mathcal{H}) \quad (5.1)$$

¹Note that the dimensions d and d' are not necessarily identical. This means that a channel can change the type of the system during processing. A typical example is a cloning-type map which produces M systems out of N , with $M > N$.

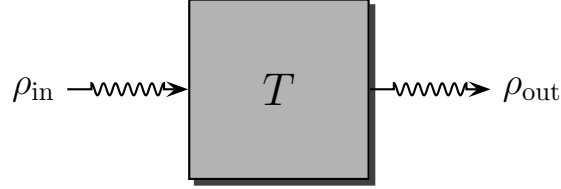


Figure 5.1. Graphical representation of a channel, transforming the system's initial state ρ_{in} into the final state ρ_{out} .

and *trace preserving*

$$\text{tr}(T(A)) = \text{tr}(A) \quad \forall A \in \mathcal{B}(\mathcal{H}). \quad (5.2)$$

Hence each channel can be described by a linear, positive and trace preserving linear map T .

However, this picture is incomplete because it is possible to apply a channel not only to the overall system but also to *subsystems*. A typical example arises if Alice and Bob share a bipartite system in an entangled state ρ_{in} and Alice applies a local quantum operation to her subsystem (and Bob does nothing). Again the crucial point is that the overall system shared by Alice and Bob end up in a valid quantum state ρ_{out} . In other words, the combination of “quantum operation performed by Alice” and “doing nothing by Bob” can be interpreted as a valid channel applied to the bipartite system (cf. Fig. 5.2). If ρ_{in} and ρ_{out} are density matrices on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}' = \mathcal{H}'_A \otimes \mathcal{H}_B$, respectively, the channel applied by Alice can be described by a positive, trace preserving linear map $T : \mathcal{B}(\mathcal{H}_A) \rightarrow \mathcal{B}(\mathcal{H}'_A)$, while “doing nothing” on Bob's system is just represented by the identity $\text{Id}_B : \mathcal{B}(\mathcal{H}_B) \rightarrow \mathcal{B}(\mathcal{H}_B)$. Hence the output state can be written as $\rho_{\text{out}} = T \otimes \text{Id}_B(\rho_{\text{in}})$. Obviously, $T \otimes \text{Id}$ is linear and trace preserving, but positivity of T is not sufficient for positivity of $T \otimes \text{Id}_B$. The most prominent example where this fails is the transposition: Although the transpose of a positive matrix is positive the *partial transpose* is in general not. To describe a physically realizable operation, the map T_A has to satisfy therefore in addition to (5.1) and (5.2) the condition that

$$T_A \otimes \text{Id}_B \quad \text{is positive}$$

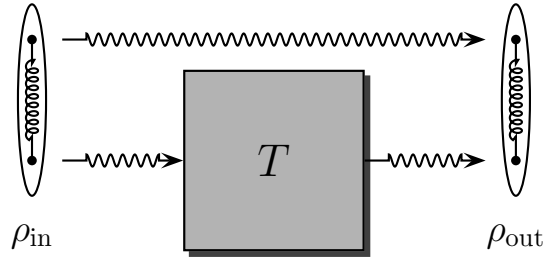


Figure 5.2. Channels can be applied to subsystems even if the overall system is in an entangled state.

and because Bob's system can be arbitrary, this should hold for any dimension of $\mathcal{H}_B$. Let us summarize the discussion up to now in the following definition:

Definition 5.1 Consider two (finite-dimensional) Hilbert spaces $\mathcal{H}, \mathcal{H}'$ and denote for each positive integer n the identity map on $\mathcal{B}(\mathbb{C}^n)$ by Id_n . A linear map $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$ is called *completely positive* (cp for short) if $T \otimes \text{Id}_n$ is positive for all $n \in \mathbb{N}$. It is called *trace preserving* if Eq. (5.2) holds, and *unital* if $T(\mathbb{1}) = \mathbb{1}$ is satisfied (where $\mathbb{1}$ denotes the unit operator on $\mathcal{H}, \mathcal{H}'$).

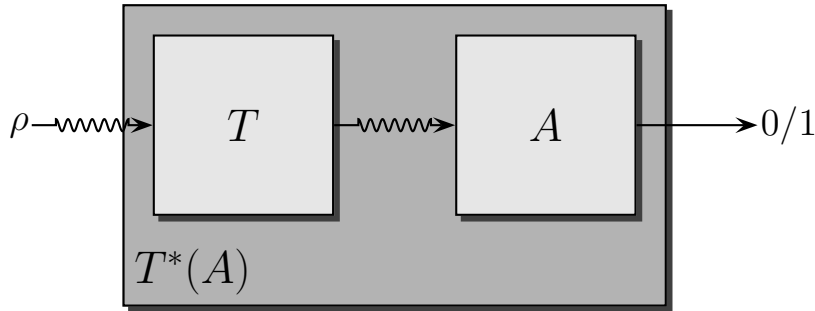


Figure 5.3. If A is an effect (i.e., a yes/no measurement) and T a channel, we can construct an effect $T^*(A)$ by first applying the channel T to the system and then performing an A measurement. The map $A \mapsto T^*(A)$ represents the channel T in the Heisenberg picture.

A channel is represented in the *Schrödinger picture* by a trace preserving cp-map. To get the *Heisenberg picture* representation we have to introduce the dual of T . It is the map $T^* : \mathcal{B}(\mathcal{H}') \rightarrow \mathcal{B}(\mathcal{H})$ uniquely defined by

$$\text{tr}(A^* T(B)) = \text{tr}(T^*(A)^* B) \quad \forall A \in \mathcal{B}(\mathcal{H}') \quad \forall B \in \mathcal{B}(\mathcal{H}).$$

It is easy to see that T^* is completely positive, if T is, and that T^* is unital if T is trace preserving (Exercise 1). If $A \in \mathcal{B}(\mathcal{H}')$ is an effect, i.e., an operator with $0 \leq A \leq \mathbb{1}$, representing a yes/no measurement,² its image $T^*(A)$ is an effect as well (since T^* is positive and unital). It should be regarded as the effect we get if we first apply the channel T to the system and then measure the effect A (cf. Fig. 5.3). Some typical examples of channels are as follows:

- *Unitary time evolution.* The most simple example is time evolution, described by a unitary operator on $\mathcal{H} = \mathcal{H}'$. The corresponding channel is described by $T(\rho) = U\rho U^*$.
- *Expansion.* Another elementary example arises if we expand a given quantum system by a second one (described by the Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ respectively). Hence initial and target Hilbert spaces are $\mathcal{H}$ and $\mathcal{H}' = \mathcal{H} \otimes \mathcal{K}$, respectively, and if the $\mathcal{K}$ -system is in the state σ the channel T becomes $T(\rho) = \rho \otimes \sigma$.

²In other words, $\text{tr}(\rho A)$ is the probability of getting the result “yes” (or 1) during an A measurement on a system in the state ρ .

- *Restriction.* The inverse operation arises if we discard a subsystem. The initial Hilbert space is now $\mathcal{H} = \mathcal{H}' \otimes \mathcal{K}$, the target Hilbert space is $\mathcal{H}'$ and T is given by $T(\rho) = \text{tr}_{\mathcal{K}}(\rho)$, where $\text{tr}_{\mathcal{K}}$ denotes the partial trace over $\mathcal{K}$.
- *Noisy time evolution.* The composition of channels is again a channel. Hence, we can combine the three examples just given: First expand the system, then let it evolve unitarily, and finally discard the system added in the first step: $\mathcal{H} = \mathcal{H}'$ and

$$T(\rho) = \text{tr}_{\mathcal{K}}(U(\rho \otimes \sigma)U^*), \quad (5.3)$$

with a unitary U on $\mathcal{H} \otimes \mathcal{K}$ and a density matrix σ on $\mathcal{K}$. Physically, this type of channel describes the influence of noise caused by interaction with the environment (represented by the $\mathcal{K}$ -system): σ is the initial state of the environment and U represents the joint evolution of the system and the environment; cf. Fig. 5.4. We will see in Section 5.4 that *each* channel can be written this way.

5.3 The Jamiolkowski Isomorphism

The subject of this section is a relation between completely positive maps and states of bipartite systems first discovered by Jamiolkowski [4], which is very useful in establishing several fundamental properties of cp maps.

The idea is based on the setup already discussed in Fig. 5.2: Alice and Bob share a bipartite system in a *maximally entangled* state

$$\chi = \frac{1}{\sqrt{d}} \sum_{\alpha=1}^d e_{\alpha} \otimes e_{\alpha} \in \mathcal{H} \otimes \mathcal{H} \quad (5.4)$$

(where $e_1, \dots, e_d$ denotes an orthonormal basis of $\mathcal{H}$) and Alice applies to her subsystem a channel $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$ while Bob does nothing. At the end of the processing the overall

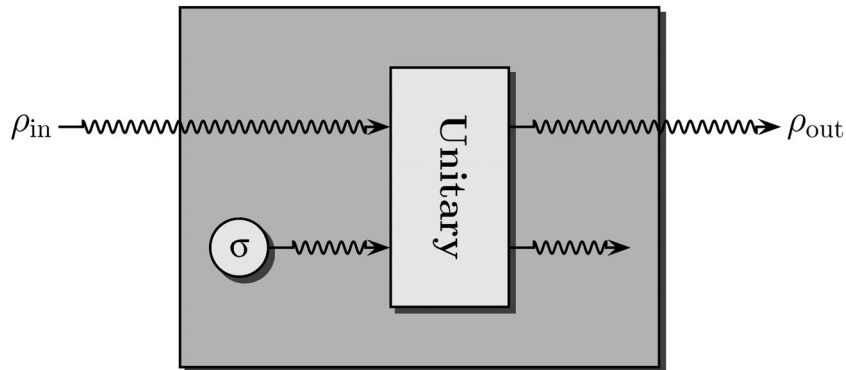


Figure 5.4. A noisy channel arising from interaction with the environment.

system ends up in a state

$$R_T = (T \otimes \text{Id})|\chi\rangle\langle\chi|. \quad (5.5)$$

Mathematically, Eq. (5.5) makes sense if T is only linear but not necessarily positive or completely positive (but then R_T is not positive either). If we denote the space of all linear maps from $\mathcal{B}(\mathcal{H})$ into $\mathcal{B}(\mathcal{H}')$ by $\mathcal{L}$ we therefore get a map

$$\mathcal{L} \ni T \mapsto R_T \in \mathcal{B}(\mathcal{K} \otimes \mathcal{H}), \quad (5.6)$$

which is easily shown to be linear (i.e., $R_{\mu T + \lambda S} = \mu R_T + \lambda R_S$ for all $\lambda, \mu \in \mathbb{C}$ and all $T, S \in \mathcal{L}$). Furthermore, this map is bijective, hence a *linear isomorphism*.

Theorem 5.1 *The map defined in Eqs. (5.6) and (5.5) is a linear isomorphism. The inverse map is given by*

$$\mathcal{B}(\mathcal{H} \otimes \mathcal{H}') \ni \rho \mapsto T_\rho \in \mathcal{L}.$$

with

$$\langle e'_\mu | T_\rho(\sigma) e'_\nu \rangle = d \operatorname{tr}(\rho (|e'_\nu\rangle\langle e'_\mu| \otimes \sigma^T)), \quad (5.7)$$

where $e'_1, \dots, e'_{d'}$ in $\mathcal{H}'$ denotes an (arbitrary) orthonormal basis of $\mathcal{H}'$ and the transposition of σ is defined with respect to the basis $e_1, \dots, e_d$ used in (5.4) to define χ .

The proof of this theorem is left as an exercise to the reader (Exercise 2). From the definition of R_T in Eq. (5.5) it is obvious that R_T is positive if T is completely positive. To see that the converse is also true, is not as trivial, because a transposition (which is not completely positive) is involved in the definition of T_ρ (5.7). It is therefore useful to rewrite Eq. (5.7) in terms of a *purification* of ρ . Hence consider an auxiliary Hilbert space $\mathcal{K}$ and $\psi \in \mathcal{H} \otimes \mathcal{H}' \otimes \mathcal{K}$ such that $\rho = \operatorname{tr}_{\mathcal{K}}(|\psi\rangle\langle\psi|)$. Note that the existence of such a ψ requires positivity of ρ , but not normalization. If $f_1, \dots, f_n \in \mathcal{K}$ denotes an orthonormal basis we can define an operator $V : \mathcal{H}' \rightarrow \mathcal{H} \otimes \mathcal{K}$ by

$$\langle e_\alpha \otimes f_j | V e'_\nu \rangle = \sqrt{d} \langle \psi | e'_\nu \otimes e_\alpha \otimes f_j \rangle. \quad (5.8)$$

Now we get with Eq. (5.7)

$$\begin{aligned} \langle e'_\mu | V^* (|e_\alpha\rangle\langle e_\beta| \otimes \mathbf{1}) V e'_\nu \rangle &= d \sum_{j=1}^n \langle \psi | e'_\nu \otimes e_\beta \otimes f_j \rangle \langle e'_\mu \otimes e_\alpha \otimes f_j | \psi \rangle \\ &= d \operatorname{tr}(\rho (|e'_\nu\rangle\langle e'_\mu| \otimes |e_\alpha\rangle\langle e_\beta|^T)) \\ &= \langle e'_\mu | T_\rho(|e_\alpha\rangle\langle e_\beta|) e'_\nu \rangle. \end{aligned}$$

Let us summarize this result for later reference in the following lemma:

Lemma 5.1 *For each positive operator $\rho \in \mathcal{B}(\mathcal{H} \otimes \mathcal{H}')$ there is a Hilbert space $\mathcal{K}$ and an operator $V : \mathcal{H}' \rightarrow \mathcal{H} \otimes \mathcal{K}$ such that*

$$T_\rho(\sigma) = V^*(\sigma \otimes \mathbf{1})V \quad (5.9)$$

holds.

Note that the definition of V in terms of ψ from Eq. (5.8) depends on the choice of the basis $f_j \in \mathcal{K}$ but not on $e'_\mu \in \mathcal{H}'$ ($e_\alpha \in \mathcal{H}$ are fixed already by the choice of χ in (5.5)). However, this ambiguity does not affect the expression $V^*(A \otimes \mathbb{1})V$, because all operators V arising from different bases in $\mathcal{K}$ are related by unitary operators on $\mathcal{K}$.

From Eq. (5.9) we see immediately that T_ρ is completely positive if ρ is positive. Together with Theorem 5.1 this leads to

Theorem 5.2 *The map T is completely positive iff the operator R_T is positive.*

As an immediate consequence of this theorem, we can simplify the original characterization of complete positivity in Definition 5.1. To this end let us define for each $n \in \mathbb{N}$ a map $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$ to be *n-positive* if $T \otimes \text{Id}_n$ is positive. Note that this is in general a *weaker* condition than complete positivity, because T is completely positive, if T is *n-positive* for each n . In the finite-dimensional case, however, it is sufficient to have *n-positivity* for sufficiently large n .

Corollary 5.3 *If $\dim(\mathcal{H}) = d$ is finite, a map $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$ is completely positive if it is *d-positive*.*

Proof. If T is *d-positive* the operator $R_T = (T \otimes \text{Id}_d)|\chi\rangle\langle\chi|$ is positive. Hence, by Theorem 5.2 T is completely positive. $\square$

5.4 The Stinespring Dilation Theorem

At the end of Section 5.2 we have claimed that each channel can be written in terms of an *ancilla* as in Eq. (5.3). We are now prepared to prove this statement. The following theorem, which goes back to Stinespring [7], is the central structure theorem about completely positive maps.

Theorem 5.4 (Stinespring dilation theorem) *Each completely positive map $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$ can be written as*

$$T(A) = V^*(A \otimes \mathbb{1})V, \quad (5.10)$$

where $V : \mathcal{H}' \rightarrow \mathcal{H} \otimes \mathcal{K}$ is a linear operator and $\mathcal{K}$ is an auxiliary Hilbert space. The pair $(V, \mathcal{K})$ is called a Stinespring representation of T .

Proof. According to Theorem 5.1 there is a (unique) positive operator $R_T \in \mathcal{B}(\mathcal{H} \otimes \mathcal{H}')$ such that $T = T_{R_T}$. Hence the statement follows from Lemma 5.1. $\square$

Let us consider now the uniqueness of Stinespring representations. Obviously, we can always enlarge the dilation space $\mathcal{K}$ by adding extra dimensions (i.e., replacing $\mathcal{K}$ by $\mathcal{K}' = \mathcal{K} \otimes \mathbb{C}^m$ and leaving V untouched). Hence, Stinespring representations are not unique. But what happens if we assume that $\mathcal{K}$ is “as small as possible,” i.e., if the dimension of $\mathcal{K}$ can not be reduced by discarding “superfluous” components? This situation is characterized by the condition

$$\text{span}\{(A \otimes \mathbb{1})V\phi \mid A \in \mathcal{B}(\mathcal{H}), \phi \in \mathcal{H}'\} = \mathcal{H} \otimes \mathcal{K}. \quad (5.11)$$

Now we have the following theorem:

Theorem 5.5 *Each completely positive map $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$ admits a Stinespring representation satisfying Eq. (5.11). This minimal Stinespring representation is unique up to unitary equivalence.*

Proof. Consider a Stinespring representation $(V, \mathcal{K})$ of T and define $\psi \in \mathcal{H}' \otimes \mathcal{H} \otimes \mathcal{K}$ by (cf. Eq. (5.8))

$$\sqrt{d}\langle\psi|e'_\nu \otimes e_\alpha \otimes f_j\rangle = \langle e_\alpha \otimes f_j|Ve'_\nu\rangle. \quad (5.12)$$

The same reasoning which has led to Lemma 5.1 shows that ψ is the purification of R_T . Hence, if

$$\psi = \sum_{j=1}^m \sqrt{\lambda_j} \tilde{e}_j \otimes \tilde{f}_j, \quad \lambda_j > 0, \quad j = 1, \dots, m, \quad (5.13)$$

is the Schmidt decomposition of ψ , the operator $R_T = \text{tr}_{\mathcal{K}}(|\psi\rangle\langle\psi|)$ becomes

$$R_T = \sum_{j=1}^m \lambda_j |\tilde{e}_j\rangle\langle\tilde{e}_j|.$$

The *minimal purification* arises if

$$\text{tr}_{\mathcal{H} \otimes \mathcal{H}'}(|\psi\rangle\langle\psi|) = \sum_{j=1}^m \lambda_j |\tilde{f}_j\rangle\langle\tilde{f}_j| \in \mathcal{B}(\mathcal{K})$$

has no zero eigenvector. Hence if the number m of summands in (5.13) is equal to the dimension n of $\mathcal{K}$. Now we can proceed with the following lemma (its proof is left to the reader as Exercise 3).

Lemma 5.2 *Equation (5.11) holds iff ψ is the minimal purification of R_T .*

This lemma shows that we get a minimal Stinespring representation if we define V and $\mathcal{K}$ in terms of (5.12) with a minimal purification ψ of R_T . Its uniqueness follows from the uniqueness (up to unitary equivalence) of the minimal purification. $\square$

Let us consider now two alternative representation theorems, which can be derived directly from the Stinespring theorem. The first is the ancilla form of a channel, which we have encountered already in Eq. (5.3).

Corollary 5.6 (Ancilla form) *Assume that $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$ is a channel (i.e., a trace preserving cp map). Then there is a Hilbert space $\mathcal{K}$, a pure state ρ_0 and a unitary map $U : \mathcal{H} \otimes \mathcal{K} \rightarrow \mathcal{H} \otimes \mathcal{K}$ such that*

$$T(\rho) = \text{tr}_{\mathcal{K}}(U(\rho \otimes \rho_0)U^*)$$

holds.

Proof. Consider the Stinespring form $T^*(A) = V^*(A \otimes \mathbf{1})V$ with $V : \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{K}$ of T^* and choose a vector $\xi \in \mathcal{K}$ such that $U(\phi \otimes \xi) = V(\phi)$ can be extended to a unitary map $U : \mathcal{H} \otimes \mathcal{K} \rightarrow \mathcal{H} \otimes \mathcal{K}$ (this is always possible since T^* is unital and V therefore isometric). If the basis $f_j, j = 1, \dots, n$, is chosen such that $f_1 = \xi$ holds, we get

$$\begin{aligned} \text{tr}[T(\rho)A] &= \text{tr}[\rho V^*(A \otimes \mathbf{1})V] = \sum_{\alpha} \langle V \rho e_{\alpha} | (A \otimes \mathbf{1}) V e_{\alpha} \rangle \\ &= \sum_{\alpha k} \left\langle U(\rho \otimes |\xi\rangle\langle\xi|)(e_{\alpha} \otimes f_k) | (A \otimes \mathbf{1}) U(e_{\alpha} \otimes f_k) \right\rangle \\ &= \text{tr}[\text{tr}_{\mathcal{K}}[U(\rho \otimes |\xi\rangle\langle\xi|)U^*]A], \end{aligned}$$

which proves the statement. $\square$

Even if the Stinespring representation $(V, \mathcal{K})$ used in the proof is the minimal one, there is a lot of freedom to define the unitary U , because it depends on the choice of ξ and of many matrix elements which in the end drop out of all results. This is a weakness of the ancilla approach in practical computations.

Let us come back now to a general (i.e., not necessarily trace preserving) cp map T and consider a Stinespring representation $(V, \mathcal{K})$ of it. If we choose vectors $\chi_x \in \mathcal{K}$ with $\sum_x |\chi_x\rangle\langle\chi_x| = \mathbf{1}$ we can define a family of operators $V : \mathcal{H}' \rightarrow \mathcal{H}$ by

$$\langle \phi | V_x \phi' \rangle = \langle \phi \otimes \chi_x | V \phi' \rangle \quad \phi \in \mathcal{H}, \quad \phi' \in \mathcal{H}'. \quad (5.14)$$

In terms of them Eq. (5.10) can be rewritten as follows (cf. Problem 4 and [2, 5]).

Corollary 5.7 (Kraus form) *Every completely positive map $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$ can be written in the form*

$$T(A) = \sum_x V_x^* A V_x, \quad (5.15)$$

with operators $V_x : \mathcal{H}' \rightarrow \mathcal{H}$.

Finally, let us state a third result which is closely related to the Stinespring theorem. It characterizes all decompositions of a given completely positive map into completely positive summands. It shows in particular that all “Kraus representations” of a given cp map (i.e., Eq. (5.15) with appropriate operators V_x) can be derived as in (5.14). By analogy with results from measure theory we will call it a Radon–Nikodym theorem (cf. [1]).

Theorem 5.8 (Radon–Nikodym theorem) *Let $T_x : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$, $x \in X$, be a family of completely positive maps and let $(V, \mathcal{K})$ be a Stinespring representation of $\bar{T} = \sum_x T_x$; then there are positive operators F_x in $\mathcal{B}(\mathcal{K})$ with $\sum_x F_x = \mathbf{1}$ and*

$$T_x(A) = V^*(A \otimes F_x)V. \quad (5.16)$$

If $(V, \mathcal{K})$ is the minimal Stinespring representation, F_x are uniquely determined.

Proof. According to Theorem 5.1 we have for each T_x an operator R_{T_x} . To simplify the notation we will denote them in the following by R_x (instead of R_{T_x}). Due to linearity of the map $T \mapsto R_T$ we have $R_{\bar{T}} = \sum_x R_x$, and positivity of R_T implies

$$\text{supp } R_x \subset \tilde{\mathcal{H}} = \text{supp } R_{\bar{T}},$$

where supp denotes the *support*, i.e., the orthocomplement of the kernel. By slight abuse of notation we will identify R_x in the following with their restriction to $\tilde{\mathcal{H}}$.

Now let us consider again the vector $\psi \in \mathcal{H}' \otimes \mathcal{H} \otimes \mathcal{K}$ defined in terms of V in Eq. (5.8). Its Schmidt decomposition is given by (cf. Eq. (5.13))

$$\psi = \sum_{j=1}^m \sqrt{\lambda_j} \tilde{e}_j \otimes \tilde{f}_j,$$

and the number m of terms in this sum is the dimension of $\tilde{\mathcal{H}}$. If we denote the subspace of $\mathcal{K}$ which is generated by $\tilde{f}_1, \dots, \tilde{f}_m$ by $\tilde{\mathcal{K}}$, we get $\psi \in \tilde{\mathcal{H}} \otimes \tilde{\mathcal{K}}$. If $A \in \mathcal{B}(\tilde{\mathcal{H}})$ and $\tilde{B} \in \mathcal{B}(\tilde{\mathcal{K}})$ are operators with matrix elements $A_{jk} = \langle \tilde{e}_j | A \tilde{e}_k \rangle$ and $\tilde{B}_{jk} = \langle \tilde{f}_j | \tilde{B} \tilde{f}_k \rangle$, respectively, we have

$$\langle \psi | A \otimes \tilde{B} \psi \rangle = \sum_{j,k=1}^m \sqrt{\lambda_j \lambda_k} A_{jk} \tilde{B}_{jk} = \sum_{j,k=1}^m A_{jk} (\sqrt{\lambda_j \lambda_k} \tilde{B}_{kj}^T).$$

Hence with $B \in \mathcal{B}(\tilde{\mathcal{H}})$ given by

$$\langle \tilde{e}_j | B \tilde{e}_k \rangle = \sqrt{\lambda_j \lambda_k} \langle \tilde{f}_j | \tilde{B}^T \tilde{f}_k \rangle \quad (5.17)$$

we get $\langle \psi | A \otimes \tilde{B} \psi \rangle = \text{tr}(AB)$. From Eq. (5.17) we see immediately that the map $\tilde{B} \mapsto B$ is invertible.

Since $R_x \in \mathcal{B}(\tilde{\mathcal{H}})$ we therefore get a (unique) operator $\tilde{R}_x \in \mathcal{B}(\tilde{\mathcal{K}})$ with

$$\text{tr}(R_x A) = \langle \psi | (A \otimes \tilde{R}_x) \psi \rangle. \quad (5.18)$$

Now let us choose the basis $f_1, \dots, f_n \in \mathcal{K}$ such that $f_j = \tilde{f}_j$ holds for $j = 1, \dots, m$ and define an operator $F_x^T = \sum_{j,k} F_{jk} |f_j\rangle \langle f_k|$ by

$$F_{jk} = \begin{cases} \langle \tilde{f}_j | \tilde{R}_x \tilde{f}_k \rangle & \text{for } j, k = 1, \dots, m \\ 0 & \text{otherwise.} \end{cases} \quad (5.19)$$

According to Eq. (5.18) we have $\text{tr}(R_x A) = \langle \psi | (A \otimes F_x^T) \psi \rangle$ and we get with Eq. (5.7):

$$\begin{aligned} \langle e'_\mu | T_{R_x}(|e_\beta\rangle \langle e_\alpha|) e'_\nu \rangle &= d \text{tr}(R_x(|e'_\nu\rangle \langle e'_\mu| \otimes |e_\beta\rangle \langle e_\alpha|^T)) \\ &= d \sum_{j,k} F_{jk} \langle \psi | e'_\nu \otimes e_\alpha \otimes f_j \rangle \langle e'_\mu \otimes e_\beta \otimes f_k | \psi \rangle \\ &= \sum_{j,k} F_{jk} \langle V e'_\mu | e_\beta \otimes f_k \rangle \langle e_\alpha \otimes f_j | V e'_\nu \rangle \\ &= \langle e'_\mu | V^* (|e_\beta\rangle \langle e_\alpha| \otimes F_x) V e'_\nu \rangle, \end{aligned}$$

where we have used again the relation between ψ and V from Eq. (5.8).

This completes the proof of Eq. (5.16). To show uniqueness, note that Lemma 5.2 and the assumption that $(V, \mathcal{K})$ is minimal imply that $\tilde{\mathcal{K}} = \mathcal{K}$ holds. Hence there is no freedom left in the definition of F_x^T in Eq. (5.19). $\square$

The properties of completely positive maps we have just discussed are only the most elementary ones. For a much more complete, in-depth presentation of this subject we would like to refer the reader to the book of Paulsen [6].

5.5 Classical Systems as a Special Case

Up to now we have only treated pure quantum systems, for which the possible observables are given by *all* bounded operators on a Hilbert space. Classical systems can be understood as a special case, with a constraint on what we can measure: namely only those observables which are diagonal in some fixed basis. Since diagonal matrices commute, this is the same as choosing a commutative subalgebra of observables.

The transition from a quantum system to a classical subdescription is made by a particular channel P , which simply kills all off diagonal terms, sometimes called “interference terms.” When $e_1, \dots, e_d \in \mathcal{H}$ denotes the particular orthonormal basis in which we want to go classical, we set

$$P(\rho) = \sum_{\mu} |e_{\mu}\rangle \langle e_{\mu}| \rho |e_{\mu}\rangle \langle e_{\mu}|. \quad (5.20)$$

This is also called a complete von Neumann measurement: the μ th term in this sum is the corresponding basis state, multiplied with the probability $\langle e_{\mu}| \rho |e_{\mu}\rangle$ for obtaining the result μ . It is easily verified that the formula for the Heisenberg picture of this channel is exactly the same as (5.20).

Clearly, the specification of elements $P(A)$ in the classical observable algebra requires only d rather than d^2 real parameters, as in the quantum case. Therefore, channels with one or classical input or output can also be described by fewer parameters. For example, a channel T with classical input has the property that $T = TP$, because its output depends only on the diagonal matrix elements of the input matrix. Hence it can be written as

$$T(\rho) = \sum_{\mu} \langle e_{\mu}| \rho |e_{\mu}\rangle \rho_{T, \mu}, \quad (5.21)$$

where $\rho_{T, \mu}$ are arbitrary states of the final system, which characterize T . The input state merely selects the weights in a convex combination of these states. Dually, channels $T = PT$ with classical output are of the form

$$T(\rho) = \sum_{\mu} \text{tr}(\rho F_{T, \mu}) |e_{\mu}\rangle \langle e_{\mu}|, \quad (5.22)$$

where $F_{T, \mu}$ are positive operators adding up to the identity operator. Thus $F_{T, \mu}$ is an observable, or positive operator valued measure.

An important special case is also a channel whose output is the tensor product of a classical and a quantum output. If e_μ , $\mu = 1, \dots, d$ is classical basis in $\mathcal{K}$, the general form of such a channel is $T : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}') \otimes \mathcal{B}(\mathcal{K})$, with

$$T(\rho) = \sum_{\mu} T_{\mu}(\rho) \otimes |e_{\mu}\rangle\langle e_{\mu}|, \quad (5.23)$$

where each of the $T_{\mu} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}')$ is completely positive. Such a channel is called an *instrument* [3]. Since there are two outputs, we get two “marginals,” i.e., the channels obtained by ignoring either output: If we do not look at the quantum output, we get an observable F in the sense of (5.22) by $\text{tr}(\rho F_{\mu}) = \text{tr} T_{\mu}(\rho)$. On the other hand, if we do not select according to the results μ , we get the channel $T = \sum_{\mu} T_{\mu}$.

5.6 Examples

5.6.1 The ideal quantum channel

The simplest possible channel is the description of “doing nothing” to a system of type A , denoted above by Id_A , i.e., the identity map on $\mathcal{B}(\mathcal{H}_A)$. This channel is what we try to achieve when we talk about the transmission of quantum information. All practical ways of sending quantum information introduce noise, which is the same as saying that they are described by channels $T \neq \text{Id}_A$. However, by suitable steps of quantum error correction (applied to multiple instances of T) we can reduce the noise and, in the limit, get a better realization of Id_A .

It is easy to construct the minimal Stinespring dilation of Id_A : We take $\dim \mathcal{K} = 1$, so that $\mathcal{H}_A \otimes \mathcal{K} = \mathcal{H}_A$, and $V = 1$. This simple observation, combined with the Radon–Nikodym theorem, has a very profound consequence, namely that in quantum mechanics *there is no measurement without disturbance*. Indeed, suppose we have an instrument as in Eq. (5.23), such that the overall state change is $T = \sum_{\mu} T_{\mu} = \text{Id}$. That is to say, if we perform any further measurements after T , we will always find the same expectations as if we had not applied T . Then, by the Radon–Nikodym theorem, all decompositions of T into completely positive summands are parameterized by operators in the dilation space $\mathcal{K}$, which is, however, one dimensional. Therefore, all T_{μ} must be proportional to T , say $T_{\mu} = p_{\mu}T$, for some probability distribution p on the outcomes. But then the observable associated with the instrument will be $F_{\mu} = p_{\mu}\mathbb{1}$, which is to say that the probabilities for the outcomes do not depend at all on the input state. Hence they do not give any information about the system, and it is fair to say that this is not a measurement at all.

5.6.2 The depolarizing channel

At the opposite extreme is a channel that destroys all input information, replacing it by a completely chaotic output state $\rho_{\text{out}} = \mathbb{1}/d$, where $d = \dim \mathcal{H}$. Slightly more generally, we can look at the channel which does this with probability ε , and otherwise ideally transmits the

input:

$$T(\rho) = \varepsilon \operatorname{tr}(\rho) \frac{1}{d} \mathbf{1} + (1 - \varepsilon) \rho. \quad (5.24)$$

Here we have included the trace factor (which is 1 for input states), so that T becomes a linear map. This channel is often used as a noise model, usually with a small depolarization probability ε . Interestingly, this channel is completely positive even for some $\varepsilon > 1$. For qubits, this has a quite intuitive interpretation in terms of transformations of the Poincaré sphere: as ε increases, the set of output states shrinks, until at $\varepsilon = 1$ it coincides with the origin. Increasing ε further means that the Poincaré sphere becomes *inverted*. For $\varepsilon = 2$ we would get a complete inversion, the so-called Universal-NOT operation, which sends every pure state to its orthogonal complement. This map is positive, but not completely positive, so it is an impossible operation. Its best approximation by completely positive channels is obtained by taking ε as large as possible ($\varepsilon = 4/3$ for qubits).

The Kraus decompositions of the fully depolarizing channel ($\varepsilon = 1$) are characterized by the equation

$$\operatorname{tr}(V_x^* V_y) = \frac{1}{d} \delta_{xy}, \quad x, y = 1, \dots, d^2.$$

This can be solved, for any d , by operators V_x , which are unitary up to a factor. Such orthogonal sets of unitaries play a central role in teleportation and dense coding schemes.

5.6.3 Entanglement breaking channels

Can quantum information be transmitted via classical channels? This would mean to first make a measurement M , transmit the results via a classical channel, and let the receiver try to reconstruct the quantum input state by a reparation R , which depends on the results of the measurement. The form of such a channel is RPM , where P is the von Neumann measurement for the intermediate classical channel. When R and M are given as in (5.21) and (5.22), respectively, and the classical signals transmitted are labeled by μ , this gives a channel of the form

$$T(\rho) = \sum_{\mu} \operatorname{tr}(\rho F_{\mu}) \rho_{\mu}. \quad (5.25)$$

It turns out that these channels are characterized by the property that $\operatorname{Id} \otimes T$ turns every entangled state into a separable state, i.e., they destroy all entanglement (Problem 6).

5.6.4 Covariant channels

Many channels of interest have a simple characterization in terms of symmetries. For example, the depolarizing channels (5.24) are the only ones which do not distinguish any basis in Hilbert space, in the sense that a basis change by a unitary operator U does not change the action of the channel: $UT(\rho)U^* = T(U\rho U^*)$. More general characterizations of symmetries involve subgroups of unitary operators, which may differ for initial and target space:

$$U_g T(\rho) U_g^* = T(U_g' \rho U_g'^*) \quad \text{for all } g \in G, \quad (5.26)$$

where G is some abstract group and $g \mapsto U'_g$ and $g \mapsto U_g$ are unitary representations of this group on the initial and target Hilbert space, respectively. Channels satisfying this condition are called *covariant*.

Since the minimal Stinespring representation is unique up to unitary equivalence, the covariance of the channel is also reflected at that level, and this often allows us to give concise formulas for all channels satisfying (5.26), given G and the representations. Let $V : \mathcal{H}' \rightarrow \mathcal{H} \otimes \mathcal{K}$ be the Stinespring isometry. Then, for every $g \in G$, $(U_g^* \otimes \mathbf{1})VU'_g$ is again a dilation, which means that this dilation must be connected with V by a unitary of the form $(\mathbf{1} \otimes U''_g)$. In other words, we find the condition

$$(U_g \otimes U''_g)V = VU'_g.$$

One readily verifies that $g \mapsto U''_g$ must be a unitary representation of G on $\mathcal{K}$. In the language of group representation theory, this relation says that V must be an intertwining operator between the representations of G , and there is a highly developed formalism to determine such operators. Let us consider two cases.

When the group is $G = SU(2)$, the irreducible representations are labeled by the spin parameter $s = 0, 1/2, 1, \dots$. Let us take both input and output representation to be irreducible with spins s and s' , respectively. This fixes the dimensions to be $\dim \mathcal{H} = 2s + 1$ and $\dim \mathcal{H}' = 2s' + 1$. Now it is easy to see that decomposing the representation U''_g into irreducibles corresponds to a convex decomposition of T . Therefore, to find the extremal covariant channels we can assume U''_g to be irreducible as well, and hence to be fixed by a spin parameter s'' . Then the Clebsch–Gordan theory of adding angular momenta tells us that a nonzero intertwiner V exists if and only if $|s - s'| \leq s'' \leq (s + s')$, and $s + s' + s''$ is integer. Moreover, the intertwiner in these cases is a unique isometry, whose matrix elements are the well-known Clebsch–Gordan coefficients.

For example, when $s = s'$, $s'' = 0$ gives the ideal channel. For $s = s'$ we can also define the channel

$$T(\rho) = \frac{1}{s(s+1)} \sum_{k=1}^3 L_k \rho L_k,$$

where L_k denotes the angular momentum operators of the spin s representation. This corresponds precisely to $s'' = 1$, because the angular momenta are the components of a vector operator, transforming with the spin 1 representation. $s'' = 2s$ gives the depolarizing channel.

Another interesting group for constructing covariant channels is the the group of phase space translations or, more precisely, the Heisenberg group, consisting of the phase space translations and the multiples of $\mathbf{1}$. The phase space displacement by the phase space vector ξ is then given by the Weyl operators $W(\xi)$, and we assume these to act irreducibly, so that there are no further degrees of freedom. By the canonical commutation relations, the Weyl operators are also characterized as the eigenvectors of the action of phase space translations on operators: i.e., $W(\xi)AW(\xi)^* = a(\xi)A$ for all ξ implies that A must be proportional to a Weyl operator $W(\eta)$, and $a(\xi)$ contains an exponential factor characterizing η . Inserting this condition into the covariance equation (5.26), one readily finds that (in the Heisenberg picture) a phase space covariant channel must take Weyl operators to multiples of Weyl operators:

$$T^*(W(\eta)) = t(\eta)W(\eta).$$

Moreover, T is a channel if and only if t is the Fourier transform of a probability measure, and T acts by making a random phase space translation, selected according to this measure.

The theory also applies, however, when the Weyl systems on the input and output side are different, and the displacement parameters are connected by some linear map between input and output phase space. For example, we could take $W(\xi) = W'(\lambda\xi)$, with some positive factor λ . This corresponds to the amplification or attenuation of a quantum optical light field (depending on whether $\lambda > 1$ or $\lambda < 1$). In this case the complete positivity condition for T is a bit more difficult to write down. It forces T to contain some noise, as is expected from the no-cloning theorem. The ancilla form of the dilation is particularly instructive: any such channel can be represented by coupling an ancillary system in a specified state to the input, making a symplectic transformation (any interaction, which is quadratic in positions and momenta), and then tracing out a part of the system. In particular, when the initial state of the ancilla is Gaussian, the channel is Gaussian as well, which means that the factor t has Gaussian form.

Exercises

1. Show that the dual T^* of a completely positive map T is completely positive, and that T^* is unital iff T is trace preserving.
2. Give a proof of Theorem 5.1.
3. Give a proof of Lemma 5.2. *Hint:* Assume that Eq. (5.11) does not hold and consider a vector $\xi \in \mathcal{H} \otimes \mathcal{K}$ orthogonal to the span of $(A \otimes \mathbf{1})V\phi$.
4. Derive the Kraus form (Corollary 5.7) from the Stinespring form (Theorem 5.4).
5. Find a Kraus decomposition for the depolarizing channel.
6. Show that the channels define in Eq. (5.25) are *entanglement-breaking*, i.e., $T \otimes \text{Id}$ turns every entangled state into a separable state. *Hint:* Use the Jamiolkowski isomorphism.

References

- [1] W. Arveson. *Subalgebras of C^* -algebras*. Acta. Math. **123**, 141–224 (1969).
- [2] M.-D. Choi. *Completely positive linear maps on complex matrices*. Lin. Alg. Appl. **10**, 285–290 (1975).
- [3] E. B. Davies. *Quantum Theory of Open Systems*. Academic Press, London (1976).
- [4] A. Jamiolkowski. *Linear transformations which preserve trace and positive semidefiniteness of operators*. Rep. Math. Phys. **3**, 275–278 (1972).
- [5] K. Kraus. *States Effects and Operations*. Springer, Berlin (1983).
- [6] V. I. Paulsen, *Completely Bounded Maps and Dilations*. Cambridge University Press, Cambridge (2002).
- [7] W. F. Stinespring. *Positive functions on C^* -algebras*. Proc. Am. Math. Soc. **6**, 211–216 (1955).

6 Quantum Algorithms

Julia Kempe

6.1 Introduction

The idea to use quantum mechanics for algorithmic tasks may be traced back to Feynman [24, 25]. The application he had in mind was the simulation of quantum mechanical systems by a universal quantum system, the quantum computer. Feynman argued that quantum mechanical systems are well equipped to simulate other quantum mechanical systems; hence a universal quantum machine might be able to efficiently do such simulations. Another approach to this question was taken by Deutsch [14], who tried to reconcile quantum mechanics and the Church–Turing principle, which (roughly speaking) states that any computable function can be calculated by what is known as a *universal Turing machine*. Deutsch put the notion of a universal machine on a physical footing and asked if the principle had to be modified if the machine was quantum mechanical, establishing what has since been known as the *Church–Turing–Deutsch principle*. In his work Deutsch was also the first to exhibit a concrete computational task, which is impossible to solve on a classical computer yet which has an easy quantum mechanical solution, *Deutsch’s algorithm* (see the next section). What is interesting about this algorithm is that not only it is the smallest algorithm, involving only two quantum bits (qubits) but also carries the main ingredients of later quantum algorithms, and is a nice toy model for understanding why and how quantum algorithms work.

A major breakthrough in quantum algorithms was made by Peter Shor, who gave an efficient quantum factoring algorithm. Factoring numbers into primes is an important problem, and no efficient classical algorithm is known for it. In fact many cryptographic systems rely on the assumption that factoring and related problems, such as discrete logarithm, are hard problems. Shor’s algorithm has put a threat on the security of many of our daily transactions—should a quantum computer be built, most current encryption schemes will be broken immediately.

The way Feynman put it, a quantum computer is a machine that obeys the laws of quantum mechanics, rather than Newtonian classical physics. In the context of computation this has two important consequences, which define the two aspects in which a quantum computer differs from its classical counterpart. First, the *states* describing the machine in time are quantum mechanical wavefunctions. Each basic unit of computation—the *qubit*—can be thought of as a two-dimensional complex vector of norm 1 in some Hilbert space. The two-dimensional basis for such a qubit is often labeled as $|0\rangle$ and $|1\rangle$, where the basis states correspond to the classical bit (which takes values 0 and 1). Second, the *dynamics* that governs the evolution

of the state in time is *unitary*, i.e., described by a unitary matrix that transforms the state at a certain time to the state at some later time. A second dynamical ingredient is the *measurement*. In quantum mechanics observing the system changes it. In the more restricted setting of a quantum algorithm a measurement can be thought of as a projection on the basis states. A particular basis state will be measured with a probability which is given by the squared amplitude in the state that is being measured.

Given this model, it is not even clear if such a quantum computer is able to perform classical computations. After all, a unitary matrix is invertible and hence a quantum computation is necessarily *reversible*. Classical computation given by some circuit with elementary gates, such as the AND and NOT gate, is not reversible, let alone because a gate such as the AND gate has two inputs and only one output. However, the question of reversibility of classical computation has been studied in the context of energy dissipation by Bennett in the 70s [8] (see also [48]), who established that classical computation can be made reversible with only a polynomial overhead in the number of bits and gates used. Classical reversible computation then implements just a permutation on the bitstrings of its input, and is in particular unitary. As a result, quantum computation is at least as strong as classical computation.

The next important question is whether it is possible to build a universal quantum machine (rather than special purpose computers). In other words, is there a small set of operations that implements any unitary transformation? Classically, it is well known that any Boolean function can be computed with a small set of gates, such as *AND* and *NOT*. Fortunately, it turns out that a similar statement is true for the quantum world; it was shown [15, 17] that there is a small set of universal quantum gates on at most two qubits. One such gate set is $\{X, PI/8, H, CNOT\}$, where X implements a single qubit bit-flip, $PI/8$ is a gate that multiplies the $|1\rangle$ basis state with $e^{i\frac{\pi}{4}}$, the Hadamard gate H maps $|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and the controlled *NOT* gate, a two-qubit operation, flips the second bit if the first bit is $|1\rangle$.

This paved the road for general quantum algorithm design. In this chapter we will trace the history of quantum algorithms with a focus on the milestones—Shor’s algorithm and Grover’s algorithm for unstructured search—and finish with a brief overview of recent developments. As we progress we will strip off more and more details to try to convey the general intuitions behind the main ideas in this exciting field. The reader will find detailed expositions of the classic quantum algorithms in the literature (in particular [36, 40]) and of more recent developments in the reference list.

6.2 Precursors

As mentioned before, the first quantum algorithm is Deutsch’s algorithm [14]. Before we describe it, let us clarify the notion of a quantum black-box function. Classically, a black-box function can be simply thought of as a box that evaluates an unknown function f . The input is some n -bit string x and the output is given by an m -bit string $f(x)$. Quantumly, such a box can only exist if it is reversible. To create a reversible box, the input (x) is output together with $f(x)$ and the black box looks like in Fig. 6.1.

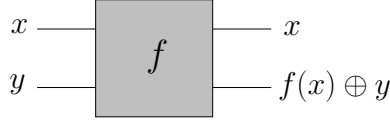


Figure 6.1. A reversible black box for a function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$.

To make the box reversible, an additional m -bit input y is added and the output of the result is $f(x) \oplus y$ where $\oplus$ denotes bitwise addition mod 2. In particular, if y is fixed to be $y = 0 \dots 0$, the output is $f(x)$. This reversible box, when given to a classical machine, is not stronger than the corresponding simple nonreversible box that maps x to $f(x)$. Note that this box now induces a transformation on $n + m$ -bit strings that can be described by a permutation of the 2^{n+m} possible strings; in particular it is unitary.

6.2.1 Deutsch's algorithm

With these notions in place we can give Deutsch's algorithm [14].

Problem: *Given a black-box function f that maps one bit to one bit, determine whether the function is constant ($f(0) = f(1)$) or balanced ($f(0) \neq f(1)$).*

Note that classically, to solve this problem with a success probability bigger than one half, a machine has to query the black box twice; both $f(0)$ and $f(1)$ are needed. Deutsch's ingenuity is to use interference of the amplitudes of the quantum state such that only one query to the black box suffices. The following circuit on two qubits gives the quantum algorithm.

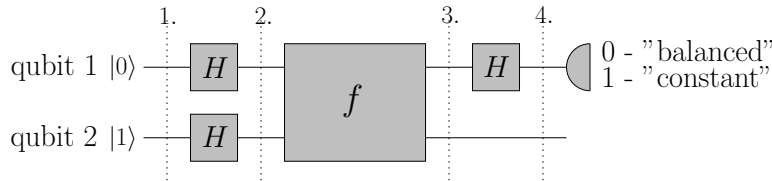


Figure 6.2. Deutsch's circuit.

1. The qubits are initialized in $|0\rangle|1\rangle$, the first ket denotes the qubit 1 and the second one qubit 2.
2. After the Hadamard transform is applied to each qubit, the state is $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$.
3. After the invocation of the black box the state of the two qubits is

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |f(0) \oplus 1\rangle) + |1\rangle(|f(1)\rangle - |f(1) \oplus 1\rangle)).$$

Note that the state of the second qubit in this expression is $\pm(|0\rangle - |1\rangle)$; the sign depends on the value of $f(0)$ (resp. $f(1)$). The state can be rewritten as

$$\frac{1}{2} \left((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) (|0\rangle - |1\rangle).$$

4. After the last Hadamard is applied, the state of the first qubit becomes

$$\frac{1}{2} \left((-1)^{f(0)} (|0\rangle + |1\rangle) + (-1)^{f(1)} (|0\rangle - |1\rangle) \right),$$

which can be rewritten as $\frac{1}{2} \left((-1)^{f(0)} + (-1)^{f(1)} \right) |0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)} \right) |1\rangle$. If the function is constant, this state is $\pm|0\rangle$, if it is balanced, the state is $\pm|1\rangle$. The final measurement will completely distinguish these two cases.

As a result, Deutsch's algorithm saves one query compared to the best possible classical algorithm for this problem. One query might seem very little, yet we will see how this algorithm has been generalized in several steps to ultimately factor numbers.

6.2.2 Deutsch–Josza algorithm

In a first step, Deutsch and Josza [16] generalized Deutsch's algorithm to give a problem where the quantum algorithm gives more than just a single query advantage. It is, however, a *promise problem*.

Problem: Given a black-box function f that maps n bits to one bit, with the promise that the function is constant ($f(x) = f(y)$) or balanced on exactly half the inputs (for all x there are exactly 2^{n-1} different y such that $f(x) \neq f(y)$), determine which one is the case.

Note that classically, to solve this problem deterministically, one needs $2^{n-1} + 1$ queries in the worst case, as in the balanced case one might have to query 2^{n-1} different y for some x before one finds a y such that $f(x) \neq f(y)$. The Deutsch–Josza algorithm solves this problem with one quantum query with the following algorithm: The analysis of this algorithm is very

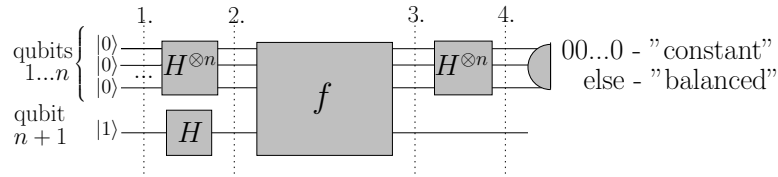


Figure 6.3. Deutsch–Josza algorithm.

similar to Deutsch's algorithm. The difference in the circuit is that the Hadamard transform on one qubit is replaced with the tensor product of n Hadamard transforms $H^{\otimes n}$ on n qubits. Let us first analyze the action of $H^{\otimes n}$ on a basis state $|x\rangle$ (x is an n -bit string). The transformation induced by a single Hadamard on a qubit i in the basis state $|x_i\rangle$ can be written as

$$H|x_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_i}|1\rangle) = \sum_{y_i \in \{0,1\}} (-1)^{x_i y_i} |y_i\rangle.$$

Applying this to $H^{\otimes n}$ with $|x\rangle = |x_1 \dots x_n\rangle$ we get

$$\begin{aligned} H^{\otimes n}|x_1 \dots x_n\rangle &= \frac{1}{\sqrt{2^n}} \left(\sum_{y_1 \in \{0,1\}} (-1)^{x_1 \cdot y_1} |y_1\rangle \right) \otimes \dots \otimes \left(\sum_{y_n \in \{0,1\}} (-1)^{x_n \cdot y_n} |y_n\rangle \right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x_1 \cdot y_1 + \dots + x_n \cdot y_n} |y\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle, \end{aligned} \quad (6.1)$$

where $x \cdot y$ is the inner product of the vectors x and y mod 2. The Hadamard transform H and $H^{\otimes n}$ are instances of a more general transformation, called the quantum Fourier transform (QFT). In our circuit $H^{\otimes n}$ gives in step 2 the state

$$\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} |y\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

As before, at step 3 the state of the system on the first n qubits is

$$|\phi_3\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f(y)} |y\rangle.$$

If the function is constant, then this state is just the uniform superposition over all bit strings (up to a global phase) and using Eq. (6.1) we see that the state at step 4 is simply $(-1)^{f(0)}|0 \dots 0\rangle$. If the final measurement gives the all zero string the output of the algorithm is “constant.” Otherwise the overlap of our state of the first n qubits at step 4, $H^{\otimes n}|\phi_3\rangle$, with the state $|0 \dots 0\rangle$ is 0, which means a measurement never gives the all zero string. To see this, note that $\langle 0 \dots 0 | H^{\otimes n} |\phi_3\rangle = (\langle 0 \dots 0 | H^{\otimes n}) |\phi_3\rangle$ and let us calculate the inner product of $|\phi_3\rangle$ with the Fourier transform of the all zero state:

$$\begin{aligned} \langle 0 \dots 0 | H^{\otimes n} |\phi_3\rangle &= \frac{1}{2^n} \left(\sum_{y_1 \in \{0,1\}^n} \langle y_1 | \right) \left(\sum_{y_2 \in \{0,1\}^n} (-1)^{f(y_2)} |y_2\rangle \right) \\ &= \frac{1}{2^n} \sum_{y_1 \in \{0,1\}^n} (-1)^{f(y_1)}. \end{aligned}$$

Using that f is balanced we get that this sum is 0. Hence in case that f is constant a measurement will always give the all zero string whereas in the balanced case we will always get an outcome different from all zeros. This completes the analysis.

Note, that the speed-up achieved by the quantum algorithm from $O(2^n)$ queries to 1 query only holds if we compare with a classical deterministic machine. If the classical machine is allowed to be probabilistic, then the classical query complexity reduces to $O(1)$: If we query the function at random then in the balanced case each of the two function values will be seen with probability 1/2 and with very high probability we will see two different function values after a constant number of queries.

In the next algorithm a quantum computer solves a problem with an exponential speed-up over the best classical *probabilistic* machine.

6.2.3 Simon's algorithm

This algorithm of Simon [47] finds the “period” of a function.

Problem: *Given a function from n bits to n bits with the promise that there is an n -bit string $a \neq 0 \dots 0$ such that for all x, y $f(x) = f(y)$ if and only if $y = x \oplus a$, find a .*

One can show that the best any classical probabilistic machine can do is to query elements at random until a collision is found. The probability of a collision for two randomly chosen elements is about 2^{-n} , and a slightly more elaborate analysis shows that the expected number of queries until a collision happens among the queried elements is $O(2^{n/2})$.

Interestingly, the quantum algorithm is very similar to the Deutsch–Jozsa algorithm with the difference that there are now $2n$ qubits as input to the black box and no Hadamard transforms on the second block of qubits, see Fig. 6.4. This circuit implements a special case of what is called quantum Fourier sampling.

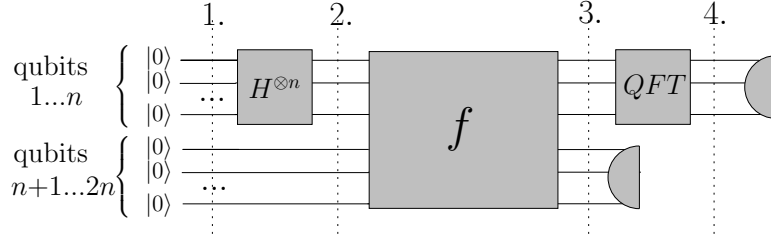


Figure 6.4. Simon's algorithm—quantum Fourier sampling. In our algorithm $QFT = H^{\otimes n}$. In general a QFT over a group G gives the quantum Fourier sampling algorithm over G .

Note that there is a partition of the 2^n input strings into two sets X and $\bar{X} = \{x \oplus a | x \in X\}$ with $|X|, |\bar{X}| = 2^{n-1}$, such that all the values $f(x)$ are distinct for $x \in X$ and similar for $\bar{X}$. At step 3 the state is

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{x \in X} \frac{1}{\sqrt{2}} (|x\rangle + |x \oplus a\rangle) |f(x)\rangle.$$

A measurement of the qubits in the second register will yield one of the 2^{n-1} values of $f(x)$ with equal probability and collapse the state of the first register to $\frac{1}{\sqrt{2}} (|x\rangle + |x \oplus a\rangle)$ for a random $x \in X$. At step 4 the state becomes

$$\begin{aligned} \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} \left((-1)^{x \cdot y} + (-1)^{(x \oplus a) \cdot y} \right) |y\rangle \\ = \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} (1 + (-1)^{a \cdot y}) |y\rangle \\ = \frac{1}{\sqrt{2^{n-1}}} \sum_{y: y \cdot a = 0} (-1)^{x \cdot y} |y\rangle. \end{aligned}$$

A measurement of the first register gives a random $y = y_1$ such that $a \cdot y_1 = 0$. We can now repeat this algorithm to obtain y_2 with $a \cdot y_2 = 0$, y_3 with $a \cdot y_3 = 0$, and so on. These y_i form a subspace of the n -dimensional vector space of all n -bitstrings (over $GF(2)$). If among the y_i there are $n - 1$ vectors that are linearly independent (i.e., such that they span a space of dimension $n - 1$), then the equations $a \cdot y_i$ completely determine $a \neq 0$. But for each set of y_i that do not yet span a space of dimension $n - 1$ the probability that the next y will be outside the space is at least $1/2$, because the space spanned by them contains at most 2^{n-2} out of the 2^{n-1} possible y 's. Hence after $O(n)$ repetitions of the algorithm with a probability exponentially close to 1 we will have enough information to determine a .

6.3 Shor's Factoring Algorithm

Conceptually it is now only a small step from Simon's algorithm to Shor's algorithm for factoring. The first necessary observation is that in order to find a factor of a number, it is sufficient to solve a problem called period finding, the problem Shor's algorithm [46] actually solves:

Problem (period finding): *Given a function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ and an integer N with the promise that there is a period $a \leq N$ such that for all x, y , $f(x) = f(y)$ if and only if $y \in \{x, x \pm a, x \pm 2a, \dots\}$, find a .*

6.3.1 Reduction from factoring to period finding

Let us assume that we want to factor the number N . Once we have an algorithm that gives one factor q of N , we can restart the algorithm on q and N/q ; we obtain all factors of N after at most $\log N$ iterations. Assume N is odd and not a power of a prime (both conditions can be verified efficiently and moreover in these cases it is easy to find a factor of N). First, we select a random $1 < y < N$ and compute $GCD(y, N)$ (this can be done efficiently using the Euclidean algorithm). If this greatest common divisor is larger than 1 we have found a nontrivial factor of N . Otherwise, y generates a multiplicative group modulo N . This group is a subgroup of $\mathbb{Z}_N^*$, the multiplicative group modulo N . The order of this group is determined by the factors of N (and is unknown to us). The smallest integer a such that $y^a \equiv 1 \pmod{N}$, known as the *order* of y , is the period of the function $f_y(x) = y^x \pmod{N}$. This function can be viewed as a function over $\mathbb{Z}$.

Invoking now the period finding algorithm we can determine a . If a is even then $N \mid (y^{\frac{a}{2}} + 1)(y^{\frac{a}{2}} - 1)$. We know that $N \nmid (y^{\frac{a}{2}} - 1)$ ($\frac{a}{2}$ is not the period of f_y), so if $N \nmid (y^{\frac{a}{2}} + 1)$ then N must have a common factor with each of $(y^{\frac{a}{2}} \pm 1)$ and we can determine it by computing $GCD(N, y^{\frac{a}{2}} - 1)$. It remains to be shown that with probability at least $1/2$ over the choice of y both conditions are satisfied, i.e., both a is even and $N \nmid (y^{\frac{a}{2}} + 1)$. This can be shown using the Chinese remainder theorem (see e.g., [36, 40, 41]).

In what follows we focus on solving the period finding problem. We use essentially the same quantum circuit as in Simon's algorithm, Fig. 6.4, namely quantum Fourier sampling with an appropriate definition of the quantum Fourier transform.

Definition: The quantum Fourier transform over $\mathbb{Z}_M$, the cyclic group of numbers mod M , implements the unitary

$$QFT : |x\rangle \longrightarrow \frac{1}{\sqrt{M}} \sum_{y \in \mathbb{Z}_M} \omega^{x \cdot y} |y\rangle,$$

where $\omega = e^{\frac{2\pi i}{M}}$ is an M th root of unity.

Note that the QFT over $\mathbb{Z}_2$ is just the Hadamard transform on one qubit, and in general the transformation $H^{\otimes n}$ in Deutsch–Josza and in Simon’s algorithms implements the QFT over the group $\mathbb{Z}_2^n$. The Fourier transform in that case is just a tensor product of single qubit unitaries. The ingenious part of Shor’s algorithm is to show that the QFT over $\mathbb{Z}_M$ is also implementable efficiently, i.e., in time polynomial in $\log M$, by a quantum circuit.

6.3.2 Implementation of the QFT

Note that the QFT implements an $M \times M$ unitary matrix with entries $\omega^{x \cdot y}$. A naive classical algorithm that computes each entry separately and then sums the appropriate rows to compute each of the amplitudes $\sum_y \omega^{x \cdot y}$ will require $O(M^2)$ steps. However, there is a well-known trick to speed up the evaluation of all these sums: The classical fast Fourier transform (FFT) takes only time $O(M \log M)$ for this task. For ease of presentation let us assume that $M = 2^n$. To evaluate $\omega^{x \cdot y} = \exp(\frac{2\pi i x \cdot y}{2^n})$, let us expand x in binary notation $x = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \dots + x_12 + x_0$ and similarly for y . In the product $x \cdot y$ we can ignore all terms divisible by 2^n as they do not contribute to the exponent. Now

$$\frac{x \cdot y}{2^n} = y_{n-1}(.x_0) + y_{n-2}(.x_1x_0) + y_{n-3}(.x_2x_1x_0) + \dots + y_0(.x_{n-1}x_{n-2} \dots x_0).$$

The terms in parenthesis are binary expansions, e.g., $.x_2x_1x_0 = x_22^{-1} + x_12^{-2} + x_02^{-3}$. The amplitude

$$\sum_{y \in \mathbb{Z}_M} \omega^{x \cdot y} = \left(\sum_{y_{n-1} \in \{0,1\}} e^{2\pi i y_{n-1}(.x_0)} \right) \dots \left(\sum_{y_0 \in \{0,1\}} e^{2\pi i y_0(.x_{n-1}x_{n-2} \dots x_0)} \right)$$

can now be evaluated sequentially in time $O(\log M)$ for each of the M values of x .

Quantum parallelism improves this drastically. We can write

$$\begin{aligned} \frac{1}{\sqrt{M}} \sum_{y \in \mathbb{Z}_M} \omega^{x \cdot y} |y\rangle &= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i(.x_0)} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i(.x_1x_0)} |1\rangle \right) \otimes \\ &\dots \otimes \left(|0\rangle + e^{2\pi i(.x_{n-1} \dots x_1x_0)} |1\rangle \right). \end{aligned}$$

Figure 6.5 shows a circuit that implements this transformation on $\mathbb{Z}_8$. The Hadamard on qubit x_i can be thought of as performing $|x_i\rangle \rightarrow (|0\rangle + e^{2\pi i(.x_i)} |1\rangle)$. The conditional rotations R_d give a phase of $e^{i\pi/2^d}$ to the qubit on which they act whenever the control qubit is in the state $|1\rangle$. The obvious generalization of this circuit to n qubits has $\frac{1}{2}n(n+1) = O(\log^2 M)$ gates.

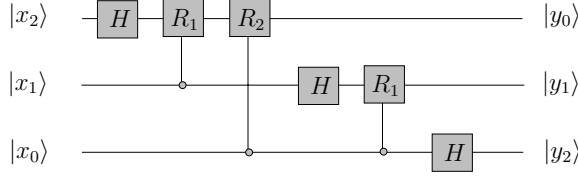


Figure 6.5. QFT on $\mathbb{Z}_8$. An element of $\mathbb{Z}_8$ is represented in binary notation $x = x_2x_1x_0$, $y = y_2y_1y_0$.

6.3.3 Shor's algorithm for period finding

With this implementation of the QFT in place we can analyze the algorithm in Fig. 6.4 for period finding. We need to choose the integer M over which the QFT is performed. For our problem ($a \leq N$) we chose $M = 2^n$ to be a power of 2 such that $N^2 < M \leq N^4$.

For the moment, let us make the simplifying assumption that the period a divides M . At step 2 the first register is in a uniform superposition over all elements of $\mathbb{Z}_M$. As in Simon's algorithm the state at step 3 after the measurement of the second register is

$$\sqrt{\frac{a}{M}} (|x\rangle + |x+a\rangle + \cdots + |x + (\frac{M}{a} - 1)a\rangle) |f(x)\rangle \quad (6.2)$$

for some random $x \in \mathbb{Z}_M$. The QFT transforms the state of the first n qubits into

$$\frac{\sqrt{a}}{M} \sum_{y \in \mathbb{Z}_M} \left(\sum_{j=0}^{M/a-1} \omega^{(x+ja)y} \right) |y\rangle = \frac{\sqrt{a}}{M} \sum_{y \in \mathbb{Z}_M} \omega^{xy} \left(\sum_{j=0}^{M/a-1} \omega^{j ay} \right) |y\rangle. \quad (6.3)$$

Since a divides M , we have that whenever $\omega^{ay} \neq 1$, i.e., whenever $y \notin \{0, M/a, 2M/a, \dots, (a-1)M/a\}$

$$\sum_{j=0}^{\frac{M}{a}-1} (\omega^{ay})^j = \frac{1 - \omega^{My}}{1 - \omega^{ay}} = 0.$$

This implies that in Eq. (6.3) the amplitudes of basis states $|y\rangle$ for y not a multiple of M/a are zero. Consequently the state at step 4 is a superposition over all $y \in \{0, M/a, 2M/a, \dots, (a-1)M/a\}$ and a measurement gives a uniformly random $y = cM/a$. To extract information about a we need to solve $y/M = c/a$. Whenever c is coprime to a (which can be shown to happen with a reasonably good probability $\Omega(1/\log \log a)$) we can write y/M as a minimal fraction; the denominator gives a .

In the (more likely case) that a does not divide M it is not hard to see that the same algorithm will give with high probability a y such that $|y/M - c/a| \leq 1/2M$ for some $0 \leq c < a$. But two distinct fractions with denominator at most N must be at least $1/N^2 > 1/M$ apart, so c/a is the unique fraction with denominator at most N within distance $1/2M$ from y/M and can be determined with the continued fraction expansion.

Note that in Shor's algorithm the function $f_y(x) = y^x \bmod M$ is not given by a black box, but needs to be computed every single time. This could be difficult since the exponent x is very large. However, using the binary expansion of x and repeated squaring, it is not hard to see that there exists a classical subroutine for computing f_y in time polynomial in $\log M$. As a result Shor's algorithm gives a factor of N with high probability in time polynomial in $\log N$.

6.4 Grover's Algorithm

The second milestone in quantum algorithm design is Grover's algorithm for unstructured search [28, 29]. The problem of unstructured search is paradigmatic for any problem where an optimal solution needs to be found in a black-box fashion, i.e., without using the possible structure of the problem:

Problem: Given a Boolean black-box function $f_w : \{0, 1\}^n \rightarrow \{0, 1\}$ which is equal to 0 for all inputs except one ("marked item" w), find the marked item w .

Classically, a deterministic algorithm needs to make $2^n - 1$ queries to identify w in the worst case and a probabilistic algorithm still needs $O(2^n)$ queries. Grover gave a quantum algorithm that solves this problem with $O(\sqrt{2^n})$ queries and this is known to be the best possible. Grover's algorithm can hence speed up quadratically any algorithm that uses searching as a subroutine.

Grover's quantum algorithm applies the subroutine of Fig. 6.6 about $\sqrt{2^n}$ times. Here,

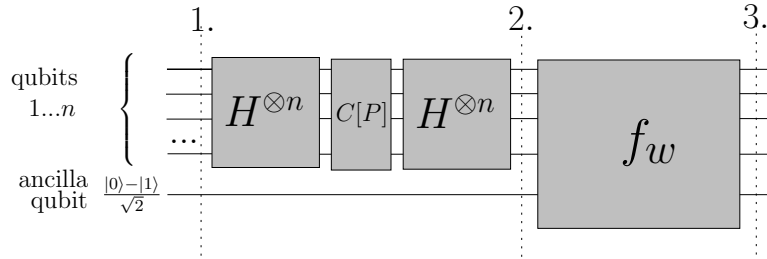


Figure 6.6. Subroutine in Grover's algorithm

the n -qubit gate $C[P]$ denotes a controlled phase; it flips the sign of all basis states except for the all zero state. Its action can be concisely written as $C[P] = 2|0 \dots 0\rangle\langle 0 \dots 0| - I_n$, where I_n denotes the identity on n qubits. This operation is conjugated by the Hadamard transform, which maps $|0 \dots 0\rangle$ to the uniform superposition $|\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$. So the net operation between steps 1 and 2 can be written as $R_\Psi = 2|\Psi\rangle\langle\Psi| - I_n$. It is sometimes called diffusion or reflection around the mean, because it flips the amplitude of a state around its "mean" $\frac{1}{\sqrt{2^n}}$. The operation between steps 2 and 3 with the ancillary qubit set to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is similar to Fig. 6.3; it gives a phase of $(-1)^{f(x)}$ to the basis state $|x\rangle$. In our case only $f(w)$ is nonzero and so only the phase of $|w\rangle$ is flipped. This operation can be written as

$R_w = I_n - 2|w\rangle\langle w|$. It is called reflection around w . Grover's algorithm first applies $H^{\otimes n}$ to the state $|0 \dots 0\rangle$ and then iterates T times the subroutine $R_w R_\Psi$ of Fig. 6.6.

Note that with input $|\Psi\rangle$ the subroutine in Fig. 6.6 leaves invariant the subspace spanned by $|\Psi\rangle$ and $|w\rangle$. Inside this space it acts as a real rotation with angle ϕ , where $\phi \approx \sin \phi = \frac{1}{\sqrt{2^n}}$. After T time steps the state rotates from $|\Psi\rangle$ toward the nearly orthogonal $|w\rangle$ by an angle $T\phi$. Choosing $T = \lfloor \frac{\pi}{2} \sqrt{2^n} \rfloor$ gives a state that overlaps with $|w\rangle$ very close to 1. A measurement now gives w with very high probability.

It is not hard to see that this algorithm also works in the case of k marked items in the database; in this case its running time is $O(\sqrt{\frac{2^n}{k}})$.

6.5 Other Algorithms

Developments in quantum algorithm design after Shor's and Grover's algorithms can be loosely grouped into three categories: algorithms that generalize Shor's algorithm (hidden subgroup algorithms), algorithms that perform some version of unstructured search ("Grover-like" algorithms) and a few algorithms that do not fit into either of these categories. The scope of this chapter restricts us to mention only a small selection of new quantum algorithms and techniques.

6.5.1 The hidden subgroup problem

Shor's algorithm can be seen as an instance of a more general problem, the hidden subgroup problem. The function f in the period finding problem, viewed over $\mathbb{Z}_M$, is constant on sets $\{x, x+a, \dots\}$ for each x and distinct on such disjoint sets; if a divides M it is constant on cosets $x + \langle a \rangle$ of the subgroup of $\mathbb{Z}_M$ generated by a and distinct on different such cosets.

Definition: The hidden subgroup problem (HSP)—given a function $f : G \rightarrow R$ on a group G , and a subgroup $H < G$ such that f is constant on (left) cosets of H and distinct for different cosets, find a set of generators for H .

The HSP is an important problem. An efficient algorithm for the group $\mathbb{Z}_M$ yields an efficient factoring algorithm. It is also a component of an efficient algorithm for the discrete logarithm over $\mathbb{Z}_M$. Discrete logarithm is another cryptographic primitive in classical cryptography which would be broken by a quantum computer. Quantumly, a slight generalization of Shor's algorithm gives an efficient algorithm for HSP for all *Abelian* groups. Kitaev [35–37] developed a quantum algorithm for the Abelian Stabilizer problem, another instance of the hidden subgroup problem, using *phase estimation*, which corresponds in a way to the quantum Fourier transform and also solves the HSP over Abelian groups. Using the Abelian HSP Hallgren [30] gives a polynomial time quantum algorithm for Pell's equation, a number theoretic problem known to be at least as hard as factoring. Among other applications of the HSP, Friedl *et al.* [26] solve the hidden translation problem: given two functions f and g defined over some group $\mathbb{Z}_p^n$ such that $f(x) = g(x+t)$ for some hidden translation t , find t .

One of the most interesting challenges since Shor is to design quantum algorithms for the non-Abelian HSP. For instance, an efficient solution for the symmetric group S_n (permutations of n elements) would give an efficient algorithm for the graph isomorphism problem: to

determine whether two given graphs are equal up to permutation of the vertices. Another important problem is the HSP over the dihedral group D_N (the group of symmetries of a regular N -gon). A solution in this case would give an algorithm for the shortest vector problem in a lattice; this reduction was shown by Regev [42]. The shortest vector problem is at the base of several classical cryptographic schemes designed as an alternative to those based on factoring or discrete logarithm.

In the context of the HSP over any group, Ettinger, Høyer and Knill [20] showed that a polynomial amount of coset states of the form

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + h\rangle |f(x)\rangle$$

(compare with Eq. (6.2)) are enough to theoretically obtain all the information about the hidden subgroup H . However, to *extract* this information they need exponential amount of time in the worst case; hence this algorithm is not efficient in general. For the HSP over the dihedral group D_{2^n} Kuperberg [38] gives a quantum algorithm that runs in time $2^{O(\sqrt{n})}$, a quadratic improvement in the exponent over [20] (and over any classical algorithm). There has been a lot of effort in analyzing the performance of quantum Fourier sampling (Fig. 6.4), when the QFT is the Fourier transform over the group G , when the hidden subgroup H is a subgroup of G . In the case of the symmetric group, the (non-Abelian) QFT is efficiently implementable by a quantum computer [7]; however a series of papers [27, 31, 33, 39] showed that this approach to the problem cannot work (in the case of measurements of one or two copies on the state in step 4 in Fig. 6.4). It is an open question whether there are any efficient quantum algorithms for the HSP using other tools, not necessarily based on the QFT.

6.5.2 Search algorithms

Several quantum algorithms that use Grover's search as a subroutine have been found and shown to have a polynomial speed up over their classical counterparts. For example, Brassard *et al.* [10] give a quantum algorithm for the problem of finding collisions in a k -to-1 function. For a k -to-1 black-box function f the task is to find a collision, i.e., two inputs $x \neq y$ such that $f(x) = f(y)$. The idea is to first classically query a set K of size $|K| = (N/k)^{1/3}$ and check it for collisions, which can be done with $O((N/k)^{1/3})$ queries. If a collision is found the algorithm outputs it and stops, otherwise we set up a Grover search for a function f defined outside K that is 1 if there is a collision with an element in K . In that case there are $(k-1)|K| \approx k^{2/3} N^{1/3}$ "marked items" and Grover's search runs in time $\sqrt{N/(k^{2/3} N^{1/3})} = (N/k)^{1/3}$. So the total number of queries of this algorithm is $O((N/k)^{1/3})$, better than any classical algorithm.

Other applications of Grover's algorithm include deciding whether all elements in the image of a function on N inputs are distinct [11], which can be done in time $O(N^{3/4})$ with Grover's algorithm as a subroutine. Note that recently a better quantum algorithm based on quantum walks has been given for this problem [4] (see the next section). In [19] optimal quantum algorithms for graph problems such as (strong) connectivity, minimum spanning tree and shortest path are given using Grover's search.

6.5.3 Other algorithms

Most known quantum algorithms are based on either the QFT or Grover's search. A few quantum algorithms fall outside these two frameworks. One such remarkable algorithm is for searching in an ordered list, a problem that classically takes time $\log_2 N + O(1)$. Two quantum algorithms have been given for this problem, both based on binary trees. The best known algorithm by Farhi *et al.* [22] finds a good quantum algorithm on a small subtree and then recurses, running with $0.526 \log_2 N$ queries. A very appealing algorithm was given by Høyer *et al.* [32] using the Haar transform on the binary tree with $\log_3 N + O(1) \approx 0.631 \log_2 N + O(1)$ queries; a very interesting application of alternative efficient quantum transformations outside the QFT.

6.6 Recent Developments

We have seen that two types of quantum algorithms dominate the field, those that implement a version of the hidden subgroup problem or use the QFT and those that use a version of Grover's search. Recently, two alternative trends have entered the field, which we will briefly outline.

6.6.1 Quantum walks

One of the biggest breakthroughs in classical algorithm design was the introduction of randomness and the notion of a probabilistic algorithm. Many problems have good algorithms that use a *random walk* as a subroutine. To give just one example, the currently best algorithm to solve 3SAT [45] is based on a random walk. Keeping this motivation in mind, quantum analogues of random walks have been introduced. There exist two different models of a quantum walk, the continuous-time model introduced in [23] and the discrete-time model of [1, 5]. The continuous model gives a unitary transformation directly on the space on which the walk takes place. The discrete model introduces an extra coin register and defines a two-step procedure consisting of a “quantum coin flip” followed by a coin-controlled walk step. The quantities important for algorithm design with random walks are their mixing time—the time it takes to be close to uniformly distributed over the domain—and the hitting time—the expected time it takes to hit a certain point. These quantities have been analyzed for several graphs in both the continuous and the discrete model. It turns out that a quantum walk can speed up the mixing time up to quadratically with respect to its classical counterpart; so the classical and quantum performance are polynomially related. The hitting behavior of a quantum walk, however, can be very different from classical. It has been shown that there are graphs and two vertices in them such that the classical hitting time from one vertex to the other is polynomial in the number of vertices of the graph, whereas the quantum walk is exponentially faster. Using this idea in [12] an (artificial) problem is constructed for which a quantum walk based algorithm gives a provable exponential speed-up over any classical probabilistic algorithm. It is open whether quantum hitting times can be used to speed up classical algorithms for relevant problems.

Based on this work a quantum walk algorithm has been introduced in [44] for the problem of finding a marked vertex in a graph. The idea is very simple: the algorithm starts in the

uniform superposition over all vertices. At each step it performs a quantum walk; there are two local rules for the walk, at an unmarked vertex the walk proceeds as usual, but at a marked vertex a different transition rule is applied (usually at an unmarked vertex a quantum coin is flipped and at a marked vertex it is not flipped). It turns out that after some time the amplitude of the state concentrates in the marked item(s); a measurement finds a marked item with high probability.

This algorithm solves Grover's problem on a graph. Why do we need a quantum walk search if we have Grover's algorithm? It turns out that there are situations when the diffusion step R_Ψ of Grover's algorithm cannot be implemented efficiently (because the local topology of the database does not allow for it, because of limitations on the quantum gates or because it is too costly in a query setting). A quantum walk only makes local transitions and can be more advantageous. One example is the search for a marked item in a two-dimensional database. In this case Grover's algorithm requires $\sqrt{N}$ queries, but to shift amplitude from one item of the database to another on the grid takes an additional $\sqrt{N}$ steps on average per query. The net complexity of the algorithm becomes $\sqrt{N} \cdot \sqrt{N} = N$ and the quantum advantage is lost. The quantum walk algorithm has been shown to find a marked item in time $O(\sqrt{N} \log N)$ [6].

A second example of the superiority of the quantum walk search over Grover's algorithm has been given in [4]. Ambainis uses a quantum walk to give an improved algorithm for element distinctness, which runs in optimal time $O(N^{2/3})$, thus improving over Grover-based algorithms for this problem (which runs in time $O(N^{3/4})$, see Section 6.5). Several new quantum walk based algorithms with polynomial improvements over Grover-based algorithms have followed suit. For references on quantum walks, see [3, 34].

6.6.2 Adiabatic quantum algorithms

Another recent alternative for algorithm design has been the introduction of adiabatic quantum algorithms by Farhi *et al.* [21]. The idea is as follows: many optimization and constraint satisfaction problems can be encoded into a sum of local Hamiltonians $H = \sum_i H_i$ such that each term H_i represents a local constraint. The ground state of H violates the smallest number of such constraints and represents the desired optimal solution. In order to obtain this state, another Hamiltonian H' is chosen such that the ground state of H' , $|\Phi'\rangle$, is easy to prepare. An adiabatic algorithm starts in the state $|\Phi'\rangle$ and applies H' . The Hamiltonian is then slowly changed from H' to H , usually in a linear fashion over time, such that the Hamiltonian at time t is given by $H(t) = (1 - t/T)H' + (t/T)H$. Here T is the total runtime of the algorithm. If this is done slowly enough, the adiabatic theorem guarantees that the state at time t will be the ground state of $H(t)$, leading to the solution, the ground state of H , at time T . The instantaneous ground state of the system is "racked." But how slow is slow enough? The *adiabatic theorem* gives bounds on the speed of change of $H(t)$ such that the state remains close to the ground state. These bounds are determined by the energies of the Hamiltonian H and by the inverse gap of the Hamiltonians $H(t)$. The gap of a Hamiltonian is the energy difference between its ground state and first excited state, or the difference between its smallest and second smallest eigenvalue when viewed as a matrix. To design an efficient adiabatic algorithm, one has to pick H and H' such that the gap of $H(t)$ at all times t is at least inverse polynomial in the size of the problem.

Farhi *et al.* set up adiabatic algorithms for NP -complete problems like 3SAT [21]. It has been impossible so far to determine the gap analytically and the number of qubits in numerical simulations is limited. However, this approach seems promising, even though there is now mounting evidence that an adiabatic algorithm cannot solve NP -complete problems efficiently. For instance, quantum unstructured search has been implemented adiabatically and shown to have the same runtime as Grover's algorithm [13, 43].

It is not hard to see that an adiabatic algorithm can be simulated efficiently with a quantum circuit [21]—one needs to implement a time-dependent unitary that is given by a set of local Hamiltonians, each one acting only on a few qubits. Recently it has been shown [2] that also any quantum circuit can be simulated efficiently by an appropriate adiabatic algorithm; hence these two models of computation are essentially equivalent. This means that a quantum algorithm can be designed in each of the two models. The advantage of the adiabatic model is that it deals with gaps of Hermitian matrices, an area that has been widely studied both by solid state physicists and probabilists. Hopefully this new toolbox will yield new algorithms.

Exercises

1. Universality.

Give an implementation of the n -qubit gate $C[P]$ in Grover's algorithm $C[P] = 2|0 \dots 0\rangle\langle 0 \dots 0| - I_n$ in terms of the elementary one- and two-qubit gates from the universal set $\{X, PI/8, H, CNOT\}$ (see Section 6.1).

2. Bernstein–Vazirani algorithm. [9]

Give a quantum algorithm for the following problem. Given a function $f_a : \{0, 1\}^n \rightarrow \{0, 1\}$, $f_a(x) = a \cdot x (= \sum_{i=1}^n a_i x_i)$ for some $a \in \{0, 1\}^n$, find a with one query only. How many queries are needed in a classical deterministic algorithm? In a classical probabilistic algorithm?

3. QFT with bounded precision.

Quantum gates cannot be implemented with perfect precision. Define the *error* of a gate U that is supposed to implement V as $E(U, V) := \max_{|v\rangle: \|v\|=1} \|(U - V)|v\rangle\|$. We have seen an implementation of the QFT over $\mathbb{Z}_N$ with about $\frac{1}{2} \log^2 N$ gates.

(a) Show: If each gate in the QFT is implemented with error at most ϵ for some $\epsilon > 0$, then this circuit approximates the QFT with error $O(\log^2 N / \epsilon)$.

(b) Give a circuit with only $O(\log N \log \log N)$ gates that for any $c > 1$ approximates the QFT to within error $1 / \log^c N$.

4. Grover with several marked items.

First, compute the runtime of Grover's algorithm when there are exactly k marked items and k is known in advance. Then, give an algorithm for Grover's problem when the number of marked items is not known.

5. Minimum finding [18]

Given N distinct integers, design a quantum algorithm that finds their minimum with $O(\sqrt{N} \log N)$ queries. *Hint:* Pick a random element and use $O(\log N)$ rounds. In each round use Grover's search to replace this element with another one that is smaller.

References

- [1] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proc. 33th ACM Symp. on the Theory of Computing (STOC)*, pp. 50–59, 2001.
- [2] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation. In *Proc. 45th Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pp. 42–51, 2004.
- [3] A. Ambainis. Quantum search algorithms (survey). *SIGACT News*, 35(2):22–35, 2004.
- [4] A. Ambainis. Quantum walk algorithm for element distinctness. In *Proc. 45th Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pp. 22–31, 2004 (Preprint quant-ph/0311001).
- [5] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous. One-dimensional quantum walks. In *Proc. 33th ACM Symp. on the Theory of Computing (STOC)*, pp. 60–69, New York, NY, 2001.
- [6] A. Ambainis, J. Kempe, and A. Rivosh. Coins make quantum walks faster. In *Proc. 16th ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pp. 1099–1108, 2005.
- [7] R. Beals. Quantum computation of Fourier transforms over symmetric groups. In *Proc. 29th STOC*, pp. 48–53, 1997.
- [8] Ch. Bennett. Logical reversibility of computation. *IBM J. Res. Dev.*, 17:5225, 1973.
- [9] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26:1411, 1997.
- [10] G. Brassard, P. Hoyer, and A. Tapp. Quantum cryptanalysis of hash and claw-free functions. In *Proc. 3rd Latin American Symp. on Theoretical Informatics (LATIN)*, (number 1380 in LNCS), pp. 163–169, 1998.
- [11] H. Buhrman, C. Dürr, M. Heiligman, P. Høyer, F. Magniez, M. Santha, and R. de Wolf. Quantum algorithms for element distinctness. In *Proc. 15th IEEE Conf. on Computational Complexity*. Extended version in *SIAM J. Comput.*, 34(6):1324–1330, 2005.
- [12] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proc. 35th ACM Symp. on the Theory of Computing (STOC)*, pp. 59–68, 2003.
- [13] W. van Dam, M. Mosca, and U. Vazirani. How powerful is adiabatic quantum computation? In *Proc. 42nd Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pp. 279–287, 2001.
- [14] D. Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97–117, 1985.
- [15] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. *Proc. R. Soc. Lond. A*, 449:669, 1995.
- [16] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A* 439:553–558, 1992.
- [17] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51(2):1015–1022, 1995.
- [18] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum. Technical report 1996 (Preprint quant-ph/9607014).

- [19] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla. Quantum query complexity of some graph problems. In *Proc. 31st Int. Colloquium on Automata, Languages, and Programming (ICALP)*, (number 3142 in LNCS), pp. 481–493, 2004.
- [20] M. Ettinger, P. Høyer, and E. Knill. Hidden subgroup states are almost orthogonal. *Inf. Process. Lett.*, 91(1):43–48, 2004.
- [21] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. *Science*, 292(5516):472–476, 2001.
- [22] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Invariant quantum algorithms for insertion into an ordered list. Technical report 1999 (*Preprint quant-ph/9901059*).
- [23] E. Farhi and S. Gutmann. Quantum computation and decision trees. *Phys. Rev. A*, 58:915–928, 1998.
- [24] R. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.
- [25] R. Feynman. Quantum mechanical computers. *Opt. News*, 11:11–21, 1985.
- [26] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proc. 35th ACM Symp. on Theory of Computing (STOC)*, pp. 1–9, 2003.
- [27] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. In *Proc. 33th ACM Symp. on Theory of Computing (STOC)*, pp. 68–74, 2001.
- [28] L. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th ACM Symp. on Theory of Computing (STOC)*, pp. 212–219, 1996.
- [29] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325, 1997.
- [30] S. Hallgren. Polynomial-time quantum algorithms for Pell’s equation and the principal ideal problem. In *Proc. 34th ACM Symp. on Theory of Computing (STOC)*, pp. 653–58, 2002.
- [31] S. Hallgren, A. Russell, and A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proc. 32nd ACM Symp. on Theory of Computing (STOC)*, pp. 627–635, 2000.
- [32] P. Høyer, J. Neerbeck, and Y. Shi. Quantum complexities of ordered searching, sorting and element distinctness. *Algorithmica*, 34(4):429–448, 2002. (Special issue in *Quantum Computation and Cryptography*).
- [33] J. Kempe and A. Shalev. The hidden subgroup problem and permutation group theory. In *Proc. 16th ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pp. 1118–1125, 2005.
- [34] J. Kempe. Quantum random walks—an introductory overview. *Contemp. Phys.*, 44(4):302–327, 2003.
- [35] A. Kitaev. Quantum measurements and the Abelian stabilizer problem 1995 *Preprint quant-ph/9511026*.
- [36] A. Y. Kitaev, A. H. Shen, and M. N. Vyalı. *Classical and Quantum Computation* (Number 47 in Graduate Series in Mathematics), AMS, Providence, RI, 2002.
- [37] A. Yu. Kitaev. Quantum computations: Algorithms and error corrections. *Russ. Math. Surveys*, 52:1191–1249, 1997.

- [38] G. Kuperberg. A subexponential-time algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005.
- [39] C. Moore, A. Russell, and L. Schulman. The symmetric group defies strong Fourier sampling. In *Proc. 46th Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pp. 479–490, 2005.
- [40] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.
- [41] J. Preskill. Quantum information and computation. *Lecture Notes*. <http://www.theory.caltech.edu/people/preskill/ph229/>, 1998.
- [42] O. Regev. Quantum computation and lattice problems. In *Proc. 43rd Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pp. 520–529, 2002.
- [43] J. Roland and N. Cerf. Quantum search by local adiabatic evolution. *Phys. Rev. A*, 65:042308, 2002.
- [44] N. Shenvi, J. Kempe, and K. B. Whaley. A quantum random walk search algorithm. *Phys. Rev. A*, 67(5):052307, 2003.
- [45] U. Schöning. A probabilistic algorithm for k -SAT and constraint satisfaction problems. In *40th Ann. Symp. on Foundations of Computer Science*, pp. 410–414, IEEE, New York, 1999.
- [46] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. preliminary version in *Proc. 35th Ann. IEEE Symp. on the Foundations of Computer Science (FOCS)*, pp. 124–134, 1994.
- [47] D. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997. preliminary version in *Proc. 26th ACM Symp. on Theory of Computing (STOC)*, pp. 116–123, 1994.
- [48] T. Toffoli. Reversible computing. In W. de Bakker and J. van Leeuwen, editors *Automata, Languages and Programming*, p. 632, Springer, New York, 1980.

7 Quantum Error Correction

Markus Grassl

7.1 Introduction

In the theory of quantum information processing, it is usually assumed that the quantum mechanical system is completely decoupled from its environment. On the other hand, when implementing quantum operations on a real quantum mechanical system, some interaction with the system is needed in order to control the dynamics of the system. Moreover, this control has only finite precision. So it seems to be inevitable that the state of the quantum system decoheres, and eventually the behavior of the system becomes more and more classical. Before Peter Shor's first paper on quantum error correction [Sho95], it was widely believed that quantum information processing was a purely theoretical computation model without any perspective of realization.

Ten years later, the theory of quantum error correction is widely developed. In what follows, we give an introduction to the basic concepts of quantum error correction, illustrated by some simple quantum error-correcting codes. We start with a brief introduction to the general mathematical framework.

7.2 Quantum Channels

Similar to the classical situation, one needs a model of the errors in order to design a code that is able to correct them. For this, we consider the joint Hilbert space $\mathcal{H}_{\text{sys/env}} := \mathcal{H}_{\text{sys}} \otimes \mathcal{H}_{\text{env}}$ of the system used for information processing and its environment. If the dimensions of both Hilbert spaces are sufficiently large, the initial state is without loss of generality pure. Moreover, we make the assumption that initially the system and its environment are decoupled, i.e., the initialization process is perfect. Again by possibly increasing the dimension of the Hilbert spaces, the interaction between the system and the environment can be modeled by a unitary transformation $U_{\text{env/sys}}$ on the joint Hilbert space (see Fig. 7.1).

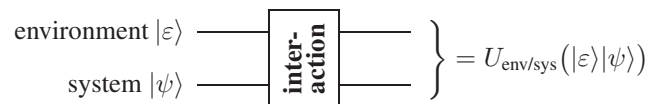


Figure 7.1. Modeling the interaction with the environment by a unitary transformation.

As we have no access to the environment, we are only interested in the state of the system and its dynamics. Tracing out the environment yields the possibly mixed state

$$\rho_{\text{out}} = \text{Tr}_{\text{env}} \left(U_{\text{env/sys}}(|\varepsilon\rangle|\psi\rangle\langle\varepsilon|\langle\psi|)U_{\text{env/sys}}^\dagger \right). \quad (7.1)$$

Equivalently, the state (7.1) can be written as a function of the input state $\rho_{\text{in}} = |\psi\rangle\langle\psi|$ in the form

$$\rho_{\text{out}} = \sum_i E_i \rho_{\text{in}} E_i^\dagger,$$

where the operators E_i are the so-called *error operators* or *Kraus operators* [Kra83]. They completely describe the quantum channel given by the initial state $|\varepsilon\rangle$ of the environment and the unitary interaction $U_{\text{env/sys}}$. Not all choices for a set of Kraus operators give rise to a quantum mechanical channel, but a quantum channel has nonetheless many degrees of freedom. In what follows, we consider some important special cases.

Example 7.1 (depolarizing channel) A *depolarizing channel* on the Hilbert space $\mathcal{H}$ of dimension $d = \dim \mathcal{H}$ with error parameter p ($0 \leq p \leq 1$) is given by the mapping

$$\rho \mapsto (1-p)\rho + p\frac{1}{d}I.$$

This channel has only a single parameter p which can be interpreted as follows: with probability $1-p$, the depolarizing channel transmits the input state unchanged, and with probability p , it is replaced by a completely mixed state. Note that the parameter p does not equal the probability of an error as it is the case, e.g., for the classical binary symmetric channel and its generalization (see Chapter 1.1, p. 8). This is due to the fact that the completely mixed state describes a completely random quantum state. Hence the probability of observing a particular pure state is $1/\dim \mathcal{H}$, independent of the pure state. So even in the “error case”, there is a nonzero probability of measuring the input state at the output.

For qubit systems, the depolarizing channel can also be described as follows:

$$\rho \mapsto (1-p)\rho + p/4 \left(\rho + \sigma_x \rho \sigma_x^\dagger + \sigma_y \rho \sigma_y^\dagger + \sigma_z \rho \sigma_z^\dagger \right).$$

In this representation, the channel transmits the state undisturbed with probability $1-p$, and with probability p an error operator is applied. The four different error operators are given by the Pauli matrices and identity, each of which is applied with equal probability. This means that in the “error case” with equal probability the spin of a spin-1/2 particle is unchanged or one of the x -, y -, or z -components is flipped.

In some sense, the depolarizing channel is the quantum mechanical generalization of a uniform symmetric channel. Any input state is treated in the same way; there are no states which are transmitted particularly well or badly. The next channel is basis dependent.

Example 7.2 (dephasing channel) A *dephasing channel* on the Hilbert space $\mathcal{H}$ with orthonormal basis $\mathcal{B} = \{|\mathbf{b}_i\rangle : i \in \mathcal{I}\}$ and error probability p ($0 \leq p \leq 1$) is given by the mapping

$$\rho \mapsto (1-p)\rho + p \sum_{i \in \mathcal{I}} |\mathbf{b}_i\rangle\langle\mathbf{b}_i| \rho |\mathbf{b}_i\rangle\langle\mathbf{b}_i|.$$

The operational interpretation of this channel is that with probability p , the channel performs a projective measurement with respect to the basis $\mathcal{B}$. The name dephasing channel is derived from the fact that this is equivalent to randomizing the phases of the basis states. The dephasing channel allows us to perfectly transmit classical information by encoding the information as basis states. Coherent superpositions of basis states, however, are changed into classical mixtures.

The quantum mechanical analogue of a memoryless channel is a *product channel* which is defined for a quantum system $\mathcal{H}$ with n subsystems of equal dimension, i.e., $\mathcal{H} = \mathcal{H}_0^{\otimes n}$. The product channel is given by n uses of a channel $\mathcal{Q}_0$ on $\mathcal{H}_0$, acting independently on each of the n subsystems. If the channel $\mathcal{Q}_0$ is given by the error operators $\mathcal{E}_0 = \{E_i : i \in \mathcal{I}\}$, the error operators of the product channel on $\mathcal{H}$ are

$$\mathcal{E} = \mathcal{E}_0^{\otimes n} := \{E_{i_1} \otimes E_{i_2} \otimes \dots \otimes E_{i_n} : (i_1, i_2, \dots, i_n) \in \mathcal{I}^n\}.$$

In order to compare quantum channels—with or without error correction—we have to quantify how close the output of a quantum state is to the input, i.e., how much the state has been changed by the channel. As we allow a channel to act on a part of the system, we additionally want to preserve a possible entanglement of the input state with the rest of the system. The situation is depicted in Fig. 7.2. The state space of the system is $\mathcal{H}_{\text{ref}} \otimes \mathcal{H}_{\text{comp}}$. The quantum channel $\mathcal{Q}$, represented by $U_{\mathcal{Q}}$, acts only on $\mathcal{H}_{\text{comp}}$. Tracing out the environment $\mathcal{H}_{\text{env}}$, we get the state ρ' on $\mathcal{H}_{\text{ref}} \otimes \mathcal{H}_{\text{comp}}$. Hence the state $|\psi\rangle$ is mapped to ρ' .

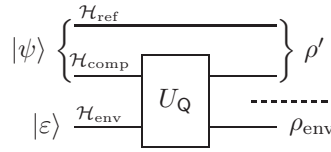


Figure 7.2. Unitary representation of a quantum channel acting on the subsystem $\mathcal{H}_{\text{comp}}$ of the composed system $\mathcal{H}_{\text{ref}} \otimes \mathcal{H}_{\text{comp}}$.

The *entanglement fidelity* of the channel $\mathcal{Q}$ described by the initial state $|\varepsilon\rangle$ of the environment and the unitary transformation $U_{\mathcal{Q}}$ is given by

$$F_e(\mathcal{Q}) := \min_{|\psi\rangle} \langle \psi | \rho' | \psi \rangle, \quad (7.2)$$

where the minimization is over all pure states $|\psi\rangle$ of the composed system $\mathcal{H}_{\text{ref}} \otimes \mathcal{H}_{\text{comp}}$. It can be shown that (7.2) is independent of the system $\mathcal{H}_{\text{ref}}$ and can be computed in terms of the error operators $\mathcal{E}_{\mathcal{Q}} = \{E_i : i \in \mathcal{I}\}$ of the channel [Schu96]:

$$F_e(\mathcal{Q}) = \min_{\rho_{\text{comp}}} \sum_{i \in \mathcal{I}_{\mathcal{Q}}} |\text{Tr}(\rho_{\text{comp}} E_i)|^2,$$

where the minimization is over all mixed states $\rho_{\text{comp}} = \text{Tr}_{\text{ref}}(|\psi\rangle\langle\psi|)$ of the system $\mathcal{H}_{\text{comp}}$.

Now we are ready to define the capacity of a quantum channel. For simplicity, we consider quantum systems which are composed of subsystems of equal dimension.

Definition 7.1 (quantum channel capacity) Let Q be a (memoryless) quantum channel on $\mathcal{H}$. By C and D we denote quantum operations mapping states from $\mathcal{H}^{\otimes k}$ to $\mathcal{H}^{\otimes n}$ and vice versa, respectively. Furthermore, let F be a fidelity measure for quantum channels. Then the *capacity* $\mathcal{Q}$ of the channel is given by

$$\mathcal{Q}(Q) := \lim_{\varepsilon \rightarrow 0} \limsup_{n \rightarrow \infty} \left\{ \frac{k}{n} \mid \exists k, C, D: F(DQ^{\otimes n}C) > 1 - \varepsilon \right\}. \quad (7.3)$$

Expression (7.3) states that in the limit of large n for a given number k of inputs to our system we can find encoding and decoding operations C and D such that the fidelity of the composed channel $DQ^{\otimes n}C$ approaches 1. As the channel is memoryless, n uses of the channel do not introduce any correlations between the subsystems. However, using entangled input states for the channel $Q^{\otimes n}$ may help us to increase the fidelity. Therefore, the capacity of the channel $Q' := Q^{\otimes 2}$ might be strictly larger than twice the capacity of Q . Because of this phenomenon of *super additivity*, it is very hard to compute the quantum channel capacity. In general, super additivity is one of the big puzzles of quantum information theory.

We close this section with a criterion for the question when perfect error correction is possible, i.e., when it is possible to attain fidelity one in (7.3) for finite n . A *quantum error-correcting code* (QECC) in this sense is a subspace $\mathcal{C}$ of the Hilbert space on which the channel acts such that restricted to that subspace the operator Q can be inverted.

Theorem 7.1 (QECC characterization [KL97]) *Let Q be a quantum channel on $\mathcal{H}$ with error operators $\{E_k: k \in \mathcal{I}_Q\}$. A subspace $\mathcal{C} \leq \mathcal{H}$ with orthonormal basis $\{|c_i\rangle: i \in \mathcal{I}_C\}$ is a quantum error-correcting code for Q if and only if the following conditions hold for arbitrary error operators E_k and E_ℓ and for arbitrary basis states $|c_i\rangle$ and $|c_j\rangle$:*

$$\langle c_i | E_k^\dagger E_\ell | c_j \rangle = 0 \quad (\text{for } i \neq j) \quad (7.4a)$$

$$\langle c_i | E_k^\dagger E_\ell | c_i \rangle = \langle c_j | E_k^\dagger E_\ell | c_j \rangle =: \alpha_{k\ell} \in \mathbb{C}. \quad (7.4b)$$

Denoting by $P_C := \sum_{i \in \mathcal{I}_C} |c_i\rangle\langle c_i|$ the projection onto the code $\mathcal{C}$, we obtain the following equivalent condition which is independent of the basis of the code:

$$\forall k, \ell \in \mathcal{I}_Q: P_C E_k^\dagger E_\ell P_C = \alpha_{k\ell} P_C.$$

From the proof of Theorem 7.1 given in [Gra02a, Gra02b] it is possible to derive an in-principle algorithm that allows the correction of errors. As in the classical case (cf. Section 1.3.4) we cannot expect to have an efficient algorithm for the general situation.

A common misinterpretation of the conditions (7.4) is that it was only possible to correct exactly those errors which are one of the error operators E_k , i.e., that only a finite number of errors could be corrected. However, the conditions (7.4) are linear in the error operators. To show this, we introduce the new error operators

$$A := \sum_k \lambda_k E_k \quad \text{and} \quad B := \sum_l \mu_l E_l$$

which are arbitrary linear combinations of the E_k . Using (7.4) we compute

$$\begin{aligned}\langle c_i | A^\dagger B | c_j \rangle &= \sum_{k,l} \overline{\lambda_k} \mu_l \langle c_i | E_k^\dagger E_l | c_j \rangle \\ &= \sum_{k,l} \overline{\lambda_k} \mu_l \delta_{i,j} \alpha_{k,l} \\ &= \delta_{i,j} \cdot \alpha'(A, B),\end{aligned}$$

where $\alpha'(A, B) \in \mathbb{C}$ is some constant depending on the operators A and B only. Hence conditions (7.4) guarantee that the effect of any error operator E that is in the linear span of the error operators $\mathcal{E}$ can be corrected. It also demonstrates that it is sufficient to check (7.4) for a vector space basis of $\mathcal{E}$ and hence for a finite set of errors. For qubit systems, the Pauli matrices

$$X \triangleq \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y \triangleq \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad Z \triangleq \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

together with identity form a vector space basis of all matrices in $\mathbb{C}^{2 \times 2}$. For a quantum code using n qubits, we consider the tensor product of Pauli matrices and identity as the so-called *error basis*. For an element of the error basis, the number of tensor factors different from identity is referred to as the *number of errors* or the *weight of an error*. This naturally generalizes to any error operator that can be written as a tensor product. The weight equals the number of subsystems on which the operator acts nontrivially.

7.3 Using Classical Error-Correcting Codes

7.3.1 Negative results: the quantum repetition code

At the end of the previous section we have seen that it is sufficient to be able to correct a finite number of different errors. Additionally, using error bases whose elements are tensor products, we have the notion of the weight of an error. This is very similar to the situation for classical error correction. In Section 1.3.1, pp. 9f, we have seen that the simplest way of protecting classical information against errors is to replicate the information several times. For quantum states, the encoding transformation for an m -fold quantum repetition code must implement the following map:

$$|\phi\rangle \mapsto \underbrace{|\phi\rangle|\phi\rangle \dots |\phi\rangle}_{m \text{ copies}}. \quad (7.5)$$

From the linearity of quantum mechanics it follows that there is no quantum transformation such that (7.5) holds for all input states $|\phi\rangle$ (cf. the “no-cloning theorem” [WZ82]).

If the input state $|\phi\rangle$ or an algorithm for its preparation is known, one can of course also prepare m independent copies of the state and send them through the quantum channel. However, at the receiver’s side, a quantum mechanical analogue of majority decision is required. Again, it is impossible to unambiguously decide if, e.g., two of three unknown quantum states

$|\phi_i\rangle$ are identical and then output a quantum state $|\phi_j\rangle$ that equals the majority of the states. While at the sender's side the no-cloning theorem could be circumvented, the direct quantum mechanical analogue of the repetition code fails at the receiver's side. An approach to avoid the no-go theorems for quantum repetition codes that is different from what we will see in the next section encodes quantum information in symmetric spaces [BBD⁺97].

7.3.2 Positive results: a simple three-qubit code

The direct application of a fundamental principle of classical error-correcting codes, namely the replication of information, essentially fails because quantum mechanics allows the coherent superposition of basis states. When restricted to basis states, the theory becomes completely classical, and error correction is possible.

So in order to implement mechanisms that allow the correction of errors, we turn our attention to the basis states and additionally require that all operations are linear, i.e., that everything works for superpositions as well. From the characterization of quantum error-correcting codes in Theorem 7.1 we have already learned that it suffices to deal with a finite set of errors. For qubit systems, these error operators are tensor products of Pauli matrices. The operator σ_x interchanges the basis states $|0\rangle$ and $|1\rangle$, hence it corresponds to a classical *bit-flip error*. Similarly, the operator σ_z changes the sign of the state $|1\rangle$, hence it is referred to as a *sign-flip error*. With respect to the Hadamard transformed basis $|+\rangle := |0\rangle + |1\rangle$ and $|-\rangle := |0\rangle - |1\rangle$, the rôle of σ_x and σ_z is interchanged, i.e., σ_z flips the basis states and σ_x changes the sign of the state $|-\rangle$. From the relations among the Pauli matrices it follows that σ_y is proportional to the product of σ_x and σ_z . Hence a σ_y error can be modeled as a combination of a bit-flip and a phase-flip error on the same qubit.

The first approach is to deal with the two basic types of errors, bit flip and phase flip, independently. If we want to correct for bit-flip errors only, we are almost in the situation of classical error-correcting codes. Therefore, we apply the principle of the repetition code to the basis states and obtain the following code, which can already be found in [Pere85]:

$$\begin{aligned} \mathcal{C}: \mathbb{C}^2 &\rightarrow (\mathbb{C}^2)^{\otimes 3} \\ |\uparrow\rangle &\mapsto |\uparrow\uparrow\uparrow\rangle \\ |\downarrow\rangle &\mapsto |\downarrow\downarrow\downarrow\rangle, \end{aligned} \tag{7.6}$$

By construction, the mapping (7.6) is linear, i.e., the superposition $\alpha|\uparrow\rangle + \beta|\downarrow\rangle$ is mapped to $\mathcal{C}(\alpha|\uparrow\rangle + \beta|\downarrow\rangle) = \alpha|\uparrow\uparrow\uparrow\rangle + \beta|\downarrow\downarrow\downarrow\rangle$. The states $|\uparrow\uparrow\uparrow\rangle$ and $|\downarrow\downarrow\downarrow\rangle$ span a two-dimensional subspace $\mathcal{C} < \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. Flipping the spin in one of the subsystems we obtain the following states:

error	state	subspace
no error	$\alpha \uparrow\uparrow\uparrow\rangle + \beta \downarrow\downarrow\downarrow\rangle$	$(I \otimes I \otimes I)\mathcal{C} =: \mathcal{C}_0$
1 st position	$\alpha \downarrow\uparrow\uparrow\rangle + \beta \uparrow\downarrow\downarrow\rangle$	$(X \otimes I \otimes I)\mathcal{C} =: \mathcal{C}_1$
2 nd position	$\alpha \uparrow\downarrow\uparrow\rangle + \beta \downarrow\uparrow\downarrow\rangle$	$(I \otimes X \otimes I)\mathcal{C} =: \mathcal{C}_2$
3 rd position	$\alpha \uparrow\uparrow\downarrow\rangle + \beta \downarrow\downarrow\uparrow\rangle$	$(I \otimes I \otimes X)\mathcal{C} =: \mathcal{C}_3$

(7.7)

The four different cases yield four mutually orthogonal subspaces, i.e., the Hilbert space of three qubits can be decomposed as follows:

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 = (I \otimes I \otimes I)\mathcal{C} \oplus (\sigma_x \otimes I \otimes I)\mathcal{C} \oplus (I \otimes \sigma_x \otimes I)\mathcal{C} \oplus (I \otimes I \otimes \sigma_x)\mathcal{C}.$$

By a projective measurement whose eigenspaces are the two-dimensional spaces $\mathcal{C}_i$ in (7.7) one obtains information about the error without disturbing the superposition within the corresponding two-dimensional subspace. However, a phase flip, say the error $\sigma_z \otimes I \otimes I$ acting on the first qubit, changes the coefficients α and β of the superposition, but the resulting state does not leave the subspace $\mathcal{C}$. Hence the measurement does not detect such an error and hence it cannot be corrected.

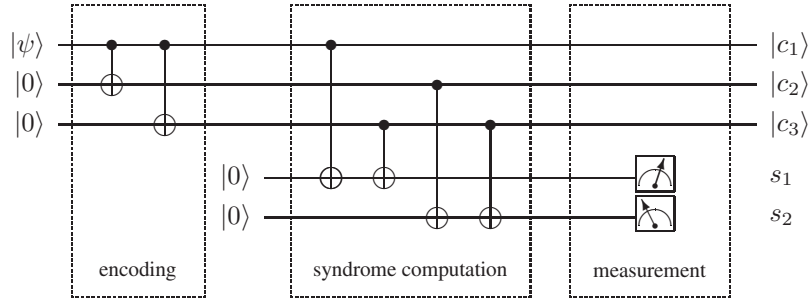


Figure 7.3. Quantum circuit for encoding one qubit, computing the error syndrome, and extracting two classical syndrome bits.

The projective measurement distinguishing the different errors can be implemented using an auxiliary quantum system. The basis states of the subspaces $\mathcal{C}_i$ are characterized by comparing the first and last as well as the second and the last qubit. Using the correspondence $|0\rangle \triangleq |\uparrow\rangle$ and $|1\rangle \triangleq |\downarrow\rangle$, comparing two qubits translates into computing the sum modulo 2 of the labels 0 and 1 of the basis states. A quantum circuit that implements the encoding (7.6) and the measurement is shown in Fig. 7.3. Measuring the two ancilla qubits one obtains two classical bits s_1 and s_2 which, like the error syndrome of a classical linear block code (see Proposition 1.3), provide information about the error. From this error syndrome, one has to deduce the most likely error and then correct it.

The quantum circuit shown in Fig. 7.4 integrates the error-correction step as well. Using multiply controlled quantum gates, the three different correction operators are applied depending on the state of the syndrome qubits $|s_1\rangle|s_2\rangle$. It can be shown that after the error-correction step, the syndrome qubits $|s_1\rangle|s_2\rangle$ are not entangled with the code qubits $|c_1\rangle|c_2\rangle|c_3\rangle$.

As already discussed above, the Hadamard transform interchanges the rôle of bit- and phase-flip errors. Therefore we can obtain a code that can correct a single phase-flip error by using essentially the same three-qubit code, but replacing the basis states $|000\rangle$ and $|111\rangle$ by $|+++ \rangle$ and $|--- \rangle$, respectively. Rewriting everything with respect to the computational basis $|0\rangle$ and $|1\rangle$, we obtain the following orthogonal decomposition of the state space shown in Table 7.1.

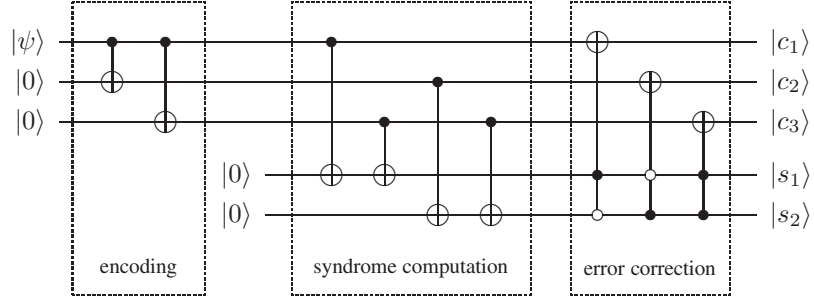


Figure 7.4. Quantum circuit for encoding one qubit, computing the error syndrome, and coherent error correction.

Table 7.1. Orthogonal decomposition corresponding to the three-qubit code correcting a single phase-flip error.

Phase flip	State	Subspace
No error	$\frac{\alpha}{2}(000\rangle + 011\rangle + 101\rangle + 110\rangle)$ $+ \frac{\beta}{2}(001\rangle + 010\rangle + 100\rangle + 111\rangle)$	$(I \otimes I \otimes I)\mathcal{H}_C$
1 st position	$\frac{\alpha}{2}(000\rangle + 011\rangle - 101\rangle - 110\rangle)$ $+ \frac{\beta}{2}(001\rangle + 010\rangle - 100\rangle - 111\rangle)$	$(Z \otimes I \otimes I)\mathcal{H}_C$
2 nd position	$\frac{\alpha}{2}(000\rangle - 011\rangle + 101\rangle - 110\rangle)$ $+ \frac{\beta}{2}(001\rangle - 010\rangle + 100\rangle - 111\rangle)$	$(I \otimes Z \otimes I)\mathcal{H}_C$
3 rd position	$\frac{\alpha}{2}(000\rangle - 011\rangle - 101\rangle + 110\rangle)$ $- \frac{\beta}{2}(001\rangle + 010\rangle + 100\rangle - 111\rangle)$	$(I \otimes I \otimes Z)\mathcal{H}_C$

7.3.3 Shor's nine-qubit code

The three-qubit code of the previous section corrects a single bit-flip error, and its Hadamard transformed version a single phase-flip error, but neither is able to correct both types of errors at the same time. A solution to this problem can be obtained by using two levels of error correction. On the first level, we use the three-qubit code (7.6) which protects against a single bit flip of any of the three qubits. So every *logical qubit* is represented by three *physical qubits*:

$$|\underline{0}\rangle \triangleq |000\rangle \quad \text{and} \quad |\underline{1}\rangle \triangleq |111\rangle. \quad (7.8)$$

A phase-flip error on any of the three physical qubits has the following effect:

$$\begin{aligned} Z \otimes I \otimes I |000\rangle &= |000\rangle & Z \otimes I \otimes I |111\rangle &= -|111\rangle \\ I \otimes Z \otimes I |000\rangle &= |000\rangle & I \otimes Z \otimes I |111\rangle &= -|111\rangle \\ I \otimes I \otimes Z |000\rangle &= |000\rangle & I \otimes I \otimes Z |111\rangle &= -|111\rangle \end{aligned} \quad (7.9)$$

In terms of the logical qubits, these operators act as an *encoded Z-operator*, i.e.,

$$\underline{Z}|0\rangle = |0\rangle \quad \text{and} \quad \underline{Z}|1\rangle = -|1\rangle,$$

where $\underline{Z}$ corresponds to any of the three-qubit operators in (7.9). For the second level of encoding, we use the three-qubit code

$$|0\rangle \mapsto |+\rangle|+\rangle|+\rangle \quad \text{and} \quad |1\rangle \mapsto |-\rangle|-\rangle|-\rangle, \quad (7.10)$$

correcting a single phase-flip error. For the states $|+\rangle$ and $|-\rangle$ in (7.10) we use the logical qubits of (7.8). This yields the following encoding [Sho95]:

$$\begin{aligned} |0\rangle \mapsto |+\rangle|+\rangle|+\rangle &= (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &= (|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \end{aligned} \quad (7.11a)$$

$$\begin{aligned} |1\rangle \mapsto |-\rangle|-\rangle|-\rangle &= (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \\ &= (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \end{aligned} \quad (7.11b)$$

This encodes one logical qubit using nine physical qubits. A single bit-flip error on the physical qubits can be corrected using the first level of encoding. So actually we can correct bit flips in any of the three groups of three physical qubits. A single phase-flip error on the physical qubits corresponds to an encoded sign-flip with respect to the first level of encoding which can be corrected using the second level of encoding. In summary, we can independently correct single bit-flip errors and single phase-flip errors. The combination of bit- and phase-flip errors corresponds to the Pauli matrix σ_y . Therefore, we can correct all single-qubit errors corresponding to the Pauli matrices. From the linearity of conditions (7.4), it follows that Shor's nine-qubit code (7.11) can correct an arbitrary error acting on any of the nine qubits.

There are even some errors of weight 2 that can be corrected. As bit-flip and phase-flip errors are corrected independently, they may act on different qubits. If there are two bit-flip errors acting on different blocks corresponding to the first level of encoding, e.g., the first and fifth qubit, they can be corrected, too. Two phase-flip errors acting on the same block have no effect at all, so there is no need to correct them. However, two phase-flip errors acting on different blocks have the same effect as a single phase-flip error and interchanging the encoded basis states. Hence the code only guarantees to be able to correct an arbitrary error of weight 1. In analogy to the notation used for linear block codes (cf. Section 1.3.3, p. 12), this code is denoted by $\mathcal{C} = \llbracket 9, 1, 3 \rrbracket$, or in general as $\mathcal{C} = \llbracket n, k, d \rrbracket$. Here k and n refer to the number of logical and physical qubits, respectively. The minimum distance d is not related to a distance in the usual sense on Hilbert or operator spaces, it rather has the following operational interpretation:

Definition 7.2 (quantum minimum distance) A quantum code $\mathcal{C}$ using n physical qubits has *minimum distance* d if there is no operator E that is a tensor product $E_1 \otimes \dots \otimes E_n$ with less

than d tensor factors E_i different from identity acting nontrivially on $\mathcal{C}$. This means that there are no linearly independent states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{C}$ such that $|\psi_2\rangle = E|\psi_1\rangle$.

For quantum codes, we get the analogue of Theorem 1.6 on p. 10:

Theorem 7.2 *Let $\mathcal{C}$ be a quantum code with minimum distance d . Then one can either detect any error that acts on strictly less than d positions or correct any error that acts on no more than $\lfloor (d-1)/2 \rfloor$ positions.*

7.3.4 Steane's seven-qubit code and CSS codes

The main idea underlying Shor's quantum error-correcting code is to use the concatenation of two codes, one being able to correct bit flips while the other code corrects phase flips. In order to obtain a more efficient QECC, i.e., a code for which the rate k/n or, equivalently, the fraction of logical qubits related to the physical qubits is larger, we have to find a code that is able to correct both types of errors using only a single layer of encoding. We have seen that quantum states which are basis states corresponding to codewords of classical binary codes, such as the triple-repetition code, are able to deal with bit-flip errors. Furthermore, the Hadamard transformation interchanges the rôle of bit and phase flips. The idea is now to use certain superpositions of states corresponding to a binary code, such that after a Hadamard transformation we are still able to correct bit-flip errors. For this, we make use of the following lemma:

Lemma 7.1 *Let $C \leq \mathbb{F}_2^n$ denote a k -dimensional linear subspace of $\mathbb{F}_2^n$ and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ two arbitrary binary vectors. Furthermore, by $H_{2^n} := H^{\otimes n}$ where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ we denote the Hadamard transformation on n qubits. Then the state*

$$|\psi\rangle := \frac{1}{\sqrt{|C|}} \sum_{\mathbf{c} \in C} (-1)^{\mathbf{a} \cdot \mathbf{c}} |\mathbf{c} + \mathbf{b}\rangle$$

is mapped by the Hadamard transformation to

$$H_{2^n} |\psi\rangle = \frac{(-1)^{\mathbf{a} \cdot \mathbf{b}}}{\sqrt{|C^\perp|}} \sum_{\mathbf{c} \in C^\perp} (-1)^{\mathbf{b} \cdot \mathbf{c}} |\mathbf{c} + \mathbf{a}\rangle.$$

Here $C^\perp$ denotes the dual code of C (see Proposition 1.4, p. 13).

Proof. The Hadamard transformation on n qubits can be written as

$$H_{2^n} = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n} (-1)^{\mathbf{x} \cdot \mathbf{y}} |\mathbf{x}\rangle \langle \mathbf{y}|,$$

where $\mathbf{x} \cdot \mathbf{y}$ denotes the inner product of the binary vectors $\mathbf{x}$ and $\mathbf{y}$.

Then

$$\begin{aligned}
H_{2^n}|\psi\rangle &= \frac{1}{\sqrt{2^n|C|}} \sum_{\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n} (-1)^{\mathbf{x} \cdot \mathbf{y}} |\mathbf{x}\rangle \langle \mathbf{y}| \sum_{\mathbf{c} \in C} (-1)^{\mathbf{a} \cdot \mathbf{c}} |\mathbf{c} + \mathbf{b}\rangle \\
&= \frac{1}{\sqrt{2^n|C|}} \sum_{\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n} \sum_{\mathbf{c} \in C} (-1)^{\mathbf{x} \cdot \mathbf{y} + \mathbf{a} \cdot \mathbf{c}} |\mathbf{x}\rangle \langle \mathbf{y}| |\mathbf{c} + \mathbf{b}\rangle \\
&= \frac{1}{\sqrt{2^n|C|}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} \sum_{\mathbf{c} \in C} (-1)^{\mathbf{x} \cdot (\mathbf{c} + \mathbf{b}) + \mathbf{a} \cdot \mathbf{c}} |\mathbf{x}\rangle \\
&= \frac{1}{\sqrt{2^n|C|}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{b} \cdot \mathbf{x}} |\mathbf{x}\rangle \sum_{\mathbf{c} \in C} (-1)^{(\mathbf{x} + \mathbf{a}) \cdot \mathbf{c}} \\
&\stackrel{(*)}{=} \frac{|C|}{\sqrt{2^n|C|}} \sum_{\mathbf{x} \in C^\perp + \mathbf{a}} (-1)^{\mathbf{b} \cdot \mathbf{x}} |\mathbf{x}\rangle \\
&= \frac{(-1)^{\mathbf{a} \cdot \mathbf{b}}}{\sqrt{|C^\perp|}} \sum_{\mathbf{d} \in C^\perp} (-1)^{\mathbf{b} \cdot \mathbf{d}} |\mathbf{d} + \mathbf{a}\rangle.
\end{aligned}$$

In $(*)$ we have used that the sum $\sum_{\mathbf{c} \in C} (-1)^{\mathbf{x} \cdot \mathbf{c}}$ vanishes iff $\mathbf{x} \neq C^\perp$. $\square$

Lemma 7.1 shows that the Hadamard transformation does not only change phase-flip errors into bit-flip errors, but also maps superpositions of all codewords of the linear binary code C to superpositions of all codewords of the dual code $C^\perp$ (cf. Proposition 1.4, p. 13). The $[7, 4, 3]$ Hamming code C of Example 1.4, p. 14 contains its dual code $C^\perp = [7, 3, 4]$, i.e., $C^\perp \subset C$. Hence we can partition the codewords of C into two cosets of $C^\perp$ as follows:

$$C = (C^\perp + \mathbf{x}_0) \dot{\cup} (C^\perp + \mathbf{x}_1) \quad \text{where } \mathbf{x}_0 = (0000000) \text{ and } \mathbf{x}_1 = (1111111).$$

Based on this decomposition, we define the following encoding:

$$|0\rangle \mapsto |\underline{0}\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{\mathbf{c} \in C^\perp} |\mathbf{c} + \mathbf{x}_0\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{\mathbf{c} \in C^\perp} |\mathbf{c}\rangle \quad (7.12a)$$

$$|1\rangle \mapsto |\underline{1}\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{\mathbf{c} \in C^\perp} |\mathbf{c} + \mathbf{x}_1\rangle. \quad (7.12b)$$

Hadamard transformation of these states yields

$$H_{2^7}|\underline{0}\rangle = \frac{1}{\sqrt{|C|}} \sum_{\mathbf{c} \in C} (-1)^{\mathbf{c} \cdot \mathbf{x}_1} |\mathbf{c}\rangle = \frac{1}{\sqrt{|C|}} \sum_{\mathbf{c} \in C} |\mathbf{c}\rangle \quad (7.13a)$$

$$H_{2^7}|\underline{1}\rangle = \frac{1}{\sqrt{|C|}} \sum_{\mathbf{c} \in C} (-1)^{\mathbf{c} \cdot \mathbf{x}_1} |\mathbf{c}\rangle. \quad (7.13b)$$

A superposition $|\psi\rangle = \alpha|\underline{0}\rangle + \beta|\underline{1}\rangle$ of the logical qubits is a superposition of words of the Hamming code $C = [7, 4, 3]$. This implies that a single bit-flip error can be corrected. From (7.13)

it can be seen that Hadamard transformation of the state $|\psi\rangle$ is again a superposition of words of the Hamming code, so a single phase-flip error can be corrected as well. Similar to Shor's nine-qubit code, for this seven-qubit code (7.12), bit flips and phase flips can be corrected independently. The generalization of this construction principle is now known as CSS codes and was independently derived by Calderbank and Shor [CS96] and Steane [Ste96a, Ste96b].

Theorem 7.3 (CSS code) *Let $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$ be linear binary codes of length n , dimension k_1 resp. k_2 and minimum distance d_1 resp. d_2 with $C_2^\perp \subseteq C_1$. Furthermore, let $\mathcal{W} = \{w_1, \dots, w_K\} \subset \mathbb{F}_2^n$ be a system of representatives of the cosets of $C_2^\perp$ in C_1 .*

The $K = 2^{k_1 - (n - k_2)}$ mutually orthogonal states

$$|\psi_i\rangle = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{c \in C_2^\perp} |c + w_i\rangle$$

span a quantum error-correcting code $\mathcal{C} = \llbracket n, k, d \rrbracket$ with $k := k_1 - (n - k_2)$. The code corrects at least $\lfloor (d_1 - 1)/2 \rfloor$ bit-flip errors and simultaneously at least $\lfloor (d_2 - 1)/2 \rfloor$ phase-flip errors. Its minimum distance is $d \geq \min\{d_1, d_2\}$.

7.3.5 The five-qubit code and stabilizer codes

By the CSS construction, the rate of a single-error-correcting code can be improved from $1/9$ for Shor's code to $1/7$. Instead of two layers of encoding, only a single layer is used, while the correction of bit-flip and phase-flip errors can still be done independently. As we will see next, integrating the error correction into a single step will result in a further improved rate.

The theory of CSS codes is closely connected to binary codes whose codewords are used as labels for the quantum states. Quantum error correction is basically reduced to the correction of bit-flip errors. This corresponds to a Schrödinger picture, i.e., the effect of the error operators on the quantum states is considered. Alternatively, we may develop a Heisenberg picture of quantum error correction (see also [Got99]).

For Shor's nine-qubit code, we have seen that there are nontrivial error operators which have no effect at all, e.g., two phase-flip errors acting on qubits within the same block. Also, flipping all bits in two blocks does not change the logical qubits $|\underline{0}\rangle$ and $|\underline{1}\rangle$. In general, we have some error operators E with

$$E|\psi\rangle = |\psi\rangle \quad \text{for all states } |\psi\rangle \in \mathcal{C}. \quad (7.14)$$

Hence the code $\mathcal{C}$ lies in the eigenspace of E with eigenvalue $+1$. We consider all operators E which are tensor products of Pauli matrices and identity, which generate to the so-called (n qubit) *Pauli group*. The elements of the Pauli group for which (7.14) holds form a subgroup, the *stabilizer group* $\mathcal{S}$ of an error-correcting code $\mathcal{C}$. For Shor's nine-qubit code (7.11), we

find the following set of error operators acting trivially on the logical qubits:

$$\begin{aligned}
g_1 &:= Z Z I I I I I I \\
g_2 &:= I Z Z I I I I I \\
g_3 &:= I I I Z Z I I I \\
g_4 &:= I I I I Z Z I I \\
g_5 &:= I I I I I Z Z I \\
g_6 &:= I I I I I I Z Z \\
g_7 &:= X X X X X X I I \\
g_8 &:= I I I X X X X X
\end{aligned} \tag{7.15}$$

where we have omitted the tensor product symbols. This set is minimal in the sense that none of the stabilizers g_i can be expressed as product of the others. Two elements of the Pauli group either commute or anticommute, i.e., $E_i E_j = \pm E_j E_i$. Together with (7.14) this implies that the stabilizer group is Abelian. Starting with an Abelian subgroup of the Pauli group, we get the following definition:

Definition 7.3 (stabilizer code) Let $\mathcal{S}$ be an Abelian subgroup of the n qubit Pauli group not containing $-I$. Then the *stabilizer code* $\mathcal{C}$ is the common eigenspace with eigenvalue $+1$ of all operators in $\mathcal{S}$.

The error-free states of the stabilizer code $\mathcal{C}$ are characterized as being an eigenstate of the stabilizers with eigenvalue $+1$. As the Pauli matrices are both unitary and Hermitian, we can interpret them as observables as well. Measuring the stabilizers (7.15), we obtain an error syndrome similar to that of classical block codes (cf. Proposition 1.3, p. 13). Here the measurements yield eight eigenvalues $(-1)^{s_i}$ which form a binary syndrome vector of length 8. A bit flip of the first qubit, i.e., the operator $e_1 = X I I I I I I I$, commutes with all but the first stabilizer g_1 . Therefore, a bit-flip error on the first position changes the first bit of the syndrome. A phase-flip error on the second position $e_2 = I Z I I I I I I$ commutes with all stabilizer apart from g_7 . Hence this error changes the entry s_7 of the syndrome. In total, we have $7 \cdot 3$ different single-qubit errors. For the error syndrome respectively the sign of the eigenvalues measured we have $2^8 = 256$ different possibilities. This indicates that, as in the classical case (cf. Table 1.2, p. 15), the code can correct more errors than what is guaranteed by its minimum distance.

For the nine-qubit code, we are measuring the eight independent commuting observables (7.15). This yields an orthogonal decomposition of the space of nine qubits into 2^8 two-dimensional spaces. Similar to (7.7) and Table 7.1, the coefficients of a superposition of logical qubits are preserved within those spaces. So measuring the stabilizers provides information about the eigenspace and thereby about the error, but does not provide any information about the logical quantum state.

Using this type of construction which is due to Gottesman [Got96] and Calderbank et al. [CRSS98], one gets the most efficient quantum error-correcting code with one logical qubit correcting one error. The stabilizer for such a five-qubit code $\mathcal{C} = \llbracket 5, 1, 3 \rrbracket$ is generated by

$$\begin{aligned}
g_1 &:= X X Z I Z \\
g_2 &:= Z X X Z I \\
g_3 &:= I Z X X Z \\
g_4 &:= Z I Z X X.
\end{aligned} \tag{7.16}$$

Measuring the stabilizers (7.16) yields four syndrome bits. The $2^4 = 16$ different possible syndromes match the total number of possible errors, namely the $5 \cdot 3$ different one-qubit errors and the no-error event.

Similarly as the CSS construction is using classical linear binary codes, the theory of stabilizer codes can be linked to block codes over the field $GF(4)$ with four elements [CRSS98] (for more details, see also [BG98]).

7.4 Further Aspects

In this introduction to quantum error-correcting codes, we have neglected almost all algorithmic aspects, such as quantum circuits for encoding and decoding. For CSS codes, one can derive efficient quantum circuits for encoding and syndrome computation consisting of CNOT and Hadamard gates only [Gra02b, Gra02a]. Quantum circuits for encoding stabilizer codes can be realized with polynomially many elementary gates as well, and the algorithm to construct them has polynomial complexity, too. Two alternative versions can be found in [CG97] and [GRB03]. Both naturally extend to quantum error-correcting codes for quantum systems whose subsystems are not qubits, but have a higher dimension. The theory of such codes is presented in [AK01]. Some aspects of finding codes with both high rate and high minimum distance are discussed in [GBR04].

The question of decoding, including the correction of errors, is a bit more complicated. Both the CSS construction and stabilizer codes reduce the problem of quantum error correction to the problem of the correction of errors for a classical code. This step, namely the computation of an error syndrome, can be solved by techniques similar to those used for the encoding circuits. The remaining task is to determine the most likely error given the syndrome. From the theory of classical error-correcting codes we have some classes of codes for which this problem can be efficiently solved at least for a subset of all correctable errors. Among these codes, the cyclic codes are particularly interesting [GB00].

Another aspect that has been ignored in this introduction is the dynamics on quantum codes. The ultimate goal is to process quantum information. In the discussion of Shor's nine-qubit code we have already seen that there are also encoded operators which preserve the code space, but act nontrivially on it. It has been shown that one can implement a universal set of encoded quantum gates in such a way that failures of a small number of gates can be corrected either in a later error-correction step, or more importantly, using concatenated codes. This eventually allows us to prove the so-called threshold theorem which implies that one can perform arbitrarily long quantum computations with bounded residual error and reasonable overhead for error correction provided that each individual gate has a failure probability below some threshold (see e.g. [KLZ98]). Unfortunately, the gap between what can be achieved in the labs and what is demanded by the theory is still large.

References

- [AK01] A. Ashikhmi and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inf. Theory*, 47(7):3065–3072, 2001 (*Preprint quant-ph/0005008*).
- [CG97] R. Cleve and D. Gottesman. Efficient computations of encodings for quantum error correction. *Phys. Rev. A*, 56(1):76–82, 1997.
- [BBD⁺97] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM J. Comput.*, 26(5):1541–1557, 1997.
- [BG98] T. Beth and M. Grassl. The quantum Hamming and hexacodes. *Fortschritte Phys.*, 46(4-5):459–491, 1998.
- [CRSS98] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory*, 44(4):1369–1387, 1998 (*Preprint quant-ph/9608006*).
- [CS96] A. Robert Calderbank, and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098–1105, 1996 (*Preprint quant-ph/9512032*).
- [GB00] M. Grassl and T. Beth. Cyclic quantum error-correcting codes and quantum shift registers. *Proc. R. Soc. Lond. A*, 456(2003):2689–2706, 8, 2000 (*Preprint quant-ph/9910061*).
- [GBR04] M. Grassl, T. Beth, and M. Rötteler. On Optimal Quantum Codes. *Int. J. Quantum Inf.*, 2(1):55–64, 2004 (*Preprint quant-ph/0312164*).
- [Got96] D. Gottesman. A class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54(3):1862–1868, 1996 (*Preprint quant-ph/9604038*).
- [Got99] D. Gottesman. The Heisenberg representation of quantum computers. In S. P. Corney, R. Delbourgo, and P. D. Jarvis, *Proc. 22nd Int. Colloquium on Group Theoretical Methods in Physics*, pp. 32–43, International Press, Cambridge, MA, 1999 (*Preprint quant-ph/9807006*).
- [Gra02a] M. Grassl. Algorithmic aspects of quantum error-correcting codes. In R. K. Brylinski and G. Chen, editors (*Mathematics of Quantum Computation*), pp. 223–252, CRC Press, Boca Raton FL, 2002.
- [Gra02b] M. Grassl. *Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen*. Shaker, Aachen, 2002. Zugl.: Universität Karlsruhe, Dissertation, 2001.
- [GRB03] M. Grassl, M. Rötteler, and T. Beth. Efficient quantum circuits for non-qubit quantum error-correcting codes. *Int. J. Found. Comput. Sci.*, 14(5):757–775, 2003 (*Preprint quant-ph/0211014*).
- [KL97] E. Knill and R. Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900–911, 1997 (*Preprint quant-ph/9604034*).
- [KLZ98] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation: error models and thresholds. *Proc. R. Soc. Lond. A*, 454(1969):365–384, 1998 (*Preprint quant-ph/9702058*).
- [Kra83] K. Kraus. *States, Effects, and Operations* (volume 190 of *Lecture Notes in Physics*), Springer, Berlin, 1983.

- [Pere85] A. Peres. Reversible logic and quantum computers. *Phys. Rev. A*, 32(6):3266–3276, 1985.
- [Schu96] B Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54(4):2614–2628, 1996.
- [Sho95] P W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4):R2493–R2496, 1995.
- [Ste96a] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77(5):793–797, 29, 1996.
- [Ste96b] A M. Steane. Simple quantum error correcting codes. *Phys. Rev. A*, 54(6):4741–4751, 1996 (*Preprint* quant-ph/9605021).
- [WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 28, 1982.

Part III

Theory of Entanglement

8 The Separability versus Entanglement Problem

Aditi Sen(De), Ujjwal Sen, Maciej Lewenstein, and Anna Sanpera

8.1 Introduction

Quantum theory, formalized in the first few decades of the 20th century, contains elements that are radically different from the classical description of Nature. An important aspect in these fundamental differences is the existence of quantum correlations in the quantum formalism. In the classical description of Nature, if a system is formed by different subsystems, complete knowledge of the whole system implies that the sum of the information of the subsystems makes up the complete information for the whole system. This is no longer true in the quantum formalism. In the quantum world, there exist states of composite systems for which we might have the complete information, while our knowledge about the subsystems might be completely random. One may reach some paradoxical conclusions if one applies a classical description to states which have characteristic quantum signatures.

During the last decade, it was realized that these fundamentally nonclassical states, also denoted as “entangled states,” can provide us with something else than just paradoxes. They may be *used* to perform tasks that cannot be achieved with classical states. As benchmarks of this turning point in our view of such nonclassical states, one might mention the spectacular discoveries of (entanglement-based) quantum cryptography (1991) [1], quantum dense coding (1992) [2], and quantum teleportation (1993) [3].

In this chapter, we will focus on bipartite composite systems. We will define formally what entangled states are, present some important criteria to discriminate entangled states from separable ones, and show how they can be classified according to their capability to perform some precisely defined tasks. Our knowledge in the subject of entanglement is still far from complete, although significant progress has been made in the recent years and very active research is currently underway.

8.2 Bipartite Pure States: Schmidt Decomposition

In this chapter, we will primarily consider bipartite systems, which are traditionally supposed to be in possession of Alice (A) and Bob (B), who can be located in distant regions. Let Alice’s physical system be described by the Hilbert space $\mathcal{H}_A$ and that of Bob by $\mathcal{H}_B$. Then the joint physical system of Alice and Bob is described by the tensor product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

Theorem 8.1 (Product and entangled pure states) *A pure state, i.e., a projector $|\psi_{AB}\rangle\langle\psi_{AB}|$ on a vector $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, is a product state if the states of local subsystems are also pure states, that is, if $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$. However, there are states that cannot be written in this form. These states are called entangled states.*

An example of entangled state is the well-known singlet state $(|01\rangle - |10\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ are two orthonormal states. Operationally, product states correspond to those states that can be locally prepared by Alice and Bob at two separate locations. Entangled states can, however, be prepared only after the particles of Alice and Bob have interacted either directly or by means of an ancillary system. A very useful representation, only valid for pure bipartite states, is the, so-called, Schmidt representation:

Definition 8.1 (Schmidt decomposition) Every $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be represented in an appropriately chosen basis as

$$|\psi_{AB}\rangle = \sum_{i=1}^M a_i |e_i\rangle \otimes |f_i\rangle,$$

where $|e_i\rangle$ ($|f_i\rangle$) form a part of an orthonormal basis in $\mathcal{H}_A$ ($\mathcal{H}_B$), $a_i > 0$, and $\sum_{i=1}^M a_i^2 = 1$, where $M \leq \dim \mathcal{H}_A, \dim \mathcal{H}_B$.

The positive numbers a_i are known as the Schmidt coefficients of $|\psi_{AB}\rangle$. Note that product pure states correspond to those states whose Schmidt decomposition has one and only one Schmidt coefficient. If the decomposition has more than one Schmidt coefficient, the state is entangled. Note that the squares of the Schmidt coefficients of a pure bipartite state $|\psi_{AB}\rangle$ are the eigenvalues of either of the reduced density matrices $\rho_A (= \text{tr}_B \rho_{AB})$ and $\rho_B (= \text{tr}_A \rho_{AB})$ of $|\psi_{AB}\rangle$.

8.3 Bipartite Mixed States: Separable and Entangled States

As discussed in the last section, the question whether a given pure bipartite state is separable or entangled is straightforward. One has just to check if the reduced density matrices are pure. This condition is equivalent to the fact that a bipartite pure state has a single Schmidt coefficient. The determination of separability for mixed states is much harder, and currently lacks a complete answer, even in composite systems of dimension as low as $\mathcal{C}^2 \otimes \mathcal{C}^4$.

To reach a formal definition of separable and entangled states, consider the following preparation procedure of a bipartite state between Alice and Bob. Suppose that Alice prepares her physical system in the state $|e_i\rangle$ and Bob prepares his physical system in the state $|f_i\rangle$. Then, the combined state of their joint physical system is given by

$$|e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i|.$$

We now assume that they can communicate over a classical channel (a phone line, for example). Then, whenever Alice prepares the state $|e_i\rangle$ ($i = 1, 2, \dots, K$), which she does with

probability p_i , she communicates that to Bob, and correspondingly Bob prepares his system in the state $|f_i\rangle$ ($i = 1, 2, \dots, K$). Of course, $\sum_i p_i = 1$. The state that they prepare is then

$$\rho_{AB} = \sum_{i=1}^K p_i |e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i|. \quad (8.1)$$

The important point to note here is that the state displayed in Eq. (8.1) is the most general state that Alice and Bob will be able to prepare by local quantum operations and classical communication (LOCC) [4].

Definition 8.2 (Separable and entangled mixed states) A mixed state ρ_{AB} is *separable* if and only if it can be represented as a convex combination of the product of projectors on local states as stated in Eq. (8.1). Otherwise, the mixed state is said to be *entangled*.

Entangled states, therefore, cannot be prepared locally by two parties even after communicating over a classical channel. To prepare such states, the physical systems must be brought together to interact¹. Mathematically, a nonlocal unitary operator² must *necessarily* act on the physical system described by $\mathcal{H}_A \otimes \mathcal{H}_B$ to produce an entangled state from an initial separable state.

The question whether a given bipartite state is separable or not turns out to be quite complicated. Among the difficulties, we note that for an arbitrary state ρ_{AB} , there is no stringent bound on the value of K in Eq. (8.1), which is only limited by the Caratheodory theorem to be $K \leq (\dim \mathcal{H})^2$ with $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ (see [6]). Although the general answer to the separability problem still eludes us, there has been significant progress in recent years, and we will review some such directions in the following sections.

8.4 Operational Entanglement Criteria

In this section, we will introduce some operational entanglement criteria. In particular, we will discuss the partial transposition criterion [7, 8], and the majorization criterion [9]. There exist several other criteria (see e.g., [10–12]), which will not be discussed here. However note that, up to now, a necessary and sufficient criterion for detecting entanglement of an arbitrary given mixed state is still lacking.

8.4.1 Partial transposition

Definition 8.3 Let ρ_{AB} be a bipartite density matrix, and let us express it as

$$\rho_{AB} = \sum_{i,j=1}^{N_A} \sum_{\mu,\nu=1}^{N_B} a_{ij}^{\mu\nu} (|i\rangle\langle j|)_A \otimes (|\mu\rangle\langle\nu|)_B,$$

¹Due to the existence of the phenomenon of entanglement swapping [5], one must suitably enlarge the notion of preparation of entangled states. So, an entangled state between two particles can be prepared if and only if, either the two particles (call them A and B) themselves come together to interact at a time in the past, or two *other* particles (call them C and D) do the same, with C (D) having interacted beforehand with A (B).

²A unitary operator on $\mathcal{H}_A \otimes \mathcal{H}_B$, is said to be “nonlocal,” if it is not of the form $U_A \otimes U_B$, with U_A (U_B) being a unitary operator acting on $\mathcal{H}_A$ ($\mathcal{H}_B$).

where $\{|i\rangle\}$ ($i = 1, 2, \dots, N_A; N_A \leq \dim \mathcal{H}_A$) ($\{|\mu\rangle\}$ ($\mu = 1, 2, \dots, N_B; N_B \leq \dim \mathcal{H}_B$)) is a set of orthonormal vectors in $\mathcal{H}_A$ ($\mathcal{H}_B$). The partial transposition, $\rho_{AB}^{T_A}$, of ρ_{AB} with respect to subsystem A is defined as

$$\rho_{AB}^{T_A} = \sum_{i,j=1}^{N_A} \sum_{\mu,\nu=1}^{N_B} a_{ij}^{\mu\nu} (|j\rangle\langle i|)_A \otimes (|\mu\rangle\langle\nu|)_B.$$

A similar definition exists for the partial transposition of ρ_{AB} with respect to Bob's subsystem. Note that $\rho_{AB}^{T_B} = (\rho_{AB}^{T_A})^T$. Although the partial transposition depends upon the choice of the basis in which ρ_{AB} is written, its eigenvalues are basis independent. We say that a state has positive partial transposition (PPT), whenever $\rho_{AB}^{T_A} \geq 0$, i.e., the eigenvalues of $\rho_{AB}^{T_A}$ are nonnegative. Otherwise, the state is said to be nonpositive under partial transposition (NPT). Note here that transposition is equivalent to time reversal.

Theorem 8.2 ([7]) *If a state ρ_{AB} is separable, then $\rho_{AB}^{T_A} \geq 0$ and $\rho_{AB}^{T_B} = (\rho_{AB}^{T_A})^T \geq 0$.*

Proof. Since ρ_{AB} is separable, it can be written as

$$\rho_{AB} = \sum_{i=1}^K p_i |e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i| \geq 0.$$

Now performing the partial transposition w.r.t. A , we have

$$\begin{aligned} \rho_{AB}^{T_A} &= \sum_{i=1}^K p_i (|e_i\rangle\langle e_i|)^{T_A} \otimes |f_i\rangle\langle f_i| \\ &= \sum_{i=1}^K p_i |e_i^*\rangle\langle e_i^*| \otimes |f_i\rangle\langle f_i| \geq 0. \end{aligned}$$

Note that in the second line, we have used the fact that $A^\dagger = (A^*)^T$. □

The *partial transposition criterion* for detecting entanglement is simple: Given a bipartite state ρ_{AB} , find the eigenvalues of any of its partial transpositions. A negative eigenvalue immediately implies that the state is entangled. Examples of states for which the partial transposition has negative eigenvalues include the singlet state.

The partial transposition criterion allows us to detect in a straightforward manner all entangled states that are NPT states. This is a huge class of states. However, it turns out that there exist PPT states which are not separable, as pointed out in [13] (see also [14]). Moreover, the set of PPT entangled states is not a set of measure zero [15]. It is, therefore, important to have further independent criteria of entanglement detection which permits us to detect entangled PPT states. It is worth mentioning that PPT states which are entangled form the only known examples of the “bound entangled states” (see Refs. [14, 16] for details). Note also that both separable and PPT states form convex sets.

Theorem 8.2 is a necessary condition of separability in any arbitrary dimension. However, for some special cases, the partial transposition criterion is both a necessary and sufficient condition for separability:

Theorem 8.3 ([8]) *In $\mathcal{C}^2 \otimes \mathcal{C}^2$ or $\mathcal{C}^2 \otimes \mathcal{C}^3$, a state ρ is separable if and only if $\rho^{T_A} \geq 0$.*

8.4.2 Majorization

The partial transposition criterion, although powerful, is not able to detect entanglement in a finite volume of states. It is, therefore, interesting to discuss other independent criteria. The majorization criterion, to be discussed in this subsection, has been recently shown to be *not* more powerful in detecting entanglement. We choose to discuss it here mainly because it has independent roots. Moreover, it reveals a very interesting thermodynamical property of entanglement.

Before presenting the criterion, we must first give the definition of majorization [17].

Definition 8.4 Let $x = (x_1, x_2, \dots, x_d)$, and $y = (y_1, y_2, \dots, y_d)$ be two probability distributions, arranged in decreasing order, i.e., $x_1 \geq x_2 \geq \dots \geq x_d$ and $y_1 \geq y_2 \geq \dots \geq y_d$. Then we define x *majorized* by y , denoted as $x \prec y$, as

$$\sum_{i=1}^l x_i \leq \sum_{i=1}^l y_i,$$

where $l = 1, 2, \dots, d-1$, and equality holds when $l = d$.

Theorem 8.4 ([9]) *If a state ρ_{AB} is separable, then*

$$\lambda(\rho_{AB}) \prec \lambda(\rho_A), \quad \text{and} \quad \lambda(\rho_{AB}) \prec \lambda(\rho_B), \quad (8.2)$$

where $\lambda(\rho_{AB})$ is the set of eigenvalues of ρ_{AB} , and $\lambda(\rho_A)$ and $\lambda(\rho_B)$ are the sets of eigenvalues of the corresponding reduced density matrix of the state ρ_{AB} , and where all the sets are arranged in decreasing order.

The majorization criterion: Given a bipartite state, it is entangled if Eq. (8.2) is violated. However, it was recently shown in [18] that a state that is not detected by the positive partial transposition criterion will not be detected by the majorization criterion also. Nevertheless, the criterion has other important implications. We will now discuss one such.

Let us reiterate an interesting fact about the singlet state: The global state is pure, while the local states are completely mixed. In particular, this implies that the von Neumann entropy³ of the global state is lower than either of the von Neumann entropies of the local states. The von Neumann entropy can however be used to quantify disorder in a quantum state. This implies that there exist bipartite quantum states for which the global disorder can be more than either of the local disorders. This is a nonclassical fact as for two classical random variables, the Shannon entropy⁴ of the joint distribution cannot be smaller than that of either. In [19], it was shown that a similar fact is true for separable states:

Theorem 8.5 *If a state ρ_{AB} is separable,*

$$S(\rho_{AB}) \geq S(\rho_A), \quad \text{and} \quad S(\rho_{AB}) \geq S(\rho_B). \quad (8.3)$$

Although the von Neumann entropy is an important notion for quantifying disorder, the theory of majorization is a more stringent quantifier [17]: For two probability distributions x

³The von Neumann entropy of a state ρ is $S(\rho) = -\text{tr } \rho \log_2 \rho$.

⁴The Shannon entropy of a random variable X , taking up values X_i , with probabilities p_i , is given by $H(X) = H(\{p_i\}) = -\sum_i p_i \log_2 p_i$.

and $y, x \prec y$ if and only if $x = Dy$, where D is a doubly stochastic matrix⁵. Moreover, $x \prec y$ implies that $H(\{x_i\}) \geq H(\{y_i\})$. Quantum mechanics therefore allows the existence of states for which global disorder is greater than local disorder even in the sense of majorization.

A density matrix that satisfies Eq. (8.2) automatically satisfies Eq. (8.3). In this sense, Theorem 8.4 is a generalization of Theorem 8.5.

8.5 Nonoperational Entanglement Criteria

In this section, we will discuss two further entanglement criteria. We will show how the Hahn–Banach theorem can be used to obtain “entanglement witnesses.” We will also introduce the notion of positive maps, and present the entanglement criterion based on it. Both the criteria are “nonoperational,” in the sense that they are not state independent. Nevertheless, they provide important insight into the structure of the set of entangled states. Moreover, the concept of entanglement witnesses can be used to detect entanglement experimentally, by performing only a few *local* measurements, assuming some prior knowledge of the density matrix [20, 21].

Technical Preface

The following lemma and observation will be useful for later purposes.

Lemma 8.1

$$\text{tr}(\rho_{AB}^{T_A} \sigma_{AB}) = \text{tr}(\rho_{AB} \sigma_{AB}^{T_A}).$$

Observation:

The space of linear operators acting on $\mathcal{H}$ (denoted by $\mathcal{B}(\mathcal{H})$) is itself a Hilbert space, with the (Euclidean) scalar product

$$\langle A | B \rangle = \text{tr}(A^\dagger B) \quad A, B \in \mathcal{B}(\mathcal{H}).$$

This scalar product is equivalent to writing A and B row-wise as vectors, and scalar multiplying them:

$$\text{tr}(A^\dagger B) = \sum_{ij} A_{ij}^* B_{ij} = \sum_{k=1}^{(\dim \mathcal{H})^2} a_k^* b_k.$$

8.5.1 Entanglement witnesses

Entanglement witness from the Hahn–Banach theorem

Central to the concept of entanglement witnesses is the Hahn–Banach theorem, which we will present here limited to our situation and without proof (see e.g., [22] for a proof of the more general theorem):

⁵A matrix $D = (D_{ij})$ is said to be doubly stochastic, if $D_{ij} \geq 0$, and $\sum_i D_{ij} = \sum_j D_{ij} = 1$.

Theorem 8.6 Let S be a convex compact set in a finite-dimensional Banach space. Let ρ be a point in the space with $\rho \notin S$. Then there exists a hyperplane⁶ that separates ρ from S .

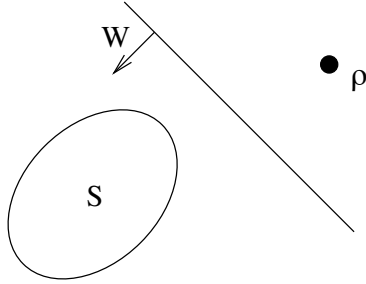


Figure 8.1. Schematic picture of the Hahn–Banach theorem. The (unique) unit vector orthonormal to the hyperplane can be used to define *right* and *left* in respect to the hyperplane by using the signum of the scalar product.

The statement of the theorem is illustrated in Fig. 8.1. The figure motivates the introduction of a new coordinate system located within the hyperplane (supplemented by an orthogonal vector W which is chosen such that it points away from S). Using this coordinate system, every state ρ can be characterized by its distance from the plane, by projecting ρ onto the chosen orthonormal vector and using the trace as scalar product, i.e., $\text{tr}(W\rho)$. This measure is either positive, zero, or negative. We now suppose that S is the convex compact set of all separable states. According to our choice of basis in Fig. 8.1, every separable state has a positive distance while there are some entangled states with a negative distance. More formally this can be phrased as

Definition 8.5 A Hermitian operator (an observable) W is called an *entanglement witness* (EW) if and only if

$$\exists \rho \text{ such that } \text{tr}(W\rho) < 0, \quad \text{while } \forall \sigma \in S, \quad \text{tr}(W\sigma) \geq 0.$$

Definition 8.6 An EW is *decomposable* if and only if there exist operators P, Q with

$$W = P + Q^{TA}, \quad P, Q \geq 0.$$

Lemma 8.2 *Decomposable EW cannot detect PPT entangled states.*

Proof. Let δ be a PPT entangled state and W be a decomposable EW. Then

$$\text{tr}(W\delta) = \text{tr}(P\delta) + \text{tr}(Q^{TA}\delta) = \text{tr}(P\delta) + \text{tr}(Q\delta^{TA}) \geq 0.$$

Here we used Lemma 8.1. □

Definition 8.7 An EW is called *nondecomposable entanglement witness* (nd-EW) if and only if there exists at least one PPT entangled state which is detected by the witness.

⁶A hyperplane is a linear subspace with dimension one less than the dimension of the space itself.

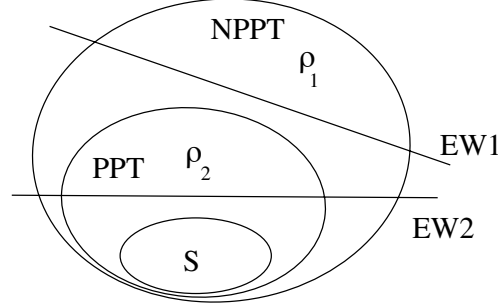


Figure 8.2. Schematic view of the Hilbert space with two states ρ_1 and ρ_2 and two witnesses EW1 and EW2. EW1 is a decomposable EW, and it detects only NPT states like ρ_1 . EW2 is an nd-EW, and it detects also some PPT states like ρ_2 . Note that neither witness detects *all* entangled states.

Using these definitions, we can restate the consequences of the Hahn–Banach theorem in several ways:

Theorem 8.7 ([8, 23–25])

1. ρ is entangled if and only if $\exists$ a witness W , such that $\text{tr}(\rho W) < 0$.
2. ρ is a PPT entangled state if and only if $\exists$ a nd-EW, W , such that $\text{tr}(\rho W) < 0$.
3. σ is separable if and only if $\forall$ EW, $\text{tr}(W\sigma) \geq 0$.

From a theoretical point of view, the theorem is quite powerful. However, it does not give any insight of how to construct for a given state ρ , the appropriate witness operator.

Examples:

For a decomposable witness

$$\begin{aligned} W' &= P + Q^{TA}, \\ \text{tr}(W'\sigma) &\geq 0, \end{aligned} \tag{8.4}$$

for all separable states σ .

Proof. If σ is separable, then it can be written as a convex sum of product vectors. So if Eq. (8.4) holds for any product vector $|e, f\rangle$, any separable state will also satisfy the same.

$$\begin{aligned} \text{tr}(W'|e, f\rangle\langle e, f|) &= \langle e, f|W'|e, f\rangle \\ &= \underbrace{\langle e, f|P|e, f\rangle}_{\geq 0} + \underbrace{\langle e, f|Q^{TA}|e, f\rangle}_{\geq 0}, \end{aligned}$$

because

$$\langle e, f|Q^{TA}|e, f\rangle = \text{tr}(Q^{TA}|e, f\rangle\langle e, f|) = \text{tr}(Q|e^*, f\rangle\langle e^*, f|) \geq 0.$$

Here we used Lemma 8.1, and $P, Q \geq 0$. □

This argumentation shows that $W = Q^{T_A}$ is also a suitable witness. Let us consider the simplest case of $\mathcal{C}^2 \otimes \mathcal{C}^2$. We can use

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

to write the density matrix

$$Q = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}. \quad \text{Then} \quad Q^{T_A} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

One can quickly verify that indeed $W = Q^{T_A}$ fulfills the witness requirements. Using

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

we can rewrite the witness:

$$W = Q^{T_A} = \frac{1}{2}(I - 2|\psi^-\rangle\langle\psi^-|).$$

This witness now detects $|\psi^-\rangle$:

$$\text{tr}(W|\psi^-\rangle\langle\psi^-|) = -\frac{1}{2}.$$

8.5.2 Positive maps

Introduction and definitions

So far we have only considered states belonging to a Hilbert space $\mathcal{H}$, and operators acting on the Hilbert space. However, the space of operators $\mathcal{B}(\mathcal{H})$ also has a Hilbert space structure. We now look at transformations of operators, the so-called maps which can be regarded as *superoperators*. As we will see, this will lead us to an important characterization of entangled and separable states. We start by defining linear maps:

Definition 8.8 A linear, self-adjoint map ϵ is a transformation

$$\epsilon : \mathcal{B}(\mathcal{H}_B) \rightarrow \mathcal{B}(\mathcal{H}_C),$$

which

- is linear, i.e.,

$$\epsilon(\alpha O_1 + \beta O_2) = \alpha \epsilon(O_1) + \beta \epsilon(O_2) \quad \forall O_1, O_2 \in \mathcal{B}(\mathcal{H}_B),$$

where α, β are complex numbers,

- and maps Hermitian operators onto Hermitian operators, i.e.,

$$\epsilon(O^\dagger) = (\epsilon(O))^\dagger \quad \forall O \in \mathcal{B}(\mathcal{H}_B).$$

For brevity, we will only write “linear map,” instead of “linear self-adjoint map.” The following definitions help us to further characterize linear maps.

Definition 8.9 A linear map ϵ is called *trace preserving* if

$$\text{tr}(\epsilon(O)) = \text{tr}(O) \quad \forall O \in \mathcal{B}(\mathcal{H}_B).$$

Definition 8.10 (positive map) A linear, self-adjoint map ϵ is called *positive* if

$$\forall \rho \in \mathcal{B}(\mathcal{H}_B), \quad \rho \geq 0 \quad \Rightarrow \quad \epsilon(\rho) \geq 0.$$

Positive maps have, therefore, the property of mapping positive operators onto positive operators. It turns out that by considering maps that are a tensor product of a positive operator acting on subsystem A, and the identity acting on subsystem B, one can learn about the properties of the composite system.

Definition 8.11 (completely positive map) A positive linear map ϵ is *completely positive* if for any tensor extension of the form

$$\epsilon' = \mathcal{I}_A \otimes \epsilon,$$

where

$$\epsilon' : \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B) \rightarrow \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_C),$$

ϵ' is positive. Here $\mathcal{I}_A$ is the identity map on $\mathcal{B}(\mathcal{H}_A)$.

Example: Hamiltonian evolution of a quantum system. Let $O \in \mathcal{B}(\mathcal{H}_B)$ and U a unitary matrix and let us define ϵ by

$$\begin{aligned} \epsilon : \mathcal{B}(\mathcal{H}_A) &\rightarrow \mathcal{B}(\mathcal{H}_A) \\ \epsilon(O) &= UOU^\dagger. \end{aligned}$$

As an example for this map, consider the time evolution of a density matrix. It can be written as $\rho(t) = U(t)\rho(0)U^\dagger(t)$, i.e., in the form given above. Clearly this map is linear, self-adjoint, positive, and trace preserving. It is also completely positive, because for $0 \leq w \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_A)$,

$$(\mathcal{I}_A \otimes \epsilon)w = (I_A \otimes U)w(I_A \otimes U^\dagger) = \tilde{U}w\tilde{U}^\dagger,$$

where $\tilde{U}$ is unitary. But then $\langle \psi | \tilde{U}w\tilde{U}^\dagger | \psi \rangle \geq 0$, if and only if $\langle \psi | w | \psi \rangle \geq 0$ (since positivity is not changed by unitary evolution).

Example: Transposition. An example of a positive but not completely positive map is the transposition T defined as

$$\begin{aligned} T : \mathcal{B}(\mathcal{H}_B) &\rightarrow \mathcal{B}(\mathcal{H}_B) \\ T(\rho) &= \rho^T. \end{aligned}$$

Of course this map is positive, but it is not completely positive, because

$$(\mathcal{I}_A \otimes T)w = w^{T_B},$$

and we know that there exist states for which $\rho \geq 0$, but $\rho^{T_B} \not\geq 0$.

Definition 8.12 A positive map is called *decomposable* if and only if it can be written as

$$\epsilon = \epsilon_1 + \epsilon_2 T,$$

where ϵ_1, ϵ_2 are completely positive maps and T is the operation of transposition.

Positive maps and entangled states

Partial transposition can be regarded as a particular case of a map that is positive but not completely positive. We have already seen that this particular positive but not completely positive map gives us a way to discriminate entangled states from separable states. The theory of positive maps provides with stronger conditions for separability, as shown in [8].

Theorem 8.8 A state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is separable if and only if for all positive maps

$$\epsilon : \mathcal{B}(\mathcal{H}_B) \rightarrow \mathcal{B}(\mathcal{H}_C),$$

we have

$$(\mathcal{I}_A \otimes \epsilon)\rho \geq 0.$$

Proof. $[\Rightarrow]$ As ρ is separable, we can write it as

$$\rho = \sum_{k=1}^P p_k |e_k\rangle\langle e_k| \otimes |f_k\rangle\langle f_k|,$$

for some $P > 0$. On this state, $(\mathcal{I}_A \otimes \epsilon)$ acts as

$$(\mathcal{I}_A \otimes \epsilon)\rho = \sum_{k=1}^P p_k |e_k\rangle\langle e_k| \otimes \epsilon(|f_k\rangle\langle f_k|) \geq 0,$$

where the last $\geq$ follows because $|f_k\rangle\langle f_k| \geq 0$, and ϵ is positive.

$[\Leftarrow]$ The proof in this direction is not as easy as the only if direction. We shall prove it at the end of this section.

Theorem 8.8 can also be recasted into the following form:

Theorem 8.9 ([8]) A state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is entangled if and only if there exists a positive map $\epsilon : \mathcal{B}(\mathcal{H}_B) \rightarrow \mathcal{B}(\mathcal{H}_C)$, such that

$$(\mathcal{I}_A \otimes \epsilon)\rho \not\geq 0. \tag{8.5}$$

Note that Eq. (8.5) can never hold for maps, ϵ , that are completely positive, and for non-positive maps, it may hold even for separable states. Hence, any positive but not completely positive map can be used to detect entanglement.

Jamiołkowski Isomorphism

In order to complete the proof of Theorem 8.8, we introduce first the Jamiołkowski isomorphism [26] between operators and maps. Given an operator $E \in \mathcal{B}(\mathcal{H}_B \otimes \mathcal{H}_C)$, and an orthonormal product basis $|k, l\rangle$, we define a map by

$$\begin{aligned} \epsilon : \mathcal{B}(\mathcal{H}_B) &\rightarrow \mathcal{B}(\mathcal{H}_C) \\ \epsilon(\rho) &= \sum_{k_1, l_1, k_2, l_2} {}_{BC} \langle k_1 l_1 | E | k_2 l_2 \rangle_{BC} \quad |l_1\rangle_{CB} \langle k_1 | \rho | k_2 \rangle_{BC} \langle l_2|, \end{aligned}$$

or in short form,

$$\epsilon(\rho) = \text{tr}_B(E\rho^{TB}).$$

This shows how to construct the map ϵ from a given operator E . To construct an operator from a given map we use the state

$$|\psi^+\rangle = \frac{1}{\sqrt{M}} \sum_{i=1}^M |i\rangle_{B'} |i\rangle_B$$

(where $M = \dim \mathcal{H}_B$) to get

$$M (I_{B'} \otimes \epsilon) (|\psi^+\rangle \langle \psi^+|) = E.$$

This isomorphism between maps and operators results in the following properties:

Theorem 8.10 ([8, 23–26])

1. $E \geq 0$ if and only if ϵ is a completely positive map.
2. E is an entanglement witness if and only if ϵ is a positive map.
3. E is a decomposable entanglement witness if and only if ϵ is decomposable.
4. E is a nondecomposable entanglement witness if and only if ϵ is nondecomposable and positive.

To indicate further how this equivalence between maps and operators works, we develop here a proof for the “only if” direction of the second statement. Let $E \in \mathcal{B}(\mathcal{H}_B \otimes \mathcal{H}_C)$ be an entanglement witness, then $\langle e, f | E | e, f \rangle \geq 0$. By the Jamiołkowski isomorphism, the corresponding map is defined as $\epsilon(\rho) = \text{tr}_B(E\rho^{TB})$ where $\rho \in \mathcal{B}(\mathcal{H}_B)$. We have to show that

$${}_C \langle \phi | \epsilon(\rho) | \phi \rangle_C = {}_C \langle \phi | \text{tr}(E\rho^{TB}) | \phi \rangle_C \geq 0 \quad \forall |\phi\rangle_C \in \mathcal{H}_C.$$

Since ρ acts on Bob’s space, using the spectral decomposition of ρ , $\rho = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|$ leads to

$$\rho^{TB} = \sum_i \lambda_i |\psi_i^*\rangle \langle \psi_i^*|,$$

where all $\lambda_i \geq 0$. Then

$$\begin{aligned} {}_C\langle\phi|\epsilon(\rho)|\phi\rangle_C &= {}_C\langle\phi|\sum_i \text{tr}_B(E\lambda_i|\psi_i^*\rangle_{BB}\langle\psi_i^*|)|\phi\rangle_C \\ &= \sum_i \lambda_i {}_{BC}\langle\psi_i^*, \phi|E|\psi_i^*, \phi\rangle_{BC} \geq 0. \end{aligned}$$

□

We can now prove the $\Leftarrow$ direction of Theorem 8.8 or, equivalently, the $\Rightarrow$ direction of Theorem 8.9. We thus have to show that if ρ_{AB} is entangled, there exists a positive map $\epsilon : \mathcal{B}(\mathcal{H}_A) \rightarrow \mathcal{B}(\mathcal{H}_C)$, such that $(\epsilon \otimes \mathcal{I}_B)\rho$ is not positive definite. If ρ is entangled, then there exists an entanglement witness W_{AB} such that

$$\begin{aligned} \text{tr}(W_{AB}\rho_{AB}) &< 0, \quad \text{and} \\ \text{tr}(W_{AB}\sigma_{AB}) &\geq 0, \end{aligned}$$

for all separable σ_{AB} . W_{AB} is an entanglement witness (which detects ρ_{AB}) if and only if W_{AB}^T (note the complete transposition!) is also an entanglement witness (which detects ρ_{AB}^T). We define a map by

$$\begin{aligned} \epsilon : \mathcal{B}(\mathcal{H}_A) &\rightarrow \mathcal{B}(\mathcal{H}_C), \\ \epsilon(\rho) &= \text{tr}_A(W_{AC}^T \rho_{AB}^{T_A}), \end{aligned}$$

where $\dim \mathcal{H}_C = \dim \mathcal{H}_B = M$. Then

$$(\epsilon \otimes \mathcal{I}_B)(\rho_{AB}) = \text{tr}_A(W_{AC}^T \rho_{AB}^{T_A}) = \text{tr}_A(W_{AC}^{T_C} \rho_{AB}) = \tilde{\rho}_{CB},$$

where we have used Lemma 8.1, and that $T = T_A \circ T_C$. To complete the proof, one has to show that $\tilde{\rho}_{CB} \not\geq 0$, which can be done by showing that ${}_{CB}\langle\psi^+|\tilde{\rho}_{CB}|\psi^+\rangle_{CB} < 0$, where $|\psi^+\rangle_{CB} = \frac{1}{\sqrt{M}} \sum_i |ii\rangle_{CB}$, with $\{|i\rangle\}$ being an orthonormal basis. □

8.6 Bell Inequalities

The first criterion used to detect entanglement was Bell inequalities, which we briefly discuss in this section. As we shall see, Bell inequalities are essentially a special type of entanglement witness. An additional property of Bell inequalities is that any entangled state detected by them is nonclassical in a particular way: It violates “local realism.”

The assumptions of “locality” and “realism” were already present in the famous argument of Einstein, Podolsky, and Rosen [27] that questions the completeness of quantum mechanics. Bell [28] made these assumptions more precise, and more importantly, showed that the assumptions are actually *testable* in experiments. He derived an inequality that must be satisfied by any physical theory of Nature that is “local” as well as “realistic,” the precise meanings of which will be described below. The inequality is actually a constraint on a linear function of results of certain experiments. He then went on to show that there exist states in quantum theory that violate this inequality in experiments. Modulo some so-called loopholes (see

e.g., [29]), these inequalities have been shown to be actually violated in experiments (see e.g., [30] and references therein). In this section, we will first derive a Bell inequality⁷ and then show how this inequality is violated by the singlet state.

Consider a two spin-1/2 particle state where the two particles are far apart. Let the particles be called A and B . Let projection valued measurements in the directions a and b be done on A and B respectively. The outcomes of the measurements performed on the particles A and B in the directions a and b are respectively A_a and B_b . The measurement result A_a (B_b), whose values can be ± 1 , may depend on the direction a (b) and some other uncontrolled parameter λ which may depend on anything, that is, may depend upon system or measuring device or both. Therefore we assume that A_a (B_b) has a definite premeasurement value $A_a(\lambda)$ ($B_b(\lambda)$). Measurement merely uncovers this value. This is the *assumption of reality*. λ is usually called a hidden variable and this assumption is also termed the hidden variable assumption. Moreover, the measurement result at A (B) does not depend on what measurements are performed at B (A). That is, for example $A_a(\lambda)$ does not depend upon b . This is the *assumption of locality*, also called Einstein's locality assumption. The parameter λ is assumed to have a probability distribution, say $\rho(\lambda)$. Therefore $\rho(\lambda)$ satisfies the following:

$$\int \rho(\lambda) d\lambda = 1, \quad \rho(\lambda) \geq 0.$$

The correlation function of the two spin-1/2 particle state for a measurement in a fixed direction a for particle A and b for particle B is then given by (provided the hidden variables exist)

$$E(a, b) = \int A_a(\lambda) B_b(\lambda) \rho(\lambda) d\lambda.$$

Here

$$A_a(\lambda) = \pm 1, \quad \text{and} \quad B_b(\lambda) = \pm 1,$$

because the measurement values were assumed to be ± 1 .

Let us now suppose that the observers at the two particles A and B can choose their measurements from two observables a, a' and b, b' respectively, and the corresponding outcomes are $A_a, A_{a'}$ and $B_b, B_{b'}$ respectively. Then

$$\begin{aligned} E(a, b) + E(a, b') + E(a', b) - E(a', b') \\ = \int [A_a(\lambda)(B_b(\lambda) + B_{b'}(\lambda)) + A_{a'}(\lambda)(B_b(\lambda) - B_{b'}(\lambda))] \rho(\lambda) d\lambda. \end{aligned}$$

Now $B_b(\lambda) + B_{b'}(\lambda)$ and $B_b(\lambda) - B_{b'}(\lambda)$ can only be ± 2 and 0, or 0 and ± 2 respectively. Consequently,

$$-2 \leq E(a, b) + E(a, b') + E(a', b) - E(a', b') \leq 2. \quad (8.6)$$

⁷We do not derive here the original Bell inequality, which Bell derived in 1964 [28]. Instead, we derive the stronger form of the Bell inequality which Clauser, Horne, Shimony, and Holt (CHSH) derived in 1969 [31]. A similar derivation was also given by Bell himself in 1971 [32].

This is the well-known CHSH inequality. Note here that in obtaining the above inequality, we have never used quantum mechanics. We have only assumed Einstein's locality principle and an underlying hidden variable model. Consequently, a Bell inequality is a constraint that any physical theory that is both, local and realistic, has to satisfy. Below, we will show that this inequality can be violated by a quantum state. Hence quantum mechanics is incompatible with an underlying local realistic model.

Detection of entanglement by Bell inequality

Let us now show how the singlet state can be detected by a Bell inequality. This additionally will indicate that quantum theory is incompatible with local realism. For the singlet state, the quantum mechanical prediction of the correlation function $E(a, b)$ is given by

$$E(a, b) = \langle \psi^- | \sigma_a \cdot \sigma_b | \psi^- \rangle = -\cos(\theta_{ab}), \quad (8.7)$$

where $\sigma_a = \vec{\sigma} \cdot \vec{a}$ and similarly for σ_b . $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, where σ_x , σ_y , and σ_z are the Pauli spin matrices. And θ_{ab} is the angle between the two measurement directions a and b .

So for the singlet state, one has

$$\begin{aligned} B_{\text{CHSH}} &= E(a, b) + E(a, b') + E(a', b) - E(a', b') \\ &= -\cos \theta_{ab} - \cos \theta_{ab'} - \cos \theta_{a'b} + \cos \theta_{a'b'}. \end{aligned} \quad (8.8)$$

The maximum value of this function is attained for the directions a, b, a', b' on a plane, as given in Fig. 8.3, and in that case

$$|B_{\text{CHSH}}| = 2\sqrt{2}.$$

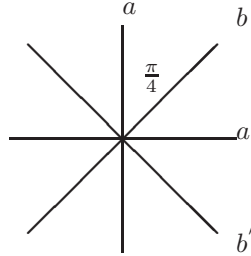


Figure 8.3. Schematic diagram showing the direction of a, b, a', b' for obtaining maximal violation of Bell inequality by the singlet state.

This clearly violates the inequality in Eq. (8.6). But Eq. (8.6) was a constraint for any physical theory which has an underlying local hidden variable model. As the singlet state, a state allowed by the quantum mechanical description of Nature violates the constraint (8.6), quantum mechanics cannot have an underlying local hidden variable model. In other words, quantum mechanics is not local realistic. This is the statement of the celebrated Bell theorem.

Moreover, it is easy to convince oneself that any separable state does have a local realistic description, so that such a state cannot violate a Bell inequality. Consequently, the violation of

Bell inequality by the singlet state indicates that the singlet state is an entangled state. Further, the operator (cf. Eqs. (8.7) and (8.8))

$$\tilde{B}_{\text{CHSH}} = \sigma_a \cdot \sigma_b + \sigma_a \cdot \sigma_{b'} + \sigma_{a'} \cdot \sigma_b - \sigma_{a'} \cdot \sigma_{b'}$$

can, by suitable scaling and change of origin, be considered as an entanglement witness for the singlet state, for a, b, a', b' chosen as in Fig. 8.3 (cf. [33]).

8.7 Classification of Bipartite States with Respect to Quantum Dense Coding

Up to now, we have been interested in splitting the set of all bipartite quantum states into separable and entangled states. However, one of the main motivations behind the study of entangled states is that some of them can be used to perform certain tasks, which are not possible if one uses states without entanglement. It is, therefore, important to find out which entangled states are useful for a given task. We discuss here the particular example of quantum dense coding [2].

Suppose that Alice wants to send two bits of classical information to Bob. Then a general result known as the Holevo bound (to be discussed below) shows that Alice must send two qubits (i.e., 2 two-dimensional quantum systems) to Bob, if only a noiseless quantum channel is available. However, if additionally Alice and Bob have previously shared entanglement, then Alice may have to send less than two qubits to Bob. It was shown by Bennett and Wiesner [2] that by using a previously shared singlet (between Alice and Bob), Alice will be able to send two bits to Bob, by sending just a single qubit.

The protocol of dense coding [2] works as follows. Assume that Alice and Bob share a singlet state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

The crucial observation is that this entangled two-qubit state can be transformed into four orthogonal states of the two-qubit Hilbert space by performing unitary operations on just a single qubit. For instance, Alice can apply a rotation (the Pauli operations) or do nothing to her part of the singlet, while Bob does nothing to obtain the three triplets (or the singlet):

$$\begin{aligned} \sigma_x \otimes I |\psi^-\rangle &= -|\phi^-\rangle, & \sigma_y \otimes I |\psi^-\rangle &= i|\phi^+\rangle, \\ \sigma_z \otimes I |\psi^-\rangle &= |\psi^+\rangle, & I \otimes I |\psi^-\rangle &= |\psi^-\rangle, \end{aligned}$$

where

$$\begin{aligned} |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \\ |\phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \end{aligned}$$

and I is the qubit identity operator. Suppose that the classical information that Alice wants to send to Bob is i , where $i = 0, 1, 2, 3$. Alice and Bob previously agree on the following

correspondence between the operations applied at Alice's end and the information i that she wants to send:

$$\begin{aligned}\sigma_x &\Rightarrow i = 0, & \sigma_y &\Rightarrow i = 1, \\ \sigma_z &\Rightarrow i = 2, & I &\Rightarrow i = 3.\end{aligned}$$

Depending on the classical information she wishes to send, Alice applies the appropriate rotation on her part of the shared singlet, according to the above correspondence. Afterwards, Alice sends her part of the shared state to Bob via the noiseless quantum channel. Bob now has in his possession the entire two-qubit state, which is in any of the four Bell states $\{|\psi^\pm\rangle, |\phi^\pm\rangle\}$. Since these states are mutually orthogonal, he will be able to distinguish between them and hence find out the classical information sent by Alice.

To consider a more realistic scenario, usually two avenues are taken. One approach is to consider a *noisy* quantum channel, while the additional resource is an arbitrary amount of shared bipartite *pure* state entanglement (see e.g., [34, 35], see also [36, 37]). The other approach is to consider a *noiseless* quantum channel, while the assistance is by a given bipartite *mixed* entangled state (see e.g., [36–41]).

Here, we consider the second approach, and derive the capacity of dense coding in this scenario, for a given state, where the capacity is defined as the number of classical bits that can be accessed by the receivers, per usage of the noiseless channel. This will lead to a classification of bipartite states according to their degree of ability to assist in dense coding. In the case where a noisy channel and an arbitrary amount of shared pure entanglement are considered, the capacity refers to the channel (see e.g., [34, 35]). However, in our case when a noiseless channel and a given shared (possibly mixed) state are considered, the capacity refers to the state. Note that the mixed shared state in our case can be thought of as an output of a noisy channel. A crucial element in finding the capacity of dense coding is the Holevo bound [42], which is a universal upper bound on classical information that can be decoded from a quantum ensemble. Below we discuss the bound, and subsequently derive the capacity of dense coding.

8.7.1 The Holevo bound

The Holevo bound is an upper bound on the amount of classical information that can be accessed from a quantum ensemble in which the information is encoded. Suppose therefore that Alice (A) obtains the classical message i that occurs with probability p_i , and she wants to send it to Bob (B). Alice encodes this information i in a quantum state ρ_i and sends it to Bob. Bob receives the ensemble $\{p_i, \rho_i\}$ and wants to obtain as much information as possible about i . To do so, he performs a measurement that gives the result m with probability q_m . Let the corresponding postmeasurement ensemble be $\{p_{i|m}, \rho_{i|m}\}$. The information gathered can be quantified by the mutual information between the message index i and the measurement outcome [43]:

$$I(i : m) = H(\{p_i\}) - \sum_m q_m H(\{p_{i|m}\}).$$

Note that the mutual information can be seen as the difference between the initial disorder and the (average) final disorder. Bob will be interested to obtain the maximal information, which

is maximum of $I(i : m)$ for all measurement strategies. This quantity is called the accessible information:

$$I_{\text{acc}} = \max I(i : m),$$

where the maximization is over all measurement strategies.

The maximization involved in the definition of accessible information is usually hard to compute, and hence the importance of bounds [42, 44]. In particular, in [42], a universal upper bound, the Holevo bound, on I_{acc} is given:

$$I_{\text{acc}}(\{p_i, \rho_i\}) \leq \chi(\{p_i, \rho_i\}) \equiv S(\bar{\rho}) - \sum_i p_i S(\rho_i).$$

See also [45–47]. Here $\bar{\rho} = \sum_i p_i \rho_i$ is the average ensemble state, and $S(\varsigma) = -\text{tr}(\varsigma \log_2 \varsigma)$ is the von Neumann entropy of ς .

The Holevo bound is asymptotically achievable in the sense that if the sender Alice is able to wait long enough and send long strings of the input quantum states ρ_i , then there exists a particular encoding and a decoding scheme that asymptotically attains the bound. Moreover, the encoding consists in collecting certain long and “typical” strings of the input states, and sending them all at once [48, 49].

8.7.2 Capacity of quantum dense coding

Suppose that Alice and Bob share a quantum state ρ_{AB} . Alice performs the unitary operation U_i with probability p_i on her part of the state ρ_{AB} . The classical information that she wants to send to Bob is i . Subsequent to her unitary rotation, she sends her part of the state ρ^{AB} to Bob. Bob then has the ensemble $\{p_i, \rho_i\}$, where

$$\rho_i = U_i \otimes I \rho_{AB} U_i^\dagger \otimes I.$$

The information that Bob is able to gather is $I_{\text{acc}}(\{p_i, \rho_i\})$. This quantity is bounded above by $\chi(\{p_i, \rho_i\})$ and is asymptotically achievable. The “one-capacity” $C^{(1)}$ of dense coding for the state ρ_{AB} is the Holevo bound for the best encoding by Alice:

$$C^{(1)}(\rho) = \max_{p_i, U_i} \chi(\{p_i, \rho_i\}) \equiv \max_{p_i, U_i} \left(S(\bar{\rho}) - \sum_i p_i S(\rho_i) \right). \quad (8.9)$$

The superscript (1) reflects the fact that Alice is using the shared state once at a time during the asymptotic process. She is not using entangled unitaries on more than one copy of her parts of the shared states ρ_{AB} . As we will see below, encoding with entangled unitaries does not help her to send more information to Bob.

In performing the maximization in Eq. (8.9), first note that the second term on the right-hand side (rhs) is $-S(\rho)$, for all choices of the unitaries and probabilities. Secondly, we have

$$S(\bar{\rho}) \leq S(\bar{\rho}_A) + S(\bar{\rho}_B) \leq \log_2 d_A + S(\bar{\rho}_B),$$

where d_A is the dimension of Alice’s part of the Hilbert space of ρ_{AB} , and $\bar{\rho}_A = \text{tr}_B \bar{\rho}$, $\bar{\rho}_B = \text{tr}_A \bar{\rho}$. Moreover, $S(\bar{\rho}_B) = S(\rho_B)$, as nothing was done at Bob’s end during the

encoding procedure. (In any case, unitary operations do not change the spectrum, and hence the entropy, of a state.) Therefore, we have

$$\max_{p_i, U_i} S(\bar{\rho}) \leq \log_2 d_A + S(\rho_B).$$

But the bound is reached by any complete set of orthogonal unitary operators $\{W_j\}$, to be chosen with equal probabilities, which satisfy the *trace rule* $\frac{1}{d_A^2} \sum_j W_j^\dagger \Xi W_j = \text{tr}[\Xi] I$, for any operator Ξ . Therefore, we have

$$C^{(1)}(\rho) = \log_2 d_A + S(\rho_B) - S(\rho).$$

The optimization procedure above sketched essentially follows that in [41]. Several other lines of argument are possible for the maximization. One is given in [39] (see also [50]). Another way to proceed is to guess where the maximum is reached (maybe from examples or by taking the most symmetric option) and then perturb the guessed result. If the first-order perturbations vanish, the guessed result is correct, as the von Neumann entropy is a concave function and the maximization is carried out over a continuous parameter space.

Without using the additional resource of entangled states, Alice will be able to reach a capacity of just $\log_2 d_A$ bits. Therefore, entanglement in a state ρ^{AB} is useful for dense coding if $S(\rho^B) - S(\rho) > 0$. Such states will be called dense-codeable (DC) states. Such states exist, an example being the singlet state.

Note here that if Alice is able to use entangled unitaries on two copies of the shared state ρ , the capacity is not enhanced (see [51]). Therefore, the one capacity is really the asymptotic capacity, in this case. Note however that this additivity is known only in the case of encoding by unitary operations. A more general encoding may still have additivity problems (see e.g., [37]). Here, we have considered unitary encoding only. This case is both mathematically more accessible, and experimentally more viable.

A bipartite state ρ^{AB} is useful for dense coding if and only if $S(\rho^B) - S(\rho) > 0$. It can be shown that this relation cannot hold for PPT entangled states [36] (see also [50]). Therefore a DC state is always NPT. However, the converse is not true: There exist states which are NPT, but they are not useful for dense coding. Examples of such states can be obtained by the considering the Werner state $\rho_p = p|\psi^-\rangle\langle\psi^-| + \frac{1-p}{4}I \otimes I$.

The discussions above lead us to the following classification of bipartite quantum states:

1. Separable states: These states are of course not useful for dense coding. They can be prepared by LOCC.
2. PPT entangled states: These states, despite being entangled, cannot be used for dense coding. Moreover, their entanglement cannot be detected by the partial transposition criterion.
3. NPT non-DC states: These states are entangled, and their entanglement can be detected by the partial transposition criterion. However, they are not useful for dense coding.
4. DC states: These entangled states can be used for dense coding.

The above classification is illustrated in Fig. 8.4. A generalization of this classification has been considered in [50, 51].

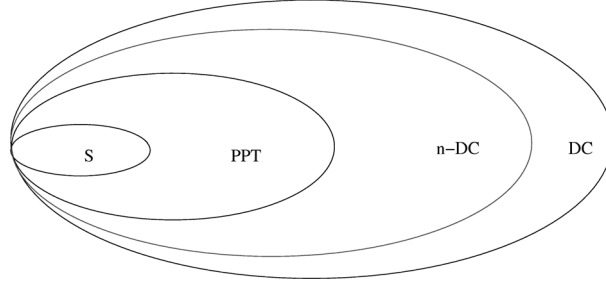


Figure 8.4. Classification of bipartite quantum states according to their usefulness in dense coding. The convex innermost region, marked as S, consists of separable states. The shell surrounding it, marked as PPT, is the set of PPT entangled states. The next shell, marked as n-DC, is the set of all states that are NPT, but not useful for dense coding. The outermost shell is that of dense-codeable states.

8.8 Further Reading: Multipartite States

The discussion about detection of bipartite entanglement presented above is of course quite far from complete. For further reading, we have presented a small sample of references embedded in the text above. We prefer to conclude this chapter with a few remarks on multipartite states.

The case of detection of entanglement of pure states is again simple. One quickly realizes that a multipartite pure state is entangled if and only if it is entangled in at least one bipartite splitting. So, for example, the state $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ [52] is entangled, because it is entangled in any one to rest bipartite splitting.

The case of mixed states is however quite formidable. In particular, the results obtained in the bipartite mixed state case cannot be applied to the multiparty scenario. One way to see this is to note the existence of states which are separable in any bipartite splitting, while the entire state is entangled. An example of such a state is given in [53]. For further results about entanglement criteria, detection, and classification of multipartite states, see e.g., [21, 54–64], and references therein.

Acknowledgments

We acknowledge support from the DFG (SFB 407, SPP1078 and SPP1116, 436POL), Spanish MEC grants BFM-2002-02588, FIS-2005-04627, the Alexander von Humboldt Foundation, the ESF Program QUEDDIS, and EU IP SCALA.

Exercises

1. Show that the singlet state has nonpositive partial transposition.
2. Consider Werner state $p|\psi^-\rangle\langle\psi^-| + (1-p)I/4$ in $2 \otimes 2$, where $0 \leq p \leq 1$ [4]. Find the values of the mixing parameter p for which entanglement in the Werner state can be detected by the partial transposition criterion.
3. Show that in $\mathcal{C}^2 \otimes \mathcal{C}^2$ the partial transposition of a density matrix can have at most one negative eigenvalue.
4. Given two random variables X and Y , show that the Shannon entropy of the joint distribution cannot be smaller than that of either.
5. Prove Theorem 8.5.
6. Prove Lemma 8.1.
7. Prove Theorem 8.10.
8. Show that each of the shells depicted in Fig. 8.4 is nonempty, and of nonzero measure. Show also that all the boundaries are convex.

References

- [1] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [2] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
- [3] C.H. Bennett, G. Brassard, C. Crepeau, R. Josza, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [4] R.F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [5] M. Żukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993); M. Żukowski, A. Zeilinger, and H. Weinfurter, Ann. N.Y. Acad. Sci. **755**, 91 (1995); S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A **57**, 822 (1998); S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A **60**, 194 (1999).
- [6] S. Karnas and M. Lewenstein, J. Phys. A: Math. Gen. **34**, 6919 (2001).
- [7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
- [9] M.A. Nielsen and J. Kempe, Phys. Rev. Lett. **86**, 5184 (2001).
- [10] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (2000).
- [11] O. Rudolph, *Further results on the cross norm criterion for separability*, Preprint quant-ph/0202121; K. Chen and L.-A. Wu, Quant. Inf. Comput., **3**, 193 (2003).
- [12] A. Doherty, P. Parillo, and F. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002); Phys. Rev. A **69**, 022308 (2004); F. Hulpke and D. Bruß, J. Phys. A: Math. Gen. **38**, 5573 (2005).
- [13] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
- [14] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

- [15] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A, **58**, 883 (1998); K. Życzkowski, Phys. Rev. A **60**, 3496 (1999); S. Szarek, *The volume of separable states is super-doubly-exponentially small*, Phys. Rev. A **72**, 032304 (2005).
- [16] D.P. DiVincenzo, P.W. Shor, J.A. Smolin, B.M. Terhal, and A.V. Thapliyal, Phys. Rev. A **61**, 062312 (2000); W. Dür, J.I. Cirac, M. Lewenstein, and D. Bruß, *ibid.* **61**, 062313 (2000).
- [17] A.W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications* (Academic Press, New York, 1979); P.M. Alberti and A. Uhlmann, *Stochasticity and Partial order: Doubly Stochastic Maps and Unitary Mixing* (D. Reidel Publishing Company, Dordrecht, 1982); R. Bhatia, *Matrix Analysis* (Springer, New York, 1997).
- [18] T. Hiroshima, Phys. Rev. Lett. **91**, 057902 (2003).
- [19] P. Horodecki and R. Horodecki, Phys. Lett. A **194**, 147 (1994).
- [20] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **66**, 062305 (2002); O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, J. Mod. Opt. **50**, 1079 (2003).
- [21] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **92**, 087902 (2004).
- [22] H.W. Alt, *Lineare Funktionalanalysis*, (Springer, Berlin, 1985).
- [23] S.L. Woronowicz, Commun. Math. Phys. **51**, 243 (1976); P. Kryszynski and S.L. Woronowicz, Lett. Math. Phys. **3**, 319 (1979); M.D. Choi, Proc. Sympos. Pure Math. **38**, 583 (1982).
- [24] B.M. Terhal, Lin. Alg. Appl. **323**, 61 (2001).
- [25] M. Lewenstein, B. Kraus, J.I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000); D. Bruß, J.I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, J. Mod. Opt. **49**, 1399 (2002).
- [26] A. Jamiolkowski, Rep. Math. Phys., **3**, 275 (1972).
- [27] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **57**, 777 (1935).
- [28] J.S. Bell, Physics **1**, 195 (1964).
- [29] E. Santos, Phys. Rev. Lett. **66**, 1388 (1991); E. Santos, Phys. Rev. A **46**, 3646 (1992); P.M. Pearle, Phys. Rev. D **2**, 1418 (1970); J.F. Clauser and M.A. Horne, Phys. Rev. D **10**, 526 (1974); P.G. Kwiat, P.H. Eberhard, A.M. Steinberg, and R.Y. Chiao, Phys. Rev. A **49**, 3209 (1994); N. Gisin and B. Gisin, Phys. Lett. A **260**, 323 (1999); S. Massar, S. Pironio, J. Roland, and B. Gisin, Phys. Rev. A **66**, 052112 (2002); R. Garcia-Patron, J. Fiurásek, N.J. Cerf, J. Wenger, R. Tualle-Brouiri, and Ph. Grangier, Phys. Rev. Lett. **93**, 130409 (2004).
- [30] S.J. Freedman and J.S. Clauser, Phys. Rev. Lett. **28**, 938 (1972); A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981); *ibid.* **49**, 91 (1982); A. Aspect, J. Dalibard, and G. Roger, *ibid.* **49**, 1804 (1982); P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995); G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998); M.A. Rowe, D. Kielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland, Nature **409**, 791 (2001); W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin, Phys. Rev. A **57**, 3229 (1998); A. Zeilinger Rev. Mod. Phys. **71**, S288 (1999).

- [31] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
- [32] J.S. Bell, in *Foundations of Quantum Mechanics*, ed. B. d’Espagnat (Academic Press, New York, 1971).
- [33] P. Hyllus, O. Gühne, D. Bruß, and M. Lewenstein Phys. Rev. A **72**, 012321 (2005).
- [34] C.H. Bennett, P.W. Shor, J.A. Smolin, and A.V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).
- [35] C.H. Bennett, P.W. Shor, J.A. Smolin, and A.V. Thapliyal, *Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem*, Preprint quant-ph/0106052.
- [36] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal, Q. Inf. Comput. **1**, 70 (2001).
- [37] A. Winter, J. Math. Phys. **43**, 4341 (2002).
- [38] S. Bose, M.B. Plenio, and V. Vedral, J. Mod. Opt. **47**, 291 (2000).
- [39] T. Hiroshima, J. Phys. A: Math. Gen. **34**, 6907 (2001).
- [40] X.S. Liu, G.L. Long, D.M. Tong, and F. Li, Phys. Rev. A **65**, 022304 (2002).
- [41] M. Ziman and V. Bužek, Phys. Rev. A **67**, 042321 (2003).
- [42] J.P. Gordon, in *Proc. Int. School Phys. “Enrico Fermi, Course XXXI”*, ed. P.A. Miles, p. 156 (Academic Press, New York, 1964); L.B. Levitin, in *Proc. VI National Conf. Inf. Theory, Tashkent*, p. 111 (1969); A.S. Holevo, Probl. Pereda. Inf. **9**, 3 1973 [Probl. Inf. Transm. **9**, 110 (1973)].
- [43] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
- [44] R. Josza, D. Robb, and W.K. Wothers, Phys. Rev. A **49**, 668 (1994).
- [45] B. Schumacher, M. Westmoreland, and W. K. Wothers, Phys. Rev. Lett. **76**, 3452 (1996).
- [46] P. Badziąg, M. Horodecki, A. Sen(De), and U. Sen, Phys. Rev. Lett. **91**, 117901 (2003).
- [47] M Horodecki, J. Oppenheim, A. Sen(De), and U. Sen, Phys. Rev. Lett. **93**, 170503 (2004).
- [48] B. Schumacher and M.D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
- [49] A.S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
- [50] D. Bruß, G.M. D’Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), and U. Sen, Phys. Rev. Lett. **93**, 210501 (2004).
- [51] D. Bruß, G.M. D’Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), and U. Sen, *Dense coding with multipartite quantum states*, Preprint quant-ph/0507146.
- [52] D.M. Greenberger, M.A. Horne, and A. Zeilinger, in *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*, ed. M. Kafatos (Kluwer Academic, Dordrecht, 1989).
- [53] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
- [54] W. Dür, J.I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
- [55] R.F. Werner and M.M. Wolf, Phys. Rev. A **64**, 032112 (2001); M. Żukowski and Č. Brukner, Phys. Rev. Lett. **88**, 210401 (2002).
- [56] G. Svetlichny, Phys. Rev. D **35**, 3066 (1987); D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, Phys. Rev. Lett. **88**, 170405 (2002); M. Seevinck and G. Svetlichny, Phys. Rev. Lett. **89**, 060401 (2002); S.M. Roy, Phys. Rev. Lett. **94**, 010402 (2005).

- [57] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **87**, 040401 (2001).
- [58] M. Horodecki, P. Horodecki, and R. Horodecki, *Separability of mixed quantum states: linear contractions approach*, Preprint quant-ph/0206008.
- [59] C. Moura Alves and D. Jaksch Phys. Rev. Lett. **93**, 110501 (2004).
- [60] W. Laskowski, T. Paterek, M. Żukowski, and Č. Brukner, Phys. Rev. Lett. **93**, 200401 (2004).
- [61] F.G.S.L. Brandao and R.O. Vianna, Phys. Rev. Lett. **93**, 220503 (2004).
- [62] G. Toth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005).
- [63] A.C. Doherty, P.A. Parrilo, and F.M. Spedalieri, Phys. Rev. A **71**, 032333 (2005).
- [64] O. Gühne, G. Toth, and H.J. Briegel, *Multipartite entanglement in spin chains*, Preprint quant-ph/0502160.

9 Entanglement Theory with Continuous Variables

Peter van Loock

9.1 Introduction

When studying the theory of entanglement of quantum mechanical systems, there are various reasons to focus on the entanglement of states described by continuous variables [1–3]. First, one may think that the analysis of entangled continuous-variable states is a very subtle task, because these states are defined in an infinite-dimensional Hilbert space. However, it turns out that for a special class of entangled continuous-variable states, the theoretical description simplifies a lot. This class corresponds to the Gaussian entangled states. Moreover, apart from the relative simplicity of their description, Gaussian entangled states represent one of the most practical resources for quantum information applications. For example, in terms of bosonic modes, only relatively modest quadratic interactions are needed in order to create such Gaussian entanglement. Within the framework of Gaussian states, many interesting topics of the theory of entanglement can be explored. Examples are entanglement witnesses [4], bound entanglement [5, 6], multipartite entanglement [7–9], and nonlocality [10, 11]. In this chapter, we are going to focus on two-party (bipartite) entanglement, both for pure and mixed Gaussian states.

The notion of entanglement (in German, “Verschränkung”) appeared explicitly in the literature first in 1935, long before the dawn of the relatively young field of quantum information, and without any reference to discrete-variable qubit states. In fact, the entangled states treated in this 1935 paper by Einstein, Podolsky, and Rosen (“EPR”) were two-particle states quantum mechanically correlated with respect to their positions and momenta [12]. EPR considered the position wavefunction $\psi(x_1, x_2) = C \delta(x_1 - x_2 - u)$ with a vanishing normalization constant C . The corresponding quantum state,

$$|\text{EPR}\rangle = \int dx_1 dx_2 \psi(x_1, x_2) |x_1, x_2\rangle \propto \int dx |x, x - u\rangle, \quad (9.1)$$

describes perfectly correlated positions ($x_1 - x_2 = u$) and momenta ($p_1 + p_2 = 0$). Although the EPR state is unnormalizable and unphysical, it can be thought of as the limiting case of a regularized version where the positions and momenta are correlated only to some finite extent given by a Gaussian width. A regularized EPR state is, for example, given by a two-mode squeezed state. The position and momentum wavefunctions for the two-mode squeezed

vacuum state are [13],

$$\begin{aligned}\psi_{\text{TMSS}}(x_1, x_2) &= \sqrt{\frac{2}{\pi}} \exp[-e^{-2r}(x_1 + x_2)^2/2 - e^{+2r}(x_1 - x_2)^2/2], \\ \bar{\psi}_{\text{TMSS}}(p_1, p_2) &= \sqrt{\frac{2}{\pi}} \exp[-e^{-2r}(p_1 - p_2)^2/2 - e^{+2r}(p_1 + p_2)^2/2],\end{aligned}$$

approaching $C \delta(x_1 - x_2)$ and $C \delta(p_1 + p_2)$, respectively, in the limit of infinite “squeezing” $r \rightarrow \infty$.

Instead of the position or momentum basis, the two-mode squeezed vacuum state may also be written in the discrete photon number (Fock) basis,

$$|\text{TMSS}\rangle = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} \lambda^n |n\rangle |n\rangle, \quad (9.2)$$

where $\lambda = \tanh r$. The form in Eq. (9.2) reveals that the two modes of the two-mode squeezed vacuum state are also quantum correlated in photon number and phase. In general, for any pure two-party state, orthonormal bases of each subsystem exist, $\{|u_n\rangle\}$ and $\{|v_n\rangle\}$ such that the total state vector can be written in the “Schmidt decomposition” [14] as $|\psi\rangle = \sum_n c_n |u_n\rangle |v_n\rangle$, with real and nonnegative Schmidt coefficients c_n satisfying $\sum_n c_n^2 = 1$. Thus, the form in Eq. (9.2) is the Schmidt decomposition for the two-mode squeezed vacuum state. A maximally entangled two-party state is usually defined via the condition that all Schmidt coefficients (of at least two) are equal. Since $\tanh r \rightarrow 1$ for $r \rightarrow \infty$, and hence $c_{n+1}/c_n \rightarrow 1$ in this limit, we can see that the state $|\text{TMSS}\rangle$ in Eq. (9.2) approaches a maximally entangled state for infinite squeezing. However, for finite squeezing r , the two-mode squeezed state represents a nonmaximally entangled state. It is the prime example for a two-party entangled Gaussian state and it has been created via the so-called optical parametric amplification in many labs around the globe.

Typically, a two-mode squeezed state is referred to as an optical state built from laser light, where the optical modes become entangled through some squeezing interaction (i.e., parametric amplification). A quantum mechanical optical mode is mathematically equivalent to a quantum harmonic oscillator with creation and annihilation operators acting upon the photon number basis as

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle, \quad \hat{a} |n\rangle = \sqrt{n} |n-1\rangle,$$

respectively. The real and imaginary parts of the mode’s (oscillator’s) photon annihilation operator, $\hat{a} = \hat{x} + i\hat{p}$, play the roles of the particle-like observables, position and momentum. Like the annihilation operator itself, also $\hat{x}$ and $\hat{p}$ shall be dimensionless, corresponding to units $\hbar = 1/2$ and the commutator $[\hat{x}, \hat{p}] = i/2$.¹ The most convenient way to describe the quantum statistics and correlations of these optical position and momentum analogs (commonly called “quadratures”) is in terms of the Wigner function. Let us now first introduce the Wigner function as the most natural tool to represent quantum states in phase space (more details on this phase-space representation are discussed in Chapter 3).

¹Note that the units chosen in the introductory chapter on continuous variables, Chapter 3, correspond to $[\hat{x}, \hat{p}] = i$ and $\hbar = 1$. Here we prefer to use units such that $\hat{a} = \hat{x} + i\hat{p}$ and $\hbar = 1/2$.

9.2 Phase-Space Description

The Wigner function can be used to calculate measurable quantities such as mean values and variances for the phase-space variables, position and momentum, in a classical-like fashion. In general, as opposed to a classical probability distribution, the Wigner function can become negative. However, the Wigner functions for describing Gaussian states are always positive definite. In the position basis, the Wigner function for a single particle or mode can be written as [15]

$$W(x, p) = \frac{2}{\pi} \int_{-\infty}^{\infty} dy e^{+4iyp} \langle x - y | \hat{\rho} | x + y \rangle .$$

Thus, any quantum state described by a density operator $\hat{\rho}$ can be equivalently represented by a Wigner function. The Wigner function $W(x, p)$ is properly normalized,

$$\int_{-\infty}^{\infty} W(x, p) dx dp = 1 ,$$

and it yields the correct marginal distributions upon integrating over either of the two phase-space variables,

$$\int_{-\infty}^{\infty} W(x, p) dx = \langle p | \hat{\rho} | p \rangle , \quad \int_{-\infty}^{\infty} W(x, p) dp = \langle x | \hat{\rho} | x \rangle .$$

Now for any symmetrized operator, the so-called Weyl correspondence [16],

$$\text{Tr}[\hat{\rho} \mathcal{S}(\hat{x}^n \hat{p}^m)] = \int_{-\infty}^{\infty} W(x, p) x^n p^m dx dp , \quad (9.3)$$

provides a rule how to calculate quantum mechanical expectation values in a classical-like fashion using the Wigner function [13]. Here, $\mathcal{S}(\hat{x}^n \hat{p}^m)$ indicates symmetrization. For example, calculating the expectation value of $\mathcal{S}(\hat{x}^2 \hat{p}) = (\hat{x}^2 \hat{p} + \hat{x} \hat{p} \hat{x} + \hat{p} \hat{x}^2)/3$ corresponds to a classical-like averaging over $x^2 p$. The Wigner function is perfectly suited to compute expectation values of quantities symmetric in $\hat{a}$ and $\hat{a}^\dagger$ such as the position $\hat{x} = (\hat{a} + \hat{a}^\dagger)/2$ and the momentum $\hat{p} = (\hat{a} - \hat{a}^\dagger)/2i$. In particular, for Gaussian states, the Wigner function is the most convenient representation. Let us now turn to the entanglement of Gaussian states.

9.3 Entanglement of Gaussian States

In this section, we will discuss the entanglement properties of Gaussian states. We will thereby focus on two-party entanglement, mainly represented by two-mode Gaussian states. While general Gaussian states and, in particular, general Gaussian operations are discussed in great detail in Chapter 3, here we will only briefly review these topics. After defining Gaussian states and their manipulation via Gaussian operations, in particular, Gaussian unitary transformations, first, we are going to consider *pure* entangled Gaussian states. Later, we will investigate the inseparability of *mixed* Gaussian states and how to witness their entanglement using inseparability criteria for continuous variables.

9.3.1 Gaussian states

A general Gaussian state is defined by having a Gaussian Wigner function or, equivalently, a Gaussian characteristic function (which is the Fourier transform of the Wigner function). For our purposes, we may introduce only Gaussian states with vanishing first moments. Nonzero means can always be removed via local phase-space displacements and hence do not affect the entanglement properties of the state. We define a normalized Gaussian N -mode Wigner function (with zero mean) as

$$W(\xi) = \frac{1}{(2\pi)^N \sqrt{\det V^{(N)}}} \exp \left\{ -\frac{1}{2} \xi \left[V^{(N)} \right]^{-1} \xi^T \right\}, \quad (9.4)$$

with the $2N$ -dimensional vector ξ containing the quadrature pairs of all N modes, $\xi = (x_1, p_1, x_2, p_2, \dots, x_N, p_N)$. The elements of the $2N \times 2N$ correlation matrix $V^{(N)}$ are the second moments symmetrized according to the Weyl correspondence in Eq. (9.3),

$$\text{Tr}[\hat{\rho} (\Delta \hat{\xi}_i \Delta \hat{\xi}_j + \Delta \hat{\xi}_j \Delta \hat{\xi}_i)/2] = \int_{-\infty}^{\infty} W(\xi) \xi_i \xi_j d^{2N} \xi = V_{ij}^{(N)}. \quad (9.5)$$

Here, we used $\hat{\xi} = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \dots, \hat{x}_N, \hat{p}_N)$ and $\Delta \hat{\xi}_i = \hat{\xi}_i - \langle \hat{\xi}_i \rangle = \hat{\xi}_i$ for zero mean values. The last equality in Eq. (9.5) defines the correlation matrix for any quantum state. For Gaussian states of the form (9.4), the Wigner function is completely determined by the second-moment correlation matrix.

The correlation matrix is real, symmetric, and positive. Moreover, it must satisfy the N -mode uncertainty relation [5, 6],

$$V^{(N)} - \frac{i}{4} \Lambda \geq 0, \quad (9.6)$$

based upon the commutation relation,

$$[\hat{\xi}_k, \hat{\xi}_l] = \frac{i}{2} \Lambda_{kl}, \quad k, l = 1, 2, 3, \dots, 2N.$$

Here, the $2N \times 2N$ “symplectic matrix” Λ is block diagonal and contains the 2×2 matrix J as diagonal entries for each quadrature pair,

$$\Lambda = \bigoplus_{k=1}^N J, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (9.7)$$

The matrix equation in Eq. (9.6) means that the matrix sum on the left-hand side has only nonnegative eigenvalues. In the simplest case of only one mode, $N = 1$, Eq. (9.6) is reduced to the statement $\det V^{(1)} \geq 1/16$, which is a more precise and complete version of the well-known Heisenberg uncertainty relation

$$\langle (\Delta \hat{x})^2 \rangle \langle (\Delta \hat{p})^2 \rangle \geq \frac{1}{4} |[\hat{x}, \hat{p}]|^2 = 1/16. \quad (9.8)$$

The correlation matrix, for example, for a pure one-mode squeezed state can be written as

$$V_{\text{OMSSX}}^{(1)} = \frac{1}{4} \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{+2r} \end{pmatrix}, \quad V_{\text{OMSSP}}^{(1)} = \frac{1}{4} \begin{pmatrix} e^{+2r} & 0 \\ 0 & e^{-2r} \end{pmatrix}, \quad (9.9)$$

where $V_{\text{OMSSX}}^{(1)}$ refers to a position-squeezed state for any $r > 0$ and $V_{\text{OMSSP}}^{(1)}$ to a momentum squeezed state for any $r > 0$. Both become the one-mode vacuum state for $r = 0$. All these *pure* states exhibit minimum uncertainty, attaining the bound given by the Heisenberg uncertainty relation in Eq. (9.8). In general, the purity condition for an N -mode Gaussian state is given by $\det V^{(N)} = 1/16^N$.

9.3.2 Gaussian operations

As for the manipulation of Gaussian states, an important class is the set of Gaussian operations [17]. The Gaussian operations are those quantum operations (completely positive maps) that map all Gaussian states onto Gaussian states. The subset of Gaussian operations that exclude Gaussian measurements such as homodyne detection (basically the projection onto the position or momentum basis) are the Gaussian *unitary* transformations. These are the most practical operations, because they can be realized via beam splitters, squeezers, and phase shifters. On the level of the correlation matrices, the Gaussian unitary transformations correspond to the *symplectic* transformations,

$$V^{(N)} \longrightarrow V^{(N)'} = S V^{(N)} S^T, \quad (9.10)$$

where $S \Lambda S^T = \Lambda$. Those transformations which are both symplectic, $O \Lambda O^T = \Lambda$, and orthogonal, $O O^T = \mathbb{1}$, belong to the class of passive transformations. These transformations, realizable via beam splitters and phase shifters, are photon number preserving, as opposed to the active squeezing transformations. Among the simplest examples for passive and for active symplectic transformations are the 50/50 beam splitter,

$$O_{\text{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \quad (9.11)$$

and the one-mode squeezers,

$$S_{\text{OMSX}} = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{+r} \end{pmatrix}, \quad S_{\text{OMSP}} = \begin{pmatrix} e^{+r} & 0 \\ 0 & e^{-r} \end{pmatrix}, \quad (9.12)$$

respectively. On the level of the mode operators, the symplectic transformations are reflected by *linear* transformations. Among these, the passive linear transformations are described by $\hat{a}_j \longrightarrow \hat{a}'_j = \sum_i U_{ji} \hat{a}_i$, with a unitary matrix U . More general linear transformations, including both passive and active elements such as multimode squeezing, are expressed by $\hat{a}_j \longrightarrow \hat{a}'_j = \sum_i A_{ji} \hat{a}_i + B_{ji} \hat{a}_i^\dagger$. Here, the matrices A and B are, in general, not unitary. With these transformations, one can see that the position and momentum operators in $\hat{a}_j = \hat{x}_j + i\hat{p}_j$ are also linearly transformed, in agreement with the matrix transformation in Eq. (9.10). In the following, we will now discuss entangled Gaussian states. First, we are going to focus on the pure-state case.

9.3.3 Pure entangled Gaussian states

The prime example for an entangled Gaussian state is the pure two-mode squeezed (vacuum) state, described by the Gaussian Wigner function

$$W_{\text{TMSS}}(\xi) = \frac{4}{\pi^2} \exp \left\{ -e^{-2r} [(x_1 + x_2)^2 + (p_1 - p_2)^2] - e^{+2r} [(x_1 - x_2)^2 + (p_1 + p_2)^2] \right\}, \quad (9.13)$$

with $\xi = (x_1, p_1, x_2, p_2)$. This Wigner function approaches $C \delta(x_1 - x_2) \delta(p_1 + p_2)$ in the limit of infinite squeezing $r \rightarrow \infty$, corresponding to the original EPR state. Though having well-defined relative position and total momentum for large squeezing, the two modes of the two-mode squeezed vacuum state exhibit increasing uncertainties in their individual positions and momenta as the squeezing grows. In fact, upon tracing (integrating) out either mode of the Wigner function in Eq. (9.13), we obtain the “thermal state”

$$\int_{-\infty}^{\infty} W_{\text{TMSS}}(\xi) dx_1 dp_1 = \frac{2}{\pi(1 + 2\bar{n})} \exp \left[-\frac{2(x_2^2 + p_2^2)}{1 + 2\bar{n}} \right],$$

with mean photon number $\bar{n} = \sinh^2 r$. As the two-mode squeezed state is the maximally entangled state at a given energy, the thermal state corresponds to the maximally mixed state at this energy. This is analogous to the finite-dimensional discrete case, where tracing out one party of a maximally entangled state yields the maximally mixed state. The correlation matrix of the two-mode squeezed state is given by

$$V_{\text{TMSS}}^{(2)} = \frac{1}{4} \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix}, \quad (9.14)$$

according to Eqs. (9.13) and (9.4). By extracting the second moments from the correlation matrix in Eq. (9.14), we can verify that the individual quadratures become very noisy for large squeezing r , whereas the relative position and the total momentum become very quiet,

$$\begin{aligned} \langle (\hat{x}_1 - \hat{x}_2)^2 \rangle &= \langle \hat{x}_1^2 \rangle + \langle \hat{x}_2^2 \rangle - 2 \langle \hat{x}_1 \hat{x}_2 \rangle = e^{-2r}/2, \\ \langle (\hat{p}_1 + \hat{p}_2)^2 \rangle &= \langle \hat{p}_1^2 \rangle + \langle \hat{p}_2^2 \rangle + 2 \langle \hat{p}_1 \hat{p}_2 \rangle = e^{-2r}/2. \end{aligned} \quad (9.15)$$

However, what about arbitrarily small, but nonzero squeezing r ? From Eq. (9.2), we can easily infer that the two-mode squeezed state is entangled for any nonzero squeezing $r > 0$, even though this entanglement appears to be very bad for small squeezing values. In fact, we may even *quantify* the entanglement of the two-mode squeezed state using the Schmidt decomposition in Eq. (9.2). A unique measure of bipartite entanglement for pure states is given by the partial von Neumann entropy [18]. This is the von Neumann entropy, $-\text{Tr} \hat{\rho} \log \hat{\rho}$, of the reduced system after tracing out either subsystem: $E_{\text{v.N.}} = -\text{Tr} \hat{\rho}_1 \log \hat{\rho}_1 = -\text{Tr} \hat{\rho}_2 \log \hat{\rho}_2 = -\sum_n c_n^2 \log c_n^2$, using the Schmidt decomposition $|\psi\rangle = \sum_n c_n |u_n\rangle |v_n\rangle$ and $\text{Tr}_2 \hat{\rho}_{12} = \hat{\rho}_1$, $\text{Tr}_1 \hat{\rho}_{12} = \hat{\rho}_2$. Using Eq. (9.2), we can then quantify the entanglement of the two-mode squeezed vacuum state via the partial von Neumann entropy [19],

$$E_{\text{v.N.}} = \cosh^2 r \log(\cosh^2 r) - \sinh^2 r \log(\sinh^2 r).$$

However, all these results are based upon the discrete Schmidt decomposition in the photon number basis rather than any nonclassical correlations in the continuous position and momentum variables.² In the next section on mixed-entangled Gaussian states and inseparability criteria, we will see how the presence of entanglement can be verified through correlations similar to those in Eq. (9.15). In the remainder of this section, we will now discuss some simple examples for transforming pure Gaussian two-mode states into two-mode squeezed states of the form (9.14). Finally, we will put these examples in a more general context.

Let us now first consider the case where a separable Gaussian two-mode state is transformed into an entangled Gaussian two-mode state. Remarkably, a simple passive linear transformation corresponding to a beam splitter operation is sufficient to accomplish this. However, obviously, this operation is a *nonlocal* Gaussian transformation acting upon both input modes globally. Otherwise, through only local operations, a separable state cannot be turned into an entangled state. We use the separable input state $|\text{OMSSP}\rangle \otimes |\text{OMSSX}\rangle$, a product state of two one-mode squeezed states, where the first one shall be squeezed in p and the second one squeezed in x . The correlation matrix of this Gaussian two-mode state is given by $V^{(2)} = V_{\text{OMSSP}}^{(1)} \oplus V_{\text{OMSSX}}^{(1)}$, using Eq. (9.9). Now applying the beam splitter operation from Eq. (9.11) to $V^{(2)}$ leads to the following transformation:

$$V^{(2)} \longrightarrow V^{(2)'} = O_{\text{BS}} V^{(2)} O_{\text{BS}}^T = V_{\text{TMSS}}^{(2)},$$

with the correlation matrix of a two-mode squeezed state in Eq. (9.14). This example demonstrates how one can actually build an entangled state from one-mode squeezed states using passive linear transformations. The corresponding method for creating Gaussian entanglement has been employed in many experiments around the world.

Our second example is even simpler. Again, we start with the separable two-mode state $|\text{OMSSP}\rangle \otimes |\text{OMSSX}\rangle$. However, this time, we only allow for *local* Gaussian unitary transformations. In other words, assuming that the two modes are shared by two spatially separated people, Alice and Bob, both Alice and Bob can only act upon their own single mode. As mentioned above, via local operations, Alice and Bob will not be able to transform their shared state into an entangled two-mode squeezed state. However, by applying local squeezers to it,

$$V^{(2)} \longrightarrow V^{(2)'} = S V^{(2)} S^T = V_{\text{TMSS}}^{(2)}(r = 0),$$

with $S \equiv S_{\text{OMSX}} \oplus S_{\text{OMSP}}$ and Eq. (9.12), they can convert their state locally into the two-mode vacuum corresponding to $V_{\text{TMSS}}^{(2)}(r = 0)$. This case is an almost trivial example for locally transforming a pure two-mode Gaussian state into the form $V_{\text{TMSS}}^{(2)}$ of Eq. (9.14). More interesting, however, is that *any* pure two-mode Gaussian state, including entangled and separable ones, can be transformed into the form $V_{\text{TMSS}}^{(2)}$ via *local* Gaussian unitary transformations [21, 22]. More generally, any bipartite pure multimode Gaussian state corresponds to a product of two-mode squeezed states (with $r_1 \geq r_2 \geq \dots \geq 0$) up to local Gaussian unitary transformations [21, 22]. Thus, the two-mode squeezed states represent a kind of standard form for pure Gaussian states. Let us now consider the case of mixed Gaussian states.

²Moreover, note that the entanglement of the two-mode squeezed vacuum state becomes infinite in the limit of infinite squeezing $r \rightarrow \infty$, corresponding to a maximally entangled (in the sense that all the Schmidt coefficients become equal), but unphysical state of infinite energy. In order to avoid these complications, one may use natural constraints to the mean energy [20], and, for instance, define a maximally entangled state as the state with the maximum entanglement at a given energy (which corresponds to the two-mode squeezed state).

9.3.4 Mixed entangled Gaussian states and inseparability criteria

A general quantum state of a two-party system is separable if its total density operator is a mixture (a convex sum) of product states [23],

$$\hat{\rho}_{12} = \sum_i \eta_i \hat{\rho}_{i,1} \otimes \hat{\rho}_{i,2} . \quad (9.16)$$

Otherwise, it is inseparable. In general, it is a nontrivial question whether a given density operator is separable or inseparable.

As for verifying the inseparability of a given two-mode continuous-variable state, Duan *et al.* derived an inequality in terms of the variances of position and momentum linear combinations [4], similar to those in Eq. (9.15). This inequality is satisfied by any separable state and is violated only by inseparable states. Thus, its violation is a sufficient, but not a necessary condition for the inseparability of arbitrary states, including non-Gaussian states. The corresponding inseparability criterion is a nice example for applying the concept of “entanglement witnesses” to continuous variables. An entanglement witness is an observable that can detect the presence of entanglement of a quantum state $\hat{\rho}$. The state $\hat{\rho}$ is entangled if there exists a Hermitian operator $\hat{W}$ such that $\text{Tr}(\hat{W}\hat{\rho}) < 0$, whereas for any separable state $\hat{\rho}$, $\text{Tr}(\hat{W}\hat{\rho}) \geq 0$ holds. The Hermitian operator $\hat{W}$ is then called an *entanglement witness*. Duan *et al.* proved that, for example, the sum of the variances of $\hat{u} \equiv \hat{x}_1 - \hat{x}_2$ and $\hat{v} \equiv \hat{p}_1 + \hat{p}_2$ can never drop below some nonzero bound for any separable state $\hat{\rho}_{12}$. However, for an inseparable state, this total variance may drop to zero. This is possible, because quantum mechanics allows the observables $\hat{u}$ and $\hat{v}$ to simultaneously take on arbitrarily well-defined values due to the vanishing commutator

$$[\hat{x}_1 - \hat{x}_2, \hat{p}_1 + \hat{p}_2] = 0 .$$

In fact, the EPR state from Eq. (9.1) is a simultaneous eigenstate of these two combinations. The proof of Duan’s criterion works as follows. Assume that a given state $\hat{\rho}_{12}$ is separable and hence can be written as in Eq. (9.16). Now we can calculate the total variance of the operators $\hat{u} \equiv \hat{x}_1 - \hat{x}_2$ and $\hat{v} \equiv \hat{p}_1 + \hat{p}_2$ for this state (here labeled by ρ),

$$\begin{aligned} \langle (\Delta \hat{u})^2 \rangle_\rho + \langle (\Delta \hat{v})^2 \rangle_\rho &= \sum_i \eta_i (\langle \hat{u}^2 \rangle_i + \langle \hat{v}^2 \rangle_i) - \langle \hat{u} \rangle_\rho^2 - \langle \hat{v} \rangle_\rho^2 \\ &= \sum_i \eta_i (\langle \hat{x}_1^2 \rangle_i + \langle \hat{x}_2^2 \rangle_i - 2\langle \hat{x}_1 \rangle_i \langle \hat{x}_2 \rangle_i + \langle \hat{p}_1^2 \rangle_i + \langle \hat{p}_2^2 \rangle_i + 2\langle \hat{p}_1 \rangle_i \langle \hat{p}_2 \rangle_i) - \langle \hat{u} \rangle_\rho^2 - \langle \hat{v} \rangle_\rho^2 \\ &= \sum_i \eta_i (\langle (\Delta \hat{x}_1)^2 \rangle_i + \langle (\Delta \hat{x}_2)^2 \rangle_i + \langle (\Delta \hat{p}_1)^2 \rangle_i + \langle (\Delta \hat{p}_2)^2 \rangle_i) \\ &\quad + \sum_i \eta_i \langle \hat{u} \rangle_i^2 - \left(\sum_i \eta_i \langle \hat{u} \rangle_i \right)^2 + \sum_i \eta_i \langle \hat{v} \rangle_i^2 - \left(\sum_i \eta_i \langle \hat{v} \rangle_i \right)^2 , \end{aligned} \quad (9.17)$$

where $\langle \cdots \rangle_i$ means the average in the product state $\hat{\rho}_{i,1} \otimes \hat{\rho}_{i,2}$. Using the Cauchy–Schwarz inequality $\sum_i \eta_i \langle \hat{u} \rangle_i^2 \geq \left(\sum_i \eta_i \langle \hat{u} \rangle_i \right)^2$, one can see that the last line in Eq. (9.17) is bounded below by zero. Considering also the sum uncertainty relation $\langle (\Delta \hat{x}_j)^2 \rangle_i + \langle (\Delta \hat{p}_j)^2 \rangle_i \geq$

$||[\hat{x}_j, \hat{p}_j]| = 1/2$ ($j = 1, 2, \forall i$), we find that the total variance itself is bounded below by 1. Thus, the inequality

$$\langle [\Delta(\hat{x}_1 - \hat{x}_2)]^2 \rangle + \langle [\Delta(\hat{p}_1 + \hat{p}_2)]^2 \rangle \geq 1 \quad (9.18)$$

is a *necessary* condition for any separable state. Any violation of it proves the inseparability of the state in question. For example, the position and momentum correlations of Eq. (9.15) confirm that the two-mode squeezed vacuum state is entangled for any nonzero squeezing $r > 0$. Note that the derivation of Eq. (9.18) does not depend on the assumption of Gaussian states. However, for two-mode Gaussian states in a particular standard form, a condition very similar to that in Eq. (9.18) turns out to be necessary and sufficient for separability [4]. This standard form can be obtained for any two-mode Gaussian state via local Gaussian unitary transformations.

Apart from Duan's criterion, a necessary and sufficient condition for proving the inseparability of two-mode Gaussian states is based on the continuous-variable version of Peres' *partial transpose criterion* [24]. In general, for any separable state as in Eq. (9.16), transposition of either subsystem's density matrix yields again a legitimate nonnegative density operator with unit trace,

$$\hat{\rho}'_{12} = \sum_i \eta_i (\hat{\rho}_{i,1})^T \otimes \hat{\rho}_{i,2} ,$$

since $(\hat{\rho}_{i,1})^T = (\hat{\rho}_{i,1})^*$ corresponds to a legitimate density matrix. This is a necessary condition for a separable state, and hence a single negative eigenvalue of the partially transposed density matrix is a sufficient condition for inseparability. Transposition is a so-called *positive, but not completely positive* map, which means its application to a subsystem may yield an unphysical state when the subsystem is entangled to other subsystems. In general, for states of arbitrary dimension, negative partial transpose (npt) is only sufficient for inseparability [25]. Entangled states with positive partial transpose (ppt) are the so-called *bound entangled states*. However, the class of $(1 \times N)$ - mode Gaussian states belongs to those classes where npt is indeed necessary and sufficient for inseparability [5, 6].

What does partial transposition applied to bipartite Gaussian or, in general, continuous-variable states actually mean? Due to the Hermiticity of a density operator, transposition corresponds to complex conjugation. Moreover, as for the time evolution of a quantum system described by the Schrödinger equation, complex conjugation is equivalent to time reversal, $i\hbar\partial/\partial t \rightarrow -i\hbar\partial/\partial t$. Hence, intuitively, transposition of a density operator means time reversal, or, expressed in terms of continuous variables, sign change of the momenta. Thus, in phase space, transposition is described by $\xi^T \rightarrow \Gamma \xi^T = (x_1, -p_1, x_2, -p_2, \dots, x_N, -p_N)^T$, i.e., by transforming the Wigner function as [5]

$$W(x_1, p_1, x_2, p_2, \dots, x_N, p_N) \longrightarrow W(x_1, -p_1, x_2, -p_2, \dots, x_N, -p_N) .$$

This general transposition rule is, in the case of N -mode Gaussian states, reduced to the transformation

$$V^{(N)} \longrightarrow V^{(N)'} = \Gamma V^{(N)} \Gamma ,$$

for the second-moment correlation matrix (where again the first moments do not affect the entanglement). Now the partial transposition of a bipartite Gaussian system can be expressed by $\Gamma_a \equiv \Gamma \oplus \mathbb{1}$. Here, $A \oplus B$ means the block-diagonal matrix with the matrices A and B as diagonal entries, and A and B are respectively $2N \times 2N$ and $2M \times 2M$ square matrices for N modes at a 's side and M modes at b 's side. According to Eq. (9.6), the condition that the partially transposed Gaussian state described by $\Gamma_a V^{(N+M)} \Gamma_a$ is unphysical,

$$\Gamma_a V^{(N+M)} \Gamma_a \not\geq \frac{i}{4} \Lambda ,$$

is sufficient for the inseparability between a and b [5,6]. For Gaussian states with $N = M = 1$ [5] and for those with $N = 1$ and arbitrary M [6], this condition is necessary and sufficient. For the general bipartite $N \times M$ case of Gaussian states, however, there is also a necessary and sufficient condition: the correlation matrix $V^{(N+M)}$ corresponds to a separable state if and only if a pair of correlation matrices $V_a^{(N)}$ and $V_b^{(M)}$ exists such that [6]

$$V^{(N+M)} \geq V_a^{(N)} \oplus V_b^{(M)} .$$

Since it is in general hard to find such a pair of correlation matrices $V_a^{(N)}$ and $V_b^{(M)}$ for a separable state or to prove the nonexistence of such a pair for an inseparable state, this criterion is not very practical. A more practical solution was proposed by [26]. The operational criteria for Gaussian states there, computable and testable via a finite number of iterations, are entirely independent of the npt criterion. They rely on a *nonlinear* map between the correlation matrices rather than a linear one such as the partial transposition. Moreover, as opposed to the npt criterion, these operational criteria also detect the inseparability of bound entangled states. Therefore, in principle, the separability problem for bipartite Gaussian states with arbitrarily many modes at each side is completely solved.

Let us now consider arbitrary bipartite two-mode states. According to the definition of the N -mode correlation matrix $V^{(N)}$ in Eq. (9.5), we can write the correlation matrix of an arbitrary bipartite two-mode system in block form,

$$V^{(2)} = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} ,$$

where A , B , and C are real 2×2 matrices. Simon's continuous-variable version of the Peres–Horodecki partial transpose criterion now reads [5],

$$\det A \det B + \left(\frac{1}{16} - |\det C| \right)^2 - \text{Tr}(AJCJB JC^T J) \geq \frac{1}{16} (\det A + \det B) , \quad (9.19)$$

where J is the 2×2 matrix from Eq. (9.7). Any separable bipartite state satisfies the inequality of Eq. (9.19), so that it represents a necessary condition for separability. Hence, its violation is sufficient for inseparability. The inequality of Eq. (9.19) is a consequence of the fact that the two-mode uncertainty relation, Eq. (9.6) with $N = 2$, is preserved under partial transpose, $W(x_1, p_1, x_2, p_2) \longrightarrow W(x_1, p_1, x_2, -p_2)$, provided the state is separable.

We may now define the following *standard form* for the correlation matrix of an arbitrary two-mode *Gaussian* state:

$$V_{\text{standard}}^{(2)} = \begin{pmatrix} a & 0 & c & 0 \\ 0 & a & 0 & c' \\ c & 0 & b & 0 \\ 0 & c' & 0 & b \end{pmatrix}. \quad (9.20)$$

This standard form is very useful and important, because it represents a compact description for analyzing the entanglement properties of arbitrary two-mode Gaussian states in terms of only four parameters a , b , c , and c' . Any two-mode correlation matrix can be transformed into this standard form via appropriate local Gaussian unitary transformations [5]. Simon's criterion does not rely on that specific standard form and can be applied to an arbitrary (even non-Gaussian) state using Eq. (9.19). For Gaussian two-mode states, however, Eq. (9.19) turns out to be a *necessary and sufficient* condition for separability [5]. With the standard form $V_{\text{standard}}^{(2)}$ from Eq. (9.20), the condition of Eq. (9.19) then simplifies to

$$16(ab - c^2)(ab - c'^2) \geq (a^2 + b^2) + 2|cc'| - \frac{1}{16}. \quad (9.21)$$

Using Eq. (9.14), one can easily verify that Simon's separability condition in the form of Eq. (9.21) with Eq. (9.20) is violated by a two-mode squeezed state for any $r > 0$.

As for the *quantification* of bipartite mixed-state entanglement, there are various measures available such as the entanglement of formation (EoF) and distillation [27]. Only for pure states do these measures coincide and equal the partial von Neumann entropy. In general, the EoF is hard to compute. However, apart from the qubit case [28], also for symmetric two-mode Gaussian states given by a correlation matrix in Eq. (9.20) with $a = b$, the EoF can be calculated via the total variances in Eq. (9.18) [29]. A Gaussian version of the EoF was proposed by Wolf *et al.* [30]. Another computable measure of entanglement for any mixed state of an arbitrary bipartite system, including bipartite Gaussian states, is the “logarithmic negativity” based on the negativity of the partial transpose [31].

9.4 More on Gaussian Entanglement

Many interesting features of quantum entanglement can be explored within the realm of Gaussian continuous-variable states. In this chapter, we have discussed only a few of them. In particular, we were interested in the *separability* problem for Gaussian states. Other topics on Gaussian entanglement, only briefly or not at all discussed in this chapter, are, for instance, entanglement distillation for Gaussian states [32–35], bound entangled Gaussian states [5, 6], multipartite entangled Gaussian states [7–9], and nonlocality of entangled Gaussian states [10, 11].

Similar to the separability problem, also the *distillability* problem for bipartite Gaussian states of arbitrarily many modes is, in principle, solved. This problem is completely characterized by the partial transpose criterion: any $N \times M$ Gaussian state is distillable if and only if it is npt [26, 36]. A state is distillable if a sufficiently large number of copies of the state can be converted into a pure maximally entangled state (or arbitrarily close to it) via local operations

and classical communication. *Entanglement distillation* [37] is essential for quantum communication. The two halves of a supply of entangled states are normally subject to noise when distributed through realistic quantum channels. Hence, first they must be distilled, before they can be finally used for, for example, high-fidelity quantum teleportation. Bound entangled npt Gaussian states definitely do not exist [26, 36]. Therefore, the set of Gaussian states is fully explored, consisting only of npt distillable, ppt entangled (undistillable), and separable states. The simplest bound entangled Gaussian states are those with two modes at each side. Explicit examples were constructed by Werner and Wolf [6]. Unfortunately, the distillation of npt Gaussian states to maximally entangled finite-dimensional states, though possible in principle [32], is not very feasible with current technology. It relies upon non-Gaussian operations. In fact, the distillation of Gaussian entanglement using only the toolbox of Gaussian operations was shown to be impossible [33–35].

Another interesting topic of entanglement theory is *multipartite entanglement*, the entanglement shared by more than two parties. Such multipartite entanglement can be a useful resource in multiparty quantum communication protocols and networks. Similar to the two-party case, genuinely multiparty entangled Gaussian states can be built from single-mode squeezed states using passive linear transformations [7]. The resulting multimode states exhibit some very distinct properties [9], compared to their discrete qubit counterparts.

Exercises

1. Pure entangled two-mode Gaussian states

- (a) Calculate the correlation matrix of the two-mode state that emerges from a 50/50 beam splitter operation applied to a momentum-squeezed vacuum mode (with squeezing r) and a vacuum mode. Confirm that the resulting state is pure and determine for what squeezing values r it is entangled. [Hint: use the inequality in Eq. (9.18).]
- (b) Quantify the entanglement of the two-mode state derived in (a). (Hint: use local squeezers to transform the state into the canonical two-mode squeezed vacuum state.)

2. Multipartite entanglement and mixed entangled two-mode Gaussian states

Consider the pure symmetric three-mode Gaussian state described by the correlation matrix

$$V^{(3)} = \frac{1}{12} \begin{pmatrix} a & 0 & c & 0 & c & 0 \\ 0 & b & 0 & d & 0 & d \\ c & 0 & a & 0 & c & 0 \\ 0 & d & 0 & b & 0 & d \\ c & 0 & c & 0 & a & 0 \\ 0 & d & 0 & d & 0 & b \end{pmatrix},$$

where $a = e^{+2r} + 2e^{-2r}$, $b = e^{-2r} + 2e^{+2r}$, $c = 2 \sinh 2r$, and $d = -c$. Show that for any $r > 0$ this is a genuinely three-party entangled state, i.e., a state that cannot be written as a product of a single mode with the remaining two modes. (Hint: look at the purity of the reduced states after tracing out one or two modes.) Further check the inseparability properties of the two-mode state after tracing out any one of the three modes.

References

- [1] S. L. Braunstein and A. K. Pati, *Quantum Information with Continuous Variables*, Kluwer Academic Press, Dordrecht, 2003.
- [2] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
- [3] J. Eisert and M. B. Plenio, Int. J. Quant. Inf. **1**, 479 (2003).
- [4] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
- [5] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
- [6] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).
- [7] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000).
- [8] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. A **64**, 052303 (2001).
- [9] G. Adesso, A. Serafini, and F. Illuminati, Phys. Rev. Lett. **93**, 220504 (2004).
- [10] K. Banaszek and K. Wódkiewicz, Phys. Rev. A **58**, 4345 (1998).
- [11] P. van Loock and S. L. Braunstein, Phys. Rev. A **63**, 022106 (2001).
- [12] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
- [13] U. Leonhardt, *Measuring the Quantum State of Light*, Cambridge University Press, Cambridge, MA, 1997.
- [14] E. Schmidt, Math. Ann. **63**, 433 (1906).
- [15] E. P. Wigner, Phys. Rev. **40**, 749 (1932).
- [16] H. Weyl, *The Theory of Groups and Quantum Mechanics*, Dover, New York, 1950.
- [17] B. Demoen, P. Vanheuverzwijn, and A. Verbeure, Lett. Math. Phys. **2**, 161 (1977); Rep. Math. Phys. **15**, 27 (1979).
- [18] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
- [19] S. J. van Enk, Phys. Rev. A **60**, 5095 (1999).
- [20] J. Eisert, C. Simon, and M. B. Plenio, J. Phys. A: Math. Gen. **35**, 3911 (2002).
- [21] G. Giedke, J. Eisert, J. I. Cirac, and M. B. Plenio, Quant. Inf. Comp. **3**, 211 (2003).
- [22] A. Botero and B. Reznik, Phys. Rev. A **67**, 052311 (2003).
- [23] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [24] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [25] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
- [26] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. Lett. **87**, 167904 (2001).
- [27] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [28] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
- [29] G. Giedke, M. M. Wolf, O. Krüger, R. F. Werner, and J. I. Cirac, Phys. Rev. Lett. **91**, 107901 (2003).
- [30] M. M. Wolf, G. Giedke, O. Krüger, R. F. Werner, and J. I. Cirac, Phys. Rev. A **69**, 052320 (2004).
- [31] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002);
K. Zyczkowski, P. Horodecki, A. Sanpera, M. Lewenstein, Phys. Rev. A **58**, 883 (1998);
J. Eisert, PhD thesis (Potsdam University, February 2001).

- [32] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **84**, 4002 (2000).
- [33] J. Eisert, S. Scheel, and M. B. Plenio, *Phys. Rev. Lett.* **89**, 137903 (2002).
- [34] J. Fiurášek, *Phys. Rev. Lett.* **89**, 137904 (2002).
- [35] G. Giedke and J. I. Cirac, *Phys. Rev. A* **66**, 032316 (2002).
- [36] G. Giedke, B. Kraus, L.-M. Duan, P. Zoller, J. I. Cirac, and M. Lewenstein, *Fortschr. Phys.* **49**, 973 (2001).
- [37] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).

10 Entanglement Measures

Martin B. Plenio and Shashank S. Virmani

10.1 Introduction

The concept of *entanglement* has played an important role in quantum physics ever since its discovery last century and has now been recognized as a key resource in quantum information science [1–5]. However, despite its evident importance, entanglement remains an enigmatic phenomenon. One important avenue to understand this enigma is via the study of *entanglement measures*. In this chapter we will discuss the motivation behind this approach, and present the implications of entanglement measures for the study of entanglement in quantum information science. Space limitations mean that there are several interesting results that we will not be able to treat in sufficient detail or that we cannot mention at all. However, we hope that this chapter will give the reader a first glimpse on the subject and will enable them to independently tackle the extensive literature on this topic. Many more details can be found in various review articles [1–6]. The majority of this chapter will concentrate on entanglement in bipartite systems, for which the most complete understanding has been obtained so far, and we will only indicate how to approach the multiparty setting. For a more careful discussion of the multiparty setting we refer the reader to Chapter 13. We will not be able at all to touch upon the study of entanglement in interacting many-body systems which has become an area of active research recently (see, e.g., [7–14]).

Any study of entanglement measures must begin with a discussion of what entanglement *is*, and how we actually *use* it. The term entanglement has become synonymous with highly nonclassical tasks such as violating locality [15], teleportation [16], and dense coding [17], and so for an initial definition we may vaguely say that entanglement is “that property of quantum states that enables these feats.” To flesh out this definition properly we need to consider how we will actually use this entanglement. A typical quantum communication situation in which we use entanglement is as follows: we assume that two distantly separated parties (the proverbial “Alice” and “Bob”) have access to one particle each from a joint quantum state. In addition we assume that they have the ability to communicate classically, and perform arbitrary local operations on their individual particles. These restrictions form the paradigm of *Local Operations and Classical Communication*, or *LOCC* for short. We allow Alice and Bob to communicate classically for two important reasons. Firstly, classical communication can be used to establish classical correlations between sender and receiver. As a consequence the additional power provided by entanglement can then be expected to be due to quantum correlations. Secondly, from a practical point of view, classical communication is also technologically simple, which justifies its addition to the set of essentially free resources.

So, given that we can exploit entangled quantum states using LOCC operations, what are the properties of entangled quantum states that make them so “useful” for the “nonclassical” tasks of quantum information? Unfortunately this question is too simplistic to have a rigorous answer. There is a vast diversity of such “nonclassical” tasks, and just because a state has properties that are “useful” for one task does not mean that it is useful for another. However, despite this variety, it is possible to make a few important remarks that apply generally:

- *Separable states contain no entanglement.* A state $\rho_{ABC\dots}$ of many parties $A, B, C, \dots$ is said to be *separable* [18], if it can be written in the form

$$\rho_{ABC\dots} = \sum_i p_i \rho_A^i \otimes \rho_B^i \otimes \rho_C^i \otimes \dots,$$

where p_i is a probability distribution. These states can trivially be created by LOCC—Alice samples from the distribution p_i , tells all other parties the outcome, and then each party X locally creates ρ_X^i . As these states can be created from scratch by LOCC they trivially satisfy a local hidden variables’ model, and do not allow us to perform teleportation [1] better than we could using LOCC only. Hence, separable states can be said to contain no entanglement and LOCC cannot create entanglement from an unentangled state. Indeed, we even have the following stronger fact.

- *The entanglement of states decreases under LOCC transformations.* Suppose that we know that a certain quantum state ρ can be transformed to another quantum state σ using LOCC operations. Then anything that we can do with σ we can also do with ρ . Hence the utility of quantum states can only decrease under LOCC operations [1, 19–21], and one can say that ρ is more entangled than σ . Note that this definition of “entangled” is implicitly related to the assumption of LOCC restrictions—if other restrictions apply, weaker or stronger, then our notion of “more entangled” is also likely to change.
- *Entanglement does not change under local unitary operations.* This is because local unitaries can be inverted by local unitaries. Hence, by the nonincrease of entanglement under LOCC, two states related by local unitaries have equivalent entanglement.
- *In two party systems consisting of two d -dimensional systems, the pure states local unitarily equivalent to $|\psi_d^+\rangle = \frac{1}{\sqrt{d}}(|0, 0\rangle + |1, 1\rangle + \dots + |d-1, d-1\rangle)$ are maximally entangled.* This is well justified, because as we shall see later, any pure or mixed state of two d -dimensional systems can be reached from such states using only LOCC operations.

The above considerations have given us the extremes of Entanglement—as long as we consider LOCC as our definitive set of operations, separable states contain zero entanglement, and we can identify certain states that have maximal entanglement. They also suggest that we can impose some form of ordering—we may say that state ρ is more entangled than a state σ if we can perform the transformation $\rho \rightarrow \sigma$ using LOCC operations. A key question is whether this method of ordering gives a partial or total order? To answer this question we must try and find out when one quantum state may be transformed to another using LOCC operations. We will consider this question in more detail in the next part, where we will find that in general LOCC ordering only results in a partial order.

This means that in general an LOCC-based classification of entanglement is extremely complicated. However, one can obtain a more digestible classification by making extra demands on our definition of entanglement. By adding extra ingredients, one can obtain real-valued functions that attempt to *quantify* the amount of entanglement in a given quantum state. This is essentially the process that is followed in the definition of entanglement measures. Various entanglement measures have been proposed over the years, such as the entanglement of distillation [19, 25], the entanglement cost [19, 27–29], the relative entropy of entanglement [20, 21], and the squashed entanglement [31]. Some of these have direct physical significance, whereas others are axiomatic quantities. The initial advantage of these measures was that they gave a physically motivated classification of entanglement that is simple to understand. However, they have also developed into powerful mathematical tools, with major significance for open questions such as the additivity of channel capacities [22, 23]. We will return to the development of entanglement measures later, but we must first understand in more detail some essential aspects of the manipulation of quantum states under local operations and classical communication.

10.2 Manipulation of Single Systems

In the previous section we had indicated that for bipartite systems there is a notion of maximally entangled states that is independent of the specific quantification of entanglement. This is so, because there are states from which all others can be created by LOCC only. We consider here the case of two two-level systems and leave the generalization as an exercise to the reader. The maximally entangled states then take the form

$$|\psi_2^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Our aim is now to justify this statement by showing that for any pure state

$$|\phi\rangle = \alpha|00\rangle + \beta|11\rangle$$

we can find a LOCC map that takes $|\psi_2^+\rangle$ to $|\phi\rangle$ with certainty. To this end we simply need to write the Kraus operators of a valid operation. Clearly,

$$K_0 = (\alpha|0\rangle\langle 0| + \beta|1\rangle\langle 1|) \otimes \mathbb{1}, \quad K_1 = (\beta|1\rangle\langle 0| + \alpha|0\rangle\langle 1|) \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|)$$

satisfies $K_0^\dagger K_0 + K_1^\dagger K_1 = \mathbb{1}$ and $K_i|\psi\rangle \sim |\phi\rangle$. It is a worthwhile exercise to try and construct this operation by adding ancillas to the systems, carrying out local unitary operations, followed by projective measurements and classical communication. Given that we can obtain with certainty any arbitrary pure state starting from $|\psi_2^+\rangle$ we can also obtain any mixed state ρ . This is because $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ where $|\phi_i\rangle = U_i \otimes V_i (\alpha_i|00\rangle + \beta_i|11\rangle)$ with unitaries U_i and V_i . It is an easy exercise, left to the reader, to construct the operation that takes $|\psi_2^+\rangle$ to ρ .

A natural next question to consider is the LOCC transformation between general pure states of two parties [33]. Indeed, a mathematical framework based on the theory of majorization has been developed that provides necessary and sufficient conditions for the interconversion between two pure states, together with protocols that achieve the task [34, 35, 37]. Let us

write the initial and final state vectors as $|\psi_1\rangle$ and $|\psi_2\rangle$ in their Schmidt basis,

$$|\psi_1\rangle = \sum_{i=1}^n \sqrt{\alpha_i} |i_A\rangle |i_B\rangle, \quad |\psi_2\rangle = \sum_{i=1}^m \sqrt{\alpha'_i} |i'_A\rangle |i'_B\rangle,$$

where n denotes the dimension of each of the quantum systems. We can take the Schmidt coefficients to be given in decreasing order, i.e., $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$ and $\alpha'_1 \geq \alpha'_2 \geq \dots \geq \alpha'_m$. The question of the interconvertability between the states can then be decided from the knowledge of the real Schmidt coefficients only. One finds that a LOCC transformation that converts $|\psi_1\rangle$ to $|\psi_2\rangle$ with unit probability exists if and only if the $\{\alpha_i\}$ are majorized [38] by $\{\alpha'_i\}$, that is, exactly if for all $1 \leq l \leq n$

$$\sum_{i=1}^l \alpha_i \leq \sum_{i=1}^l \alpha'_i.$$

Various refinements of this result have been found that provide the largest success probabilities for the interconversion between two states by LOCC together with the optimal protocol where a deterministic interconversion is not possible [35, 37]. These results allow in principle to decide any question concerning the LOCC interconversion of pure state by employing techniques from linear programming [37]. Although the basic mathematical structure is well understood, surprising and not yet fully understood effects such as entanglement catalysis are still possible [40]. It is a direct consequence of the above structures that there are *incomparable* states, i.e., pairs of states such that neither can be converted into the other with certainty. These states are called incomparable as neither can be viewed as more entangled than the other. The following part will serve to overcome this problem for pure states.

10.3 Manipulation in the Asymptotic Limit

The study of the LOCC transformation of pure states so far has enabled us to justify the concept of maximally entangled states and also permitted, in some cases, to assert that one state is more entangled than another. However, we know that exact LOCC transformations can only induce a partial order on the set of quantum states. The situation is even more complex for *mixed* states, where even the question of the transformation from one state into another by LOCC is a difficult problem with no transparent solution.

All this means that if we want to give a definite answer as to whether one state is more entangled than another for any pair of states, it will be necessary to consider a more general setting. In this context a very natural way to quantify entanglement is to study LOCC transformations of states in the so-called *asymptotic regime*. Instead of asking whether an single initial state ρ may be transformed to a final state σ by LOCC operations, we may ask whether for some large integers m, n we can implement the “wholesale” transformation $\rho^{\otimes n} \rightarrow \sigma^{\otimes m}$ to a high level of *approximation*. In a loose sense that will be made more rigorous later, we may use the optimal possible rate of transformation m/n as a measure of how much more (or less) entanglement ρ has as compared to σ . This asymptotic setting may be viewed as a limiting case of the above theorems for arbitrarily high dimensions, and indeed predated it [19].

It turns out that in the pure state case the study of the asymptotic regime gives a very natural measure of entanglement that is essentially unique.

To understand the asymptotic regime precisely, we first need to understand the issue of *approximation*. In principle we could ask what the optimal rate of conversion m/n is for *exact* transformations of the form $\rho^{\otimes n} \rightarrow \sigma^{\otimes m}$. However, from the theorems of the previous section we know that exact pure state transformations are not always possible with LOCC. Therefore, the fact that there are incomparable pure states means that we will not be able to use asymptotic conversion rates to quantify entanglement for all states unless we admit some form of imperfection. One way to admit such imperfections is to allow transformations such that for finite n the output only approximates the target according to a suitably chosen distance measure, such that these imperfections vanish in the limit $n \rightarrow \infty$. From a physical point of view allowing such approximate transformations is quite acceptable, as vanishingly small imperfections will not affect observations of the output in any perceptible way.

Let us formalize these notions for one of the most important entanglement measures, the *entanglement cost*, $E_C(\rho)$. For a given state ρ this measure quantifies the maximal possible rate at which one can convert input maximally entangled states of two qubits into output states that approximate ρ . If we denote a general trace preserving LOCC operation by Ψ , and write $\Phi(K)$ for the density operator corresponding to the maximally entangled state vector in K dimensions, i.e., $\Phi(K) = |\psi_K^\pm\rangle\langle\psi_K^\pm|$, then the entanglement cost may be defined as

$$E_C(\rho) = \inf \left\{ r : \lim_{n \rightarrow \infty} \left[\inf_{\Psi} D(\rho^{\otimes n}, \Psi(\Phi(2^{rn}))) \right] = 0 \right\},$$

where $D(x, y)$ is a suitable measure of distance. A variety of possible distance measures may be proposed, but two natural choices are the trace distance or the Bures distance [38, 56], as these functions can be used to bound the statistical differences between two states. It has been shown that the definition of entanglement cost is independent of the choice of distance function, as long as these functions are equivalent in a way that is independent of dimension (see [29] for further explanation), and so we will fix the trace norm as our choice for $D(x, y)$.

The entanglement cost is an important measure because it quantifies a wholesale “exchange rate” for converting from maximally entangled states to copies of ρ , and maximally entangled states are in essence the “gold standard currency” with which one would like to compare all quantum states. Although computing $E_C(\rho)$ is extremely difficult, we will later discuss its important implications for the study of channel capacities, in particular via another important entanglement measure known as the *entanglement of formation*, $E_F(\rho)$.

In addition to the entanglement cost, another important asymptotic entanglement measure is the *distillable entanglement*, $D(\rho)$, which is a kind of dual measure to the entanglement cost. Just as $E_C(\rho)$ measures how many maximally entangled states are required to create copies of ρ , we can ask about the reverse process: at what rate may we obtain maximally entangled states (of two qubits) from an input supply of ρ . This process is known in the literature either as *entanglement distillation*, or as *entanglement concentration*. Again we allow the output of the procedure to approximate many copies of a maximally entangled state, as the exact transformation from $\rho^{\otimes n}$ to even one singlet state is in general impossible [39]. In analogy to the definition of $E_C(\rho)$, we can make the precise mathematical definition of $D(\rho)$ as

$$D(\rho) := \sup \left\{ r : \lim_{n \rightarrow \infty} \left[\sup_{\Psi} \text{tr} |\Psi(\rho^{\otimes n}) - \Phi(2^{rn})| \right] = 0 \right\}.$$

$D(\rho)$ is an important measure because if entanglement is required in a two party quantum information protocols, then it is usually required in the form of maximally entangled states. So $D(\rho)$ tells us the rate at which noisy mixed states may be converted back into the “gold standard” singlet states. In defining $D(\rho)$ we have overlooked a couple of important issues. Firstly, our LOCC protocols are always taken to be trace preserving. However, one could conceivably allow probabilistic protocols that have varying degrees of success depending upon various measurement outcomes. Fortunately, a thorough paper by Rains [25] shows that taking into account a wide diversity of possible success measures still leads to the same notion of distillable entanglement. Secondly, we have always used two qubits maximally entangled states as our “gold standard,” if we use other entangled *pure* states, perhaps even on higher dimensions, do we arrive at significantly altered definitions? We will very shortly see that this is not the case, and there is no loss of generality in taking singlet states as our target.

A remarkable feature of the asymptotic transformations regime is that pure state transformations become *reversible*. Indeed, for pure states it turns out that both $D(\rho)$ and $E_C(\rho)$ are identical and equal to the entropy of entanglement [19], which for a pure state $|\psi\rangle$ is defined as

$$E(|\psi\rangle\langle\psi|) := (S \circ \text{tr}_B)(|\psi\rangle\langle\psi|) = D(|\psi\rangle\langle\psi|) = E_C(|\psi\rangle\langle\psi|),$$

where S denotes the von-Neumann entropy $S(\rho) = -\text{tr}[\rho \log_2 \rho]$, and tr_B denotes the partial trace over subsystem B. This reversibility means that in the asymptotic regime we may immediately write the optimal rate of transformation between *any* two pure states $|\psi_1\rangle$ and $|\psi_2\rangle$. Given a large number N of copies of $|\psi_1\rangle\langle\psi_1|$, we can first distill $\approx NE(|\psi_1\rangle\langle\psi_1|)$ singlet states and then create from those singlets $M \approx NE(|\psi_1\rangle\langle\psi_1|)/E(|\psi_2\rangle\langle\psi_2|)$ copies of $|\psi_2\rangle\langle\psi_2|$. In the infinite limit these approximations become exact, and as a consequence $E(|\psi_1\rangle\langle\psi_1|)/E(|\psi_2\rangle\langle\psi_2|)$ is the optimal asymptotic conversion rate from $|\psi_1\rangle\langle\psi_1|$ to $|\psi_2\rangle\langle\psi_2|$. It is the reversibility of pure state transformations that enables us to define $D(\rho)$ and $E_C(\rho)$ in terms of transformations to or from singlet states—use of any other entangled state (in any other dimensions) simply leads to a constant factor multiplied in front of these quantities.

Following these basic considerations we are now in a position to formulate a more rigorous and axiomatic approach to entanglement measures that try to capture the lessons that have been learned in the previous sections. In the final section we will then review several entanglement measures and discuss their significance for various topics in quantum information.

10.4 Postulates for Axiomatic Entanglement Measures: Uniqueness and Extremality Theorems

In the previous section we considered the quantification of entanglement from the perspective of LOCC transformations in the asymptotic limit. This approach is interesting because it can be solved completely for pure states, and leads to two of the most important entanglement measures for mixed states—the distillable entanglement and entanglement cost. However, computing these measures is extremely difficult for mixed states, and so in this section we will discuss a more axiomatic approach to quantifying entanglement. This approach has proven

very fruitful: among other applications axiomatic entanglement measures have been used to assess the quality of entangled states produced in experiments, to understand the behavior of correlations during quantum phase transitions, to bound fault tolerance thresholds in quantum computation, and derive several interesting results in the study of channel capacities.

So what exactly are the properties that a good entanglement measure should possess? An entanglement measure is a mathematical quantity that should capture the essential features that we associate with entanglement, and ideally should be related to some operational procedure. Depending upon your aims, this can lead to variety of possible desirable properties. The following is a list of possible postulates for entanglement measures, some of which are not satisfied by all proposed quantities [21, 59]:

1. A *bipartite* entanglement measure $E(\rho)$ is a mapping:

$$\rho \rightarrow E(\rho) \in \mathbb{R}^+$$

defined for states of arbitrary bipartite systems. A normalization factor is also usually included such that the singlet state $|\psi^-\rangle$ of two qubits has $E(|\psi^-\rangle\langle\psi^-|) = 1$.

2. $E(\rho) = 0$ if the state ρ is separable.
3. E does not increase on average under LOCC, i.e.,

$$E(\rho) \geq \sum_i p_i E(\rho_i),$$

where in a LOCC protocol applied to state ρ the state ρ_i with label i is obtained with probability p_i .

4. For pure state $|\psi\rangle\langle\psi|$ the measure reduces to the entropy of entanglement

$$E(|\psi\rangle\langle\psi|) = (S \circ \text{tr}_B)(|\psi\rangle\langle\psi|).$$

We will call any function E satisfying the first three conditions an *entanglement monotone*, usually reserving the term *entanglement measure* only for quantities satisfying the fourth condition. In the literature these terms are often used interchangeably. Frequently, some authors also impose additional requirements for entanglement measures. One common example is requiring convexity, i.e., $E(\sum_i p_i \rho_i) \leq \sum_i p_i E(\rho_i)$. This mathematically very convenient property is sometimes justified as capturing the notion of the loss of information, i.e., describing the process of going from a selection of identifiable states ρ_i that appear with rates p_i to a mixture of these states of the form $\rho = \sum_i p_i \rho_i$. We would like to stress, however, that this particular requirement is not essential. Indeed, in the first situation, before the loss of information about the state, the whole ensemble can be described by the single quantum state

$$\sum_i p_i |i\rangle_M \langle i| \otimes \rho_i^{AB},$$

where $\{|i\rangle_M\}$ denote some orthonormal basis belonging to one party. Clearly a measurement of the marker particle M reveals the identity of the state of parties A and B . The process of the

forgetting is then described by tracing out the marker particle M to obtain $\rho = \sum p_i \rho_i$ [41]. Therefore we can require that $E(\sum_i p_i |i\rangle_M \langle i| \otimes \rho_i^{AB}) \geq E(\rho)$, which is already captured by condition 3 above. Hence there is no need to require convexity, except for the mathematical simplicity that it might bring.

The first three conditions listed above seem quite natural—the first two conditions are little more than setting the scale, and the third condition is a generalization of the idea that entanglement can only decrease under LOCC operations to incorporate probabilistic transformations. The fourth condition may seem a little strong. However, it turns out that it is also quite a natural condition to impose. The fact that $S(\rho_A)$ represents the reversible rate of conversion between pure states in the asymptotic regime actually forces any entanglement monotone that is (a) additive on pure states, and (b) sufficiently continuous, to be equal to $S(\rho_A)$ on the pure states. A very rough argument is as follows. We know from the asymptotic pure state distillation protocol that from n copies of a pure state $|\phi\rangle$ we can obtain a state ρ_n that closely approximates the state $|\psi^-\rangle^{\otimes nE(|\phi\rangle)}$ to within ϵ , where $E(|\phi\rangle)$ is the entropy of entanglement of $|\phi\rangle$. Suppose therefore that we have an entanglement monotone L that is *additive* on pure states. Then we may write

$$nL(|\phi\rangle) = L(|\phi\rangle^{\otimes n}) \geq L(\rho_n).$$

If the monotone L is sufficiently continuous, then $L(\rho_n) = L(|\psi^-\rangle^{\otimes nE(|\phi\rangle)}) + \delta(\epsilon) = nE(|\phi\rangle) + \delta(\epsilon)$, where $\delta(\epsilon)$ will be small. Then we obtain

$$L(|\phi\rangle) \geq E(|\phi\rangle) + \frac{\delta(\epsilon)}{n}.$$

If the function L remains sufficiently continuous as the dimension increases then $\delta(\epsilon)/n \rightarrow 0$, and we obtain $L(|\phi\rangle) \geq E(|\phi\rangle)$. We will see a little later exactly what *sufficiently continuous* means. Invoking the fact that the entanglement cost for pure states is also given by the entropy of entanglement gives the reverse inequality $L(|\phi\rangle) \leq E(|\phi\rangle)$ using similar arguments. Hence sufficiently continuous monotones that are additive on pure states will naturally satisfy $L(|\phi\rangle) = E(|\phi\rangle)$. Of course these arguments are not rigorous, as we have not undertaken a detailed analysis of how δ or ϵ grow with n . A rigorous analysis is presented in [59], where it is also shown that our assumptions may be slightly relaxed. The result of this rigorous analysis is that a function is equivalent to the entropy of entanglement on pure states *if and only if* it is (a) normalized on the singlet state, (b) additive on pure states, (c) nonincreasing on *deterministic* pure state to pure state LOCC transformations, and (d) *asymptotically continuous* on pure states. The term *asymptotically continuous* is defined as the property

$$\frac{L(|\phi\rangle_n) - L(|\psi\rangle_n)}{1 + \log(\dim H_n)} \rightarrow 0$$

whenever the trace norm $\| |\phi\rangle\langle\phi|_n - |\psi\rangle\langle\psi|_n \|$ between two sequences of states $|\phi\rangle_n, |\psi\rangle_n$ on a sequence of Hilbert spaces $H_n \otimes H_n$ tends to 0 as $n \rightarrow \infty$. It is interesting to note that these constraints only concern pure state properties of L , and that they are *necessary and sufficient*. It is interesting to note that any monotones that satisfy (a)–(d) cannot have qualitative agreement with each other, i.e., imposing the same order on states, unless they are exactly the same [24] (see [52] for ordering results for other entanglement quantities).

In addition to the above uniqueness theorem, it turns out that similar arguments may be used to show that the entanglement cost $E_C(\rho)$ and the distillable entanglement $D(\rho)$ are in some sense *extremal* measures [59, 60], in that they are upper and lower bounds for many “wholesale” entanglement monotones. To be precise, suppose that we have a quantity $L(\rho)$ satisfying conditions (1)–(3), that is also asymptotically continuous on mixed states, and also has a *regularization*:

$$\lim_{n \rightarrow \infty} \frac{L(\rho^{\otimes n})}{n}.$$

Then it can be shown that

$$E_C(\rho) \geq \lim_{n \rightarrow \infty} \frac{L(\rho^{\otimes n})}{n} \geq D(\rho).$$

Equations such as these may be useful for deriving upper bounds on $D(\rho)$. However, the resulting bounds may be very difficult to calculate if the entanglement measures involved are defined as variational quantities. In this context it is important to mention a quantity known as the *conditional entropy*, which is defined as $C(A|B) := S(\rho_{AB}) - S(\rho_B)$ for a bipartite state ρ_{AB} . It was known for some time that $-C(A|B)$ gives a lower bound for both the entanglement cost and another important measure known as the *relative entropy of entanglement* [42]. This bound was also recently shown to be true for the one way distillable entanglement:

$$D(\rho_{AB}) \geq D_{A \rightarrow B}(\rho_{AB}) \geq \max\{S(\rho_B) - S(\rho_{AB}), 0\},$$

where $D_{A \rightarrow B}$ is the distillable entanglement under the restriction that the classical communication may only go one way from Alice to Bob [43]. This bound is known as the *Hashing inequality*, and is significant as it is a computable, nontrivial, *lower bound* to $D(\rho)$, and hence supplies a nontrivial lower bound to many other entanglement measures.

10.5 Examples of Axiomatic Entanglement Measures

In this section we discuss a variety of the bipartite axiomatic entanglement measures that have been proposed in the literature. All the following quantities are entanglement *monotones*, in that they cannot increase under LOCC, and hence when they can be calculated, can be used to determine whether certain LOCC transformations are possible, often both in the finite and asymptotic regimes. However, some measures have a wider significance, that we will discuss as they are introduced. Note that the list of entanglement measures mentioned here is only a subset of many proposals. We have selected this list of measures on the basis of those with which we are most familiar, and there are many other important approaches that we are not able to discuss in detail.

- *Entanglement of formation*. For a mixed state ρ this measure is defined as

$$E_F(\rho) := \inf \left\{ \sum_i p_i E(|\psi_i\rangle\langle\psi_i|) \mid \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \right\}.$$

The heuristic motivation for this measure is that it is the minimal possible average entanglement over all pure state decompositions of ρ , where $E(|\psi\rangle\langle\psi|) = S(\text{tr}_B\{|\psi\rangle\langle\psi|\})$ is taken as the measure of entanglement for pure states. The variational problem that defines E_F is extremely difficult to solve. However, closed solutions are known for two-qubit states, and for certain cases of symmetry [28]. The *regularized* or *asymptotic* version of the entanglement of formation is defined as $E_F^\infty(\rho) := \lim_{n \rightarrow \infty} \frac{E_F(\rho^{\otimes n})}{n}$. The regularized version is important as it can be rigorously shown to be equal to the entanglement cost [29]

$$E_F^\infty(\rho) = E_C(\rho).$$

A *major* open question in quantum information is to decide whether E_F is an additive quantity, i.e., whether:

$$E_F(\rho^{AB} \otimes \sigma^{AB}) = E_F(\rho^{AB}) + E_F(\sigma^{AB}).$$

This problem is known to be equivalent to the *strong superadditivity* of E_F

$$E_F(\rho_{12}^{AB}) \stackrel{?}{\geq} E_F(\rho_1^{AB}) + E_F(\rho_2^{AB}).$$

The major importance of these additivity problems stems not only from the fact that they would show that $E_F = E_C$, but also because they are *equivalent* to *both* the additivity of the minimal output entropy of quantum channels, *and* the additivity of the classical communication capacity of quantum channels!

E_F is an important example of a *convex roof* construction. The convex roof of a function f that is defined on the extremal points of a convex set is the largest convex function that matches f on the extreme points. It is easy to see that E_F is the convex roof of the entropy of entanglement, and is hence the largest of all convex functions that agree with $S(\rho_A)$ on the pure states. The convex roof method can be used to construct entanglement monotones from any unitarily invariant (including isometric embeddings) concave function of density matrices [36].

- *Relative entropy of entanglement* [20, 21, 42]. An intuitive way of constructing an entanglement measure is to quantify how difficult it is to discriminate an entangled state from a set X of disentangled states. The relative entropy is one way of quantifying this. For two quantum states ρ, σ it is defined as

$$S(\rho|\sigma) := -S(\rho) - \text{tr}\{\rho \log \sigma\}.$$

So a natural entanglement measure, dependent upon the choice of X , is

$$E_R^X(\rho|\sigma) := \inf_{\sigma \in X} S(\rho|\sigma).$$

This definition leads to a class of entanglement measures known as the *relative entropies of entanglement*. In the bipartite setting the set X can be taken as the set of separable, PPT, or nondistillable states, depending upon your favorite definition of disentangled. In

the multipartite setting there are even more possibilities [44, 45]. In the bipartite setting the measures E_R^X are equal to the entropy of entanglement for bipartite pure states. The bipartite relative entropies have been used to compute tight upper bounds to the distillable entanglement of certain states, and as an invariant to help decide the asymptotic interconvertibility of multipartite states.

The relative entropy measures are known in general not to be additive, as bipartite states can be found where

$$E_R^X(\rho^{\otimes n}) \neq nE_R^X(\rho).$$

In some such cases the regularized versions of some relative entropy measures can be calculated [46, 47].

The relative entropy functional is only one possible “distinguishability measure” between states, and in principle one could use other distance functions to quantify how far a particular state is from a chosen set of disentangled states. Many interesting examples of other functions that can be used for this purpose may be found in the literature (see, e.g., [20, 26]). It is also worth noting that the relative entropy functional is *asymmetric*, in that $S(\rho|\sigma) \neq S(\sigma|\rho)$. This is connected with asymmetries that can occur in the discrimination of probability distributions [21]. One can consider reversing the arguments and tentatively define an LOCC monotone $J^X(\rho) := \inf\{S(\sigma|\rho) | \sigma \in X\}$. The resulting function has the advantage of being additive, but unfortunately it has the problem that it can be infinite on pure states [48].

- *Logarithm of the negativity.* The partial transposition with respect to party B of a bipartite state ρ_{AB} expanded in given local orthonormal basis as $\rho = \sum \rho_{ij,kl} |i\rangle\langle j| \otimes |k\rangle\langle l|$ is defined as

$$\rho^{T_B} := I \otimes T_B(\rho) := \sum_{i,j,k,l} \rho_{ij,kl} |i\rangle\langle j| \otimes |l\rangle\langle k|.$$

The spectrum of the partial transposition of a density matrix is independent of the choice of local basis, and is independent of whether the partial transposition is taken over party A or party B . The positivity of the partial transpose of a state is a necessary condition for separability, and is sufficient to prove that $D(\rho) = 0$ for a given state. The quantity known as the *Negativity* [51, 52], $N(\rho)$, is an entanglement monotone [53, 54] that attempts to quantify the negativity in the spectrum of the partial transpose. We will define the Negativity as

$$N(\rho) := \|\rho^{T_B}\|,$$

where $\|X\| := \text{tr}\sqrt{X^\dagger X}$ is the trace norm. Note that many authors define the Negativity differently as $(\|\rho^{T_B}\| - 1)/2$. With the convention that we follow, the *Logarithm of the Negativity* is defined as

$$E_N(\rho) := \log \|\rho^{T_B}\| = \log(N(\rho)).$$

E_N is an entanglement monotone that cannot increase under deterministic LOCC operations, as well as on average under probabilistic LOCC transformations. It is additive by construction, and convex due to its monotonic relationship to a norm. Although E_N is manifestly continuous, it is not asymptotically continuous, and hence does not reduce to the entropy of entanglement on all pure states. Later we will see that $N(\rho)$ is part of a larger family of monotones that be constructed in a similar way.

The major practical advantage of E_N is that it can be calculated very easily; however, it also has various operational interpretations as an upper bound to $D(\rho)$, a bound on teleportation capacity [54], and an asymptotic entanglement cost under the set of PPT operations [49].

E_N can also be combined with a relative entropy approach to give another monotone known as the *Rains' Bound* [55], which is defined as:

$$B(\rho) := \min_{\text{all states } \sigma} [S(\rho|\sigma) + E_N(\sigma)]$$

One can see that almost by definition $B(\rho)$ is a lower bound to $E_R^{PPT}(\rho)$, and it can also be shown that it is an upper bound to the distillable entanglement. It is interesting to observe that for Werner states $B(\rho)$ happens to be equal to $\lim_{n \rightarrow \infty} E_R^{PPT}(\rho^{\otimes n})/n$ [46, 55], a connection that has been explored in more detail in [47, 49, 50].

- *Norm-based monotones.*

In [54] it was noted that the Negativity described above is part of a general family of entanglement monotones (related to an even wider concept known as a *base norm*). To construct this family we require two sets X, Y of Hermitian matrices satisfying the following conditions: (a) X, Y are closed under LOCC operations (even measuring ones), (b) X, Y are convex cones (i.e., also closed under multiplication by nonnegative scalars), and (c) any Hermitian operator h may be expanded as

$$h = a\Omega - b\Delta,$$

where $\Omega \in X, \Delta \in Y$ are normalized (i.e., trace 1) but not necessarily positive, and $a, b \geq 0$. Given two such sets X, Y and any Hermitian operator h we may define

$$R_{X,Y}(h) := \inf_{\Omega \in X, \Delta \in Y} \{b \mid h = a\Omega - b\Delta, a, b \geq 0\}$$

$$\|h\|_{X,Y} := \inf_{\Omega \in X, \Delta \in Y} \{a + b \mid h = a\Omega - b\Delta, a, b \geq 0\}$$

Note that for when ρ is a state (i.e., positive, trace 1), the first of these functions $R_{X,Y}$ may be rewritten as

$$\begin{aligned} R_{X,Y}(\rho) &= \inf \{b \mid b \geq 0, \exists \Delta \in Y, \Omega \in X \text{ such that } \frac{\rho + b\Delta}{1+b} = \Omega\} \\ &= \frac{\|h\|_{X,Y} - 1}{2}. \end{aligned}$$

From this equation we see if Ω, Δ are also states, then $R_{X,Y}$, which is monotonically related to $R_{X,Y}/(1 + R_{X,Y})$, quantifies the minimal noise of type Y that must be mixed with ρ to give a state of the form X . For this reason we will refer to quantities of the type of $R_{X,Y}(\rho)$ as *robustness monotones*. It can be shown that the restrictions on X, Y force $R_{X,Y}(\rho)$ to be convex, $\|h\|_{X,Y}$ to be a norm, and both quantities to be LOCC monotones.

Examples of robustness monotones are the “*robustness*,” where both X, Y are the set of separable states, and the “*global robustness*,” where X is the set of separable states and Y is the set of all states [61, 62] (note that the “*random robustness*” is not a monotone, for definition and proof see [61]). These monotones can often be calculated or at least bounded nontrivially, and have found applications in areas such as bounding fault tolerance [61, 62]. The Negativity introduced above also fits into this class of monotones—it is simply $\|\rho\|_{X,Y}$ where both X, Y are the set of normalized Hermitian matrices with positive partial transposition.

Another form of norm-based entanglement monotone is the *cross norm* monotone proposed in [30]. The *greatest cross norm* of an operator A is defined as

$$\|A\|_\gamma := \inf \left[\sum_{i=1}^n \|u_i\|_1 \|v_i\|_1 : A = \sum_i u_i \otimes v_i \right], \quad (10.1)$$

where $\|y\|_1 := \text{tr}\{\sqrt{y^\dagger y}\}$ is the trace norm, and the infimum is taken over all decompositions of A into finite sums of product operators. It can be shown that a density matrix ρ_{AB} is separable iff $\|\rho\|_\gamma = 1$, and that the quantity

$$E_\gamma(\rho) := \|\rho\|_\gamma - 1$$

is an entanglement monotone [30]. As it is expressed as a complicated variational expression, $E_\gamma(\rho)$ can be difficult to calculate. However, for pure states and cases of high symmetry it may often be computed exactly. Although $E_\gamma(\rho)$ does not fit precisely into the family of base norm monotones discussed above, there is a relationship. If the sum in (10.1) is restricted to *Hermitian* u_i and v_i , then we recover precisely the base norm $\|A\|_{X,Y}$, where X, Y are taken as the set of separable states. Hence E_γ is an upper bound to the robustness [30].

- *Squashed entanglement*. The “squashed” entanglement [31] (see also [32]) is a recently proposed measure that is defined as

$$E_{\text{sq}} := \inf \left[\frac{1}{2} I(\rho_{ABE}) \mid \text{tr}_E\{\rho_{ABE}\} = \rho_{AB} \right]$$

$$\text{where } I(\rho_{ABE}) := S(AE) + S(BE) - S(ABE) - S(E).$$

In this definition $I(\rho_{ABE})$ is the *quantum conditional mutual information*, which is often also denoted as $I(A; B|E)$. The squashed entanglement is a convex entanglement monotone that is a lower bound to $E_F(\rho)$ and an upper bound to $D(\rho)$, and is hence automatically equal to $S(\rho_A)$ on pure states. It is also additive on tensor products, and

is hence a useful nontrivial lower bound to $E_C(\rho)$. The intuition behind E_{sq} is that it “squashes out” the classical correlations between Alice, Bob, and the third party Eve, an idea motivated by related quantities in classical cryptography.

Acknowledgments This work is part of the QIP-IRC (www.qipirc.org) supported by EPSRC (GR/S82176/0) as well as the EU (IST-2001-38877) the Leverhulme Trust, and the Royal Commission for the Exhibition of 1851.

References

- [1] M.B. Plenio and V. Vedral, *Contemp. Phys.* **39**, 431 (1998).
- [2] B. Schumacher, *Preprint* quant-ph/0004045.
- [3] M. Horodecki, *Quant. Inf. Comp.* **1**, 3 (2001).
- [4] P. Horodecki and R. Horodecki, *Quant. Inf. Comp.* **1**, 45 (2001).
- [5] J. Eisert and M.B. Plenio, *Int. J. Quant. Inf.* **1**, 479 (2003).
- [6] M.B. Plenio and S. Virmani, *Preprint* quant-ph/0504163 to appear in *Quant. Inf. Comp.* January 2007.
- [7] K. Audenaert, J. Eisert, M.B. Plenio and R.F. Werner, *Phys. Rev. A* **66**, 042327 (2002).
- [8] A. Botero and B. Reznik, *Phys. Rev. A* **70**, 052329 (2004).
- [9] H. Carteret, *Preprint* quant-ph/0405168.
- [10] J. Eisert, M.B. Plenio, S. Bose and J. Hartley, *Phys. Rev. Lett.* **93**, 190402 (2004)
- [11] F. Verstraete, M.-A. Martin-Delgado and J.I. Cirac, *Phys. Rev. Lett.* **92**, 087201 (2004)
- [12] J.K. Pachos and M.B. Plenio, *Phys. Rev. Lett.* **93**, 056402 (2004).
- [13] M.B. Plenio, J. Eisert, J. Dreißig and M. Cramer, *Phys. Rev. Lett.* **94**, 060503 (2005).
- [14] M. Cramer, J. Eisert, M.B. Plenio and J. Dreißig, *Phys. Rev. A* **73**, 012309 (2006).
- [15] J.S. Bell, *Physics* **1**, 195 (1964).
- [16] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [17] C.H. Bennett and S. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
- [18] R.F. Werner, *Phys. Rev. A* **40**, 4277 (1989).
- [19] C.H. Bennett, H. Bernstein, S. Popescu and B. Schumacher, *Phys. Rev. A* **53**, 2046 (1996).
- [20] V. Vedral, M.B. Plenio, M.A. Rippin and P.L. Knight, *Phys. Rev. Lett.* **78**, 2275 (1997).
- [21] V. Vedral and M.B. Plenio, *Phys. Rev. A* **57**, 1619 (1998).
- [22] P.W. Shor, *Commun. Math. Phys.* **246**, 453 (2004).
- [23] K.M.R. Audenaert and S.L. Braunstein, *Commun. Math. Phys.* **246**, 443 (2003).
- [24] S. Virmani and M.B. Plenio, *Phys. Lett. A* **288**, 62 (2000).
- [25] E. Rains, *Phys. Rev. A* **60**, 173 (1999); *ibid* **60**, 179 (1999).
- [26] T. Wei and P. Goldbart, *Phys. Rev. A* **68**, 042307 (2003); C. Witte and M. Trucks, *Phys. Lett. A* **257**, 14-20 (1999).
- [27] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin and W.K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [28] W.K. Wootters, *Phys. Rev. Lett.* **80**, 2245 (1998).

- [29] P. Hayden, M. Horodecki and B.M. Terhal, J. Phys. A: Math. Gen. **34**, 6891 (2001).
- [30] O. Rudolph, J. Phys. A: Math Gen **33**, 3951 (2000); O. Rudolph, J. Math. Phys. **42**, 2507 (2001); O. Rudolph, *Preprint* quant-ph/0202121.
- [31] M. Christandl and A. Winter, J. Math. Phys. **45**, 829 (2004).
- [32] R.R. Tucci, *Preprint* quant-ph/9909041; R. R. Tucci, *Preprint* quant-ph/0202144.
- [33] H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001).
- [34] M.A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
- [35] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).
- [36] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
- [37] D. Jonathan and M.B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999).
- [38] R. Bhatia, *Matrix Analysis* (Springer, Berlin, 1997).
- [39] A. Kent, Phys. Rev. Lett. **81**, 2839 (1998).
- [40] D. Jonathan and M.B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).
- [41] M.B. Plenio and V. Vitelli, Contemp. Phys. **42**, 25 (2001).
- [42] M.B. Plenio, S. Virmani and P. Papadopoulos, J. Phys. A: Math. Gen. **33**, L193 (2000).
- [43] I. Devetak and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005).
- [44] M.B. Plenio and V. Vedral, J. Phys. A: Math. Gen. **34**, 6997 (2001)
- [45] V. Vedral, M.B. Plenio, K. Jacobs and P.L. Knight, Phys. Rev. A **56**, 4452 (1997).
- [46] K. Audenaert, J. Eisert, E. Jané, M.B. Plenio, S. Virmani and B. DeMoor, Phys. Rev. Lett. **87**, 217902 (2001).
- [47] K. Audenaert, B. DeMoor, K.G.H. Vollbrecht and R.F. Werner, Phys. Rev. A **66**, 032310 (2002).
- [48] J. Eisert, K. Audenaert and M.B. Plenio, J. Phys. A: Math. Gen. **36**, 5605 (2003).
- [49] K. Audenaert, M. B. Plenio and J. Eisert, Phys. Rev. Lett. **90**, 027901 (2003).
- [50] S. Ishizaka, Phys. Rev. A **69**, 020301(R) (2004).
- [51] K. Zyczkowski, P. Horodecki, A. Sanpera and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).
- [52] J. Eisert and M.B. Plenio, J. Mod. Opt. **46**, 145 (1999); K. Zyczkowski and I. Bengtsson, Ann. Phys. **295**, 115 (2002); A. Miranowicz and A. Grudka, J. Opt. B: Quantum Semiclass. Opt. **6**, (2004) 542-548
- [53] J. Eisert, PhD thesis (University of Potsdam, February 2001).
- [54] G. Vidal and R.F. Werner, Phys. Rev. A **65**, 032314 (2002).
- [55] E.M. Rains, IEEE Trans. Inf. Theory **47**, 2921 (2001).
- [56] M. Nielsen and I. Chuang, *Quantum Information and Computation* (Cambridge University Press, Cambridge, MA) 2000
- [57] K.G.H. Vollbrecht and R.F. Werner, Phys. Rev. A **64**, 062307 (2001).
- [58] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
- [59] M.J. Donald, M. Horodecki and O. Rudolph, J. Math. Phys. **43**, 4252 (2002).
- [60] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).
- [61] G. Vidal and R. Tarrach, Phys. Rev. A. **59**, 141 (1999).
- [62] M. Steiner, Phys. Rev. A **67**, 054305 (2003); A. Harrow and M. Nielsen, Phys. Rev. A **68**, 012308 (2003); F.G.S.L. Brandao, Phys. Rev. A **72**, 022310 (2005).

11 Purification and Distillation

Wolfgang Dür and Hans.-J. Briegel

11.1 Introduction

Entanglement is a unique feature of quantum mechanics which has puzzled physicists since its first discussion by E. Schrödinger in 1935 [1]. For many decades, mainly fundamental issues—such as the relation of entanglement to the existence of local hidden variable models—have been discussed. Only quite recently, questions related to practical aspects of entanglement have emerged. It was realized that entanglement is not only a strange feature of quantum mechanics, but can also be a valuable *resource*. First applications of entanglement appeared in the context of quantum communication and quantum cryptography. It was shown that bipartite, maximally entangled pure states can be used for teleportation [2] and to establish a secret key [3] between two communication partners. The latter allows one to achieve provable secure communication, leading to widespread possible applications in modern communication technology. Entanglement also plays a fundamental role in other types of quantum information processing, e.g., in the context of quantum computation or quantum simulation, and allows for an alternative approach for the realization of such processes. Examples are teleportation-based quantum gates or the one-way quantum computer [4]. The theoretical developments were followed by impressive experimental progress, where many of the basic building blocks of both quantum communication and computation have been demonstrated. First commercial quantum-crypto systems for short range communication are already available in the market, being considered as the precursor of an emerging quantum technology. Quantum repeaters [5, 6] were shown to allow, in principle, also for quantum communication over arbitrary distances.

Most applications of entanglement in quantum information processing are based on in some sense maximally entangled pure states. The creation and manipulation of pure state entanglement thus became a key issue. However, pure entangled states are not readily available in the laboratory. In particular, when dealing with realistic systems, system degrees of freedom will interact with uncontrollable degrees of freedom of the environment, resulting in inevitably decoherence. The resulting states will thus be mixed, and the fidelity of the states, i.e., the overlap with the required maximally entangled pure state, will be smaller than unity.

Entanglement purification allows one to overcome this limitation and to produce from several noisy copies of an entangled state a few copies with high fidelity arbitrary close to unity. In this chapter, we will use the term *entanglement distillation* to refer to the manipulation of an ensemble of states in such a way that (a reduced number of) maximally entangled states

are distilled. Entanglement distillation uses entanglement purification as a building block to increase the information about the ensemble, and hence to achieve this aim. Entanglement purification was introduced in the context of quantum communication [7, 8] to overcome noise induced on the system when sending (parts of) maximally entangled states through noisy quantum channels. However, the picture that has recently emerged is that the application of entanglement purification is not limited to quantum communication, but provides a fundamental tool in quantum information processing. For instance, one may use teleportation-based gates rather than conventional gates based on direct two-particle interactions. In this case, the generation of certain (multipartite) entangled states, together with Bell measurements, suffices to realize arbitrary two-qubit gates. This may be easier to achieve than a controlled direct interaction of two systems (e.g., in the case of photons). Such measurement-based approaches to quantum computation offer a new perspective, where the one-way quantum computer [4] represents the extreme case in which quantum computation is performed only by a suitable sequence of single-qubit measurements on a specific, multipartite entangled state, the so-called cluster state [9]. Quite remarkably, it was shown that entanglement purification is also possible in realistic scenarios where not only the states to be purified, but also the operations involved in the manipulation of the state (i.e., in the purification procedure) are noisy. In this case, the fidelity of the states can still be significantly increased, although no maximally entangled pure states can be created. Some entanglement purification protocols were shown to be remarkably robust under the influence of noisy control operations, tolerating errors of the order of several percent. In this context, entanglement purification was suggested to be used as a tool to design (fault-tolerant) quantum computation schemes with less stringent error thresholds [10, 11]. First experimental realizations of entanglement purification using photons have been reported [12].

It is worth mentioning that the distillation of pure entangled states is not only of practical relevance, but also leads to a possible way to classify and quantify entanglement. The corresponding entanglement measure is known as *entanglement of distillation* E_D and gives the maximal amount of pure-state entanglement that can be created per copy from M copies of a mixed state ρ in the limit $M \rightarrow \infty$ by means of local operations. The entanglement of distillation thus has a well-defined physical meaning, which makes it an outstanding measure of entanglement. Although the exact value of E_D is in general very difficult—if not impossible—to calculate, both upper and lower bounds based on different criteria are known. Many states with interesting entanglement features have been discovered. Among them are (i) bound entangled states, i.e., entangled states with zero distillable entanglement and (ii) states where the manipulation of entanglement is irreversible, i.e., the entanglement cost (the amount of entanglement to prepare the state) is strictly larger than the distillable entanglement (the entanglement that can be extracted from the state).

In this chapter we will discuss both fundamental and practical aspects of entanglement distillation. We start with entanglement distillation of pure states in Section 11.2. We will define the notion of distillability and bound entanglement in bipartite systems for general mixed states in Section 11.3, where we also discuss necessary and sufficient conditions for distillation. In Section 11.4 we describe different protocols for entanglement distillation of bipartite states. Distillation of multipartite entangled states will be considered in Section 11.5 and the corresponding purification protocols in Section 11.6. We study the effect of noisy local control operations in Section 11.7 and discuss applications of entanglement purification in quantum

information processing in Section 11.8. We summarize and conclude in Section 11.9. The focus of this chapter lies on entanglement distillation protocols for bipartite and multipartite systems, which are discussed and explained in detail. Sections on entanglement manipulation, distillability and bound entanglement are supposed to provide an overview rather than an in-depth introduction to these subjects.

11.2 Pure States

We consider n spatially separated parties $A_1, \dots, A_n$, each holding a d -level system, corresponding to a Hilbert space $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$. We will refer to $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}_{A_j}$ as the computational basis of particle j held by A_j . We will mainly consider two-level systems $d = 2$, i.e., qubits, where $\{|0\rangle, |1\rangle\}$ are eigenstates of Pauli operator σ_z . A pure state can be written in the computational basis and is specified by $(2d)^n - 1$ real parameters,

$$|\Psi\rangle = \sum_{j_1=0}^{d-1} \sum_{j_2=0}^{d-1} \dots \sum_{j_n=0}^{d-1} a_{j_1 j_2 \dots j_n} |j_1\rangle_{A_1} \otimes |j_2\rangle_{A_2} \dots \otimes |j_n\rangle_{A_n}. \quad (11.1)$$

11.2.1 Bipartite systems

For bipartite systems, i.e., $n = 2$, we denote the parties by A and B , often referred to as Alice and Bob. Any bipartite pure state $|\Psi\rangle$ can be written in its Schmidt decomposition, i.e., there exist local unitary operations $U_A \otimes U_B$ such that

$$U_A \otimes U_B |\Psi\rangle = \sum_{k=0}^{d-1} \sqrt{\lambda_k} |k\rangle_A \otimes |k\rangle_B, \quad (11.2)$$

where $\lambda_0 \geq \lambda_1 \geq \dots \geq \lambda_d$ are ordered Schmidt coefficients which are positive and real and sum up to 1. Since the unitary operations U_A, U_B correspond to the choice of a local basis in A, B , the entanglement properties of a pure state $|\Psi\rangle$ are completely determined by its Schmidt coefficients. A state $|\Psi\rangle$ is entangled if it has two (or more) nonzero Schmidt coefficients, while it is a product state if $\lambda_0 = 1$. The state is called maximally entangled if all Schmidt coefficients are equal, $\lambda_0 = \lambda_1 = \dots = \lambda_{d-1} = 1/d$.

In the context of quantum information processing, it is an important question whether a certain pure state $|\Psi\rangle$ can be transformed by means of local operations and classical communication (LOCC) to some other pure state $|\Phi\rangle$ and vice versa. If this is possible, the two pure states can be used to perform the same tasks and can be used for the same applications. There are many variants of this problem, reaching from restricted kinds of classical communication to entanglement-assisted transformation leading to catalysis effects. We will consider throughout this paper only two-way classical communication and arbitrary sequences of local operations, where in the case of pure-state transformations it turns out that one-way classical communication is in many cases already sufficient. For arbitrary finite-dimensional systems, a simple necessary and sufficient criterion for the LOCC transformation of states $|\Psi\rangle$ to states $|\Phi\rangle$ is known, both for deterministic and probabilistic transformations [13–15]. While in the first case the transformation always succeeds, in the latter case the transformation only

succeeds with some nonzero probability p . The criterion can be expressed as a simple majorization relation between the Schmidt coefficients $\{\lambda_k^\Psi\}$ of state $|\Psi\rangle$ and $\{\lambda_k^\Phi\}$ of state $|\Phi\rangle$. A deterministic transformation from $|\Psi\rangle$ to $|\Phi\rangle$ by means of LOCC is possible if and only if $\{\lambda_k^\Psi\}$ is majorized by $\{\lambda_k^\Phi\}$, i.e.,

$$\sum_{k=1}^j \lambda_k^\Psi \leq \sum_{k=1}^j \lambda_k^\Phi, \forall j = 1, \dots, d-1. \quad (11.3)$$

Similarly, the maximal success probability for the transformation can be determined from the maximum p such that $\{\lambda_k^\Psi\}$ is majorized by $\{p\lambda_k^\Phi\}$. Note that these theorems can also be applied to systems consisting of multiple copies of a certain pure state. For instance, one can answer question whether N copies of a pure state $|\Psi\rangle$ can be transformed to M copies of a pure state $|\Phi\rangle$,

$$|\Psi\rangle^{\otimes N} \rightarrow |\Phi\rangle^{\otimes M}, \quad (11.4)$$

and the maximal success probability for this transformation can be determined. As a special instance, this includes distillation of maximally entangled states, where target states $|\Phi\rangle$ are maximally entangled states with equal Schmidt coefficients.

In the asymptotic limit of many copies, $N \rightarrow \infty$, it turns out that a single quantity, the *entropy of entanglement* S_A , determines the ratio M/N for transformations between pure states. The entropy of entanglement of a pure state $|\Psi\rangle$ is given by the von Neumann entropy of the reduced density operator $\rho_A = \text{tr}_B |\Psi\rangle\langle\Psi|$, $E(\Psi) = -\text{tr} \rho_A \log_2 \rho_A$, which only depends on the Schmidt coefficients, $E(\Psi) = -\sum_{k=1}^{d-1} \lambda_k^\Psi \log_2 \lambda_k^\Psi$. The transformation $|\Psi\rangle^{\otimes N} \rightarrow |\Phi\rangle^{\otimes M}$ by means of LOCC succeeds with vanishing error if and only if [16–18]

$$\frac{M}{N} \leq \frac{E(\Psi)}{E(\Phi)}. \quad (11.5)$$

In particular, this implies that transformations between pure states are reversible in the asymptotic limit. In this sense, the entropy of entanglement is a unique measure of entanglement for finite-dimensional bipartite systems. For instance, Eq. (11.5) implies that N copies of a nonmaximally entangled state $|\Psi\rangle$ can be transformed into $NS_A(\Psi)$ copies of maximally entangled pure qubit states $|\Phi\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ and vice versa. In this asymptotic sense, all bipartite entangled pure states are *qualitatively* equivalent, while the quantitative measure is provided by the entropy of entanglement.

11.2.2 Multipartite systems

For multipartite systems, the situation is far more involved, mainly due to the fact that no analog of the Schmidt decomposition exists [19, 20]. However, the Schmidt measure [21], that is the minimum number of product terms required to represent a state, is an analog of the Schmidt number for bipartite systems (the number of terms in the Schmidt decomposition). The Schmidt measure is an entanglement measure which gives rise to a (coarse grained) classification of multipartite quantum states [21, 22], and to necessary conditions for state transformation. However, no simple necessary and sufficient criterion for transformation by means of (probabilistic or deterministic) LOCC between single copies of multipartite pure states is

known, and for more than three parties, in general two pure states cannot be transformed into each other with nonzero probability of success [23, 24]. Only certain special cases, e.g., the optimal transformation of an arbitrary three-qubit state to maximally entangled GHZ states,

$$|\text{GHZ}\rangle = 1/\sqrt{2}(|000\rangle + |111\rangle), \quad (11.6)$$

have been solved.

Also the asymptotic transformation in the many copy limit—which lead to a significant simplification in the bipartite case—seems to be less tractable. In order to obtain reversible transformations between multiple copies of an arbitrary state $|\Psi\rangle$ and some set of standard states, it was shown that this set has to include several different kinds of multipartite entangled states. In particular, all kinds of maximally entangled bipartite states shared between parties A_k and A_l as well as all combinations of m -party GHZ states have to be included in this set, as they cannot be reversibly transformed into each other [25]. For instance, the three different maximally entangled bipartite states shared between $A_1 - A_2$, $A_1 - A_3$ and $A_2 - A_3$ cannot be reversibly converted into tripartite GHZ states. For special classes of multipartite pure states it was shown that reversible transformation between states within this class and the set of m -party GHZ states (including all possible permutations for all $m \leq n$) is possible [26]. However, in general the set of states has to be enlarged to ensure reversible interconvertability [27], and it is not known whether a set with finite cardinality is sufficient in general [28].

11.3 Distillability and Bound Entanglement in Bipartite Systems

We now turn to mixed states described by density operators ρ . We start by considering bipartite systems consisting of two d -dimensional systems A, B with corresponding Hilbert $\mathcal{H} = (\mathbb{C}^d)^{\otimes 2}$. We will again consider the conversion of (many copies of) a given mixed state ρ_{AB} to a maximally entangled pure state $|\Phi\rangle = 1/\sqrt{d} \sum_{k=0}^{d-1} |k\rangle_A \otimes |k\rangle_B$, i.e., the distillation of pure state entanglement. As already mentioned above, the possibility of such a transformation as well as the optimal ratio of transformation are both of fundamental importance and of practical relevance. From a practical point of view, such a transformation allows one to obtain maximally entangled pure states that can be used as a resource to perform quantum information tasks. From the optimal ratio M/N of the transformation, one obtains an entanglement measure with a clear physical interpretation, the entanglement of distillation.

11.3.1 Distillable entanglement and yield

Given N copies of an arbitrary bipartite mixed state, $\rho^{\otimes N}$, the distillable entanglement E_D is defined as the fraction M/N of the number of copies M of maximally entangled pure states of two qubits, $|\Phi\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ that can be created in an asymptotic, approximate sense by means of LOCC. That is, in the limit $N \rightarrow \infty$ one is interested in the fraction of maximally entangled EPR pairs that one can generate, where the entanglement of distillation is measured in e-bits. Here one allows for *approximate* transformations, i.e., the (global) fidelity of the resulting state $\sigma^{\otimes M}$ needs to be ϵ close to 1, $F = \langle \Phi |^{\otimes M} | \sigma^{\otimes M} | \Phi \rangle^{\otimes M} \geq 1 - \epsilon, \forall \epsilon > 0$ (see [28] for more details).

The sequence of local operations and classical communication that achieves the transformation $\rho^{\otimes N} \rightarrow \sigma^{\otimes M}$ (with σ close to maximally entangled pairs) is often called an entanglement purification protocol (EPP), and the fraction M/N is referred to as the *yield* of the procedure. In this sense, the entanglement of distillation is given by the yield of the optimal procedure.

11.3.2 Criteria for entanglement distillation

In general it is very difficult to calculate the entanglement of distillation, as this entanglement measure is operationally defined. That is, one has to maximize over *all* LOCC procedures that accomplish the transformation in question. These LOCC procedures may, e.g., include (possibly infinite) sequences of (weak) measurements in A , classical communication of the results to B , measurements in B (depending on the outcome of A), communication of the results to A , measurement in A (depending on all previous outcomes) etc. The class of LOCC transformations is very difficult to deal with, which makes the calculation of E_D a highly nontrivial task. In general, only upper and lower bounds are known. Any entanglement purification protocol which is capable of purifying a certain state provides us with a lower bound for the entanglement of distillation. The lower bound is given by the yield of the protocol. Upper bounds can be derived by considering the transformation of states under larger classes of operations—including the set of LOCC transformations as special instances. For example, one can consider operations that preserve the positivity of the partial transpose (see Section 11.3.2.1 for the definition of partial transposition) which are easier to handle than LOCC and derive in this way upper bounds for the efficiency of transformations. Upper bounds for the efficiency for all protocols based on positivity-preserving operations automatically lead to upper bounds for distillable entanglement (using protocols based on LOCC) [29]. There exist examples of states where upper and lower bounds coincide and hence the distillable entanglement is known. This is the case for incoherent mixtures of two maximally entangled states of two qubits,

$$\rho_B(F) = F|\Phi^+\rangle\langle\Phi^+| + (1-F)|\Psi^+\rangle\langle\Psi^+|, \quad (11.7)$$

with $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, $|\Psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$. Here the distillable entanglement is given by

$$E_D(\rho_B(F)) = -F \log_2(F) - (1-F) \log_2(1-F). \quad (11.8)$$

In general, the value of E_D , even for simple mixed states such as Werner states [42] (a mixture of a maximally entangled state with a completely mixed state), is however not known. More strikingly, even the question whether a given (high dimensional) mixed state is distillable entangled or not can in general not be answered. As we will see below, there exist necessary criteria for distillation, and sufficient criteria for distillation. In general, these criteria are not conclusive in the sense that for many states it is not possible to judge whether the state is distillable entangled or not. Only for low-dimensional systems, in particular all $2 \times d$ systems, a necessary and sufficient condition is known.

11.3.2.1 Partial transposition as a necessary criterion for distillation

The partial transposition of a density operator turns out to provide a simple, necessary criterion for distillation. The partial transposition of a density operator ρ with respect to the first subsystem, ρ^{TA} , written in the standard basis $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ is given by [30]

$$\rho^{TA} \equiv \sum_{i,j=0}^{d-1} \langle i|\rho|j\rangle |j\rangle\langle i|. \quad (11.9)$$

The partial transposition ρ^{TA} is basis dependent, but the eigenvalues are not. We say that ρ has positive partial transposition (PPT) if all eigenvalues of ρ^{TA} are positive, while ρ is said to be NPPT (nonpositive partial transposition) or simply NPT (negative partial transposition) if at least one of the eigenvalues of ρ^{TA} is negative. If all eigenvalues of ρ^{TA} are positive, the state ρ is said to be PPT (positive partial transpose). It turns out [31, 32] that *NPT of ρ is a necessary condition for distillability*. This can be readily seen from the fact that any sequence of local operations does not change the positivity of the partial transposition. One uses the operator identity

$$A \otimes B \rho^{TA} C \otimes D = (C^T \otimes B \rho A^T \otimes D)^{TA}, \quad (11.10)$$

where one only needs to consider the case $C = A^\dagger, D = B^\dagger$. That is, a density operator ρ (i.e., an operator with a positive spectrum) which is PPT by assumption is converted by local transformation in another density operator (right-hand side of Eq. (11.10)). The partial transposition of this transformed density operator can also be obtained by applying (different) local transformations on the partial transpose of the initial density operator (left-hand side of Eq. (11.10)). As the spectrum of ρ^{TA} is positive by assumption, also the spectrum of the operator on the left-hand side of Eq. (11.10) is positive. Hence also the spectrum of the locally transformed operator (right-hand side of Eq. (11.10)) is positive. As the maximally entangled target state $|\Phi\rangle\langle\Phi|$ is NPT, it follows that only states which are initially also NPT can be converted to $|\Phi\rangle$. The argument also holds for approximative transformations and multiple copies.

For $2 \times d$ systems, i.e., states consisting of a qubit and a d -level system, NPT turns out to be a necessary and sufficient condition for distillability [32, 33]. This can be shown as follows: First, there exists a projector into a two-dimensional subspace in B such that the resulting state is still *NPT* [33]. Second, in 2×2 systems NPT implies that there exist local filtering measurements such that a state $\tilde{\rho}$ can be created from ρ which has fidelity $F = \langle\Phi|\tilde{\rho}|\Phi\rangle > 1/2$ [32]. Finally, there exists an entanglement distillation protocol which allows one to create maximally entangled states whenever $F > 1/2$ [7]. This protocol will be discussed in more detail in Section 11.4.

For higher dimensional $d_1 \times d_2$ systems, there exist, however, states which have the puzzling property that they are PPT (and hence not distillable), but which are nevertheless entangled (i.e., nonseparable) [31]. These states are called *bound entangled*, as their entanglement can not be converted to a useful (pure state) form. Whether NPT is also a sufficient condition for distillability for $d \times d$ systems is presently unknown. Strong evidences for the existence of such NPT bound entangled states have been reported in [33, 34] (see also [35, 36]). Note that the existence of such states would imply the nonadditivity of entanglement of distillation [37],

as one can distill entanglement if both certain (conjectured) NPT bound entangled states and PPT bound entangled states are available.

11.3.2.2 Sufficient conditions for distillation

Only few sufficient criteria for distillability are known. A criterion which is simple to check and valid for $d \times d$ systems is the reduction criterion developed by the Horodecki family [38]. In particular, we have that if a state ρ violates the reduction criterion,

$$\rho_A \otimes \mathbb{1} - \rho \geq 0, \quad (11.11)$$

then the state is distillable. For mixtures of a maximally entangled state and a completely mixed state (global white noise, described by a density operator $\frac{1}{d}\mathbb{1}$), the criterion reads $F \geq 1/d$. However, many distillable states are not detected by the reduction criterion.

A second criterion follows from the fact that NPT is a sufficient condition for distillation in 2×2 systems. Hence, if for a $d \times d$ system in a mixed state ρ local projections in two-dimensional subspaces in A, B exist such that the resulting state is NPT, then ρ is distillable. This property is in fact called 1-distillability, where k -distillability is defined as the existence of such projectors when operating jointly on k copies of ρ , $\rho^{\otimes k}$. A state is distillable if there exists a k such that it is k -distillable. This criterion is however not a practical one, as in general it is difficult to check due to the optimization over all two-dimensional projections.

More practical criteria are in a certain sense provided by entanglement distillation protocols, where successful applicability of a protocol clearly implies distillability of the corresponding state. In this sense, the regime where a protocol can be successfully applied (which can often be expressed in terms of fidelity or of diagonal entries of the density matrix written in a certain basis, as we will see in Section 11.4) automatically translates into a sufficient condition for distillability. For instance, a fidelity $F > 1/2$ with a maximally entangled state is sufficient for the applicability of the protocols [7, 8] for two-qubit systems and is hence a sufficient condition for distillability.

11.4 Bipartite Entanglement Distillation Protocols

We now turn to explicit entanglement purification protocols. A number of different protocols exist, which differ in their purification range (i.e., the set of states they can purify), the efficiency, and the number of copies of the states they operate on. In the following we will consider filtering protocols (which operate on a single copy), recurrence protocols (which operate on two copies simultaneously at each step), as well as hashing and breeding protocols (which operate simultaneously on a large number $N \rightarrow \infty$ of copies). We also discuss $N \rightarrow M$ protocols, which operate on N input copies and produce M output copies.

11.4.1 Filtering protocol

The most simple protocols operate on a single copy of the mixed state ρ and consist in the application of local filtering measurements (including weak measurements). A weak measurement may, e.g., be realized by a joined, local operation on the system and an (high dimensional) ancilla, followed by a von Neumann measurement of the ancilla. Hence (sequences of)

local operations, including (weak) measurements, are applied in such a way that for specific measurement outcomes the resulting state σ is more entangled than the initial state ρ . Note that the output state σ is obtained only with a probability $p < 1$. Mixed states where such a filtering method can be applied include, e.g., certain rank two states [39]

$$\rho = F|\Psi^+\rangle\langle\Psi^+| + (1 - F)|00\rangle\langle 00|. \quad (11.12)$$

Application of the local operators $O_A = O_B = \sqrt{\epsilon}|0\rangle\langle 0| + |1\rangle\langle 1|$ (which correspond to a specific branch of a local positive operator valued measure, POVM) leads to a nonnormalized state of the form $\rho' = F\epsilon|\Psi^+\rangle\langle\Psi^+| + (1 - F)\epsilon^2|00\rangle\langle 00|$. The fidelity of the resulting state is given by $F' = F\epsilon/[F\epsilon + (1 - F)\epsilon^2]$. Note that for small ϵ , $F' \rightarrow 1$, i.e., states arbitrarily close to the maximally entangled state $|\Psi^+\rangle$ can be created. However, the probability to obtain the desired outcome corresponding to O_A, O_B , $p_{\text{suc}} = F\epsilon + (1 - F)\epsilon^2$, goes to zero as $\epsilon \rightarrow 0$. There is a tradeoff between the reachable fidelity of the output state and the probability of success of the procedure.

It turns out that filtering protocols are of limited applicability for general mixed states, even for the simplest case of two qubits. In particular, as shown in [40, 41], the fidelity of a single copy of a full rank state can in general *not* be increased by any local operation. This seriously restricts the applicability of filtering procedures and requires one to consider protocols that operate jointly on two (or more) copies of the state in order to increase fidelity and ultimately to obtain maximally entangled states.

11.4.2 Recurrence protocols

In the following we discuss a class of conceptually related protocols [7, 8, 10] that allow one to produce states arbitrarily close to a maximally entangled pure state by iterative application. Before we go into technical details, we describe the general concept underlying these (and more generally, almost all) entanglement purification protocols. The basic idea of all entanglement purification protocols is to decrease the degree of mixedness of the ensemble of mixed state. To this aim, one needs to gain information which is done by performing suitable measurements. As the relevant information is nonlocal, one needs to use the entanglement inherent in states of the ensemble to reveal this information. In fact, by first operating on several copies of the ensemble in a local way, information about this subensemble is transferred to one of the states. This state is then measured to reveal the information, and in this way to increase the information about the remaining states. In many protocols the remaining states are only kept if a specific measurement outcome was found. This is due to the fact that one finds for certain measurement outcomes (measurement branches) that the entanglement of the remaining states is increased, while for other outcomes it is decreased or the states are no longer entangled. In this way it is also guaranteed that on average, entanglement cannot increase under local operations and classical communication. Recurrence protocols operate in each purification step on two identical copies of a mixed state. After local manipulation, one of the copies is measured, and depending on the outcome of the measurement the other copy is kept (we refer to this as a successful purification step) or discarded. In the case of a successful purification step, the fidelity of the remaining pair is increased. The procedure is iterated, whereby states resulting from a successful purification round are used as an input

for the next purification round. Typically, these protocols converge to a fixed point which—in case the initial fidelity was sufficiently large—is given by a maximally entangled state.

We now turn to specific recurrence protocols that allow one to purify bipartite entangled states. We will not describe these protocols as they were originally presented, but provide an equivalent description which will allow us a unified treatment of bipartite and multipartite entanglement purification protocols. In particular, we describe protocols that operate on states in a (locally) rotated basis and describe the corresponding states in terms of their stabilizing operators. To this aim, we start by fixing some notation. We consider two parties, A and B , each holding several copies of noisy entangled states described by a density operator ρ_{AB} acting on Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$. We denote by

$$|\Phi_{00}\rangle \equiv 1/\sqrt{2}(|0\rangle_z|0\rangle_x + |1\rangle_z|1\rangle_x), \quad (11.13)$$

a maximally entangled state of two qubits, where $|0\rangle_z, |1\rangle_z$ [$|0\rangle_x, |1\rangle_x$] are eigenstates of σ_z [σ_x] with eigenvalue (± 1) respectively. That is, $\sigma_x|1\rangle_x = -|1\rangle_x$, and $|0\rangle_x = 1/\sqrt{2}(|0\rangle_z + |1\rangle_z)$. We also define

$$|\Phi_{k_1 k_2}\rangle \equiv \sigma_z^{k_1} \sigma_z^{k_2} |\Phi_{00}\rangle, \quad (11.14)$$

with $k_1, k_2 \in \{0, 1\}$. The states $\{|\Phi_{k_1 k_2}\rangle\}$ form a basis of orthogonal, maximally entangled states, the so-called Bell basis. We remark that the states $|\Phi_{k_1 k_2}\rangle$ are joint eigenstates of correlation operators

$$K_1 = \sigma_x^{(A)} \sigma_z^{(B)}, K_2 = \sigma_z^{(A)} \sigma_x^{(B)}, \quad (11.15)$$

with eigenvalues $(-1)^{k_1}$ and $(-1)^{k_2}$ respectively. Whenever several copies of a mixed state are involved, we will refer to the different copies by numbers. For instance, $\rho_{A_1 B_1}$ refers to the first copy of a state, while $\rho_{A_2 B_2}$ refers to the second copy. In this case, party A holds two qubits, A_1 and A_2 .

We consider mixed states ρ'_{AB} which we write in the Bell basis,

$$\rho'_{AB} = \sum_{k_1, k_2, j_1, j_2=0}^1 \lambda'_{k_1 k_2 j_1 j_2} |\Phi_{k_1 k_2}\rangle \langle \Phi_{j_1 j_2}|. \quad (11.16)$$

One can always *depolarize* the state to a standard form by a suitable sequence of (random) local operations in such a way that the fidelity of the state, $F \equiv \langle \Phi_{00} | \rho_{AB} | \Phi_{00} \rangle$ is not altered. To be specific, by probabilistically applying one of the local operations corresponding to $\{\mathbb{1}, K_1, K_2, K_1 K_2\}$ one produces a density operator which is diagonal in the Bell basis,

$$\rho_{AB} = \sum_{k_1, k_2=0}^1 \lambda_{k_1 k_2} |\Phi_{k_1 k_2}\rangle \langle \Phi_{k_1 k_2}|, \quad (11.17)$$

and in which diagonal coefficients remain unchanged, $\lambda_{k_1 k_2} \equiv \lambda'_{k_1 k_2 k_1 k_2}$. This can be understood as follows: Consider for instance the action of K_1 on basis states $|\Phi_{k_1 k_2}\rangle$. For $k_1 = 0$, the state is left invariant while a phase of (-1) is picked up if $k_1 = 1$. It follows that off-diagonal elements of the form $|\Phi_{k_1 k_2}\rangle \langle \Phi_{j_1 j_2}|$ in (11.16) are transformed to $(-1)^{k_1 \oplus j_1} |\Phi_{k_1 k_2}\rangle \langle \Phi_{j_1 j_2}|$, i.e., pick up a phase if $k_1 \neq j_1$. Consequently, when applying the local operation K_1 with probability $p = 1/2$ and with probability $p = 1/2$ leaving the state unchanged, the resulting density operator $\rho' = 1/2(K_1 \rho K_1^\dagger + \rho)$ has no off-diagonal elements

where $k_1 \neq j_1$. In a similar way, all off-diagonal elements are cancelled by the (random) application of $\mathbb{1}, K_1, K_2, K_1 K_2$. Note that all diagonal elements—in particular the fidelity of state—remain unchanged by this depolarization procedure. Using similar techniques, one can further depolarize the state by equalizing all but one of the diagonal elements. The resulting states are called Werner states [42],

$$\rho_W(x) = x|\Phi_{00}\rangle\langle\Phi_{00}| + (1-x)/4\mathbb{1}_{AB}, \quad (11.18)$$

where the fidelity $F = (3x+1)/4$ is unchanged. This can be accomplished by randomly applying local unitary operations that leave the state $|\Phi_{00}\rangle$ (up to a phase) invariant, which is the case for all operations of the form $U \otimes HU^*H$ with H being the Hadamard gate [43] and $*$ denoting complex conjugation. The unitaries can be chosen uniformly (according to the Haar measure), or selected from a specific finite set of operations [7]. What is important in our context is that any state with fidelity F can always be brought to Werner form. It is thus sufficient to provide an entanglement purification method which works for Werner states, because such a method automatically allows one to purify all states with same fidelity. We consider such a purification procedure in the following.

11.4.2.1 BBPSSW protocol

In 1996, Bennett *et al.* [7] introduced a purification protocol that allows one to create maximally entangled states with arbitrary accuracy starting from several copies of a mixed state ρ , provided that the fidelity F with some maximally entangled state fulfills $F > 1/2$. The protocol consists of the following steps: (i) Depolarize ρ to Werner form; (ii) apply bilateral local CNOT operations $U_{\text{CNOT}}^{A_1 \rightarrow A_2} \otimes U_{\text{CNOT}}^{B_2 \rightarrow B_1}$ [44]; (iii) local measurement of qubit A_2 [B_2] in eigenbasis of σ_z [σ_x] with corresponding results $(-1)^{\xi_1}$ [$(-1)^{\zeta_1}$] respectively, where $\xi_1, \zeta_1 \in \{0, 1\}$. The effect on other particles of this local measurement is the same as the measurement of the observable $K_2^{(A_2 B_2)}$; (iv) keep the state of $A_1 B_1$ if $(\xi_1 + \zeta_1) \bmod 2 = 0$, i.e., measurement results coincide.

Given two copies of a state with fidelity F , it is straightforward to calculate the fidelity of the resulting state when applying (i–iv). The effect of (ii) on two Bell states is given by

$$|\Phi_{k_1, k_2}\rangle_{A_1 B_1} |\Phi_{j_1, j_2}\rangle_{A_2 B_2} \rightarrow |\Phi_{k_1 \oplus j_1, k_2}\rangle_{A_1 B_1} |\Phi_{j_1, k_2 \oplus j_2}\rangle_{A_2 B_2}. \quad (11.19)$$

The effect of (iii) and (iv) is to select states in $A_2 B_2$ which are eigenstates of $K_2^{A_2 B_2}$ with eigenvalue (+1), while eigenstates with eigenvalue (-1) are discarded. That is, only initial states $|\Phi_{k_1, k_2}\rangle_{A_1 B_1} |\Phi_{j_1, j_2}\rangle_{A_2 B_2}$ with $k_2 \oplus j_2 = 0$ will pass the measurement procedure, which implies that, when considering mixed states, only these components will contribute to the final density operator. The final state turns out to be not of Werner form; however due to step (i) the state is brought back to Werner form when iterating the procedure. Hence the essential parameter is the fidelity F' after successful purification. One finds

$$F' = \frac{F^2 + [(1-F)/3]^2}{F^2 + 2F(1-F)/3 + 5[(1-F)/3]^2}, \quad (11.20)$$

which fulfills $F' > F$ for $F > 1/2$. The success probability is given by the denominator of Eq. (11.20), $p_{\text{suc}} = F^2 + 2F(1-F)/3 + 5[(1-F)/3]^2$. The iteration of the procedure, which means to take two identical copies of states with fidelity F' , resulting from a previous,

successful purification round, allows us to further increase the fidelity. In fact, it is straightforward to see that the map Eq. (11.20) has $F = 1$ as an attractive fixed point. Hence states arbitrarily close to maximally entangled states can be produced. Although the probability of success of the purification steps tends to 1 for $F \rightarrow 1$, the yield of the procedure goes to zero as always one pair is measured and has to be discarded. Fixing however the desired accuracy of resulting states to a value $F > 1 - \epsilon$, a finite number of purification steps suffices and hence the yield will be finite. We remark that obtaining states with $F = 1$ seems to be a question of only theoretical relevance, since imperfections in a apparatus used in the preparation of the state and in the purification procedure limit the reachable fidelity.

11.4.2.2 DEJMPS protocol

The DEJMPS, introduced by Deutsch *et al.* in [8], is conceptually very similar to the BBPSSW protocol. It operates however not on Werner states, but on states diagonal in a Bell basis (see Eq. (11.17)). The main advantage of this protocol is that it has better efficiency. The protocol operates on two identical copies of a state and consists essentially of the same steps as the BBPSSW protocol. The only difference is that step (i) is replaced by depolarization of ρ to a Bell diagonal state (Eq. (11.17)), and in addition applying before step (ii) some as step (i)a, an additional local basis change $|0\rangle_z \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_z - i|1\rangle_z)$, $|1\rangle_z \rightarrow \frac{1}{\sqrt{2}}(|1\rangle_z - i|0\rangle_z)$ in A and $|0\rangle_x \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_x + i|1\rangle_x)$, $|1\rangle_x \rightarrow \frac{1}{\sqrt{2}}(|1\rangle_x + i|0\rangle_x)$ in B . The action of step (i)a is (up to some irrelevant phases) to flip the diagonal components of $|\Phi_{10}\rangle$ and $|\Phi_{11}\rangle$, i.e., $\lambda_{10} \leftrightarrow \lambda_{11}$. The total effect of the protocol (steps (i–iv)) can be described as a nonlinear map for the diagonal components of ρ to ρ' (written in the Bell basis), i.e., a map from $\mathbb{R}^4 \rightarrow \mathbb{R}^4$. To be specific, the map reads

$$\begin{aligned} \lambda'_{00} &= (\lambda_{00}^2 + \lambda_{11}^2)/N, & \lambda'_{01} &= (\lambda_{01}^2 + \lambda_{10}^2)/N, \\ \lambda'_{10} &= 2\lambda_{00}\lambda_{11}/N, & \lambda'_{11} &= 2\lambda_{01}\lambda_{10}/N, \end{aligned} \quad (11.21)$$

where $N = (\lambda_{00} + \lambda_{11})^2 + (\lambda_{01} + \lambda_{10})^2$ is the probability of success of the protocol. Again, the protocol can be iterated, and the diagonal coefficients of the state (written in the Bell basis) after k successful purification steps can be calculated by k iterations of the map Eq. (11.21). One can show that the map has $\lambda_{00} = 1$, $\lambda_{ij} = 0$ for $ij \neq 11$ as an attracting fixed point, and in fact all states with $\lambda_{00} > 1/2$ (i.e., $F > 1/2$) can be purified [45].

11.4.2.3 (Nested) entanglement pumping

While both the BBPSSW and DEJMPS protocol allow one to successfully produce entangled states with arbitrary high fidelity, the requirements on local resources are rather demanding. In particular, since at every round two identical states resulting from previous successful purification rounds are required, the total number of pairs that have to be available initially increases (exponentially) with the number of steps and will typically be of the order of several hundred. In particular, these pairs have to be stored by some means. For many physical set-ups, however, the number of particles that can be stored is limited.

The requirements in memory space can however be translated into temporal resources. The corresponding purification protocol is called (nested) entanglement pumping. The basic idea is to repeatedly produce elementary entangled pairs (e.g., resulting from sending parts

of a locally generated maximally entangled state through noisy channels) and using always a fresh elementary pair to purify a second pair. If a purification step is not successful, one has to start again from the beginning, using two elementary pairs. The actual sequence of local operations is either given by the BBPSSW or DEJMPS protocol, where the pair to be purified acts as pair 1 (source pair), while the fresh, elementary pair plays the role of pair 2 (target pair) that is measured. In case the purification step was successful, the fidelity of the first pair is increased by a certain amount. It is straightforward to determine the maps corresponding to Eqs. (11.20), (11.21) for nonidentical input states. One finds

$$F' = \frac{F_1 F_2 + \left(\frac{1-F_1}{3}\right) \left(\frac{1-F_2}{3}\right)}{F_1 F_2 + F_1 \left(\frac{1-F_2}{3}\right) + \left(\frac{1-F_1}{3}\right) F_2 + 5 \left(\frac{1-F_1}{3}\right) \left(\frac{1-F_2}{3}\right)}. \quad (11.22)$$

in the case of two Werner states with fidelity F_1, F_2 . In this map, F_2 is to be considered as a constant since the second pair is always an elementary one. For two Bell diagonal states with coefficients λ_{ik} and μ_{ik} we obtain

$$\begin{aligned} \lambda'_{00} &= (\lambda_{00}\mu_{00} + \lambda_{11}\mu_{11})/N, & \lambda'_{01} &= (\lambda_{01}\mu_{01} + \lambda_{10}\mu_{10})/N, \\ \lambda'_{10} &= (\lambda_{00}\mu_{11} + \lambda_{11}\mu_{00})/N, & \lambda'_{11} &= (\lambda_{01}\mu_{10} + \lambda_{10}\mu_{01})/N. \end{aligned} \quad (11.23)$$

Again, the second pair is always an elementary one, and hence μ_{ik} is fixed. Iteration of the corresponding maps allows in both cases to improve the fidelity; however in general *no* maximally entangled states can be generated. That is, the fixed point of the maps, Eqs. (11.22) and (11.23) depends on the fidelity of the elementary pair (or more generally on the coefficients μ_{ik}) [33].

As elementary pairs can be generated on demand, they do not need to be stored. Hence in A and B only two qubits need to be stored (corresponding to the pair to be purified and the elementary pair respectively). The reduction in spatial resources leads however to an increase of temporal resources. In protocols BBPSSW and DEJMPS, the purification of different pairs corresponding to a single purification step can be implemented in parallel (i.e., the temporal resources are given by the number of steps), while the probabilistic character of entanglement purification manifests itself in the fact that many identical pairs need to be simultaneously available. In entanglement pumping, in contrast the probabilistic character of purification leads to increased number of required repetitions, as in the case of an unsuccessful purification step the procedure has to be started from beginning and pairs are *sequentially* generated.

One can improve the entanglement pumping scheme in such a way that the number of qubits that have to be locally stored remain small (≈ 4 for practical purposes), while it is possible to generate maximally entangled states rather than only enhancing the fidelity by a finite amount. The corresponding scheme is called *nested entanglement pumping* [10] and works as follows: At nesting level 1, elementary pairs created between $A_1 - B_1$ are used to purify a pair shared between $A_2 - B_2$ via entanglement pumping. The fidelity of elementary pairs at level 1 is given by F_1 . It turns out that after a few purification steps, the fidelity of the pair $A_2 - B_2$, F_2 , is already close to the reachable fixed point. The resulting pair with improved fidelity F_2 now serves as elementary pair at nesting level 2. That is, an elementary pair at nesting level 2 shared between $A_3 - B_3$ is purified by means of entanglement pumping, where always (elementary) pairs (of nesting level 2) with fidelity F_2 shared between $A_2 - B_2$ are used. The fidelity of the resulting pair $A_3 - B_3$ after a few purification steps is given by F_3 with $F_3 > F_2 > F_1$. We remark that an unsuccessful purification step at a higher nesting

level requires to restart the procedure at the lowest nesting level 1. Still, the required temporal resources increase only polynomially. The overall procedure can be viewed as a stochastic process, or equivalently as a one side bounded random walk. With each nesting level, one additional particle has to be stored at each location. However, it turns out that for practical purposes (say required accuracy of $\epsilon = 10^{-7}$) a few nesting levels (≈ 3) suffice to generate states with fidelity $F > 1 - \epsilon$ [10]. Hence the storage requirements remain very moderate, while the required temporal resources increase.

11.4.3 $N \rightarrow M$ protocols, hashing, and breeding

The protocols discussed in the previous section operate on two copies of a given mixed state, and produce one copy as output if they are successful. More general protocols are conceivable that operate on N input copies of the state and produce M copies as output. We will refer to such protocols as $N \rightarrow M$ protocols, and discuss them in this subsection. A protocol of this kind of particular importance is the so-called hashing protocol, which operates in the limit $N, M \rightarrow \infty$. The general idea behind $N \rightarrow M$ protocols is very similar as in the case of standard recurrence protocols operating on two copies: To obtain information about a subensemble—in this case consisting of M copies of the state—the remaining $N - M$ copies are measured after applying suitable local operations.

11.4.3.1 $N \rightarrow M$ protocols for finite N

The $2 \rightarrow 1$ recurrence protocols discussed in the previous sections can be considered as two-stage procedures. In the first stage, the two (copies) of the input state(s) are manipulated by local operations. The effect of these local operations on Bell diagonal states is a certain *permutation* of the basis elements. In the second stage, the second pair is measured, and depending on the outcome of the measurement the first pair is either kept or discarded. General $N \rightarrow M$ protocols operate in a very similar fashion. In fact, in [49] all possible permutations achievable by local operations have been constructed for qubit systems, and accordingly a large number of possible $N \rightarrow M$ entanglement purification protocols were constructed and analyzed. It was found that in certain regimes such $N \rightarrow M$ protocols operate more efficiently (i.e., have a higher yield) than standard $2 \rightarrow 1$ protocols [49, 50]. Typically, for small initial fidelities the ratio of final pairs M to initial pairs N may be small, $M/N \ll 1$, while one expects that $M/N \approx 1$ for large fidelities as only a slight amount of information about the remaining ensemble needs to be revealed. Generalizations of this concept to the purification of entangled d -level systems are possible [53].

We would also like to remark that a general connection between error correcting (stabilizer) codes and $N \rightarrow M$ purification protocols exists [48]. In fact, for each code one can construct a corresponding $N \rightarrow M$ entanglement purification protocol.

11.4.3.2 Hashing and breeding protocols

Hashing protocols can be considered as special instances of $N \rightarrow M$ protocols that operate in the limit $N \rightarrow \infty$. Hashing was introduced in [7]. The basic idea is similar as in $N \rightarrow M$ recurrence protocols. Here, random subsets of size n of the total N copies of the state are

chosen, and bilateral local CNOT operations with each of the n pairs as source, and one selected pair as target, are performed (or vice versa, i.e., the selected pair as source). The selected pair is finally measured, revealing at most one bit of information about the remaining ensemble. Measurements of this kind are repeated m times. One can in fact show that the information gain per measurement is close to one bit.

Hashing is conceptually closely related to breeding, which might be slightly easier to understand. In the case of breeding, in addition to the N copies of the state one assumes that one possesses m prepurified, maximally entangled Bell pairs which are used to gain information about the remaining ensemble. In the asymptotic limit of large N the density matrix $\rho^{\otimes N}$ is approximated to an arbitrary high accuracy by its “likely subspace approximation,” i.e., the density matrix Γ obtained by projecting $\rho^{\otimes N}$ into a subspace P (the likely subspace), where the dimension of P is $2^{(S(\rho)+\delta)N}$. In the case of Werner states $\rho_W(F)$ (see Eq. (11.18), $F = (3x+1)/4$), this likely subspace contains essentially states of the form $\otimes |\Phi_{ij}\rangle^{\otimes m_{ij}}$ and permutations thereof, where $m_{00} = FN$, $m_{01} = m_{10} = m_{11} = (1-F)/3N$ [55]. That is, the density matrix $\rho^{\otimes N}$ can be interpreted as an equal mixture of all these possible configurations, where the number of Bell states $|\Phi_{ij}\rangle$ is essentially fixed to m_{ij} , while the order (or position) of the states is unknown. The number of possible configurations of states of this form is—for large N —approximately given by $2^{NS(F)}$, where $S(F) = -F \log_2 F - (1-F) \log_2 (\frac{1-F}{3})$. The task thus reduces to reveal which of these possible configurations one is dealing with. Clearly, this requires $NS(F)$ bits of information. Since one can gain at most one nonlocal bit of information about the ensemble with the help of each maximally entangled pair, one needs at least $m = NS(F)$ additional maximally entangled pairs to perform this task. Having obtained the required information, one possesses a pure state consisting of N Bell states (in different bases), i.e., some (known) permutation of the state $\otimes |\Phi_{ij}\rangle^{\otimes m_{ij}}$. Since $m = S(F)N$ maximally entangled pairs have been consumed during the process, the total yield of the breeding protocol is given by $D = 1 - S(F)$. Note that $S(F) = S(\rho_W)$, where $S(\rho_W) = -\text{tr}(\rho_W \log_2 \rho_W)$ is the von Neumann entropy of ρ_W . It follows that for Werner states, breeding only works if the initial fidelity is sufficiently high, $F \gtrsim 0.81$.

A similar kind of reasoning can be applied to hashing, where no prepurified pairs are required. The analysis is slightly more involved since one has to take a kind of back action (influence of the remaining pairs because the measured pair was not in a pure state) into account. The yield of the hashing procedure is, however, exactly the same as for breeding. For Bell-diagonal states, one obtains that the yield of hashing protocols is given by $D(\rho) = 1 - S(\rho)$.

The yield of hashing and breeding protocols can be further improved, see, e.g., [51]. In addition, one can generalize hashing and breeding to d -dimensional systems for prime d [52]. The optimal entanglement distillation protocol for two-way classical communication is in general unknown. Only for specific two-qubit states, for instance incoherent mixtures of two Bell states, the known upper bounds on the yield coincide with the achievable rate for known protocols, in this case the hashing protocol. When assuming only one-way classical communication, the problem becomes tractable. In fact, the optimal distillation protocol for one-way classical communication was obtained in [54].

11.5 Distillability and Bound Entanglement in Multipartite systems

11.5.1 n -party distillability

In the following we will consider distillability of mixed states in multipartite systems. We denote by $A_1, A_2, \dots, A_n$ n (possibly spatially separated) parties, and by ρ a n -qubit density operator they share. We will be interested in the entanglement properties of ρ , i.e., in its nonlocality properties. As in the case of bipartite systems, one can consider distillation of pure state entanglement, i.e., the question whether one can create from many copies of the state ρ some entangled pure states by means of local operations assisted by classical communication. We will assume that two-way classical communication between any pair of parties is available.

In contrast to the bipartite case, many variations of the problem are conceivable. The most natural one is the n -party distillation of some genuine n -party entangled pure state. In this case, all operations are n -local, where locality is understood with respect to the parties. That is, each of the parties is allowed to operate on their qubits (belonging to different copies of ρ), where the action may depend on results of previous measurements and operations performed by other parties, and arbitrary sequences of this kind of operations can be performed. We remark that *any* genuine multiparty entangled pure state can be used in the definition of n -party distillability. This is due to the fact that any pair of genuine multipartite entangled pure states $|\psi_1\rangle, |\psi_2\rangle$ can be interconverted if many copies are available. That is, Bell pairs between pairs of parties can be generated from many copies of $|\psi_1\rangle$, which can then be connected or used for teleportation to create any other desired state. To be more precise, from the results of [56] (Lemma 1) follows that from a genuine multipartite entangled pure state, one can generate Bell pairs shared between pairs of parties in such a way that these Bell pairs form a connected graph. This already implies that each pair of parties can be connected by Bell pairs, and hence teleportation can be applied. Note that this qualitative equivalence of all kinds of multipartite entangled pure states no longer holds when considering a single copy of the state, or some restricted kind of classical communication.

We emphasize that the possibility of distilling a n -party entangled pure state is equivalent to the possibility of distilling Bell pairs between all pairs of parties, where the remaining parties can assist the distillation process. This provides a convenient tool to prove n -party distillability of states.

11.5.2 m -party distillability with respect to coarser partitions

One may also consider different partitions of the system into $m < n$ groups of parties, and determine the distillability properties of ρ with respect to a given partition. That is, local operations are understood with respect to the m groups of parties (i.e., the partition), and one attempts to distill a m -party entangled state shared among the n groups of parties. When considering *bipartitions* of the system, i.e., partitions into two groups of particles, one recovers the situation discussed in section 11.3. In particular, the criteria for distillation discussed in this Section can be applied. Recall for instance that a necessary condition for distillability of a state with respect to a given partition is that its partial transpose is nonpositive (NPT) with respect to this bipartition.

Similarly, one can obtain necessary conditions for distillation with respect to arbitrary partitions [47]. For instance, one finds that *all* bipartitions that include a given m -partition need to be NPT in order that the state can be m -party distillable (i.e., the bipartition can be obtained from the m -partition by joining some of the groups of parties). This follows again from the fact that local operations cannot change the state from PPT to NPT for a given bipartition. Since this is not possible by operations which are local with respect to a given bipartition, this implies that also no local operations with respect to the finer m -partition can achieve this. However, the desired m -party entangled pure state is NPT with respect to all such bipartitions. Hence the necessity of NPT with respect to all bipartitions including the n -partition of the initial state follows.

11.5.3 Bound entanglement in multipartite systems

The strong requirement that a state needs to be NPT with respect to a large number of bipartitions in order to be distillable leads to various kinds of multipartite bound entangled states with rather puzzling properties. Examples of such states have been discussed in [47]. For instance, one can construct states where one can choose for each bipartition independently whether the state should be distillable with respect to this partition or not. This allows one to find states where entanglement can only be distilled if certain groups of parties join. That is, the entanglement is bound when considering the n party system (i.e., the corresponding n -partition), but can be activated by allowing some parties to join (or, equivalently, by allowing these parties to share entanglement) (see also [33, 58]). For instance, states where entanglement can be distilled only if two groups of macroscopic size (i.e., each including, say, more than 40% of the particles) are formed can be constructed.

Even more surprisingly, by classically mixing different states, all of which are nondistillable with respect to the finest n -partition, one can obtain a distillable state [57]. Given the close connection of distillability properties of multipartite states and the quantum capacity of multipartite quantum channels [56], binding entanglement channels (corresponding to the bound entangled states) can be constructed in such a way that their channel capacity is not additive, but in fact superadditive [56].

11.6 Entanglement Purification Protocols in Multipartite Systems

We now turn to explicit entanglement purification protocols for n -party systems. The first protocol of this kind was introduced in [59] and further analyzed in [50], and is capable of distilling n -party GHZ states. Here, we will discuss recurrence and hashing protocols for all stabilizer states, or equivalently, all two colorable graph states. These protocols were introduced in [60] and further elaborated in [61]. Before we describe these protocols, we briefly review the concept of graph states.

11.6.1 Graph states

We start by defining graph states. A graph G is given by a set of n vertices $\{1, 2, \dots, n\}$ connected in a specific way by edges E . To every such graph there corresponds a basis of n -qubit states $\{|\Phi_{\mu}\rangle_G\}$, where each of the basis states $|\Phi_{\mu}\rangle_G$ is the common eigenstate of n commuting correlation operators K_j^G with eigenvalues $(-1)^{\mu_j}$, $\mu = \mu_1\mu_2\cdots\mu_n$. To relax notation, we will omit the index G and assume that an arbitrary but fixed graph G is considered. Graph states fulfill the set of eigenvalue equations

$$K_j^G |\Phi_{\mu}\rangle_G = (-1)^{\mu_j} |\Phi_{\mu}\rangle_G, \quad (11.24)$$

$j = 1, \dots, n$. The correlation operators are uniquely determined by the graph G and are given by

$$K_j = \sigma_x^{(j)} \prod_{\{k,j\} \in E} \sigma_z^{(k)}. \quad (11.25)$$

A graph is called two-colorable if there exists two groups of vertices, A, B such that there are no edges inside either of the groups, i.e., $\{k, l\} \notin E$ if $k, l \in A$ or $k, l \in B$. For graph states associated with two-colorable graphs, which we call two-colorable graph states, we will split the multiindex μ into two parts, $\mu = \mu_A, \mu_B$, belonging to subsets A and B respectively.

Graph states have first been introduced in [63], generalizing the notion of cluster states as introduced in [4]. A detailed investigation of their entanglement properties has recently been given in the paper by Hein *et al.* [22]. Graph states occur in various contexts in quantum information theory, in which multiparty quantum correlations play a central role. Examples are multiparty quantum communication, measurement-based quantum computation, and quantum error correction. Prominent examples of two-colorable graph states are GHZ states, cluster states [4], and codewords of error correction codes [66] (see, e.g., [61]). In fact, as has been shown recently [64], two colorable graph states are equivalent to codewords of the CSS codes. We also remark that the correlation operators $\{K_j\}$ are the generators of a group which is often called stabilizer of the state $|\Phi_0\rangle_G$, and the corresponding description in terms of the stabilizers is also referred to as the stabilizer formalism.

We will also consider mixed states ρ , which for a given graph G can be written in the corresponding graph state basis $\{|\Phi_{\mu}\rangle_G\}$, $\rho = \sum_{\mu, \nu} \lambda_{\mu\nu} |\Phi_{\mu}\rangle \langle \Phi_{\nu}|$. We will often be interested in fidelity of the mixed state, i.e., the overlap with some desired pure state, say $|\Phi_0\rangle_G$, $F = \langle \Phi_0 | \rho | \Phi_0 \rangle$. We remark that depolarization of ρ to a standard form ρ_G ,

$$\rho_G = \sum_{\mu} \lambda_{\mu} |\Phi_{\mu}\rangle \langle \Phi_{\mu}| \quad (11.26)$$

can be achieved by randomly applying correlation operators K_j [60, 61]. The diagonal elements, in particular the fidelity, are left unchanged by this depolarization procedure. Note that both the notation and the description of the depolarization procedure are similar to those used for Bell states in this chapter. Bell states—as used in this chapter—are in fact graph states with two vertices, connected by a single edge.

11.6.2 Recurrence protocol

In the following, we will discuss a family of entanglement purification protocols that allow one to purify an arbitrary two-colorable graph state. To be precise, for each two colorable graph

there exists a purification protocol that allows one to obtain the pure state $|\Phi_0\rangle_G$ as output state, provided the initial fidelity is sufficiently large. The recurrence scheme [60,61] to purify a two-colorable graph state is very similar to the BBPSSW and DEJMPS protocol to purify Bell pairs. We consider two subprotocols, $P1$ and $P2$, each of which acts on two identical copies $\rho_1 = \rho_2 = \rho$, $\rho_{12} \equiv \rho_1 \otimes \rho_2$. The basic idea consists again in transferring (nonlocal) information about the first pair to the second, and reveal this information by measurements.

In subprotocol $P1$, all parties who belong to the set A apply local CNOT operations [44] to their particles, with the particle belonging to ρ_2 as source, and ρ_1 as target. Similarly, all parties belonging to set B apply local CNOT operations to their particles, but with the particle belonging to ρ_1 as source, and ρ_2 as target. The action of such a multilateral CNOT operation is given by [60]

$$|\Phi_{\mu_A, \mu_B}\rangle |\Phi_{\nu_A, \nu_B}\rangle \rightarrow |\Phi_{\mu_A, \mu_B \oplus \nu_B}\rangle |\Phi_{\nu_A \oplus \mu_A, \nu_B}\rangle, \quad (11.27)$$

where $\mu_A \oplus \nu_A$ denotes bitwise addition modulo 2.

The second step of subprotocol $P1$ consists of a measurement of all particles of ρ_2 , where the particles belonging to set A [B] are measured in the eigenbasis $\{|0\rangle_x, |1\rangle_x\}$ of σ_x [$\{|0\rangle_z, |1\rangle_z\}$ of σ_z] respectively. The measurements in sets A [B] yield results $(-1)^{\xi_j}$ [$(-1)^{\zeta_k}$], with $\xi_j, \zeta_k \in \{0, 1\}$. Only if the measurement outcomes fulfill $(\xi_j + \sum_{\{k,j\} \in E} \zeta_k) \bmod 2 = 0 \forall j$ —which implies $\mu_A \oplus \nu_A = 0$ —the first state is kept. In this case, one finds that the remaining state is again diagonal in the graph-state basis, with new coefficients

$$\tilde{\lambda}_{\gamma_A, \gamma_B} = \sum_{\{(\nu_B, \mu_B) | \nu_B \oplus \mu_B = \gamma_B\}} \frac{1}{2K} \lambda_{\gamma_A, \nu_B} \lambda_{\gamma_A, \mu_B}, \quad (11.28)$$

where K is a normalization constant such that $\text{tr}(\tilde{\rho}) = 1$, indicating the probability of success of the protocol.

In subprotocol $P2$ the roles of sets A and B are exchanged. The action of the multilateral CNOT operation is in this case given by

$$|\Psi_{\mu_A, \mu_B}\rangle |\Psi_{\nu_A, \nu_B}\rangle \rightarrow |\Psi_{\mu_A \oplus \nu_A, \mu_B}\rangle |\Psi_{\nu_A, \nu_B \oplus \mu_B}\rangle, \quad (11.29)$$

which leads to new coefficients

$$\tilde{\lambda}'_{\gamma_A, \gamma_B} = \sum_{\{(\nu_A, \mu_A) | \nu_A \oplus \mu_A = \gamma_A\}} \frac{1}{2K} \lambda_{\nu_A, \gamma_B} \lambda_{\mu_A, \gamma_B}, \quad (11.30)$$

for the case in which the protocol $P2$ was successful.

The total purification protocol consists in a sequential application of subprotocols $P1$ and $P2$. While subprotocol $P1$ serves to gain information about μ_A , subprotocol $P2$ reveals information about μ_B . Typically, subprotocol $P1$ increase the weight of all coefficients λ_{0, μ_B} , while $P2$ amplifies coefficients $\lambda_{\mu_A, 0}$. In total, this leads to the desired amplification of $\lambda_{0,0}$.

The regime of purification in which these recurrence protocols can be successfully applied is rather difficult to determine analytically, due to the nontrivial structure of the nonlinear maps describing the protocol. Numerical investigation has been performed in [61], and we refer the interested reader to this article for details. We remark here that the fidelity does not provide a suitable measure to compare purification regimes for different number of particles n , as typically the required fidelity will decrease exponentially for all states. This is related

to the exponential growth of the dimension of the Hilbert space with the number of particles n . One can alternatively consider the maximum acceptable amount of local noise per particle such that the state remains distillable by means of the recurrence protocol. That is, one assumes that each of the particles belonging to a given graph state is sent through a noisy quantum channel (e.g., a depolarizing channel) to its final location. One then finds for linear cluster states (or, more generally, all graph states with a constant degree) that the maximum acceptable amount of noise per particle is essentially independent of the particle number. For GHZ states, however, the acceptable amount of noise per particle decreases with increasing particle number. That is, GHZ states of large number of particles become more and more difficult to purify as the number of particles increases.

11.6.2.1 Example: Binary-type like mixture

It is illustrative to consider the purification of a special family of states in some detail. We consider the example of mixed states of the form

$$\rho_A \equiv \sum_{\mu_A} \lambda_{\mu_A,0} |\Phi_{\mu_A,0}\rangle \langle \Phi_{\mu_A,0}|. \quad (11.31)$$

These states arise, e.g., in a (hypothetical) scenario where all particles within set A are only subjected to phase flip errors (described by σ_z), while all particles within set B are subjected to bit flip errors (σ_x). The iterative application of protocol $P1$ is sufficient to purify states of the form (11.31), as only information about μ_A has to be extracted. A single application of protocol $P1$ leads again to a state of the form ρ_A , with new coefficients

$$\tilde{\lambda}_{\mu_A,0} = \lambda_{\mu_A,0}^2 / K, \quad (11.32)$$

where $K = \sum_{\mu_A} \lambda_{\mu_A,0}^2$ is a normalization constant indicating the probability of success of the protocol. That is, the largest coefficient is amplified with respect to the other ones. Iteration of the protocol $P1$ thus allows one to produce pure graph states $|\Phi_{0,0}\rangle$ with arbitrary high accuracy, given the coefficient $\lambda_{0,0}$ is larger than all other coefficients $\lambda_{\mu_A,0}$. The family of states ρ_A includes states up to rank 2^{n_A} , where n_A denotes the number of particles in group A . Depending on the corresponding graph, n_A can be as high as $n - 1$ and hence the rank can be as high as 2^{n-1} .

As a concrete example, consider the one parameter family $\rho_A(F)$ with $\lambda_{0,0} = F$, $\lambda_{\mu_A,0} = (1 - F)/(2^{n_A} - 1)$ for $\mu_A \neq 0$, where F is the fidelity of the desired state. Application of protocol $P1$ keeps the structure of those states and leads to

$$\tilde{F} = \frac{F^2}{F^2 + (1 - F)^2 / (2^{n_A} - 1)}. \quad (11.33)$$

This map has $\tilde{F} = 1$ as an attracting fixed point for $F \geq 1/2^{n_A}$. The probability of success for a single step is given by $p = F^2 + (1 - F)^2 / (2^{n_A} - 1)$.

11.6.3 Hashing protocol

In a similar way, one can design a hashing protocol for any two-colorable graph state. The first protocol of this type, capable of purifying GHZ states with nonzero yield, was introduced

in [50]. Hashing protocols for arbitrary two-colorable graph states were presented in [61, 64]. The central tool in these protocols is already evident from Eqs. (11.27), (11.29). These equations state how information about indices are transferred from one state to another. To be more precise, information about all indices belonging to set A is transferred from copy one to copy two by the multilateral CNOT operations as specified in the first step of protocol $P1$, while information transfer occurs for all indices corresponding to set B when the direction of CNOT operations is reversed (as it is done in $P2$). Again, by determining the parity of the bit values for random subsets—which is done in a similar way as for Bell pairs, but here all bits belonging to set A or B can be determined simultaneously—one can learn the required amount of information in such a way that the remaining ensemble is in a tensor product of pure graph states. To be precise, one needs to learn the classical information which nonlocal state is at hand.

The yield of the hashing protocol approaches unity for any state diagonal in the graph state basis with $\lambda_0 \rightarrow 1$, independent of the specific form of the state. This implies that a given mixed state of sufficiently high fidelity F can be purified with nonzero yield using the hashing protocol (combined with the depolarization procedure).

11.6.4 Entanglement purification of nonstabilizer states

While all bipartite and multipartite entanglement purification protocols we have described so far purify stabilizer states, i.e., states which are eigenstates of local stabilizer operators, very recently a multipartite entanglement purification protocol was obtained [65] that allows one to purify a nonstabilizer state, in particular a W state,

$$|W\rangle = 1/\sqrt{3}(|001\rangle + |010\rangle + |100\rangle). \quad (11.34)$$

This protocol is a $3 \rightarrow 1$ protocol and, among other interesting features, it has not only the 3-particle W state but also maximally entangled states shared between two of the parties as attracting fixed points [65].

11.7 Distillability with Noisy Apparatus

In this section, we investigate the performance of entanglement distillation protocols under nonidealized conditions, i.e., for noisy local control operations. The main effect of noise is that no longer maximally entangled states can be produced, but the achievable fidelity is limited to values smaller than unity. Similarly, the required initial fidelity in the case of noisy local control operations is larger. While recurrence protocols remain applicable to increase the fidelity of states, hashing and breeding protocols become impractical.

11.7.1 Distillable entanglement and yield

Using the standard definition of distillability and yield is clearly inappropriate in the case of imperfect local operations. In particular, no maximally entangled pure states can be created in this case. This implies that no state will be distillable, and that the yield is zero. We therefore have to adopt the definition of distillability and yield to account for these facts.

Rather than demanding that maximally entangled pure states can be created (fidelity $F = 1$), we will consider the creation of states with certain fidelity. Distillability refers in this case to the possibility of approximating a given target state ψ with fidelity $F \geq F_c$. Clearly, such a definition of distillability depends on both the required target state ψ and the desired fidelity F_c . To be more precise, we say that a given mixed state ρ is distillable with respect to a target state ψ and fidelity F_c if one can generate from possible many copies of ρ by means of local operations and classical communication a state σ such that the fidelity of σ with respect to ψ is larger than or equal to F_c , $\langle \psi | \sigma | \psi \rangle \geq F_c$.

One may also consider the yield of purification procedures corresponding to this notion of distillability, D_{ψ, F_c} . In this case, however one needs to specify the exact structure of target states. In particular, when considering general distillation procedures (e.g., $N \rightarrow M$ protocols), one obtains as output a mixed state Γ of a large number of particles. Here we will demand that the output state Γ is a *tensor product* of states σ_k , $\Gamma = \otimes \sigma_k$, where each of the σ_k fulfills $\langle \psi | \sigma_k | \psi \rangle \geq F_c$. That is, we require that after the purification procedure one possesses independent copies of the state with desired fidelity. One may also use the weaker criterion that all reduced density operators $\tilde{\sigma}_k$ (corresponding to different output “copies” of the output state) have fidelity $F \geq F_c$, where $\tilde{\sigma}_k$ are obtained from Γ by tracing out all particles but those corresponding to state k . In this case, however, it is not clear whether the different output states can be independently used for all applications. While their fidelities certainly fulfill $F \geq F_c$, there might be classical correlations among the output states that are limiting their applicability, e.g., for security applications such as key distribution.

In this context it would be interesting to see whether the definition of yield with respect to fidelities of reduced density operators is equivalent to those we use here. To this aim, one would need to show that one can produce from an ensemble of states where all reduced density operators have a sufficiently high fidelity an ensemble which consists of a tensor product of copies, where the size of the ensembles might be diminished by a sublinear amount, or the fidelity be reduced by some (arbitrarily small) δ_F . Such a “purification of classical correlations” has, however, not been reported so far.

11.7.2 Error model

To analyze the influence of noisy local operations, we will consider a simple error model where only local two-qubit operations are noisy, and the noise is of a simple, local form. More general error models, including correlated noise and also errors in measurements, have been analyzed, leading essentially to the same qualitative behavior of entanglement purification protocols [6, 10, 61, 62].

We model a noisy two-qubit operation U by first applying local noise to each of the qubits, followed by the perfect unitary operation U ,

$$\mathcal{E}_{kl}\rho = U_{kl}[\mathcal{M}_k\mathcal{M}_l\rho]U_{kl}^\dagger. \quad (11.35)$$

We will mainly assume that local completely positive maps $\mathcal{M}_k, \mathcal{M}_l$ are described by white noise (depolarizing channels),

$$\mathcal{M}_k\rho = p\rho + (1-p)/4 \sum_{j=0}^3 \sigma_j^{(k)} \rho \sigma_j^{(k)}, \quad (11.36)$$

where σ_j denote Pauli operators with $\sigma_0 = \mathbb{1}$. In some cases, we will consider even more restricted noise models, namely local dephasing channels (or phase-flip channels), $\mathcal{M}_k^P \rho = p\rho + (1-p)/2(\rho + \sigma_3^{(k)} \rho \sigma_3^{(k)})$ and local bit-flip channels, $\mathcal{M}_k^B \rho = p\rho + (1-p)/2(\rho + \sigma_1^{(k)} \rho \sigma_1^{(k)})$.

11.7.3 Bipartite recurrence protocols

We start by analyzing the BBPSSW protocol, where we assume local white noise channels as described by Eq. (11.36), but for simplicity perfect local measurements. Given two copies of a Werner state Eq. (11.18), the influence of noisy local control operations—in this case noisy CNOT operations—can be readily obtained. The action of noisy bilateral CNOT operations is the same as applying noiseless bilateral CNOT operations to two copies of Werner states with reduced fidelity. In particular, one finds that the parameter x is reduced to xp^2 due to the local depolarizing noise. That is, one applies the original protocol to two copies of Werner states $\rho_W(xp^2)$. Rewriting Eq. (11.20), i.e., the fidelity of output state as a function of input state, in terms of parameter $x = (4F - 1)/3$, one obtains $x' = (4x^2 + 2x)/(3x^2 + 3)$. Taking into account the effect of noisy local operations, i.e., the reduction of x , we obtain that the output state after applying one purification step is again a Werner state $\rho_W(x')$ with

$$x' = \frac{4x^2 p^4 + 2xp^2}{3x^2 p^4 + 3}. \quad (11.37)$$

That is, the purification curve (the fidelity of the output state plotted against the fidelity of the input state) is shifted down (see Fig. 11.1).

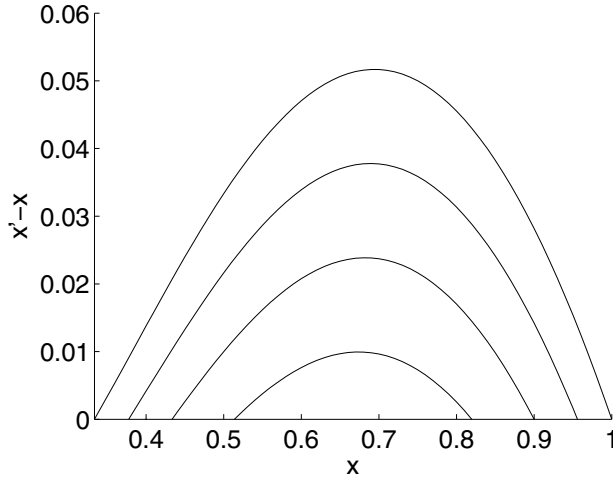


Figure 11.1. Purification curve for the BBPSSW protocol. Gain in output fidelity $x' - x$, plotted against input fidelity x . Curves from top to bottom correspond to error parameters $p = 1, 0.99, 0.98, 0.97$ respectively.

It is now straightforward to determine the maximal reachable fidelity as well as the minimal required fidelity such that entanglement purification can be successfully applied. These quantities are given by the fixed points of the map, Eq. (11.37). One finds

$$x_{\pm} = \frac{2}{3} \pm \frac{1}{3} \sqrt{4 + 6p^{-2} - 9p^{-4}}, \quad (11.38)$$

where the maximum reachable fidelity $F_{\max} = (3x_+ + 1)/4$ and the minimum required fidelity $F_{\min} = (3x_- + 1)/4$. The threshold value for p such that a finite purification regime remains (i.e., $x_+ > x_-$) is given by $p_{\min} = 0.9628$. This implies that errors of the order of 4% are tolerable.

One can perform a similar analysis for the DEJMPS and (nested) entanglement pumping protocol. There, the fixed points of the corresponding nonlinear maps are more difficult to obtain analytically. One can, however, perform the analysis numerically and obtains [6, 10] that (i) the maximum reachable fidelity $F_{\max}$ for the DEJMPS protocol is significantly higher than for the BBPSSW protocol; (ii) the minimal required fidelity $F_{\min}$ for the DEJMPS is significantly smaller than for the BBPSSW; (iii) the threshold for noisy operations described by $p_{\min}$ is smaller for the DEJMPS protocol and (iv) reachable fidelity, minimum required fidelity and threshold for noisy operations seem to be the same for nested entanglement pumping and for the original DEJMPS protocol [10].

When assuming correlated white noise errors for local operations and errors in measurements of same order of magnitude [33], one finds tolerable errors of about 3% for the BBPSSW protocol, and 5% in the case of the DEJMPS protocol.

11.7.4 Multipartite recurrence protocols

A similar analysis can be performed for multipartite entanglement purification protocols [61]. Numerical results for the purification range (minimal required and maximal reachable fidelity) as well as error threshold for linear cluster states of different sizes are given in Fig. 11.2. Again, errors of the order of several percent are tolerable.

An important observation is that the threshold value $p_{\min}$ is for linear cluster states independent of the number of particles n . That is, also multipartite states of large number of particles can be successfully purified, and the requirements on local control operations are independent of the system size. This is not true when attempting to purify GHZ states [61], where one finds that the required fidelity of local control operations depends on the particle number.

The qualitative difference of cluster and GHZ states can already be understood from an analytically solvable toy model [61], where one considers mixtures of GHZ states $|\Phi_{0,0}\rangle$ and $|\Phi_{1,0}\rangle$ and a restricted error model of only bit flip errors in set B that keep the structure of such states. Using that bit flip errors in B act as phase flip errors in A , and the fact that subprotocol $P1$ is sufficient to purify such states, one obtains a lower bound on the threshold value $p_{\min}$ given by $p_{\min} = (\frac{1}{2})^{1/(n-1)}$. This follows from arguments along the same lines as used in the derivation of purification curve for the bipartite BBPSSW protocol. Performing a similar analysis for binary-like mixtures of linear cluster states under this restricted noise model, one observes that the threshold value $p_{\min}$ is essentially independent of the number of particles

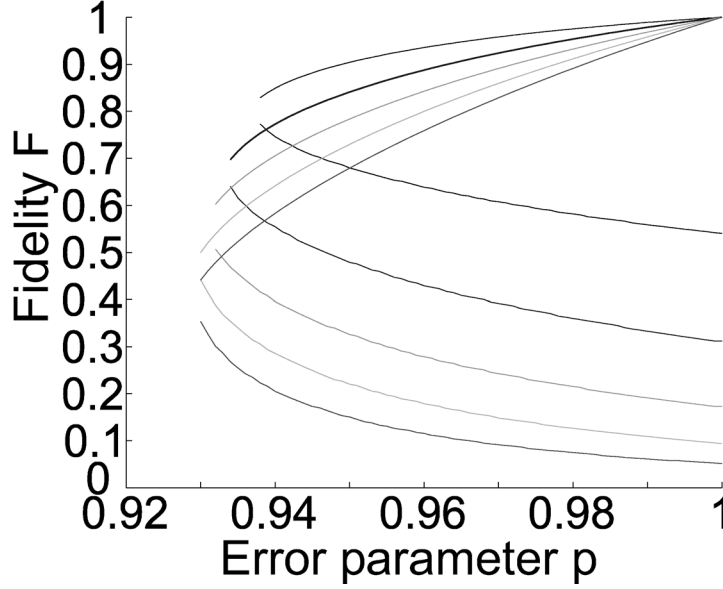


Figure 11.2. Maximal reachable fidelity $F_{\max}$ and minimal required fidelity $F_{\min}$ plotted against error parameter p (local operations) for density operators arising from single-qubit white noise. Curves from top to bottom correspond to linear cluster states with $n = 2, 4, 6, 8, 10$ particles. Figure taken from [60].

n , in agreement with the numerical observations for systems of up to size $n = 10$ for a more general noise model.

11.7.5 Hashing protocols

While for perfect local operations recurrence protocols have zero yield, only hashing protocols, operating simultaneously on an asymptotic number of copies, have a nonzero yield. For imperfect local operations, the situation changes drastically. When requiring output states to have only a sufficiently high fidelity $F \geq F_c$, one finds that recurrence protocols may have a nonzero yield as long as $F_c \leq F_{\max}$, i.e., as long as the required fidelity is smaller than the fidelity reachable by the protocol. At the same time, the hashing protocol fails completely in the case of imperfect local operations. The reason for this is that one operates on a asymptotic amount of states $m \rightarrow \infty$ to reveal one bit of information. That is, one performs m bilateral CNOT operations with a given copy always serving as target state. As each of the CNOT operations is noisy, noise is accumulated in the target state. Assuming that the target state was initially in a maximally entangled pure state, the target state ends up in a Werner state $\rho_W(p^{2m})$. Clearly, if the amount of noise is too big (as is the case for sufficiently large m , in particular for $m \rightarrow \infty$, even if p is close to 1), no information about the remaining ensemble can be extracted. In other words, the information loss due to imperfect local operations ex-

ceeds the possible information gain per measurement (maximum one bit). This implies that hashing in its original form cannot be applied in the case of imperfect local operations.

It would be interesting to perform a detailed analysis of the performance of general $N \rightarrow M$ protocols for finite N in the presence of noisy operations. First steps in this direction have been reported in [48].

11.8 Applications of Entanglement Purification

We now turn to applications of entanglement purification. Although entanglement purification was introduced in the context of quantum communication—as a means to overcome the limitations of noisy quantum channels—additional applications of entanglement purification were subsequently identified. In fact, over the last few years the picture has emerged that entanglement purification constitutes a fundamental tool in quantum information processing. Here, we briefly discuss applications of entanglement purification in quantum communication, secure state distribution, quantum error correction, and quantum computation.

11.8.1 Quantum communication and cryptography

In a (multiparty) quantum communication scenario, two (or more) parties attempt to communicate and exchange quantum information. They might, e.g., want to establish a secret key—to ensure secure classical communication, or to perform distributed quantum computation. When dealing with realistic scenarios, both the quantum channels and local control operations are noisy. This limits the possibility to faithfully transmit quantum information in a direct way, and additional effort is required to overcome the influence of noise.

While classical information can be transmitted over basically arbitrary distances using repeaters, the situation is more complicated in the case of quantum information. There, the no-cloning theorem does not permit to copy or amplify a quantum signal. However, one may use techniques from quantum error correction, and encode each qubit of the transmitted signal into several qubits. This technique, known as redundant coding, allows one in principle to faithfully transmit quantum information over noisy channels. One has, however, a substantial overhead, and the requirements on intermediate error detection and correction procedures are rather stringent (same as for fault-tolerant quantum computation).

An alternative approach is given by entanglement purification. It is sufficient to generate a *known* maximally entangled state shared between two parties to ensure perfect quantum communication. This is due to the fact that such states (together with classical communications) provide the necessary resource to perform teleportation. Thus the problem of transmitting *arbitrary, unknown quantum* states over noisy channels reduces to the generation of a *specific, known* maximally entangled state as long as classical communication is available. Such a task seems to be much easier to achieve. In fact, when assuming perfect local control operations, entanglement purification protocols for bipartite systems allow one to faithfully transmit quantum information if the channel noise is not too big. To be precise, a sufficient condition that entanglement purification can be applied is, when sending part of a maximally entangled state through the noisy channel, that the output state has fidelity $F > 1/2$. If this is not the case—

as might for example happen if the distance between parties is large—one may use *quantum repeaters*, described in detail in Chapter 26.

In the case where not only the channels but also the local operations are imperfect, entanglement purification can still be applied. As we have seen in the previous section, one can increase the fidelity of entangled states—and hence the quality of the channel when using the purified entangled states for teleportation. More importantly, the entanglement produced by entanglement purification, although not perfect, is *private* [67]. That is, although no maximally entangled states can be produced, any eavesdropper will be factored out. This implies that a secret key can be established between two parties, even in the presence of noisy channels and imperfect apparatus [67]. This provides an alternative proof of unconditional security of quantum key distribution, and is an important application of entanglement purification for quantum cryptography.

11.8.2 Secure state distribution

The secure and secret distribution of an unknown multipartite state with high fidelity provides a basic quantum primitive, as multipartite entangled states can serve as a resource to perform certain quantum information processing tasks. The specific type of entanglement determines the tasks that can be performed. Hence it is easy to imagine scenarios where the involved parties do not want any third party to learn which secret state they possess, and they wish at the same time their entanglement to be private. While in an idealized scenario where one assumes perfect local operations, this task can be achieved rather easily, under nonidealized conditions (as one typically faces) the problem becomes nontrivial. (Multipartite) entanglement purification is the main tool to achieve the secure and secret distribution of high-fidelity multipartite entanglement. However, standard entanglement purification protocols need to be adopted to take care of additional secrecy and security requirements. In particular, even parties involved in the purification process may not be allowed to learn which state they are purifying.

In [68], three different solutions to the secure-state distribution problem were put forward. The first solution is based on bipartite entanglement purification, which serves to purify channels. Together with teleportation, this enables one to generate arbitrary multipartite entangled states. The second solution makes use of direct multipartite entanglement purification protocols, which is combined with basis randomization and adopted accordingly to ensure security. Security in the third solution, again based on direct multipartite purification, is ensured by purifying enlarged states. Each of the solutions offers its own advantages, and there in fact exist parameter regimes (for local noise, channel noise, desired target fidelity) such that one of the three schemes can be applied, while the other two fail.

11.8.3 Quantum error correction

Since certain two-colorable graph states constitute codewords of error correction codes, one may use the purification of these graph states to achieve high fidelity encoding without making use of complicated encoding networks [61]. In particular, a certain 7-qubit code (a Calderbank-Shore-Steane $(7, 1, 3)$ code) can be obtained by using a two-colorable graph state of eight vertices (a cube) as resource, and teleportation. Concatenated codes of this kind can be obtained by appending to each vertex of the cube another cube. Encoding into the graph

state can be achieved by a single Bell measurement [61], where the qubit to be encoded is coupled by the Bell measurement to the eighth vertex of the cube. A similar procedure is considered for the (5, 1, 3) code in [66], where the notion of graph codes was introduced. The fidelity of the encoding mainly depends on the fidelity of the two-colorable graph state used in the procedure described above. Hence, multipartite entanglement purification can be applied to generate high fidelity entangled states which are then used to achieve high fidelity encoding.

11.8.4 Quantum computation

11.8.4.1 One-way quantum computation

In the one-way quantum computer model, a multipartite entangled state, the cluster state, serves as a universal resource for quantum computation [4]. That is, given a cluster state of suitable size, an arbitrary quantum algorithm can be implemented by a sequence of single qubit measurements. In a similar way, other graph states represent algorithmic specific resources, i.e., allow one to implement a specific algorithm (depending on the graph state) by means of single qubit measurements [63]. In the presence of imperfect operations, the cluster or graph state may not be available with unit fidelity. However, entanglement purification may be applied to increase fidelity and hence to reduce errors in quantum computation. To what extent the purification of graph states can be used in fault-tolerant quantum computation is subject of current research.

11.8.4.2 Improving error thresholds

Under certain circumstances, entanglement purification can be used directly to weaken the requirements for fault-tolerant quantum computation [10]. Consider a situation where n systems, each of them possessing d degrees of freedom, are available. For instance, one may think of n neutral atoms or trapped ions, each of them constituting a d level system. While typically only two of the levels are used for quantum computation, in principle many levels are available. In this case, one can show that the threshold for fault-tolerant quantum computation essentially only depends on the fidelity of single system operations [10]. Two system operations, i.e., interactions between two systems, are typically more difficult to realize than single system operations (e.g., operations on a single atom). However, it turns out that one can tolerate a noise level of more than 50% for two-system operations, while still achieving fault-tolerant quantum computation if the single system operations are of sufficiently high fidelity.

The basic idea is that one uses each d -level system to represent one qubit for computation, while the remaining degrees of freedom serve as auxiliary levels. The noisy two-system interaction serves to entangle auxiliary degrees of freedom, and one may use entanglement purification to increase the fidelity of this entanglement. Finally, high fidelity entangled states are used to realize two-system gates, e.g., by means of teleportation-based gates. The fidelity of the two-system gate is essentially determined by the fidelity of the entangled state, which, in turn, is determined by the fidelity of single-system operations used in entanglement purification.

We remark that at least four auxiliary levels should be available. By using nested entanglement pumping, as discussed in Section 11.4.2.3, it turns out in relevant parameter regimes, a few (2-3) nesting levels are sufficient to obtain high fidelity entanglement. This translates into a total requirement of about 16 levels per system, and a required error threshold of about 10^{-5} for single system operations to achieve errors of 10^{-4} for (logical) two-system operations, which is sufficient to achieve fault-tolerant quantum computation. The error rate of the physical two-system operation can, however, be almost arbitrarily large (more than 50%).

A similar method can be used in a more direct way to achieve lower error thresholds for quantum computation. The basic idea is to generate multiparty, high fidelity entangled states, either by entanglement purification or by using error detection schemes or combination of both. These multipartite entangled states serve to implement one- and two-qubit gates among the logical (encoded) qubits, e.g., by using teleportation-based gates. A proposal along these lines was recently put forward by Knill [11], where he reports a substantial reduction of required error threshold for fault-tolerant quantum computation. He estimates an error threshold of the order of 10^{-2} , i.e., tolerable errors of the order of 1.

11.9 Summary and Conclusions

In this chapter, we have given a brief overview over entanglement purification and distillation. We started by considering the transformation of (multipartite) pure entangled states. In the later sections, we focused on mixed states. For bipartite systems, we introduced the concept of distillability, and gave necessary and sufficient conditions. We also discussed a number of known entanglement purification protocols, in particular recurrence protocols and the hashing protocol. We generalized the notion of distillability to multipartite systems. Based on necessary conditions for distillability, we have identified different bound entangled states. We have also discussed entanglement purification protocols for all entangled states that correspond to two-colorable graphs. We analyzed both bipartite and multipartite purification protocols in the presence of imperfect operations, and found a remarkable robustness against local noise. We finally discussed a number of possible applications of entanglement purification. We are confident that entanglement purification will turn out to constitute one of the main tools for quantum information processing, and will find widespread application in both quantum communication and quantum computation.

Acknowledgments

This work was supported in part by the Austrian Science Foundation (FWF), the European Union (IST-2001-38877,-39227,OLAQUI,SCALA), the Österreichische Akademie der Wissenschaften through project APART (W.D.), and the Deutsche Forschungsgemeinschaft (DFG).

Glossary

LOCC: local operations and classical communication

SLOCC: stochastic local operations and classical communication

PPT: positive partial transpose, all eigenvalues of the partial transposed operator are positive, that is, larger than or equal to zero (see Section 11.3.2.1)

NPT: negative partial transpose, at least one eigenvalue of the partial transposed operator is negative (see Section 11.3.2.1)

GHZ-state: Greenberger–Horne–Zeilinger state, $|\Psi\rangle = 1/\sqrt{2}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$.

References

- [1] E. Schrödinger, Die Naturwissenschaften **23**, 807–812; 823–828; 844–849 (1935); E. Schrödinger, Proc. Camb. Phil. Soc. **31**, 555 (1935).
- [2] Bennett C. H., Brassard, G., Crepeau, C., Josza, R., Peres, and A. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [3] A. K. Ekert, Phys. Rev. Lett. **70**, 661 (1991).
- [4] R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
- [5] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
- [6] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169–181 (1999).
- [7] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [8] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
- [9] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
- [10] W. Dür and H.-J. Briegel, Phys. Rev. Lett. **90**, 067901 (2003).
- [11] E. Knill, Nature **434**, 39 (2005); E. Knill, *Preprint* quant-ph/0410199.
- [12] J.W. Pan, C. Simon, C. Brukner, and A. Zeilinger, Nature **409**, 1067 (2001).
- [13] M.A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
- [14] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
- [15] M. Nielsen and G. Vidal, Quant. Inf. Comp. **1**, 76 (2001).
- [16] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
- [17] H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001).
- [18] L. Hardy, Phys. Rev. A **60**, 1912 (1999).
- [19] A. Acin, A. Andrianov, L. Costa, E. Jane, J. I. Latorre, and R. Tarrach, Phys. Rev. Lett. **85**, 1560 (2000).
- [20] H. A. Carteret, A. Higuchi, and A. Sudbery, J. Math. Phys. **41**, 7932 (2000).
- [21] J. Eisert and H.-J. Briegel, Phys. Rev. A **64**, 022306 (2001).

- [22] M. Hein, J. Eisert, and H.-J. Briegel, Phys. Rev. A **69**, 062311 (2004).
- [23] W. Dür, G. Vidal, and J.I. Cirac, Phys. Rev. A **62**, 062314 (2000).
- [24] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde, Phys. Rev. A **65**, 052112 (2002).
- [25] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, *Preprint quant-ph/9912039*.
- [26] G. Vidal, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **85**, 658 (2000).
- [27] A. Acin, G. Vidal, and J. I. Cirac, Quant. Inf. Comp. **3**, 55 (2003).
- [28] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal Phys. Rev. A **63**, 012307 (2001).
- [29] E. M. Rains, Phys. Rev. A **60**, 179 (1999); Erratum Phys. Rev. A **63**, 019902 (2001). E.M. Rains, *Preprint quant-ph/0008047*.
- [30] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [31] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
- [32] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
- [33] W. Dür, D. Bruss, M. Lewenstein, and J.I. Cirac, Phys. Rev. A **61**, 062313 (2000).
- [34] D. P. DiVincenzo, R. Jozsa, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
- [35] S. Bandyopadhyay and V. Roychowdhury, Phys. Rev. A **68**, 022319 (2003).
- [36] J. Watrous, Phys. Rev. Lett. **93**, 010502 (2004).
- [37] P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **86**, 2681-2684 (2001).
- [38] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
- [39] N. Gisin, Phys. Lett. A **210**, 151 (1996).
- [40] N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **81**, 3279 (1998).
- [41] A. Kent, Phys. Rev. Lett. **81**, 2839 (1998).
- [42] R.F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [43] The Hadamard operation H maps basis state of z basis to basis states of x basis and vice versa, i.e., $H|k\rangle_z = |k\rangle_x$, $H|k\rangle_x = |k\rangle_z$ with $k = 0, 1$.
- [44] The CNOT operation is defined by $|i\rangle_A|j\rangle_B \rightarrow |i\rangle_A|i \oplus j\rangle_B$, where $\oplus$ denotes addition modulo 2.
- [45] C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
- [46] W. Dür and J. I. Cirac, Phys. Rev. A **61**, 042314 (2000);
- [47] W. Dür and J. I. Cirac, Phys. Rev. A **62**, 022302 (2000).
- [48] H. Aschauer, PhD thesis, Sektion Physik, Ludwig Maximilians Universität München (2004).
- [49] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Phys. Rev. A **67**, 022310 (2003).
- [50] E. N. Maneva and J. A. Smolin, in *Quantum Computation and Quantum Information*, edited by J. Samuel J. Lomonaco (American Mathematical Society, Providence, RI, 2002), Vol. 305 of *AMS Contemporary Mathematics*; see also *Preprint quant-ph/0003099*.
- [51] K. G. H. Vollbrecht and F. Verstraete, *Preprint quant-ph/0404111*.

- [52] K. G. H. Vollbrecht and M. M. Wolf, Phys. Rev. A **67**, 012303 (2003).
- [53] H. Bombin and M.A. Martin-Delgado, *Preprint* quant-ph/0503013.
- [54] I. Devetak and A. Winter, Proc. R. Soc. Lond. A, **461**, 207 (2005).
- [55] To be precise, one has to consider in addition also states with $m_{00} = (FN \pm O(\sqrt{N}))$ and similarly for m_{ij} .
- [56] W. Dür, P. Horodecki and J.I. Cirac, Phys. Rev. Lett. **93**, 020503 (2004).
- [57] W. Dür and J. I Cirac, J. Phys. A: Math. Gen. **34**, 6837(2001).
- [58] J. A. Smolin, Phys. Rev. A **63**, 032306 (2001).
- [59] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, R4075 (1998).
- [60] W. Dür, H. Aschauer and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).
- [61] H. Aschauer, W. Dür and H.-J. Briegel, Phys. Rev. A **71**, 012319 (2005).
- [62] G. Giedke, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 2641 (1999).
- [63] R. Raussendorf, D. Browne, and H.-J. Briegel, Phys. Rev. A **68**, 022312 (2003).
- [64] Kai Chen and Hoi-Kwong Lo, *Preprint* quant-ph/0404133.
- [65] A. Miyake and Hans J. Briegel, *Preprint* quant-ph/0506092.
- [66] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2002); M. Grassl *et al.*, in *Proceedings of the ISIT, Lausanne, 2002* (IEEE, Piscataway, NJ, 2002), p. 45.
- [67] H. Aschauer and H.-J. Briegel, Phys. Rev. Lett. **88**, 047902 (2002).
- [68] W. Dür, J. Calsamiglia, and H.-J. Briegel, Phys. Rev. A **71**, 042336 (2005).

12 Bound Entanglement

Paweł Horodecki

12.1 Introduction

Quantum entanglement is one of the central notions of quantum information theory [1]. One of the basic questions in the entanglement theory is distillability of composite mixed quantum states [2]. Roughly speaking a state is distillable if it can be converted into a pure maximally entangled state via local operations and classical communication (LOCC) [2, 3]. The concept of distillation of “noisy” entanglement has played an important role in quantum communication. In particular, it provides a useful technique to achieve quantum channel capacity [3]. It has been shown [4] that all two-spin- $\frac{1}{2}$ $2 \otimes 2$ states are distillable. This result suggested that all noisy states are distillable. However soon it has been proved that for higher dimensions there are entangled states, which cannot be converted by LOCC operations into pure singled form [5]. This new kind of entanglement (called bound entanglement) appeared to be very peculiar and difficult to detect. In a sense it can be seen as a black hole of quantum information theory [6]—in fact it happens that it represents a kind of irreversibility of the process formation of entangled states. Moreover the existence of the bound entanglement suggested that there exists stronger limit on the distillation rate than were expected before. However, on the other hand, it happens that this “black hole” in some sense evaporates, since bound entanglement happened to be useful both directly or as a kind of support resource.

The aim of this paragraph is to present a state-of-the-art of this new form of entanglement and its role in quantum information theory.

12.2 Distillation of Quantum Entanglement: Repetition

12.2.1 Bipartite entanglement distillation

12.2.1.1 LOCC operations.

In entanglement distillation one has an important notion of LOCC operation $\mathcal{L}_{\text{LOCC}}$. This is any map that can be performed with local (in general quantum) operations and classical operations. The LOCC operation that in addition is trace preserving is called a LOCC protocol. The mathematical definition of LOCC protocol is—in general—complicated (see [7]), however any LOCC operation can be represented as a separable operation [8] (though not vice

versa [9]) which is defined as LOCC operation as

$$\mathcal{L}(\varrho_{AB}) = \frac{\sum_i A_i \otimes B_i \varrho_{AB} A_i^\dagger \otimes B_i^\dagger}{\text{Tr}[\sum_i A_i \otimes B_i \varrho_{AB} A_i^\dagger \otimes B_i^\dagger]}, \quad \sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i \leq I \otimes I. \quad (12.1)$$

The LOCC operation is called deterministic (probabilistic) iff it can be performed with unit (arbitrary) probability which on the level of separable superoperators corresponds to $\sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i = I \otimes I$ ($\sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i \leq I \otimes I$). Deterministic LOCC operations are also called *protocols* or *superoperators*.

Let us note that there is a classification of LOCC protocols with respect to the class of classical communication that is allowed to use. Here we shall use only the largest one sometimes called “two-way” LOCC or—in short—just LOCC class.

Example: Important classes of LOCC trace-preserving operation (protocol) are $U \otimes U^*$ and $U \otimes U$ *twirling* operations acting on any $d \otimes d$ states:

$$\begin{aligned} \tau(\varrho) &= \int dU U \otimes U^* \varrho (U \otimes U^*)^\dagger \\ \tau'(\varrho) &= \int dU U \otimes U \varrho (U \otimes U)^\dagger. \end{aligned} \quad (12.2)$$

Especially the first operation is of our interest since it moves any state ϱ into $(U \otimes U^*$ invariant) *isotropic* state [12]

$$\varrho_{\text{iso}}(F) = \frac{1-F}{d^2-1} \mathbb{I} + \frac{Fd^2-1}{d^2-1} P_+, \quad 0 \leq F \leq 1 \quad (12.3)$$

with a parameter

$$F = F_d(\varrho) \equiv \text{Tr}[\varrho P_+^d] \quad (12.4)$$

which is *invariant* under twirling τ for any ϱ . Here by P_+^d we denote a special maximally entangled state of $d \otimes d$ systems:

$$P_+^d = |\Psi_+^d\rangle\langle\Psi_+^d|, \quad (12.5)$$

where $|\Psi_+^k\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle$ belongs to $\mathcal{C}^d \otimes \mathcal{C}^d$. Isotropic states are known to be separable iff $F \leq \frac{1}{d}$ which is an equivalent PPT property [29].

The second twirling is also very important and it moves any state into $(U \otimes U$ invariant) Werner state [14]:

$$\varrho_W(\alpha) = \frac{\mathbb{I} + \alpha V}{d^2 + \alpha d}, \quad -1 \leq \alpha \leq 1 \quad (12.6)$$

with parameter α also uniquely determined by ϱ and invariant under twirling τ' . Werner states are also separable iff they have PPT property.

Example: An important class of probabilistic LOCC operation is local filtering (see [10, 11]) $\tilde{\mathcal{L}}$ in which there is only one product element $A \otimes B(\cdot) A^\dagger \otimes B^\dagger$ instead of the sum in Eq. (12.1).

12.2.1.2 Distillation of entanglement—definition and primary results

In short, distillation of bipartite entanglement is a process [2] in which two distant observers sharing large number n of copies of systems' mixed states produce by means of local (in general quantum) operations and classical communication some number of k_n pairs of qubits close (in the limit of large n) to k_n pairs of maximally entangled two-qubit states.

Equivalently, instead of the latter—as shown in [17]—they can produce bipartite state of two $d_n \otimes d_n$ system close to the maximally entangled state $P_+^{d_n}$ with $k_n = \log d_n$ (here we shall use logarithm with base 2).

More formally one has the following:

Definition 12.1 One can distill entanglement from given bipartite state ϱ_{AB} defined on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ if there exists a sequence of LOCC protocols $\mathcal{P}^n : \mathcal{H}_A \otimes \mathcal{H}_B \rightarrow \mathcal{C}^{d_n} \otimes \mathcal{C}^{d_n}$ such that as a result one gets asymptotically maximally entangled state, i.e.,

$$F_{d_n}(\mathcal{P}^n(\varrho^{\otimes n})) \xrightarrow{n \rightarrow \infty} 1. \quad (12.7)$$

Distillable entanglement of state ϱ_{AB} under the protocols $\mathcal{P}^n$ is defined by $\mathcal{E}_D^{\{\mathcal{P}^n\}}(\varrho_{AB}) \equiv \limsup_n \log d_n/n$. Distillable entanglement of ϱ_{AB} is defined as $\mathcal{D}(\varrho_{AB}) \equiv \sup \mathcal{E}_D^{\{\mathcal{P}^n\}}(\varrho_{AB})$ where supremum is taken over all possible sequences of LOCC protocols $\{\mathcal{P}^n\}$. Finally ϱ_{AB} is called distillable iff $E_D(\varrho_{AB}) > 0$.

The above definition is one of the quite a few ones. Fortunately they all are equivalent (see [17]). There is an important theorem [4] saying that

Proposition 12.1 Any entangled two-qubit state is distillable.

A fundamental property exploited in the proof was that any single copy of entangled two-qubit state can be transformed by probabilistic LOCC filtering operation followed by twirling τ into $2 \otimes 2$ isotropic state with parameter $F > \frac{1}{2}$ for which LOCC distillation—combination of the so-called recurrence and hashing protocols—was already known from [2, 3].

This technique of concatenating LOCC protocols has allowed us to prove the following important result saying that:

Theorem 12.1 The following statements are equivalent:

- (i) Given bipartite state ϱ_{AB} on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ is distillable
- (ii) ([5]) there exist some two-dimensional projectors P, Q (acting on $\mathcal{H}_A^{\otimes n}$ and $\mathcal{H}_B^{\otimes n}$ respectively) and some natural n , such that the “two-qubit-like” state $\varrho^{(n)}(\varrho_{AB}) = P \otimes Q \varrho_{AB}^{\otimes n} P \otimes Q / \text{Tr}[P \otimes Q \varrho_{AB}^{\otimes n} P \otimes Q]$ is entangled.
- (iii) ([5, 81, 84]) there exists LOCC operation (may be probabilistic) such that $\mathcal{L} : \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \rightarrow \mathcal{C}^2 \otimes \mathcal{C}^2$ and natural n such that the resulting state $\mathcal{L}(\varrho_{AB})$ is a two-qubit entangled state.
- (iv) (see [12, 20]) there exists $d \geq 2$, natural n and LOCC (may be probabilistic) operation $\tilde{\mathcal{L}} : \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \rightarrow \mathcal{C}^d \otimes \mathcal{C}^d$ and n such that

$$F_d[\tilde{\mathcal{L}}(\varrho_{AB}^{\otimes n})] > \frac{1}{d}. \quad (12.8)$$

- (v) (cf. [5], [12]) there exists $d \geq 2$ and sequence of LOCC (may be probabilistic) operations $\tilde{\mathcal{L}}^n : \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \rightarrow \mathcal{C}^d \otimes \mathcal{C}^d$ and n such that

$$F_d[\tilde{\mathcal{L}}(\varrho_{AB}^{\otimes n})] \longrightarrow 1. \quad (12.9)$$

In the above case we also have important definition:

Definition 12.2 For any distillable state ϱ take a minimal natural number n_0 for which (ii) is satisfied. We call ϱ the n_0 -copy distillable state.

Quite remarkably there is an important fact [22] (cf. [21]) which shows that with the above results one cannot decide distillability taking only the property of single copy : for $d \geq 9$ and any natural n there exists $d \otimes d$ state such that it is n copy nondistillable but $n + 1$ copy distillable.

The property (iv) above may be to some extent related to the so-called *reduction criterion* of separability connected also to positive maps theory: [12] which states that any separable state ϱ_{AB} satisfies $\varrho_A \otimes \mathbb{I} - \varrho_{AB} \geq 0$, $\mathbb{I} \otimes \varrho_B - \varrho_{AB} \geq 0$ ¹. There is an interesting role of that criterion in distillation:

Theorem 12.2 ([12]) *From any state violating reduction criterion one can distill entanglement. In particular any entangled isotropic state is distillable.*

The explicit so-called recurrence protocol is given in [12]. On the other hand it was a well-known fact that *no entanglement can be distilled from separable states* [3] since there is an elementary Lemma

Lemma 12.1 *Separable operations preserves separability of the state. In particular no entanglement can be created from separable state with help of LOCC operations.*

In fact such a creation would violate monotonicity [23] of any given entanglement measure under LOCC operations.

However, for two years, 1996–1998 the intriguing question whether all the entanglement states are distillable was unsolved, since there was no natural rule, like the above one, known to forbid the positive answer.

12.2.2 Multipartite entanglement distillation

The idea of entanglement distillation can be generalized to multipartite case [24]. The m -partite separable state is defined as

Definition 12.3 The m -partite ϱ is *separable* with respect to the partition $\{I_1, \dots, I_k\}$ and I_i being disjoint subsets of the set of indices $I = \{1, \dots, m\}$ ($\cup_{i=1}^k I_i = I$) iff $\varrho = \sum_{i=1}^N p_i \varrho_1^i \otimes \dots \otimes \varrho_k^i$ where ϱ_i^j is defined on tensor product of all elementary Hilbert spaces corresponding to indices belonging to set I_i . The m -partite state is called *semiseparable* iff it is separable with respect to all 1-to-($m-1$) partitions: $I_k = \{k\}$, $I_k^\perp = \{1, \dots, k-1, k+1, \dots, m\}$, $1 \leq k \leq m$. The m -partite state is called *separable* (or *fully separable*) if it is separable under maximal (m -partite) partition $I_k = \{k\}$, ($k = 1, \dots, m$).

¹Recall that $X \geq 0$ for Hermitian X means that it has nonnegative eigenvalues

The above suggests, what has been shown to be true by analysis initiated in [66], that in general m -partite scenario there are many multipartite pure state classes that are not LOCC equivalent to each other. However, for many reasons, the role of maximally entangled state is considered to be played by GHZ state of $d^{\otimes m} = d \otimes d \otimes \cdots \otimes d$ type

$$|\Psi_+\rangle^{d,(m)} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes m}, \quad (12.10)$$

where $m = 2$ reproduces bipartite case. The definition of distillation of entanglement can be immediately generalized from bipartite to multipartite case via natural generalization of LOCC protocols and operations from multipartite case (local operations and classical communication between all parties). They are also in the class of corresponding separable deterministic and probabilistic operations made from (12.1) by replacing bipartite product operators $A_i \otimes B_i$ with m -partite ones $\otimes_{k=1}^m A_i^k$. There is a theorem (see [24, 26]) based on some fundamental property of the GHZ state

Theorem 12.3 *One can distill m -partite entanglement of GHZ type from given m -party state ϱ if and only if one can distill bipartite entanglement between some party and any of the remaining $m - 1$ parties.*

Here “if” part is based on teleportation argument, while “only if” part follows directly from the property of the GHZ state. There is also an important Lemma

Lemma 12.2 *Any m -partite separable superoperator preserves separability under any chosen partition.*

For given m -partite state ϱ one can define hierarchy of distillable entanglement $\tilde{E}_D^s$ ($s = 2, \dots, m$) (the tilde stands here for distillation of specific, i.e., GHZ type of entanglement) of possible distillation of all $\Psi_+^{d,(s)}$. The above theorem ensures that $\tilde{E}_D^s > 0$ implies $\tilde{E}_D^{s'} > 0$ ($s \geq s'$) but not vice versa: bipartite entangled state Ψ_{AB} in product with any state ϱ_C forms tripartite state ϱ_{ABC} which obviously has $\tilde{E}_D^2 > 0$ but $\tilde{E}_D^3 = 0$, because the above Lemma ensures that C will always be separable against AB under LOCC protocol while distillation of GHZ between ABC will, in particular, require entanglement between AB and C .

12.3 Bound Entanglement—Bipartite Case

12.3.1 Bound entanglement—the phenomenon

The essential quantum property that led us to the observation of bound entanglement [5] was the existence of entanglement with PPT property, i.e., bipartite entangled states with positive partial transpose. In fact, following the mathematical literature, it was observed [27, 28] that for any system $m \otimes n$ type where $mn > 6$ there exist mixed states that are entangled but satisfy the PPT separability condition [29] which has been shown to be necessary and sufficient for separability for $nm \leq 6$. In other words, the set of states that satisfies PPT property is in those cases *strictly larger* than set of separable states (for examples see Section 12.3.3.2). Now there are three elementary observations that are crucial for further analysis:

Theorem 12.4 *The PPT property of bipartite states is preserved under (i) separable (and hence also LOCC) operations and (ii) tensoring (i.e., tensor product of PPT bipartite states is also PPT).*

Proof. The proof (see Exercise 1) of the first property (i) follows easily from the following technical lemma:

Lemma 12.3 *For any operators A, B, C, D one has*

$$(A \otimes B \varrho C \otimes D)^{\Gamma_B} = A \otimes D^T \varrho^{\Gamma_B} C \otimes B^T. \quad (12.11)$$

The proof of (ii) is elementary. The above Lemma guarantees that the PPT property is invariant under $U_A \otimes U_B$ operations. This shows that it is enough to check the PPT property in a single, arbitrarily chosen product basis.

Consider two bipartite states ϱ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\sigma_{A'B'}$ on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ that are PPT. As such they are PPT also in standard product bases. Now consider a state $\Sigma_{AA',BB'} = \varrho_{AB} \otimes \sigma_{A'B'}$. We can check its partial transpose in a natural product basis which is a product of standard product bases $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ respectively. If we calculate partial transpose of $\Sigma_{AA',BB'}$ in that basis we easily see that $\Sigma_{AA',BB'}^{\Gamma_{BB'}} \equiv [\varrho_{AB} \otimes \sigma_{A'B'}]^{\Gamma_{BB'}}$ has exactly the same matrix elements as the matrix $\varrho_{AB}^{\Gamma_B} \otimes \sigma_{A'B'}^{\Gamma_{B'}}$. But the latter is nonnegative as, by assumption is a product of nonreactive matrices. So $\Sigma_{AA',BB'}^{\Gamma_{BB'}}$ also has a nonreactive spectrum ergo $\varrho_{AB} \otimes \sigma_{A'B'}$ that satisfies PPT test of separability if both $\varrho_{AB}, \sigma_{A'B'}$ are PPT.

There is another proposition

Theorem 12.5 *Any PPT state ϱ of $d \otimes d$ type satisfies*

$$F_d(\varrho) \leq \frac{1}{d}. \quad (12.12)$$

Proof. Consider ϱ satisfying above assumptions. Then by the very definition we have $F_d(\varrho) \equiv \text{Tr}(\varrho P_d^+) = \text{Tr}(\varrho^{\Gamma_B} V)/d \leq \frac{1}{d}$ where we have used two facts: (i) identity $P_d^+ = \frac{V^{\Gamma_B}}{d}$ where V is a swap operator (ii) the only eigenvalues of (Hermitian) operator V are ± 1 . $\square$

Theorem 12.6 *If the state is PPT then it is nondistillable. In particular all PPT entangled states represent nondistillable entanglement.*

Proof. From the definition of distillation of entanglement from given ϱ there should exist a sequence of LOCC protocols $\mathcal{P}^n$ such that $F_{d_n}(\mathcal{P}^n(\varrho^{\otimes n}))$ approaches 1 in the limit of large n . Take any ϱ that is PPT. Then $\varrho^{\otimes n}$ is also PPT (because of (ii) property from Theorem 12.4) and hence (because of (i) from that theorem and the fact that any LOCC operation is separable) the state $\mathcal{P}^n(\varrho^{\otimes n})$ is PPT as well. But it means that the parameter F_{d_n} of the latter must not exceed $\frac{1}{d_n}$ and as such cannot approach unity. $\square$

Definition 12.4 We shall call nondistillable (distillable) entanglement bound (free) entanglement.

There is a natural theorem:

Theorem 12.7 *The set of bipartite $m \otimes n$ nondistillable states is (i) [5] closed under LOCC, i.e., no separable or bound entangled state can be transformed into free entangled one by means of any LOCC (ii) compact [103] and (iii) of finite volume. Moreover the set of $m \otimes n$ bound entangled states is also of finite volume (see [103]).*

Proof. Note that the property (iii) follows immediately from the fact that set of separable states (which has a finite nonzero volume [104]) is a subset of the set of all nondistillable states. Subsequently we shall provide the proof of (i) above for probabilistic LOCC. Suppose that by some LOCC operations $\mathcal{L}$ we could produce free entangled state ϱ_{free} from ϱ_{nondist} with some nonzero probability $p > 0$. The state ϱ_{sep} is distillable, so by the very definition of distillation of entanglement there exists LOCC protocol $\mathcal{L}'$ and natural n, d_n such that $d_n \otimes d_n$ state $\mathcal{L}'(\varrho_{\text{free}}^{\otimes n})$ has the parameter F strictly greater than $\frac{1}{d_n}$. But, concatenating the two operations $\mathcal{L}^{\otimes n}$ and $\mathcal{L}'$, it means that with nonzero probability $p^n > 0$ we can produce the states with $F > \frac{1}{d_n}$ out of the state $\varrho_{\text{nondist}}^{\otimes n}$. This means, due to the point (iv) of Theorem 12.4, that the latter is distillable. But Definition 12.1 easily implies that if $\varrho^{\otimes m}$ is distillable for some natural m then the state ϱ also is, which leads to the desired contradiction. $\square$

12.3.2 Bound entanglement and entanglement measures. Asymptotic irreversibility

The existence of bound entangled states has interesting implications on entanglement measures theory [30].

There are many mathematical entanglement measures in the entanglement measure theory. Note that in entanglement measures there are two important physical measures (see [30, 67]). The first is *distillable entanglement* [3] E_D which measures the maximal amount of pure entanglement that can be distilled from ϱ in asymptotic limit of many copies. The second is *entanglement cost* which measures the minimal amount of pure entanglement that is enough to produce ϱ in the limit of many copies (see [68]). Its definition is quite complicated but it has a nice link with another entanglement measure—entanglement of formation [3]:

$$E_F(\varrho_{AB}) = \sup \sum_i p_i S(\text{Tr}_B(|\Psi\rangle\langle\Psi|)), \quad (12.13)$$

where supremum is taken over all ensembles $\{p_i, |\Psi_i\rangle\}$ reproducing ϱ_{AB} . Namely there is a formula [68]:

$$E_C = E_F^\infty \equiv \lim_n \frac{E_F(\varrho^{\otimes n})}{n}. \quad (12.14)$$

Since $E_F(\varrho) > 0$ iff ϱ is entangled bound entangled states have always $E_F > 0$. It was natural to ask about the *asymptotic irreversibility of formation of entanglement*: is there any state ϱ such that one has to use strictly more singlets to produce ϱ than the number of singlets which can be distilled from the state (in the limit of large copies of ϱ)? Or, in other words: *are there states for which $E_D < E_C$?*

The natural candidates for the irreversibility were bound entangled states. They have $E_D = 0$ by definition. On the other hand since $E_F(\varrho) > 0$ iff ϱ is they have always $E_F > 0$. If we knew that E_F is additive we had asymptotic irreversibility proven immediately. Unfortunately additivity of E_F is an open problem which is the one of the most intriguing challenges of quantum information theory [69]. Hence, one has to find other ways to solve the problem. In the paper, [70] asymptotic irreversibility has been proven by showing that for some BE states (based on unextendible produce bases techniques [32], see one of the following sections) $E_C > 0$. Quite recently it has been shown [71] that *all* entangled states have $E_C > 0$ which implies the irreversibility for all bound entangled states. *Nonzero pure entanglement has to be spent to form a bound entangled state in the asymptotic process, but no pure entanglement can be retrieved.* In that sense bound entanglement may be interpreted as a kind of “black hole” of quantum entanglement theory [6].

It is remarkable that there is yet another entanglement measure that corresponds to the asymptotical physical process. This is distillable cryptographic key E_K (for formal definition see [72, 73]) which, on the basis of the quantum privacy amplification effect [74], was known to satisfy $E_D \leq E_K$ and to vanish [75] on all separable states. For a long time there was a common belief that (like E_D) E_K must also vanish for all bound entangled states. Quite surprisingly it has been proven [72, 73] that, at least for some BE states, this is *not* true. We shall come back to that subject in one of the subsequent sections.

Moreover it has been shown [73] that $E_K \leq E_R^\infty$, where the latter measure (asymptotic relative entropy of entanglement) was known to be a lower bound for E_C . A careful reader will note that in this way asymptotic irreversibility of formation of entanglement has been proven independently for all those BE states which have $E_K > 0$.

Finally let us note that there is an important entanglement measure called logarithmic negativity [76] E_N that is an upper bound for E_D . It is defined as $E_N(\varrho_{AB}) = \log \|\varrho_{AB}^{\Gamma_B}\|_{\text{Tr}}$ where $\|\cdot\|_{\text{Tr}}$ stands for a trace norm. There is an important bound on distillable entanglement which is $E_D(\varrho) \leq E_N(\varrho)$. From this fact (which requires a separate proof) one can independently infer that any PPT state is not distillable (Theorem 12.6).

12.3.3 Which states are bound entangled ?

12.3.3.1 NPPT bound entanglement problem.

There is a natural question which states are bound entangled. No state violating reduction criterion can be distilled since any state of that kind is distillable (see Theorem 12.2). Also, any state which violates entropic separability criterion [77, 78] for von Neumann entropy:

$$S(\varrho_{AB}) \geq S(\varrho_A), S(\varrho_B) \quad (12.15)$$

is free entangled [79] due to the proof [79] of hashing inequality (see [80]) saying that one-way (with classical communication allowed only from Alice to Bob) distillable entanglement is bounded from below by coherent information:

$$I_{A>B}(\varrho(AB)) = \max[0, S(\varrho_B) - S(\varrho_{AB})] \quad (12.16)$$

by the so-called hashing protocol. Since there are in general states that cannot be distilled in this way but are distillable [2, 3] in general this cannot lead to full characterization of free (bound) entanglement.

In particular the very natural question was to ask whether the converse of Theorem 12.6 holds, i.e., whether all NPPT entanglement states are distillable. This problem can be reduced by the following theorem (see Exercise 10):

Theorem 12.8 ([12]) *All NPPT $d \otimes d$ states are distillable if and only if all NPPT $d \otimes d$ Werner states (12.6) are distillable.*

It was also observed (cf. Exercise 3) that [84]

Theorem 12.9 *All NPT $2 \otimes N$ states are distillable.*

hence there is no NPPT bound entanglement of $2 \otimes N$ type. Also known no rank two states representing BE exist [82] and if rank three BE states exist they must be NPPT [83] because of the following general theorem:

Theorem 12.10 *Any state ϱ_{AB} having rank less than maximum of local ranks (i.e., ranks of ϱ_A , ϱ_B) is distillable (hence entangled) [82]. Any state having its rank equal its maximum of local ranks and satisfying the PPT property is separable [83].*

It was also realized (see Problem 4) that all NPPT (and hence entangled) $d \otimes d$ Werner states are not 1-copy distillable for some regime of parameter α and the nondistillability of such states has been put into question [81, 84]. However due to the result [22] mentioned already in Section 12.2.1.2 this does not automatically determine distillability property of the states and makes the corresponding problem hard.

It has been known that the existence of NPPT bound entanglement of some Werner states would lead to strange effects, i.e., nonconvexity and nonadditivity (via the so-called asymptotic activation effect, see the next section) of distillable entanglement [85] and also nonadditivity of quantum capacities (cf. [86]).

The situation is different in multipartite case where there are many BE states that violate PPT criterion in some manner (see subsequent sections).

12.3.3.2 Methods for searching bound entangled states

Numerous results on the construction of entangled states which are PPT have been obtained. Main techniques applied in this direction were range criterion [27], nondecomposable positive maps (technique on physical ground initiated in [28] following mathematical literature [35–38]; for further development see [39–46]) linear contraction criteria [48–50], and nonlinear entanglement tests based among others on uncertainty relations [59–61, 65]. On the other hand the analysis of highly symmetric states has been also performed from the point of view of PPT entanglement [62–64].

The *range criterion* states that (see Exercise 5)

Theorem 12.11 ([27]) *If the state ϱ is separable then there exists set of product vectors $|e_i\rangle|f_i\rangle$ such that they span range of ϱ and their partial complex conjugates $|e_i\rangle|f_i^*\rangle$ span range of ϱ^{Γ^B} .*

Let us recall here that range of Hermitian operator H on finite-dimensional Hilbert space may be defined as a subspace spanned by all eigenvectors corresponding to nonzero eigen-

values. The criterion is independent of that of PPT. While it is useless for states of full rank, some of the PPT states violate it.

Example. The example is a $2 \otimes 4$ mixture ϱ_b of the projections corresponding to the following eigenvectors (with the corresponding eigenvalues): (i) $\psi_i = \frac{1}{\sqrt{2}}(|0\rangle|i-1\rangle + |1\rangle|i\rangle)$, $i = 1, 2, 3$ ($\lambda_i = \frac{2b}{7b+1}$) (ii) $\psi_4 = |0\rangle|3\rangle$, ($\lambda_4 = \frac{b}{7b+1}$) (iii) $\psi_5 \equiv (\sqrt{\frac{1+b}{2}}|1\rangle|0\rangle + \sqrt{\frac{1-b}{2}}|1\rangle|2\rangle)$ ($\lambda_5 = \frac{1}{7b+1}$) where $\{|i\rangle\}$ is a standard basis. The state ϱ_b is PPT but it is entangled since partial complex conjugate of product states belonging to the range does not fit to the range of partial transpose of the state. For other PPT bound entangled states violating the criterion, see [27, 34].

There is, however, much more extremal way to violate the criterion, that is, complete absence of product vectors in the range of given ϱ . A mathematically interesting method to generate such states has been provided in [32, 33] where definition of *unextendible product bases* (UPB) has been introduced:

Definition 12.5 Unextendible product basis is a set $\mathcal{S}$ of orthonormal product set of vectors from bipartite Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ such that it does not span the whole $\mathcal{H}_{AB}$, but at the same time there is no product vector orthogonal to all of them.

Clearly, any state that has its range contained in $\mathcal{S}$ is entangled. The crucial observation was that any state which is projected onto the maximal subspace orthogonal to unextendible product basis $\mathcal{S}$ is not only entangled, but also PPT (see Problem 6).

Example. An example of UPB from $\mathcal{C}^3 \otimes \mathcal{C}^3$ is [32] $S_{\text{UPB}} \equiv \{|0\rangle(|0\rangle + |1\rangle), (|0\rangle + |1\rangle)|2\rangle, |2\rangle(|1\rangle + |2\rangle)(|1\rangle + |2\rangle)|0\rangle, (|0\rangle - |1\rangle + |2\rangle)(|0\rangle - |1\rangle + |2\rangle)\}$. Consequently, if by P we denote an operator projecting on $\mathcal{S}$ then according to range criterion the state $\varrho_{\text{UPB}} = \frac{1}{4}(I - P)$ is PPT and entangled.

The existence of bound entanglement based on the UPB method has led to the development of the construction of new nondecomposable positive maps. The seminal paper in this direction was due to Terhal [39] (see also connections to Bell inequalities [47]) extended to the optimized procedure in [40].

A novel powerful separability criterion that can detect some PPT entangled states is the so called *realignment criterion* which says [48, 49] that the result of linear operation $\mathcal{R}$ defined through matrix elements relation (for alternative equivalent ones see [50], cf. [51]):

$$\mathcal{R}(\varrho)_{m\mu, n\nu} \equiv \varrho_{\mu\nu, mn} \quad (12.17)$$

in standard product basis $\{|m\rangle|\mu\rangle\}$ should be a contraction in a trace norm, i.e., for any separable ϱ one should have $\|\mathcal{R}(\varrho)\| \geq 1$. This result has been further linked with positive maps' approach [52]. On the other hand the general concurrence method led to the method of detection of bound entanglement [53] (cf. [54]). Realignment and concurrence methods have been further unified in [58]. Also special uncertainty relations [59–61, 65] have been developed that can detect PPT entanglement. We refer the reader to the literature on this subject.

We must stress that all the methods here have their multipartite counterparts.

12.3.4 Applications in single copy case

12.3.4.1 Limits

There is an interesting fact, namely that bound entanglement *cannot be applied in quantum dense coding* [88] which is basically due to the fact, mentioned in the previous section, that its coherent information (12.16) must always be zero.

Another interesting issue is the question about violation of Bell inequality, which may be related to the communication complexity problems, since it has been shown that violation of any Bell inequality implies improvement of communication complexity in some problems.

There is a conjecture due to Asher Peres [89] that all PPT states satisfy all possible Bell inequalities. So far no example of bipartite BE states violating Bell inequalities is known. In particular it has been shown that such a violation cannot be achieved in the Bell experiment with two settings per site [90]

Another interesting limit of application of BE is connected with quantum teleportation [92, 93]. To see this we need the notion of generalized probabilistic teleportation based on the idea of conclusive teleportation [91], [93] in which given state ϱ_{AB} can be used for teleportation with the help of arbitrary probabilistic operation on the state. There is the following theorem:

Theorem 12.12 ([93]) *Let $F_{\max}(\varrho_{AB})$ be a maximal parameter (12.4) F that can be achieved from given ϱ_{AB} by means of probabilistic LOCC operations. Let $f_{\max}(\varrho_{AB})$ be a maximal teleportation fidelity that can be achieved by means of probabilistic LOCC operation and ϱ_{AB} . Then the equality holds:*

$$f_{\max}(\varrho_{AB}) = \frac{dF_{\max}(\varrho_{AB}) + 1}{d + 1}. \quad (12.18)$$

With this we shall prove the following:

Theorem 12.13 ([93]) *Maximal fidelity of the teleportation d level system with classical resources (i.e., LOCC operations and no entanglement shared) is $f_{cl} = \frac{2}{d+1}$. Teleportation through any nondistillable (either separable or bound entangled) state cannot achieve better fidelity.*

In other words bound entanglement, as a single resource, cannot provide better teleportation fidelity than purely classical resources. This fact was first proven in special case of one parameter family of bound entangled states in Ref. [92]. We shall prove the above theorem.

Proof. We shall first prove the converse. Suppose first that the limit f_{cl} can be beaten with the help of LOCC and some nondistillable state ϱ_{nondist} (either separable or bound entangled), i.e., that with the help of that state we shall get $f_{\max} > f_{cl}$. Then from (12.18) we see that $F_{\max}(\varrho_{AB})$ would have to be strictly greater than $\frac{1}{d}$. This, by definition of $F_{\max}$ means that from ϱ_{nondist} one can produce by LOCC operations the new state ϱ' with parameter $F(\varrho') > \frac{1}{d}$. Application of the condition (iv) of entanglement distillation from Theorem 12.1 leads to the conclusion that ϱ_{nondist} is free entangled (distillable) which is a desired contradiction.

In this way we have proven that f_{cl} cannot be exceeded by nondistillable states. To prove that this is possible with LOCC operations alone one observes that with LOCC one can produce arbitrary $d \otimes d$ separable state say product state $|00\rangle\langle 00|$. Then the standard teleportation protocol [94] will achieve the bound f_{cl} . $\square$

12.3.4.2 Activation of bound entanglement: BE enhanced probabilistic quantum teleportation.

Despite restrictions described above, an interesting effect called activation of bound entanglement [95] shows explicit nonadditivity of quantum resources and leads to new class of considered quantum operations.

Namely there are some free entangled $d \otimes d$ state ϱ such that their $F_{\max}$ parameter (see (12.18)) is strictly less than some value $F_{\max} \leq C < 1$ so we have not only the threshold C on achievable F but also a threshold for teleportation ($\frac{dC+1}{d+1}$). It happens, however, that if we provide some large supply of copies of the same BE state (which in fact are a single copy of the BE state but on Hilbert space of higher dimension as one can easily show with the help of Theorem 12.7) then we can produce probabilistically the $d \otimes d$ state with F being arbitrarily close to unity (only the probability of production approaches zero if F approaches unity). The same immediately holds for f , so bound entanglement can remove the threshold on the teleportation process via the given state ϱ_{AB} .

The above effect reported in [95] is called *single copy activation* of BE. It has inspired the new class of LOCC operations with supply of arbitrary amount of bound entanglement (the so-called BE+LOCC operations). Since there may be some nonadditivity effects due to the possible existence of NPPT BE the natural restriction to PPT bound entanglement can be restricted. Such a class of operations (LOCC + PPT bound entanglement) can be easily proven to be PPT preserving (see Problem 7).

This property can be considered on the level of quantum protocols in terms of the class of PPT-preserving protocols (trace-reserving maps that preserve PPT property, see [96, 97]). Using some techniques from operations theory (exploiting the so-called Jamiołkowski–Choi isomorphism [35, 37]) [98] one can show that the last two classes are closely linked but we do not have place to present this issue here. Let us mention only that in ([97]) it has been shown that pure entanglement can be distilled from any NPPT state with the help of PPT-preserving superoperators.

Finally let us mention that there is a nice generalization of the above effect [99, 100] which shows, in particular, that all BE states can take part in the bound entanglement activation processes in a sense that they can break some teleportation threshold in single copy regime.

12.3.4.3 Probabilistic convertibility of pure states.

The idea of LOCC + BE operations had yet another interesting application [101]. It is well known that the so-called Schmidt rank of given bipartite pure states Ψ (rank of either of its reduced states) cannot be increased by LOCC operations. Any Ψ' produced from Ψ will have the rank not greater than the original state. It happens, however that there is

Theorem 12.14 ([101]) *Any pure states Ψ can be probabilistically transformed into any other pure state Ψ' (irrespectively on Schmidt ranks of Ψ , Ψ') with the help of some LOCC + BE protocol.*

We shall recall here the protocol of converting pure projectors P_+^m into P_+^d . The bound entangled state on the Hilbert space $\mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ where $\mathcal{H}_{AA'} = \mathcal{H}_{BB'} = \mathcal{C}^m \otimes \mathcal{C}^m$ is

$$\begin{aligned} \Sigma_{AA'BB'} = \frac{1}{m^2(d-1)} & \left[(m-1)(P_+^m)_{AB} \otimes (P_+^d)_{A'B} \right. \\ & \left. + \frac{1}{d+1}(I_m - P_+^m)_{AB} \otimes (I_d - P_+^d)_{A'B} \right]. \end{aligned} \quad (12.19)$$

The protocol is quite simple and based on the scheme from [98]: Alice and Bob teleport locally (in their labs) local parts A'' , B'' of initially shared $((P_+^m)_{A''B''})$ through the state $\Sigma_{AA'BB'}$. Locally it looks like teleportation of $(I_m/m)_{A''}$ $((I_m/m)_{B''})$ through the state $\Sigma_{AA'}$ $(\Sigma_{BB'})$. They trace over the systems A , A'' . They exchange the (recorded) results of teleportation measurements and keep the system $A'B'$ shared if and only if they do not need to correct their teleportation processes (the special, distinguished, result of possible m^2 results of teleportation from its higher dimensional $m \otimes m$ version [94]). This happens with probability $\frac{1}{m^2}$ and then the shared state is just P_+^d .

12.3.5 Applications in asymptotic regime

12.3.5.1 Asymptotic activation problem

Asymptotic activation of bound entanglement is any superadditivity of $E_D : E_D(\varrho^1 \otimes \varrho^2) > E_D(\varrho^1) + E_D(\varrho^2)$ when one of the states is bound entangled. In its most striking version that can be called *asymptotic superactivation*² tensor product of few bound entangled states would be distillable (for example in the above both states were BE). Still an effect of superactivation of bipartite BE has been conjectured in [95] and it was shown [85] that if NPT bound entanglement of some Werner states existed then the above conjecture was true. Actually it can be shown that any NPT bound entanglement would lead to asymptotic activation of bound entanglement but we do not have space to consider it here. Let us only mention that this follows from the already mentioned result that from any NPPT entangled state one can distill entanglement by means of PPT preserving protocol [97].

12.3.5.2 Quantum cryptography

As we mentioned already, for a long time it was believed that nondistillable states have distillable cryptographic key E_K equal to zero. This was basically due to the fact that both the first entanglement based cryptographic protocols [74, 105] and proofs of the so-called unconditional security of the so-called BB84 protocol were based on the entanglement distillation idea.

To see the application of entanglement distillation in quantum cryptography, let us consider standard scenario from [74] of production of secure cryptographic key on the basis of entanglement distillation from many copies of given state ϱ_{AB} . In such cases one assumes that Alice, Bob, and eavesdropper (Eve) share many copies of pure state

$$|\Psi_{ABE}\rangle, \quad \text{Tr}_E[|\Psi_{ABE}\rangle\langle\Psi_{ABE}|] = \varrho_{AB}, \quad (12.20)$$

²We adopt here the term from the paper [114].

i.e., that all which is not in Alice and Bob hands is in Eve ones. The aim of Alice and Bob is to get as much as secure key with the help of LOCC operations where classical communication is considered to be public. Thus LOCC operations in secure key distillation is called LOPC (from “local operations and public communication”).

The idea of getting secure key through distillation was to distill (in the limit of large n) $k = \log d_n$ bits of maximal entanglement in a form of the state $P_+^{d_n}$. Once Alice and Bob share that state, they can project it locally in the same standard basis

$$\mathcal{B}_{\text{stand}} \equiv \{|i\rangle|j\rangle\}, \quad i, j = 0, \dots, d_n - 1 \quad (12.21)$$

to get $k = \log d_n$ bits of key which are secure since due to entanglement monogamy their (maximally entangled) state $P_+^{d_n}$ is product with states of the Eve physical system E . Since the number of bits are equal to the amount of entanglement distilled we have $E_D \leq E_K$ since in principle there may be better protocol to distill the key. In fact there are much better protocols than the above. To see this, note that once one has maximally entangled state $P_+^{d_n}$ distilled Alice and Bob have a lot of freedom, since *any* measurement in *rotated* standard basis $\mathcal{B}_{\text{rot}} = \{U \otimes U^*|i\rangle|j\rangle\}$ will give them the same E_D amount of key.

In [72, 73] it was observed that to get cryptographic key distilled one needs only to keep security with respect to single basis, say the standard one $\mathcal{B}_{\text{stand}}$. The corresponding theory is rather complicated. We shall quote here the most important result that is in some analogy to entanglement distillation. To this aim we have to consider bipartite states that have Alice and Bob subsystems composite in general, i.e., AA' and BB' . It may happen, however, that the primed ones A' , B' are trivial (corresponding to the one-dimensional Hilbert space.)

Theorem 12.15 ([72, 73]) *A bipartite state $\varrho_{ABA'B'}$ defined on $\mathcal{H}_{ABA'B'} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ with $\mathcal{H}_A = \mathcal{H}_B \sim \mathcal{C}^d$ represents $\log d$ bits of secure key with respect to $\mathcal{B}_{\text{stand}} = \{|i\rangle|j\rangle\}$, $i, j = 0, \dots, d - 1$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ iff it is of the special form:*

$$\varrho_{AB,A'B'} = \gamma_{ABA'B'}^{(d)} \equiv \sum_{ij} |i\rangle|i\rangle\langle j|\langle j| \otimes U_i \sigma_{A'B'} U_j \quad (12.22)$$

for some state $\sigma_{A'B'}$ and unitary operations $\{U_i\}$ on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$.

The state $\gamma^{(d)}$ is called private dit (p -dit).

There is also very important theorem saying that one can distill secure bit iff one can produce private dit.

Theorem 12.16 ([75]) *With the help of LOPC operations it is impossible to distill secure cryptographic key from bipartite separable state.*

Theorem 12.17 ([72, 73]) *The state ϱ_{AB} has distillable cryptographic key iff there exists sequence of LOCC (may be probabilistic) operations $\tilde{\mathcal{L}}^n : \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \rightarrow \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ and sequence of some p -bits $\gamma_n^{(2)}$ such that*

$$\left\| \tilde{\mathcal{L}}(\varrho_{AB}^{\otimes n}) - \gamma_n^{(2)} \right\|_{\text{Tr}} \rightarrow 0. \quad (12.23)$$

Moreover if we represent the sequence of $\Sigma_n \equiv \tilde{\mathcal{L}}(\varrho_{AB}^{\otimes n})$ (living on $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$) in terms of block matrix form:

$$\Sigma_n = \begin{bmatrix} A_{00,00}^n & A_{00,01}^n & A_{00,10}^n & A_{00,11}^n \\ A_{01,00}^n & A_{01,01}^n & A_{01,10}^n & A_{01,11}^n \\ A_{10,00}^n & A_{10,01}^n & A_{10,10}^n & A_{10,11}^n \\ A_{11,00}^n & A_{11,01}^n & A_{11,10}^n & A_{11,11}^n \end{bmatrix} \quad (12.24)$$

then condition (12.23) is equivalent to the following simple one:

$$\|A_{00,11}^n\|_{\text{Tr}} \rightarrow \frac{1}{2}. \quad (12.25)$$

The above theorem is basically cryptographic analog of the condition (v) (with $d = 2$) of distillation of entanglement. It basically says that if Alice and Bob can distill single bit of secure correlations (represented by $\gamma_n^{(2)}$) then they can also distill infinitely many bits of secure correlations.

Below we shall show that one can distill secure bits of key from bound entanglement.

Theorem 12.18 ([72]) *There exist bound entangled states with $K_D > 0$.*

Proof. The above theorem requires examples of BE states with $K_D > 0$. Original examples [72] were quite complicated. Here we shall discuss simpler ones [106].

Consider the $4 \otimes 4$ state $\varrho_{ABA'B'}$ with $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}_{A'} = \mathcal{H}_{B'} = \mathcal{C}^2$ in the following form:

$$\varrho_{ABA'B'} = \frac{1}{4(\sqrt{2} + 1)} \begin{bmatrix} I/\sqrt{2} & 0 & 0 & U_H^{\Gamma_B} \\ 0 & P_{\text{cl}} & U_H & 0 \\ 0 & U_H & P_{\text{cl}} & 0 \\ U_H^{\Gamma_B} & 0 & 0 & I/\sqrt{2} \end{bmatrix} \quad (12.26)$$

where I is the identity matrix on two-qubit space, $P_{\text{cl}} = |0\rangle\langle 0| + |1\rangle\langle 1|$ and U_H is the two-qubit partial isometry built from matrix elements H_{ij} of Hadamard matrix as $U_H = \sum_{i,j=0}^1 H_{ij} |i\rangle\langle j|$.

We see that the state is nondistillable since it is PPT (in fact it is PPT invariant by construction). Note that at that moment *we do not know whether they are entangled*. To see that the state has distillable secure key let us apply the LOCC recurrence protocol [3] to the AB part: In k th step of the protocol (i) take the state (12.26) as a target $\varrho_{ABA'B'}$, and source state $\varrho_{\bar{A}\bar{B}\bar{A}'\bar{B}'}$ being result of $k-1$ step of the protocol (ii) apply bilateral C-NOT³ $U_{\bar{A}\bar{A}}^{\text{C-NOT}} \otimes U_{\bar{B}\bar{B}}^{\text{C-NOT}}$ and perform the measurement of Pauli matrix σ_3 on source subsystems $\bar{A}, \bar{B}$ and exchange results via the classical channel. (iii) discard the source and keep the target

³ $U_{XY}^{\text{C-NOT}} = (|0\rangle\langle 0|)_X \otimes I_Y + (|1\rangle\langle 1|)_X \otimes \sigma_Y^3$ with X, Y being source and target respectively, and I_Y (σ_Y) stands for identity (Pauli third matrix) on subsystem Y .

iff the compared results are the same. After k th iteration the state of the system is

$$\varrho_{ABA'B'}^k = \frac{1}{2^{k+1}(2^{1-k/2} + 1)^k} \times \begin{bmatrix} (I/\sqrt{2})^{\otimes k} & 0 & 0 & (U_H^{\Gamma_B})^{\otimes k} \\ 0 & (P_{cl})^{\otimes k} & (U_H)^{\otimes k} & 0 \\ 0 & (U_H)^{\otimes k} & (P_{cl})^{\otimes k} & 0 \\ (U_H^{\Gamma_B})^{\otimes k} & 0 & 0 & (I/\sqrt{2})^{\otimes k} \end{bmatrix} \quad (12.27)$$

Now it is easy to see that the right-up corner matrix block satisfies

$$\|A_{00,11}(\varrho_{ABA'B'}^k)\| = \frac{1}{2} \frac{1}{1 + 2^{-k/2}} \xrightarrow{k \rightarrow \infty} \frac{1}{2} \quad (12.28)$$

which via Theorem 12.17 guarantees that one can distill secure key. In particular the above protocol is an example of probabilistic distillation of secure bit from (12.26).

Finally we must stress that *since one can distill secure key from that state it means that the state is entangled* (see Theorem 12.16) and because it is PPT, it is *bound entangled*. $\square$

It is interesting to note that, quite surprisingly, there is even much better purely one-way protocol of key distillation from the considered states [106], but we do not have space to present it here.

12.3.5.3 Feedback to classical cryptography: Bound information phenomenon

Since we already know that entanglement distillation is not necessary for secure key distillation, the natural question is which bipartite states allow for the latter. Are they all entangled states? We do not know that, though there is an important equivalence [107]: not all entangled states would admit secure key distillation if and only if the conjectured “bound information” [108] existed in classical cryptography.

In this way we come to the intriguing feedback of bound entanglement in classical cryptography, which, initiated in [108] resulted already in the discovery of two new phenomena in classical bipartite [110] and multipartite [111] cryptographies.

The existence of the so-called bound information was conjectured in [108] as an analog of bound entanglement in classical cryptography. This analog is defined as a possible property of tripartite probability distributions $\vec{p}_{ABE} = \{p_{ABE}(x, y, z)\}$. The property would be that the so-called intrinsic information (see [109]) $I_{\vec{p}}(A : B \downarrow E)$ is strictly positive (which means that Eve does not have full access to the correlations shared by Alice and Bob) but no secure key K_D^{cl} can be distilled from $\vec{p}$ in a classical manner.

The possible candidates for distributions containing bound information are [108] distributions inherited from some bound entangled states via their special extensions to pure states.

One of the difficulties in the open problem of existence of bound information via quantum methods is that the so-called *qqq* scenario (where all Alice, Bob, and Eve have quantum power) is in general difficult to compare the so-called *ccc* scenario (where all parties have already performed local measurement on single copy and perform classical postprocessing afterwards). However some unifying analysis of the two scenarios was recently provided [112].

The problems of the above type can be omitted [111] in multipartite case and we shall come back to it subsequently (see Section 12.4.5).

However even in the bipartite case bound entanglement inspired already the discovery of weaker version of bound information [110]: there are classical distributions such that the gap between intrinsic information is an distillable key: K_D^{cl} can be made arbitrarily large: $I(A : B \downarrow E) \gg K_D^{\text{cl}}$.

12.3.5.4 Connections with quantum communication channels: binding entanglement channels.

There are two ways (found independently in [102] and [33]) to naturally associate quantum channels with quantum BE states. The one way [33] is the channel formed by teleportation of quantum states through bound entangled state.

The second one (see [102]) is formed by Jamiołkowski–Choi isomorphism [35, 37]:

$$\varrho_{AB}(\Lambda) = [I_A \otimes \Lambda_B](P_+^d) \quad (12.29)$$

which produces one-to-one correspondence between channels and states ϱ_{AB} that have maximally mixed left reduced density matrix ϱ_A . From any BE state that has ϱ_A of maximal rank one can filter the state with ϱ_A being maximally mixed and produce some special channel. All channels produced in such a way as well can be shown to coincide [102] with the class of the so-called *binding entanglement channels*

Definition 12.6 (see [102], [33]) The channel is called binding entanglement channel iff cannot be used by Alice and Bob to share free entanglement, but still they can produce some bound entanglement which help of that channel.

Theorem 12.19 (see [103]) *Binding entanglement channels have all zero-way, and two-way quantum capacities zero*⁴.

Note that bipartite binding entanglement channels are interesting candidates for superadditivity of quantum channel capacity in bipartite case [95]. Moreover multipartite version of binding entanglement channels have been already shown to lead to such superadditivity effect [132] (see Section 12.4.6).

12.4 Bound Entanglement: Multipartite Case

12.4.1 Which multipartite states are bound entangled?

In the multipartite case the situation is quite different, since there are more examples of bound entangled states. Here by multipartite bound entangled state one defines as

Definition 12.7 The m-partite state $\varrho_{A_1, \dots, A_m}$ is called *bound entangled* if $\tilde{E}^s(\varrho_{A_1, \dots, A_m}) = 0$ for all $s = 2, \dots, m$ but the state is not fully separable.

This definition means that no GHZ entanglement can be distilled between any subset of parties, but the state itself is entangled (cf. Section 12.2.2). There is a simple generalization of the Theorem 12.7 saying that

⁴For definitions of various types of quantum capacities see [3].

Theorem 12.20 *The set of multipartite $d_1 \otimes d_2 \otimes \dots \otimes d_m$ nondistillable states is (i) closed under LOCC, i.e., no separable or bound entangled states can be transformed into free entangled one by means of any LOCC (ii) compact and (iii) of finite volume. Moreover the set of $d_1 \otimes d_2 \otimes \dots \otimes d_m$ bound entangled states is also of finite volume.*

Another, a little more complicated generalization of the result from the bipartite case is

Theorem 12.21 *If the m -partite state possesses PPT or separability property with respect to bipartite partition into $\{I_1, I_2\}$, and I_i being disjoint subsets of the set of indices $I = \{1, \dots, m\}$ ($I_1 \cup I_2 = I$) then no k -partite GHZ type entanglement ($k \geq m$) can be distilled that simultaneously involves subsystems from both I_1 and I_2 . In particular if the state satisfies PPT property with respect to some $m - 1$ of m elementary subsystems then it is nondistillable.*

The proof of the above theorem is easy by reducing the problem to the bipartite case (see Exercise 8).

Also a natural generalization of the separability PPT and range criterion from Theorem 12.11 is possible in the case of fully separable state. The only difference is that one can consider not only PPT operation (or—respectively—complex conjugate operation on product vectors in range criterion) involving all elementary m subsystems, but also their collections. There is, however, a special novelty in the multipartite case, namely the special BE state that is *semiseparable but entangled*.

Example: Consider the state ϱ_{Shift} that is based on $2 \otimes 2 \otimes 2$ unextendible product basis $S_{\text{Shift}} = \{|0\rangle|0\rangle|0\rangle, |+\rangle|1\rangle|-\rangle, |1\rangle|-\rangle|+\rangle, |-\rangle|+\rangle|1\rangle\}$, (with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$). There is no tripartite product state orthogonal to all those states so, by definition, the above set defines unextendible product basis set. Then it is easy to see that the state $\varrho_{\text{Shift}} = \frac{1}{4}(I - P_{\text{Shift}})$ with P_{Shift} projecting on space spanned by S_{Shift} is entangled. However it can be shown to be not only nondistillable, but even semiseparable [32] (see Problem 11). This kind of one semiseparable bound entangled states is a kind of surprise and it represents “genuine” tripartite entanglement. In general they must be detected by multipartite linear Hermitian maps (and the corresponding witnesses) criteria [55] that is a natural generalization of [28] Entanglement of ϱ_{Shift} can be detected in the framework of linear contractions approach [50] by partial realignment criterion [50, 51]. Also the concurrence approach has been extended to the multipartite case [57].

Let us also note that there are bound entangled states which violate NPT criteria against some cuts. Here we have a nice example

Example: [113] Consider the following three-qubit projectors $P_{ij}^\pm$ corresponding to the GHZ basis: $|\Psi_{ij}^\pm\rangle = \frac{1}{\sqrt{2}}(|i\rangle|j\rangle|0\rangle \pm |i \oplus 1\rangle|j \oplus 1\rangle|0\rangle)$ The following state

$$\varrho_{ABC}^{\text{asym}} = \frac{1}{3}P_{00}^+ + \frac{1}{6}[P_{01}^+ + P_{01}^- + P_{10}^+ + P_{10}^-] \quad (12.30)$$

satisfies PPT criteria: $(\varrho_{ABC}^{\text{asym}})^{\Gamma_B}, (\varrho_{ABC}^{\text{asym}})^{\Gamma_C} \geq 0$ and as such is nondistillable. Still it violates the PPT criterion against the third (A versus BC) partition (i.e., $(\varrho_{ABC}^{\text{asym}})^{\Gamma_A} \geq 0$ does not hold) hence it is bound entangled. It is important to note that the state becomes bipartite free entangled if the subsystems B, C are considered as a single, joint subsystem BC . This is because then it becomes $2 \otimes 4$ NPPT state but all NPPT states of $2 \otimes N$ type are distillable (see Section 12.3.3.1). For the m partite generalization of the above states, see [113].

Example: Yet another important example of multipartite four-qubit bound entangled state is [56]

$$\varrho_{ABCD}^{\text{unloc}} = \frac{1}{4} \sum_{i=1}^4 |\Phi_i\rangle\langle\Phi_i| \otimes |\Phi_i\rangle\langle\Phi_i|, \quad (12.31)$$

where $\{|\Phi_i\rangle\}$ stands for four Bell states $\{\frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)\}$.

The state can be shown to be permutationally invariant and hence separable under any partition into any two-qubit parts. On the other hand it is entangled since it violates the PPT criterion with respect to any single qubit versus the remaining ones (e.g., $(\varrho_{ABCD}^{\text{unloc}})^{\Gamma_A}$ and all its permutations with respect to local subsystems are not positive semidefinite matrices).

Clearly it is bound entangled which follows from (careful) application of Theorem 12.21. It has, however, *unlockability* property [56] which means that it becomes free entangled if any two parties are considered as a single system. Below we shall describe several important effects that lead to application multipartite bound entanglement.

The general $2 - k$ partite ($k \geq 2$) version of the above states has been introduced in [117] and, independently in [118]. The first paper reported general unlockability effects and explicit EPR form of the state while the second has investigated in details all applications of generalized Smolin states such as remote entanglement concentration, unlocking entanglement, and violation of Bell inequalities together with its application to communication complexity. We shall come back to some of these issues below.

In general classification of multipartite bound and free entanglement is a hard and unsolved problem. For special cases of three qubits general classification has already been performed resulting with an onion structure containing different *GHZ*, *W* and biseparable type of entanglement [120].

12.4.2 Activation effects

There are few activation effects that have been discovered in the multipartite case. The first is multipartite asymptotic activation [26]. We take two three-qubit states:

- (i) the pure state σ_{ABC} corresponding to the vector $|\psi_+\rangle_{AB}|0\rangle_C$, one which is free entangled and has $\tilde{E}_D^2 > 0$ but $\tilde{E}_D^3 = 0$.
- (ii) the bound entangled state (12.30) (by definition with $\tilde{E}_D^2 = \tilde{E}_D^3 = 0$).

With the help of the pure state σ_{ABC} one can teleport qubit from B to A (or vice versa) producing from (12.30) $2 \otimes 4$ NPT entanglement between A and C (or B and C). As we already know by Theorem 12.9 that these states are distillable. In this way we can distill (in two separate protocols) maximally entangled states between sites C and A , and also between sites C and B independently, which by Theorem 12.3 guarantees distillability of the tripartite state $\sigma \otimes \varrho^{\text{asym}}$ to the GHZ form. i.e., $\tilde{E}_D^3(\varrho^{\text{asym}} \otimes \sigma) > 0$ though none of the two states had this property separately. Thus 3-particle BE of ϱ^{asym} was activated by biparticle FE contained in σ . We call the above activation asymptotic since they concern asymptotic quantities $\tilde{E}_D$ rather than single copy quantity like quantum teleportation fidelity which was considered in the bipartite case (see 12.3.4).

Even more striking effect is asymptotic activation of purely bound entanglement by itself [113] which can be called asymptotic *superactivation*. To this aim one takes $\varrho_{ABC}^{\text{asym}}$ and its two cyclic permutations $\varrho_{CAB}^{\text{asym}}, \varrho_{BCA}^{\text{asym}}$. By LOCC operation the three parties can produce the equiprobable mixture of those three states, but the latter has been shown to be distillable to the GHZ form (see [113]). Thus the tensor product of the three bound entangled states (i.e., with all parameters $\tilde{E}_D^2 = \tilde{E}_D^3 = 0$) represents the free entangled state with $\tilde{E}_D^3 > 0$.

Finally we shall discuss very strong version [114] of superactivation of bound entanglement which requires only finite number of copies of quantum state and, as such, does not require asymptotic analysis of large number of copies. Consider the state

$$\varrho_{ABCDE} \equiv \sigma^A \otimes \varrho_{BCDE}^{\text{unlock}} \quad (12.32)$$

(with arbitrary fixed state σ^A) and all its cyclic permutations i.e. $\varrho_{EABCD}, \varrho_{DEABC}, \varrho_{CDEAB}, \varrho_{BCDEA}$. Each of them is still a BE state. But there are protocols producing from the state $M_{ABCDE} \equiv \varrho_{ABCDE} \otimes \varrho_{EABCD} \otimes \varrho_{DEABC} \otimes \varrho_{CDEAB} \otimes \varrho_{BCDEA}$ maximally entangled bipartite state P_+^2 between any two of the parties $ABCDE$ with probability one in a few steps. Thus, not only one has $D^5(M_{\text{symm}}^{ABCDE}) > 0$ but also the corresponding protocol distilling single GHZ state is *finite* here.

12.4.3 Remote quantum information concentration

There is a nice effect that uses the unlockable state to concentrate quantum information of one qubit spread over three spatially separated locations. Suppose Alice, Bob, and Charlie share 3-particle state $\psi_{ABC}(\phi)$ being an output of quantum cloning machine (see [116]). The initial information about cloned qubit ϕ is delocalized and they cannot concentrate it back with the help of LOCC. But if each of them has in addition one particle of the 4-particle system in state ϱ_{unloc} with the remaining fourth particle handed to another party (David) then means of simple LOCC action Alice, Bob, Charlie can “concentrate” the state ϕ back remotely at David site.

12.4.4 Violation of Bell inequalities and communication complexity reduction

Historically the first paper reporting Bell inequalities was due to Dür [121] who showed that some multiqubit BE states violate two-settings inequalities called Mermin–Klyshko inequalities. The states considered in [121] were a sort of m -qubit generalizations of the states (12.30) and were reported to violate the inequalities for $m \geq 8$ with two settings per site (for further improvements see [125, 126]). The relation of m -partite Bell inequalities to distillability of bipartite has been analyzed in [127].

Quite surprisingly in some cases [118, 128] $m = 4$ bound entanglement violates some Bell inequality *maximally in a sense that no quantum state can violate that inequality better*. In fact we take the following four-partite inequality belonging to the class from [123, 124]

$$|E(1, 1, 1, 1) + E(1, 1, 1, 2) + E(2, 2, 2, 1) - E(2, 2, 2, 2)| \leq 2. \quad (12.33)$$

where mean values $E(i, j, k, l) = \langle A_i^{(1)} A_j^{(2)} A_k^{(3)} A_l^{(4)} \rangle$ of dichotomic (i.e., with only possible measurement outcomes equal to ± 1) observables $A_i^{(k)}$ where $i = 1, 2$ represents number of possible local settings and k enumerates the specific subsystem. Now if we take the observables $A_i^{(1)} = A_i^{(2)} = A_i^{(3)} = \sigma_i$ and $A_i^{(4)} = \frac{1}{\sqrt{2}}(\sigma_1 + (-1)^i \sigma_2)$ we get that the Smolin state ϱ^{unlock} (12.31) provides mean value $2\sqrt{2}$ which clearly violates the bound (12.33). This violation can be shown to be maximal [128] in the sense, that no other state can violate it better.

It is important to note that due to the results [119, 129] for any Bell inequality one can associate a communication complexity problem, for which there exists a protocol exploiting the state violating the inequality, that is more efficient than any classical protocol. In this way we can see that multipartite bound entanglement *can help in solving communication complexity problems*.

This is remarkable however that violation of m-partite Bell inequality does not automatically lead to the possibility of distillation of secure key in m-partite scenario. In fact we have a simple generalization of theorem 12.16 (see [118]):

Theorem 12.22 *If the m-partite state possesses separability property with respect to bipartite partition into $\{I_1, I_2\}$ and I_i being disjoint subsets of the set of indices $I = \{1, \dots, m\}$ ($I_1 \cup I_2 = I$) then no k-partite secure cryptographic key ($k \geq m$) can be distilled between parties belonging to both subsets I_1 and I_2 .*

Using the above theorem and exploiting symmetric invariance of the Smolin state (12.31) it can be easily proven that no secure bit can be distilled from bound entanglement contained in that state. It happens irrespective of the fact that the state violates maximally some Bell inequalities. This observation shows that some more subtle properties of multipartite Bell inequalities should be taken into account in order to imply cryptographic security.

12.4.5 Feedback to classical theory: multipartite bound information and its activation

There is an interesting effect based on quantum states $\varrho_{ABC}^{\text{asym}}$ (12.30). Namely one can consider the natural purification of that state Ψ_{ABCE} and produce four-partite classical probabilistic distribution $\vec{p}_{ABCE}$ via local von Neumann measurements on all subsystems. It can be relatively easily shown that (see [111]) that the parties can distill no cryptographic key if they are far apart. On the other hand there is kind of secrecy in the above distribution since if the parties A and B are together (or—if they can communicate through a secret channel) then Eve E cannot prevent distillation of the key between AB and C . This phenomenon discovered in [111] is called *multipartite bound information*. Moreover it can be shown that this bound information can be asymptotically activated (or more precisely—superactivated) in full analogy to superactivation of bound entanglement of original states (12.30).

The above example shows a quite fundamental thing: bound entanglement phenomenon *can help us to find and solve a new and interesting problem in the classical information theory*.

12.4.6 Bound entanglement and multiparty quantum channels

There is already a proof of nonadditivity of multipartite version of two-way quantum capacity of quantum channels in [132] where multiparty quantum channels has been shown in general setting.

We shall explain the idea on an example. Consider the broadcast channel when A is supposed to transfer some quantum messages to B and C . One as usual defines capacity regions as all possible pairs of transfer rates $Q_{A \rightarrow B}, Q_{A \rightarrow C}$. It can be shown that the binding entanglement quantum channel $\Lambda_{A \rightarrow B, C}$ based on some extension of the BE state (12.30) (see [132]) or even of the channel $\Lambda_{A \rightarrow B, C}$ based on the BE state itself has both capacities zero. the same can be shown for the two of its suitable permutations (here respectively BE channels $\Lambda_{B \rightarrow A, C}, \Lambda_{C \rightarrow A, B}$). Still, if Alice has all three channels at her disposal (here it would be $\Lambda' = \Lambda_{A \rightarrow B, C} \otimes \Lambda_{B \rightarrow A, C} \otimes \Lambda_{C \rightarrow A, B}$) then she can produce the averaged channel $\Lambda'' = \frac{1}{3}(\Lambda_{A \rightarrow B, C} + \Lambda_{B \rightarrow A, C} + \Lambda_{C \rightarrow A, B})$ which can be easily shown to have two-way capacity nonzero with the help of quantum entanglement distillation procedures. The existence of similar one-way or zero-way effect is an open problem.

12.5 Further Reading: Continuous Variables

The quick review of most important aspects of bound entanglement needs further analysis, but we shall conclude our lecture at that point. We shall also mention few results on continuous variables bound entanglement. The analysis has been initiated in [130] and [131] where it has been shown that BE in continuous variables states is a rare phenomenon (i.e., it has a sort of zero volume). Bound entanglement has been very well studied in the field of Gaussian states. First bound entangled Gaussian state has been constructed in [134]. Analysis of bipartite entanglement with single mode on one site [133, 134] was further concluded with the result that all entangled $1 \times n$ Gaussian states are distillable and there is no NPPT BE in bipartite Gaussians at all [135].

There are interesting results on key distillation from Gaussian free entangled states with Gaussian operations [136] but the topic of applications of Gaussian bound entanglement has not been explored yet.

Exercises

1. Prove Lemma 12.3 and the property (i) of Theorem 12.4.
2. Prove Theorem 12.8.
3. Prove Theorem 12.9.
4. Find, for which parameters of α the Werner state is not single-copy distillable and compare with the region for which the state is separable.
5. Prove Theorem 12.11. Using it shows that the state ϱ_b provided in Section 12.3.3.2 is bound entangled.

6. Show that any state which is a normalized projection onto the subspace orthogonal on unextendible product basis must be both PPT and entangled.
7. Prove that operations LOCC + PPT bound entanglement preserves the PPT property of quantum states.
8. Prove Theorems 12.20, 12.21.
9. Prove that the set of bound entangled states on finite-dimensional Hilbert space is (i) of nonzero volume and (ii) compact.
10. Prove that BE state ϱ_{Shift} from Section 12.4.1 is semiseparable. Prove that the set of product states used in the construction was an unextendible product basis.
11. Prove that set of free entangled states is dense in the set of all states in the set of all quantum states defined on infinite Hilbert space (this corresponds to “zero volume” of the set of continuous variables bound entangled states).

References

- [1] G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, and A. Zeilinger, *Quantum information: An Introduction to Basic Concepts and Experiments* (Springer, Berlin, 2001).
- [2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
- [3] C. H. Bennett, D. P. Di Vincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3814 (1997).
- [4] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
- [5] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
- [6] B. M. Terhal, M. W. Wolf, and A. C. Doherty, Phys. Today **56**, 46 (2003).
- [7] M. J. Donald, M. Horodecki, and O. Rudolph, J. Math. Phys. **43**, 4252 (2002).
- [8] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, (1997) 2275.
- [9] C. H. Bennett, D. DiVincenzo, Ch. Fuchs, T. Mor, E. Rains, P. Shor, J. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
- [10] N. Gisin, Phys. Lett. A **210**, 151 (1996).
- [11] C. H. Bennett, H. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
- [12] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4026 (1999).
- [13] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [14] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [15] S. Popescu, Phys. Rev. Lett. **72**, 797–799 (1994).
- [16] S. Popescu, Phys. Rev. Lett. **74**, 2619–2622 (1995).
- [17] E. Rains, Phys. Rev. A **60**, 173 (1999).

- [18] D.P. DiVincenzo, P. W. Shor, J. A. Smolin, B. Terhal, and A. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
- [19] D. Dür, J. I. Cirac, M. Lewenstein, and D. Bruss, Phys. Rev. A **61**, 062313 (2000).
- [20] P. Horodecki and R. Horodecki, Quant. Inf. Comp. **1**, **45** (2001).
- [21] S. Bandyopadhyay and V. Roychowdhury, Phys. Rev. A **68**, 022319 (2003).
- [22] J. Watrous, Phys. Rev. Lett. **93**, 010502 (2004).
- [23] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
- [24] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 4075 (1998).
- [25] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
- [26] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
- [27] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
- [28] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
- [29] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [30] M. Horodecki, Quant. Inf. Comp. **1**, 3 (2001).
- [31] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).
- [32] C. H. Bennett, D. DiVincenzo, T. Mor, P. Shor, J. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
- [33] D. DiVincenzo, T. Mor, P. Shor, J. Smolin, and B. M. Terhal, Comm. Math. Phys. **238**, 379 (2003); also *Preprint* quant-ph/9908070.
- [34] D. Bruß and A. Peres, Phys. Rev. A **61**, 30301(R) (2000).
- [35] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
- [36] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1975).
- [37] M.-D. Choi, Proc. Sympos. Pure Math. **38**, 583 (1982).
- [38] E. Stormer, Proc. Amer. Math. Soc. **86**, 402 (1982).
- [39] B. M. Terhal, Lin. Algebr. Appl. **323**, 61 (2000).
- [40] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).
- [41] A. Kossakowski, Open Syst. Inf. Dyn. **10**, 213 (2003); G. Kimura, A. Kossakowski, *ibid.* **11**, 343 (2004).
- [42] F. Benatti, R. Floreanini, and M. Piani, Open Syst. Inf. Dyn. **11**, 325 (2004); also *Preprint* quant-ph/0411095.
- [43] K.-C. Ha and S.-H. Kye, Phys. Lett. A, **325**, 315 (2004); K.-C. Ha and S.-H. Kye, J. Phys. A: Math. Gen. **38**, 9039 (2005).
- [44] M. Piani, *Preprint* quant-ph/0411098.
- [45] H.-P. Breuer, Phys. Rev. Lett. **97**, 080501 (2006); W. Hall, *Preprint* quant-ph/0607035.
- [46] D. Chruściński and A. Kossakowski, *Preprint* quant-ph/0606211.
- [47] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).
- [48] O. Rudolph, *Preprint* quant-ph/0202121.
- [49] K. Chen and L.A. Wu, Quant. Inf. Comp. **3**, 193 (2003).
- [50] M. Horodecki, P. Horodecki, and R. Horodecki, Open Syst. Inf. Dyn. **13**, 103 (2006); also *Preprint* quant-ph/0206008.

- [51] K. Chen and L.-A. Wu, Phys. Lett. A **306**, 14 (2002).
- [52] K. Chen, L.-A. Wu, Phys. Rev. A **69**, 022312 (2004).
- [53] F. Mintert, M. Kuś, and A. Buchleitner, Phys. Rev. Lett. **92**, 167902 (2004).
- [54] P. Badziag, P. Deuar, M. Horodecki, P. Horodecki, and R. Horodecki, J. Mod. Opt. **49**, 1289 (2002).
- [55] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **283**, 1 (2001).
- [56] J. A. Smolin, Phys. Rev. A **63**, 032306 (2001).
- [57] F. Mintert, M. Kuś, and A. Buchleitner, Phys. Rev. Lett. **95**, 260502 (2005).
- [58] K. Chen, S. Albeverio, and S.-M. Fei, Phys. Rev. Lett. **95**, 040504 (2005).
- [59] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003).
- [60] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).
- [61] O. Gühne and M. Lewenstein, Phys. Rev. A **70**, 062317 (2004).
- [62] H.-P. Breuer, Phys. Rev. A **71**, 062330 (2005).
- [63] D. Chruściński and A. Kossakowski, Phys. Rev. A **73**, 062313 (2006); *ibid.* **73**, 062314 (2006).
- [64] D. Chruściński and A. Kossakowski, Phys. Rev. A **74**, 022308 (2006).
- [65] O. Gühne and N. Lütkenhaus, Phys. Rev. Lett. **96**, 170502 (2006).
- [66] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
- [67] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).
- [68] P. Hayden, M. Horodecki, and B. Terhal, J. Phys. A: Math. Gen. **34**, 6891 (2001).
- [69] P. W. Shor, J. Math. Phys. **43**, 4334 (2002).
- [70] G. Vidal and J. I. Cirac, Phys. Rev. Lett. **86**, 5803 (2001).
- [71] D. Yang, M. Horodecki, R. Horodecki, and B. Synak-Radtke, Phys. Rev. Lett. **95**, 190501 (2005).
- [72] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
- [73] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *Preprint quant-ph/0506189*.
- [74] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
- [75] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
- [76] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).
- [77] R. Horodecki and P. Horodecki, Phys. Lett. A **194**, 147 (1994).
- [78] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **210**, 377 (1996).
- [79] I. Devetak and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005); also *Preprint quant-ph/0306078*.
- [80] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 433 (2000).
- [81] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. Terhal, and A. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
- [82] P. Horodecki, J. Smolin, B. Terhal, and A. Thapliyal, Theor. Comput. Sci. **292**, 589 (2003).

- [83] P. Horodecki, M. Lewenstein, G. Vidal, and I. Cirac, Phys. Rev. A **62**, 032310 (2000).
- [84] D. Dür, J. I. Cirac, M. Lewenstein, and D. Bruss, Phys. Rev. A **61**, 062313 (2000).
- [85] P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **86**, 2681 (2001).
- [86] P. Horodecki, Acta Physica Polonica **101**, 399 (2002).
- [87] G. Giedke, J. Eisert, J.I. Cirac, and M.B. Plenio, Quant. Inf. Comp. **3**, 211 (2003).
- [88] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal, Quant. Inf. Comp. **1**, 70 (2001).
- [89] A. Peres, Found. Phys. **29**, 589 (1999).
- [90] R. F. Werner and M. M. Wolf, Phys. Rev. A **61**, 062102 (2000).
- [91] T. Mor and P. Horodecki, *Preprint* quant-ph/9906039; G. Brassard, P. Horodecki, and T. Mor, IBM J. Res. Dev. **48**, 87 (2004).
- [92] N. Linden, S. Popescu, Phys. Rev. A **59**, 137 (1999).
- [93] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
- [94] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [95] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1046 (1999).
- [96] E. M. Rains, IEEE Trans. Inform. Theory **47**, 2921 (2001); also *Preprint* quant-ph/0008047.
- [97] T. Eggeling, K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf Phys. Rev. Lett. **87**, 257902 (2001)
- [98] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
- [99] Ll. Masanes, Phys. Rev. Lett. **96**, 150501 (2006).
- [100] Ll. Masanes, *Preprint* quant-ph/0510188.
- [101] S. Ishizaka, Phys. Rev. Lett. **93**, 190501 (2004).
- [102] P. Horodecki, M. Horodecki, and R. Horodecki, J. Mod. Opt. **47**, 347 (2000), also *Preprint* quant-ph/9904092.
- [103] P. Horodecki, Cent. Eur. J. Phys. **1**, 695 (2003).
- [104] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).
- [105] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [106] K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki, *Preprint* quant-ph/0506203.
- [107] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
- [108] N. Gisin and S. Wolf, in: CRYPTO 2000 p. 482; also *Preprint* quant-ph/0005042.
- [109] U. Maurer and S. Wolf, IEEE Transactions on Information Theory **45**, 499 (1999).
- [110] R. Renner and S. Wolf, Advances in Cryptology—EUROCRYPT '03, Lecture Notes in Computer Science (Springer, Berlin, 2003).
- [111] A. Acín, J. I. Cirac, and Ll. Masanes, Phys. Rev. Lett. **92**, 107903 (2004).
- [112] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, R. Renner, *Preprint* quant-ph/0608199.
- [113] W. Dür and J. I. Cirac, J. Phys. A: Math. Gen. **34**, 6837 (2001).
- [114] P. W. Shor, J. A. Smolin, and A. V. Thaplyal, Phys. Rev. Lett. **90**, 107901 (2003).

- [115] M. Murao and V. Vedral, Phys. Rev. Lett. **86**, 352 (2001).
- [116] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
- [117] S. Bandyopadhyay, I. Chattopadhyay, V. P. Roychowdhury, and D. Sarkar, Phys. Rev. A **71**, 062317 (2005); also *Preprint* quant-ph/0411082.
- [118] R. Augusiak and P. Horodecki, Phys. Rev. A **73**, 012318 (2006); also *Preprint* quant-ph/0411142.
- [119] C. Brukner, M. Zukowski, J.-W. Pan, and A. Zeilinger, Phys. Rev. Lett. **92**, 127901 (2004).
- [120] A. Acin, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **87**, 040401 (2001).
- [121] W. Dür, Phys. Rev. Lett. **87**, 230402 (2001).
- [122] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990); A. V. Belinskii and D. N. Klyshko, Phys. Usp. **36**, 6533 (1993).
- [123] R. F. Werner and M. W. Wolf, Phys. Rev. A **64**, 032112 (2001).
- [124] M. Zukowski and C. Brukner, Phys. Rev. Lett. **88**, 210421 (2002).
- [125] D. Kaszlikowski, L. C. Kwek, J. Chen, and C. H. Oh, Phys. Rev. A **66**, 052309 (2002).
- [126] A. Sen(De), U. Sen, and M. Żukowski, Phys. Rev. A **66**, 062318 (2002).
- [127] A. Acin, Phys. Rev. Lett. **88**, 027901 (2002).
- [128] R. Augusiak and P. Horodecki, Phys. Rev. A **74**, 010305 (2006).
- [129] C. Brukner, M. Zukowski, and A. Zeilinger, Phys. Rev. Lett. **89**, 197901 (2002).
- [130] P. Horodecki and M. Lewenstein, Phys. Rev. Lett. **85**, 2657 (2000).
- [131] P. Horodecki, J. I. Cirac, and M. Lewenstein, *Bound entanglement in continuous variables is a rare phenomenon*, in: S. L. Braunstein and A. K. Pati (eds.) Quantum Information with Continuous Variables, p. 211.
- [132] W. Dür, J. I. Cirac, and P. Horodecki, Phys. Rev. Lett. **93**, 020503 (2004).
- [133] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000); R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
- [134] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).
- [135] G. Giedke, Lu-Ming Duan, J. I. Cirac, and J. I. Zoller, Quant. Inf. Comp. **1**, 79 (2001).
- [136] M. Navascués, J. Bae, J. I. Cirac, M. Lewenstein, A. Sanpera, and A. Acin, Phys. Rev. Lett. **94**, 010502 (2005).

13 Multiparticle Entanglement

Jens Eisert and David Gross

13.1 Introduction

Multiparticle entanglement is genuinely different from entanglement in quantum systems consisting of two parts. The prefix *multi* may refer here to quantum systems composed of a macroscopic number of subsystems, such as the parts of an interacting many-body system, or it may mean merely “three.” To fathom what is so different consider, say, a quantum system that is composed of three qubits. Each of the qubits is thought to be held by one of the paradigmatic distantly separated parties. It may come as quite a surprise that states of such composite quantum systems may contain tri-partite entanglement, while at the same time showing no bipartite entanglement at all. Such quantum states can only be generated when all parties come together and prepare the state using local physical devices. Whenever any two parties group together, the state becomes separable, and hence contains no bipartite entanglement at all.

In this chapter, we aim at fleshing out in what ways this multipartite setting is different from the situation that we encountered earlier in this book. It is still true that entanglement can be conceived as that property of states that can be exploited to overcome constraints of locality. Yet, locality refers here to the several distinct subsystems, and we indeed already encounter a much richer situation when asking questions of what states are equivalent up to a mere local change of basis. In sharp contrast to the bipartite setting, there is no longer a natural “unit” of entanglement, the role that was taken by the maximally entangled state of a system of two qubits. Quite strikingly, the very concept of being maximally entangled becomes void. Instead, we will see that in two ways there are “inequivalent kinds of entanglement.” We will explore some of the ramifications of these inequivalent kinds of entanglement.

Space limitations do not allow for a treatment of this subject matter in full detail, yet, we aim at “setting the coordinates” and guiding through the extensive literature in this field. Our coordinate system chosen for this chapter has the axes labeled pure and mixed states on the one hand, entanglement in single specimens and the asymptotic setting on the other hand. We very briefly mention ways to detect multiparticle entanglement, and introduce the concept of stabilizer and graph states. Finally, we stress that multiparticle entanglement does not only have applications in information processing as such, but also in metrology, for example in the context of precision frequency standards using trapped ions. This chapter emphasizes on the theory of multiparticle entanglement in finite-dimensional quantum systems; however, we will mention key experimental achievements whenever possible, notably using ion traps and purely optical systems.

13.2 Pure States

We will first fix one dimension in our coordinate system, and consider multiparticle entanglement of *pure* quantum states. This is the study of state vectors in a Hilbert space

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_N$$

of a quantum mechanical system of N constituents. We will first take a closer look at entanglement in single specimens of multipartite systems, that is of single “copies.” We will then turn to the asymptotic regime, where one asks questions of inconvertibility when one has many identically prepared systems at hand.

13.2.1 Classifying entanglement of single specimens

A theory of entanglement should not discriminate states that differ only by a local operation. Here, “local operation” can mean merely a change of local bases (LU operations) or, else, general local quantum operations assisted by classical communication, that are either required to be successful at each instance (LOCC) or just stochastically (SLOCC). For each notion of locality, the questions that have to be addressed are how many equivalence classes exist, how are they parameterized, and how can one decide whether two given states belong to the same class? We will briefly touch upon these problems, limiting our attention to equivalence under LU operations and SLOCC in turn.

For the case of LU-equivalence of bipartite qubit states, the *Schmidt normal form*

$$\sin \theta |0, 0\rangle + \cos \theta |1, 1\rangle$$

gives a concise answer to all the above questions. Two quantum states are LU equivalent if and only if their respective Schmidt normal forms coincide. All classes are parameterized by only one real parameter: the angle θ .

Some simple *parameter counting* arguments show that in the case of N qubit systems the situation must be vastly more complex. Indeed, disregarding a global phase, it takes $2^{N+1} - 2$ real parameters to fix a normalized quantum state in $\mathcal{H} = (\mathbb{C}^2)^{\otimes N}$. The group of local unitary transformations $SU(2) \times \cdots \times SU(2)$ on the other hand has $3N$ real parameters. Because the set of state vectors that are LU equivalent to a given $|\psi\rangle$ is the same as the image of $|\psi\rangle$ under all local unitaries, the dimension of an equivalence class cannot exceed $3N$ (it can be less if $|\psi\rangle$ is *stabilized* by a continuous subset of the local unitaries). Therefore, one needs at least $2^{N+1} - 3N - 2$ real numbers to parameterize the sets of inequivalent pure quantum states [1]. Perhaps surprisingly—considering the rough nature of the argument—this lower bound turns out to be tight [2]. It is a striking result that the ratio of nonlocal to local parameters grows exponentially in the number of systems. In particular, the finding rules out all hopes of a naive generalization of the Schmidt normal form. A general pure tri-partite qubit state, say, *cannot* be cast into the form

$$\sin \theta |0, 0, 0\rangle + \cos \theta |1, 1, 1\rangle$$

by the action of local unitaries [3].

Considerable effort has been undertaken to describe the structure of LU-equivalence classes by the use of *invariants* or *normal forms* [1, 2, 4–6]. By now, even for a general multiparticle system a normal form is known which is a generalization of the Schmidt form in the sense that it uses a minimal number of product vectors from a factorizable orthonormal basis to express a given state [2]. To give the reader an impression of how such generalized forms look like, we will briefly sketch the derivation of the simplest case, being defined on three qubits [6]. We start with a general state vector

$$|\psi\rangle = \sum_{i,j,k} \alpha_{i,j,k} |i, j, k\rangle.$$

Define two matrices T_0, T_1 by $(T_i)_{j,k} = \alpha_{i,j,k}$. If we apply a unitary operator U_1 with matrix elements $u_{i,j}$ to the first qubit, then the matrix T_0 transforms according to $T'_0 = u_{0,0}T_0 + u_{0,1}T_1$. The algebraic constraint $\det(T'_0) = 0$ amounts to a quadratic equation in $u_{0,1}/u_{0,0}$ and can thus always be fulfilled. We go on to diagonalize T'_0 by applying two unitaries U_2, U_3 to the second and third systems such that

$$U_2 T'_0 U_3 = \begin{pmatrix} \lambda_0 & 0 \\ 0 & 0 \end{pmatrix}.$$

By absorbing phases into the definition of the basis states $|0\rangle_1, |1\rangle_1, |1\rangle_2, |1\rangle_3$, we arrive at

$$\begin{aligned} (U_1 \otimes U_2 \otimes U_3)|\psi\rangle &= \lambda_0 |0, 0, 0\rangle + \lambda_1 e^{i\phi} |1, 0, 0\rangle \\ &\quad + \lambda_2 |1, 0, 1\rangle + \lambda_3 |1, 1, 0\rangle + \lambda_4 |1, 1, 1\rangle \end{aligned} \quad (13.1)$$

with real coefficients λ_i . Normalization requires $\sum_i \lambda_i^2 = 1$. It is shown in [6] that $0 \leq \phi \leq \pi$ can always be achieved and further that for a generic¹ state vector the form (13.1) is unique. In accordance with the formula we derived earlier, the normal form depends on five independent parameters.

How does the situation look like if one allows the local operations to be SLOCC? An SLOCC protocol that maps a state vector $|\psi\rangle$ to $|\phi\rangle$ with some probability of success consists of several rounds in each of which the parties perform operations on their respective systems, possibly depending on previous measurement results. One can think of the protocol as splitting into different *branches* with each measurement. It should be clear that $|\psi\rangle \rightarrow |\phi\rangle$ is possible if and only if at least *one* of these branches does the job. The effect of each single branch on the state vector can be described by one *Kraus operator* A_i per system:

$$|\psi\rangle \mapsto (A_1 \otimes \cdots \otimes A_N)|\psi\rangle.$$

If $|\psi\rangle$ and $|\phi\rangle$ are *equivalent* under SLOCC, then the operators A_i can be chosen to be invertible [7–9]. Note that the term *filtering operation* is used synonymously with SLOCC.

Having thus established a framework for dealing with SLOCC operations, we can repeat the parameter counting argument from the LU case. By simply substituting the local unitary group by $\text{SL}(\mathbb{C}^2) \times \cdots \times \text{SL}(\mathbb{C}^2)$ one finds a lower bound of $2^{N+1} - 6N - 2$ parameters that are necessary to label SLOCC equivalence classes of qubit systems. The inevitable next step

¹In this context *generic* means for all state vectors but a set of measure zero.

would be to adopt the classification of equivalence classes by invariants and normal forms from the LU case to the SLOCC one. While this has indeed been done [7], we are instead going to focus on a particularly interesting special case. Indeed, for the case of three qubits, the above estimation formula does not give a positive lower bound for the number of parameters and therefore one might expect that there is only a discrete set of inequivalent classes.

Five SLOCC-inequivalent subsets of three-qubit pure states can be identified by inspection [9]. *Product vectors*

$$|\psi\rangle_1|\phi\rangle_2|\pi\rangle_3$$

certainly form a class of their own because local operations can never create entanglement between previously unentangled systems. For the same reason vectors of the form

$$|\psi\rangle_1|\Phi\rangle_{2,3}$$

with some nonfactoring state vector $|\Phi\rangle_{2,3}$ constitute an SLOCC-equivalence class, the class of *bipartite* entangled states that factor with respect to the *split* 1-23 of the set of systems. There are three such splits (1-23, 12-3, 13-2) giving rise to three bipartite classes. Calling these sets *equivalence classes* is justified, because any two entangled bipartite pure states are equivalent under SLOCC for qubit systems. Finally, we are left with the set of *fully entangled* vectors that admit no representation as tensor products. Do they form a single equivalence class? It turns out that this is not the case.

To understand why this happens, we will employ an invertible SLOCC invariant [9, 10]. Any pure state can be written in the form

$$|\psi\rangle = \sum_{i=1}^R \alpha_i |\psi_1^i\rangle_1 \otimes \cdots \otimes |\psi_N^i\rangle_N. \quad (13.2)$$

Now let $R_{\min}$ be the minimal number of product terms needed to express $|\psi\rangle$. A moment of thought shows that this number is constant under the action of invertible filtering operations (we will re-visit this invariant in Section 13.4 where its logarithm is called the *Schmidt measure*). Now consider the states vectors

$$\begin{aligned} |\text{GHZ}\rangle &= (|0, 0, 0\rangle + |1, 1, 1\rangle)/\sqrt{2}, \\ |\text{W}\rangle &= (|0, 0, 1\rangle + |0, 1, 0\rangle + |1, 0, 0\rangle)/\sqrt{3}. \end{aligned}$$

It takes a few lines [9] to show that there is no way of expressing $|\text{W}\rangle$ using only two product terms and hence the two states cannot be converted into each other by SLOCC. In this sense, there are two “inequivalent forms” of pure tri-partite entanglement of three qubits. Notably, neither form can be transformed into the other with any probability of success (however, see Section 13.3.1). Three-qubit W states and GHZ states have already been experimentally realized, both purely optically using postselection [11, 12] and in ion traps [13]. This picture is complete: any fully entangled state is SLOCC equivalent to either $|\text{GHZ}\rangle$ or $|\text{W}\rangle$ [9]. We conclude that the three qubits’ pure states are partitioned into a total of six SLOCC equivalence classes.

We take the occasion to exemplify some concepts in multiparticle entanglement theory by studying the properties of the GHZ and the W state. A simple calculation shows that after a measurement of the observable corresponding to the Pauli matrix X_1 on the first qubit, both $|\text{GHZ}\rangle$ and $|\text{W}\rangle$ collapse into a Bell state on the systems labeled 2 and 3 *regardless of the measurement outcome*. Because either state is invariant under system permutations, we can project—with certainty—any pair of systems into a Bell state by performing a suitable measurement on the remaining qubit. This property can immediately be generalized to states on more than three systems and is known as *maximal connectedness* [14]. The maximum degree of entanglement of the state into which a pair can be projected by suitable local measurements on the other parts is the *localizable entanglement* [15].

The two states behave differently, however, if a system is traced out. Specifically, tracing out the first qubit of the GHZ state will leave the remaining systems in a complete mixture. Yet, for $|\text{W}\rangle$ we have

$$\text{tr}_1[|\text{W}\rangle\langle\text{W}|] = \frac{1}{3}|0,0\rangle\langle 0,0| + \frac{2}{3}|\Psi^+\rangle\langle\Psi^+|, \quad (13.3)$$

where $|\Psi^+\rangle = (|0,1\rangle + |1,0\rangle)/\sqrt{2}$. The operator in Eq. (13.3) is a mixed *entangled* bipartite state. It is in that sense, that the entanglement of $|\text{W}\rangle$ is more *robust* under particle loss than that of $|\text{GHZ}\rangle$ [9]. Can a “super-robust” fully entangled three-qubit state be conceived that leaves any pair of systems in a Bell state if the third particle is lost? Unfortunately not, because if $|\psi\rangle$ does not factor, $\text{tr}_1[|\psi\rangle\langle\psi|]$ is mixed—and in particular not fully entangled [16]. This phenomenon has been dubbed the *monogamous nature* of entanglement.

13.2.2 Asymptotic manipulation of multiparticle quantum states

Needless to say, instead of manipulating quantum systems at the level of single specimens, entanglement manipulation is meaningful in the asymptotic limit. Here, one assumes that one has many identically prepared systems at hand, in a state $\rho^{\otimes n}$, and aims at transforming them into many other identical states $\sigma^{\otimes m}$, for large n and m , involving collective operations. This is the asymptotic setting that we have previously encountered in this book. As mentioned before, one does not require that the target state is reached exactly, but only with an error that is asymptotically negligible. This setting is notably different from that of the previous subsection, where transformations were considered for single specimens of multipartite quantum systems.

It is instructive again to briefly reconsider the situation when only two subsystems are present. In that case, the task of classifying different “kinds” of entanglement is void. Any bipartite entanglement of pure states is essentially equivalent to that of an EPR pair. One can asymptotically transform any bipartite state into a number of maximally entangled qubits’ pairs and back, the achievable optimal rate in this transformation being given by the entropy of the reduction [17]. In this sense, one can say that there is only one ingredient to asymptotic bipartite entanglement: this is the maximally entangled qubit pair. Pure states can be characterized by the content of this essential ingredient, giving rise to the *entropy of entanglement*, which is the unique measure of entanglement. How is this for multiparticle systems?

Again, it turns out that the situation is much more complex than before. Before stating how the situation is like in the multiparticle setting, let us first make the concept of *asymptotic*

reversibility more precise. If $\rho^{\otimes n}$ can be transformed under LOCC into $\sigma^{\otimes m}$ to arbitrary fidelity, there is no reason why n/m should be an integer. So to simplify notation, one typically also takes noninteger yields into account. One says that $|\psi\rangle^{\otimes x}$ is *asymptotically reducible* to $|\phi\rangle^{\otimes y}$ under LOCC, if for all $\delta, \varepsilon > 0$ there exist natural n, m such that

$$\left| \frac{n}{m} - \frac{x}{y} \right| < \delta, \|\Psi(|\psi\rangle\langle\psi|^{\otimes n}), |\phi\rangle\langle\phi|^{\otimes m}\|_1 > 1 - \varepsilon.$$

Here, $\|A\|_1 = \text{tr}|A| = \text{tr}[(A^\dagger A)^{1/2}]$ denotes the trace-norm of an operators A as a distance measure, and Ψ is the quantum operation which is LOCC. If both $|\psi\rangle^{\otimes x}$ can be transformed into $|\phi\rangle^{\otimes y}$ and $|\phi\rangle^{\otimes y}$ into $|\psi\rangle^{\otimes x}$, the transformation is *asymptotically reversible*. In the bipartite case, it is always true that any $|\psi\rangle$ can be transformed into

$$|\psi^+\rangle^{\otimes E(|\psi\rangle\langle\psi|)}, \quad |\psi^+\rangle = (|0, 0\rangle + |1, 1\rangle)/\sqrt{2},$$

where $E(|\psi\rangle\langle\psi|) = S(\text{tr}_2[|\psi\rangle\langle\psi|])$ is the entropy of entanglement, and this transformation is asymptotically reversible [17–19]. Such a maximally entangled qubit pair can hence be conceived as the only essential ingredient in bipartite entanglement of pure states. This holds true not only for qubit systems, but also for systems of any finite dimension, and with small technicalities even for infinite-dimensional systems [20].

In the multipartite setting, there is no longer a single essential ingredient, but many different ones. For pure states on $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$, given a set of state vectors

$$S = \{|\psi_1\rangle, \dots, |\psi_k\rangle\}$$

for some k , one may consider their *entanglement span* as the set of pure states that can reversibly be generated using S under asymptotic LOCC [18]. In the bipartite setting, the entanglement span is always given by the set of all pure states (not taking the trivial case into account where S contains only product states). In the multipartite case, however, it is meaningful to introduce the concept of a *minimal reversible entanglement generating set (MREGS)*. An MREGS S is a set of pure states such that any other state can be generated from S by means of reversible asymptotic LOCC. It must be minimal in the sense that no set of smaller cardinality possesses the same property [18, 21, 22].

After this preparation, what is now the MREGS for, say, a tri-partite quantum system? The irony is that even in this relatively simple case, no conclusive answer is known. Only a few states have been identified that must be contained in any MREGS. At first one might be tempted to think that three different maximally entangled qubit pairs, shared by two systems each, already form an MREGS. This natural conjecture is not immediately ruled out by what we have seen in the previous subsection: after all, we do not aim at transforming quantum states of single specimens, but rather allow for asymptotic state manipulation. Yet, it can be shown that merely to consider maximally entangled qubit pairs is not sufficient to construct an MREGS [21]. What is more, even

$$S = \{|\psi^+\rangle_{1,2}, |\psi^+\rangle_{1,3}, |\psi^+\rangle_{2,3}, |\text{GHZ}\rangle\}$$

does not suffice. All these pure states are *inequivalent with respect to asymptotic reducibility*, but there are pure states that cannot be reversibly generated from these ones alone [23]. So

again, we see that there are *inequivalent kinds of entanglement*. Because we allowed for asymptotic manipulations, the present inequivalence is even more severe than that encountered in the last section.

To find general means for constructing MREGS constitutes one of the challenging open problems of the field: as long as this question is generally unresolved, the development of a “theory of multiparticle entanglement” in the same way as in the bipartite setting seems unfeasible. Whereas in the latter case the “unit” of entanglement is entirely Unambiguous—it is the EPR pair—there is no substitute for it in sight for multipartite systems. This motivates after all to consider more pragmatic approaches to grasp multiparticle entanglement.

13.3 Mixed States

13.3.1 Classifying mixed state entanglement

The program pursued in Section 13.2—parameterizing all equivalence classes of states under various types of local operations—can in principle also be applied to mixed states [4, 24]. However, we will content ourselves with sketching a more rough classification scheme based on *separability properties* [25].

At the lowest level there is the class of states that can be prepared using LOCC alone. Its members are called *fully separable* and can be written in the form

$$\rho = \sum_i p_i (\rho_1^i \otimes \cdots \otimes \rho_N^i).$$

Evidently, states of this kind do not contain entanglement. Now arrange the N parts of the multiparticle system in $k \leq N$ groups. We can conceive the groups as the constituents of a k -partite quantum system. This *coarse graining* procedure is called forming a *k-partite split* of the system and indeed, we have less explicitly encountered that concept before in Section 13.2. Having set up this terminology, it is meaningful to ask with respect to which splits a given quantum state is fully separable. Two states belong to the same *separability class* if they are separable with respect to the same splits. Clearly, being in the same class in this sense is a necessary condition for being equivalent under any type of local operations.

A state is referred to as *k-separable*, if it is fully separable considered as a state on some k -partite split. By the use of this terminology, the separability classes can be brought into a hierarchy, where k -separable classes are considered to be more entangled than l -separable ones for $k < l$. States that are not separable with respect to any nontrivial split are *fully inseparable*.

The number of all splits of a composite system grows exorbitantly fast with the number N of its constituents. One is naturally tempted to reduce the complexity by identifying *redundancies* in this classification. After all, once it is established that a state is fully separable, there is no need to consider any further splits. While such redundancies certainly exist, pinpointing them turns out to be subtle and indeed gives rise to one of the more peculiar results in quantum information theory, as will be exemplified by means of our standard example, the three-qubit system.

The five possible splits of three systems (1-2-3, 12-3, 1-23, 13-2, 123) have already been identified in Section 13.2. It is a counter-intuitive fact that there are mixed states that are separable with respect to any bipartite split but are not fully separable [28]. An analogous phenomenon does not exist for pure states. The following subclasses of the set of biseparable² states are all nonempty [25].

- *1-qubit biseparable states* with respect to the first system are separable for the split 1-23 but not for 12-3 or 13-2.
- *2-qubit biseparable states* with respect to the first and second system are separable for the split 1-23 and 2-13, but not for 12-3.
- *3-qubit biseparable states* are separable with respect to any bipartite split but are not fully separable.

Together with the inseparable states and the fully separable ones, the above sets constitute a complete classification of mixed three-qubit states modulo system permutations [26].

We end this subsection with a refinement of the class of inseparable states that will play a role in the following subsection [27]. In this paragraph, the fully separable states are denoted by S , the biseparable ones by B , and lastly, the set of all mixed states including the fully inseparable ones by F . Clearly, $S \subset B \subset F$ is a hierarchy of convex sets. Now, recall the two different classes of genuine three-qubit pure state entanglement that were identified in Section 13.2. We define W to be the set of states that can be decomposed as a convex combination of biseparable ones and projections onto W -type vectors and finally rename the set of all states GHZ . This leaves us with a finer partitioning $S \subset B \subset W \subset GHZ$ of the state space in terms of convex sets. The definition suggests that the GHZ -type vectors are in some way more entangled than the W states—which until now we had no reason to suspect.³

In order to justify the construction, we need to employ another tool from Section 13.2: the generalized Schmidt normal form. A pure three-particle state is SLOCC equivalent to the W state if and only if its Schmidt normal form reads

$$\lambda_0|0, 0, 0\rangle + \lambda_1|1, 0, 0\rangle + \lambda_2|1, 0, 1\rangle + \lambda_3|1, 1, 0\rangle, \quad (13.4)$$

that is, if $\lambda_4 = \phi = 0$. Comparing (13.4) to the general form (13.1) shows that $|W\rangle + \epsilon|1, 1, 1\rangle$ must be of GHZ type for any $\epsilon > 0$. Physically, this means that even though one cannot turn a GHZ -type vector into $|W\rangle$ using SLOCC, one can *approximate* it as closely as desired. Therefore, we can transform states (at least approximately) from the outer to the inner classes: $GHZ \rightarrow W \rightarrow B \rightarrow S$ by means of noninvertible local filtering operations. Note that invertible local operations leave the classification of a state invariant. As a last remark, formula (13.4) and the parameter counting considerations in Section 13.2 show that both the product vectors and the W -type vectors form a subset of measure zero among all pure states. Notwithstanding, it can be shown [27] that S as well as $W \setminus B$ are of finite volume in the set of mixed states.

²Biseparable means 2-separable.

³The higher Schmidt measure of the W state even suggests the contrary.

13.3.2 Methods of detection

One way of experimentally detecting multiparticle entanglement is to perform a complete quantum state tomography, and to see whether the resulting estimated state is consistent with an entangled state.⁴ Depending on the context, this can be a costly procedure. It may be desirable to detect entanglement without the need of acquiring full knowledge of the quantum state. Such an approach can be advantageous when certain types of measurements are more accessible than others, and when one intends to detect entanglement based on data from these restricted types of measurements, as such insufficient to fully reconstruct the state. This is where *entanglement witnesses* come into play.

An entanglement witness A is an observable that is guaranteed to have a positive expectation value on the set S of all separable states. So whenever the measurement of A on some quantum state ρ gives a negative result, one can be certain that ρ contains some entanglement. It is, however, important to keep in mind that witnesses deliver only *sufficient* conditions. In addition to S , there might be other, nonseparable states that have a positive expectation value with respect to A .

We are now going to take a more systematic look at this technique and, at the same time, generalize it from S to any compact convex set C in state space. To that end, we note that the set of quantum states σ that satisfy the equation $\text{tr}[\sigma A] = 0$ for some observable A form a *hyperplane* which partitions the set of states into two half spaces. If C is contained in one of these half spaces, the plane is called a *supporting hyperplane* of C . Each half space is characterized by the fact that for all its respective elements σ the sign of $\text{tr}[\sigma A]$ is fixed. Now, if ρ is a state contained in the half space “opposing” C , we have, for all $\sigma \in C$,

$$\text{tr}[A\rho] < 0, \quad \text{tr}[A\sigma] \geq 0.$$

But $\text{tr}[A\rho]$ is nothing but the expectation value of A and a negative result suffices to assert that $\rho \notin C$. In this way, entanglement witnesses witness entanglement.

Witnesses can be constructed for all the convex sets that appeared in the classification of the previous subsection. For example, a GHZ witness is an operator that detects states that are not of W type. It is not difficult to see that

$$A_{\text{GHZ}} = \frac{3}{4}\mathbb{I} - |\text{GHZ}\rangle\langle\text{GHZ}|$$

is a GHZ witness: We have that $\langle\text{GHZ}|\rho|\text{GHZ}\rangle \leq 3/4$ for any W-type state, and hence $\text{tr}[A_{\text{GHZ}}\rho] \geq 0$ for any W-type state. More generally, such witnesses can be constructed as

⁴The question that we will only touch here is the one of how to *computationally determine whether a known quantum state is in one of the mentioned separability classes*. It turns out that already in the bipartite case, deciding separability is an NP-hard problem [29]. One can nevertheless construct hierarchies of efficiently decidable sufficient criteria for a state being, say, fully inseparable. This is possible in a way insuring that every fully entangled state is necessarily detected in some step of the hierarchy [30, 31]. One route toward finding such criteria is to cast the problem into a polynomially constrained optimization problem, involving polynomials of degree 3 only. This is feasible due to the fact that any Hermitian matrix for which $\text{tr}[M^2] = 1$, $\text{tr}[M^3] = 1$ is a matrix that satisfies $\text{tr}[M] = 1$, $M = M^2$, $M \geq 0$, so is one that corresponds to a pure quantum state [30, 32]. This can be used to parameterize the separable states from some separability class in terms of polynomial expressions. Relaxing the problem to hierarchies of efficiently decidable semi-definite programs then amounts to a two-way test of being fully inseparable [30]. For alternative algorithms for deciding multiparticle entanglement, see [31, 33, 34].

$A_{\text{GHZ}} = Q - \varepsilon \mathbb{I}$ with an appropriate $\varepsilon > 0$, where $Q \geq 0$ is a matrix that does not have any W-type state in its kernel. In turn, $\rho = |\text{GHZ}\rangle\langle\text{GHZ}|$ is a state that will evidently be detected as not being of W type. Similarly, a W witness is given by

$$A_{\text{W}} = \frac{2}{3} \mathbb{I} - |\text{W}\rangle\langle\text{W}|. \quad (13.5)$$

Needless to say, such witnesses are an especially convenient tool in the multipartite setting, when they are evaluated using only local measurements. Just in the same way as one can choose a basis consisting of product matrices when performing a tomographic measurement, expectation values of witness operators can be obtained with appropriate local measurements, using local decompositions [37]. The detection of multiparticle entanglement using witness operators has already been experimentally realized [38]. Indeed, one of the estimated witness operators in the experiment was of the form given in Eq. (13.5).

13.4 Quantifying Multiparticle Entanglement

Entanglement measures give an answer to the question to what degree a quantum state is entangled. Their values are typically related to the usefulness of the state for quantum information applications. Entanglement measures can, for example, be related to teleportation fidelities or rates at which a secure key can be extracted. As has been pointed out in the case of the bipartite setting, there are two approaches to quantify entanglement. Firstly, in the axiomatic approach, one specifies certain criteria that any meaningful entanglement measure must satisfy, and identifies functions that fulfill all these criteria. Secondly, one may quantify a state's entanglement directly in terms of rates of a certain protocol that can optimally be achieved using that state.

In the case considered in this chapter, the route taken in the bipartite setting is not accessible: in particular, one cannot evaluate asymptotic rates at which one can distill the elements of an MREGS from a given state. This would be the analog of the distillable entanglement. In turn, the cost would correspond to the rates at which one can prepare a state asymptotically starting from MREGS elements. This route is inaccessible; one of the reasons being that the MREGS are unknown.

More pragmatically, one can still quantify multiparticle entanglement in terms of meaningful functions that are multiparticle *entanglement monotones*, that is, positive functions vanishing on separable states that do not increase under LOCC, equipped with some physical interpretation.

- The *Schmidt measure* E_S [10, 39] is the logarithm of the minimal number of products in a product decomposition $E_S = \log_2(R_{\min})$ (see Eq. (13.2)). It provides a classification of multiparticle entangled states and is an entanglement monotone. In the bipartite case, this measure reduces to the *Schmidt rank*, i.e., the rank of the reduction. This measure is particularly suitable to quantify entanglement in graph states with many constituents.

- Another candidate is the *global entanglement* E_{Global} of [40]. This is a measure of entanglement for an N -qubit system, equipped with a Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes N}$.⁵
- The *geometric measure of entanglement* [41] makes use of a geometric distance to the set of product states:

$$E_{\text{Geometric}} = \min \| |\psi\rangle\langle\psi| - \sigma \|_2,$$

where $\|\cdot\|_2$ is the Hilbert–Schmidt norm, and the minimum is taken over all product states.

- The *tangle* [16] is a measure of entanglement suitable for systems consisting of three qubits. This measure of entanglement is based on the entanglement of formation, or rather on the *concurrence*, as

$$\tau(\rho) = C^2(\rho_{1-23}) - C^2(\rho_{1-2}) - C^2(\rho_{1-3}).$$

Here, $C(\rho_{i-j})$ is the concurrence of the reduction with respect to systems labeled i, j , and $C(\rho_{1-23})$ is the concurrence of ρ in the split $1-23$. The concurrence, in turn, is given by $C(\rho) = \max\{0, \lambda_1^{1/2} - \lambda_2^{1/2} - \lambda_3^{1/2} - \lambda_4^{1/2}\}$, where $\lambda_1, \dots, \lambda_4$ are the singular values of $\rho\tilde{\rho}$, nonincreasingly ordered, and $\tilde{\rho} = \mathbb{I} \otimes \mathbb{I} - \rho_1 \otimes \mathbb{I} - \mathbb{I} \otimes \rho_2 + \rho$. As is by no means obvious, this quantity is invariant under permutation of the three systems and is in fact an entanglement monotone for three-qubit systems. It can be efficiently computed and applied to mixed states without the need for taking convex hulls.

- The *relative entropy of entanglement* in the multipartite setting is defined as the minimal distance of a given state to the set of fully separable states, quantified in terms of the quantum relative entropy [42].

13.5 Stabilizer States and Graph States

We now turn to a specific class of multiparticle entangled states which provides a very useful theoretical “laboratory”: The stabilizer formalism provides a powerful picture for grasping a wide class of states and operations. Stabilizer states are multiqubit quantum states that

⁵This measure of entanglement is defined as follows: Starting point is a map f_j

$$f_j(b)|b_1, \dots, b_N\rangle = \delta_{b, b_j} |b_1, \dots, b_{j-1}, b_{j+1}, \dots, b_N\rangle, \quad (13.6)$$

where the vectors $|b_1, \dots, b_N\rangle$ with $b_i \in \{0, 1\}$ span the Hilbert space $\mathcal{H}$. The right-hand side of Eq. (13.6) is hence either zero, or the entry b_j is omitted. This map can be extended to a map $\mathbb{C}^2 \otimes (\mathbb{C}^2)^{\otimes N} \rightarrow (\mathbb{C}^2)^{\otimes N-1}$ by linearity. In turn, for two vectors $x, y \in (\mathbb{C}^2)^{\otimes N-1}$ one may write $x = \sum_i x_i |i\rangle$ and $y = \sum_i y_i |i\rangle$ with $0 \leq i \leq 2^{N-1}$. For a state vector $|\psi\rangle$ the quantity

$$E_{\text{Global}} = \frac{4}{N} \sum_{j=1}^N d(f_j(0)|\psi\rangle, f_j(1)|\psi\rangle),$$

where $d(x, y) = \sum_{i < j} |x_i y_j - x_j y_i|^2$ is indeed a monotone on pure states. Convex hulls of pure-state entanglement monotones deliver convex monotones for mixed quantum states.

play a crucial role in quantum information science, in particular in the field of quantum error correction. It is beyond the scope of the present chapter to give an introduction to the rich literature on the stabilizer formalism. Instead, we will very briefly introduce the very concept of a stabilizer state and a graph state.

Stabilizer states form a set of quantum states that allow for an efficient description in terms of the operators they are eigenstates of. Let us exemplify this using the familiar GHZ state on three qubits. Recall that X , Y , and Z denote the well-known *Pauli operators*. It is not difficult to see that the state vector $|\text{GHZ}\rangle = (|0, 0, 0\rangle + |1, 1, 1\rangle)/\sqrt{2}$ is an eigenstate of $Z_1 \otimes Z_2 \otimes \mathbb{I}_3$, $\mathbb{I}_1 \otimes Z_2 \otimes Z_3$, and $X_1 \otimes X_2 \otimes X_3$ to the eigenvalue $+1$. This alone should not be too surprising. But then, the state vector of the GHZ state is the only state vector that has this property, up to a global phase. So instead of explicitly writing the GHZ state vector, we could have specified it by saying that it is an eigenstate of $Z_1 Z_2$, $Z_2 Z_3$, and $X_1 X_2 X_3$.

This idea can be pushed much further—and this is when the advantage of such a formalism becomes apparent. The central ingredient is the *Pauli group*. For a single system, it is given by

$$G = \{\pm \mathbb{I}, \pm i\mathbb{I}, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}.$$

The phases ensure that the group is actually closed under multiplication. The Pauli group on N qubits, G_N , in turn consists of N -fold tensor products of elements of G . It is a basic fact from linear algebra that a set of N operators $\{P_1, \dots, P_N\}$ from G_N allow for a basis of common eigenvectors if they commute mutually. The key insight lies in the observation that this basis always contains a unique element which is a common eigenvector $|\psi\rangle$ of all P_i to the eigenvalue $+1$ [44]. In other words, the operators P_i *stabilize* $|\psi\rangle$. Clearly then, $|\psi\rangle$ is also stabilized by any product of elements of $\{P_i\}_{i=1\dots N}$. The set of all such products forms an Abelian group, the *stabilizer group* which is said to be *generated* by P_i . The vector $|\psi\rangle$ is the associated *stabilizer state*, which is, again, uniquely defined by the requirement

$$P_i |\psi\rangle = |\psi\rangle.$$

We have yet to make the claim precise that the stabilizer formalism offers an efficient description. State vectors are usually specified by their expansion coefficients with respect to some product basis in Hilbert space. By computing lower bounds of the Schmidt measure (cf. Section 13.4), e.g., it can be established that there are stabilizer states that require in the order of 2^N nonvanishing terms when described in any product basis [14, 39]. Their stabilizer group, on the other hand, is determined by only N generators.

There is an even more compact description of stabilizer states, based on the familiar concept of a *graph* $G(V, E)$ which is specified by a set of vertices V and an edge set E [39, 43, 45]. With each graph on N vertices, a stabilizer group is associated by the following construction. We label the vertices with numbers 1 to N and denote by N_a the *neighbors* of the a th vertex, that is, the set of vertices directly connected to a . Now, with any vertex a , we associate an element K_a of the Pauli group via

$$K_a = X_a \prod_{b \in N_a} Z_b.$$

Using the fact that the relation of “being a neighbor” is symmetric, one can show that the K_a commute mutually and therefore specify a unique stabilized $|G\rangle$, the *graph state vector*

of G . As an example, consider a *linear graph* on four vertices. It gives rise to the generators $\{X_1Z_2, Z_1X_2Z_3, Z_2X_3Z_4, Z_3X_4\}$ and that the following vector is stabilized by each of them:

$$|\text{Cluster}\rangle = \frac{1}{4} \bigotimes_{a=1}^4 (|0\rangle Z_{a+1} + |1\rangle),$$

where we have set $Z_5 = \mathbb{I}$. It is the *four-qubit cluster state* [14], an instance of a family of states which form the central resource for measurement-based quantum computing. The four-qubit cluster state has recently been prepared in an optical experiment [46].

Any stabilizer state can be brought into the form of a graph state using only local unitaries [45]. In particular, this means that all multiparticle entanglement properties of stabilizer states can be described entirely in terms of properties of graphs. The same holds true for the effects of local Pauli measurements [39, 45, 47] and *Clifford* operations⁶ [39, 48] on graph states. Multiparticle entanglement, for example in terms of the Schmidt measure, can be assessed for graph states [39]. Stabilizer circuits can be simulated computationally more cheaply when expressed in terms of graph states [49] using the rules of [39]. They also form a convenient and physically motivated testbed to assess the question how robust multiparticle entangled states may be under decoherence processes [50, 51].

13.6 Applications of Multiparticle Entangled States

Any protocol of quantum information science making use of quantum systems with more than two constituents may be conceived as an application of multiparticle entanglement. To pinpoint the specifics of multiparticle entanglement that make a certain task possible is yet less straightforward. Multiparticle entanglement is certainly crucial for quantum error correction, where the idea is to encode logical qubits into a larger number of qubits in a multiparticle entangled state, as a protection against the entanglement with an environment beyond actual control. This, in John Preskill's words, is to "fight entanglement with entanglement." In quantum key distribution, we will encounter several applications of multiparticle entanglement. In quantum computing, multiparticle entanglement plays a key role. In measurement-based computing, as we will see later, multiparticle entangled states form the resource. The use of multiparticle entanglement can then even be "monitored" in the course of the computation [39]. It is, however, not yet entirely understood what exact criteria concerning their entanglement the involved states have to fulfill to render an efficient classical simulation impossible.

Yet, multiparticle entanglement does not only facilitate processing or transmission of information, but also allow for applications in *metrology* [52–55]. We will shortly sketch an idea to enhance the accuracy of the *estimation of frequencies* using multiparticle entangled states. This applies in particular to frequency standards based on laser-cooled ions, which can achieve very high accuracies [55]. Starting point is to prepare N ions that are loaded in a trap in some internal state with state vector $|0\rangle$. One may then drive an atomic transition with natural frequency ω_0 to a level $|1\rangle$ by applying an appropriate Ramsey pulse with frequency

⁶In the context of quantum information theory, a *Clifford* operation is a unitary operator that maps elements of the Pauli group to elements of the Pauli group under conjugation.

ω , such that the ions are in an equal superposition of $|0\rangle$ and $|1\rangle$. After a free evolution for a time t , the probability to find the ions in level $|1\rangle$ is given by

$$p = (1 + \cos((\omega - \omega_0)t))/2.$$

Given such a preparation, one finds that if one estimates the frequency ω_0 with such a scheme, the uncertainty in the estimated value is given by

$$\delta\omega_0 = (NTt)^{-1/2}.$$

This theoretical limit, the *shot-noise* limit, can in principle be overcome when entangling the ions initially. This idea has been first explored in [54], where it was suggested to prepare the ions in an N -particle GHZ state with state vector $|\text{GHZ}\rangle = (|0, 0, \dots, 0\rangle + |1, 1, \dots, 1\rangle)/\sqrt{2}$. With such a preparation, and neglecting decoherence effects, one finds an enhanced precision,

$$\delta\omega_0 = (Tt)^{-1/2}/N,$$

beating the above limit by a factor of $1/\sqrt{N}$. Unfortunately, while the GHZ state provides some increase in precision in an ideal case, it is at the same time subject to decoherence processes. A more careful analysis shows that under realistic decoherence models this enhancement actually disappears for the GHZ state. Notwithstanding these problems, the general idea of exploiting multiparticle entanglement to enhance frequency measurements can be made use of: For example, for $N = 4$ the partially entangled preparation

$$\begin{aligned} |\psi\rangle = & \lambda_0(|0, 0, 0, 0\rangle + |1, 1, 1, 1\rangle) + \lambda_1(|0, 0, 0, 1\rangle + |0, 0, 1, 0\rangle + |0, 1, 0, 0\rangle \\ & + |1, 0, 0, 0\rangle + |1, 1, 1, 0\rangle + |1, 1, 0, 1\rangle + |1, 0, 1, 1\rangle + |0, 1, 1, 1\rangle \\ & + \lambda_2(|0, 0, 1, 1\rangle + |0, 1, 0, 1\rangle + |1, 0, 0, 1\rangle + |1, 1, 0, 0\rangle + |1, 0, 1, 0\rangle + |0, 1, 1, 0\rangle) \end{aligned}$$

can lead to an improvement of more than 6%, when the probability distribution $\lambda_0, \lambda_1, \lambda_2$ is appropriately chosen and appropriate measurements are performed [55]. For four ions, exciting experiments have been performed in the meantime [56], and applied for two ions to precision spectroscopy [57], indeed showing that the shot noise limit can be beaten with the proper use of entanglement.

Acknowledgments

This work was supported by the EPSRC, the EU (IST-2002-38877), the DFG (SPP 1116, SPP 1078), and the European Research Councils (EURYI).

References

- [1] N. Linden and S. Popescu, *Fortschr. Phys.* **46**, 567 (1998).
- [2] H.A. Carteret, A. Higuchi, and A. Sudbery, *J. Math. Phys.* **41**, 7932 (2000).
- [3] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1995).
- [4] M. Grassl, M. Rötteler, and T. Beth, *Phys. Rev. A* **58**, 1853 (1998).

- [5] E.M. Rains, *Preprint* quant-ph/9703048.
- [6] A. Acín, A. Andrianov, E. Jané, and R. Tarrach, *J. Phys. A: Math. Gen.* **34**, 6725 (2001).
- [7] F. Verstraete, J. Dehaene, and B. De Moor, *Phys. Rev. A* **68**, 012103 (2003).
- [8] A. Miyake and F. Verstraete, *Phys. Rev. A* **69**, 012101 (2004).
- [9] W. Dür, G. Vidal, and J.I. Cirac, *Phys. Rev. A* **62**, 062314 (2000).
- [10] J. Eisert and H.-J. Briegel, *Phys. Rev. A* **64**, 022306 (2001).
- [11] M. Eibl, N. Kiesel, M. Bourennane, C. Kurtsiefer, and H. Weinfurter, *Phys. Rev. Lett.* **92**, 077901 (2004).
- [12] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.* **82**, 1345 (1999).
- [13] C.F. Roos, M. Riebe, H. Häffner, W. Hänsel, J. Benhelm, G.P.T. Lancaster, C. Becher, F. Schmidt-Kaler, and R. Blatt, *Science* **304**, 1479 (2004).
- [14] H.J. Briegel and R. Raussendorf, *Phys. Rev. Lett.* **86**, 910 (2001).
- [15] M. Popp, F. Verstraete, M.A. Martin-Delgado, and J.I. Cirac, *Phys. Rev. A* **71**, 042306 (2005).
- [16] V. Coffman, J. Kundu, and W.K. Wootters, *Phys. Rev. A* **61**, 052306 (2000).
- [17] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [18] C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin, and A.V. Thapliyal, *Phys. Rev. A* **63**, 012307 (2001).
- [19] G. Vidal, W. Dür, and J.I. Cirac, *Phys. Rev. Lett.* **85**, 658 (2000).
- [20] J. Eisert, C. Simon, and M.B. Plenio, *J. Phys. A: Math. Gen.* **35**, 3911 (2002).
- [21] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, *Preprint* quant-ph/9912039.
- [22] E.F. Galvao, M.B. Plenio, and S. Virmani, *J. Phys. A: Math. Gen.* **33**, 8809 (2000).
- [23] A. Acín, G. Vidal, and J.I. Cirac, *Quant. Inf. Comp.* **3**, 55 (2003).
- [24] N. Linden, S. Popescu, and A. Sudbery, *Phys. Rev. Lett.* **83**, 243 (1999).
- [25] W. Dür and J.I. Cirac, *Phys. Rev. A* **61**, 042314 (2000).
- [26] W. Dür, J.I. Cirac, and R. Tarrach, *Phys. Rev. Lett.* **83**, 3562 (1999).
- [27] A. Acín, D. Bruss, M. Lewenstein, and A. Sanpera, *Phys. Rev. Lett.* **87**, 040401 (2001).
- [28] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, *Phys. Rev. Lett.* **82**, 5385 (1999).
- [29] L. Gurvits, Annual ACM Symposium on Theory of Computing, Proceedings of 35th ACM Symposium on Theory of Computing, San Diego, CA, USA (2003).
- [30] J. Eisert, P. Hyllus, O. Gühne, and M. Curty, *Phys. Rev. A* **70**, 062317 (2004).
- [31] A.C. Doherty, P.A. Parrilo, and F.M. Spedalieri, *Phys. Rev. A* **71**, 032333 (2005).
- [32] N.S. Jones and N. Linden, *Preprint* quant-ph/0407117.
- [33] F.G.S.L. Brandao and R.O. Vianna, *Phys. Rev. Lett.* **93**, 220503 (2004).
- [34] F. Hulpke and D. Bruss, *J. Phys. A: Math. Gen.* **38**, 5573 (2005).
- [35] B.M. Terhal, *J. Th. Comput. Sci.* **287**, 313 (2002).
- [36] D. Bruss, J.I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, *J. Mod. Opt.* **49**, 1399 (2002).

- [37] O. Gühne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, *J. Mod. Phys.* **50**, 1079 (2003).
- [38] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruss, M. Lewenstein, and A. Sanpera, *Phys. Rev. Lett.* **92**, 087902 (2004).
- [39] M. Hein, J. Eisert, and H.J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
- [40] D.A. Meyer and N.R. Wallach, *J. Math. Phys.* **43**, 4273 (2002).
- [41] T.-C. Wei and P.M. Goldbart, *Phys. Rev. A* **68**, 042307 (2003).
- [42] M.B. Plenio and V. Vedral, *J. Phys. A: Math. Gen.* **34**, 6997 (2001).
- [43] D. Schlingemann and R.F. Werner, *Phys. Rev. A* **65**, 012308 (2002).
- [44] D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).
- [45] D. Schlingemann, *Quant. Inf. Comp.* **3**, 431 (2003).
- [46] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, *Nature* **434**, 169 (2005).
- [47] M. van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **70**, 034302 (2004).
- [48] M. van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **69**, 022316 (2004).
- [49] S. Anders and H.J. Briegel, *Phys. Rev. A* **73**, 022334 (2006).
- [50] M. Hein, W. Dür, and H.J. Briegel, *Phys. Rev. A* **71**, 032350 (2005).
- [51] A.R.R. Carvalho, F. Mintert, and A. Buchleitner, *Phys. Rev. Lett.* **93**, 230501 (2004).
- [52] P. Cappelaro, J. Emerson, N. Boulant, C. Ramanathan, S. Lloyd, and D.G. Cory, *Phys. Rev. Lett.* **94**, 020502 (2005).
- [53] V. Giovannetti, S. Lloyd, and L. Maccone, *Science* **306**, 1330 (2004).
- [54] D.J. Wineland, J.J. Bollinger, W.M. Itano, and D.J. Heinzen, *Phys. Rev. A* **50**, 67 (1994).
- [55] S.F. Huelga, C. Macchiavello, T. Pellizzari, A.K. Ekert, M.B. Plenio, and J.I. Cirac, *Phys. Rev. Lett.* **79**, 3865 (1997).
- [56] C.A. Sackett, D. Kielpinski, B.E. King, C. Langer, V. Meyer, C.J. Myatt, M. Rowe, Q.A. Turchette, W.M. Itano, D.J. Wineland, and C. Monroe, *Nature* **404**, 256 (2000).
- [57] V. Meyer, M.A. Rowe, D. Kielpinski, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland, *Phys. Rev. Lett.* **86**, 5870 (2001).

Part IV
Quantum Communication

14 Quantum Teleportation

Luciana C. Dávila Romero and Natalia Korolkova

14.1 Introduction

The concept of teleportation can be very different depending on its context. Most generally, teleportation is defined as the transfer of an object by disappearing it from one point in space and reappearing it in another location. Nevertheless, teleportation of a system can also mean the transfer in space of the information that fully characterizes all its properties. With this information, it is then possible to generate a copy of the original object in a different location. Within this context, there is no need to actually transfer the original components of the object, just a true copy of the original suffices. It is this definition that characterizes quantum teleportation. Classical systems can be fully described by measuring all its relevant properties. A common example is a faxing machine, where the information of a document is transferred from one place to another, even though the original document remains in the senders' hands. In the quantum realm information is given by the states of the components of the system, atoms and/or photons. However, these states cannot be determined fully by measurement, since a measurement of physical variable A will cause the state to collapse to one of the eigenstates of the operator $\hat{A}$ linked to such physical quantity. So, is it possible to quantum teleport a quantum state of a particle onto another one? In 1993, Bennett *et al.* [1] first showed that it is possible, provided one does not get any information about such state in the course of the process, i.e., without measurement on the system to be teleported. The nonlocality property of quantum systems, also known as entangled states, is the key that makes quantum teleportation viable. The existence of nonlocal correlation between pairs of particles, known as Einstein–Podolsky–Rosen pairs, or EPR pairs for short [2], facilitates the transfer of information, or more precisely the teleportation of an intact quantum state from one place to another by a sender who knows neither the state to be teleported nor the location of the receiver. Another vital difference between quantum teleportation and the classical example mentioned is that in the quantum case the original state is destroyed so that no violation of the noncloning theorem is incurred [3].

Although we will restrict our discussion to photons, it is necessary to mention that experiments of quantum teleportation have also been successfully achieved for atomic qubits [4,5].

14.1.1 Setting up the problem and the role of entanglement

Consider an observer, Alice, who has a quantum system a in a particular state $|\phi\rangle_a$, unknown to her. She wishes to teleport such a system to a receiver, Bob, by communicating the neces-

sary information which will allow him to make an accurate copy of the system's original state. We assume that it is not possible to directly send the quantum system to Bob, due to losses in the quantum coherence through the available quantum channels between Alice and Bob.

We need to define the quantum system. The simplest case is a spin-1/2 particle, known as a qubit. This is a system within a two-dimensional Hilbert space, where the quantum variables are discrete. A general and unknown pure state of such system can be described as a linear combination of its two possible orthogonal states

$$|\phi\rangle_a = a|\uparrow\rangle_a + b|\downarrow\rangle_a, \quad (14.1)$$

where the normalization condition $|a|^2 + |b|^2 = 1$ is satisfied.

To teleport the information of the quantum state a it is necessary to consider an auxiliary system shared by Alice and Bob. This system is the vehicle with which Alice maps the quantum information to Bob, without reading or even knowing anything about it. The auxiliary system is a composite system of more than one particle, in accordance with the number of recipients. In the case of Alice and Bob it is a two-particle auxiliary system, while for multi-channel teleportation more particles will be present. Initially, its state $|\chi\rangle$ is known, and it is such that the quantum states of its composite particles are intertwined. This specific characteristic of the state $|\chi\rangle$ ensures that, whenever the auxiliary system interacts with the spin-1/2 particle at Alice's station, there is an impact on Bob's share of the auxiliary system. Thus, after such interaction, the auxiliary system is left in an unknown state $|\chi'\rangle$, while the particle a is in a state $|\phi'\rangle_a$. With the state $|\chi'\rangle$ and the use of local operations, Bob can then revert the actions taken in order to prepare a replica of the original state $|\phi\rangle_a$. In summary, for teleportation to be possible, the auxiliary system's initial state must have very particular properties, which are present only in an *entangled* state. It is therefore, necessary to first discuss the importance of entanglement in quantum systems, before proceeding to describe the process of teleportation.

Entanglement is a puzzling property of quantum mechanics and very counterintuitive to our classical preconceptions. Let us consider a composite system. The simplest case would be a two-particle system, b and c , where each particle can be in either of two states, i.e., each one in a qubit. From Eq. (14.1) we can see that the basis which describes a state of the composite system (bc) is

$$|\uparrow\uparrow\rangle_{bc}, |\uparrow\downarrow\rangle_{bc}, |\downarrow\uparrow\rangle_{bc}, |\downarrow\downarrow\rangle_{bc}. \quad (14.2)$$

Any pure state $|\chi\rangle_{bc}$ of the two-qubits system can be expressed as a linear combination of these four states. An interesting property for states of composites systems can emerge. If the states of the two particles are not correlated then the state of the composite system is simply $|\chi\rangle_{bc} \equiv |\phi\rangle_b \otimes |\varphi\rangle_c$. However, not all states of a composite system can be expressed in such way. Let us consider a particular state given by

$$|\chi\rangle_{bc} \equiv |\Psi^-\rangle_{bc} = \frac{1}{\sqrt{2}}[|\uparrow\downarrow\rangle_{bc} - |\downarrow\uparrow\rangle_{bc}]. \quad (14.3)$$

After careful observation we can arrive at the conclusions that such a state can not be expressed as a direct product of a state for each particle. In other words, even if a composite quantum

system is in a given pure state, as in our example, the states of its parts are not necessarily defined. In such a case their states are intertwined, *entangled*, and neither part has a state of its own, i.e., in our example $|\Psi^-\rangle_{bc} \neq |\phi\rangle_b \otimes |\varphi\rangle_c$. Once the state $|\Psi\rangle_{bc}$ is entangled no matter whether the composite parts are physically far apart or not, their states will remain entangled. Quantum state $|\Psi^-\rangle_{bc}$, Eq. (14.3), together with states

$$|\Psi^+\rangle_{bc} = \frac{1}{\sqrt{2}}[|\uparrow\rangle_b |\downarrow\rangle_c + |\downarrow\rangle_b |\uparrow\rangle_c], \quad (14.4)$$

$$|\Phi^\pm\rangle_{bc} = \frac{1}{\sqrt{2}}[|\uparrow\rangle_b |\uparrow\rangle_c \pm |\downarrow\rangle_b |\downarrow\rangle_c], \quad (14.5)$$

is mutually orthogonal quantum states with maximum entanglement. These are called Bell states [6] and form a complete basis set for the quantum system bc , which is an alternative basis to that given in Eq. (14.2). Entangled states demonstrate the nonlocality of quantum mechanics. It is important to stress that even though entangled systems remain correlated when separated at a great distance, no superluminal communication is possible. The correlation is shared by the quantum entangled systems and not by the observers. For the observers to communicate, a classical channel is also needed. See Chapter III for more discussions about entanglement.

14.1.2 A template for quantum teleportation

We here discuss Bennett and co-workers' seminal work on quantum teleportation [1]. The process involves the quantum system, particle a , which we wish to teleport and an EPR pair, particles b and c . It can be seen in Fig. 14.1, that the entangled pair is represented by a crossed loop (dotted line). We have an initial composite quantum system of three particles two of

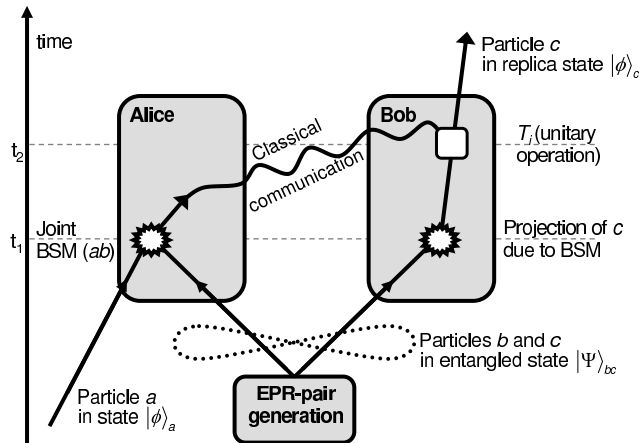


Figure 14.1. Teleportation scheme.

which are entangled. Particle a is in an unknown state $|\phi\rangle_a$ while the EPR pair is in one of the four Bell states (14.3)–(14.5). The state of the system as a whole can be written as

$$\begin{aligned} |\Psi\rangle_{abc} &= |\phi\rangle_a \otimes |\Psi^-\rangle_{bc} \\ &= \frac{a}{\sqrt{2}} [|\uparrow\rangle_a |\uparrow\rangle_b |\downarrow\rangle_c - |\uparrow\rangle_a |\downarrow\rangle_b |\uparrow\rangle_c] \\ &\quad + \frac{b}{\sqrt{2}} [|\downarrow\rangle_a |\uparrow\rangle_b |\downarrow\rangle_c - |\downarrow\rangle_a |\downarrow\rangle_b |\uparrow\rangle_c], \end{aligned} \quad (14.6)$$

where we consider that the system bc is in state $|\Psi^-\rangle_{bc}$. Initially particle a is in Alice hands, and so is one of the EPR particles, say particle b , while the other EPR particle c is given to Bob. Although this gives the possibility of nonclassical correlations between Alice and Bob, the EPR pair has no information about the unknown state $|\phi\rangle_a$. The entire system is a pure product which does not involve classical correlations nor quantum entanglement between the particle to be teleported and the EPR pair (but does have entanglement between b and c). So no measure of one or both of the EPR particles can yield any information about $|\phi\rangle_a$. However, a measurement of the composite system ab , the two particles in Alice's hands, gives us less trivial results. The next step, therefore, is for Alice to couple a and b . To do so, she is asked to perform a complete measurement of the von Neumann type on the joint system ab , in the Bell operator basis $\{|\Psi^-\rangle_{ab}, |\Psi^+\rangle_{ab}, |\Phi^-\rangle_{ab}, |\Phi^+\rangle_{ab}\}$. It can be readily seen that these four states are a complete orthonormal basis for the system ab , so that the state given by Eq. (14.6) can be rewritten in terms of this basis

$$\begin{aligned} |\Psi\rangle_{abc} &= \frac{1}{2} [|\Psi^-\rangle_{ab} (-a|\uparrow\rangle_c - b|\downarrow\rangle_c) + |\Psi^+\rangle_{ab} (-a|\uparrow\rangle_c + b|\downarrow\rangle_c) \\ &\quad + |\Phi^-\rangle_{ab} (a|\downarrow\rangle_c + b|\uparrow\rangle_c) + |\Phi^+\rangle_{ab} (a|\downarrow\rangle_c - b|\uparrow\rangle_c)]. \end{aligned} \quad (14.7)$$

From this expression it can be seen that regardless of the unknown state $|\phi\rangle_a$ the four possible outcomes for Alice's measurement are equally probable, and more importantly as a consequence of this measurement Bob's EPR particle c will have been projected into one of the four pure states superposed in Eq. (14.7), all of which are unitary transformations of the state $|\phi\rangle_c = a|\uparrow\rangle_c + b|\downarrow\rangle_c$. These unitary transformations are simple basis rotations

$$\begin{aligned} \mathbf{T}_1 &= -\mathbf{1}, & \mathbf{T}_2 &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = -\sigma_z, \\ \mathbf{T}_3 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x, & \mathbf{T}_4 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_y. \end{aligned} \quad (14.8)$$

Then the state of the system abc can be expressed as

$$|\Psi\rangle_{abc} = \frac{1}{2} [|\Psi^-\rangle_{ab} \mathbf{T}_1 + |\Psi^+\rangle_{ab} \mathbf{T}_2 + |\Phi^-\rangle_{ab} \mathbf{T}_3 + |\Phi^+\rangle_{ab} \mathbf{T}_4] |\phi\rangle_c.$$

For each of the possible outcomes of Bell measurement Bob's EPR particle is related in a simple way to the state $|\phi\rangle_a$. The only thing remaining for the quantum teleportation to be completed is for Alice to classically communicate the result of her measurement. With this knowledge Bob will know which unitary transformation $\mathbf{T}_i$ he must perform to convert the

state of the EPR particle c into a replica of Alice's original state $|\phi\rangle_a$. It is also possible to choose to identify only one of the four Bell states; in this case teleportation is successfully achieved one out of four times. In all cases the transport of the particle's a state is achieved by two channels, one quantum and the other classical. Each channel by itself carries no information about the original state $|\phi\rangle_a$, the quantum channel by itself is in a completely mixed state and the classical is worthless on its own, since the results of the measurement occur with equal probability independent of $|\phi\rangle_a$. In summary, the unknown state of Alice's particle a is teleported to Bob's location by use of a shared entangled pair. It is important to note that the original state of particle a is destroyed and consequently there is no violation of the noncloning theorem [3].

14.1.3 Efficiency and fidelity

The experimental realization of quantum teleportation is measured in terms of certain features, namely *efficiency* and *fidelity*. The efficiency ε of a particular process concerns its success rate, given an input state. Within Bennett's scheme, 100% efficiency, or $\varepsilon = 1$, is achieved when all four Bell states of particles ab can be uniquely determined by Alice. However, if only one or two of these states are distinguishable, teleportation will still be possible, but with a 25% or 50% efficiency respectively. There are other factors that also determine the success of teleportation, such as the degree of entanglement between the EPR pair, losses within propagation and detection, etc. Each particular experimental setup diverges in one way or the other from ideal conditions, reducing the efficiency of the process even further.

In the ideal scenario and when teleportation is successful, the unknown state which goes into Alice's hands is the same one that emerges in Bob's location. By this we mean that all the information available about the initial quantum system, which reacts in one way or other in a given experimental situation, will be transferred from one party to the other. A third party, who actually knows this information and possibly the person who prepared the initial quantum state should be able to verify the accuracy of the quantum communication. However, in less than ideal conditions such as in any experiment, the input and output states will differ. Even if the particular input state is pure, $|\phi\rangle_{\text{in}}$, it is likely that the outcome will be represented by a mixed state density operator, $\hat{\rho}_{\text{out}}$. The fidelity F of a particular process is a measure of their similarity and is simply given by their overlap, $F = {}_{\text{in}}\langle\phi|\hat{\rho}_{\text{out}}|\phi\rangle_{\text{in}}$. This measure satisfies

$$F = \begin{cases} 1 \Leftrightarrow \hat{\rho}_{\text{out}} = |\phi\rangle_{\text{in}} {}_{\text{in}}\langle\phi|, \\ 0 \Leftrightarrow \text{the two states are orthogonal.} \end{cases} \quad (14.9)$$

The fidelity provides a way of quantifying the extent to which the result of measuring any observable on the input state corresponds to performing such measurement on the output state. It must be emphasized that this gives information for any observable, and not one in particular. By classical channel alone it is possible to reach a fidelity of $\frac{1}{2}$, any value that exceeds this must therefore involve some sort of entanglement and consequently quantum communication [7, 8]. Furthermore, if the process needs to ensure that neither Alice or Bob have in some way acquired information which would allow them to second guess the possible state of particle a , then the fidelity for a single qubit must be over $F = \frac{2}{3}$ (for a comprehensive explanation

see [7]). This will ensure that the output state c is a result of true quantum teleportation. Also, having fidelity of $F = \frac{2}{3}$ or over ensures that Bob holds the best copy of the original quantum state, guaranteeing that any copy produced by a third party will have less fidelity [8, 9].

14.2 Experimental Realization

To experimentally achieve teleportation of a quantum state, several steps must be followed. These present practical challenges that need to be addressed in order to successfully realize the process. Within these steps we have

- Generation of particle a state.
- Generation of the auxiliary system, the EPR pair.
- Bell state measurement (BSM).
- Verification that the quantum teleportation is successful.

Second and third points are particularly complicated. In the ideal case, teleportation occurs when the unknown state going out is the same as the one going in. Therefore, it is important to establish what parameters an ideal quantum teleportation experiment should satisfy [7]:

- Particle's a initial state, the input state, should be arbitrary and unknown to both Alice and Bob. A third party, Victor, should supply such state.
- The output quantum state, particle's c final state, must be an instantaneous copy of the input state.
- The BSM must be able to distinguish the complete set of the orthogonal Bell states, which ensures 100% ideal efficiency. This is known as unconditional teleportation. A less strict condition would be conditional teleportation.
- For any given input state teleportation should be deterministic and not probabilistic.
- The amount of information broadcast over the classical channel should be much smaller than the information required to specify the unknown states.
- Alice and Bob should not have to know each other's location to carry the process through to completion.

These goals may vary depending on the particular application of the original protocol. They are set for the ideal case and are not always easily translated into the laboratory, experiments being able to address some of them better than others. Since Bennett *et al.* proposal, several research teams have pursued the idea of quantum teleportation, with varied success. Here, we review three such experiments, each with its own characteristics. First, we consider the experiment performed by Bouwmeester *et al.* [10], one of the first ones to successfully achieve teleportation. Then we discuss Shih *et al.* [11] experiment which has the best unconditional fidelity. Lastly, we review the long-distance teleportation experiment performed by Zeilinger and co-workers [12].

14.2.1 The first quantum teleportation experiment

The experiment of Bouwmeester *et al.* [10] involves the successful teleportation of the state of a photon a in an unknown $|\phi^{(\lambda)}\rangle_a$ polarization λ state, i.e., an unknown superposition of the vertically and horizontally polarized state. The state is completely unknown, and furthermore it is undefined, due to the fact that particle a is a part of a EPR pair (source 1). Its EPR partner a' serves as a marker indicating whether a is emitted or not (if this EPR pair is generated by a type-II crystal, then a' is in $|\phi^{(\lambda')}\rangle_{a'}$ state, orthogonal to $|\phi^{(\lambda)}\rangle_a$).

Here, an outline of the experiment is given; more detail of its setup can be found in the original paper [10]. The auxiliary entangled pair bc is a pair of photons generated by the type-II parametric down-conversion nonlinear optical process (source 2). In such a process a photon interacting with a nonlinear crystal can decay into two photon which are in state (14.3). Alice's BSM measurement is performed by linear interactions alone. In this method only one particular Bell state can be discriminated, giving only 25% absolute efficiency. When successful, the photons ab are projected onto $|\Psi^-\rangle_{ab}$, making them entangled. This is achieved by superposing the two photons at a 50/50 beam splitter (BS) and locating two detectors at each of its outputs, f_1 and f_2 respectively, see Fig. 14.2. It can be shown that the photons are projected into the Bell state $|\Psi^-\rangle_{ab}$ whenever simultaneous detections in f_1 and f_2 are registered (coincidences). Teleportation, which occurs simultaneously as a coincidence is detected, results in photon c being projected in the same polarization state as the initial state of photon a , as is shown from Eq. (14.7). Verification of the process is carried out by passing photon c through a polarizing beam splitter which selected σ' and σ polarizations, with detectors d_1 and d_2 in each output. Then recording a three-fold coincidence $d_2 f_1 f_2$ (σ analysis) together with the absence of a three-fold coincidence $d_1 f_1 f_2$ (σ' analysis) is a proof that the polarization of photon a has been teleported to photon c .

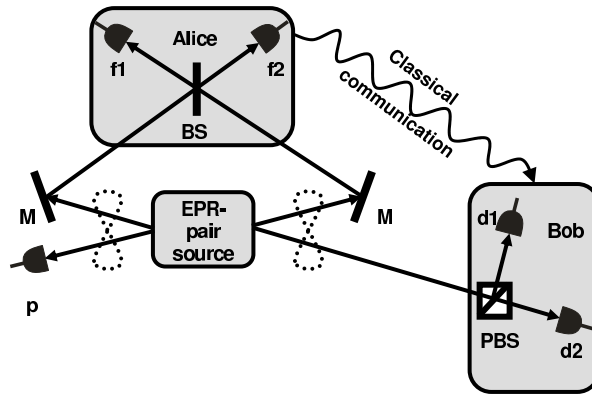


Figure 14.2. Bouwmeester *et al.* experimental setup [10]. BS: beam splitter; PBS: polarization beam splitter, M: mirror; f1,f2,d1,d2,p: detectors.

Certain conditions need to be addressed in order to ensure that teleportation has indeed taken place.

- Photons ab are generated in such a manner that they cannot be distinguished by their arrival time at the beam splitter.
- The experiment is first carried out for a known linear polarization basis ($\lambda = \pm 45^\circ$) which is not in the preferred direction to the set-up. Then, quantum teleportation is performed on a superposition of such states, such as circularly polarization. This guarantees that any unknown quantum state can be teleported.
- To ensure a positive result of teleportation, the polarization of photon c is verified by analyzing it with detectors $d1$ and $d2$. However this destroys the state of c .
- There is the possibility of three-fold coincidences when no teleportation has occurred. This is due to a two-pair down conversion on source 2 while no photon a is absent. These spurious three-fold coincidences can be excluded by conditioning to the detection of photon a' , which effectively projects photon a onto a single particle state.

This first teleportation experiment satisfied some of the ideal characteristics, outlined at the beginning of this section, such as the arbitrariness and lack of knowledge of the state to be teleported and the output being an instantaneous copy of the input state. However, other criteria are not met. Most importantly, this experiment is not an unconditional teleportation. Furthermore, the teleported state is destroyed in the last verification step. Also Braunstein *et al.* [13, 14] raised the question that due to the nature of the experimental process, not always a teleported photon is observed conditioned on a coincidence recording. This affects the fidelity to a level where identical results could be obtained by classical channels. Nevertheless, the experiment is the first of its kind and it significantly demonstrates the feasibility of quantum teleportation.

14.2.2 Further experiments

Since 1997, when Bouwmeester *et al.* first succeeded in carrying out Bennett's scheme, several experiments have been developed, in pursue of satisfying ideal conditions. It is not the aim here to review each one of these cases, a task which goes beyond the scope of this chapter. Nevertheless, here we briefly outline two particular experiments, each of which successfully ensures one of the ideal clauses, namely, unconditionality and long-distance teleportation.

In 2001 Shih's team reported a quantum teleportation experiment [11], where a complete Bell state measurement was achieved, i.e., unconditional teleportation. Following Bennett's scheme, this quantum teleportation experiment resolves the problem of accurately discriminating between all four Bell states by basing the BSM analyzer on a nonlinear optical process known as sum frequency generation (SFG). Photons a and b paths are intercepted by four (two type-I and two type-II) nonlinear crystals which generate a higher frequency photon d . The crystals are positioned in a particular arrangement which, together with the aid of four detectors allow for all four states, $|\Phi^-\rangle_{ab}$, $|\Phi^+\rangle_{ab}$, $|\Psi^-\rangle_{ab}$ and $|\Psi^+\rangle_{ab}$ to be distinguished resulting in an efficiency $\varepsilon = 1$ when no other losses are taken into account. The rest of the scheme is unchanged. Alice is always able to pass the BSM analyzer outcome via a classical channel to

Bob, who therefore can perform the necessary unitary transformation to the state of particle c and the teleportation of the input state is then accomplished. In this case, to ensure that quantum teleportation has taken place, the joint detection rates between Alice's four detectors and Bob's two detectors are measured, resulting in a fidelity of $F \approx 0.83$ [11].

Another achievement into the ultimate goal of practical quantum communication was accomplished in 2004 by the Vienna group led by Zeilinger [12]. In this “real-world experiment” the aim is to realize teleportation at distances beyond those given in a lab and over standard telecommunication links, i.e., where Alice and Bob are effectively at different locations and not just at two different parts of the optical table. Based on Bennett's protocol, the process requires a quantum teleportation channel which allows Alice and Bob to share the auxiliary EPR pair of photons bc . This involved the use of an 800 m optical fiber installed in a public sewer running underneath the river Danube. For simplicity, only linear interactions are used in the BSM analyzer and therefore only two Bell states can be identifiable [15]. The rest of the setup is fairly conventional, a microwave channel is used for classical communications and Bob uses a fast electro-optical modulator to perform the necessary unitary transformations T_i corresponding to the two identifiable Bell states. The optical fiber reduces the velocity of the EPR photon c by a fraction of $\frac{2}{3}$, a time delay which ensures a successful operation since it allows the receiver to set the adequate unitary transformation. With this setup high-fidelity teleportation over a distance of 600 m can be ensured, reaching fidelity values above 0.85 for different polarization states.

14.3 Continuous Variables—Concept and Extension

In the previous sections, attention has been on the teleportation of systems within a two-dimensional Hilbert space, i.e., photons with two possible polarization states. In these schemes the entangled state involves a pair of spin- $\frac{1}{2}$ particles in a Bell state, (14.3)–(14.5). It would be easy to conclude that quantum teleportation beyond the dichotomic problem would be complicated, due to the difficulty in measuring, or even accurately defining, entanglement in such systems. This is true for systems described by discrete variables, within a $n > 2$ -dimensional Hilbert space. However, in the work done by Vaidman [16] and later extended by Braunstein *et al.* [17] it was shown that it is possible to achieve quantum teleportations in systems characterized by continuous variables corresponding to states of infinite-dimensional systems such as optical fields or the motion of massive particles. Vaidman showed that teleportation is feasible for the wavefunction of a one-dimensional particle where the EPR pair shared by Alice and Bob has perfect correlation in position and momentum [16]. Braunstein *et al.* [17] later extended these results, demonstrating that teleportation can also be accomplished with finite degree of correlation among the relevant particles.

Quantum teleportation over continuous variables in general represents an alternative approach to quantum communication using electromagnetic modes of light or atomic ensembles, as opposed to single photons and atoms in more conventional quantum information processing. As already mentioned, in this latter approach, which uses the discrete quantum states, nonlinear interactions are needed to perform the complete BSM or for the realization of quantum logic. This represents a substantial experimental challenge, and as a result of this, unconditional quantum teleportation was achieved first in the continuous variable regime in 1998

based on the proposal by Braunstein *et al.* [17]. It was not until 2000 that unconditional discrete variable (DV) teleportation involving nonlinear elements for BSM was realized [11], 7 years after the underlying theoretical proposal of Bennett *et al.* [1]. However, despite its experimental advantages and its higher efficiency, CV information processing is restricted in maximal achievable degree of entanglement. CV entanglement is deterministic, but maximal entanglement would need infinite energy resources, which is in contrast to readily available—but probabilistic—maximal DV entanglement. Lower degrees of entanglement result in lower teleportation fidelity. The first continuous variable quantum teleportation of a coherent state has been implemented at Caltech [18] with a fidelity of $F \approx 0.58$ and repeated later by the same group [19] and the ANU group [20] with an increased fidelity of $F \approx 0.63$. In 2005, Takei *et al.* [21] reported the first CV unity-gain teleportation of entangled state (entanglement swapping) and the first teleportation of coherent state with fidelity over the noncloning limit, $F \approx 0.70 > 2/3$. This value is still lower than the fidelity of the unconditional DV experiment, $F \approx 0.83$ [11].

In summary, in the continuous variable realm, the possibility of performing Bell-state-like measurements and quantum logic operations using just linear transforms, e.g., beam splitters and phase shifters, provides an elegant and simple method to extend the conventional teleportation scheme on a single-photon basis [1] to the case of continuous variables [17]. The scheme for CV quantum teleportation is represented in see Fig. 14.3. The Bell-state measurement at Alice's station is accomplished by mixing the incoming unknown state to be teleported with one of the entangled beams on a beam splitter and consequently measuring the two conjugate field amplitudes (quadrature-phase amplitudes) in two different output beams. The resulting photocurrents of these two homodyne detections are transmitted to Bob via classical channels. Bob uses this classical information to extract the copy of the original state from his part of the EPR beam. The operation equivalent to the unitary transformation in single-photon case is the mapping of the result of the Bell measurement on Bob's EPR beam via amplitude and phase modulation. Let us describe this teleportation process in the Heisenberg picture by first introducing the pair of continuous variables of the electric field (x, p) , called the quadrature-phase amplitudes, which describe the infinite-dimensional state of the optical fields. These variables are analogous to the canonically conjugate variables of position and momentum of a massive particle. The EPR beams have nonlocal correlations similar to those first described by Einstein *et al.* [2]. Thus, for the combined mode bc , perfect entanglement is exhibited in the limit case of

$$\hat{x}_b - \hat{x}_c \rightarrow 0, \quad \hat{p}_b + \hat{p}_c \rightarrow 0. \quad (14.10)$$

More on CV entanglement can be found in the original papers of Drummond and Reid [22] and in the recent review on quantum information with continuous variables [23].

Alice wants to teleport an unknown input mode described by a pair of variables $(\hat{x}_a, \hat{p}_a)$. Alice and Bob share a continuous variable EPR pair bc with the entangled mode $(\hat{x}_b, \hat{p}_b)$ and $(\hat{x}_c, \hat{p}_c)$ respectively. As a next step, Alice performs the Bell measurement on the mode to be teleported and on her part of the EPR beam. As already mentioned, this is done by combining them on a 50/50 beam splitter and performing $\hat{x}$ -measurement in one output and $\hat{p}$ -measurement in the other, which delivers the following results (for the quantum description

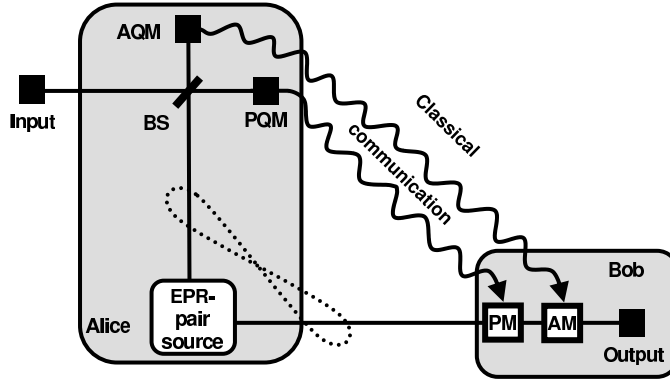


Figure 14.3. Teleportation scheme for continuous variables. AQM/PQM: amplitude/phase quadrature measurement; AM/PM: amplitude/phase modulation.

of the beam splitter transformations, see [24]):

$$\hat{x}_1 = \frac{1}{\sqrt{2}}(\hat{x}_a - \hat{x}_b), \quad \hat{p}_2 = \frac{1}{\sqrt{2}}(\hat{p}_a + \hat{p}_b). \quad (14.11)$$

The measured values (x_1, p_2) for $(\hat{x}_1, \hat{p}_2)$ represent the classical information corresponding to the Bell measurement result in the discrete variable case and are transmitted to Bob via the classical channel. At this stage, a particular feature of the continuous variable teleportation can come into play: the classical photocurrents corresponding to (x_1, p_2) can be electronically scaled at will introducing an electronic gain g_x, g_p for each of the variables (amplification or de-amplification of the signal), which can improve the fidelity of teleportation. However, using the nonunity gain means a restriction in the type of quantum state to be teleported, a teleporter of an *arbitrary* unknown state should always have its gains set to unity [21, 25].

Before the Bell measurement is performed by Alice, Bob's initial mode $(\hat{x}_c, \hat{p}_c)$ can be represented in terms of the original mode $(\hat{x}_a, \hat{p}_a)$, the EPR pair $(\hat{x}_b - \hat{x}_c, \hat{p}_b + \hat{p}_c)$, and the results of the Bell measurement (14.11) (the mode remains unchanged; it is only formally rewritten):

$$\hat{x}_c = \hat{x}_a - (\hat{x}_b - \hat{x}_c) - \sqrt{2}\hat{x}_1, \quad \hat{p}_c = \hat{p}_a + (\hat{p}_b + \hat{p}_c) - \sqrt{2}\hat{p}_2 \quad (14.12)$$

(see also [18, 21]). On receiving the measurement results of Alice $(\hat{x}_1, \hat{p}_2)$, Bob performs the following displacement of his mode:

$$\hat{x}_c \rightarrow \hat{x}_{\text{out}} = \hat{x}_c + \sqrt{2}g_x\hat{x}_1, \quad \hat{p}_c \rightarrow \hat{p}_{\text{out}} = \hat{p}_c + \sqrt{2}g_p\hat{p}_2. \quad (14.13)$$

The mapping of the Bell measurement results onto Bob's mode is performed by driving the amplitude and phase modulators, placed in Bob's mode, with photocurrents (x_1, p_2) applying electronic gains g_x, g_p . This last step accomplishes the teleportation process and (for unity gain) the output mode becomes:

$$\hat{x}_{\text{out}} = \hat{x}_a - (\hat{x}_b - \hat{x}_c), \quad \hat{p}_{\text{out}} = \hat{p}_a + (\hat{p}_b + \hat{p}_c), \quad (14.14)$$

which in the ideal case of perfect EPR correlations (14.10) provides Bob with a perfect copy of the initial state, $\hat{x}_{\text{out}} \rightarrow \hat{x}_a, \hat{p}_{\text{out}} \rightarrow \hat{p}_a$. In real situations, where unperfect CV entanglement is present, the teleported state has additional fluctuations which reduce the fidelity and, in the case of nonunity gains, requires some additional measures to quantify the quality of teleportation.

Details of the experimental scheme depend on the nature of the used EPR source. In the Caltech group experiments [18, 19] and in the experiment by Takei *et al.* [21], the entangled state shared by Alice and Bob is a highly squeezed¹ two-mode state of the electromagnetic field, with quadrature amplitudes of the field playing the roles of position and momentum. For the Bell measurement, Alice uses two homodyne detectors, $D_{x,p}$, including two local oscillators $LO_{x,p}$.

In the case where a two-mode squeezed vacuum is used as an EPR source, one has to use an auxiliary beam on which the modulation with the results of the Bell measurement is achieved (or two beams, to avoid mixing of amplitude and phase modulations). Bob's mode ($\hat{x}_c, \hat{p}_c$) is then combined with the modulated beam(s) on a highly transmissive (for Bob's mode) mirror, a 99/1 beam splitter. This results in an appropriate displacement in the phase space so that Bob's mode becomes a copy of the original state [18, 19, 21].

For intense entangled beams, this scheme may be simplified. In the first proposal along these lines by Ralph and Lam [27], two intense squeezed continuous wave beams interfere at a beam splitter to produce nonlocal quantum correlations. In this scheme, one of the interfering beams is required to be substantially more intense than the other. The use of bright beams allows one to simplify the inverse Bell-state-like measurement at Bob's side: the amplitude and phase fluctuations from the photocurrents are mapped by Bob directly onto the second EPR beam (Fig. 14.3). The continuous teleportation scheme of Leuchs *et al.* [28] is essentially the same as that reported by [27], the difference being that the entangled beams are bright optical pulses of the same intensity and with a more complicated spectral structure. The use of the EPR beams of the same average power allows for a particularly simple detection scheme for teleportation: the amplitude and phase quadrature detectors with local oscillators [18, 19, 21, 27] are now replaced by standard direct amplitude detectors in both outputs of Alice's beam splitter thus avoiding the cumbersome local oscillator techniques.

The characterization of the quality of the CV quantum teleportation in terms of fidelity is essentially the same as already described in subsection (14.1.3). The important point here is the choice of gain, the issue which is specific to CV teleportation. The choice of nonunity gain can partially compensate for the additional fluctuations in the teleported state emerging from the unperfect EPR entanglement ($\hat{x}_b - \hat{x}_c \neq 0, \hat{p}_b + \hat{p}_c \neq 0$) by an appropriate rescaling of the output state in the phase space. Hence in some cases the best fidelity of teleportation is achieved by using optimal, nonunity gains [20, 25, 29]. However, this optimization is state specific, i.e., such a teleporter is optimal only for a particular class of the input states and the improved fidelity is calculated only for this particular class of states. The general goal, however, is to teleport an unknown *arbitrary* quantum state. To characterize teleportation of an arbitrary state, the fidelity is averaged over the whole phase space [30]. When using nonunity gains, the displacement of the teleported state does not match the original displacement of

¹By squeezed or squeezing it is meant reduction of quantum uncertainty in one of the conjugate variables at the cost of an increase in the other variable [26].

the input state and the fidelity calculated over the whole phase space goes to zero. Thus, teleportation of an arbitrary state requires the gains in the classical channel to be set to unity [21, 30].

Nevertheless, the optimal quantum teleportation of a particular class of input quantum states is of interest and can find its own applications. Such teleportation schemes providing optimal transfer of quantum information for nonunity gains were termed by Bowen *et al.* [25] *nonunity gain teleportation* as opposed to *unity gain teleportation*, delivering output states identical to input ones (with some noise added). For nonunity gain teleportation, fidelity does no longer provide satisfactory measure of teleportation quality [25]. The emphasis here lies not on producing an exact copy of the original state, but on optimal transfer of quantum information contained in quantum uncertainties of the input state. This leads to introducing new measures [25, 27, 31, 32], borrowed from traditional quantum optics, in particular using concepts of information transfer in quantum nondemolition measurements (QND) [33]. Following three figures of merit were suggested to quantify CV teleportation in a wider context of optimal quantum information transfer:

- *Fidelity* [7, 8, 17]. It is a decisive measure to characterize quantum teleportation of an arbitrary unknown state in a sense of producing the best distant copy of the original state.
- *$T - V$ diagram* [25, 27, 31, 32]. The measure takes more exact account of transfer of quantum information contained in quantum uncertainties of the original state. It uses the signal transfer coefficients T_q and conditional variance product V_q between the input and output states. These quantities have been originally introduced in the context of QND measurements [33]. Signal transfer coefficient is defined as a relation between signal-to-noise ratios (SNR) between output and input states. It characterizes how good the original signal is transferred to the output and is directly linked to the teleportation gain. Conditional variance characterizes the quantum correlations between input and output states and is a measure of the noise introduced during the protocol. Transfer coefficients and conditional variances are then calculated for both conjugate variables and are combined in a certain manner to deliver figures of merit T_q and V_q , which build up the $T - V$ diagram. Interpretation of the results is then similar to analyzing the QND measurement. Surpassing the $T_q = 1$ limit means that Bob has got over the half of the signal from Alice and thus have more information on the input state than any third party. Surpassing the $V_q = 1$ limit is required for the reconstruction of nonclassical features of the input state (squeezing, entanglement, etc). For unity gains, $T_q = V_q = 1$ means surpassing the teleportation noncloning limit $F = 2/3$. The $T - V$ graph is two dimensional and conveys more information about the teleportation process than fidelity. For more details of the $T - V$ diagram analysis, see [25, 27, 31, 32].
- *Gain normalized conditional variance product* [25]. This measure was specially designed to provide a single number as figure of merit for nonunity gain teleportation (such as fidelity is a single number characterizing unity gain teleportation). It is directly related to the $T - V$ characterization above.

There are several advantages of using continuous variable systems for quantum communication: (i) firstly, CV will allow the integration of quantum teleportations into the communication technology arena; (ii) these methods can also be applied to other quantum computational

protocols, such as quantum error correction for CV and superdense coding in optical information; (iii) lastly simple communication schemes with CV can be implemented where only linear operations are considered for BSM; therefore there is no need for nonlinear interactions beyond the generation of the EPR pair.

References

- [1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Pries, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and EPR channels*, Phys. Rev. Lett. **70**, 1895–1899, 1993.
- [2] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev. **47**, 777–780, 1935.
- [3] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299**, 802–803, 1982.
- [4] M. Riebe, H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James, and R. Blatt, *Deterministic quantum teleportation with atoms*, Nature **429**, 734–737, 2004.
- [5] M. D. Barrett, J. Chlaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer D. Leibfried, R. Ozeri, and D. J. Wineland, *Deterministic quantum teleportation of atomic qubits*, Nature **429**, 737–739, 2004.
- [6] D. Bohm, *Quantum Theory* Prentice-Hall, Englewood Cliffs, NJ, USA, Chapter 22, pp 611–623, 1951.
- [7] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble, *Criteria for continuous-variable quantum teleportation*, J. Mod. Opt. **47**, 267–278, 2000.
- [8] S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock, *Quantum versus classical domains for teleportation with continuous variables*, Phys. Rev. A **64**, 022321, 2001.
- [9] F. Grosshans and P. Grangier, *Quantum cloning and teleportation criteria for continuous quantum variables*, Phys. Rev. A **64**, 010301, 2001.
- [10] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Experimental quantum teleportation*, Nature **390**, 575–579, 1997.
- [11] Y.-H. Kim, S. P. Kulik, and Y. Shih *Quantum teleportation of a polarisation state with a complete Bell state measurement*, Phys. Rev. Lett. **86**, 1370–1373, 2001.
- [12] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger, *Quantum teleportation across the Danube*, Nature **430**, 849, 2004.
- [13] S. L. Braunstein and H. J. Kimble, *A posteriori teleportation*, Nature **840**, 840–841, 1998.
- [14] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, M. Zukowski, and A. Zeilinger, *Reply to A posteriori teleportation*, Nature **840**, 841, 1998.
- [15] S. L. Braunstein and A. Mann. *Measurement of the Bell operator and quantum teleportation*, Phys. Rev. A **51**, R1727–R1730, 1995.
- [16] L. Vaidman, *Teleportation of quantum states*, Phys. Rev. A **49**, 1473–1476, 1994.
- [17] S. L. Braunstein and H. J. Kimble, *Teleportation of continuous quantum variables*, Phys. Rev. Lett. **80**, 869–872, 1998.

- [18] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs H. J. Kimble, and E. S. Polzik *Unconditional quantum teleportation*, Science **282**, 706–709, 1998.
- [19] T. Z. Zhang, K. W. Goh, C. W. Chou, P. Ladahl, and H. J. Kimble *Quantum teleportation of light*, Phys. Rev. A **67**, 033802, 2003.
- [20] W. P. Bowen, N. Treps, B. C. Buchler, R. Schnabel, T. C. Ralph, H.-A. Bachor, T. Symul, and P. K. Lam *Experimental investigation of continuous-variable quantum teleportation*, Phys. Rev. A, **67**, 032303, 2003.
- [21] N. Takei, H. Yonezawa, T. Aoki, and A. Furusawa *High-fidelity teleportation beyond the no-cloning limit and entanglement swapping for continuous variables*, Phys. Rev. Lett. **94**, 220502, 2005.
- [22] M. D. Reid and P. D. Drummond, *Quantum correlations of phase in nondegenerate parametric oscillation*, Phys. Rev. Lett. **60**, 2731–2733, 1988.
M. D. Reid, *Demonstration of the Einstein–Podolsky–Rosen paradox using nondegenerate parametric amplification*, Phys. Rev. A **40**, 913–923, 1989.
- [23] S. L. Braunstein and P. van Loock, *Quantum information with continuous variables*, Rev. Mod. Phys. **77**, 513–577, 2005.
S. L. Braunstein and A. K. Pati (eds.), *Quantum information with continuous variables*, Kluwer, Dordrecht, The Netherlands, 2003.
- [24] U. Leonhardt. *Quantum physics of simple optical instruments*, Rep. Prog. Phys. **66**, 1207–1249, 2003.
- [25] W. P. Bowen, N. Treps, B. C. Buchler, R. Schnabel, T. Symul, T. C. Ralph, and P. K. Lam, *Unity gain and non-unity gain quantum teleportation*, IEEE J. Sel. Top. Quantum Electron. **9**, 1519–1532, 2003; Preprint quant-ph/0303179.
- [26] R. Loudon, *The Quantum Theory of Light* 3rd ed. Oxford Science Publications, Oxford, UK, 2001.
- [27] T. C. Ralph and P. K. Lam, *Teleportation with bright squeezed light*, Phys. Rev. Lett. **81**, 5668–5671, 1998.
- [28] G. Leuchs, T. C. Ralph, C. Silberhorn, and N. Korolkova, *Scheme for the generation of entangled solitons for quantum communication*, J. Mod. Opt. **46**, 1927–1939, 1999.
- [29] X. Jia, X. Su, Q. Pan, J. Gao, C. Xie, and K. Peng, *Experimental demonstration of unconditional entanglement swapping for continuous variables*, Phys. Rev. Lett. **93**, 250503, 2004.
- [30] P. van Loock, S. L. Braunstein, and H. J. Kimble, *Broadband teleportation*, Phys. Rev. A **62**, 022309, 2000.
- [31] T. C. Ralph, P. K. Lam, and R. E. S. Polkinghorne, *Characterizing teleportation in optics*, J. Opt. B-Quantum Semiclass. Opt. **1**, 483–489, 1999
- [32] T. C. Ralph, *Teleportation criteria: form and significance Lecture Notes in Physics: Directions in Quantum Optics*, Springer, Berlin, 2001; Preprint quant-ph/0004093.
- [33] J.-Ph. Poizat, J. F. Roch, and P. Grangier, *Characterization of quantum non-demolition measurements in optics*, Ann. Phys. **19**, 265–297, 1994.
P. Grangier, J. A. Levenson, and J.-Ph. Poizat, *Quantum-non-demolition measurements in optics*, Nature **396**, 537, 1998.

15 Theory of Quantum Key Distribution (QKD)

Norbert Lütkenhaus

15.1 Introduction

There are several communication tasks in which two parties would like to protect their communication against third party interference. One of them is secret communication, where the two parties would like to assure that no other party can gain some knowledge about the messages they exchange. Another task, for instance, is the problem of authenticating a message, i.e., to enable a receiver of a message to verify that it indeed comes from the alleged sender in its exact form. Typically, a secret key is used up in the communication process, so one has to find a way to distribute secret keys. It turns out that this task cannot be achieved in a communication scenario that can be described purely by classical communication without making additional assumptions. However, by resorting to communication that makes explicit use of a quantum mechanical signal structure, it is possible to construct a scheme, called quantum key distribution (QKD), that continuously generates fresh secret key, once it is started.

In this chapter we will see how to construct QKD protocols. We show that these schemes can be made robust against noise in the quantum channels, thereby opening the path for practical implementations.

15.2 Classical Background to QKD

Today's security of (classical) key distribution, and as well that of secure communication, is based on the practical unfeasibility of decoding encrypted messages by unauthorized parties. In the case of public key cryptography, the secrecy is based on the experience that the factorization of large numbers requires computational resources growing exponentially with the length of the considered number. For symmetric block ciphers, such as DES or AES, which uses relatively short secret keys shared by two parties, the security is based on the lack of structure in the encoding and decoding operation. Note that the security is not proven, but is based on failed attempts to break these scheme so far. That might change with the discovery of new classical algorithms, or in the case of public key cryptography, with the advent of quantum computers. Therefore, we are aiming at a key distribution scheme that is provable secure, and therefore secure against future technological advances.

As a motivation to the use of QKD, we analyze the only classical protocol for secure communication that can actually be *proven* to be secure without additional assumptions: the one-time pad, also called Vernam cipher [23]. The rules for this protocol are easy. Consider

a set of messages, M , represented by binary strings of length n . Alice wants to send the message $m \in M$ to Bob. Alice and Bob share a secret key k to start with, that is, a random binary sequence of the same length n . Then they execute the following steps:

1. Alice computes the cipher text c as $c = m \oplus k$. Here $\oplus$ refers to the bitwise addition modulo 2, which corresponds to the bitwise XOR of the two bit strings.
2. Alice sends the cipher text c over a public channel to Bob.
3. Bob calculates the XOR between the cipher text c and the key k and recovers the message m as $c \oplus k = m \oplus k \oplus k = m$.

Note that it is essential to use each key k only once, hence the name one-time-pad, otherwise correlations might reveal information on the messages. For example, consider the simplest possible scenario: Alice wants to send two bits secretly to Bob, but they share only one bit of secret key. So Alice encrypts both message bits as cryptograms $c_1 = m_1 \oplus k$ and $c_2 = m_2 \oplus k$ and sends them over the public channel to Bob, who then decodes them. Now anyone overhearing the public channel know the values c_1 and c_2 . Now, by computing the XOR of the cipher texts $c_1 \oplus c_2 = m_1 \oplus m_2$ it is possible to learn the parity of the two message bits. So two of the possible message combinations can be ruled out.

15.3 Ideal QKD

The one-time pad essentially shifts the problem from secret communication to the problem of distributing secret random key. This is an essential step, as in creating keys one can now use random processes. Moreover, one can now use schemes that can reject keys that cannot be guaranteed to be secret without compromising the secret message itself.

So how does the distribution of a key work, and what role does quantum mechanics play in this? The crucial observation is the following: if an eavesdropper, traditionally called Eve, attempts to obtain information about signals passing through a quantum channel, she needs to perform a quantum mechanical measurement. In general, such a measurement has a back-reaction on the signals that disturbs them. Alice and Bob can now search for traces of this disturbance. The absence of the disturbance assures them that no eavesdropping activity took place, and they can use the signals to generate a secret key. If they find a disturbance, they abort the attempt, and start over again. This is an idealized view, and we will refine it later. In order for the basic idea to work, we need to use signals that are represented by non-orthogonal quantum mechanical states. This is so since classical messages can be represented by an orthogonal set of quantum mechanical signals.

We will now present a first protocol that performs QKD, the so-called BB84 protocol. It is due to Bennett and Brassard [4] while its idea goes back to Wiesner [27]. The basic tools are a quantum channel connecting Alice and Bob and a public classical channel, where Eve can listen to the classical communication, but she cannot change the signals. The implications of this will be discussed later. For the quantum channel, we use four signal states, and we will think for now about signals realized as single photons in the polarization degree of freedom, so that we have qubits. Consider two sets of orthogonal signals, one formed by a horizontal and a vertical polarized photon, and the other formed by a $+45^\circ$ and -45° polarized photon.

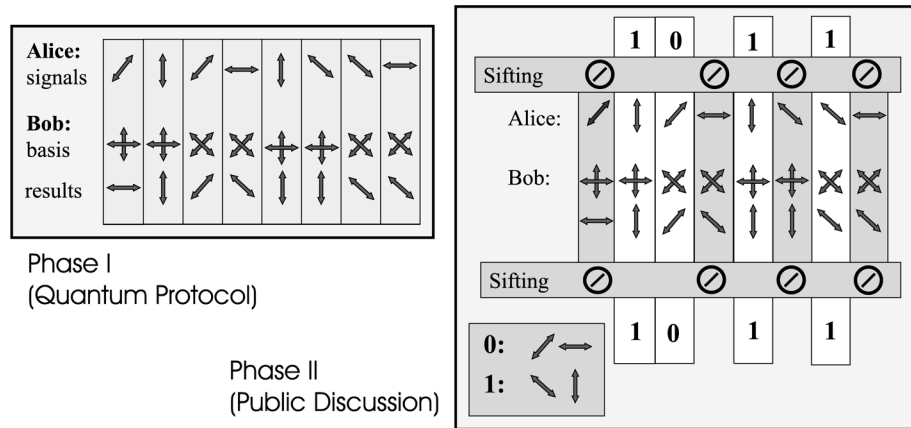


Figure 15.1. The two phases of the BB84 protocol

These four signal states are non-orthogonal, as the overlap probability between signals from different sets is just one half. Bob has two measurement devices at his hand, one in the horizontal/vertical polarization, the other in the $\pm 45^\circ$ basis. Both measurement do not commute, as required.

With these tools, we can execute the following protocol: (See Fig. 15.1.)

1. Phase I (Quantum Protocol)
 - (a) Alice sends a random sequence of n signals to Bob.
 - (b) Bob selects for each signal at random the polarization basis to measure it, and performs that measurement.
 - (c) Bob confirms that he received and measured all signals.
2. Phase II (Public Discussion Protocol)
 - (a) Alice announces the polarization basis for each signal, Bob announces the polarization basis of each measurement he performed. Both discard all events where these bases do not agree.
 - (b) Alice reveals a fraction p of all remaining events in random positions and transmits the positions and the corresponding signals to Bob. Bob compares the signals with his measurement outcomes and tells Alice whether the signals agree with his measurement results.
 - (c) In case of agreement, Alice and Bob translate their signals and measurement results to binary digits, e.g. by calling all horizontal and $+45^\circ$ signals a '0', and the other signals a '1' and use the resulting binary string as secret key.

The first phase of the protocol utilizes the signals and measurements via the quantum channel. Alice then has a classical record of the signal states she sent, Bob has a classical record of the measurement devices he has chosen together with the measurement results he obtained.

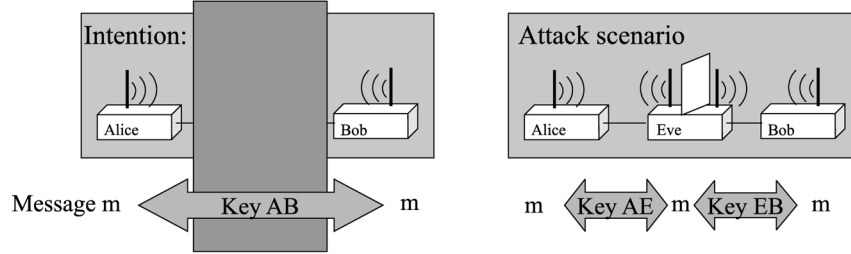


Figure 15.2. Without authentication of the classical channel, no secure QKD is possible as Eve might impersonate the legitimate partners.

In the second phase, Alice and Bob use their public channel to discuss their data. We find two classes of data: those where Bob's measurement outcome is deterministic, since he applied the polarization measurement that matches the polarization basis of the signal, and those signals where the two bases do not match. By opening up their respective basis used in preparation and measurement and discarding those events where the bases do not match, they retain only the deterministic events. This procedure is referred to as *sifting*. Next, they test whether the retained events are indeed perfectly correlated. In the presence of an eavesdropper we know that the signals will be changed on average, so at least some of the input signals will no longer be represented by the original state vector. As a consequence, the projection onto the original state or its orthogonal complement will now sometimes give the orthogonal state as outcome. This can be detected by Alice and Bob by comparing a fraction of their data as statistical test for these error outcomes. Within the statistical error margin, they may conclude whether eavesdropping activity took place or not. If no eavesdropping activity is detected, they translate their signal and measurement results into a binary string and use it as a key.

We already pointed out that the signal structure must contain non-orthogonal quantum states. Note that it is also essential that there is no measurement that would possibly commute with Bob's measurement, otherwise the disturbance of Eve's measurement would not be detectable by Alice and Bob. Here, the random choice of the two polarization measurements guarantees this property. The formal criteria can be expressed by describing Bob's total measurement strategy by a positive operator valued measure (POVM) with four elements. They contain some pairwise non-commuting elements, which gives us the desired property.

Note that it is essential that the public classical channel assures that Eve may listen to the signals, but she may not change the data flow between Alice and Bob. Consider the setting that Alice and Bob use a channel where Eve can also change the signals in the classical channel. Following the BB84 protocol, they might assume that they share a secret key in the end. (See Figure 15.2.) Instead, Alice might have talked to Eve, establishing actually a secret key with Eve, and not with Bob. Similarly, Eve might impersonate Alice to Bob, establishing a secret key also with Bob. If Alice now encrypts her secrets with the first key, Eve can decode it, and encode it with her second key she shares with Bob. As a result, Alice and Bob can communicate, but their communication will not be secure at all.

This can be prevented if Alice and Bob *authenticate* their public discussion. This is a technique drawn from classical cryptography [26]. It uses requires that the two parties share

some initial key of the order $\log \log |M|$ where $|M|$ is the size of the possible message space to be authenticated. This method provides unconditional security in the sense that the success probability of faking the authentication can be made exponentially small, and thus does not degrade the security of QKD. Once we authenticate the classical communication with the initial key, we can obtain a much larger amount of new secure key. Part of that can be used for authentication in subsequent rounds of QKD. The fact that there is no degradation of security by using this new secure key is called *composability* and has been investigated recently in a rigorous manner [2]. As a result, we should strictly speak of quantum key distribution as *quantum key growing*, though we stick here to the more common label QKD.

There are other QKD protocols. As Bennett showed, it is sufficient to use any two non-orthogonal quantum states as signal states with a suitable detection process. This is formulated as two-state protocol [3]. Another qubit protocol which shows a high symmetry of signal states is the six-state protocol [1, 5]. A different class of QKD schemes is based on the distribution of entangled bi-partite quantum states [7].

15.4 Idealized QKD in noisy environment

The BB84 protocol as described above will not work in any realistic implementation. This is due to the presence of errors even when there is no eavesdropping activity. These errors can originate from misalignment of devices, loss and noise in fibers, or dark counts in single-photon detectors. We need, therefore, to extend the protocol in such a way that it remains stable in the presence of some small error rate.

In a conservative view, all observed errors must be ascribed to the activities of an eavesdropper. Therefore we face two effects of the noise on the key drawn from the sifted data:

1. since the data of Alice and Bob do not agree, the partners do not share a common key
2. the errors are a signature of eavesdropping, and Eve can be correlated with Alice's and Bob's data, so the key is not secret.

First, we should convince ourselves that in this situation it can be possible to create a secret key. For this, we remember that the important idea is to transport non-orthogonal signals states across a channel without the signal being changed. We have to do this in the presence of noisy and lossy channels. This problem is very similar to classical noiseless communication via noisy channels, and the solution to that problem is classical error correction. (See Chapter 1.) Here a classical message is encoded redundantly, sent across a channel which adds some noise to the redundant message, and then asymptotically perfectly decoded. (See Chapter 7.) The same idea can be realized with quantum signals sent via a quantum channel. We encode the non-orthogonal signals with a quantum error correction code (QECC), send them over the channel and then decode them. So we obtain an effective perfect channel even in the presence of noise. It is therefore possible to perform perfectly secure QKD in the BB84 protocol even over noisy channels, just using QECCs.

For a realistic implementation, this would leave us with encoding and decoding operations which require controlled entangling and disentangling operations of several qubits. This is beyond our present technological capability. Fortunately, as we show next, we do not really need to implement these operations. As shown by Shor and Preskill [21], these operations

are equivalent to a protocol that uses the same quantum operations as in the first phase of the BB84 protocol, only the second phase of the protocol needs to be complemented by two new classical communication protocols:

2. Phase II (continued)

- (d) Alice and Bob perform classical error correction via linear error correction codes.
- (e) Alice and Bob perform privacy amplification by taking parity bits of random subsets as their final key.

Both protocols are motivated by the Calderbank-Shor-Steane (CSS) quantum error correction codes [6, 22]. In these codes, the bit and the phase errors occurring (see Chapter 7) in the channel can be corrected independent of each other. Classical error correction corresponds to the bit error correction and reconciles Alice's and Bob's sifted bit string. For this, Alice encodes a random bit string k into a code word w of a linear error correction code. Then she encodes the result with bits of her sifted key s and obtains $c = w \oplus s$. Finally, she sends c over the public channel to Bob. Bob has a sifted bit string $s' = s \oplus e$ where e is the error string characterizing the difference between Alice's and Bob's sifted key. Bob can calculate $w' = c \oplus s' = w \oplus e$. By measuring the error syndrome of w' , Bob now can determine e and decode the random sequence k chosen by Alice. With that, Alice and Bob share a new random sequence k which is shorter than the original sifted key. Given Shannon's theory of error correction, the length of the key shrinks ideally only to the factor $1 - I(A; B)$ where $I(A; B)$ is the mutual information shared by Alice and Bob. For the binary situation we are facing here, we find the new rate of corrected key per sifted key as $r_{corrected} = 1 - h(e)$ with the binary entropy function $h(e) = -e \log_2 e - (1 - e) \log_2 (1 - e)$.

After Alice and Bob reconciled their key, we still need to take care of the correlation Eve might have with this corrected key. This is done in the step of privacy amplification which corresponds to the phase error correction in QECC. Actually, since we already measured the qubits, we cannot correct the phase errors. Instead, we take care of the influence the phase error correction would have had on the decoding procedure of the quantum signals before measuring. This corresponds to a shrinking of the corrected bit string via a linear map which is derived from the CSS code. Denote by P a matrix representing a linear map induced by the CSS code, and denote by k the corrected key resulting from bit error correction, taken as a vector with binary values. Then the key resulting from the operation $k_{final} = P \cdot k_{corrected}$ is a secret key shared by Alice and Bob. Here the operations are taken modulo 2. The dimensions of the matrix P are chosen such that the final rate of secret key per element of the sifted key is given by

$$r_{final} = 1 - 2h(e). \quad (15.1)$$

The resulting rate shows that we can obtain a secret key with this method up to an error rate of ca. 11%. The rate assumes an identical distribution of phase and bit errors as they would result from a random permutation of the signals. In that case, the Shannon limits in error correction and privacy amplification hold. Without those permutations, the rate would drop to $r_{final} = 1 - h(2e) - h(e)$. This comes from the Gilbert-Varshamov bound [16] in classical error correction theory, which affects the choice of dimensions of the privacy amplification matrix.

We still need to discuss the final security statement. As we have seen above, we are using the knowledge of an error rate for bit and phase errors. These are identical in the BB84 protocol due to the equal use of the two polarization basis which interchanges bit and phase errors. So the security of the final key is guaranteed to the level that the QECC behind the scheme would be able to correct all the bit and phase errors that occurred during the transmission. At this point, classical statistics comes into the game. Alice and Bob can open up some random signals and compare them via the public channel. From these data they can conclude that the total number of bit and phase errors e is below the number which the QECC's can cope with. To obtain valid estimations is actually one of the tricky part in the security proofs of QKD.

This security proof is valid against all attacks of an eavesdropper within the laws of quantum mechanics. The only restriction is that we assume that Eve has only access to the quantum mechanical systems as they pass through the quantum channel and to the full information flowing through the public channel. She cannot access Alice's or Bob's sending and detection devices, e.g. to read off the setting that generate the signals for Alice or chooses Bob's measurement devices. This assumption is natural; actually no secure communication can be performed without it. However, it needs always to be enforced by technology. Moreover, in quantum optical implementations one has to take special care of this, as an optical channel (fiber or free space open air) provides a clear path right to the heart of the devices. We refer to this scenario as 'unconditional security'. Obviously not because we do not make any assumptions (we do make assumptions about the isolation of Alice's and Bob's devices), but because this term parallels the established notion in classical cryptography meaning that no assumptions are made about computational power of an eavesdropper analyzing the encrypted data.

This general eavesdropping attack is typically referred to as *coherent attack* since Eve can interact coherently with all the signals. In contrast to that, we refer to an attack as *individual attack* if Eve interacts with each signal separately, e.g by attaching to each signal a probe and then measuring that probe. There is an intermediate level of attack in which Eve interacts with each signal individually, attaching to each an independent probe. However, she then can perform joint measurements on all probes. This type of attack is called *collective attack*. Due to the structure of the BB84 protocol (random sequence of signals and measurements) it is believed that the collective attacks is indeed optimal. However, a rigorous proof that we can restrict ourselves to collective attacks is still missing.

15.5 Realistic QKD in noisy and lossy environment

As we have seen, the BB84 protocol can be made stable against noisy channels as long as the noise leads to a reasonable error rate below ca. 11%. However, for an implementation with polarization signals, we would require single photon sources. Presently, no perfect single photon source is available, though there are quite many research groups that work into that direction. The purpose is not only an implementation of QKD: single photon sources are useful also for implementation of small set of quantum gates in linear optics implementations (see Chapter 19). As we will see in this section, it is not necessary to use single photon sources in order to perform unconditionally secure QKD.

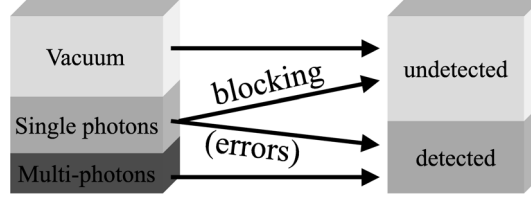


Figure 15.3. In the PNS attack Eve can guide the signals depending on the total photon number. From all multi-photon signals Eve splits off one photon while forwarding all remaining photons to Bob, thus leading to detection events. All vacuum signals are forwarded directly, leading to no detection. Some of the single photon signals are blocked to mimic the detection rate of the lossy channel, while Eve can interact with the remaining single-photon signals to extract information about their state. This is the only process that introduces some error rate.

As we look at optical implementations of QKD, we find that one uses either attenuated laser pulses or signals generated by parametric down-conversion. Both signals do not generate single photons.

In a typical realization, the attenuated laser pulses can be described by a Poissonian distribution of photon-number states (Fock states), that is, the density matrix of the signal states is $\rho = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n|$. Here μ is the average photon number of the signals. Alice imprints her signal information on the polarization of these photons. Bob measures the polarization of the arriving light pulses. The signals are attenuated, for example one chooses $\mu = 0.1$ so that most of the signals are vacuum signals, some contain single photons, and a fraction of order 0.005 signals contains several photons.

Let us now consider what happens if we use this signal source instead of the single-photon source in the BB84 protocol. The vacuum component of the signal reduces the signal rate since no signal will be detected by Bob. The single photon signals work ideally. The problematic part are the multi-photon pulses. Their presence allows Eve to perform the *photon-number splitting attack* (PNS). This attack is particularly powerful in the presence of loss in the quantum channel. In the PNS attack Eve replaces the lossy channel by a perfect quantum channel. Then she performs a quantum non-demolition measurement of the total photon number of the pulses. Such a measurement tells Eve the exact number of photons in the signal, but it does not disturb their polarization. Now she can act on the signals according to the total photon number. (See Fig. 15.3.) Whenever she finds a vacuum signals, she forwards a vacuum signal to Bob since she cannot learn anything about the polarization of the signal. If she finds a multi-photon signal, she splits off one photon from the pulse and sends the remaining to Bob. This does not disturb the signal polarization either in the photon she split off, nor in the photons she sends on. Later in the protocol, Alice will reveal the polarization basis of the signal and this allows Eve to perform the correct measurement on the single photon she split off, thereby obtaining perfect information about the signal encoded in multi-photon pulses. The remaining signals are single-photon pulses. Here Eve blocks a fraction of the signals to match the expectation of detection events for Bob's detectors. On those single-photon signals that she does not block, she can perform any coherent eavesdropping attack. This means, in

the worst-case scenario, all errors are concentrated in signals arising from eavesdropping in single-photon signals.

Let us illustrate this attack with a Poissonian photon number distribution in a channel with single-photon transmittivity η . In that case, the signal source emits vacuum, single-photon and multi-photon signals with the probability

$$P_{vac} = e^{-\mu} \quad (15.2)$$

$$P_{single} = \mu e^{-\mu} \quad (15.3)$$

$$P_{multi} = 1 - (1 + \mu)e^{-\mu} \quad (15.4)$$

The channel is lossy, so in the absence of an eavesdropper we would expect the photon number distribution to be Poissonian with average detected photon number $\mu\eta$. Therefore we find, that Bob expects to find non-vacuum signals with the probability $p_{exp} = 1 - e^{-\mu\eta}$. Eve can mimic the loss of the original channel with the PNS attack. For this, she follows the above description, and she lets only the fraction of $(p_{exp} - p_{multi})/p_{single}$ single photon signals pass. Still, as long as there are single-photon signals contributing to the observed events, we can distill a secret key. The resulting key rate is given by

$$G = p_{exp} (R[1 - h(e/R)] - h(e)) \quad (15.5)$$

where $R = (p_{exp} - p_{multi})/p_{exp}$ is the fraction of detected signals that come from single-photon signals. The formula is easily understood. Only that fraction of signals can lead to a secret key where at least one photon has been detected, therefore the leading factor p_{exp} . Within that set, only the fraction R of the sifted key can lead to a secret key and is affected by a rescaled error rate e/R , so that the amount of privacy amplification we need to apply is $R h(e/R)$. The amount of classical error correction is still just $h(e)$ and applies to all signals, whether they come from the single or multi-photon case. In the case of ideal single photon sources, we find $R = 1$ and recover Eqn. (15.1). Clearly, only if this rate is positive, we can achieve QKD. This poses constraints on the tolerable loss and the tolerable error rate. To understand that we can treat the single-photon and the multi-photon signal separately, let us introduce the idea of tagging [9, 12]. We consider any multi-photon signal which is split by Eve as a tagged single photon signal, that is, a single photon signals where we have given an eavesdropper the full information about the signal. Clearly, from these events we cannot generate a secret key, while from the remaining events we can. But in the implementation we do not know which bits come from which part. So we apply classical error correction to all the bits, regardless from which set they are drawn. Next we apply privacy amplification on the total reconciled key. Actually, we consider here privacy amplification methods that are linear in the sifted key, so we obtain

$$k^{final} = P \cdot k_{corrected} = P_m \cdot k_m \oplus P_s \cdot k_s = k_m^{final} \oplus k_s^{final} . \quad (15.6)$$

Here we separate $k_{corrected}$ into the two components, which induces a separation of the privacy amplification matrix P into two sub-matrices P_s and P_m , acting onto the single and the multi-photon signals respectively. Therefore, the final key consists of two components, k_m and k_s . The multi-photon contribution k_m is completely known to the eavesdropper. However, if we choose P_s such that the key component k_s is secure, then also the final key k_{final}

is secure! Actually, P can be chosen to be a random matrix [18, 19], and then also P_s is a random matrix, no matter what the decomposition into single-photon and multi-photon signals is. So by choosing the dimensions of P appropriately, one can assure that the matrix P_s has the correct dimensions to assure the privacy of k_s , and therefore of k_{final} .

Clearly, we see that the loss is the leading effect in limiting the key rate. In the absence of errors, we find for a Poissonian distribution with average photon number μ and a single photon transmittivity of η in the channel the secret key rate

$$G \sim p_{exp} - p_{multi} = [1 - e^{-\mu\eta}] - [1 - (1 + \mu)e^{-\mu}] . \quad (15.7)$$

We can optimize the key rate over the choices of μ and find $\mu_{opt} \approx \eta$, so that in total we have

$$G \sim \eta^2 \quad (15.8)$$

This rate should be compared to the single-photon implementation of the BB84 protocol. Here the loss of single photons reduces only the key rate as $G \sim \eta$. Even when this rate is higher, it is important to note at this point that attenuated laser pulses allow us to implement unconditional secure QKD with simple technology that is available today! Actually, by now QKD entered the commercial world [11, 17].

15.6 Improved Schemes

Clearly, one goal is to find practical QKD schemes that scale more favorable with the loss in the quantum channel. Here we discuss briefly the basic ideas.

The background of the new schemes is that we have an excellent physical model for a lossy channel. This model consists of a perfect channel with a beam-splitter that mimics the loss [24]. Applied to our simple case of an incoming Poissonian mixture of photon-number states and the auxiliary mode in the vacuum state, we obtain two outgoing independent Poissonian distribution. The outgoing average photon number for the signal mode is $\mu\eta$, while the one for the auxiliary state is $\mu(1 - \eta)$. The auxiliary mode is available to the eavesdropper. So if Eve uses this model for her eavesdropping, we find that she can obtain full information about the signal in the sifted key only if she *and* Bob receive at least one photon. This probability, which refer to as *splitting probability* is given by

$$p_{split} = [1 - e^{-\mu\eta}] [1 - e^{-\mu(1-\eta)}] . \quad (15.9)$$

With that, the final key rate, *assuming* beam-splitting as eavesdropping method, will be

$$G \sim p_{exp} - p_{split} = (1 - e^{-\mu\eta}) e^{-\mu(1-\eta)} . \quad (15.10)$$

Note that this expression is positive for any combination of average photon number μ and transmittivity η . The optimization over μ leads to $\mu_{opt} \approx 1$ and therefore to

$$G \sim \eta . \quad (15.11)$$

Clearly, this rate scales much better than the worst case scenario from the PNS attack. Actually, it is the same scaling behavior as the implementation of the BB84 protocol with single

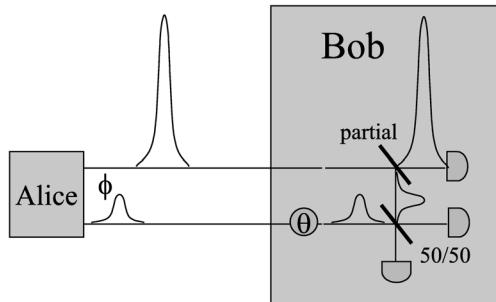


Figure 15.4. In the strong phase reference scheme Alice sends a weak coherent pulse and a strong reference pulse. The signal is imprinted onto the relative phase. In Bob's receiver a weak signal is taken from the strong reference pulse and brought to interference with the weak part. The presence of the remaining strong signal is also detected.

photon signals would provide with a lossy channel. So the question is how to restrict Eve to beam-splitting rather than the photon-number splitting? Presently, we know of two such strategies.

The first approach is based on the strong phase reference pulse ideas and aims to ban *neutral* signals. These signals are, in the standard BB84 with weak coherent pulses, the vacuum pulses Eve can forward to Bob. For these pulses, Eve can be sure that Bob will not obtain a sifted key, and moreover, no error will be created for any neutral signal. Banishing neutral signals is a strong defense against attacks such as the photon-number splitting. In that attack it is essential that Eve can separate the pulses in two sets: one on which she can extract easily information and which she wishes Bob to detect, and another set that leaves her with no or minimal information, and which she wishes Bob not to detect, especially not to detect with an error.

The new set-up is illustrated in Fig. 15.4. The signals consist of a strong coherent pulse and a weak coherent pulse. The signal information is imprinted on the relative phase of the two pulses. In principle Eve can implement attacks that correspond to the PNS attack, but she now faces the problem that there is no way to suppress signals without causing errors. The reason is the following: the detection device splits off a weak pulse from the strong coherent pulse and interferes it with the weak pulse of the signal in order to read off the relative phase. The remaining part of the strong signal pulse will be detected by a detector showing a strong classical photo-current. Eve cannot suppress the strong pulse without this being noticed immediately. If she sends only the strong pulse, but no weak counterpart, then the two detectors monitoring the output of the interference beam-splitter will show random outcome if a photon is detected. Since the strong pulse is present, at least the weak pulse stemming from that signal will impinge on the beam-splitter. Therefore, the resulting error rate will be non-zero. This effect has been recently demonstrated in a related set-up by Koashi [13] who showed that the provably secure rate scales indeed, as hoped, as $G \sim \eta$.

The second approach is even simpler. When looking at the PNS attack, we notice that in the optimal attack, Eve will have to suppress a fraction of the single-photon signals, simply

by replacing them with neutral vacuum signals. This fraction is determined by the loss in the original quantum channel and by the knowledge of the average photon number of the signals. So we can make Eve's life harder by using signals where the signal strength is varied at random in the so called decoy state protocol [10]. Alice and Bob can later sort their signals and detection events by the chosen signal strength and note down the rate of received signals for each of these subsets. Eve cannot do anything like this. When she observes one photon, she does not know from which photon number distribution this photon comes. Her optimal strategy can no longer be the simple PNS attack as shown above. Actually, as shown by Lo et al. [14], in the limit of an infinite number of different choices, the only strategy that will produce the correct number of detected signals for all secretly chosen average photon number of the signal is the beam-splitting attack. In practice, it turns out that already two different settings improve the rate and distance of the secret key generation drastically [15, 25].

15.7 Improvements in Public Discussion

The rate versus distance characteristics of QKD protocols can not only be improved by changing the physical set-up, e.g. by using different signal states or measurements. More potential lies also in improvements of the public discussion. The secure key rate of the BB84 protocol based on single photon signals can be made robust to tolerate about 20% error rate, instead of the tolerated 11% error rate according to the Shor-Preskill security proof, by applying a specific two-way communication protocol [8]. In the case of the BB84 protocol with weak coherent pulses, as described above, an improvement has been found by Scarani et al. [20] which is designed to counteract the PNS attack. For this, observe that a two-photon pulse gives away all of its signal information in the BB84 protocol only because Alice and Bob announce the polarization bases of their signals and measurements. Only then Eve can find out the proper signal without error by measuring her remaining single photon. Scarani et al. propose a new public announcement in which Alice announces sets of two signal states instead of the polarization basis. These signal sets contain the signal she actually sent plus a random choice of one of the neighboring states. For example, if she sent a horizontally polarized photon, she announces at random either the set {horizontal, $+45^\circ$ } or {horizontal, -45° }. Let us assume, she announces the set {horizontal, $+45^\circ$ }. Bob still performs the random measurement. In case that he chooses the $\pm 45^\circ$ basis and find the outcome -45° , he can unambiguously identify the signal "horizontal" as signal state. For the other outcome he cannot conclude which signal state has been sent. Anyway, Alice and Bob can postselect events in this way for which Bob can with certainty identify the signal. The situation of Eve for these signal states is different. She can also perform one of the two polarization measurements on her retained photon, but she has to live with the fact that she can identify the correct signal only with some probability, as she has no power to influence the postselection process. Due to the non-orthogonality of the states of the split-off photons, there is also no other measurement she could perform that would fare better in always telling the two signal apart. Therefore, multi-photon signals no longer give away all of their information, and one can extract secret key even for lossy channels where the PNS attack for the original protocol would no longer give secret keys.

15.8 Conclusion

As we have seen in this section, quantum mechanics offers a solution to distribute a secret key to two parties once they are provided with an authenticated public channel. This can be done, for example, by sharing some initial secret key. The whole procedure can be made robust under noise and loss in the quantum channel. Moreover, we can use relatively simple signal sources, such as attenuated laser pulses, to achieve this goal. It is important to keep in mind that this progress does not mean that research on the theory in QKD is already completed. One has to find protocols that cope efficiently with the paramount problem in QKD: the loss in the transmission lines. To optimize protocols is today's challenge, and we find that the toolbox for optimal protocols is not complete yet.

References

- [1] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography. *Phys. Rev. A* **59**, 4238–4248, 1999.
- [2] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. *quant-ph/0409078*, 2004.
- [3] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, (21), 3121–3124, 1992.
- [4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, pages 175–179, New York, 1984. IEEE.
- [5] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018–3021, 1998.
- [6] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A* **54**, 1098–1105, 1996.
- [7] A. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, (6), 661–663, 1991.
- [8] D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **49**, 457, 2003.
- [9] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **4**, (5), 325, 2004.
- [10] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett* **91**, 57901, 2003.
- [11] IdQuantique, Geneva. <http://www.idquantique.com>.
- [12] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *Quant-ph/0107017*, 2001.
- [13] M. Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Physical Review Letters* **93**, 120501, 2004.
- [14] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Physical Review Letter* **94**, 230504, 2005.
- [15] X. Ma, and B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *quant-ph/0503005v4*.

- [16] F. J. MacWilliams and J. J. A. Sloane. The Theory of Error-Correcting Codes. North Holland, Amsterdam, 1977.
- [17] MagiQ Technologies, Inc., New York. <http://www.magiqtech.com>.
- [18] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In Advances in Cryptology — Proceedings of Crypto '96, pages 343–357, Berlin, 1996. Springer. Available as quant-ph/9606003.
- [19] D. Mayers. Unconditional security in quantum cryptography. JACM **48**, (3), 351–406, May 2001.
- [20] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. **92**, 057901, 2004.
- [21] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441–444, 2000.
- [22] A. M. Steane. Error correcting codes in quantum theory. Phys. Rev. Lett. **77**, 793, 1996.
- [23] G. S. Vernam. Cipher printing telegraph systems. Journal of the AIEE **45**, 295, 1926.
- [24] W. Vogel, D.-G. Welsch, and S. Wallentowitz. Quantum Optics: An Introduction. Wiley-VCH, Berlin, 2nd edition, 2001.
- [25] X.-B. Wang. A decoy-state protocol for quantum cryptography with 4 intensities of coherent light. quant-ph/0411047.
- [26] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. J. Comp. Syst. Sci. **22**, 265–279, 1981.
- [27] S. Wiesner. Conjugate coding. Sigact News **15**, 78, 1983.

16 Quantum Communication Experiments with Discrete Variables

Harald Weinfurter

16.1 Aunt Martha

After learning about the first quantum communication protocol, the BB84 protocol enabling secure key exchange, one might think that it is straightforward to set up the experiment. Yet, it took quite a few years, and in particular also the initiative of the inventors Bennett and Brassard, who, together with Beette, Savail, and Smolin, started experiments on QKD. The first secure quantum key between Alice and Bob was established back in 1991 in laboratories of IBM research center at Yorktown Heights (Fig. 16.1) [1]. In this setup, called “Aunt Martha,” attenuated light pulses have been transmitted over 32 cm between the sender and the receiver unit. Based on the BB84 protocol, the authors demonstrated how Alice and Bob, indeed, can verify whether an eavesdropper disturbs the transmission or whether they can extract a secure key. The first experiment used a light emitting diode as the light source and fast Pockels cells to choose the polarization direction. In this first experiment a key rate of a few hundred bits per second was achieved and a number of eavesdropping attacks was simulated. Already there it was demonstrated how to correct residual bit errors and how to guarantee full security even in the presence of (experimental) noise.

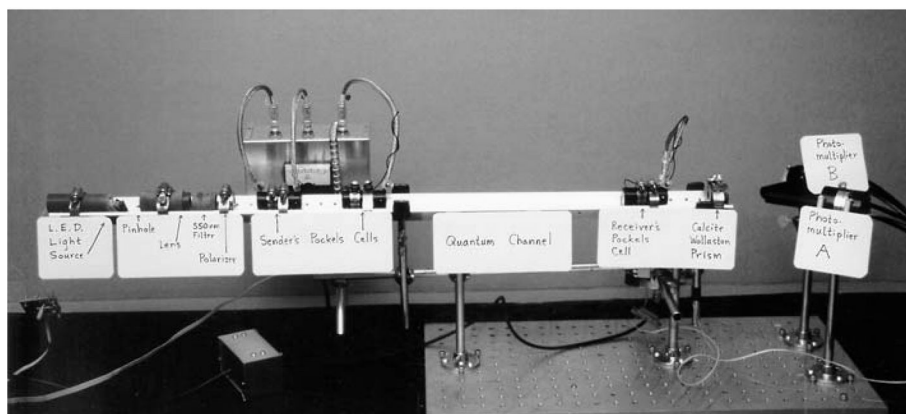


Figure 16.1. Setup of the first quantum cryptography demonstration [1], copyright Ch. Bennett.

This shining example became the model for numerous quantum cryptography systems developed worldwide. This chapter gives an overview of the current status of developments which recently led to the first commercial systems (for a detailed review of QKD see also [3]. In addition it gives a brief introduction to experiments on other quantum communication protocols such as quantum dense coding and first demonstrations of quantum error correction.

16.2 Quantum Cryptography

The most important criteria for quantum cryptography are high key rates and long distances. Usually one cannot optimize both at the same time and some compromises have to be made. No compromise, however, is acceptable when it comes to reliability and user friendliness. To make QKD a real application it is thus necessary to develop new optics, quite different from the standard quantum optics setups. These allow high flexibility, but they are quite expensive and, due to the many alignment options, are usually not stable enough for continuous operation.

The distance between Alice and Bob is limited mainly by losses in the quantum channel and by the efficiency and noise of single photon detectors. Losses or low efficiency reduce the number of detected photons and thus the number of bits in the raw key. Noise (dark counts) in Bob's detectors result in a noise floor from bit errors which are indistinguishable from those caused by eavesdropping attacks. It can be corrected for, but only on the cost of raw key material. For low efficiency or high loss, this noise floor can easily reach the 11% level, where no secure key can be distilled anymore. Any attempts to amplify the single photon signal have to fail as well, since, according to the no-cloning theorem, any amplifier introduces the same noise as an eavesdropper would do. This would therefore ruin the remarkable advantages of quantum key distribution. Only the quantum repeater, intermediate quantum error correction and memory stages along the quantum channel, could enable truly long distance communication. Its basic components are being developed now. As it will take some time until we will use it, we have to rely on conventional means to transmit the single photons.

Two options for quantum channels are available, which determine the wavelength and consequently distinguish the complete systems. Photons can be distributed either using glass fiber connecting Alice and Bob, or with telescopes aligned mutually for optimal coupling. In the following the two systems are compared as they are implemented for prototypes or already in commercial systems. Most systems under development rely on attenuated light pulses, as this is less expensive and enables high rate systems. Single photon options and entanglement-based systems are described thereafter.

16.2.1 Faint pulse QKD

16.2.1.1 Fiber-based QKD

Glass fiber systems best use the standard telecom fibers. They are already available between the main communication centers or could be installed with reasonable effort. Standard telecom wavelengths are 1300 nm or 1550 nm, respectively, where dispersion or loss, respectively, reach a minimum. State preparation, manipulation and analysis can be achieved with standard

telecom components. The high standard of such components allows a relatively fast development time of the basic setup of such QKD systems.

Glass fiber is slightly birefringent. Over the long distances this effect sums up. Care has to be taken, as this birefringence might vary, depending on the stress or the temperature of the fiber. As a result, a well-defined initial polarization fluctuates strongly at the receiver. In principle, one can try to compensate birefringence, but it is more advisable to define a new encoding for the qubit. The two-state system in this case is defined by two possible times, where the photon can be detected (“time-bin coding”). A (variable) beamsplitter determines the relative size between the amplitudes for the two paths of an interferometer with different path lengths. A phase shifter in one of the paths behind the beamsplitter enables to set any desired state. The two paths are recombined at a second beamsplitter. If the length of the two paths differs by more than the coherence time of the light, no interference occurs at the second beamsplitter, and the light exits at two time slots this unbalanced interferometer. One output is only chosen, which even does not reduce the efficiency as this is still done within Alice. At Bob an equivalent, unbalanced interferometer is used to split the incoming amplitudes again, and, after application of Bob’s phase, allows us to observe the interference depending on Alice’s and Bob’s phase with 50% efficiency. Accepting this reduction one is thus able to observe interference over very large distances independent of possible phase fluctuations along the quantum channel.

Disadvantage of this wavelength regime is the high noise and the relatively low efficiency of the single photon detectors available (germanium- or InGaAs-avalanche diodes). Optimization of these detectors enabled one to steadily increase the distance over the few last years. With 122 km the team of Toshiba (leader Andrew Shields) in the moment stays ahead of its competitors NEC and Mitsubishi [2]. New detector systems will enable longer distances, 200 km seem feasible within the next few years.

A very reliable and stable system was developed at the University of Geneva. The group of Nicolas Gisin and Hugo Zbinden found a tricky extension of the basic principle, which significantly increased the stability and quality of the system [3]. In addition to using time-bin coding to reduce the influence of the fiber, they made the receiver Bob the source of the light pulses (Fig. 16.2). He first generates bright coherent pulses at two different times with a polarizing, unbalanced interferometer and sends them to Alice. She can now use the bright pulses to easily synchronize her actions consisting of the application of one out of four possible phase shifts, backreflection at a Faraday mirror, and attenuation to the single photon level. On the way back to Bob, the light undoes all rotations and, only then, Bob applies his phase shift. Under the assumption that all fluctuations occur on a much slower time scale as it takes the light to travel from Bob to Alice and back again, all disturbances cancel. Only the phase difference between Alice’s and Bob’s modulations stays and determines the result of the measurement. By using the polarizing interferometer together with Faraday mirror (rotates the polarization of the reflected light by 90°) this system does not suffer from the usual 50% reduction of time-bin coding systems. From the measurement results Alice and Bob can infer the mutual phase settings and obtain the key bits, which are now more or less immune to any disturbance.

With such a so-called “plug&play” system QKD was demonstrated between the cities of Geneva and Lausanne over a distance of 67 km at a rate of about 150 bit/s. Even more remarkable, the glass fiber connecting Alice and Bob was a standard fiber of Swisscom. Sender and

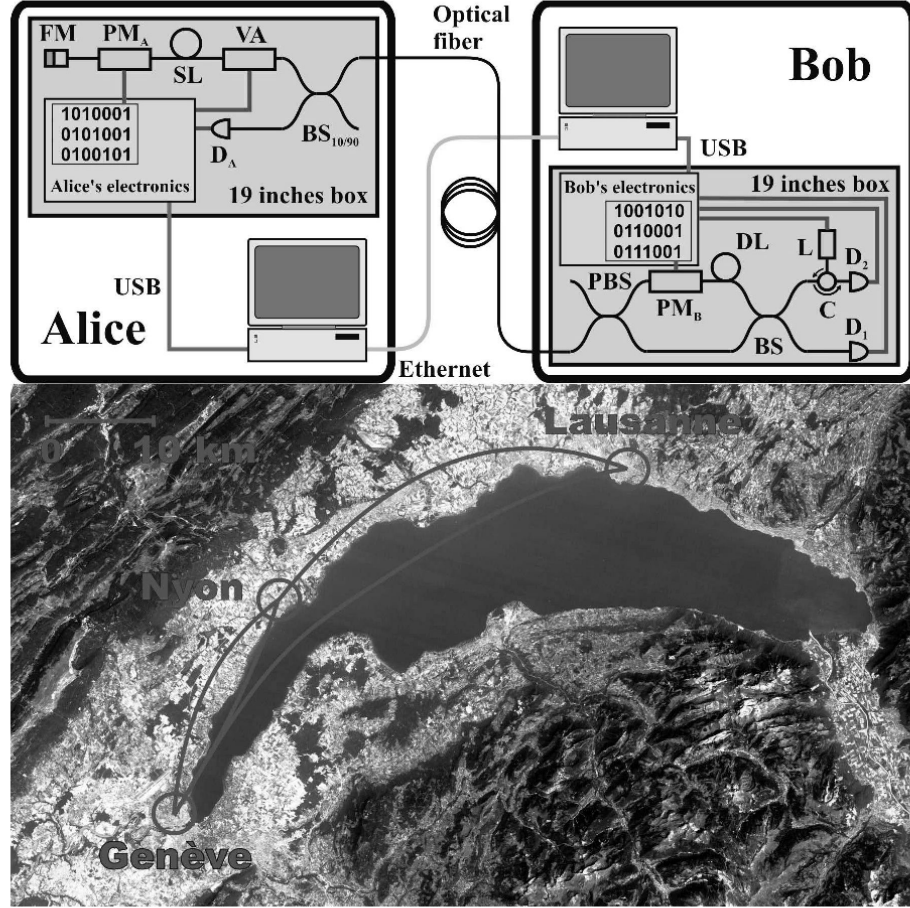


Figure 16.2. Quantum cryptography along a glass fiber of 67 km between Geneva and Lausanne. [3]

receiver modules were integrated in 19" racks and placed in buildings of Swisscom, which are quite different from the air-conditioned labs of standard quantum optics experiments. This very reliable system was the basis for the development of the first commercial QKD system by the spin-off company idQuantique. Now, Vectis offers secure point-to-point connection integrable into standard communication networks. Similarly, Magiq, so far the second company commercializing QKD, developed a network router, which offers the additional option of secure communication enabled by quantum cryptography (Fig. 16.3).

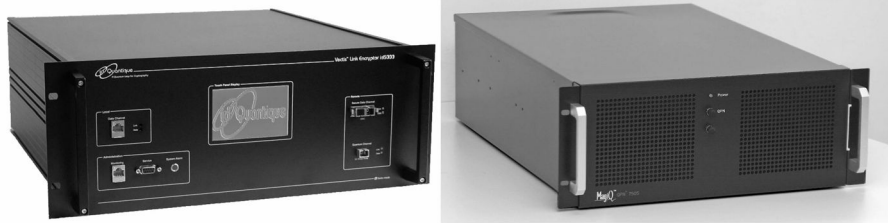


Figure 16.3. First commercial network components offering QKD-enabled secure communication (www.idquantique.com; www.magiqtech.com).

16.2.1.2 Free-space QKD

If direct line of sight is available coupling sender and receiver with telescopes becomes possible. High transmission through air is achieved for wavelengths in the range from 780 nm to 850 nm. For this range highly efficient, low-noise Silicon-avalanche photodiodes are available. All components, in particular the laser diodes, are low price, standard products. It is thus more economic to use four differently oriented laser diodes instead of costly polarization modulators. By activating only one of the four laser diodes at a time the required polarized, attenuated light pulses are generated. Free-space links mainly suffer from air turbulences, which reduce the effective aperture of the telescopes significantly. Thus, for collecting a maximum number of attenuated pulses large receiver telescopes are required.

Figure 16.4 shows the scheme of sender and receiver modules developed for free-space QKD. In the sender four laser diodes are mounted on a ring around a gold plated cone such that light reflected at the cone into the quantum channel already is oriented along four different directions. The optics of the receiver module is mounted in a very compact configuration on dedicated mounts. Optics and electronics is placed within $5 \times 5 \times 5 \text{ cm}^3$ for the sender and within $5 \times 10 \times 5 \text{ cm}^3$ for the receiver, respectively. The design warrants high stability under harsh conditions.

The power of the modules and their suitability for future applications was demonstrated in a long-distance experiment over 23.4 km in a collaboration between the Munich University, Germany, and QinetiQ, UK, led by Christian Kurtsiefer [4]. To work in calm and clean air, the test range was set up in the Alps between Zugspitze and westl. Karwendelspitze. In spite of the quite tough atmospheric conditions, like temperatures down to -20° and strong winds, secure key could be exchanged with a rate of about 1000 bit/s.

Such free-space links offer two possible applications. First, secure links can be established between buildings of a city (typical distance 4 km). For example, between the buildings of a bank or a company, or the last mile from the network provider to the user, quantum cryptography can then enable secure communication for low price.

Secondly, the direct coupling via telescopes could also enable QKD to low earth orbit satellites. Most likely, the sender will be placed in the satellite. From a height of about 500–1000 km the sender tracks the ground station and sends polarized light pulses which in turn should be collected by a big telescope on earth to exchange a first secret key. If the satellite flies over another ground station, the second secret key can be exchanged. Combining the two

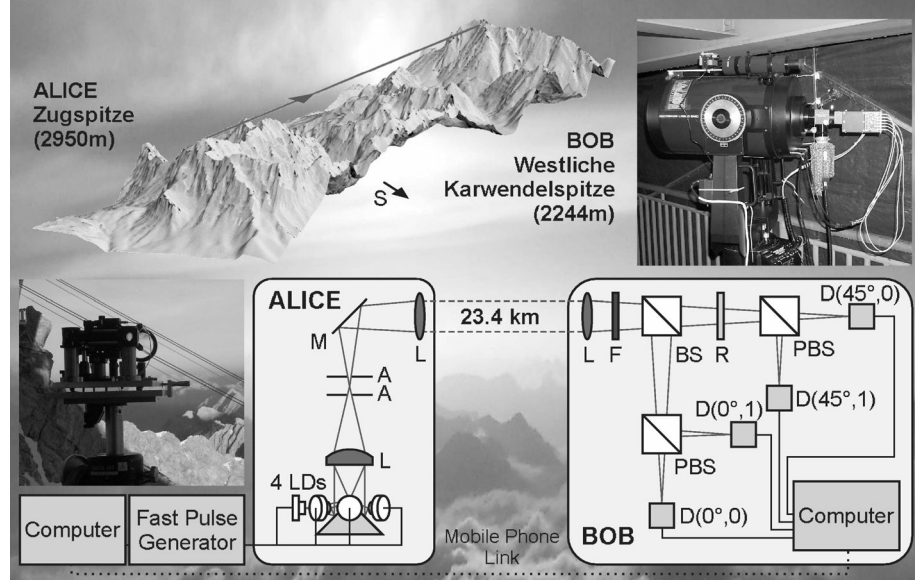


Figure 16.4. QKD demonstration over 23.4 km between Zugspitze and westl. Karwendelspitze. The right inset shows Bob's mirror telescope with the QKD-receiver modul mounted. Alice's sender moduli (left) is directly mounted inside a Galileo telescope.

keys at the satellite gives a secure key between the ground stations and enables worldwide communication.

While the above long-distance QKD due to the snow around Alice's sender telescope could operate only during night, the group of Richard Hughes, Los Alamos, also demonstrated the feasibility of daylight key exchange over a distance of 10 km [5]. Necessary for this are fine filtering in the frequency domain and the spatial domain as well as fine selection of the detection time. The currently fastest system was designed at NIST, Gaithersburg [6]. Highly integrated electronics made pulse rates of 125 MHz possible. Key rates of as high as 1 MHz were achieved for the distance of 400 m.

16.2.2 Entanglement-Based QKD—Single Photon QKD

Faint pulse systems suffer from the requirement that, in order to ensure secure QKD, the probability for detecting a photon in a pulse has to be much smaller than 1, and also now depends on the loss in the system (see the previous chapter). Improved schemes can cope with this, but have to be implemented in realistic scenarios first. An alternative solution is to use true single photon sources or entangled pairs of photons.

Right from the beginning of experimental quantum communication a series of papers demonstrated how entanglement-based quantum cryptography can be performed, with different types of integration of the setups and of communication protocols [7]. There, first a

are single atoms or ions trapped by electromagnetic fields. Such experiments required vacuum vessels, narrow band lasers, etc., and are thus not that well suited for QKD. However, they are excellent for more demanding applications, like linear optics quantum computation. Other possibilities are quantum dots or single, fluorescing defects in diamond [10]. First demonstrations show not only the feasibility of such systems but also their drawbacks. Quantum dots achieve high rates but need cryogenic cooling below 4 K; NV defects in diamond are simple and reliably used at room temperature but still lack high rate and have too wide emission spectrum. The future will bring new and better systems, but they will have to compete with attenuated pulse QKD based on improved protocols not requiring the strong attenuation.

16.3 Entanglement-Based Quantum Communication

Quantum teleportation is of course the best known representative of the new protocols showing improvements of classical communication by quantum means. But there are also other methods for quite diverse purposes.

16.3.1 Quantum Dense Coding

The closest protocol to teleportation is quantum dense coding. It enables the transmission of two bits of classical information by sending only a single qubit. Assume, Alice and Bob want to communicate classical information. Alice might use quantum particles, all prepared in the same state by some source. She translates the bit values of the message to either leaving the state of the qubit unchanged, or to flip it to the other, orthogonal state, and Bob consequently will observe the particle in one or the other state. That means that Alice can encode one bit of information in a single qubit. Obviously, she cannot do better, since in order to avoid errors, the states arriving at Bob have to be distinguishable, which is only guaranteed when using orthogonal states. In this respect, they do not gain anything by using qubits as compared to classical bits. Also, if she wants to communicate two bits of information, Alice has to send two qubits.

C.H. Bennett and S. Wiesner found a clever way to circumvent the classical limit and showed a way how to increase the channel capacity by utilizing entangled particles [11]. Suppose, the particle which Alice obtained from the source is entangled with another particle, which was directly sent to Bob (Fig. 16.6). The two particles are in one of the four Bell states, say $|\Psi^-\rangle$. Alice can now use the particular feature of the Bell basis that manipulation of one of the two entangled particles suffices to transform to any other of the four Bell states. Thus she can perform one out of *four* possible transformations—that is, doing nothing, shift the phase by π , flip the state, or flip and phase shift the state—to transform the two-particle state of their common pair to another one. After Alice has sent the transformed two-state particle to Bob, he can read the information by performing a combined measurement on both particles. He will make a measurement in the Bell-state basis and can identify which of the four possible messages was sent by Alice. Thus it is possible to encode two bits of classical information by manipulating and transmitting a single two-state system. Entanglement enables one to communicate information more efficiently than any classical system could do.

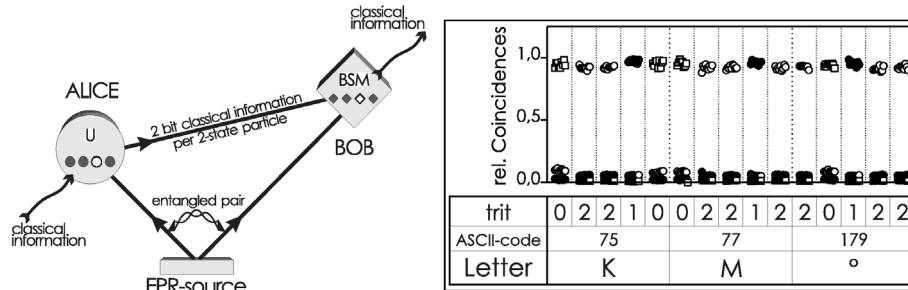


Figure 16.6. Left: Scheme for the efficient transmission of classical information by quantum dense coding [11] (BSM—Bell-state measurement, U—unitary transformation). Right: “1.58 bit per photon” quantum dense coding: The ASCII codes for letters “KM°” (i.e., 75, 77, 179) are encoded in 15 trits instead of the 24 bits usually necessary. The data for each type of encoded state are normalized to the maximum coincidence rate for that state [12].

For the experiment, the source of entangled photons was aligned such that the state $|\Psi^-\rangle$ was prepared. One photon was sent directly to Bob, the other to Alice, where half-wave and quarter-wave retardation plates were used to apply the desired manipulation encoding the classical information. Then this photon is also sent to Bob, where, for correct path length adjustment, two photon interference can be used to distinguish at least three of the four Bell states [12]. In principle, interferometric Bell-state analysis can identify two of the four Bell states, with the other two giving the same result. If Alice thus uses only three encodings all three types of messages can be distinguished. In principle, only the application of quantum logic gates allows the full analysis of the four Bell states. However, this is not possible for photons, yet. More recently, new approaches to Bell-state analysis have been demonstrated. One uses POVM measurements to also identify three states, another employs entanglement in another degree of freedom to enable the analysis of all four states [13]. Recently, Knill, Laflamme, and Milburn showed that efficient quantum computation is possible using only beam splitters, phase shifter, single photon sources, and photodetectors distinguishing between one, two photons etc. [14]. The method exploits feedback from photodetectors and is robust against errors from photon loss and detector inefficiency. The basic elements are accessible to experimental investigation with current technology; however the full implementation still needs a significant amount of photons and thus is not possible to be performed today. Bell-state analysis with linear optics quantum logic gates was achieved now, but without using a significant amount of ancilla photons, the gate employed has a success rate of only 1/9 [15].

16.3.2 Error Correction

For any quantum communication application a reliable quantum channel is of tremendous importance. As any link will introduce some noise it is necessary to either try to compensate the disturbance, or, if this is not possible, to correct for the errors occurring. This, similarly to Bell-state analysis requires quantum logic operations, which, however, are not available. In addition, quantum memories would be required, as well. Fortunately, two pairs of entangled

photons can be obtained from parametric downconversion, which allows us to demonstrate the first step without memories, and two-photon interference once again proves to be an excellent help to circumvent the necessity of logic gates.

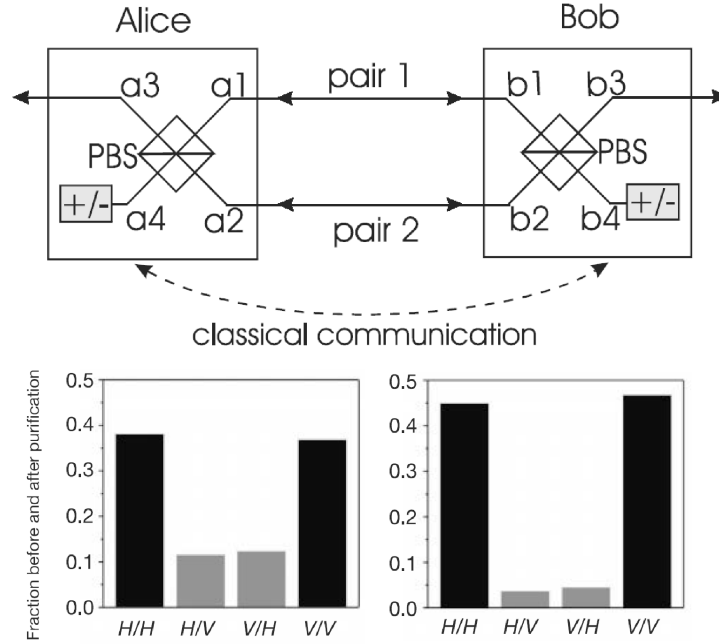


Figure 16.7. Top: Scheme for entanglement purification. Left: Detection probabilities before purification (fidelity 75%). Right: After purification, clearly showing the reduction of unwanted states (fidelity 92%).

Two options are available: for global errors, that is, several qubits are influenced by the same transformation, “decoherence-free” coding can immunize a quantum state if it is encoded in (at least) four qubits [16]. The other possibility is to combine noisy realizations of a state and perform logic operations and measurements such that one can identify the error and correct it. Due to the lack of gates, again, this is not fully possible for photons, yet, but quite a number of initial steps can be performed based on two photon interference.

To show this, we consider qubits defined by the polarization states of photons, that is, we identify $|0\rangle$ and $|1\rangle$ by linear horizontal $|H\rangle$ and vertical polarization $|V\rangle$, respectively. The entanglement purification is based on a simple optical element, the PBS. Initially, two photons enter the PBS from two different inputs. The PBS has the property that horizontally polarized photons are transmitted and vertically polarized ones are reflected. If we find one photon in each of the two outputs, then either both have been transmitted, and are $|H\rangle$, or both have been reflected, and are thus $|V\rangle$. We see, both have the same polarization. If the two incident photons have different polarization (V and H), then they will end up in the same output mode of the PBS and are not considered any longer. This feature of the PBS has been used in the

observation of multiphoton entanglement and also plays an important role in the simulation of quantum computation by linear optics [17].

From the viewpoint of error correction or entanglement purification the PBS together with conditioning on the detection is equivalent to a parity check and can therefore be used for that purpose [18]. For the experiment two pairs of entangled photons are created simultaneously by one laser pump pulse and pairwise overlapped at a PBS. Given that one detects one photon in each of the outputs, and given equal results from the parity check measurement on each side, the remaining two photons exhibit higher entanglement than the initial pairs.

16.4 Conclusion

Quantum cryptography was the first quantum communication experiment, and nowadays became already a real commercial application. Methods such as quantum teleportation and quantum dense coding were demonstrated. Due to the low rate of entangled multiphoton states it is currently difficult to use them. However, given all the necessary infrastructure also these methods will find their application, most prominently as part of the quantum repeater, where entanglement swapping, a variation of teleportation, is one of the most crucial ingredients. First steps in quantum error correction and entanglement distillation have been performed, yet, one still requires of course quantum memories. With all this at hand long distance quantum communication will be possible.

Other methods are already demonstrated or just under preparation. Quantum cloning enables the distribution of quantum states onto several qubits [19]. Multiparty applications are coming close with quantum secret sharing (the extension of quantum cryptography to several partners) [20] or communication complexity [21].

References

- [1] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptol.* **5**, 3 (1992).
- [2] C. Gobby, Z.L. Yuan, and A.J. Shields, *Quantum key distribution over 122 km of standard telecom fiber*, *Appl. Phys. Lett.* **84**, 3762–3764 (2004).
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [4] Ch. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. Gorman, P.R. Tapster, and J.G. Rarity, *Nature* **419**, 450 (2002).
- [5] R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson, *New J. Phys.* **4**, 43 (2002).
- [6] J.C. Bienfang, A.J. Gross, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, R. Lu, D.H. Su, C.W. Clark, C.J. Williams, E.W. Hagley, and J. Wen, *Opt. Express* **12**, 2011 (2004).
- [7] Initial demonstrations: A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma: *Phys. Rev. Lett.* **69**, 1293 (1992); P.D. Townsend, J.G. Rarity, and P.R. Tapster, *Electron. Lett.* **29**, 634 (1993); P.R. Tapster, J.G. Rarity, and P.C.M. Owens: *Phys. Rev. Lett.* **73**, 1823 (1994); separation of 400m, full protocol: T. Jennewein, Ch. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.* **84**, 4729 (2000); locally, various eavesdropping attacks: D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, *Phys.*

- Rev. Lett. **84**, 4733 (2000); telecom wavelength: W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000);
- [8] A. Poppe, A. Fedrizzi, R. Ursin, H.R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, Opt. Express **12**, 3865 (2004).
 - [9] G. Ribordy, J. Brendel, J.D. Gautier, N. Gisin, and H. Zbinden, Long distance entanglement based quantum key distribution, Phys. Rev. A **63**, 012309 (2001).
 - [10] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, Phys. Rev. Lett. **89**, 187901 (2002); E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto, Nature **420**, 762 (2002).
 - [11] C.H. Bennett and S.J. Wiesner: Phys. Rev. Lett. **69**, 2881 (1992)
 - [12] K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger: Phys. Rev. Lett. **76**, 4656 (1996)
 - [13] J.A.W. van Houwelingen, N. Brunner, A. Beveratos, H. Zbinden, N. Gisin, Phys. Rev. Lett. **96**, 130502 (2006); C. Schuck, G. Huber, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. Lett. **96**, 190501 (2006).
 - [14] E. Knill, R. Laflamme, G. J. Milburn, Nature **409**, 46 (2001).
 - [15] N. K. Langford, et al., Phys. Rev. Lett. **95**, 210504 (2005); N. Kiesel et al., Phys. Rev. Lett. **95**, 210505 (2005).
 - [16] D.A. Lidar, D. Bacon, J. Kempe, and K.B. Whaley, Phys. Rev. A **61**, 052307 (2000); J. Kempe, D. Bacon, D.A. Lidar, and K.B. Whaley, Phys. Rev. A **63**, 042307 (2001); P.G. Kwiat, A.J. Berglund, J.B. Altepeter, and A.G. White, Science **290**, 498 (2000); M. Bourennane, M. Eibl, S. Gaertner, Ch. Kurtsiefer, A. Cabello, and H. Weinfurter, Phys. Rev. Lett. **92**, 107901 (2004).
 - [17] D. Bouwmeester, Phys. Rev. A **63**, 040301 (2001); A. Zeilinger, M.A. Horne, H. Weinfurter, and M. Zukowski, Phys. Rev. Lett. **78**, 3031 (1997); D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
 - [18] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Nature **423**, 417 (2003).
 - [19] A. Lamas-Linares, C. Simon, J.C. Howell, and D. Bouwmeester, Science **296**, 712 (2002), S. Fasel *et al.*, Phys. Rev. Lett. **89**, 107901 (2002); F. De Martini, V. Buzek, F. Sciarrino, and C. Sias, Nature **419**, 815 (2002).
 - [20] C. Schmid, P. Trojek, H. Weinfurter, M. Bourennane, M. Zukowski, C. Kurtsiefer, Phys. Rev. Lett. **95**, 230505 (2005).
 - [21] L.-P. Lamoureux, E. Brainis, D. Amans, J. Barrett, S. Massar, Phys. Rev. Lett. **94**, 050503 (2005); P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Zukowski, H. Weinfurter, Phys. Rev. A **72**, 050305 (2005).

17 Continuous Variable Quantum Communication

Ulrik L. Andersen and Gerd Leuchs

17.1 Introduction

Much of the theory as well as experiments on quantum information science have originally been developed in the realm of discrete variables (quantum bits) since a lot of intuition of classical information concepts carries over to the quantum domain. Recently, it became clear that infinite-dimensional quantum systems are also attractive candidates for quantum information processing. In such systems information is usually encoded into a continuous variable (CV) of the electromagnetic field, examples being the amplitude and phase of light [1–3].

The main advantages of using the continuous variable components of the electromagnetic field, in contrast to the discrete variables, are that they are relatively easy to manipulate and they can be detected with very high speed and high efficiency. These prospects for high-rate quantum communication systems that may result from the use of standard off-the-shelf telecommunication components pave the way for CV quantum information processing.

Communication is the art of sending information from one place to another. Quantum communication is also the art of sending information between two parties, but now these parties' ability to communicate is enhanced by the exploitation of the two quantum features: entanglement and nonorthogonality. For example, by using the feature that quantum states can be nonorthogonal, that is, they are not perfectly distinguishable, an unconditionally secure key can in principle be distributed hereby enabling secure cryptography. Furthermore, shared entanglement between two parties, traditionally called Alice (A) and Bob (B), enables communication of quantum information using a classical channel (teleportation) or allows for an increased channel capacity (dense coding).

Several experiments have been carried out in this regime, namely quantum teleportation [4], quantum key distribution [5, 6], quantum secret sharing [7], quantum memory [8], quantum cloning [9, 10], quantum erasing [11], coherent state purification [12], and entanglement swapping [19]. In this chapter we develop the basic ideas and ingredients that are needed to understand these experiments. After introducing the basic concepts and ideas, a few quantum communication protocols are discussed.

17.2 Continuous Variable Quantum Systems

What are the continuous variables? There are of course many different continuous variables describing quantum systems, central examples being the position and momentum of a particle

or the collective atomic spin of an atom cloud. In this chapter, however, we will deal with the continuous quadrature amplitudes of the quantized electro-magnetic field. Such a field is formally described as [13, 16]

$$\hat{E} \propto \hat{x} \cos(\omega t) + \hat{p} \sin(\omega t), \quad (17.1)$$

where ω is the angular frequency, and x and p are the quadrature components defined as

$$\hat{x} = \hat{a} + \hat{a}^\dagger \quad (17.2)$$

$$\hat{p} = -i(\hat{a} - \hat{a}^\dagger), \quad (17.3)$$

where $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators, respectively. If a reference field (which is normally coined the local oscillator field) oscillates as $\cos(\omega t)$, $\hat{x}$ is referred to as the amplitude quadrature while $\hat{p}$ is the phase quadrature since they are respectively in and out of phase with the local oscillator. The choice, however, of the reference phase is arbitrary, and thus we can define a generalized quadrature: $\hat{x}_\theta = \hat{x} \cos \theta + \hat{p} \sin \theta$.

The quantumness of the optical field arises because the quadrature components are maximally incompatible conjugate quantum variables, and thus they do not commute:

$$[\hat{x}, \hat{p}] = \hat{x}\hat{p} - \hat{p}\hat{x} = 2i. \quad (17.4)$$

This commutation relation is easily derived from the standard commutation relation for the annihilation and creation operator: $[\hat{a}, \hat{a}^\dagger] = i$. These relations are a direct result of the granularity (that is the quantization) of the optical field. However, one should keep in mind that although this granularity is introduced, the observables (here the quadratures) are still continuous. This is in contrast to the discrete variables which refers to the quantized energy in each mode, i.e., photons measured by photon counting. In the regime of continuous variables, the commutation relation in (17.4) states the fact that it is not possible to “get hold off” two conjugate observables simultaneously (each with arbitrary precision): if one variable is well defined the conjugate one is random. This apparent indeterminacy of conjugate observables is in fact the quantum mechanical feature that enables quantum information processing over continuous variables. So if information is carried by the continuous quadrature pair $(\hat{x}, \hat{p})$ a set of different quantum computational tasks can be realized.

In classical statistical mechanics the amplitude and phase of the optical field are described by a joint probability distribution. In this case the probability distribution can be a delta function corresponding to a field oscillating with a well-defined amplitude and phase in time and space. This however is not the case for conjugate continuous quantum variables according to the commutation relation (17.4), and thus a joint probability distribution does not exist in quantum mechanics. It is however common to introduce a quasi-probability distribution, the Wigner function [14], which describes the distribution of quadratures in a pseudo-classical way. Interpreting the Wigner function over one of the conjugate variables generates a so-called marginal distribution which is positive definite and thus has all the properties of a classical probability distribution. There are, however, some striking properties of this distribution that makes it nonclassical. For example it can go negative! Does it mean that there is a negative probability for the oscillation to attain certain values? Not really. One should keep in mind that the stage of the oscillation is never well defined; there is an intrinsic indeterminacy given

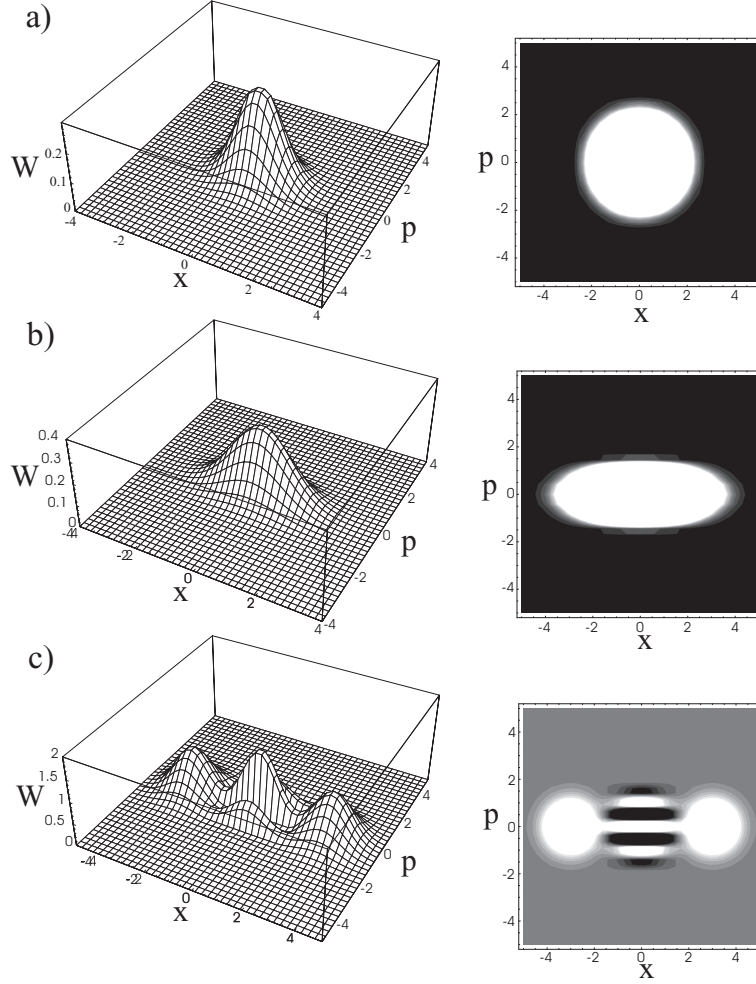


Figure 17.1. Wigner functions of three different pure states: (a) vacuum state, (b) squeezed vacuum state and (c) Schrödinger cat state.

by the area associated with vacuum fluctuations (or the commutation relation). The Wigner function is thus not a real probability distribution and is not required to be positive definite.

The Wigner function is formally defined as [15] (in the coordinate basis y)

$$W(x, p) = \frac{2}{\pi} \int_{-\infty}^{\infty} dy e^{4iyp} \langle x - y | \hat{\rho} | x + y \rangle, \quad (17.5)$$

where $\hat{\rho}$ is the state's density operator. For pure states the wavefunction is $|\Phi\rangle = \sum c_n |n\rangle$ where $|n\rangle$ is the Fock states and c_n is the probability amplitude [13]. In this case the Wigner

function can be calculated by inserting the density operator for the pure state, e.g., $\hat{\rho} = |\Phi\rangle\langle\Phi|$, into Eq. (17.5). Three important examples of pure states are illustrated in Fig. 17.1.

The coherent and squeezed states in Fig. 17.1 are described by Gaussian Wigner functions, i.e., distributions having Gaussian cross sections in any direction; thus they are referred to as Gaussian states. Experimentally these states are particularly interesting because they are efficiently producible and many interesting protocols can be carried out with these states. Furthermore, Gaussian states are relatively easy to deal with theoretically since they can be uniquely characterized by their first- and second-order moments. In addition since the quantum properties are independent of the first moments, normally only the second moments (summarized in the covariance matrix) need to be considered. For illustrating Gaussian states, it is not necessary to display the full Wigner function; the contour line at half maximum is sufficient. Contours for various quantum states are shown on the right-hand side in Fig. 17.1. The width of the cross section through a Wigner function in direction θ is determined by the second moment of $\Delta\hat{X}_\theta = \hat{X}_\theta - \langle\hat{X}_\theta\rangle$, see problem 1.

The states introduced above can either serve as information carriers, as we already pointed out, or as ancillary states (or resource states) that enable the execution of a certain quantum information protocol. For example, the entangled states are carriers of information in the dense coding protocol whereas in the teleportation protocol the entangled state enables its execution.

17.3 Tools for State Manipulation

Universal quantum communication and computation with continuous variables can be performed using combinations of linear optical components, squeezers, homodyne detectors with feed forward, and photon counters [20–22, 34]. Except for the latter, these devices are readily available in the lab, and fortunately, it turns out that remarkably many protocols can in fact be realized using only these feasible operations. Therefore in the following we introduce the various Gaussian transformations (produced by linear elements, squeezers, and homodyne detectors) in detail and discuss only briefly the non-Gaussian ones.

17.3.1 Gaussian transformations

All devices that map Gaussian states onto other Gaussian states can be concisely described by simple linear input–output relations in the Heisenberg picture. From the Hamiltonian for the device in question, $\hat{H}$, we deduce the unitary evolution operator $\hat{U} = \exp(i\hbar\hat{H}t)$ from which we derive the input–output relation using the transformation:

$$\hat{x}_{\text{in}} \rightarrow \hat{x}_{\text{out}} = \hat{U}\hat{x}_{\text{in}}\hat{U}^\dagger \quad (17.6)$$

The input–output relation of a beam splitter, a phase shifter, a single-mode squeezer, a two-mode squeezer (entangler), and a phase insensitive amplifier are presented in Fig. 17.2.

The ubiquitous device in quantum optics is the beam splitter. It is for example used to build interferometers which are unavoidable devices in almost all experimental setups. The

Device	Unitary	Transformation
	$\hat{U}_{BS} = \exp(i\varphi(\hat{x}_1\hat{p}_2 - \hat{p}_1\hat{x}_2));$ $\varphi = 2\text{Arc cos}\sqrt{T}$	$\hat{x}_{out1} = \sqrt{T}\hat{x}_1 + \sqrt{R}\hat{x}_2$ $\hat{x}_{out2} = \sqrt{R}\hat{x}_1 - \sqrt{T}\hat{x}_2$ $\hat{p}_{out1} = \sqrt{T}\hat{p}_1 + \sqrt{R}\hat{p}_2$ $\hat{p}_{out2} = \sqrt{R}\hat{p}_1 - \sqrt{T}\hat{p}_2$
	$\hat{U}_\theta = \exp(-i\theta(\hat{x}^2 + \hat{p}^2 - 2))$	$\hat{x}_{out} = \hat{x}\cos\theta + \hat{p}\sin\theta$ $\hat{p}_{out} = -\hat{x}\sin\theta + \hat{p}\cos\theta$
	$\hat{D}(x,p) = \exp(2i(p_d\hat{x} - x_d\hat{p}))$	$\hat{x}_{out} = \hat{x} + x_d$ $\hat{p}_{out} = \hat{p} + p_d$
	$\hat{S}(\xi) = \exp(i\xi(\hat{x}\hat{p} + \hat{p}\hat{x}))$ $\xi = \ln\sqrt{G}$	$\hat{x}_{out} = \frac{1}{\sqrt{G}}\hat{x}$ $\hat{p}_{out} = \sqrt{G}\hat{p}$
	$\hat{S}(\xi) = \exp(\xi(\hat{x}_1\hat{p}_2 + \hat{p}_1\hat{x}_2))$ $\xi = \ln\sqrt{G}$	$\hat{x}_{out1} = \frac{1}{\sqrt{2}}(\sqrt{G}\hat{x}_1 + \frac{1}{\sqrt{G}}\hat{p}_2)$ $\hat{p}_{out1} = \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{G}}\hat{p}_1 + \sqrt{G}\hat{x}_2)$ $\hat{x}_{out2} = \frac{1}{\sqrt{2}}(\sqrt{G}\hat{x}_1 - \frac{1}{\sqrt{G}}\hat{p}_2)$ $\hat{p}_{out2} = \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{G}}\hat{p}_1 - \sqrt{G}\hat{x}_2)$
	Not unitary	$\hat{x}_{out} = \sqrt{G}\hat{x} + \sqrt{G+1}\hat{x}_v$ $\hat{p}_{out} = \sqrt{G}\hat{p} + \sqrt{G+1}\hat{p}_v$

Figure 17.2. Table of Gaussian transformations. BS: Beam splitter, PS: Phase shifter, D: Displacement, Sqz: Squeezing, EPR: Etangler, Amp: Amplification.

beam splitter has two modes at the input, interferes them and creates two output modes. The quadratures of these modes are combined via the input–output relation shown in Fig. 17.2.

A phase shifter is a device which changes either the relative phase between two spatially separated modes or the phase between two orthogonal modes in the same spatial mode in order to change the polarization state of light. In the laboratory, the relative phase between two spatially separated modes is either accomplished using a mirror attached to a piezo ceramic

which moves as a function of an applied voltage, or by an electro-optic modulator through which the beam is transmitted. The polarization state of light can be controlled also by an electro-optic modulator but normally if no fast switching times are required a half-wave or a quarter-wave plate is used for convenience.

The displacement operation corresponds to a shift of the uncertainty area in phase space. The most important displacer in the lab is a laser: the input to the laser is a vacuum state and the output is, ideally, a coherent state; thus a displaced vacuum state (see also problem 1b). The laser is however a complex device which is not, in practice, performing a perfect displacement operation. Alternatively one can use a very asymmetric beam splitter, which is almost perfectly transmitting the state to be shifted and reflecting a small part of a laser beam enabling the displacement. The size of the displacement is controlled by the power of the auxiliary beam. It is also clearly seen that the transformation (Fig. 17.2) for the beam splitter reduces to that of a displacement transformation for a very asymmetric beam splitting ratio. Fast displacement operations are obtained using a phase or an amplitude modulator which displaces the state with a speed given by the bandwidth of the modulator. It is also possible with these modulators to displace only a certain frequency mode (a sideband), by applying an electronic modulation with a frequency equal to the frequency of the sideband mode.

The next device in the figure is the squeezer which is a device that squeezes the state in phase space (see problem 1c). A squeezer requires a nonlinear optical interaction. The standard way of squeezing a state is by using a degenerate optical parametric amplifier. Such a device is pumped by a strong field and produces two output modes (the so-called signal and idler modes) which are degenerate in polarization, thus indistinguishable. Under the parametric approximation where the pump field is assumed to be treated classically, the amplifier accomplishes a Gaussian squeezing operation. In many cases the parametric amplifier is embedded in a cavity, which supports a comb of resonantly enhanced frequency modes, hereby making the process more efficient for these particular frequencies. The parametric amplifier is mediated by a second-order nonlinearity, but a third-order nonlinearity such as the Kerr effect (or four wave mixing) can be also used. Also in this case the operation is identical to the Gaussian squeezing transformation if the pump beam is treated classically. Normally the Kerr effect is generated by propagating short pulses through a long optical fibre. Note that the squeezing operation can also be placed off-line so that squeezed vacuum only serves as an off-line resource for accomplishing the squeezing transformation on an arbitrary input state. Details about such a scheme can be found in [23]. A summary of various squeezing experiments is given in [17].

When the parametric amplifier or the four wave mixing process operate in a nondegenerate configuration (either in polarization or direction), it produces entanglement in two different modes [36]. Another, but theoretically identical, way to produce continuous variable entanglement is to interfere two squeezed beams on a symmetric beam splitter which produces entangled output beams [4, 37] (see problem 2c).

Phase insensitive amplification is also an important device in quantum communication. In contrast to the other devices in the table, the amplifier is not unitary: Excess noise is inevitable introduced to the amplified state, rendering the amplified state in a mixed state [38]. There are numerous examples of devices that, in principle, accomplish ideal phase insensitive amplification, examples being the fibre-based Er doped amplifier, parametric amplifiers, processes involving four-wave mixing and solid-state laser amplifiers. In practice, however, none of

these devices operate at the ideal quantum limit. Another approach that comes arbitrarily close to the ultimate quantum limit, in particular in the low gain regime, has recently been proposed and demonstrated. It relies solely on linear optical components, homodyne detection and feedforward (See problem 2b). Details about such a scheme can be found in [25].

17.3.2 Homodyne detection and feed forward

A homodyne detector, the most important measurement device in continuous variable quantum communication, is shown in Fig. 17.3: The signal under interrogation is combined with a much brighter local oscillator (LO) at a 50/50 beam splitter [27]. The outputs are directed to two balanced PIN photodetectors and subsequently the difference of the two detector outcomes is produced. By using a linearized model it can be shown that the resulting photo current is linearly proportional to a certain quadrature amplitude of the signal; which specific amplitude is detected is determined by the phase of the LO relative to the signal. Thus by controlling the phase of the local oscillator, any given quadrature can be measured. Another great advantage of the homodyne detector is that the LO selects effectively a certain spatial, temporal, and polarization mode among a general mixture of modes in the signal [15]. A dual-homodyne detector aims at measuring conjugate quadratures simultaneously, e.g., it may correspond to a simultaneous measurement of the amplitude and phase quadrature. Such a measurement is performed using a 50/50 beam splitter followed by two homodyne detectors located at the two outputs of the beam splitter [39]. One is set to measure the amplitude quadrature whereas the other is measuring the phase quadrature. Since one cannot perform sharp measurements simultaneously of conjugate quadratures according to the basic laws of quantum mechanics, the accuracy with which the quadratures are determined is intrinsically limited. One unit of vacuum noise is introduced in the measurement and it can be traced back to the vacuum noise entering the empty port of the 50/50 beam splitter. Note also that if this vacuum state is substituted with a state which is entangled to another mode, the measurement is identical to a continuous variable Bell measurement [4].

An important tool for executing many quantum informational tasks in the continuous variable regime is that of feedback or feedforward. Such a control system measures a certain property of the system (possibly embedded in noise like in the case of a dual-homodyne measurement), manipulates it by some signal analysis and finally, based on the gained information, controls some dynamics of the system [26]. In Fig. 17.3c and d we give two simple examples: in the first example (Fig. 17.3c) a homodyne detector measures a certain quadrature (say $\hat{x}_{in1}$) of a subsystem, and displaces the same quadrature of another subsystem with a magnitude proportional to the measurement outcome and scaled with an electronic gain g . In the second example (Fig. 17.3d) a dual-homodyne detector measures conjugate quadrature of a subsystem and drives another subsystem with the measurement outcomes. Simple examples of such feedforward systems can be found in [24] and [9].

17.3.3 Non-Gaussian transformations

As we will see in the next section the toolbox in Fig. 17.2 consisting of linear transformations provides essential tools for generating and manipulating quantum states. However some operations cannot be carried out with only this set of transformations. For example entanglement

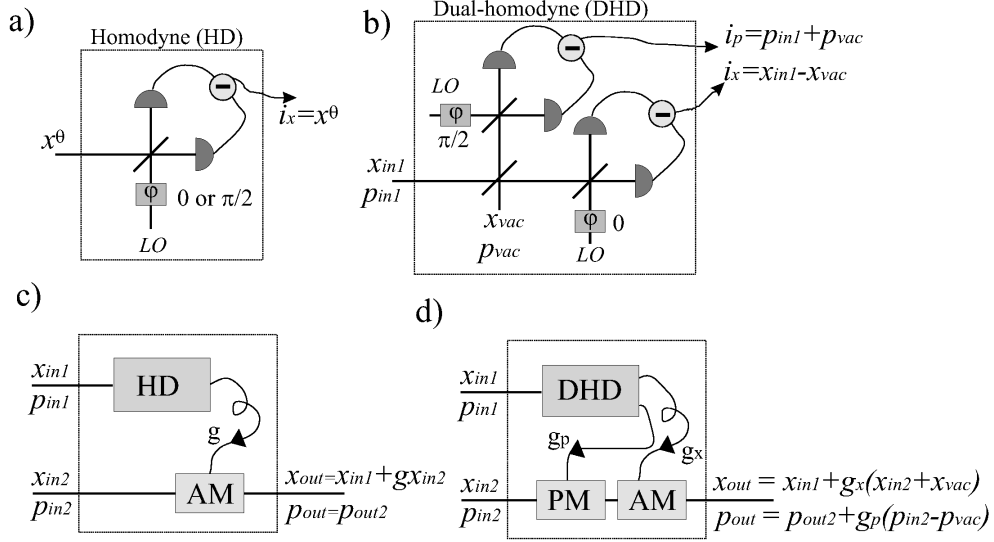


Figure 17.3. Schematic diagram of commonly used detector systems as well as simple feedforward systems.

distillation of highly entangled states from a Gaussian mixture as well as efficient quantum computation cannot be carried out with these Gaussian operations only. To enable these tasks one must resort to non-Gaussian transformations. Such transformations are experimentally quite challenging since an extremely high third-order nonlinearity is required. For example, for the generation of macroscopic superposition states, which might serve as a resource state for continuous variable quantum computing, by exploiting the Kerr effect in standard fiber one needs a loss- and noise-free optical fiber of about 1500 km to reach the required nonlinearity [28, 29]! Alternatively, using electromagnetic-induced transparency a giant Kerr effect can in principle be produced [30–32], but this technology has not yet reached the realm of quantum optics. Recently it was shown that by combining a “relatively low” Kerr nonlinearity with homodyne detection followed by a selection of the measurement outcomes and feed forward can enable the required nonlinearity [35]. However, this “low” nonlinearity is still too large for immediate experimental realization. Another approach to create large third-order nonlinearities is by photon counting and conditional measurements [33, 34]. This scheme, however, requires a highly efficient photon counting device, a technology which is still in its infancy.

17.4 Quantum Communication Protocols

With the above-mentioned tools at our disposal a whole range of different continuous variable quantum information protocols can be realized. The protocols can be roughly divided into two groups: one which relies on only Gaussian operations and one which requires, in addition to Gaussian operation, non-Gaussian operations. Most experimental work has so far been

devoted to protocols realizable with Gaussian operation, due to the relative simplicity of these operations. We will therefore mainly focus on this work and only very briefly in Section 17.4.3 discuss protocols relying on non-Gaussian operations.

17.4.1 Quantum dense coding

Dense coding is a protocol that enhances the communication capacity of a channel by the usage of entanglement. The protocol was originally proposed [40] and experimentally realized [41] for polarization encoded qubits (see also Chapter 16), and later on the idea was translated to the CV regime [42, 43]. It was shown that by using CV entanglement the classical channel capacity could ultimately be doubled.

Information is sent by encoding a message with distinguishable symbols onto physical entities, such as optical quantum states, and subsequently transmitting it to the receiver who employs a certain measurement strategy to extract the information. The symbols sent by Alice (A) is defined by the alphabet $A = \{a\}$ each member occurring with probability p_a , whereas the alphabet received by Bob (B) is given by $B = \{b\}$ with occurrence probabilities p_b [1]. Due to fundamental quantum noise of the information carriers as well as noise in the channel, the two alphabets are in general not identical. The interesting information theoretical parameter is the so-called mutual information, which quantifies the information A and B have in common. When classical information is encoded into quantum states, this quantity is given by

$$I_{\text{mutual}} = \sum \text{Tr}(\hat{E}_b \rho_a) \log \left(\frac{\text{Tr}(\hat{E}_b \rho_a)}{p_b} \right), \quad (17.7)$$

where $\text{Tr}(\hat{E}_b \rho_a) = p_{b|a}$ is the conditional probability (the probability that A sent the letter a if B received the letter b). $\hat{E}_b$ is an operator that characterizes the measurement strategy applied by B, examples being the standard homodyne and dual-homodyne detectors for which $\hat{E}_b = |x_\theta\rangle\langle x_\theta|$ and $\hat{E}_b = |\alpha\rangle\langle\alpha|$, respectively. Finally ρ_b is the density operator associated with the quantum states.

The channel capacity, which states the maximum achievable channel throughput per usage, is now found by maximizing the mutual information over the input alphabet and all possible measurement strategies:

$$C = \max_{p_a; E} I_{\text{mutual}} \quad (17.8)$$

In fact, due to the intrinsic indeterminacy of quantum mechanics, there is an upper bound on the mutual information, and therefore on the channel capacity. This famous bound, which is called the Holevo bound [44], puts a fundamental limit to the maximum information transfer. How can this limit be reached for continuous variable states?

Dealing with continuous variable states, the capacity can in principle be infinitely large because the phase space is infinitely large. Therefore in order to get a finite value on the capacity, we need to place some constraints on the usage of the channel. Because of the ever-growing traffic on optical communication lines, it is reasonable (and common) to assume that the mean power traveling down the channels per usage is constrained. Using this constraint on

the mean number of photons per usage, the best communication strategy, that is, the strategy that reaches Holevo's bound, is the one which make use of Fock state encoding [45]. If the sender uses a Fock state alphabet distributed according to a thermal distribution, the channel capacity is $C = (1 + \bar{n}) \ln(1 + \bar{n}) - \bar{n} \ln \bar{n}$ which is the optimal capacity for single channel communication ($\bar{n}$ is the mean photon number). Other nonoptimum choices of the input alphabets are the coherent state and the squeezed state alphabets. For these alphabets the maximal throughputs are $C_{\text{coherent}} = \ln(1 + \bar{n})$ and $C_{\text{squeezed}} = \ln 2 + \ln(\bar{n})$, respectively.

Now, if Alice and Bob share an entangled state, the channel throughput per usage can be higher than for the Fock state encoding; a protocol referred to as dense coding: Alice encodes information into her part of the EPR state, sends it to Bob, who obtains information about conjugate observables by combining the two parts of the EPR states on a beam splitter and performing homodyne measurements at the two outputs of the beam splitter. Because this protocol performs better than the Fock state protocol, at first sight the dense coding result seems to contradict the result of Holevo! However, it does not violate Holevo's theorem, because the shared state must also be conveyed from A to B, which means that it is a two-channel protocol. Information is, however, only sent in one channel, so the unencoded half of the EPR state can in principle be sent off-peak and stored although this technology has still to be developed.

The channel capacity for the dense coding protocol is given by

$$C_{\text{dense}} = \ln(1 + \bar{n} + \bar{n}^2). \quad (17.9)$$

This capacity is always larger than that for coherent state communication. The squeezed state protocol is however better than the dense coding protocols for a certain range of mean photon numbers and squeezing degrees. For $\bar{n} > 1$ squeezing degrees higher than 4.77 dB however assures that the dense coding beats the squeezed state protocol. Most interestingly the optimal single channel capacity is beaten only for a two-mode squeezing degree higher than 6.78 dB.

There have been some attempts to experimentally implement the dense coding protocol. Li *et al.* [46] used bright squeezed beams to generate entanglement via a 50:50 beam splitter. One half of the entangled state was modulated both in amplitude and phase quadrature and subsequently sent to Bob. The state was then combined with the other half of the entangled state on a 50:50 beam splitter and finally the output states were measured directly and the difference and sum currents were produced to yield information about the amplitude and phase quadrature below the shot noise limit. Mizuno *et al.* [47] performed a similar experiment, but with "vacuum" entangled state (that is entangled states without a carrier) rather than bright entangled states. Both experiments performed better than the coherent state protocol; however dense coding was not demonstrated because of lack of quantum correlations.

17.4.2 Quantum key distribution

By means of quantum key distribution (QKD) followed by one-time pad, two authenticated parties (Alice and Bob) can, in principle, exchange confidential information with unconditional security independent of the technological power of an eavesdropper (Eve) who might interfere with the conveyed signal. Correlations between the legitimate users are established by sending quantum states from Alice to Bob through an insecure channel (controlled by Eve).

These quantum correlations are turned into a set of classically correlated symbols, a set which is partly determined by the specific measurement strategy. Subsequently, by the use of an authenticated public channel and classical algorithms Alice and Bob can distil from their list of partially correlated data a secret key about which Eve has only negligible information.

There are normally two approaches to QKD; one which is relying on shared entanglement between Alice and Bob [48] and one which involves the sending of nonorthogonal states and measurements in conjugate bases [49] (see Chapter 16 for a discussion on these approaches in the discrete variable regime). For continuous variables only the latter has been implemented experimentally, and therefore only this one will be subject to discussion in the following. (We should however note that the two schemes can be treated under equal footing since the correlations obtained by Alice and Bob can be modeled as if they had shared an entangled state [50].) The scheme is referred to as a prepare & measure scheme since Alice prepares nonorthogonal states chosen randomly from a predefined set of states, she sends it to Bob who measures the states in conjugate bases: e.g., the amplitude and the phase quadrature bases. In the original CV QKD prepare & measure proposal information was encoded into a discrete [53–55] (or continuous [56]) set of squeezed or entangled states and randomly measuring the amplitude and phase quadrature. Only later it was realized that coherent state encoding and homodyne detection also serves as an interesting route to secure QKD [6, 59]. Note that the new ingredient in these proposals was the detection system at the receiver, namely homodyne detection. Coherent state encoding was already proposed in 1992 by Bennett [51], and recently a slightly modified protocol was proven to be unconditionally secure [52].

The idea of using coherent state and homodyne detection as a mean of QKD was first put forward by Ralph [57] and further elaborated on by Grosshans and Grangier [58], but they came to the conclusion that the scheme was only secure if the losses in the channel were less than 50%: If the loss exceeds 50%, the mutual information between an eavesdropper (who measured the part that would have been leaking into the environment and replaces the lossy channel with a perfect one) and Alice was higher than that between Bob and Alice, rendering the protocol insecure. However, this apparent “3 dB” penalty was overcome using classical distillation techniques, namely postselection [59] or reverse reconciliation [6].

The first experimental demonstration of CV QKD was performed by Hirano *et al.* [5] and by Grosshans *et al.* [6]. In the former experiment information was encoded into four different coherent states in a BB84-type encoding strategy, whereas the latter experiment relies on a Gaussian distribution of coherent states. In this experiment Alice continuously varies the amplitude and phase quadrature and Bob randomly measures these quadratures using fast homodyne detection. Using the reverse reconciliation algorithm, Bob then converts the continuous data set into a secret binary key. There has been several other implementations of CV QKD: Lorenz *et al.* [60] used a BB84-type strategy followed by post selection as did Hirano *et al.* [5], but instead of using the quadrature amplitudes the Stokes parameters served as the encoding variables. Recently this experiment was simplified by considering only a two-state protocol [61]. Lance *et al.* [62] implemented a protocol where Bob performs dual homodyning; in terms of security there is no need of switching between x - and p -basis as realized by Weedbrook *et al.* [63]. Lodewyck *et al.* [65] and Legre *et al.* [66] have implemented a fiber based QKD scheme operating at the telecommunication wavelength of 1.5 μm .

When a certain QKD scheme is designed, the next question that arises is whether the scheme is secure against eavesdropping attacks. Normally, three different levels of attacks are

considered: (1) Individual attack: Eve couples each state to a probe, and stores the state in a quantum memory until Bob reveals the measurement basis. She then measures each probe independently of the others. (2) Collective attack: Eve again interacts individually with all the signal states but now all the probes are stored in a big quantum memory and after the classical communication she measures all the probes jointly in complex generalized measurement that extracts maximum information. (3) Coherent attack: Eve couples a preentangled multimode probe with all the states sent from Alice to Bob. This highly dimensional state is stored in a large quantum memory and after classical authentication, Eve uses an optimal strategy to extract information. In the literature there are various proofs for security on different levels. Individual attacks are considered in [56, 58, 59, 63, 64, 67], the collective attack in [68, 69], and the coherent attacks in [70, 71].

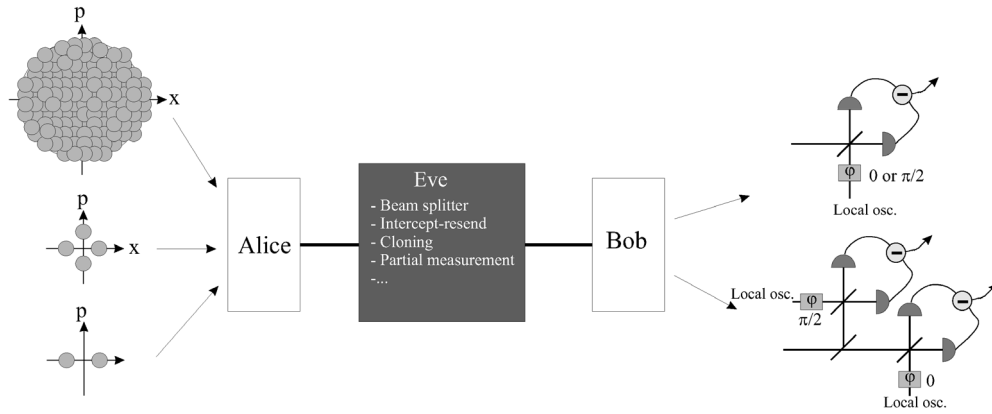


Figure 17.4. Continuous variable quantum key distribution based on coherent state encoding and homodyne detection. The system is basically divided into three parts: (a) A preparation stage where Alice encodes information into the states, (b) a sending stage where the state is in the possession of Eve and (c) a receiving stage where Bob turns the quantum states into classical numbers. The input alphabet may consist of a continuous Gaussian distribution or a discrete distribution (two or four states) of coherent state, and Bob may use either a homodyne detector which switches between measuring conjugate quadratures or he may measure conjugate quadratures simultaneously using a dual-homodyne detector.

17.4.3 Long distance communication

Quantum information must be distributed via quantum channels, that is channels preserving the quantumness (or quantum information) of the state. Examples of quantum communication channels are free space and fibers. However, these channels are in practice imperfect because they are lossy. One way of diminishing the losses is to use an appropriate wavelength: silica fibers possess low loss at $1.55 \mu\text{m}$ whereas free-space communication is best at around 800 nm . For communication outside the earth's atmosphere, where scattering losses are almost nonexistent, any wavelength can be used.

The bottom line is, however, that long-distance quantum communication is not possible with the losses in present day communication channels. Naively one might think that a way around this is to amplify the state. But, according to basic quantum mechanical considerations, amplification is not possible without the introduction of noise which in turn demolishes the quantum coherence.

So what does this mean? Is quantum communication confined to short distances only? The answer is no. By using a quantum repeater one can, in principle, extend the communication channel to arbitrary long distances [72]. Such a device, is however, quite challenging since it requires the combination of quantum teleportation, a quantum memory and entanglement distillation. Teleportation is a protocol that enables the communication of quantum information via a classical channel (e.g., via a mobile phone) between two parties that share an entangled state [18], and a quantum memory is a device that can store quantum coherence. The former protocol was described in Chapter 14 and the latter was the subject of Chapter 26. Entanglement distillation is a way to distil, from a large ensemble of weakly entangled states, a smaller ensemble of highly entangled states. This protocol, in contrast to the teleporter and the memory, requires the use of non-Gaussian operations.

By combining these three protocols we can build a quantum repeater [72]: Let us assume that quantum information is to be sent from A to C. There is a person B in between. An entangled state is then sent to A and B from the midpoint, using a realistic, that is imperfect, channel. The entanglement is subsequently distilled using non-Gaussian operations. The distilled states are then stored in quantum memories. The same protocols are performed between B and C. Now, the entanglement between B and C is used to teleport perfectly the half of the entangled state that B has, and consequently, A and B share an entangled pair which finally can be used to faithfully transmit (teleport) quantum information. The full construction of such a quantum repeater is experimentally very challenging, but also a very active field of research. Alternative routes to long distance communication include a protocol based on photon storage in atomic ensembles [74] and a scheme which is based on photon emission from solid-state devices [73].

Exercises

1. Calculate the expectation values of the first and second moments $\langle \hat{x} \rangle$, $\langle \hat{x}^2 \rangle$, $\langle \hat{p} \rangle$ and $\langle \hat{p}^2 \rangle$ as well as the variances $\langle \Delta \hat{x}^2 \rangle$, and $\langle \Delta \hat{p}^2 \rangle$ for the following states:

$$(a) \quad |\Phi\rangle = |0\rangle \quad (17.10)$$

$$(b) \quad |\Phi\rangle = \frac{1}{\sqrt{1+\epsilon^2}}|0\rangle + \epsilon|1\rangle \quad (17.11)$$

$$(c) \quad |\Phi\rangle = \frac{1}{\sqrt{1+\epsilon^2}}|0\rangle + \epsilon|2\rangle \quad (17.12)$$

[Note: $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$ and $\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$.] ϵ is a complex number characterizing the state. For $\epsilon \ll 1$ b) corresponds to a weak coherent state and c) to a squeezed state.

2. Use the input–output relations in Fig. 17.2 and 17.3 to show that

- (a) the entanglement source (row 5 in Fig. 17.2) can be built using two squeezing sources (with equal squeezing degrees), a phase shifter (with $\theta = \pi/2$), and a symmetric beam splitter ($R = T = 0.5$). See Fig. 17.5a.
- (b) the amplifier (row 6 in Fig. 17.2) can be built using a beam splitter, a dual-homodyne detector followed by feedforward. See Fig. 17.5b. Note that the electronic gains can be set freely in order to enable the required transformation.

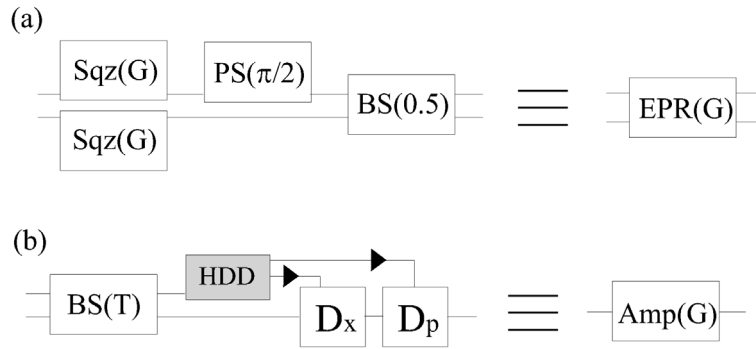


Figure 17.5. Implementation of an entangler and an amplifier using alternative approaches.

References

- [1] S.L. Braunstein and P. van Loock, *Rev. Mod. Phys.* **77**, 513 (2005).
- [2] S.L. Braunstein and A.K. Pati (eds.), *Quantum Information Theory with Continuous Variables* (Kluwer, Dordrecht, 2003).
- [3] N.J. Cerf, G. Leuchs, and E. Polzik (eds.), ().
- [4] A. Furusawa, J.L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, *Science* **282**, 706 (1998).
- [5] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, *Phys. Rev. A* **68**, 042331 (2003).
- [6] F. Grosshans, G.V. Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, *Nature* **421**, 238 (2003).
- [7] A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, and P.K. Lam, *Phys. Rev. Lett.* **92**, 177903 (2004).
- [8] B. Julsgaard, J. Sherson, J. Fiurasek, I. Cirac, and E. Polzik, *Nature* **432**, 482 (2004).
- [9] U.L. Andersen, V. Josse, and G. Leuchs, *Phys. Rev. Lett.* **94**, 240503 (2005).
- [10] S. Koike, H. Takahashi, H. Yonezawa, N. Takei, S.L. Braunstein, T. Aoki, and A. Furusawa, *Phys. Rev. Lett.* **96**, 060504 (2006).
- [11] U.L. Andersen, O. Glöckl, S. Lorenz, G. Leuchs, and R. Filip, *Phys. Rev. Lett.* **93**, 100403 (2004).

- [12] U.L. Andersen, R. Filip, J. Fiurasek, V. Josse, and G. Leuchs, *Phys. Rev. A Rapid Commun.* **72**, 060301 (2005).
- [13] D.F. Walls, and G.J. Milburn, *Quantum Optics* (Springer, Berlin 1995).
- [14] W. Schleich, *Quantum Optics in Phase Space* (Wiley-VCH Verlag Berlin, 2001).
- [15] U. Leonhardt, *Measuring the Quantum State of Light*, (Cambridge University Press, Cambridge, MA, 1997).
- [16] M. Scully and M.S. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, MA, 1997).
- [17] H.-A. Bachor and T. Ralph, *A Guide to Experiments in Quantum Optics* (Wiley-VCH, Berlin 2004).
- [18] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [19] X. Jia, X. Su, Q. Pan, J. Gao, C. Xie, and K. Peng, *Phys. Rev. Lett.* **93**, 250503 (2004).
- [20] S. Lloyd and S.L. Braunstein, *Phys. Rev. Lett.* **82**, 1784 (1999).
- [21] S.D. Bartlett, B.C. Sanders, S.L. Braunstein, and K. Nemoto *Phys. Rev. Lett.* **88**, 097904 (2002).
- [22] S.D. Bartlett and B.C. Sanders, *Phys. Rev. A* **65**, 042304 (2002).
- [23] R. Filip, P. Marek, and U.L. Andersen, *Phys. Rev. A* **71**, 042308 (2005).
- [24] P.K. Lam, T.C. Ralph, E.H. Huntington, and H.A. Bachor, *Phys. Rev. Lett.* **79**, 1471 (1997).
- [25] V. Josse, M. Sabuncu, N. Cerf, G. Leuchs, and U.L. Andersen, *Phys. Rev. Lett.* **96**, 163602 (2006).
- [26] H.M. Wiseman, *Phys. Rev. A* **49**, 2133 (1994).
- [27] H. Yuen and V. Chan, *Opt. Lett.* **8**, 177 (1983).
- [28] C.C. Gerry, *Phys. Rev. A* **59**, 4095, (1999).
- [29] B.C. Sanders and G.J. Milburn, *Phys. Rev. A* **45**, 1919 (1992).
- [30] H. Schmidt and A. Imamoglu, *Opt. Lett.* **21**, 1936 (1995).
- [31] M.D. Lukin and A. Imamoglu, *Phys. Rev. Lett.* **84**, 1419 (2000).
- [32] L.V. Hau, S.E. Harris, Z. Dutton, and C.H. Behroozi, *Nature* **397**, 594 (1999).
- [33] M. Dakna, T. Anhut, T. Opatrný, L. Knöll, and D.-G. Welsch *Phys. Rev. A* **55**, 3184 (1997).
- [34] E. Knill, R. Laflamme, and G.J. Milburn, *Nature* **409**, 46 (2001).
- [35] H. Jeong, M.S. Kim, T.C. Ralph, and B.S. Ham, *Phys. Rev. A* **70**, 061801(R) (2004).
- [36] Z.Y. Ou, S.F. Pereira, H.J. Kimble, and K.C. Peng *Phys. Rev. Lett.* **68**, 3663 (1992).
- [37] Ch. Silberhorn, P.K. Lam, O. Weiß, F. König, N. Korolkova, and G. Leuchs *Phys. Rev. Lett.* **86**, 4267 (2001).
- [38] C.M. Caves, *Phys. Rev. D* **26**, 1817 (1982).
- [39] E. Arthurs and M. S. Goodman, *Phys. Rev. Lett.* **60**, 2447 (1988).
- [40] C. H. Bennett and S.J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
- [41] K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger, *Phys. Rev. Lett.* **76**, 4556 (1996).
- [42] M. Ban, *J. Opt. B: Quantum Semiclass. Opt.* **1**, L9 (1999).

- [43] S.L. Braunstein and H.J. Kimble, Phys. Rev. A **61**, 042302 (2000).
- [44] A.S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
- [45] H.P. Yuen and M. Ozawa, Phys. Rev. Lett. **70**, 363 (1993).
- [46] X. Li, Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng, Phys. Rev. Lett. **88**, 047904 (2002).
- [47] J. Mizuno, K. Wakui, A. Furusawa, and M. Sasaki, Phys. Rev. A **71**, 012304 (2005).
- [48] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [49] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal processing, Bangalore, India* (IEEE, New York), 175 (1984).
- [50] C.H. Bennett, G. Brassard, and N. David Mermin Phys. Rev. Lett. **68**, 557 (1992).
- [51] C. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
- [52] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
- [53] T. Ralph, Phys. Rev. A **61**, 010303 (1999).
- [54] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
- [55] M. Reid, Phys. Rev. A **62**, 062308 (2000).
- [56] N.J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
- [57] T.C. Ralph, Phys. Rev. Lett. **88**, 057902 (2000).
- [58] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
- [59] Ch. Silberhorn, T.C.Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
- [60] S. Lorenz, N. Korolkova and G. Leuchs, Appl. Phys. B, **79**, 273 (2004).
- [61] C. Lorenz, J. Rigas, M. Heid, U.L. Andersen, N. Lütkenhaus, and G. Leuchs, *Preprint* quant-ph/0603271
- [62] A.M. Lance, T. Symul, V. Sharma, C. Weedbrook, T.C. Ralph, and P.K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
- [63] A. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph, and P.K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
- [64] R. Namiki and T. Hirano, Phys. Rev. Lett. **92**, 117901 (2004).
- [65] J. Lodewyck, T. Debuisschert, R. T.-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303 (2005).
- [66] M. Legre, H. Zbinden, N. Gisin, *Preprint* quant-ph/0511113
- [67] F. Grosshans and N.J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
- [68] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).
- [69] M. Navascues and A. Acin, Phys. Rev. Lett. **94**, 020505 (2005).
- [70] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
- [71] S. Iblisdir, G. Van Assche, and N.J. Cerf, Phys. Rev. Lett. **93**, 170502 (2004).
- [72] H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
- [73] L. Childress, J.M. Taylor, A.S. Sørensen, and M.D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).
- [74] L.M. Duan, M.D. Lukin, J.I. Cirac, and P. Zoller, Nature **414**, 413 (2001).

Part V

Quantum Computing: Concepts

18 Requirements for a Quantum Computer

Artur Ekert and Alastair Kay

The classical theory of computation usually does not refer to physics. Pioneers such as Turing, Church, Post, and Gödel managed to capture the correct classical theory by intuition alone and, as a result, it is often falsely assumed that its foundations are self-evident and purely abstract. They are not!

Computers are physical objects and computation is a physical process. Hence, when we improve our knowledge about physical reality, we may also gain new means of improving our knowledge of computation. From this perspective it should not be very surprising that the discovery of quantum mechanics has changed our understanding of the nature of computation.

18.1 Classical World of Bits and Probabilities

We tend to view computation as an operation on abstract symbols. Any finite set of symbols is called an alphabet and any finite sequence of symbols from that alphabet is called a string. Here, without any loss of generality, we will use the binary alphabet $\{0, 1\}$. We shall denote the set of all 2^n possible binary strings of length n as $\{0, 1\}^n$. Binary digits can be added, $\oplus$, and multiplied, $\times$, as

$$\begin{array}{llll} 0 \oplus 0 = 0, & 0 \oplus 1 = 1, & 1 \oplus 0 = 1, & 1 \oplus 1 = 0, \\ 0 \times 0 = 0, & 0 \times 1 = 0, & 1 \times 0 = 0, & 1 \times 1 = 1. \end{array}$$

The addition is also known as the logical XOR (exclusive OR) and the multiplication as the conjunction or the logical AND ($\wedge$). Given two binary strings, x and y , we can add them bit by bit, e.g., $x = 0110$ and $y = 1100$ can be added as $x \oplus y = 1010$. Note that for any binary string x , $x \oplus x = 0$.¹ We can also view a string of n bits as a vector of n binary components and define the inner product by the standard rule of multiplying corresponding components and summing the results, e.g., $x \cdot y = (0110) \cdot (1100) = 1$.

From a mathematical perspective, a computer is an abstract machine that evaluates a function

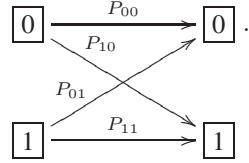
$$f : \{0, 1\}^n \mapsto \{0, 1\}^m,$$

i.e., given n bits of input it produces m bits of output. Such a function is equivalent to m functions, each with a one-bit output, known as Boolean functions,

$$f : \{0, 1\}^n \mapsto \{0, 1\}.$$

¹The set $\{0, 1\}^n$ together with the addition $\oplus$ forms an Abelian group Z_2^n .

Thus, one might as well say that computers evaluate Boolean functions. There are 2^{2^n} deterministic Boolean functions acting on n bits. We shall start our discussion with the simplest one. Consider the most general computing machine that performs a computation on one bit, i.e., it maps $\{0, 1\}$ to itself. The action of the machine may be represented by the diagram,



This machine has the property such that if we prepare the input with the value j ($j = 0$ or 1) and then measure the output, we obtain the value i ($i = 0$ or 1) with probability P_{ij} . More generally, if we prepare the input j with probability p_j , then we obtain the output i with probability $p'_i = \sum_j P_{ij} p_j$. It is convenient to tabulate the transition probabilities and express the action of the machine in a matrix form²

$$\begin{pmatrix} p'_0 \\ p'_1 \end{pmatrix} = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}.$$

OUTPUT $\leftarrow$ EVOLUTION $\leftarrow$ INPUT.

The state of a physical bit, e.g., the input or the output, is described by the probability vector and its evolution by a transition matrix. The transition matrix has nonnegative elements P_{ij} satisfying the standard probability conditions $\sum_i P_{ij} = 1$, i.e., entries in each column add up to one, which means that each column can be viewed as a probability vector. Such matrices are called stochastic. For example, here are five stochastic matrices; the first four describe all possible deterministic limits of a one bit computation and the fifth one describes a completely random switch.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

IDENTITY NEGATION CONSTANT 0 CONSTANT 1 RANDOM SWITCH.

The identity, negation, and random switch matrices are, in fact, doubly stochastic, meaning that both their rows and columns add to 1. In general, stochastic matrices may have different numbers of rows and columns. For example, probability vectors can be viewed as single-column-stochastic matrices. Any machine evaluating a function $f : \{0, 1\}^n \mapsto \{0, 1\}^m$ can

²All diagrams are to be read from left to right, but when we write matrices and vectors the order is reversed. It is an unfortunate but well-established convention, so beware of the possibility of confusion.

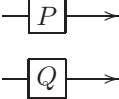
be described by a $2^m \times 2^n$ stochastic matrix with entries P_{ij} , where the input $j \in \{0, 1\}^n$ and the output $i \in \{0, 1\}^m$. In particular, if the evolution of the machine is deterministic, then the entries P_{ij} take only two values, zero and one, and the matrix can also be used to define the function f , instead of, for example, a truth table. Let us also mention that any computation can be embedded into reversible computation. For any function f taking n bits to m , there exists an invertible function $\bar{f}$ taking $n + m$ bits to $n + m$ which evaluates f as

$$\bar{f} : (x, y) \longrightarrow (x, y \oplus f(x)).$$

Initially, the input string $j = (x, y) \in \{0, 1\}^{n+m}$ is a concatenation of two strings: the first n bits represent the string x and the remaining m bits are set to represent an arbitrary string y . After the function evaluation the output $i = (x, y \oplus f(x))$ is a concatenation of two strings; the first n bits still represent x but the remaining m bits are set to the value $y \oplus f(x)$. If you run the computation again, the string $i = (x, y \oplus f(x))$ will evolve to $(x, y \oplus f(x) \oplus f(x))$ which is equal to the initial (x, y) . Consequently, and without any loss of generality, we can focus on machines performing reversible computations, where all the matrices describing the evolution are square.

It seems obvious that *any* machine whose action depends on no other input or stored information and which performs a computation on a single bit is described by some 2×2 stochastic matrix. In general, we may conjecture that any machine which performs a computation on a physical system with N distinguishable states is described by some $N \times N$ stochastic matrix. The entries of such matrices can be derived from the laws of physics governing the dynamics of machines. We may not know their specific values but at least we know they exist. This is a very reasonable conjecture, so let us have a closer look at some of its consequences.

Given two independent machines described by the stochastic matrices P and Q , we can make them work together either in parallel or in sequence. The resulting, composed, machines are described by some new stochastic matrices which are denoted as $P \otimes Q$ and QP , respectively,

PARALLEL	SEQUENTIAL
	
$P \otimes Q$	QP

The entries in the new stochastic matrices can be calculated following a few simple rules, or axioms if you wish, of classical probability theory. They state that with any event E one

can assign a number $P(E)$ between 0 and 1 such that if E represents a definite event, then $P(E) = 1$. Moreover, probabilities are added for mutually exclusive events and multiplied for independent events.

- If E_1 and E_2 are mutually exclusive events, then the probability of the event (E_1 or E_2) is the sum of the probabilities of the constituent events,

$$p(E_1 \cup E_2) = p(E_1) + p(E_2).$$

- If E_1 and E_2 are independent events, then the probability of the event (E_1 and E_2) is the product of the probabilities of the constituent events,

$$p(E_1 \cap E_2) = p(E_1)p(E_2).$$

It is worth stressing that independence and mutual exclusivity are different. Two independent events can both occur in the same trial, whereas two mutually exclusive events cannot. In our case, individual machines act independently from each other, be it in parallel or in sequence, and events such as two transitions from the same initial state to different final states cannot both occur at the same time, and are thus mutually exclusive.

18.1.1 Parallel composition = tensor products

When we bring together a system with N states labeled by $n = 0, 1, \dots, N - 1$ ³ and a system with M states labeled by $m = 0, 1, \dots, M - 1$, we form a composite system with NM states labeled by pairs of labels (n, m) . For example, if we bring together two bits, we obtain a system with four states which can be labeled as $(0, 0)$, $(0, 1)$, $(1, 0)$, and $(1, 1)$. The composite labels such as (n, m) are often written simply as strings nm , and it should be clear from the context that it is a concatenation of two symbols and not a product of two numbers. In the two bit case we write the composite labels as binary strings 00, 01, 10, and 11.

Now, let us suppose you prepare the input of the first system with the value n and that of the second one with the value m , and let P act on the first system and Q on the second one. Your chance of observing the output (k, l) , i.e., the first system in k and the second in l , is $P_{kn}Q_{lm}$. This is because the actions of the two machines are independent, and thus the probability that transitions n to k in the first machine and m to l in the second machine will happen is the product of the two, i.e., $P_{kn}Q_{lm}$. The $NM \times NM$ stochastic matrix that describes transitions in the composed system between (n, m) and (k, l) is written as $P \otimes Q$ and has matrix elements $(P \otimes Q)_{kl, nm} = P_{kn}Q_{lm}$. The symbol $\otimes$ stands for the tensor product of two matrices. Our definition of $P \otimes Q$ can be applied to any two matrices P and Q regardless of their shape and properties. This includes any two vectors since they can be viewed as matrices with just one column. In particular, if the first system is described by the probability vector p with components p_n and the second one by the probability vector q with components q_m and if the two systems are independent, then the composed system is described by the tensor product vector $p \otimes q$ with NM components $(p \otimes q)_{nm} = p_n q_m$. Here

³Which are the equivalent decimal representations of all binary strings $\{0, 1\}^{\log_2 N}$.

is an example of a tensor product of two vectors p and q , and a tensor product of a 3×2 matrix A with entries A_{ij} and any matrix B (the $A \otimes B$ matrix has a characteristic block form)

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \otimes \begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{pmatrix}, \quad A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B \\ A_{21}B & A_{22}B \\ A_{31}B & A_{32}B \end{pmatrix}.$$

It should be stressed, however, that not all probability vectors of composed systems and not all stochastic matrices operating on such systems can be written as tensor products. For example, consider two bits and a controlled-NOT operation defined as follows: flip the bit value of the second bit if the first bit has value 1 and do nothing otherwise. This operation can correlate the two bits, i.e., evolve a probability vector which is a tensor into a probability vector which is not,

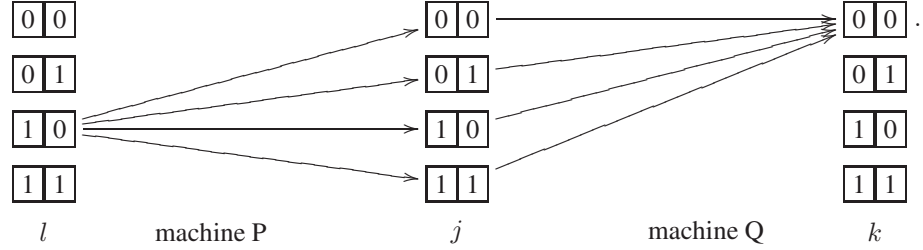
$$\begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Following some manipulation, you will see that neither the controlled-NOT nor the correlated probability vector at the output admit a tensor product decomposition. As we shall soon see, a similar, but much more subtle, effect called entanglement will be responsible for many counter-intuitive features of quantum theory.

18.1.2 Sequential composition = matrix products

If a machine P is followed by another machine Q , the resulting machine is described by the matrix product QP (note the order in which we multiply the matrices). This follows from the axiom which asserts that the probability of mutually exclusive events add up.

We may argue that any transition between input $l \in \{0, 1\}^n$ and output $k \in \{0, 1\}^n$ in the composite machine can happen in 2^n mutually exclusive ways, namely through 2^n intermediate states $j \in \{0, 1\}^n$. The probability that the input l evolves into the output k via the intermediate states j is given by $\sum_j Q_{kj} P_{jl}$. Reading from right to left, we see that first l evolves into j with the probability P_{jl} and subsequently j evolves into k with the probability Q_{kj} . The probability for this particular transition is $Q_{kj} P_{jl}$. If we vary j , we obtain alternative paths connecting the input l with the output k . Thus, we must sum over all values j . Consequently, the stochastic matrix of the new machine is the matrix product QP with entries $\sum_j Q_{kj} P_{jl}$. For example, the diagram below illustrates our discussion in the case of two machines operating on two bits.



The probability of the $(10) \rightarrow (00)$ transition can be written as $\sum_{j=\{0,1\}^2} Q_{00,j} P_{j,10}$.

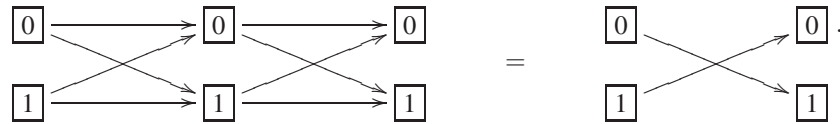
Here we have made a tacit assumption that the matrices P and Q act on the same number of bits. If this is not the case, we can always make them act on the same number by introducing the identity operation in parallel to the smaller machine. For example, if P acts on N bits, and Q acts on the first $M = N - 1$ bits, then the stochastic matrix describing the overall evolution is given by

$$\left[Q \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right] P.$$

In summary, when we compose two independent machines in parallel, we take tensor products and when in sequence, we take matrix products. The results are new stochastic matrices. The tensor product is associative, $P \otimes Q \otimes R = (P \otimes Q) \otimes R$, so we can extend machines to act on any number of bits. This way, we can construct stochastic matrices of complicated machines composed of many elementary sub-machines and view them as computers made of elementary gates. Does this approach describe all possible computations?

18.2 Logically Impossible Operations?

It seems obvious that all possible computations are described by stochastic matrices. Surprisingly, this is not the case—the physical dynamics can be more subtle. In order to see this, let us define two new machines. We will call the first one the square root of NOT, also written as $\sqrt{\text{NOT}}$, because when this particular machine is followed by another, identical machine, the output is always the negation of the input. The flow of probabilities in such a machine can be expressed schematically as



The second machine will be called the square root of SWAP. The SWAP operation interchanges the bit values of two bits, e.g., $00 \mapsto 00$, $01 \mapsto 10$, $10 \mapsto 01$, $11 \mapsto 11$. The square root of SWAP ($\sqrt{\text{SWAP}}$) operates on two bits in such a way that two consecutive applications

result in the full SWAP. Note that the $\sqrt{\text{SWAP}}$ is the identity when restricted to inputs 00 and 11 and acts as the $\sqrt{\text{NOT}}$ when restricted to inputs 01 and 10. Thus, once we find a stochastic matrix for the $\sqrt{\text{NOT}}$ we will be able to construct a stochastic matrix for the $\sqrt{\text{SWAP}}$.

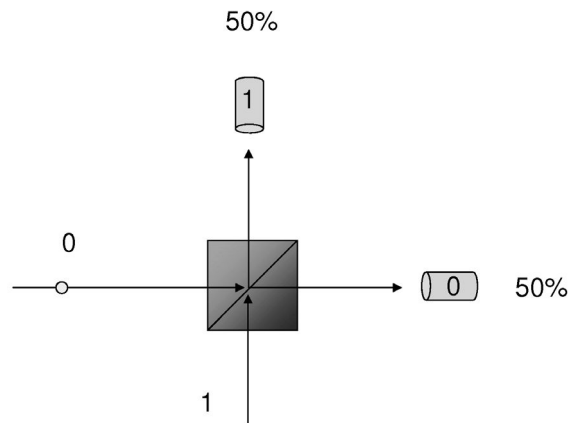
Suppose the square root of NOT is indeed described by some stochastic matrix P . The matrix product $PP = P^2$ should give a stochastic matrix corresponding to the logical NOT. This leads to contradiction because

$$\begin{aligned} PP &= \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} \\ &= \begin{pmatrix} P_{00}^2 + P_{01}P_{10} & P_{01}(P_{00} + P_{11}) \\ P_{10}(P_{00} + P_{11}) & P_{11}^2 + P_{10}P_{01} \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \end{aligned}$$

recalling that $P_i \geq 0$. There is no stochastic matrix P such that P^2 gives the logical NOT. A similar line of arguments shows that there is no stochastic matrix for the square root of SWAP. Thus, the square root of NOT is logically impossible, and so is the square root of SWAP.

It may seem reasonable to argue that since there is no such operation in logic, the $\sqrt{\text{NOT}}$ and the $\sqrt{\text{SWAP}}$ machines cannot exist. But they do exist! Some of them are as simple as half-silvered mirrors.

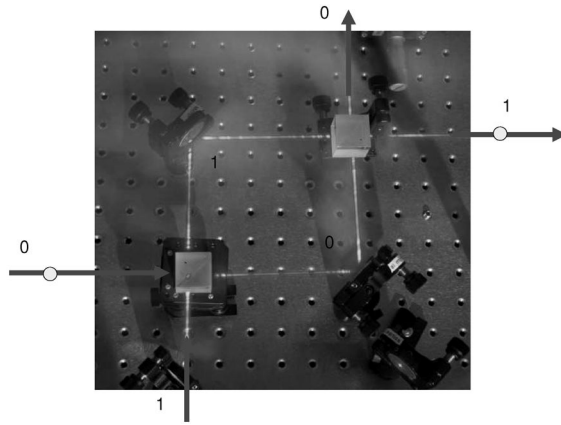
A symmetric beam splitter is a half-silvered mirror that reflects half the light that impinges upon it, while allowing the remaining half to pass through unaffected. It has two input ports and two output ports. We label the two input ports and the two output ports by “0” and “1” as shown below.



Let us aim a single photon⁴ at such a beam splitter using one of the input ports, e.g., port “0.” What happens? One thing we know is that the photon doesn’t split in two: We can place

⁴For the purpose of this introduction, we have selected the particle to be a photon and we have neglected issues related to second quantization. However, if one is prepared to ignore experimental details, the discussion presented here is equally valid for neutrons, electrons, atoms, ions, or molecules.

photodetectors wherever we like in the apparatus, fire in a photon, and verify that if any of the photodetectors registers a hit, none of the others do. In particular, if we place a photodetector behind the beam splitter in each of the two possible exit beams, the photon is detected with equal probability at either detector, no matter whether the photon was initially fired from input port “0” or “1.” You may conclude that the beam splitter is just a random switch. Moreover, it may seem obvious that at the very least, the photon is *either* in the transmitted beam “0” *or* in the reflected beam “1” during any single run of this experiment. However, that is not necessarily the case. Let us introduce a second beam splitter and let us place two normal mirrors so that both paths intersect at the second beam splitter.



If we assume that a beam splitter is a random switch, then a simple matrix multiplication of stochastic matrices shows that a concatenation of two beam splitters is also a random switch,

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

This makes perfect sense, apart from the fact that if we set up such an experiment, it is not what happens! It turns out that in the arrangement shown above, i.e., when the optical paths between the two beam splitters are the same, the photon *always* strikes detector 1 and *never* detector 0. Thus a beam splitter acts as the square root of NOT gate.

Is there something wrong with our reasoning here? Why does probability theory fail to predict the outcome of this simple experiment? One thing that is wrong is the assumption that the processes that lead the photon from the initial state to detector 0 are *mutually exclusive*. In reality, the photon must, in some sense, have traveled both routes at once! Another important issue is the status of probability theory. There is no reason why probability theory, or any other a priori mathematical construct, should make any meaningful statements about outcomes of physical experiments. For this we need a physical theory—knowledge that is created as the result of conjectures, experimentation, and refutations. Enter quantum mechanics!

18.3 Quantum World of Probability Amplitudes

In order to calculate probabilities that agree with experimental data, we must introduce the concept of *probability amplitudes*—complex numbers α such that the quantities $|\alpha|^2$ are interpreted as probabilities. Probability amplitudes are added for mutually exclusive events and multiplied for independent events. In particular the rule of additivity of probability amplitudes replaces the classical axiom of additivity in probability theory, and it is this simple rule which sets the quantum and the classical worlds apart. It states:

Additivity of probability amplitudes

If a particular event can happen in several alternative ways, then the overall probability amplitude for the event is the sum of the probability amplitudes for each of the constituent events considered separately.

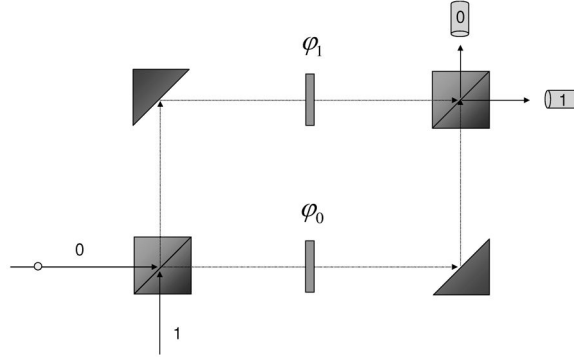
This is basically the essence of quantum mechanics—the rest is just a set of convenient mathematical tools developed for the purpose of book-keeping of probability amplitudes.

In order to see this rule in action, consider an event that can happen in two alternative ways with probability amplitudes α_1 and α_2 , respectively. It is convenient to write these two complex numbers in terms of their moduli and phase factors: $\alpha_1 = |\alpha_1|e^{i\phi_1}$ and $\alpha_2 = |\alpha_2|e^{i\phi_2}$. The probability amplitude of this event is $\alpha_1 + \alpha_2$ and the probability P of the event is then given by

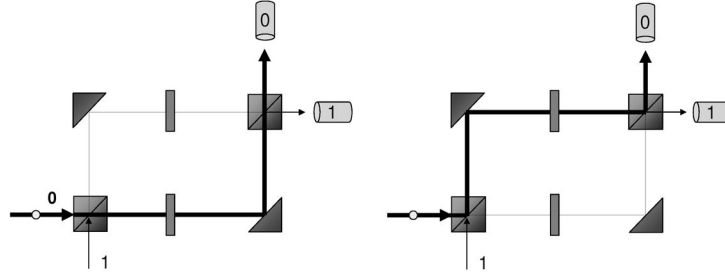
$$\begin{aligned} P &= |\alpha_1 + \alpha_2|^2 = |\alpha_1|^2 + |\alpha_2|^2 + \alpha_1\alpha_2^* + \alpha_1^*\alpha_2 \\ &= |\alpha_1|^2 + |\alpha_2|^2 + 2|\alpha_1||\alpha_2|\cos(\phi_1 - \phi_2) \\ &= P_1 + P_2 + 2|\alpha_1||\alpha_2|\cos(\phi_1 - \phi_2). \end{aligned}$$

The very last term on the right-hand side marks the departure from the classical theory of probability. The probability of any two mutually exclusive events is the sum of the probabilities of the individual events, $P_1 + P_2$, modified by what is called the interference term, $2|\alpha_1||\alpha_2|\cos(\phi_1 - \phi_2)$. Depending on the relative phase $\phi_1 - \phi_2$, the interference term can be either negative (destructive interference) or positive (constructive interference), leading to either suppression or enhancement of the total probability P . Note that the important quantity is the relative phase $\phi_1 - \phi_2$ rather than the absolute values ϕ_1 and ϕ_2 . These phases can be very fragile and may fluctuate rapidly due to spurious interactions with the environment. In this case, the interference term may average to zero and we recover the classical addition of probabilities. This phenomenon is known as *decoherence*. It is very conspicuous in physical systems made of many interacting components and is chiefly responsible for our classical description of the world—without interference terms we may as well add probabilities instead of amplitudes. However, there are many beautiful experiments in which we can control the phases of the amplitudes and observe truly amazing quantum phenomena.

One of the simplest quantum devices that allows control of quantum interference, and is also the simplest quantum computing device, is a Mach–Zehnder interferometer, shown below.



Between the beam splitters, we have inserted slivers of glass with a different thickness for each of the possible paths. The glass slows down propagating photons and introduces slight delays during their journey between the two beam splitters. The slivers of glass are usually referred to as “phase shifters” and their thicknesses, φ_0 and φ_1 , are measured in units of the photon’s wavelength multiplied by 2π . We have labeled the two input and the two output ports of the interferometer as 0 and 1. When we fire a single photon into the input port 0, it can end up in detector 0 in two alternative ways, as shown below.



In each of the beam splitters, the incoming photon is reflected with a probability amplitude of $i/\sqrt{2}$ and transmitted with a probability amplitude $1/\sqrt{2}$.⁵ The effect of the slivers of glass is to multiply the probability amplitude on the lower path (labeled as path 0) by $e^{i\varphi_0}$ and on the upper path (labeled as path 1) by $e^{i\varphi_1}$. The lower path involves two transmissions and the upper path two reflections. The probability amplitude of the two consecutive reflections including the phase shift is $(i/\sqrt{2})e^{i\varphi_1}(i/\sqrt{2})$ and the probability amplitude of the two consecutive transmissions and the phase shift on the lower path is $(1/\sqrt{2})e^{i\varphi_0}(1/\sqrt{2})$. By using the rule of additivity of probability amplitudes, we can calculate the probability that the

⁵Although many probability amplitudes can be calculated from “first” principles, e.g., using QED, it is more common to use a phenomenological approach. Here you can justify the reflection amplitude being $i/\sqrt{2}$ on the grounds of consistency with classical electromagnetism.

photon ends up in detector “0,”

$$\begin{aligned} P_{00} &= \left| \left(\frac{i}{\sqrt{2}} \right) e^{i\varphi_1} \left(\frac{i}{\sqrt{2}} \right) + \left(\frac{1}{\sqrt{2}} \right) e^{i\varphi_0} \left(\frac{1}{\sqrt{2}} \right) \right|^2 \\ &= \frac{1}{4} + \frac{1}{4} - \frac{1}{2} \cos(\varphi_1 - \varphi_0) = \sin^2 \left(\frac{\varphi}{2} \right). \end{aligned}$$

The same approach allows us to calculate the probability amplitudes, U_{ij} , and the probabilities, P_{ij} , of any j to i transition ($i, j = 0, 1$), and tabulate them in matrices,

$$\begin{aligned} \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} &= i e^{i \frac{\varphi_0 + \varphi_1}{2}} \begin{pmatrix} -\sin \varphi/2 & \cos \varphi/2 \\ \cos \varphi/2 & \sin \varphi/2 \end{pmatrix} \\ \longrightarrow \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} &= \begin{pmatrix} \sin^2 \varphi/2 & \cos^2 \varphi/2 \\ \cos^2 \varphi/2 & \sin^2 \varphi/2 \end{pmatrix}, \end{aligned} \quad (18.1)$$

where $\varphi = \varphi_1 - \varphi_0$. The entries of the stochastic matrix P_{ij} are obtained from the corresponding probability amplitudes—we take the squared moduli of probability amplitudes, $P_{ij} = |U_{ij}|^2$. However, here the transition matrix is the matrix of amplitudes U , not the matrix of probabilities P ! Once we operate on amplitudes, the rules of the game are identical to those of classical probabilities: we multiply amplitudes of independent events and add amplitudes of “mutually exclusive” events.

The matrices which describe transitions in quantum machines are not just any matrices with complex entries. The probabilistic interpretation of amplitudes requires that any matrix U that describes an admissible physical operation is *unitary*, i.e., that it satisfies $\sum_k U_{ki}^* U_{kj} = \delta_{ij}$ where δ_{ij} , known as the “Kronecker delta,” is a symbol that is defined to be zero for $i \neq j$ and to be one for $i = j$. In matrix form, the unitarity condition reads

$$U^\dagger U = U U^\dagger = \mathbf{1}.$$

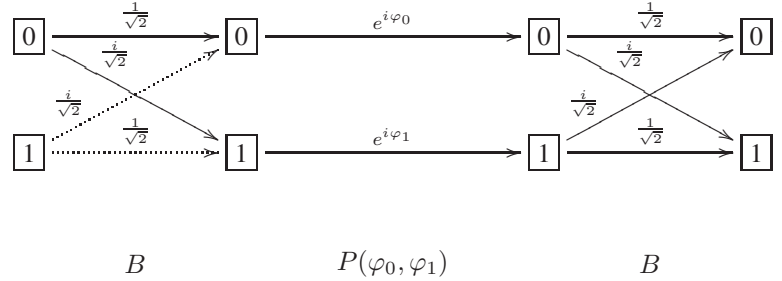
Recall that the *adjoint* or *Hermitian conjugate* $M^\dagger$ of any matrix M with complex entries M_{ij} is obtained by taking the complex conjugate of every element in the matrix and then interchanging rows and columns $M_{ij} \rightarrow M_{ji}^*$.

Probably the most striking observation when we inspect the transition probabilities in quantum interference experiments, is that the qubit reacts only to the phase *difference*, $\varphi = \varphi_1 - \varphi_0$. The phases φ_0 and φ_1 in the Mach–Zehnder interferometer can be set up independently from each other, and the two arms of the interferometer may be miles apart, and yet it is the difference between the two phases that determines which of the two detectors will eventually click. The inescapable conclusion is that somehow the photon must have experienced both of them! It is very counter-intuitive, but this is what experiments show. Between the two beam splitters, the photon is in a truly quantum state which is referred to as a quantum superposition of the lower and the upper path. We have labeled these paths as 0 and 1, and thus the two binary values can co-exist. Quantum computers can operate on such superpositions of the binary values, a property which sets them apart from their classical counterparts.

If we remove the phase shifters from the interferometer, which is equivalent to setting $\varphi_1 = \varphi_0 = 0$, the formula (18.1) shows that the two beam splitters effect the logical NOT. One can also set up experiments which demonstrate the existence of $\sqrt{\text{SWAP}}$. Addition of probability amplitudes explains the behavior of $\sqrt{\text{NOT}}$, $\sqrt{\text{SWAP}}$ and many other gates, and correctly predicts the probabilities of all the possible outputs no matter how we concatenate the gates. This knowledge was created as the result of conjectures, experimentation, and refutations. Genuine scientific knowledge cannot be certain, nor can it be justified a priori. Instead, it must be conjectured, and then tested by experiment. Hence, reassured by the physical experiments that corroborate this theory, logicians are now entitled to propose new logical operations $\sqrt{\text{NOT}}$ and $\sqrt{\text{SWAP}}$. Why? Because faithful physical models for them exist in nature!

18.4 Interference Revisited

Using the optical Mach–Zehnder interferometer is just one way of performing a quantum interference experiment—there are many others. Atoms, molecules, nuclear spins, and many other quantum objects can be prepared in two distinct states, internal or external, labeled as 0 and 1 and manipulated so that transition amplitudes between these states are the same as in a beam splitter or in a phase shifter. However, there is no need to learn these technologies to understand quantum interference. You may conveniently forget about any specific technology (hardware) and refer to any quantum object with two distinct states labeled 0 and 1 as a quantum bit or a qubit. The interference of a single qubit can then be visualized as

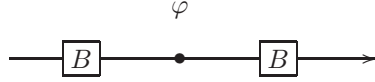


The diagram shows all possible transitions between the states 0 and 1, and their corresponding probability amplitudes; it has the same features as the diagram of the Mach–Zehnder interferometer. We can view the action of the interferometer as a sequence of three elementary operations called quantum logic gates: a beam splitter B followed by a phase shift P_φ , followed by another beam splitter B . Each quantum gate is described by its matrix of transition amplitudes

$$B = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \quad P_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

$\sqrt{\text{NOT}}$
PHASE.

We usually draw this sequence of operations as a quantum circuit,



Quantum circuit diagrams are read from left to right. The horizontal line represents a quantum wire, which inertly carries a qubit from one quantum operation to another. The wire may describe translation in space, e.g., atoms traveling through cavities, or translation in time, e.g., a sequence of operations performed on a trapped ion. This is a sequential composition of gates and, as with the case of stochastic matrices, all we have to do is to multiply the matrices,

$$\begin{aligned} B P_\varphi B &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \\ &= i e^{i\frac{\varphi}{2}} \begin{pmatrix} -\sin \varphi/2 & \cos \varphi/2 \\ \cos \varphi/2 & \sin \varphi/2 \end{pmatrix}. \end{aligned}$$

In one swoop, this takes care of the multiplication and addition of probability amplitudes corresponding to different interfering paths in the interferometer. The phase shift φ effectively controls the evolution and determines the output.

We should mention here that the phase matrix $P_\varphi = \text{diag}(1, e^{i\varphi})$ contains only the relative phase. This is because $\text{diag}(e^{i\varphi_0}, e^{i\varphi_1})$ can be written as $e^{i\varphi_0} \text{diag}(1, e^{i\varphi})$ with $\varphi = \varphi_1 - \varphi_0$, and we have already seen that it is the relative phase that really matters.

We have already mentioned that a qubit undergoing quantum interference enters a peculiar quantum state, a superposition of 0 and 1, in which it simultaneously represents the two binary values. In the classical world the state of a physical bit is described by a probability vector; a qubit, in all its possible superpositions, is described by a vector of probability amplitudes, known as a state vector, which evolves as

$$\begin{pmatrix} \alpha'_0 \\ \alpha'_1 \end{pmatrix} = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

OUTPUT $\leftarrow$ EVOLUTION $\leftarrow$ INPUT.

A sequence of operations in quantum interference evolves the state vector of the qubit as

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \xrightarrow{B} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \xrightarrow{\varphi} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i e^{i\varphi} \end{pmatrix} \xrightarrow{B} \begin{pmatrix} -\sin \varphi/2 \\ \cos \varphi/2 \end{pmatrix}$$

INPUT

OUTPUT,

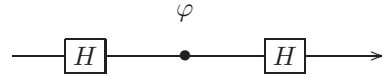
where we have omitted an overall phase factor $ie^{i\frac{\varphi}{2}}$ from the output state. Probability vectors can be constructed at any stage by squaring the moduli of the components of the evolving state vector. In particular, at the output, the two binary values 0 and 1 are registered with respective probabilities, $\sin^2 \varphi/2$ and $\cos^2 \varphi/2$.

In general, any isolated physical system with N distinguishable states is described by a state vector with N complex components and *any* machine whose action depends on no other input or stored information and which performs a computation on a physical system with N distinguishable states is described by some $N \times N$ matrix of probability amplitudes i.e., an $N \times N$ unitary matrix.

Last but not least, quantum interference may be implemented in a number of different ways. For example, in the lore of quantum computation, a beam splitter is often substituted by the very popular Hadamard gate, H ,

$$\text{---} \boxed{H} \text{---} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and single-qubit interference is represented as



The transition probability amplitudes in the circuit are calculated by the matrix multiplication $HP_\varphi H$,

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = e^{i\varphi/2} \begin{pmatrix} \cos \varphi/2 & i \sin \varphi/2 \\ i \sin \varphi/2 & \cos \varphi/2 \end{pmatrix}.$$

This simple quantum process contains, in a nutshell, the essential ingredients of quantum computation. The sequence of Hadamard - phase shift - Hadamard will appear over and over again. It reflects a natural progression of quantum computation: first we prepare different computational paths, then we evaluate a function which effectively introduces phase shifts into different computational paths, then we bring the computational paths together at the output.

18.5 Tools of the Trade

18.5.1 Quantum states

Although the addition of probability amplitudes is basically all we need to know to practice quantum mechanics, it is very convenient to have good tools and notation for the “book keeping” of probability amplitudes. A mathematical setting for the quantum formalism is a vector

space with an inner product, often referred to as a Hilbert space.⁶ Here we are primarily interested in $\mathbb{C}^N$, the space of column vectors with N complex entries. We shall follow the notation introduced by Paul Dirac in the early days of quantum theory and write column vectors as

$$|a\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_{N-1}|N-1\rangle$$

and the adjoint vector, $|a\rangle^\dagger$, as $\langle a|$,

$$\langle a| = \begin{pmatrix} \alpha_0^* & \alpha_1^* & \cdots & \alpha_{N-1}^* \end{pmatrix} = \langle 0|\alpha_0^* + \langle 1|\alpha_1^* + \cdots + \langle N-1|\alpha_{N-1}^*.$$

In this notation, the scalar product of two vectors, $|a\rangle$ and $|b\rangle$, is written as

$$\langle a|b\rangle = \alpha_0^*\beta_0 + \alpha_1^*\beta_1 + \cdots + \alpha_{N-1}^*\beta_{N-1}.$$

Much of linear algebra grew out of the need to generalize the basic geometry of vectors in two and three dimensions. The scalar product enables the definition of angles, lengths and distances. Vectors for which $\langle a|b\rangle = 0$ are perpendicular—in $\mathbb{C}^N$ they are called orthogonal. Any maximal set of pairwise orthogonal vectors forms an orthonormal basis and any vector can be expressed as a linear combination of the basis vectors. We have already used the standard orthonormal basis in $\mathbb{C}^N$, denoted as $\{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$, where $|n\rangle$ stands for a column vector with 1 in the $(n+1)$ th entry and zeros elsewhere. For example, the standard basis in $\mathbb{C}^2$ is $\{|0\rangle, |1\rangle\}$ but there are infinitely many other orthonormal bases, e.g., $\{|+\rangle, |-\rangle\}$ where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

Once we have defined an inner product, we can define the norm, or the length, of $|a\rangle$ as $\|a\| = \sqrt{\langle a|a\rangle}$. Using the norm, we can define the distance between any two vectors $|a\rangle$ and $|b\rangle$ as $\|a - b\|$; we say that $|a\rangle$ is within a distance ε of $|b\rangle$ if $\|a - b\| \leq \varepsilon$.

- **Quantum states** For any isolated quantum system which can be prepared in N distinguishable states, we can associate a space $\mathbb{C}^N$ such that each vector of unit length represents a quantum state of the system.

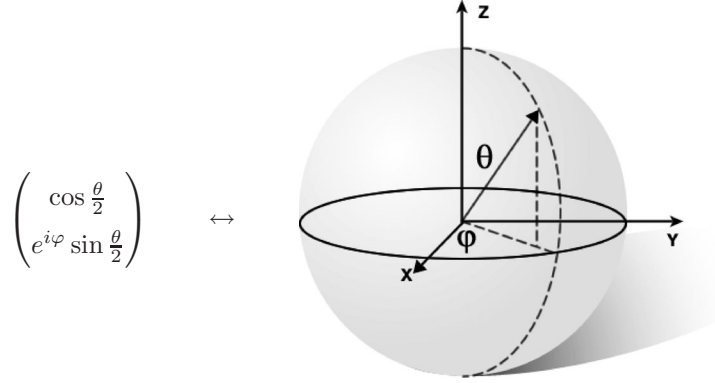
Quantum states of individual qubits are rather special. The complex components of the state vector

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

are constrained only by the normalization condition $|\alpha_0|^2 + |\alpha_1|^2 = 1$ and can be conveniently parameterized as $\alpha_0 = \cos \theta/2$ and $\alpha_1 = e^{i\varphi} \sin \theta/2$, where $0 \leq \theta \leq \pi$ and $0 \leq \varphi \leq 2\pi$. Thus we can map all of the single-qubit states onto the surface of a sphere, i.e., we can interpret

⁶We will restrict our attention to finite-dimensional vector spaces, which helps to avoid many mathematical subtleties.

θ as the polar angle and ϕ as the azimuthal angle. The sphere is called the Bloch sphere and the unit vector $\vec{s}$ defined by θ and ϕ is called the Bloch vector. The Bloch vector in the Euclidean space should never be confused with the state vector in the Hilbert space.



Please note that the two basis states $|0\rangle$ and $|1\rangle$ are represented on the Bloch sphere as two antipodal Bloch vectors with $\theta = 0$ and $\theta = \pi$. The Bloch sphere may look at this stage as an unnecessary complication but soon it will become a useful tool which helps to visualize relations between states of individual qubits and single-qubit unitary operations.

We shall often refer to quantum systems with N distinguishable states as quantum systems in $\mathbb{C}^N$. The vector space structure of quantum states means that if $|a\rangle$ and $|b\rangle$ are two possible quantum states then the properly normalized superposition $\alpha|a\rangle + \beta|b\rangle$ is also a valid quantum state. This is sometimes referred to as the superposition principle. From a mathematical point of view, it is a trivial remark, but we have already seen that its physical consequences are anything but trivial. It implies, for example, that a single photon can take two different paths in its passage through an interferometer, that an atom can be both in its ground and excited state, in general, that a qubit can represent both logical 1 and 0 at the same time.

Let us add that an $N \times M$ matrix P can be viewed as a vector in $\mathbb{C}^{N \times M}$; we simply string out the entries of P_{ij} into an NM -component column vector. In particular, given two complex square matrices with entries A_{ij} and B_{kl} we can write their scalar product as

$$(A|B) \equiv \sum_{ij} A_{ij}^* B_{ij} = \text{Tr}(A^\dagger B),$$

where the trace symbol Tr denotes the sum over all diagonal elements, i.e., $\text{Tr}(P) = \sum_i P_{ii}$. Written in this particular way, the scalar product of two matrices is often referred to as the Hilbert–Schmidt product. Given a scalar product we can now talk about norms and distances between matrices.

18.5.2 Unitary operations

Any linear operation on vectors is called an operator and any operator M is completely determined by its action on the basis vectors. It can be written as

$$M = \sum_{kl} M_{kl} |k\rangle\langle l|, \quad (18.2)$$

where $|k\rangle\langle l|$ is the matrix with 1 in the (kl) entry and zeros elsewhere. The result of $|k\rangle\langle l|$ acting on vector $|a\rangle$ is $|k\rangle\langle l|a\rangle$, i.e., vector $|k\rangle$ multiplied by a complex number $\langle l|a\rangle$. In the Dirac notation, the matrix elements M_{ij} are written as $\langle i|M|j\rangle$, which follows directly from expression (18.2) when we sandwich M between $\langle i|$ and $|j\rangle$, and use $\langle i|k\rangle = \delta_{ik}$, $\langle l|j\rangle = \delta_{lj}$. Here we will usually refer to the standard basis in $\mathbb{C}^N$ and make little distinction between operators and matrices. Still, one should remember that a matrix representation is basis dependent and the operator M may be represented by different matrices in different bases.

We will refer to the properties of operators by referring to the properties of their matrices. For example, an operator M is called unitary if its matrix is unitary, i.e., $MM^\dagger = M^\dagger M = \mathbf{1}$, it is called Hermitian if $M = M^\dagger$, and it is called normal if $MM^\dagger = M^\dagger M$. Both unitary and Hermitian operators are normal and all normal operators can be diagonalized by unitary matrices U . More precisely, M is normal if and only if there exists a unitary U such that

$$M = UDU^\dagger,$$

where D is the diagonal matrix, $D = \text{diag}(\lambda_0, \lambda_1, \lambda_2, \dots)$. The diagonal elements λ_j are known as the eigenvalues or the spectrum of M and the column vectors of U , which we can write as $|m_j\rangle = \sum_i U_{ij}|i\rangle$, are the corresponding eigenvectors of M , i.e., $M|m_j\rangle = \lambda_j|m_j\rangle$ and $\langle m_i|m_j\rangle = \delta_{ij}$, $\sum_j |m_j\rangle\langle m_j| = \mathbf{1}$. Thus, any normal operator admits the spectral decomposition, $M = \sum_j \lambda_j |m_j\rangle\langle m_j|$. Eigenvalues of Hermitian operators are real, whereas for all unitary operators they are complex numbers of unit length: $\lambda_j = e^{i\alpha_j}$ for some real α_j .

Unitary operators are special—they preserve the scalar product. If $|a'\rangle = U|a\rangle$ and $|b'\rangle = U|b\rangle$ then $\langle a'| = \langle a|U^\dagger$ and

$$\langle a'|b'\rangle = \langle a|U^\dagger U|b\rangle = \langle a|\mathbf{1}|b\rangle = \langle a|b\rangle.$$

This implies that unitary operations preserve the length of state vectors; the probabilities are conserved.

- **Quantum evolution** Evolution of any isolated quantum system in $\mathbb{C}^N$ is described by a unitary operator acting on this space.

The set of all unitary $N \times N$ matrices with matrix multiplication forms a group denoted as $U(N)$; the unit element is the $N \times N$ identity matrix and the inverse of U is obtained by taking the Hermitian conjugate $U^\dagger$. The order in which we multiply matrices matters, usually $UV \neq VU$, thus the $U(N)$ group is non-Abelian. We have already mentioned that we are allowed to ignore overall phase factors. We can avoid ambiguities of overall phase factors by restricting ourselves to matrices which belong to the special unitary group $SU(N)$, i.e., all

unitary $N \times N$ matrices with determinants equal to unity. Having said this, the convention of writing phase gates in the form $\text{diag}(1, e^{i\varphi})$ rather than $\text{diag}(e^{-i\varphi/2}, e^{i\varphi/2})$ means that our matrices are often not in $SU(N)$, but then we can always fix it by playing with global phase factors.

Any unitary matrix can be represented as the exponential of some Hermitian matrix, H and a real coefficient, α ,

$$e^{i\alpha H} \equiv \mathbf{1} + i\alpha H + \frac{(i\alpha)^2}{2} H^2 + \frac{(i\alpha)^3}{2 \cdot 3} H^3 \dots = \sum_{n=0}^{\infty} \frac{(i\alpha)^n}{n!} H^n. \quad (18.3)$$

This is analogous to writing complex numbers of unit moduli in the polar form as $e^{i\alpha}$. The time evolution of a quantum state is a unitary process which is generated by a Hermitian operator called the Hamiltonian, H . The Hamiltonian contains a complete specification of all interactions within the system under consideration. In an isolated system, the state vector $|\psi(t)\rangle$ changes smoothly in time according to the Schrödinger equation

$$\frac{d}{dt} |\psi(t)\rangle = -\frac{i}{\hbar} H |\psi(t)\rangle.$$

For time-independent Hamiltonians the formal solution reads

$$|\psi(t)\rangle = U(t) |\psi(0)\rangle \quad \text{where} \quad U(t) = e^{-\frac{i}{\hbar} H t}$$

Here $\hbar$ denotes Planck's constant, which has the value

$$\hbar = 1.05 \times 10^{-34} \text{ J s.}$$

However, theorists always choose to work with a system of units where $\hbar = 1$.

Equation (18.3) acquires a deceptively simple form when H squares to the identity, $H^2 = \mathbf{1}$. In this case we obtain

$$e^{i\alpha H} = \cos \alpha \mathbf{1} + i \sin \alpha H.$$

Among the most popular single-qubit operations are the PAULI gates, described by the Pauli matrices $\sigma_x \equiv X$, $\sigma_y \equiv Y$, and $\sigma_z \equiv Z$,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Two of the PAULI gates are already very familiar, the Z gate is a special phase gate with $\varphi = \pi$ and the X gate is the logical NOT gate, but we have written them again for completeness. The two gates, X and Z , are often referred to as the bit flip and the phase flip, respectively. The Pauli matrices square to the identity

$$X^2 = Y^2 = Z^2 = \mathbf{1},$$

and they satisfy the relations

$$XY + YX = 0, \quad XY = iZ \quad (\text{and cyclic permutations}).$$

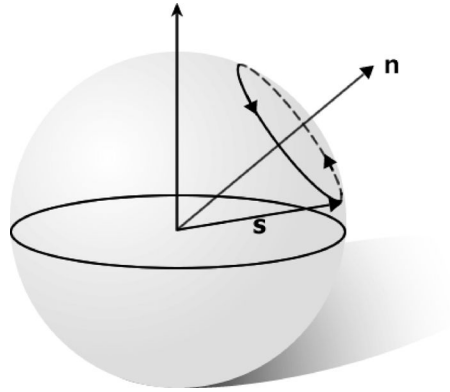
As well as being useful gates in their own right, the combination of the three Pauli matrices and the identity is useful in providing a decomposition of 2×2 Hermitian matrices. When multiplied by the normalization factor $1/\sqrt{2}$ they form an orthonormal basis with respect to the Hilbert–Schmidt product. Any 2×2 matrix can be written as

$$\begin{pmatrix} n_0 + n_z & n_x - in_y \\ n_x + in_y & n_0 - n_z \end{pmatrix} = n_0 \mathbf{1} + n_x X + n_y Y + n_z Z \equiv n_0 \mathbf{1} + \vec{n} \cdot \vec{\sigma},$$

where $\vec{\sigma}$ represents the vector of the Pauli matrices $\vec{\sigma} = \{X, Y, Z\}$. This decomposition allows us to see some special properties of one-qubit unitary rotations. Any element of $SU(2)$ can be written as

$$\exp i\alpha(\vec{n} \cdot \vec{\sigma}) = \cos \alpha \mathbf{1} + i \sin \alpha (\vec{n} \cdot \vec{\sigma}),$$

where $\vec{n}$ is a unit vector with three real components n_x , n_y and n_z . There is a remarkable connection between unitary matrices which are in $SU(2)$ and three-dimensional rotation matrices, which form a group denoted as $SO(3)$. In our particular case, applying a unitary operation $\exp i\alpha(\vec{n} \cdot \vec{\sigma})$ to a qubit described by a Bloch vector $\vec{s}$ amounts to rotating $\vec{s}$ by the angle α about the axis defined by the unit vector $\vec{n}$.



The correspondence is established by the formula

$$[\exp i\alpha(\vec{n} \cdot \vec{\sigma})] (\vec{s} \cdot \vec{\sigma}) [\exp -i\alpha(\vec{n} \cdot \vec{\sigma})] = \vec{s}' \cdot \vec{\sigma},$$

where $\vec{s}'$ is the Bloch vector $\vec{s}$ rotated by the angle α about the axis defined by the unit vector $\vec{n}$. This gives a very simple geometrical solution of the Schrödinger equation with the Hamiltonian

$$H = \vec{\Omega} \cdot \vec{\sigma} = \Omega(\vec{n} \cdot \vec{\sigma}).$$

The vector $\vec{\Omega}$ with components $(\Omega_x, \Omega_y, \Omega_z)$ is called the Rabi vector and $\Omega = \sqrt{\Omega_x^2 + \Omega_y^2 + \Omega_z^2}$ is often referred to as the Rabi frequency. The Bloch vector $\vec{s}$ simply rotates around the Rabi vector $\vec{\Omega}$ with the Rabi frequency Ω equal to the length of $\vec{\Omega}$.

18.5.3 Quantum measurements

The state of the form $\alpha_0|0\rangle + \alpha_1|1\rangle$ contains all the information about the qubit, but when we measure the bit value, we register either 0 or 1 with probabilities $|\alpha_0|^2$ and $|\alpha_1|^2$, respectively. Although measurement can, in principle, be explained in terms of unitary operations, here we will view it as a special, nonunitary, quantum gate, defined as

$$\alpha_0|0\rangle + \alpha_1|1\rangle \longrightarrow \boxed{k} \longrightarrow |k\rangle \quad \text{with probability } |\alpha_k|^2$$

where $k = 0$ or $k = 1$. If we choose to measure the bit value of a qubit in state $|a\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ then the result of measurement is 0 with probability $|\alpha_0|^2$ and 1 with probability $|\alpha_1|^2$. The outcome of measurement, k , is written in the icon representing measurement, and the output state of measurement gate is $|k\rangle$. However, do not think that by measuring a given qubit over and over again you could accumulate enough data to estimate the magnitudes of the two probability amplitudes. This does not work because measurements modify quantum states. As you can see in the diagram above, if the measurement result is 0, the postmeasurement state of the qubit is no longer $|a\rangle$, but $|0\rangle$, and if the result is 1 the postmeasurement state is $|1\rangle$. The original state $|a\rangle$ is irretrievably lost. This sudden change of state, $|a\rangle \rightarrow |0\rangle$ with probability $|\alpha_0|^2$ and $|a\rangle \rightarrow |1\rangle$ with probability $|\alpha_1|^2$, due to a measurement is often called a “collapse” or a “reduction” of the state. The status of this “reduction” in the formulation of quantum mechanics is still debated.

A convenient mathematical formalism for quantum measurements performed on any quantum objects in $\mathbb{C}^N$ is based on projection operators. The expression $|k\rangle\langle k|$ describes a projection onto $|k\rangle$. Indeed, the result of $|k\rangle\langle k|$ acting on any vector $|a\rangle \in \mathbb{C}^N$ is $|k\rangle\langle k|a\rangle$, i.e., vector $|k\rangle$ multiplied by $\langle k|a\rangle$. The sum of projections on vectors from *any* orthonormal basis gives the identity operator, i.e.,

$$\mathbf{1} = \sum_k |k\rangle\langle k|.$$

This is a useful expression known as the decomposition of the identity. We can use it to expand any vector $|\psi\rangle$ in *any* basis as

$$|\psi\rangle = \mathbf{1}|\psi\rangle = \sum_k |k\rangle\langle k|\psi\rangle = \sum_k \alpha_k |k\rangle \quad \text{where} \quad \alpha_k = \langle k|\psi\rangle.$$

Any measurable physical property of a quantum system in $\mathbb{C}^N$, which takes values in some set of symbols labeled by k , is represented by a set of projectors $P_k = |k\rangle\langle k|$ which form the decomposition of the identity $\sum_k P_k = \mathbf{1}$.

- **Quantum measurement** Given a quantum system in the state $|\psi\rangle$ measurement of a physical property described by projectors $\{P_k\}$ gives outcome $\bar{k}$ with the probability $\langle\psi|P_{\bar{k}}|\psi\rangle = \langle\psi|\bar{k}\rangle\langle\bar{k}|\psi\rangle$ and leaves the system in a properly normalized state $P_{\bar{k}}|\psi\rangle$, i.e., $|\bar{k}\rangle$.

For example, the standard measurement on a qubit is described by the projectors $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ which form the decomposition of the identity $P_0 + P_1 = \mathbf{1}$. Given

a qubit in state $|\psi\rangle$, measurement gives outcome $\bar{k}$, $k = 0, 1$, with probability $|\alpha_k|^2 = \langle\psi|\bar{k}\rangle\langle\bar{k}|\psi\rangle$ and leaves the system in state $|\bar{k}\rangle$. However, we can also measure other properties, for example, defined by the projectors $P_+ = |+\rangle\langle+|$ and $P_- = |-\rangle\langle-|$, $P_+ + P_- = \mathbf{1}$. The two projectors define another measurement with two possible outcomes labeled by $+$ and $-$. In the following, unless specified otherwise, all measurements are assumed to be performed in the standard basis. This is because any measurement can be reduced to the standard measurement by performing some prior unitary transformation. For example, $P_+ = HP_0H$ and $P_- = HP_1H$ and $\langle\psi|P_+|\psi\rangle = \langle\psi|HP_0H|\psi\rangle$, $\langle\psi|P_-|\psi\rangle = \langle\psi|HP_1H|\psi\rangle$, thus measuring $\{P_+, P_-\}$ on $|\psi\rangle$ is equivalent to measuring $\{P_0, P_1\}$ on $H|\psi\rangle$,

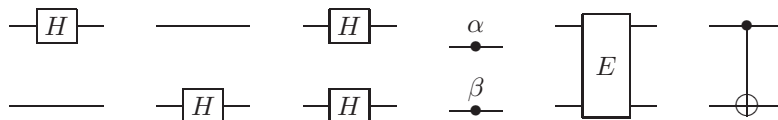
$$|\psi\rangle \text{ --- } \boxed{k} \text{ ---} \equiv |\psi\rangle \text{ --- } \boxed{H} \text{ --- } \boxed{k} \text{ ---} \\ P_+, P_- \qquad \qquad \qquad P_0, P_1$$

In some textbooks, quantum measurement is associated with Hermitian operators having the spectral decomposition $\sum_j \lambda_j |m_j\rangle\langle m_j|$ ($\sum_j |m_j\rangle\langle m_j| = \mathbf{1}$) and the different outcomes are described by the real values λ_j . As a result, it is often falsely claimed that the outcomes of quantum measurements must be labeled by real numbers. We emphasize, however, that we are really just labeling the measurement results, and hence we can associate any symbols we wish with the possible outcomes.

18.6 Composite Systems

Given that quantum machines are described by their respective unitary matrices and that the rules of addition and multiplication of amplitudes are the same as that of probabilities, we can construct more complex machines following the familiar composition rules: when two quantum machines, which are described by some unitary matrices U and V , act in parallel, their action is described by the tensor product $U \otimes V$, and when the action of U is followed by V , the resulting unitary matrix is the matrix product VU . You can check that both tensor and matrix products of unitary matrices give another unitary matrix, i.e., both parallel and sequential compositions of quantum devices give another quantum device, as expected. In both cases the order does matter, i.e., in general $VU \neq UV$ and $U \otimes V \neq V \otimes U$. The tensor product is associative, $U \otimes V \otimes W = (U \otimes V) \otimes W$, so we can extend quantum operations to any number of qubits.

If we bring two qubits together, we form a system with 2^2 distinguishable states, which we label as 00, 01, 10, and 11. The circuits below show six unitary operations on the two qubits,



The first four are described, respectively, by 4×4 unitary matrices which are tensor products

$$\begin{aligned}
 H \otimes \mathbf{1} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} & \mathbf{1} \otimes H &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \\
 H \otimes H &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} & P(\alpha) \otimes P(\beta) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\beta} & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i(\alpha+\beta)} \end{pmatrix}
 \end{aligned}$$

Please note that $(H \otimes \mathbf{1})(\mathbf{1} \otimes H) = H \otimes H$. The n -fold tensor product of Hadamard gates $H^{\otimes n} = H \otimes H \cdots \otimes H$, i.e., applying H to each qubit, is referred to as the n -qubit Hadamard transform. The matrices of the two remaining gates, known as the square root of SWAP and controlled-NOT, stand out as they do not admit a tensor product decomposition in terms of single-qubit operations,

$$\begin{aligned}
 E &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} & \frac{ie^{i\frac{\pi}{4}}}{\sqrt{2}} & 0 \\ 0 & \frac{ie^{i\frac{\pi}{4}}}{\sqrt{2}} & \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\
 &\sqrt{\text{SWAP}} & \text{c-NOT.}
 \end{aligned}$$

There is a whole family of square root of SWAP matrices. Our choice here, with the $e^{i\frac{\pi}{4}}$ phase factor in the central sub-matrix, is directly related to its most common experimental realization (the Heisenberg interaction). The controlled-NOT (c-NOT) performs the phase flip, i.e., logical NOT, on the second (target) qubit if the first (control) qubit represents logical 1 and does nothing if the control qubit represents 0.

Let us take a closer look at how the mathematical formalism introduced in the previous section can be applied to composite systems, i.e., systems made out of several subsystems. For this we need to revisit the tensor product operation. We shall start with the simplest possible composite system, namely two qubits.

Two isolated qubits live in a tensor product space denoted as $\mathbb{C}^2 \otimes \mathbb{C}^2$. The tensor product operation is a way of putting vector spaces together to form larger vector spaces. When we bring two qubits together, the first one in state $|a\rangle \in \mathbb{C}^2$ and the second in state $|b\rangle \in \mathbb{C}^2$, we

form a new state $|a\rangle \otimes |b\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ often written as $|a\rangle|b\rangle$, or simply $|a, b\rangle$, or even $|ab\rangle$. The elements of $\mathbb{C}^2 \otimes \mathbb{C}^2$ are linear combinations of $|a\rangle \otimes |b\rangle$. The scalar product in $\mathbb{C}^2 \otimes \mathbb{C}^2$ is defined by the identity

$$(\langle a_1| \otimes \langle b_1|) (|a_2\rangle \otimes |b_2\rangle) \equiv \langle a_1|a_2\rangle \langle b_1|b_2\rangle,$$

and the space can be spanned by the four vectors of the standard basis $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$, usually written as $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. Thus if

$$|a\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \quad , \quad |b\rangle = \beta_0|0\rangle + \beta_1|1\rangle,$$

then the state of a composite system can be written as

$$|a\rangle \otimes |b\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle,$$

where we have used the fact that the tensor product is a linear operation. However, not all vectors in $\mathbb{C}^2 \otimes \mathbb{C}^2$ are of the form $|a\rangle \otimes |b\rangle$. To see this, consider the most general quantum state of two qubits

$$c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle.$$

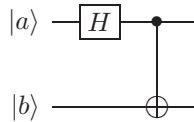
The complex amplitudes c_l are constrained only by the normalization condition $\sum_{l \in \{0,1\}^2} |c_l|^2 = 1$. This means that, in general, $c_{ij} \neq \alpha_i\beta_j$, where $i, j = 0, 1$, which implies that not all quantum states of two qubits can be written in the form $|a\rangle \otimes |b\rangle$. Those that can be are called *separable* and those that cannot be are called *entangled*. For example, of the two states

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle),$$

the first one is separable because it can be written as $|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ whereas the second one is entangled because it does not admit such a decomposition. Thus a system of two qubits as a whole can be prepared in a quantum state which does not allow the attribution of separate state vectors to its parts. The four popular entangled states are the so-called Bell states,

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \quad , \quad |\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle).$$

In order to entangle two (or more) qubits, we need gates which couple two qubits, for example, the square root of SWAP or the controlled-NOT, e.g., the circuit



evolves the four inputs, $|ab\rangle$, $a, b = 0, 1$, into the four Bell states. At present, the most common source of entangled qubits is a quantum optical process called “parametric down conversion.” A photon from a laser beam enters a beta-borium-borate crystal and gets absorbed, exciting

an atom in the crystal in the process. The atom subsequently decays, emitting two photons whose polarizations are entangled.

We can extend the tensor product operation to any number of qubits. The n -fold tensor product space $(\mathbb{C}^2)^{\otimes n}$ is the 2^n -dimensional complex vector space with the standard computational basis labeled by all binary strings of length n . The elements of $(\mathbb{C}^2)^{\otimes n}$ are all possible linear combinations of the vectors from the computational basis, in particular any quantum states of n isolated qubits can be written as

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} c_x |x\rangle.$$

In addition to the single-qubit Pauli operations, we can also define bit flips and phase flips on selected qubits, X_c and Z_c , where the binary string c indicates the location of the flip, for example $X_{101} = X \otimes \mathbf{1} \otimes X$, $Z_{110} = Z \otimes Z \otimes \mathbf{1}$. The Hadamard gate squares to the identity and it can turn the action of the X gate into Z and vice versa; the circuit HXH is equivalent to the action of a single Z and conversely $HZH \equiv X$. In general, the Hadamard transform can turn X_c into Z_c and vice versa.

$$\begin{array}{ccc} \text{---} \boxed{H} \text{---} \boxed{X} \text{---} \boxed{H} \text{---} & = & \text{---} \boxed{Z} \text{---} \\ \text{---} \boxed{H} \text{---} & & \text{---} \boxed{H} \text{---} \boxed{Z} \text{---} \boxed{H} \text{---} \\ \text{---} \boxed{H} \text{---} \boxed{X} \text{---} \boxed{H} \text{---} & = & \text{---} \boxed{Z} \text{---} \end{array} \quad , \quad \begin{array}{ccc} \text{---} \boxed{H} \text{---} \boxed{Z} \text{---} \boxed{H} \text{---} & = & \text{---} \boxed{X} \text{---} \\ \text{---} \boxed{H} \text{---} & & \text{---} \boxed{H} \text{---} \boxed{Z} \text{---} \boxed{H} \text{---} \\ \text{---} \boxed{H} \text{---} \boxed{X} \text{---} \boxed{H} \text{---} & = & \text{---} \boxed{Z} \text{---} \end{array}$$

The two circuit identities represent the two relations, $H^{\otimes 3} X_{101} H^{\otimes 3} = Z_{101}$ and $H^{\otimes 3} Z_{110} H^{\otimes 3} = X_{110}$.

Labels, i.e., binary strings x , can be used to define unitary operations. For example, for any x and any constant c in $\{0,1\}^n$ we can express X_c and Z_c as

$$\begin{aligned} X_c : |x\rangle &\longrightarrow |x \oplus c\rangle \quad , & X_c &= \sum_{x \in \{0,1\}^n} |x \oplus c\rangle \langle x| \\ Z_c : |x\rangle &\longrightarrow (-1)^{c \cdot x} |x\rangle \quad , & Z_c &= \sum_{x \in \{0,1\}^n} (-1)^{c \cdot x} |x\rangle \langle x| \end{aligned}$$

and the Hadamard transform on n qubits can be defined as

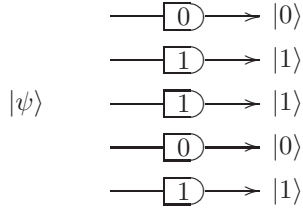
$$|x\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \quad , \quad H^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \langle x|$$

and implemented by applying the Hadamard gate to each of the n qubits. This action is easily understood by using the fact that

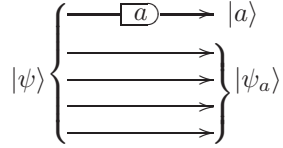
$$H^{\otimes n} |x\rangle = H^{\otimes n} X_x |0\rangle = Z_x H^{\otimes n} |0\rangle.$$

Projectors $P_x = |x\rangle \langle x|$ for $x \in \{0,1\}^n$ are tensor products of projectors pertaining to individual qubits, e.g., $P_{01} = |01\rangle \langle 01| = |0\rangle \langle 0| \otimes |1\rangle \langle 1|$. They form a decomposition of the

identity $\sum_{x \in \{0,1\}^n} P_x = \mathbf{1}$ and define the standard measurement on n qubits. More precisely, given n qubits in some quantum state $|\psi\rangle$, we can measure the qubits, obtaining the binary string x with the probability $|c_x|^2 = \langle\psi|P_x|\psi\rangle$. For example, for $n = 5$ we may register the binary string $k = 01101$.



This happens with the probability $|c_{01101}|^2$ and the state after the measurement is $|01101\rangle$. But, what if we choose to measure only some of the five qubits, say the first one?



In this case, measurement is described by the two projectors

$$\tilde{P}_0 = |0\rangle\langle 0| \otimes \mathbf{1} \otimes \mathbf{1} \otimes \mathbf{1} \otimes \mathbf{1}, \quad \tilde{P}_1 = |1\rangle\langle 1| \otimes \mathbf{1} \otimes \mathbf{1} \otimes \mathbf{1} \otimes \mathbf{1}.$$

They satisfy $\tilde{P}_0 + \tilde{P}_1 = \mathbf{1}$. The two results of measurement are 0 and 1 with the probabilities $\langle\psi|\tilde{P}_0|\psi\rangle$ and $\langle\psi|\tilde{P}_1|\psi\rangle$, respectively. The corresponding state after measurement is a properly normalized result of the projection $\tilde{P}_0|\psi\rangle$ and $\tilde{P}_1|\psi\rangle$. Translating this into a simple algebra, we may write the initial state $|\psi\rangle$ as

$$\alpha_0|0\rangle|\psi_0\rangle + \alpha_1|1\rangle|\psi_1\rangle,$$

where

$$\alpha_0 = \sqrt{\sum_{k \in \{0,1\}^4} |c_{0k}|^2}, \quad \alpha_1 = \sqrt{\sum_{k \in \{0,1\}^4} |c_{1k}|^2},$$

and

$$|\psi_0\rangle = \frac{1}{\alpha_0} \sum_{k \in \{0,1\}^4} c_{0k}|k\rangle, \quad |\psi_1\rangle = \frac{1}{\alpha_1} \sum_{k \in \{0,1\}^4} c_{1k}|k\rangle.$$

Thus, the result of measurement on the first qubit is 0 with the probability $|\alpha_0|^2$ or 1 with the probability $|\alpha_1|^2$, and the postmeasurement states are $|0\rangle|\psi_0\rangle$ and $|1\rangle|\psi_1\rangle$, respectively.

This shows us that there is more to quantum states of n qubits than just being unit vectors in $\mathbb{C}^{2^n}$. When we have a composite system, we can ask questions about the relation of a quantum system of the whole to quantum states of its components. The tensor product structure of the underlying Hilbert space is surprisingly rich and there is much more in $\mathbb{C}^2 \otimes \mathbb{C}^2 \cdots \otimes \mathbb{C}^2$ as compared to $\mathbb{C}^{2^n}$.

18.6.1 Density operators

The notion of an entangled state will probably make you wonder about the usefulness of state vectors as a good description of quantum states. Indeed, the tensor product structure allows us to describe a separable state of two qubits by using a state vector for each of the qubits. However, when we have an entangled state, this is not the case—we cannot attribute state vectors to individual qubits. We shall not discuss this problem in detail here, but let us mention that in order to describe one subsystem of a larger system, we are forced to generalize the concept of a quantum state to the density matrix. All the states which we have met so far have been described by a state vector $|\psi\rangle$ and are known as *pure* states. These can be rewritten as a density matrix of $\rho = |\psi\rangle\langle\psi|$. From this definition, we can see how unitary evolution must be represented, $\rho \rightarrow U|\psi\rangle\langle\psi|U^\dagger$. However, the point of introducing density matrices is that they are more general than pure states, and we can represent what are known as *mixed* states. These can be expressed in the form

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

where $\sum_i p_i = 1$, and cannot be written as a single state $|\psi\rangle\langle\psi|$. How does this relate to the state of a subsystem? Consider that we have a pure state over two subsystems A and B,

$$|\psi^{AB}\rangle = \sum \alpha_i |\psi_i^A\rangle |\psi_i^B\rangle,$$

but we would like to describe the state of just subsystem A. If we were to measure subsystem B, then we would get the result $|0^B\rangle$ with probability p_0 , leaving subsystem A in the (unnormalized) state

$$|\phi_0^A\rangle = \langle 0^B | \psi^{AB} \rangle = \sum \alpha_i |\psi_i^A\rangle \langle 0^B | \psi_i^B \rangle,$$

where $p_0 = \langle \phi_0^A | \phi_0^A \rangle$, and we can make similar statements for all the possible measurement results on subsystem B. If we wish to describe subsystem A, we do not measure B, but we can treat it as if we had measured it, but did not know the measurement result, i.e., subsystem A is in the state $|\phi_i^A\rangle\langle\phi_i^A|$ with probability p_i . The density matrix formalism allows us to describe this by

$$\rho_A = \sum_i |\phi_i^A\rangle\langle\phi_i^A|,$$

where the definitions of the states automatically encapsulate the probabilities. Mathematically, this procedure is known as taking the partial trace over subsystem B,

$$\rho_A = \text{Tr}_B(|\psi^{AB}\rangle\langle\psi^{AB}|) = \sum_i \langle i^B | \psi^{AB} \rangle \langle \psi^{AB} | i^B \rangle.$$

where the $|i^B\rangle$ can be any complete basis over subsystem B. The reduced density matrix ρ_A is a useful description to be able to determine the outcomes of actions applied only to subsystem A, and is also the first step in quantifying the amount of entanglement shared between two

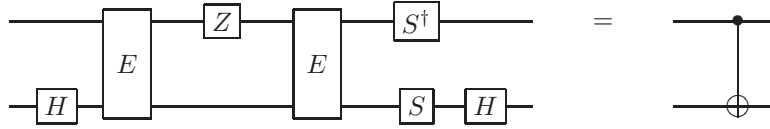
subsystems. Finally, it allows us to easily describe probabilistic operations. For example, if we started with a state ρ , it could experience a unitary rotation U with probability p , or nothing could happen with probability $1 - p$. If we don't know whether it happens or not, we have to take into account the fact that it might have happened by describing our new state as

$$\rho' = (1 - p)\rho + pU\rho U^\dagger.$$

For pure states, which are sufficient to describe ideal computations, state vectors and density matrices are entirely interchangeable, and we tend to stick to state vectors for simplicity.

18.7 Quantum Circuits

Many interesting quantum operations can be obtained by parallel and sequential compositions of quantum gates. For example, the circuit below, which you should read from left to right, effects the operation $(\mathbf{1} \otimes H)(S^\dagger \otimes S) E (Z \otimes \mathbf{1}) E (\mathbf{1} \otimes H)$, which you should read from right to left.



It shows how to construct the controlled-NOT with the square root of SWAP and two phase gates Z ($\varphi = \pi$) and S ($\varphi = \pi/2$) which occur often enough to warrant separate symbols

$$\text{---} \boxed{Z} \text{---} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{---} \boxed{S} \text{---} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

The square root of NOT, all possible phase gates and the square root of SWAP suffice to construct any unitary matrix acting on any number of qubits. These three operations do not have any classical analogues. Consequently, it should not be very surprising that most machines built out of these operations do not have any classical analogs and some of their properties are counter intuitive.

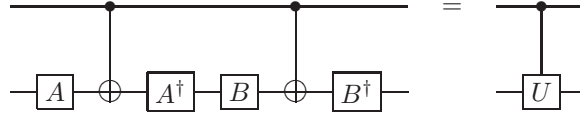
The square root of NOT, phase gates, and the square root of SWAP are not special; there are many sets of gates which can be combined to form all possible unitary operations. Such a set is said to be *universal*. Some gates are very popular because of their nice mathematical properties and some because of their simplicity of experimental implementation.

The gates $\{H, S, \text{c-NOT}\}$ are known as the **CLIFFORD** gates. The Clifford group contains all unitary operations that can be written as a product of tensor products of the Clifford gates and it plays an important role in the theory of quantum computation and quantum error correction. The Clifford gates are not universal, but it is known that **CLIFFORD** together with *any* other single-qubit gate, not generated by the gates in **CLIFFORD**, form a universal set of gates. Typically the standard discrete set of universal gates is **CLIFFORD** augmented by the phase gate $P_{\pi/4}$. It can be used to approximate any unitary operation.

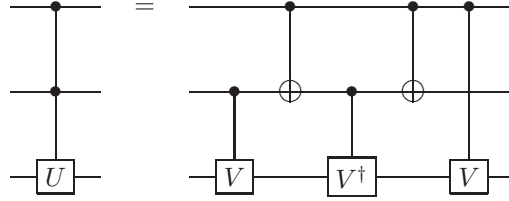
Given controlled-NOT we can implement any controlled- U , for some single-qubit unitary transformation U . The controlled- U gate (c- U) applies the identity transformation to the target qubit when the control qubit represents logical 0 and applies the operation U when the control qubit represents logical 1. Any unitary operation on a single qubit U , up to an overall phase factor, can be written as

$$U = B^\dagger X B A^\dagger X A,$$

for some unitaries A and B . Thus, any controlled- U operation can be constructed using controlled-NOT gates as



and, subsequently, any controlled-controlled- U as



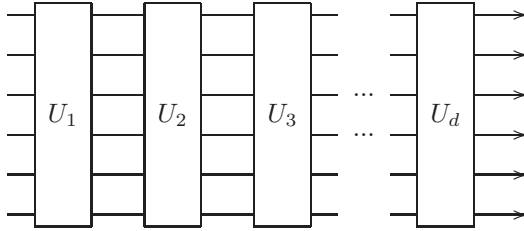
where V is any unitary matrix satisfying $V^2 = U$. The choice $V = \sqrt{\text{NOT}}$ leads to another useful gate, known as the controlled-controlled-NOT gate (c^2 -NOT), or the Toffoli gate. It flips the target only if the two control qubits are both set to 1 and does nothing otherwise. This gate appears frequently in circuits which evaluate Boolean functions and we shall discuss its action in more detail later on.

18.7.1 Economy of resources

Unitary operations on one qubit are described by 2×2 unitary matrices, on two qubits by 4×4 matrices, on three qubits by 8×8 matrices and, in general, on n qubits by $2^n \times 2^n$ matrices. The state vector of n qubits has 2^n complex components α_l which evolve as $\alpha'_k = \sum_{l \in \{0,1\}^n} U_{kl} \alpha_l$, i.e.,

$$\begin{bmatrix} \alpha'_{0\dots 00} \\ \alpha'_{0\dots 01} \\ \vdots \\ \alpha'_{1\dots 11} \end{bmatrix} = \begin{bmatrix} U_{0\dots 00,0\dots 00} & U_{0\dots 00,0\dots 01} & \dots & U_{0\dots 00,1\dots 11} \\ U_{0\dots 01,0\dots 00} & U_{0\dots 01,0\dots 01} & \dots & U_{0\dots 01,1\dots 11} \\ \vdots & \vdots & \ddots & \vdots \\ U_{1\dots 11,0\dots 00} & U_{1\dots 11,0\dots 01} & \dots & U_{1\dots 11,1\dots 11} \end{bmatrix} \begin{bmatrix} \alpha_{0\dots 00} \\ \alpha_{0\dots 01} \\ \vdots \\ \alpha_{1\dots 11} \end{bmatrix}.$$

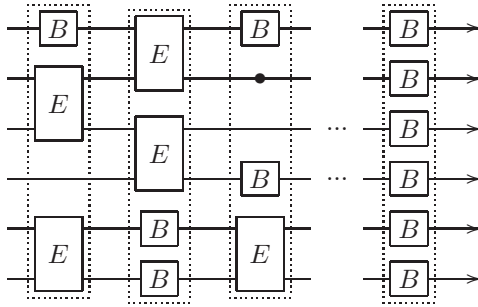
Quantum computation is a carefully controlled quantum interference which involves not one, but many qubits. A sequence of quantum operations on n qubits, $U_1, U_2, \dots, U_d$ can be visualized as the circuit



Each horizontal line represents one qubit. A complex quantum interference involving transitions between the 2^n basis states is described by the matrix product

$$U = U_d \cdots U_3 U_2 U_1.$$

However, each unitary operation U_k may have an internal structure—it may be composed of unitary operations acting in parallel on selected qubits, for example, as in the circuit below



We construct $U_1, U_2, \dots, U_d$ by taking tensor products of the elementary gates acting in parallel. For example, $U_1 = B \otimes E \otimes \mathbf{1} \otimes E$, $U_2 = E \otimes E \otimes B \otimes B$, etc. Thus, the whole circuit is a matrix product of tensor products of elementary gates.

Needless to say, building large quantum circuits requires large supplies of preselected quantum gates. The total number of gates in the circuit is called the size of the circuit. The depth of the circuit d is the number of time steps required to complete the computation, assuming that each gate operation takes one time step and that gates acting on distinct bits can operate simultaneously. This is the number of unitary layers made out of tensor products, i.e., $U_1, \dots, U_d$. The width of the circuit is the maximum number of gates that act in any one time step. How many different quantum gates do we need as our elementary building blocks and how many will be used in our constructions? This seemingly innocuous question is rather deep and leads to the studies of the universality of preselected components and the complexity of quantum circuits.

Any unitary operation on n qubits, i.e., any $2^n \times 2^n$ unitary matrix, can be constructed as a quantum circuit. Moreover, in order to accomplish this task, all we need is an ample supply of very few types of elementary gates. However, it should be stressed that no matter what

our choice of elementary building blocks, constructing a unitary operation on n qubits is not easy and the size of the circuit, C_n , usually grows very rapidly with n . In order to quantify this growth, we shall frequently use the asymptotic notation that suppresses multiplicative constants. Given a positive function $f(n)$, the symbol $O(f(n))$ means bounded from above by $c f(n)$ for some constant $c > 0$ (for sufficiently large n). For example, $15n^2 + 4n + 7$ is $O(n^2)$. Another common symbol, $\Omega(f(n))$, means bounded from below by $c f(n)$ for some constant $c > 0$, and $\Theta(f(n))$ means both $O(f(n))$ and $\Omega(f(n))$. A circuit is *polynomially bounded* if its size is $O(n^c)$ for some constant c . When we build quantum circuits, we care about the economy of resources; after all each gate we use may cost us money. Circuits with logarithmic $O(\log n)$, linear $O(n)$, or polynomial size are considered reasonable, whereas circuits with exponential size, $O(c^n)$, are viewed as rather expensive. We shall return to this point later on.

18.7.2 Computations

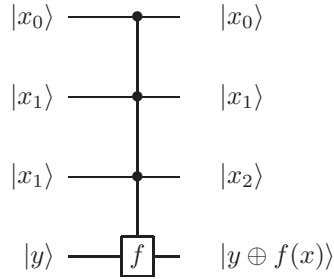
The circuits and quantum gates are more than just tools for constructing unitary operations. We want to give them some computational meaning, associate them with algorithms and quantify the complexity of these algorithms by patterns and numbers of gates in the corresponding circuits. Classical computers evaluate Boolean functions,

$$f : \{0, 1\}^n \mapsto \{0, 1\}.$$

Quantum computers embed it into reversible computation and evaluate as a unitary operation

$$U_f : |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle,$$

where $x \in \{0, 1\}^n$, $y \in \{0, 1\}$. The corresponding circuit diagram is (for $n = 3$),



and the unitary matrix can be written as

$$U = \sum_{x,y} |x, y \oplus f(x)\rangle \langle x, y| \equiv \sum_{x,y} |x\rangle \langle x| \otimes |y \oplus f(x)\rangle \langle y|,$$

with the summation over all $x \in \{0, 1\}^n$ and $y \in \{0, 1\}$.

Any Boolean function can be expressed as a formula containing only binary addition and multiplication. For example, the elementary Boolean operations, negation (NOT, $\neg$), disjunction (OR, $\vee$), and NAND ($\uparrow$) can be expressed in terms of addition $\oplus$ and multiplication $\times$ as

$$\neg a = 1 \oplus a \quad , \quad a \vee b = a \oplus b \oplus (a \times b) \quad , \quad a \uparrow b = 1 \oplus (a \times b),$$

where $a, b \in \{0, 1\}$. Once we have NOT, AND, and OR, we can write any Boolean function as a disjunction of conjunctions. For example, if a Boolean function $f(x_1, x_2, x_3, x_4)$ takes value 1 only for the string 0110, i.e., when $x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0$, then f can be expressed as a conjunction,

$$f(x_1, x_2, x_3, x_4) = \bar{x}_1 \wedge x_2 \wedge x_3 \wedge \bar{x}_4,$$

where we have written $\bar{x}_k$ instead of $\neg x_k$. If f takes value 1 only for the strings 0110 and 1000 then f can be expressed as a disjunction of the two conjunctions,

$$f(x_1, x_2, x_3, x_4) = (\bar{x}_1 \wedge x_2 \wedge x_3 \wedge \bar{x}_4) \vee (x_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4).$$

In general, any f can be written as a disjunction of conjunctions, which is called the disjunctive normal form (DNF). The corresponding formula can be easily deduced from the truth table of f —we find all the inputs $x = x_1x_2 \cdots x_n$ for which $f(x) = 1$, then for each particular string, a , such that $f(a) = 1$, we construct a conjunction, $f_a(x)$, such that $f_a(x) = 1$ if and only if $x = a$, and then we take the disjunction of all $f_a(x)$. We have also used COPY because each $f_a(x)$ in the disjunctive normal form expansion of f requires its own copy of x to act on.

Quantum function evaluation can then be implemented with quantum gates such as the controlled-NOT

$$|x\rangle|y\rangle \longrightarrow |x\rangle|x \oplus y\rangle,$$

which takes care of the binary addition, $\oplus$, in a reversible manner and the controlled-controlled-NOT (Toffoli gate)

$$|x\rangle|y\rangle|z\rangle \longrightarrow |x\rangle|y\rangle|z \oplus (x \times y)\rangle,$$

which takes care of the binary multiplication $\times$, or the logical AND, and effectively all the logical connectives we need for arithmetic.

The controlled-NOT also takes care of COPY of binary digits,

$$|x\rangle|0\rangle \longrightarrow |x\rangle|x\rangle,$$

for $x = 0, 1$. One might suppose that this gate could also be used to copy superpositions such as $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ so that

$$|\psi\rangle|0\rangle \longrightarrow |\psi\rangle|\psi\rangle,$$

for any $|\psi\rangle$. This is not so! The unitarity of the c-NOT requires that the gate turns superpositions in the control qubit into entanglement of the control and the target.

$$|\psi\rangle|0\rangle \longrightarrow \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle.$$

So far, our construction of a quantum circuit that computes f tacitly assumes that we know the truth table of f . Needless to say, this is not the case in real computation—we compute because we do not know the answer. There is a fundamental difference between constructing circuits using look-up tables and using simple prescriptions called algorithms, which describe

how to construct the function with $(n + 1)$ -bits of input from a function with n -bits of input. For the vast majority of Boolean functions $f : \{0, 1\}^n \mapsto \{0, 1\}$ we do not know any better way to “compute” f than to consult the look-up table. In fact, Claude Shannon used a simple gate counting argument to show that almost any Boolean function $f : \{0, 1\}^n \mapsto \{0, 1\}$ has a circuit size that is lower bounded by $2^n/n$, i.e., of $\Omega(2^n/n)$. We are interested in a tiny minority of Boolean functions to which this bound does not apply. Their circuits have patterns that we can spot. Any algorithm can be represented by a family of circuits $(C_1, C_2, C_3, \dots)$, where the circuit C_n acts on all possible input instances of size n bits. Any useful algorithm should have such a family specified by an example circuit C_n and a *simple rule* explaining how to construct the circuit C_{n+1} from the circuit C_n . These are called *uniform* families of circuits. An algorithm is said to be *efficient* if it has a uniform and polynomial-size family of circuits.

What makes this quantum evaluation of Boolean functions really interesting is its action on a superposition of different inputs x . For example,

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$$

produces $f(x)$ for all x in a single run and one may hope that this is the origin of the power of quantum computation. Unfortunately this is more complicated. We cannot learn all the values $f(x)$ from the entangled state $\sum_x |x\rangle|f(x)\rangle$ because any bit-by-bit measurement on the first n qubits will yield one particular value $x' \in \{0, 1\}^n$ and the final qubit will then be found with the value $f(x') \in \{0, 1\}$. In order to achieve novel results, different to classical computation, we usually sandwich the quantum function evaluation inbetween other operations, such as the Hadamard transform, and ask questions about some global properties of f that depend on many values of $f(x)$, e.g., periodicity. For example, the Mach–Zehnder interferometer allows us to determine an unknown relative phase $\varphi = \varphi_1 - \varphi_0$. In particular, if φ is guaranteed to be either 0 or π , we only require one photon to determine this, whereas, classically, two photons are required.

It turns out that in this case families of quantum circuits are more powerful than their classical counterparts. One such example is the factoring problem—given an n -bit number x , find a list of prime factors of x . The smallest known uniform classical family which solves the problem is of size $O(2^{d\sqrt{n \log n}})$, where d is a constant. In contrast, there exists a uniform family of quantum circuits of $O(n^2 \log \log n \log(1/\epsilon))$ size that solve the factoring problem. Since the outcomes of measurements are probabilistic, there is some chance of failure of quantum algorithms, and we describe an acceptable probability of a failure by the parameter ϵ . Of course, if such a failure occurs, we can readily detect it because testing if the product of two potential factors is equal to x is easy.

18.8 Summary

In this chapter, we have explored how computation is a physical process, and the workings of a computer are governed by the laws of physics. This has caused us to replace the classical description of a process, using probabilities and stochastic matrices, with a new description,

using probability amplitudes and unitary matrices. Many classical mathematical techniques translate to this new scenario, such as the composition of gates by tensor products and matrix multiplication, or that all possible operations can be decomposed in terms of a small number of building blocks, the universal gates. These new, quantum gates not only subsume the operations of a classical computer, but go well beyond them, allowing the possibility of intrinsically quantum algorithms that are more powerful than their classical counterparts.

Exercises

1. Conjunctive Normal Form (CNF) is where a Boolean function of the variables x_i is written as a conjunction (AND $\wedge$) of disjunctions (OR $\vee$) of literals. Any Boolean function can be written in this form. Take 2 variables, x_1 and x_2 . Write down, in conjunctive normal form, a Boolean function that returns 1 if the two variables are different, and 0 if the two variables are the same.

If a function f takes value 1 only for the strings 0110 and 1000, then it can be written in disjunctive normal form as

$$f(x_1, x_2, x_3, x_4) = (\bar{x}_1 \wedge x_2 \wedge x_3 \wedge \bar{x}_4) \vee (x_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4).$$

Rewrite this in CNF.

2. The SAT problem is the oldest known NP problem. That is, its solution is easy to verify but hard to find. The SAT problem asks whether there is a consistent solution for the variables x_i such that a function, written in CNF, gives the solution 1. Are there any solutions to the following function?

$$f(x_1, x_2, x_3, x_4, x_5) = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_2 \vee x_4 \vee x_5) \wedge (\bar{x}_1 \vee x_4)$$

What are the possible solutions?

If a function, f , (in CNF) has m sets of three variable disjunctions, and n variables x_i (this is known as the 3-SAT problem) then how would you expect the method you just applied to scale?

3. If you have a classical circuit that accepts n bits as inputs and produces a single bit as its output, then how many possible circuits are there? (i.e., how many unique functions are there?)

Consider constructing a circuit of s nodes. Each node accepts 2 input bits and outputs a single bit. How many different types of nodes are there?

We are free to choose the inputs to each node from any of the $n + s$ bits in the system, and we are free to choose the output of the computation from any of the s nodes. We can do this because a single bit can be input to any number of nodes.

For each node in the circuit, how many possible organizations are there? Hence, estimate the number of Boolean circuits of size s with n input bits. This is denoted by $C(n, s)$.

Estimate the number of functions computable with at most $s = 2^n/n$ gates. Hint: Use Stirling's approximation. Compare this to the number of possible circuits.

4. Let $|0\rangle, |1\rangle$ be an orthonormal basis for $\mathcal{H} = \mathbb{C}^2$. Write out the tensor product basis for $\mathcal{H} \otimes \mathcal{H}$.

Let P be the operator that exchanges subsystem 1 with subsystem 2. We say that $|v\rangle \in \mathcal{H} \otimes \mathcal{H}$ is symmetric if $P|v\rangle = |v\rangle$ and antisymmetric if $P|v\rangle = -|v\rangle$. Identify which elements of the tensor product basis are symmetric, antisymmetric, or none of both.

Symmetrize the vectors $|0\rangle \otimes |1\rangle$ and $|1\rangle \otimes |0\rangle$, i.e., find superpositions that are either symmetric or antisymmetric. Show that they form, together with $|0\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$ a basis of $\mathcal{H} \otimes \mathcal{H}$. Ensure that your result is normalized.

5. Show that if X is self-adjoint then $U = e^{iXt} = \sum_n \frac{(it)^n}{n!} X^n$ is unitary for any real t . Show that for any real α and for any X such that $X^2 = \mathbf{1}$

$$e^{i\alpha X} = \cos \alpha \mathbf{1} + i \sin \alpha X$$

6. Suppose the initial state of two qubits is a separable state $|a\rangle \otimes |b\rangle$. Let the two qubits be coupled via the interaction Hamiltonian,

$$H = \lambda \sigma \cdot \sigma \equiv \lambda (\sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z),$$

where λ is the coupling constant. This coupling is known as the Heisenberg, or the exchange, interaction. In matrix form in the computational basis the Hamiltonian can be written as

$$H = \lambda \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = 2\lambda \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

i.e., $\sigma \cdot \sigma = 2V - \mathbf{1}$, where V is the state swap operator $V|a\rangle|b\rangle = |b\rangle|a\rangle$ for any two vectors $|a\rangle$ and $|b\rangle$. Calculate the evolution due to this Hamiltonian after a time t .

Suppose the two qubits stop interacting after $t = \frac{\pi}{8\lambda}$. Show that this implements the square root of swap gate on the two qubits.

7. If two quantum states $|a\rangle$ and $|b\rangle$ are within a distance ε of each other, what is the maximum possible value of an element of the difference between the corresponding probability vectors of the two states?

19 Probabilistic Quantum Computation and Linear Optical Realizations

Norbert Lütkenhaus

19.1 Introduction

Quantum computation is usually thought of as a sequence of quantum gates. This sequence of gates decomposes the desired total unitary operation of our computation. It is followed by a measurement that extracts the result of the computation. In Chapter 11 a different concept is introduced and a specific, highly entangled input state prepared. The computation is performed by measuring out the individual systems in a specific pattern. Both approaches have one thing in common: in principle they work deterministic. In this chapter we introduce a concept of computation, which allows us to incorporate probabilistic elements into a computation which in the end becomes deterministic again. The reason for proceeding in this manner is that some specific physical systems do not allow implementing unitary operations that exactly implement basic two-qubit gates, e.g., a controlled-NOT (CNOT) operation. An example for such a physical system is an optical realization where qubits are represented by single photons with the polarization degree of freedom forming the two-dimensional Hilbert space. If we restrict the manipulation of such qubits to linear optics, that is, using only combinations of beam splitters and phaseshifters, we find that we cannot realize CNOT gates perfectly even if we add feed-forward with auxiliary photonic systems and photon-counting. Following the ideas outlined by Knill, Laflamme, and Milburn [3], with the concepts introduced in this chapter, we will see that one can use the same resources for universal computation with the help of probabilistic gates. We refer to this scheme as the KLM scheme.

We will introduce the basic mechanism, which shifts the difficulty of the gate operation from the direct deterministic operation to the problem of generation probabilistically an off-line resource of a certain auxiliary states. Then we will introduce more specifically the framework of linear optics and the realization of qubits. In the main section, we introduce the KLM scheme, which shows how one can realize universal computation using linear optics.

19.2 Gottesman/Chuang Trick

In this first section, we show that computation can be performed not only in the paradigm of quantum gates, but also by preparing entangled auxiliary states, measurements and single-qubit operations. The essential observation comes from an article by Gottesman and

Chuang [1]: Consider two qubits on which one would like to perform a CNOT operation. One can do so by using two teleportation steps (see Chapter 14), as shown in Fig. 19.1a, with a subsequent CNOT operation. Next, one can replace a set of single-qubit Pauli operators

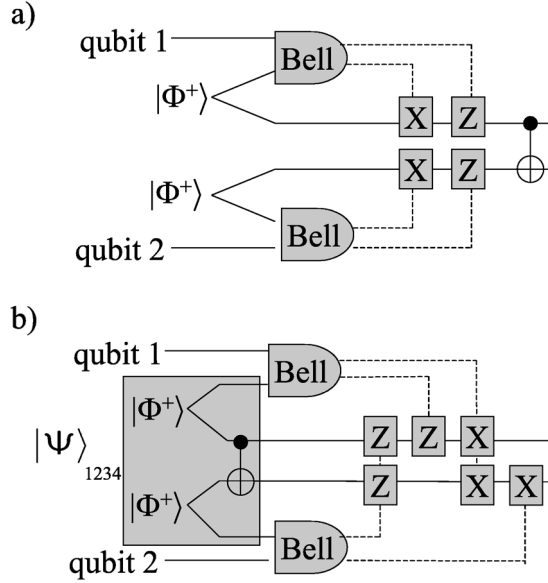


Figure 19.1. The teleportation procedure in (a) allows to shift the problem of deterministic gate performance to the probabilistic generation of the off-line resource of the state $|\Psi\rangle_{1,2,3,4}$.

followed by a CNOT gate by another arrangement where one first applies the CNOT gate and then applies a different set of Pauli operators. A simple set of translation rules (see Fig. 19.2) allows to calculate the required set of new Pauli operators. As a result, we can think of our device as preparing a new state $|\Psi\rangle_{1,2,3,4}$, which is then connected with the input qubits via Bell measurements. Then the application of Pauli operations effects a CNOT operation (see Fig. 19.1b).

With that we have performed a conceptually important step. The ability to produce the state $|\Psi\rangle_{1,2,3,4} = \text{CNOT}_{2,3}|\Phi^+\rangle_{1,2}|\Phi^+\rangle_{3,4}$, where the subscripts denote the qubits involved, together with the ability to perform the Bell measurements suffice to perform universal quantum computing. Typically, the generation of the required state $|\Psi\rangle_{1,2,3,4}$ is difficult, but now we have the opportunity to generate these state probabilistically. In repeated attempts, once we have successfully generated the state, we can use it deterministically in the scheme outlined above. Clearly, though, for this procedure we require quantum memory to store the qubits on which we want to perform the CNOT, until we succeed in creating the resource state $|\Psi\rangle_{1,2,3,4}$.

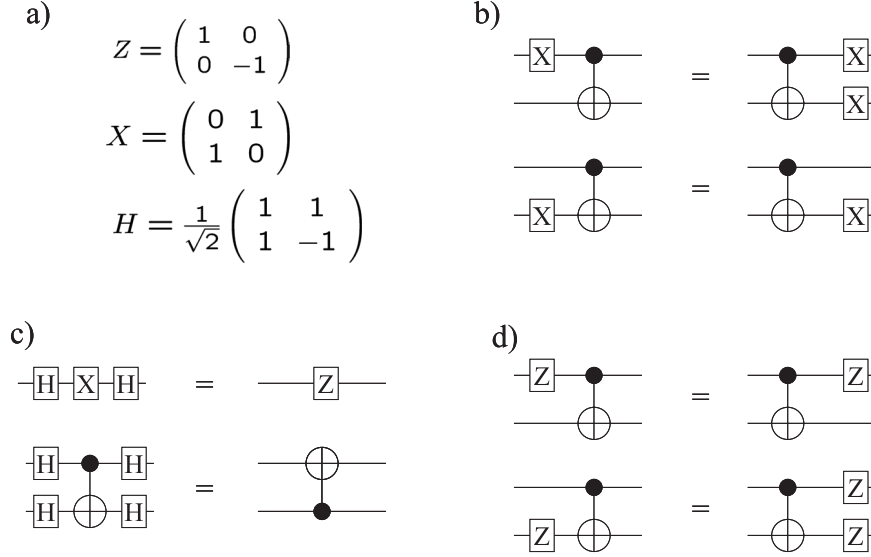


Figure 19.2. (a) The definition of the basic single-qubit operations. (b) One can verify directly these identities in the canonical basis of eigenstates of the Z operator. (c) The Hadamard transformation H provides useful identities so that the identities of b) directly lead to the identities of (d).

19.3 Optical Background

In this section we introduce the basic ideas from optics and show how to realize qubits in optics. Then we introduce a restricted class of optical operations, called linear optics, which are important in an experimental setting, as these operations can be implemented with basic optical tools, such as beam splitters and phaseshifters.

19.3.1 Optical qubits

The idea of Gottesman and Chuang is particularly important for the implementation of quantum logic operation with optical qubits. Typically, the qubits are represented by single photons, although other implementations have been proposed. In practice, there are no nonlinear optical interactions available that are strong enough to allow the implementation of unitary CNOT operations. However, as we will see, once we are able to use probabilistic operations, we can perform CNOT operations that succeed asymptotically with probability one even with linear optics alone. Before we come to this point, let us explain how one can implement qubits in optics.

The first implementation is the occupation-number qubit. It uses the superposition of Fock states of a single optical mode A . Here we have the logical basis states (where *occ* stands for

occupation number)

$$|\underline{0}\rangle_{occ} = |0\rangle_A \quad (19.1)$$

$$|\underline{1}\rangle_{occ} = |1\rangle_A. \quad (19.2)$$

On the left-hand side, the notations $\underline{0}$ and $\underline{1}$ denote logical values corresponding to an orthogonal basis set. On the right-hand side the ket-representation denotes the photon number in mode A . The problem with this qubit realization is that the qubit subspace is not formed of energy eigenstates, resulting in problems with decoherence, and that single-qubit operations are not readily available.

The most widespread implementation of a qubit is the bosonic qubit, also referred to as dual-rail encoding. Here one uses two optical modes A and B with one photonic excitation in total. The logical states of this system can be represented by

$$|\underline{0}\rangle_{\text{dual}} = |0, 1\rangle_{AB} \quad (19.3)$$

$$|\underline{1}\rangle_{\text{dual}} = |1, 0\rangle_{AB} \quad (19.4)$$

where the numbers on the right-hand side, e.g., in $|0, 1\rangle_{AB}$ refer again to the photonic excitation in modes A and B . An example of this implementation is a single photon with the polarization degree of freedom. The two modes are any two orthogonal polarization modes of the photon. In this case the qubit is part of an energy eigenspace. Moreover, single-qubit operations are simply polarization rotations of the photon in the Poincare sphere, which can be achieved easily.

Both representations are related as the dual rail encoding corresponds to two complementary photon-number qubit representation in its two modes. In that sense we have, for a general state, the relation

$$\alpha|\underline{0}\rangle_{\text{dual}} + \beta|\underline{1}\rangle_{\text{dual}} = \alpha|0, 1\rangle_{AB} + \beta|1, 0\rangle_{AB} = \alpha|\underline{0}, \underline{1}\rangle_{occ} + \beta|\underline{1}, \underline{0}\rangle_{occ}. \quad (19.5)$$

19.3.2 Linear Optics Framework

The work horse of optical experiments is the manipulation via linear optical elements, such as beam splitters and phaseshifters. This class of manipulations can be described using the creation and annihilation operators a_i and $a_i^\dagger$ of the involved optical modes $i = 1, \dots, N$. The basic properties of these operators are given by their commutation relation $[a_i, a_j^\dagger] = \delta_{i,j}$, $[a_i, a_j] = 0$, $[a_i^\dagger, a_j^\dagger] = 0$ and by their operation on the Fock states, $a|n\rangle = \sqrt{n}|n-1\rangle$, $a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$. Then a beam splitter can be described by a unitary operation $U_{\text{BS}} = e^{i\theta(a_1^\dagger a_2 + a_1 a_2^\dagger)}$, where the real number θ determines the transmittivity of the beam splitter. A phaseshifter acts with the unitary operation $U_P = \exp(i\phi a^\dagger a)$, where the real number ϕ is the value of the optical phaseshift. Actually, any combination of phaseshifters and beam splitters on N modes can be described by the unitary evolution operator [8]

$$U_{\text{LO}} = e^{-i\vec{a}^\dagger \Lambda \vec{a}}, \quad (19.6)$$

where Λ is a Hermitian $N \times N$ matrix and $\vec{a} = (a_1, a_2, \dots, a_N)$. We can understand the action of this evolution in the Heisenberg picture and find between input and output mode

operators the relation

$$\vec{a}_{\text{out}} = e^{-i\Lambda} \vec{a}_{\text{in}} . \quad (19.7)$$

The action of any linear optical network can be given in the form of Eq. (19.7). Moreover, Reck et al. [7] have also shown that any input–output relation of the form of Eq. (19.7) can be realized by a combination of beam splitters and phaseshifters. The number of required optical elements scales as N^2 with the number of involved optical modes.

Unfortunately, the interaction provided by linear optics does not suffice to implement exact Bell measurements on polarization qubits [4]. Nevertheless, as we will see below, it is possible to approximate a Bell measurement with arbitrary precision with rising costs of resources, e.g. in the form of highly entangled states. We refer to this as a near-deterministic process. The production of the entangled states required in the Gottesman–Chuang trick cannot be prepared deterministically, and here we will see later how to do this probabilistically with linear optics.

19.4 Knill–Laflamme–Milburn (KLM) scheme

So far we have learned that computation can be performed by a combination of preparation of auxiliary states, measurements, and single-qubit operations. It turns out that the Bell measurements required in the Gottesman–Chuang trick cannot be implemented perfectly with linear optics. Moreover, the generation of entangled auxiliary states is hard to achieve in general. Knill, Laflamme, and Milburn solved this problem in several steps. In the first step, they extended the Gottesman–Chuang procedure on the qubit level and then showed that the measurements required for this extended scheme can be implemented by linear optics near deterministically. That is, the probability of failure can be made arbitrary small with increasing resources, e.g., the number of qubits in the required auxiliary state. To solve the problem of preparation of these auxiliary states they made use of the fact that the auxiliary states can be generated probabilistically without affecting the overall computation. We will show how a set of universal gates can be implemented probabilistically with linear optics.

19.4.1 Extension of Gottesman–Chuang trick

We start by extending the procedure of Gottesman and Chuang on the abstract level of qubits. In the extension we use not only a maximally entangled state of 2 qubits, but a state $|\Phi_{2n}^+\rangle$ of $2n$ qubits, numbered $1, \dots, 2n$. This state is described by the equation

$$|\Phi_{2n}^+\rangle = \sum_{j=0}^n \underbrace{|\underline{1}\rangle^j |\underline{0}\rangle^{n-j}}_{n \text{ first qubits}} \underbrace{|\underline{0}\rangle^j |\underline{1}\rangle^{n-j}}_{n \text{ last qubits}}, \quad (19.8)$$

where we use terms like $|\underline{1}\rangle^j$ as a short hand for the state $\overbrace{|\underline{1}\rangle \dots |\underline{1}\rangle}^{j \text{ times}}$.

To see how one can use this state to teleport a general input $\alpha|\underline{0}\rangle_0 + \beta|\underline{1}\rangle_0$ prepared in qubit 0, let us proceed in two steps. In the first step we perform a measurement on the input qubit and on the first n qubits of the state $|\Phi_{2n}^+\rangle$. It is a quantum nondemolition (QND)

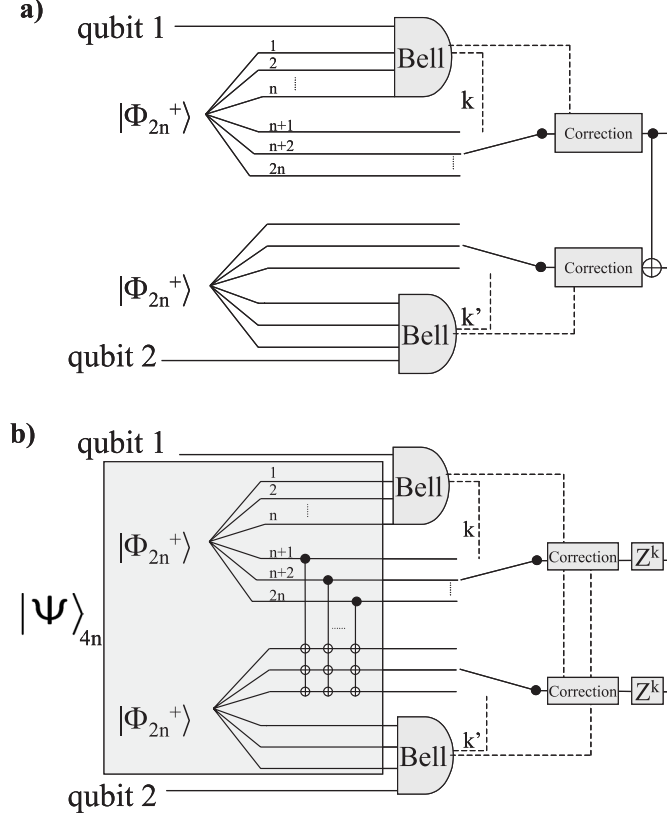


Figure 19.3. (a) The basic trick of Gottesman and Chuang can be extended using the two pairs of input states $|\Phi_{2n}^+\rangle$ with $2n$ qubit each, as given in the text. As a result of the extended Bell measurement, one finds the teleported qubit in qubit k , which is then selected. After this teleportation, one has to apply a correction operation on that qubit before applying the CNOT gate. (b) In the replacement picture, one first applies generalized CNOT gates to the input states. Then, after the Bell measurements, one performs correction operations. Here we explicitly wrote the correction Z^k that becomes necessary because of the influence of the nonselected qubits via the generalized CNOT gates.

measurement of the total number of qubits being in the state $|1\rangle$. The QND measurement with outcome k effects a projection of the input state onto a subspace spanned by all qubit states of input and the first n qubits with exactly k qubits in state $|1\rangle$. The range of the result k is $[0, \dots, n+1]$. For the inner values $0 < k < n+1$, that is, for $k \neq 0$ and $k \neq n+1$, we find the conditional state

$$|\phi_{\text{out}}^k\rangle = \alpha|0\rangle_0|1\rangle^k|0\rangle^{n-k}|0\rangle^k|1\rangle^{n-k} + \beta|1\rangle_0|1\rangle^{k-1}|0\rangle^{n-k+1}|0\rangle^{k-1}|1\rangle^{n-k+1}. \quad (19.9)$$

Obviously, only the qubits $0, k$, and $n+k$ differ in the terms of the superposition. Omitting

the remaining qubits, we have

$$|\phi_{\text{out}}^k\rangle = \alpha|\underline{0}\rangle_0|\underline{1}\rangle_k|\underline{0}\rangle_{n+k} + \beta|\underline{1}\rangle_0|\underline{0}\rangle_k|\underline{1}\rangle_{n+k}. \quad (19.10)$$

Now we perform a measurement to project out the qubits 0 and k to recover the teleported state in qubit k . Any measurement on qubits 0 and k will serve our purpose as long as all of its outcomes project onto states of the form $\frac{1}{2}(e^{i\varphi_0}|\underline{0}\rangle_0|\underline{1}\rangle_k + e^{i\varphi_1}|\underline{1}\rangle_0|\underline{0}\rangle_k)$. Then we find the conditional state $\alpha|\underline{0}\rangle_{n+k} + e^{i(\varphi_1-\varphi_0)}\beta|\underline{1}\rangle_{n+k}$, up to an unimportant global phase. The relative phase between the two terms depends on the measurement outcome of this last step. It is therefore known and can be corrected by applying a single-qubit operation. Therefore, once we find $0 < k < n$, we have successfully teleported the state of qubit 0 to the qubit $n+k$. This qubit can then be selected to be the output qubit.

In the case where we find for k the value 0 or $n+1$, only one term appears in the expression of the conditional state, and the teleportation attempt fails since the input state is effectively measured to be $|\underline{0}\rangle_0$ or $|\underline{1}\rangle_0$. This happens with the total failure probability $\frac{1}{n+1}$, which is independent of the input state. If there were a dependence, then the fact that one does not obtain these values would give away information about the input state, which contradicts the assumption of perfect teleportation. For a growing n the failure probability goes to zero, so that we have a near-deterministic teleportation.

Let us come back to the implementation with linear optics. The extension of the Gottesman–Chuang trick as described above is important since the measurement outlined above can be performed by linear optics alone. Before discussing this measurement let us show how these measurements can be used to implement a CNOT operation on two qubits. The total network is shown in Fig. 19.3a and uses a generalisation of the CNOT operation where not only one, but several qubits are affected by a bit-flip operator X conditioned on the state of the source qubit. Here we use it after the generalized Bell measurement. The knowledge of k tells us not only which qubit carries the input signal (up to the operation which corrects the relative phase), but we project also the input modes $1, \dots, n$, without k , into a definite state. Therefore, we can apply correcting bit-flip operations X for all those generalized CNOT operations that were conditioned on these qubits. More specifically, we have to apply the operation Z^{k-1} whenever the input qubit is teleported to output qubit k .

It turns out that one can again interchange the multi-qubit operations with the set of single-qubit operations as shown in Fig. 19.3b, although the exact form of the single-qubit operations goes beyond the scope of this section.

19.4.2 Implementation with linear optics

In the previous section we found an extension to the procedure of Gottesman and Chuang which performs quantum computation with auxiliary states and measurements. Although this operation is now no longer deterministic, the success probability can be brought arbitrarily close to one so that we refer to this as near deterministic. What we want to show next is that we can implement the measurements introduced in this scheme by linear optics alone.

Looking back at the two steps of the extended Bell measurement, which we introduced above, what we need to do is to perform a projection measurement on the input qubit and the first n qubits of the state $|\Phi_{2n}^+\rangle$ in such a way that we learn the number of qubits being in

the state $|\underline{1}\rangle$, but we cannot trace back which qubits were in this state. In the implementation with dual-rail bosonic qubits, one needs to perform a *complete* measurement on the $n + 1$ first modes of the $n + 1$ dual-rail qubits, and also in a second step of the $n + 1$ second modes of these qubits, so that we have no information from which modes the photons came. The two measurements, on the first and on the second mode of each qubit, are identical, so we first concentrate on a measurement on the first set of modes.

Actually, a linear optical network realizing a discrete Fourier transform on the $n + 1$ first modes followed by a photon-number measurement in these modes serves our purpose. It is described by the input–output relations for the annihilation operators of these $n + 1$ modes, denoted by $\vec{a}$, as

$$\vec{a}_{\text{out}} = F_{n+1} \vec{a}. \quad (19.11)$$

The matrix F_{n+1} has matrix elements $\{F_{n+1}\}_{pq} = \frac{e^{i2\pi pq/(n+1)}}{\sqrt{n+1}}$. This transformation is a special case of Eq. (19.7). It can therefore be implemented by linear optics with the number of optical elements scaling as n^2 . Clearly, this type of measurement gives us the value k via the total number of registered photons. The value k indicates where to find the teleported qubit. One can calculate what happens to the two remaining contributions once we observe a certain pattern of photon detections in the $n + 1$ output modes. It turns out [3] that the photon detection pattern determines the relative phase between the two contribution, which can be compensated by a local optical phaseshift on the first mode of qubit $n + k$, which influences the phase of the $|\underline{1}\rangle_{n+k}$ state, while it leaves the state $|\underline{0}\rangle_{n+k}$ invariant.

The same type of measurement is then performed on the second modes of the dual rail qubits of input and the first n qubits, so that we complete the decoupling of the output qubit $n + k$ from the qubits 0 and k in Eq. (19.10). Necessarily, the total photon number after this second Fourier transform will now be $n + 1 - k$. This allows us to detect whether some loss of photons occurred in the set-up, either in the linear optical elements or in the photon detectors themselves. Loss will lead to a failure of the teleportation step, although we do not consider it here. Still, the exact pattern of photon detection gives rise again to a relative phase between the two contributions in the teleportation step, and can now be corrected by a single-qubit operation on the output qubit $n + k$.

19.4.3 Offline probabilistic gates

In the previous sections we have seen how we can perform universal quantum computation by measurements that can be realized by linear optics. As a prerequisite we need some entangled auxiliary states. We now demonstrate how to generate these entangled states using only linear optics. For this we make use of the fact that these states can be generated probabilistically, as they are now an off-line resource that is integrated into our computation scheme only once we succeed in generating the state.

Here we do not demonstrate how to generate the exact auxiliary state which we require in the KLM scheme. Instead we show that one can realize a universal set of gates probabilistically via linear optics, so that in principle any quantum state of dual-rail qubits can be generated.

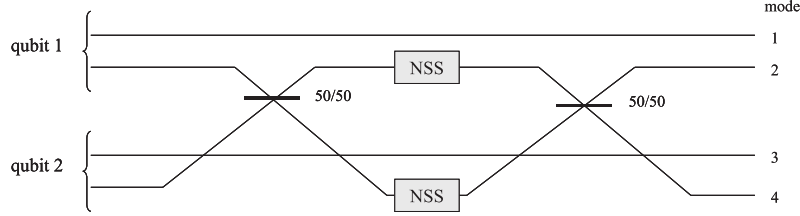


Figure 19.4. A CSIGN gate can be implemented using two nonlinear sign shift gates. (See text). Both beam splitters have equal transmission and reflection coefficients.

The single photon sources prepare initial states $|0\rangle$, e.g., via the polarization state of the generated photon. Single-qubit operations are simple polarization rotations. So we are left to show that we can probabilistically implement at least one two-qubit operation which allows us to complete a universal set of gates. We choose here the controlled SIGN (CSIGN) gate which realizes the unitary mapping

$$|0, 0\rangle \rightarrow |0, 0\rangle \quad (19.12)$$

$$|0, 1\rangle \rightarrow |0, 1\rangle \quad (19.13)$$

$$|1, 0\rangle \rightarrow |1, 0\rangle \quad (19.14)$$

$$|1, 1\rangle \rightarrow -|1, 1\rangle. \quad (19.15)$$

In the optical implementation of dual-rail qubits, this gate can be decomposed as shown in Fig. 19.4. This decomposition utilizes an operation which is no longer based on the qubit idea: the nonlinear-sign-shift gate (NSS) acts on the Fock space of a single mode with up to two excitations. The unitary operation is defined as

$$\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle \xrightarrow{\text{NSS}} \alpha_0|0\rangle + \alpha_1|1\rangle - \alpha_2|2\rangle. \quad (19.16)$$

Clearly, this operation cannot be realized by linear optics deterministically. However, it is sufficient to generate this transformation probabilistically within the domain of linear optics. Here we show how to do this.

The NSS operation acts as the identity operation on the Fock space with 0 or 1 photons. In the complete set-up of Fig. 19.4, two photons can enter the NSS gate devices only if both qubits are in the state $|1\rangle$, since in that case the interference effects assure that there are two photons either in mode 2 or in mode 4. More precisely, the beam splitter BS_1 acting on modes 2 and 4 realizes the transformation

$$|1, 1\rangle_{2,4} \rightarrow \frac{1}{\sqrt{2}} (|2, 0\rangle - |0, 2\rangle). \quad (19.17)$$

Then the two NSS-devices assure that both terms acquire a minus sign. The second beam splitter BS_2 then recombines the states in a way that restores the dual-rail qubit form so that we obtain overall the output state $-|1, 1\rangle_{2,4}$. In all, this effects the CSIGN gate on the dual rail qubits.

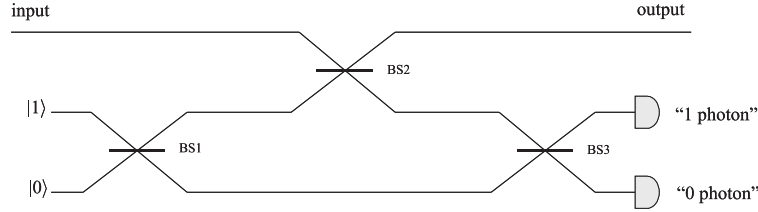


Figure 19.5. A probabilistic nonlinear sign shift gate can be implemented using a single photon source and three beam splitters. For the values of the transmittivities see text. The gate works successfully if the upper detector detects one photon, while the lower detector does not detect a photon.

So far, we shifted the problem of generating the CSIGN gate to the implementation of the NSS gate. A probabilistic implementation has been proposed by Knill, Laflamme, and Milburn [3]. It uses three beam splitters, one auxiliary photon and two photodetectors. The scheme is sketched in Fig. 19.5. The NSS gate works successfully whenever the detector D_1 detects exactly one photon, and the detector D_2 registers no photon. The calculations are straightforward [6], and one finds that the required beam-splitting ratios are given by $\eta_2 = (\sqrt{2} - 1)^2$ and $\eta_1 = \eta_3 = \frac{1}{4-2\sqrt{2}}$. The success probability of such an NSS gate is $1/4$, so that the construction of a CSIGN gate based on two NSS gate operations succeeds with probability of $\frac{1}{16}$. One can optimize the linear optical set-up for a CSIGN operation directly and finds an improved success probability of $2/27$ [2]. There are different set-ups to realize gates, using also polarization entangled photon pairs to realize gates [5]. For us, however, it is important to see that one can indeed realize probabilistically a set of universal gates, so that with some probability of success we can engineer the states which are required to perform near-deterministic gate operations of the CNOT gate.

References

- [1] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402**, 390–393, 1999.
- [2] E. Knill. Quantum gates using linear optics and postselection. *Phys. Rev. A*, **66**, 052306, 2002.
- [3] E. Knill, R. Laflamme, and G. Milburn. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46, 2001.
- [4] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen. Bell measurements for teleportation. *Phys. Rev. A* **59**, 3295–3300, 1999.
- [5] T. B. Pittman, B. C. Jacobs, and J. D. Franson. Demonstration of nondeterministic quantum logic operations using linear optical elements. *Phys. Rev. Lett.* **88**, 257902, 2002.
- [6] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn. Simple scheme for efficient linear optics quantum gates. *Phys. Rev. A* **65**, 012314, 2002.
- [7] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73**, 58–61, 1994.
- [8] W. Vogel, D.-G. Welsch, and S. Wallentowitz. *Quantum Optics: An Introduction*. Wiley-VCH, Berlin, 2nd edition, 2001.

20 One-way Quantum Computation

Dan Browne and Hans J. Briegel

20.1 Introduction

The circuit model of quantum computation [1–3] has been a powerful tool for the development of quantum computation, acting both as a framework for theoretical investigations and as a guide for experiment. In the circuit model (also called the network model), unitary operations are represented by a network of elementary quantum gates such as the CNOT gate and single-qubit rotations. Many proposals for the implementation of quantum computation are designed around this model, including physical prescriptions for implementing the elementary gates. By formulating quantum computation in a different way, one can gain both a new framework for experiments and new theoretical insights. *One-way quantum computation* [4] has achieved both of these.

Measurements on entangled states play a key role in many quantum information protocols, such as quantum teleportation and entanglement-based quantum key distribution. In these applications an entangled state is required, which must be generated beforehand. Then, during the protocol, measurements are made which convert the quantum correlations into, for example, a secret key. To repeat the protocol a fresh entangled state must be prepared. In this sense, the entangled state, or the quantum correlations embodied by the state, can be considered a resource which is “used up” in the protocol.

In one-way quantum computation, the quantum correlations in an entangled state called a *cluster state* [6] or *graph state* [7] are exploited to allow universal quantum computation through single-qubit measurements alone. The quantum algorithm is specified in the choice of bases for these measurements and the “structure” of the entanglement (as explained below) of the resource state. The name “one-way” reflects the resource nature of the graph state. The state can be used only once, and (irreversible) projective measurements drive the computation forward, in contrast to the reversibility of every gate in the standard network model.

In this chapter, we will provide an introduction to one-way quantum computation, and several of the techniques one can use to describe it. In this section we will introduce graph and cluster states and develop a notation for general single-qubit measurements. In Section 20.2 we will introduce the key concepts of one-way quantum computation with some simple examples. After this, in Section 20.3, we shall investigate how one-way quantum computation can be described without using the quantum circuit model. To this end, we shall introduce a number of important tools including the stabilizer formalism, the logical Heisenberg picture and a representation of unitary operations especially well suited to the one-way quantum computa-

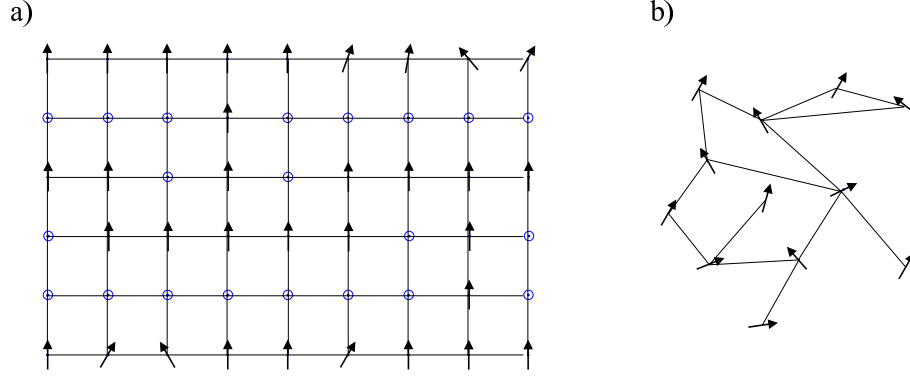


Figure 20.1. One way quantum computation consists of single-qubit measurements in certain bases and in a certain order on an entangled resource state. Cluster states have a square lattice structure (a) while the freedom of choosing specific general graph states such as illustrated in (b) can reduce the number of qubits needed for a given computation significantly.

tion model. In Section 20.4, we will briefly describe a number of proposals for implementing one-way quantum computation in the laboratory. In Section 20.5 we will conclude with a brief survey of some recent research developments in measurement-based quantum computation.

A different perspective of one-way quantum computation and measurement-based computation in general can be found in these recent reviews [8, 9]. A comprehensive tutorial and review on the properties of graph states can be found in [10].

20.1.1 Cluster states and graph states

Cluster states and graph states can be defined constructively in the following way [6, 10]. With each state, we associate a graph, a set of vertices and edges connecting vertex pairs. Each vertex on the graph corresponds to a qubit. The corresponding “graph state” may be generated by preparing every qubit in the state $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ and applying a controlled σ_z (CZ) operation $|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_z$ on every pair of qubits whose vertices are connected by a graph edge. Cluster states are a sub-class of graph states, whose underlying graph is an n -dimensional square grid. The extra flexibility in the entanglement structure of graph states means that they often require far fewer qubits to implement the same one-way quantum computation. However, there are a number of physical implementations where the regular layout of cluster states means that they can be generated very efficiently (see Section 20.4).

20.1.2 Single-qubit measurements and rotations

Single-qubit measurements in a variety of bases play a key role in one-way quantum computation, so here we introduce a convenient and compact way to describe them. Using a Bloch sphere picture, every projective single-qubit measurement can be associated with a unit vector on the sphere, which corresponds to the $+1$ eigenstate of the measurement. We can then

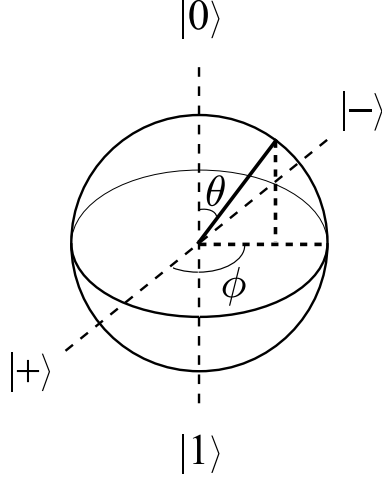


Figure 20.2. Single-qubit projective measurements will be represented by the pair of angles (θ, ϕ) of the co-latitude θ and longitude ϕ of their $+1$ eigenstate on the Bloch sphere. This corresponds to a measurement of the observable $U_z(\phi + \pi/2)U_x(\theta)ZU_x(-\theta)U_z(-\phi - \pi/2)$.

parameterize observables by the co-latitude θ and longitude ϕ of this vector (illustrated in figure 20.2). We shall write this compactly as a pair of angles (θ, ϕ) .

Unitary operations corresponding to rotations on the Bloch sphere have the following form. A rotation around the k axis (where k is x , y , or z) by angle ϕ can be written

$$U_k(\phi) = e^{-\frac{i\phi}{2}\sigma_k}. \quad (20.1)$$

For brevity and clarity, we will use the notation $X \equiv \sigma_x$, etc. in the rest of this chapter. We also adopt standard notation for the eigenstates of Z and X :

$$\begin{aligned} Z|0\rangle &= |0\rangle \\ -Z|1\rangle &= |1\rangle \\ X|+\rangle &= |+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ -X|-\rangle &= |-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \quad (20.2)$$

A measurement with angles (θ, ϕ) corresponds to a measurement of the observable $U_z(\phi + \pi/2)U_x(\theta)ZU_x(-\theta)U_z(-\phi - \pi/2)$. One way of implementing such a measurement is to apply the single-qubit unitary $U_x(-\theta)U_z(-\phi - \pi/2)$ to the qubit before measuring it in the computational basis.

20.2 Simple examples

Many of the features of one-way quantum computation can be illustrated in a simple two-qubit example. Consider the following simple protocol; a qubit is prepared in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. A second qubit is prepared in the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. A CZ operation is applied on the two qubits. The state of the qubits is then

$$\frac{1}{\sqrt{2}}(\alpha|0\rangle|+\rangle + \beta|1\rangle|-\rangle). \quad (20.3)$$

The first qubit is now measured in the basis $\{(1/\sqrt{2})(|0\rangle \pm e^{i\phi}|1\rangle)\}$, where ϕ is a real parameter. Using the notation introduced in Section 20.1.2 this measurement is denoted $(\pi/2, \phi)$. This corresponds, in the Bloch sphere picture, to a unit vector in the x - y plane at angle ϕ to the x axis. There are two possible outcomes to the measurement, which occur with equal probability. If the measurement returns the $+1$ eigenvalue, the second qubit will be projected into the state

$$\alpha|+\rangle + e^{i\phi}\beta|-\rangle. \quad (20.4)$$

If the -1 eigenvalue is found the state of qubit two becomes

$$\alpha|+\rangle - e^{i\phi}\beta|-\rangle. \quad (20.5)$$

We can represent both possibilities in a compact way if we introduce the binary digit $m \in \{0, 1\}$ to represent a measurement outcome of $(-1)^m$. The state of qubit two can then be written, up to a global phase,

$$X^m H U_z(\phi) |\psi\rangle. \quad (20.6)$$

We see that the unknown input state which was prepared on the first qubit has been transferred to qubit two without any loss of coherence. In addition to this it has undergone a unitary transformation: $X^m H U_z(\phi)$. Notice that the angle of the rotation $U_z(\phi)$ is set in the choice of measurement basis. The unitary transformation $H U_z(\phi)$ is accompanied by an additional Pauli transformation (X) when the measurement outcome is -1 . This is a typical feature of one-way quantum computation; due to the randomness of the measurement outcomes, any desired unitary can be implemented only up to random but known Pauli transformations. Since these Pauli operators are an undesired by-product of implementing the unitary in the one-way model, we call them “by-product operators” [4,5]. As we shall see below, these extra Pauli operations can be accounted for by altering the basis of later measurements, making the scheme deterministic but introducing an unavoidable time-ordering.

In Fig. 20.3a, this protocol is represented using a graphical notation that we will use throughout this chapter. The input qubit is represented by a square, and the output qubit by a lozenge, a smaller square tilted at 45° . The CZ operation applied to the two qubits is represented by a line between them. This is an example of a one-way graph and measurement pattern, or “one-way pattern” for short, a convenient representation which specifies both the entanglement graph for the resource state and the measurements required to implement a unitary operation (always up to a known but random Pauli transformation) in the one-way model. As an alternative to this graphical approach, an algebraic representation of one-way patterns called the “measurement calculus” has been developed recently [12].

So far, the protocol described above seems rather different from the description of one-way quantum computation as a series of measurements on a special entangled resource state. We shall see below how the two pictures are related. First however, we show how one-way patterns may be connected together to perform consecutive operations.

20.2.1 Connecting one-way patterns - arbitrary single-qubit operations

Due to Euler’s rotation theorem any single-qubit $SU(2)$ rotation can be decomposed as a product of three rotations $U_z(\gamma)U_x(\beta)U_z(\alpha)$. Thus, by repeating the simple two-qubit protocol

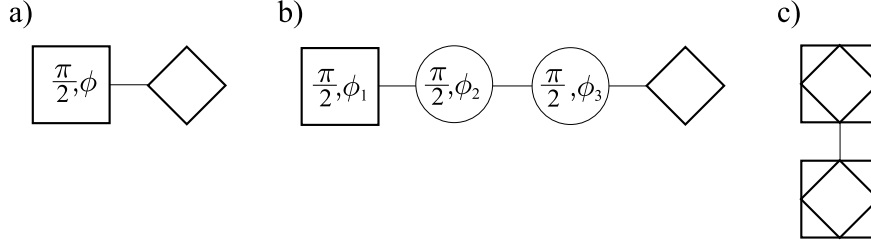


Figure 20.3. The one-way graph and measurement patterns for a) the single-qubit operation $HU_z(\phi)$ and b) an arbitrary single-qubit operation, $U_z(\gamma)U_x(\beta)U_z(\alpha)$, when the measurement angles are set $\phi_1 = \alpha$, $\phi_2 = (-1)^{m_1}\beta$ and $\phi_3 = (-1)^{m_2}\gamma$, and m_a is the binary measurement outcome of the measurement on qubit a . Note that this imposes an ordering in the measurements of this pattern. This second pattern is made by composing three copies of the pattern (a) with differing measurement angles as described in the text. Pattern (c) implements a CZ operation. Input and output qubits coincide for this pattern.

three times, any arbitrary single-qubit rotation may be obtained (up to an extra Hadamard, which can be accounted for). Two one-way patterns are combined as one would expect, the output qubit(s) of one pattern become the input qubit(s) of the next. The main issue in connecting patterns together is to track the effect of the Pauli by-product operators which have accumulated due to the previous measurements.

Concatenating the two-qubit protocol three times, with different angles ϕ_1 , ϕ_2 and ϕ_3 gives the one-way pattern illustrated in Fig. 20.3 (b). To see the effect of the by-product operators from each measurement, let us label the binary outcome from each m_a . The unitary implemented by the combined pattern is therefore

$$U = HZ^{m_3}U_z(\phi_3)HZ^{m_2}U_z(\phi_2)HZ^{m_1}U_z(\phi_1). \quad (20.7)$$

Since $HZH = X$ and $HU_z(\phi)H = U_x(\phi)$ this can be rewritten

$$HZ^{m_3}U_z(\phi_3)X^{m_2}U_x(\phi_2)Z^{m_1}U_z(\phi_1). \quad (20.8)$$

We can rewrite this further using the identities $XU_z(\phi) = U_z(-\phi)X$ and $ZU_x(\phi) = U_x(-\phi)Z$,

$$X^{m_3}Z^{m_2}X^{m_1}HU_z((-1)^{m_2}\phi_3)U_x((-1)^{m_1}\phi_2)U_z(\phi_1). \quad (20.9)$$

Now we have split up the operation in the same way as the two-qubit example, a unitary plus a known Pauli correction. In this case, however, this unitary is not deterministic – the sign of two of the rotations depends on two of the measurements. Nevertheless, if we perform the measurements sequentially and choose measurement angles $\phi_1 = \alpha$, $\phi_2 = (-1)^{m_1}\beta$ and $\phi_3 = (-1)^{m_2}\gamma$, we obtain deterministically the desired single-qubit unitary.

The dependency of measurement bases on the outcome of previous measurements is a generic feature of one-way quantum computation, occurring for all but a special class of operations, the Clifford group (described below). This dependency means that there is a minimum

number of time-steps in which any one-way quantum computation can be implemented, as discussed further in Section 20.3.

The Pauli corrections remaining at the end of the implemented one-way quantum computation are unimportant and never need to be physically applied; they can always be accounted for in the interpretation of the final measurement outcome. For example, if the final state is to be read out in the computational basis any extra Z operations commute with the measurements and have no effect on their outcome. Any X operations simply flip the measurement result, and thus can be corrected via classical post-processing.

20.2.2 Graph states as a resource

It is worth discussing how the above description of one-way patterns relates to the description of one-way quantum computation in the introduction, namely as measurements on an entangled resource state. The first observation is that, given a one-way pattern, all of the measurements can be made after all the CZ operations have been implemented. Secondly, quantum algorithms usually begin by initializing qubits to a fiducial starting state. This state is usually $|0\rangle$ on each qubit, but the state $|+\rangle$ would be equally suitable. When the input qubits of a one-way graph measurement pattern are prepared in $|+\rangle$, then the entangled state generated by the CZ gates is a graph state. Thus the graph state can be considered a resource for this quantum computation. We shall see in Section 20.4 that for certain implementations, such as in linear optics, the resource description is especially apt.

20.2.3 Two-qubit gates

So far we have seen how an arbitrary single-qubit operation could be achieved in one-way quantum computation in a simple linear one-way pattern. However, for universal quantum computation, entangling two-qubit gates are necessary. One such gate is a CZ gate. There is a particularly simple way in which the CZ can be implemented within the one-way framework. This is simply to use the CZ represented by a single graph-state edge to implement the CZ directly. This leads to the one-way pattern illustrated in Fig. 20.2 (c). Notice that here the input qubits are also the output qubits. This is indicated by the superimposed squares and lozenges.

20.2.4 Cluster-state quantum computing

In a number of proposed implementations of one-way quantum computation (see Section 20.4) square lattice cluster states can be generated efficiently and arbitrarily connected graph states are hard to make. The simple method outlined above for the construction of one way patterns will usually lead to graph state layouts which do not have a square lattice structure. Nevertheless, a cluster state on a large enough square lattice of two or more dimensions is still sufficient to implement any unitary [4]. A number of measurement patterns for quantum gates designed specifically for two-dimensional square lattice cluster states can be found in [5].

20.3 Beyond quantum circuit simulation

We have shown that the one-way quantum computer can implement deterministically a universal set of gates and thus any quantum computation. However, part of the power of one-way quantum computation derives from the fact that unitary operations can be implemented more compactly than a naive network construction would suggest [11]. In fact we shall see in the following sections that other ways of decomposing unitary operations are more natural and useful. The main tool we shall use in our investigation of these properties is the *stabilizer formalism*.

20.3.1 Stabilizer formalism

The stabilizer formalism [13, 14] is a powerful tool for understanding the properties of graph states and one-way quantum computation. Stabilizer formalism is a framework whereby states and sub-spaces over multiple qubits are described and characterized in a compact way in terms of operators under which they are invariant. In standard quantum mechanics one uses complete sets of commuting observables in a similar fashion, such as in the description of atomic states by “quantum numbers” (see e.g. [17]).

An operator K *stabilizes* a subspace $\mathcal{S}$ when, for all states $|\psi\rangle \in \mathcal{S}$,

$$K|\psi\rangle = |\psi\rangle. \quad (20.10)$$

In other words, $|\psi\rangle$ is an eigenstate of K with eigenvalue $+1$.

In the stabilizer formalism one focuses on operators which, in addition to this stabilizing property, are Hermitian members of the Pauli group, i.e. tensor products of Pauli and identity operators. The key principle of the stabilizer formalism is to identify a set of such stabilizing operators which uniquely defines a given state or sub-space - i.e. there is no state outside the sub-space (for a specified system) which the same set of operators also jointly stabilizes. The sub-spaces (and states) which can be defined uniquely using stabilizing operators from the Pauli group are called *stabilizer sub-spaces* (or stabilizer states).

Stabilizer states and sub-spaces occur widely in quantum information science and include Bell states, GHZ states, many error-correcting codes, and, of course, graph states and cluster states. Note that there are other joint eigenstates of the stabilizing operators with some -1 eigenvalues. However, only states with $+1$ eigenvalue are “stabilized”, by definition. This set of operators then embodies all the properties of the state and can allow an easier analysis, for example, of how the state transforms under measurement and unitary evolution. Since the product of two stabilizing operators is itself stabilizing, the set of operators which stabilize a sub-space has a group structure. It is called the *stabilizer group* or simply the *stabilizer* of the sub-space. The group can be compactly expressed by identifying a set of generators. For a k -qubit sub-space in an n qubit system, $n - k$ generators are required (see Exercise 2).

We do not have enough space here for a detailed introduction to all of the techniques of stabilizer formalism – excellent introductions can be found in [3, 13] – but instead we will focus on those which are useful for understanding one-way quantum computation. Most will be stated without proof but can be verified using the properties of Pauli group operators described in [3].

A simple example of a stabilizer state is the state $|+\rangle$. Its stabilizer group is generated by X alone. The stabilizer for the tensor product state $|+\rangle^{\otimes n}$ is then generated by n operators $K_a = X_a$ acting on each qubit a . From this we can derive the stabilizer generators for graph states. Consider a stabilizer state transformed by the unitary transformation V . The stabilizers of the transformed state are then given by $VK_aV^\dagger$. Since the CZ gate transforms $X \otimes \mathbf{1}$ to $X \otimes Z$ under conjugation, we find that the stabilizer generators for graph states have the form

$$K_a = X_a \prod_{b \in N(a)} Z_b \quad (20.11)$$

for every qubit a in the graph. $N(a)$ is the neighbourhood of a , i.e. the set of qubits sharing edges with a on the graph (this corresponds to nearest neighbours in a cluster state).

20.3.2 A logical Heisenberg picture

We are going to use the stabilizer formalism to understand the one-way patterns which implement unitary transformations in the one-way model. We shall see that it is convenient to describe logical action of a one-way pattern in a *logical Heisenberg picture* [14].

The Schrödinger picture is the most common approach to describing the time-evolution of quantum systems. Temporal changes in the system are reflected in changes in the state vector or density matrix, e.g. for unitary evolution $|\psi\rangle \mapsto U(t)|\psi\rangle$ or $\rho \mapsto U(t)|\psi\rangle\rho U(t)^\dagger$. The observables which characterize measurable quantities, such as Pauli observables X , Y and Z , remain invariant in time. In the Heisenberg picture, on the other hand, time-evolution is carried exclusively by physical observables which evolve $O(t) \mapsto U(t)^\dagger O U(t)$. States and density matrices remain constant in time.

A *logical Heisenberg picture*, also called a “Heisenberg representation of quantum computation” [14], is a middle-way between these two approaches, containing elements of both. We shall introduce it with an example, starting in the Schrödinger picture with a single-qubit density matrix $\rho(t)$ evolving in time. Since the n -qubit Pauli-group operators form a basis in the vector space of n -qubit Hermitian operators, we can write ρ at time $t = 0$ as

$$\rho(t=0) = a\mathbf{1} + bX + cY + dZ \quad (20.12)$$

where a, b, c and d are real parameters which define the state.

At time t , the state has been transformed through unitary $U(t)$. In the usual Schrödinger picture one would reflect this in a transformation of the matrix elements of the state, or, equivalently, of the parameters a, b, c and d to $a(t), b(t)$, etc.. However, one can also write

$$\rho(t) = U(t)\rho U(t)^\dagger = a\mathbf{1} + bU(t)XU(t)^\dagger + cU(t)YU(t)^\dagger + dU(t)ZU(t)^\dagger. \quad (20.13)$$

By introducing time-evolving observables $\overline{X}(t) = U(t)XU(t)^\dagger$ and similar expressions for $\overline{Y}(t)$ and $\overline{Z}(t)$, we can express this as

$$\rho(t) = a\mathbf{1} + b\overline{X}(t) + c\overline{Y}(t) + d\overline{Z}(t). \quad (20.14)$$

The time evolution is thus captured by the evolution of these logical observables, and the parameters a, b, c and d remain fixed. Since $\overline{X}(t), \overline{Y}(t)$, etc. define the logical basis in which ρ is expressed, we call them *logical observables*.

Since $\overline{Y}(t) = i\overline{X}(t)\overline{Z}(t)$, determining $\overline{X}(t)$ and $\overline{Z}(t)$ specifies the evolution $U(t)$ completely. More generally, an n -qubit unitary is defined in this picture by the evolution of $\overline{X}(t)_a$ and $\overline{Z}(t)_a$ for each qubit a . It is important to emphasise that the logical observables $\overline{X}(t)$, $\overline{Y}(t)$, and so forth, are no longer equal to the physical observables X , Y etc. which remain constant in time. Here time evolution is characterized by the evolution of *logical* observables. In analogy to the (standard) Heisenberg picture, where *physical* observables evolve in time, we call this a *logical Heisenberg picture*¹.

The logical Heisenberg picture can be illustrated with some simple examples. First, let us consider a Hadamard $U(t) = H$. This is represented in the logical Heisenberg picture through $\overline{X}(t) = Z$ and $\overline{Z}(t) = X$. Second, let us look at the representation of the SWAP gate in this picture. We find that $\overline{X}_1(t) = X_2$ and $\overline{X}_2(t) = X_1$ (similarly for the Z variables). The logical Heisenberg picture clearly encapsulates the action of these gates; in the case of the Hadamard, we see X and Z interchanged and for SWAP, the operators on the two qubits are switched round. In the one-way quantum computer logical time evolution is discrete and driven by single-qubit measurements, so in the following we will often suppress the time labelling t .

A logical Heisenberg picture becomes particularly useful when describing the *encoding* of quantum information. As well as density matrices, one can also represent the evolution of pure state vectors in a logical Heisenberg picture. The time evolution is carried by the *logical basis* states, the joint eigenstates of $\overline{Z}(t)_a$ with phase relations fixed by $\overline{X}(t)_a$. Consider a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ imagine we encode it via some unitary transformation U . We would write $|\psi\rangle = \alpha U|0\rangle + \beta U|1\rangle = \alpha|0'\rangle + \beta|1'\rangle$, where $|0'\rangle$ and $|1'\rangle$ are the new (encoded) logical basis states. Thus “encoding” implicitly adopts a logical Heisenberg picture. The state coefficients remain constant while logical basis vectors are transformed.

20.3.3 Dynamical variables on a stabilizer sub-space

This formalism can be combined with the stabilizer formalism to track the evolution of logical observables on a sub-space of a larger system. The stabilizer group then defines the logical sub-space, and the dynamical logical operators track the evolution of this sub-space. The logical operators act only to map states around the sub-space, therefore they must commute with the stabilizers of that sub-space.

Let us use the well-known three-qubit error correcting code as an example. In this code, the logical $|0\rangle$ is represented by $|0\rangle|0\rangle|0\rangle$ and $|1\rangle$ by $|1\rangle|1\rangle|1\rangle$. The stabilizer group for this sub-space is generated by $Z \otimes Z \otimes \mathbb{1}$ and $\mathbb{1} \otimes Z \otimes Z$. The logical observables associated with this basis are $\overline{Z} = Z \otimes \mathbb{1} \otimes \mathbb{1}$ and $\overline{X} = X \otimes X \otimes X$. One can easily verify that these operators have the desired action on the logical basis states.

However, even though the logical basis is entirely symmetric under interchange of the qubits, the logical $\overline{Z}$ is not. Due to the symmetry of the situation one would expect that $\mathbb{1} \otimes Z \otimes \mathbb{1}$ and $\mathbb{1} \otimes \mathbb{1} \otimes Z$ would be equivalent to the physical representation of $\overline{Z}$ we have chosen above. That these operators have the same action on the logical basis states is easy to confirm and it reflects an important characteristic of logical operators on a sub-space, namely that they are not unique. Given a stabilizer operator for the sub-space K_a and logical operator

¹In geometric terms, evolution in the Schrödinger picture corresponds to an active transformation of a state. A logical Heisenberg picture corresponds to a passive transformation – the state remains fixed with respect to a changing logical basis.

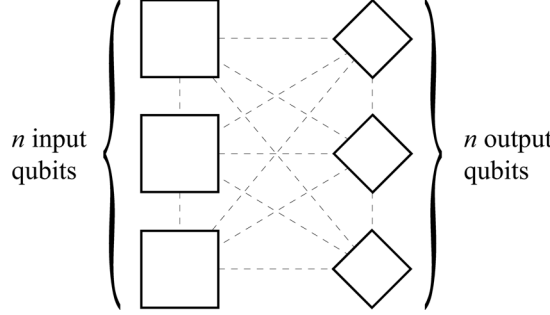


Figure 20.4. Any n -qubit Clifford group operation may be implemented (up to local Clifford corrections) by a one-way pattern with $2n$ -qubits. Dotted lines represent possible edges in the patterns.

$\bar{L}$, the product $K_a \bar{L}$ has the same action on the logical sub-space as $\bar{L}$. Thus there are a number of physical representations for a given logical observable. Formally this set is in fact a coset of the stabilizer group. In order to define this set, only one member of the set need be specified. When we write a particular physical operator corresponding to $\bar{L}$ this is just a “representative” of the whole coset.

20.3.4 One-way patterns in the stabilizer formalism

We introduced the term “one-way pattern” to describe a layout of qubits, graph state edges and measurements which implements a given unitary in the one-way model. More specifically, the patterns contain a set of qubits labelled input qubits and a set labelled output qubits, a set of auxiliary qubits and a set of edges connecting those qubits. We will now show how, using the rules for transforming stabilizer sub-spaces under measurement, that the one-way pattern will lead to the transformation of the logical operators $\bar{X}_a \mapsto \pm U \bar{X}_{a'} U^\dagger$ and $\bar{Z}_a \mapsto \pm U \bar{Z}_{a'} U^\dagger$. This is a logical Heisenberg picture representation of the desired unitary U , plus the displacement of the logical state from input qubit(s) a to output qubit(s) a' . The extra factor ± 1 reflects the presence of by-product operators (due to the randomness of the measurement outcomes) since $XZX = -Z$ and $ZXZ = -X$.

20.3.5 Pauli measurements

Before we consider one-way patterns with general one-qubit measurements, let us first consider patterns consisting solely of Pauli measurements. These measurements change the logical variables’ encoding according to the desired evolution of the logical state. As the logical evolution is unitary, each measurement must reveal no information about the logical state. By considering commutation relations, one can show that these requirements are equivalent to demanding that the measured observable anti-commute with at least one stabilizer generator.

The effect of performing a measurement of a (multi-qubit) Pauli observable Σ on a sub-space is as follows (such methods are described in more detail in [3]). If Σ does not commute

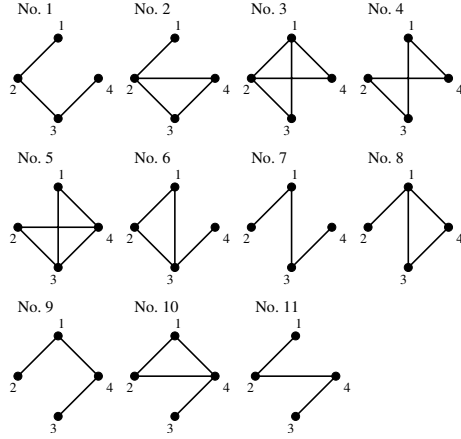


Figure 20.5. The full orbit of locally equivalent four-qubit graph states. Each graph state is obtained from the previous one by application of the “local complementation rule.” This figure is taken from M. Hein, J. Eisert and H.J. Briegel, Phys. Rev. A 69, 062311 (2004) ©APS.

with the complete stabilizer group, one can always construct a set of stabilizer generators such that only one of the generators K_a anti-commutes with Σ . The stabilizers which commute with Σ must also stabilize the transformed sub-space after the measurement, which will be an eigenspace of Σ with eigenvalue ± 1 . Thus $\pm \Sigma$ will itself belong to the new stabilizer. We can thus construct a set of generators for the stabilizer of the transformed sub-space, by simply replacing K_a , which anti-commutes with Σ , with $\pm \Sigma$.

The logical observables transform in a similar way. This time, just one member of the coset for each logical observable needs to be found which commutes with Σ . If the representative logical operator $\bar{L}$ commutes with Σ it remains a valid representative logical operator after the measurement (the full coset will be different though due to the changed stabilizer). If $\bar{L}$ does not commute with Σ , then the product $\bar{L}K_a$ does commute, so logical operators for the transformed sub-space are easy to find.

A final step involves finding a reduced description of the state which ignores the now unimportant measured qubit. This is achieved by choosing a set of stabilizer generators where all but one ($\pm \Sigma$ itself) act as the identity on the measured qubit. This is achieved by multiplying all the generators not already in this form with $\pm \Sigma$. In the same way representative logical operators can be chosen that are also restricted to the unmeasured qubits.

After all but the designated output qubits in a pattern have been measured, the one-way pattern has been completed. The reduced description of the output qubits has a stabilizer group consisting of the identity operator alone and logical operators have become $\bar{X}_a = \pm U X_{a'} U^\dagger$ and $\bar{Z}_a = \pm U Z_{a'} U^\dagger$. We interpret this in the logical Heisenberg picture. The one-way pattern has implemented the unitary transformation U plus known Pauli corrections and the logical sub-space has been physically displaced from the input qubits a to output qubits a' .

This method can be used to design and verify one-way patterns (e.g. see Exercise 3). It may seem complicated for such simple examples, but its power lies in its generality. In the next section, we show how measurement patterns for arbitrary Clifford operations may be evaluated using these techniques.

20.3.6 Pauli measurements and the Clifford group

In the previous section, all of the transformations of the logical observables keep their physical representations within the Pauli group. Unitary operators which map Pauli group operators to the Pauli group under conjugation are known as Clifford group operations. The Clifford group is the group generated by the CZ, Hadamard and $U_z(\pi/2)$ gates. Since all of these gates can be implemented by one-way patterns with Pauli measurements only (i.e. by choosing $\phi = 0$ or $\phi = \pi/2$ in Fig. 20.3 (a)) any Clifford group operation can be achieved by Pauli measurements alone.

The Clifford group plays an important role in quantum computation theory. Clifford group circuits are the basis for most quantum error correction schemes, and many interesting entangled states (including, of course, graph states) can be generated via Clifford group operations alone. However, Gottesman and Knill [14] showed that notwithstanding this, Clifford group circuits acting on stabilizer states (such as the standard input $|0\rangle^{\otimes n}$) can be simulated efficiently on a classical computer [15, 16]. This is because of the simple way the logical observables transform (in the logical Heisenberg picture) under such operations.

Let us consider the effect of the by-product Pauli operators, generated every time a measurement outcome is -1 , when Clifford operations are implemented in the one-way quantum computer. Given a Clifford operation C , by the definition of the Clifford group, $C\Sigma C^\dagger = \Sigma'$ where Σ and Σ' are Pauli group operators. Therefore $C\Sigma = \Sigma'C$ meaning that interchanging the order of Clifford operators and Pauli corrections will leave the Clifford operation unchanged. This means that there is no need to choose measurement bases adaptively. We thus see that in any one-way quantum computation all Pauli measurements can be made simultaneously in the first measurement round.

These results imply that Pauli measurements on stabilizer states will always leave behind a stabilizer state on the unmeasured qubits. Additionally, any stabilizer state can be transformed to a graph state by local Clifford operations [19, 20]. Furthermore, this graph state is in general not unique, by further local Clifford operations a whole family of locally equivalent graph states can be achieved [7, 20]. The rules for this local equivalence are simple – a graph can be transformed into another locally equivalent graph by “local complementation” [20] which is a graph-theoretical primitive [21]. In local complementation, a particular vertex of the graph is singled out and the sub-graph given by all vertices connected to it is “complemented” (i.e. all present edges are removed and any missing edges are created). The set of locally equivalent four-qubit graph states is illustrated in figure 20.5.

This theorem allows us to understand the effect of Pauli measurements on a graph state in a new way. Any Pauli measurement on a graph state simply transforms it (up to a local Clifford correction) into another graph state. A graphical description of how the graph is transformed and which local corrections must be applied can be found in [7, 18]. The rule for Z -measurements is simple, the measured qubit and all edges connected to it are removed from the graph. If the -1 eigenvalue was measured, extra Z transformations on the adjacent qubits must be applied to bring the state to graph state form. Rules for X and Y measurements are more complicated and can be found in [7].

Since the effect of Pauli measurements is to just transform the graph, given any one-way pattern containing Pauli measurements, the transformation rules can be used to find a one-way pattern which implements the same operation with fewer qubits. The local corrections

can often be incorporated in the bases of remaining measurements. If not they lead to an additional local Clifford transformation on the output qubit. Since the Pauli measurements correspond to the implementation of Clifford group operations, this leads to a stronger result than the Gottesman–Knill theorem. All Clifford operations, wherever they occur in the quantum computation are reduced to classical pre-processing of the one-way pattern. A further consequence is that any n -qubit Clifford group operation can be implemented (up to the local Clifford corrections) on a $2n$ qubit pattern, as illustrated in Fig. 20.4.

20.3.7 Non-Pauli measurements

The method above does not yet allow us to treat non-Pauli measurements, specified by measurement directions other than along the X -, Y - or Z -axis. However, one can still treat such measurements within the stabilizer formalism. The stabilizer eigenvalue equations (Eq. (20.10)) can be rearranged to generate a family of non-Pauli unitary operations which also stabilize the sub-space [5]. Consider the state $|\psi\rangle$ stabilized by operator $Z \otimes X$. We rearrange the stabilizer equation as follows

$$\begin{aligned} Z \otimes X |\psi\rangle &= |\psi\rangle \\ Z \otimes \mathbf{1} |\psi\rangle &= \mathbf{1} \otimes X |\psi\rangle \\ (Z \otimes \mathbf{1} - \mathbf{1} \otimes X) |\psi\rangle &= 0 \end{aligned} \tag{20.15}$$

thus for all ϕ ,

$$\exp \left[i \frac{\phi}{2} (Z \otimes \mathbf{1} - \mathbf{1} \otimes X) \right] |\psi\rangle = |\psi\rangle. \tag{20.16}$$

Thus we have a unitary $U_z(-\phi) \otimes U_x(\phi)$ which itself stabilizes $|\psi\rangle$. This implies that

$$U_z(\phi) \otimes \mathbf{1} |\psi\rangle = \mathbf{1} \otimes U_x(\phi) |\psi\rangle. \tag{20.17}$$

Similar unitaries and similar expressions can be generated from any stabilizer operator. We will show in the next section, how this technique allows a simple analysis of the one-way pattern for general unitaries diagonal in the computational basis, and in fact, the technique allows one to understand any one-way pattern solely within the stabilizer formalism and was used to design and verify many of the gate patterns presented in [5]. This indicates that the effect of non-Pauli measurements in a one-way quantum computation can always be understood as the implementation of a *generalized rotation* $\exp[-i(\phi/2)\Sigma]$ where Σ can be any n -qubit Pauli group operator. We shall discuss the consequences of this further in section 20.3.9.

20.3.8 Diagonal unitaries

Earlier in the chapter we saw that a CZ gate can be implemented such that the input qubit is also the output qubit. Coinciding input and output qubits in a one-way pattern reduces the size of the pattern so it is natural to ask which unitaries can be implemented this way and one can show (see Exercise 4) that it is only those unitaries diagonal in the computational-basis.

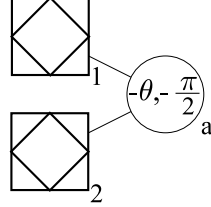


Figure 20.6. The one-way pattern which implements the unitary “double-z rotation” $e^{-i\frac{\theta}{2}Z \otimes Z}$. Note that input and output qubits coincide.

In fact, there is a simple one-way pattern for any diagonal unitary transformation. Any such n -qubit operator can be written (up to a global phase) in the following form

$$D_n = \prod_{\vec{m}} \exp \left[i \frac{\phi \vec{m}}{2} (Z_1)^{m_1} (Z_2)^{m_2} \cdots (Z_n)^{m_n} \right] \quad (20.18)$$

where $(Z_a)^{m_a}$ is equal to the identity if $m_a = 0$ and Z acting on qubit a when $m_a = 1$, and the sum is over all binary vectors $\vec{m}$ of length n .

Each element of this product is a generalized rotation acting on a subset of the qubits and has a very simple implementation in the one-way quantum computer. To illustrate this, consider the two-qubit transformation $e^{-i\frac{\phi}{2}Z \otimes Z}$. This can be implemented on a one-way pattern with three qubits as illustrated in Fig. 20.6. In this pattern the qubits labelled 1 and 2 are the joint input-output qubits, and qubit a is an ancilla. The entanglement graph has two edges connecting a to 1 and 2. A measurement in basis $(-\phi, -\pi/2)$, i.e. of observable $U_x(-\phi)ZU_x(\phi)$, implements $e^{-i\frac{\phi}{2}Z_1Z_2}$ on the input state, with by-product operator Z_1Z_2 .

To see this, we recall that the stabilizer for the sub-space corresponding to such a graph is $X_aZ_1Z_2$. The corresponding eigenvalue equation can be transformed, as described in the previous section, to generate the stabilizing unitary $[U_x(\theta)]_a e^{i\frac{\theta}{2}Z_1Z_2}$. Measuring qubit a in basis $(-\phi, -\pi/2)$ is equivalent to performing $[U_x(\phi)]_a$ and then measuring Z_a , hence the one-way pattern implements the logical unitary $e^{-i\frac{\phi}{2}Z_1Z_2}$.

We can generalize this pattern to quite general n -qubit diagonal unitaries. (Verify this in Exercise 5). For example, the pattern for an arbitrary diagonal three-qubit unitary is given in Fig. 20.7. This is a highly parallelized and efficient implementation of the unitary².

Since the by-product operators for these patterns are diagonal themselves they commute with the desired logical diagonal unitaries. Thus there is no dependency in the measurement bases on the outcome of measurements within this pattern and all measurements can be achieved in a single measurement round. Thus, not only can a quantum circuit consisting of Clifford gates alone be implemented in a single-time step – this is true for any diagonal unitary followed by a Clifford network.

²This is reminiscent of the results reported in [22] regarding the parallelization of diagonal unitaries, where, however a different definition of parallelization is used. We treat the CZ operations generating the graphs state as occurring in a single time-step. Physically this is entirely reasonable as operations generated by commuting Hamiltonians can often be implemented simultaneously as we shall see in our discussion of optical lattices in Section 20.4.

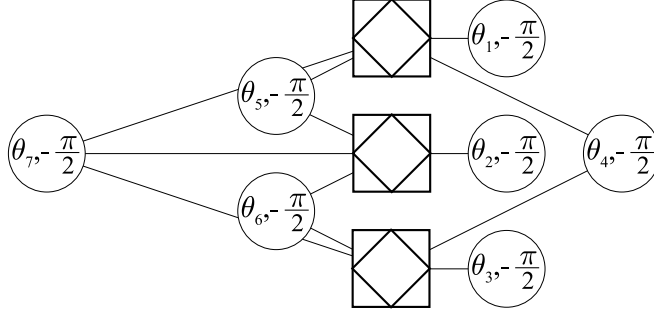


Figure 20.7. Arbitrary diagonal unitaries may be implemented in a single round of measurements by measurement patterns with coinciding input and output qubits. This example shows an arbitrary diagonal three-qubit unitary $\exp[\frac{i}{2}(\theta_1 Z \otimes \mathbf{1} \otimes \mathbf{1} + \theta_2 \mathbf{1} \otimes Z \otimes \mathbf{1} + \theta_3 \mathbf{1} \otimes \mathbf{1} \otimes Z + \theta_4 Z \otimes \mathbf{1} \otimes Z + \theta_5 Z \otimes Z \otimes \mathbf{1} + \theta_6 \mathbf{1} \otimes Z \otimes Z + \theta_7 Z \otimes Z \otimes Z)]$. For example, by setting the angles to $\theta_1 = \theta_2 = \theta_3 = \theta_7 = -\pi/4$ and $\theta_4 = \theta_5 = \theta_6 = \pi/4$, we obtain a control-control Z gate or “Toffoli-Z gate.” See [5] for a cluster-state implementation of this gate.

20.3.9 Gate patterns beyond the standard network model –CD-decomposition

We have seen that one can construct one-way patterns to implement a unitary operation described by a quantum circuit by simply connecting together patterns for the constituent gates. Furthermore, such patterns can be made more compact by evaluating the graph state transformations corresponding to any Pauli measurements present. This can change the structure of the pattern such that the original circuit is hard to recognize (see for example, the quantum Fourier transform patterns in [7]).

We have also seen that non-Pauli measurements in a measurement pattern lead to generalized rotations on the logical state of the form $\exp[-(i/2)\phi\Sigma]$ where Σ is some Pauli group operator. The implementation of any non-Clifford unitary on the one-way quantum computer is thus best understood as a sequence of operators of this form. Two such operators $\exp[-(i/2)\phi\Sigma]$ and $\exp[-(i/2)\phi'\Sigma']$ may, if $[\Sigma, \Sigma'] = 0$ be combined to give $\exp[-(i/2)[\phi\Sigma + \phi'\Sigma']$. In general, any operators of the form $\exp[(i/2)[\sum_a \alpha_a \Sigma_a]$, where $[\Sigma_a, \Sigma_{a'}] = 0$, can be diagonalized by a Clifford group element C to $CDC^\dagger$, where D is a diagonal unitary. Composing two operations this form, e.g. $C_1 D_1 C_1^\dagger$ and $C_2 D_2 C_2^\dagger$ will give $C_1 D_1 C_1^\dagger C_2 D_2 C_2^\dagger = C_1 D_1 C_3 D_2 C_2^\dagger$ where $C_3 = C_1^\dagger C_2$, and we call the casting of a unitary in this form a *CD-decomposition*.

There are several observations to be made about such decompositions. We have already seen that both diagonal unitaries and Clifford group operations have compact implementations in one-way quantum computations. This means that CD-decompositions are very useful in the design of compact one-way patterns. One simply combines the one-way patterns for diagonal unitaries presented above with patterns for Clifford operations, which we have seen require at most $2n$ qubits for an n -qubit operation and which can be constructed either by employing Pauli transformation rules on a pattern for a network of CZ, Hadamard and $U_z(\pi/2)$ gates,

or by inspection of the logical Heisenberg form of the operation. In [5] this decomposition, together with stabilizer techniques described above, was used to design cluster-state implementations for several gates and simple algorithms including controlled Z-rotations and the quantum Fourier transform (QFT).

A further advantage in working with a CD-decomposition is that it immediately provides an upper bound in the number of time steps needed for the implementation of the one-way pattern. This is simply the number of “CD units” in the decomposition. We saw in Section 20.3.8 that a single CD unit can be implemented in a single time step. Each CD unit in turn will create by-product operators, which may need to be accounted for in the choice of measurement bases for following diagonal unitaries. A decomposition which minimized the number of CD units would give a (possibly tight) upper bound on the minimal number of time-steps and would be one measure of how hard the unitary is to implement in the one-way model. For example, Euler’s rotation theorem tells us that the optimal CD-decomposition for an arbitrary rotation consists of three CD units and correspondingly requires three measurement rounds for implementation on the one-way quantum computer.

Note that there is considerable freedom in choosing a CD form. For example, one can construct the decomposition such that all the diagonal gates are solely local, single-qubit operations and only the Clifford gates are non-local. This gives a degree of flexibility in the design one-way patterns.

Quantum circuits described in terms of Clifford group gates plus rotations can readily cast in CD form by decomposing the rotations into Z -axis rotations and Hadamards. One can then reduce the size of the corresponding pattern by applying the Pauli measurement transformation rules³. Quantum circuits for the simulation of general Hamiltonians are usually expressed using the Trotter formula (see [3]) which leads to unitaries which are a sequence of generalized rotations which can be cast in CD form in a straightforward manner. Thus the one-way quantum computer is very well suited to Hamiltonian simulation (see e.g. [23]), which will be an important application of quantum computers.

20.4 Implementations

20.4.1 Optical lattices

Beyond its theoretical value, there are a number of physical implementations where one-way quantum computation gives distinct practical advantages. One of these is in systems where graph states or cluster states can be generated efficiently, such as “optical lattices.” In an optical lattice, cold neutral atoms are trapped in a lattice structure, given by the periodic potential due to a set of superposed laser fields. The potential “seen” by each atom depends on its internal state. This means that neighbouring atoms in different states can be brought close together by changing the relative positions of the minima of the periodic potentials, leaving an interaction phase on the atoms’ state [24]. If this is timed such that this interaction

³It is important to note, however, that the Pauli measurement rules alone do not usually provide a CD-decomposition which is optimal in the sense of consisting of the smallest number of CD units. An optimal CD-decomposition will allow the construction of a one-way pattern for the unitaries with fewer measurement rounds, and often a more compact entanglement graph, than application of the Pauli transformation rules alone.

phase is -1 the process implements, essentially, a CZ gate between the two atoms. However, every atom in the lattice will be affected when these potentials move and thus CZ gates can be implemented between neighbouring qubits across the lattice simultaneously. Thus, by preparing all atoms in a superposition of these internal states beforehand, a very large cluster state can be generated very efficiently. In recent years there has been much progress in the generation and manipulation of ultra-cold atoms in optical lattices in the laboratory [25], and a number of schemes for the generation of arbitrary graph states in these systems have been proposed [26]. Possibly the most difficult obstacle to overcome for the implementation of one-way quantum computation in optical lattices is the difficulty in addressing individual atoms in the lattice.

20.4.2 Linear optics and cavity QED

Photons make excellent carriers on quantum information and are relatively decoherence free. A key difficulty in implementing universal quantum computation using photons is that two-qubit gates such as CZ cannot be implemented by the simple linear optical elements of the optics laboratory (e.g. beam-splitters and phase shifters) alone. By employing photon number measurements, non-deterministic entangling gates are possible. Most times, however, the gate fails, and this failure leads to the measurement of the qubits' state which disrupts the computation. Naively, one would expect that scaling this up into a circuit would lead to an exponential decrease in success probability, but, by using a combination of techniques including gate teleportation [27] and error correction, scalable quantum computation is indeed possible [28]. A key disadvantage of this particular approach, however, is that each gate requires a large number of ancilla photons in a difficult-to-prepare entangled state.

A much more efficient strategy is to use the non-deterministic gates to build an entangled resource state for measurement-based quantum computation [29,30]. Cluster states can be generated efficiently [31] using so-called “fusion operations”, which can be performed (non-deterministically) with simple linear optics. Fusion operations [31,32] are implementations of operators such as $|0\rangle\langle 00| + |1\rangle\langle 11|$, which when applied to two qubits in different graph states, replace both qubits by a single one which inherits all the graph state edges of each, thus “fusing” the two graph states together. Recently, three and four-qubit graph states have been created in the laboratory using methods based on down-conversion and post-selection [33] and fusion measurements [34]. Single-qubit measurements on these states demonstrated many of the key elements of one-way quantum computation [33]. More details of linear optical quantum computation can be found in other chapters of this book and in a recent review [35].

Quantum computation with photons is not the only scenario where gates are inherently non-deterministic. Similar techniques can be used to implement non-deterministic gates between atoms or ions trapped in separate cavities. Cavity QED implementations of the one-way quantum computer is a fast-developing area and recently there have been a number of promising experimental proposals [36].

20.5 Recent developments

In addition to these developments toward the implementation of one-way quantum computation there have been a number of interesting papers exploring its theoretical structure. The relationship between the one-way quantum computer and other models of measurement-based quantum computation [27, 37] has been explored in [32, 38–40] and an algebraic representation of one-way graph measurement patterns [12] has been developed. The simulability of one-way quantum computations with one-way patterns of various depths and geometries has been investigated [8, 41]. Looking beyond qubit implementations, an analogue of graph states in continuous-variable harmonic oscillator systems [42] has been investigated and generalizations of one-way quantum computation to d -level systems [43] have been explored. A version of one-way quantum computation based on three-qubit interactions has been proposed [44].

Any practical quantum computation proposal must be able to function in the presence of a degree of experimental noise and decoherence. Standard approaches to fault-tolerant quantum computation have been firmly rooted in the network model and it was not clear whether they would translate to the one-way model. It was shown in [45] and later [46] that physical errors in the one-way quantum computer would be manifested as logical errors quite different from those that one would expect in a standard gate network implementation. Nevertheless for a number of physically reasonable independent noise models there is an error threshold below which fault-tolerant quantum computation is possible [45, 46]. A simple proof of this for both Markovian and non-Markovian local errors is presented in [47]. The implementation of these techniques in linear optical quantum computation has been simulated [48], leading to estimated error thresholds of around 0.0001 for depolarisation errors and 0.003 for loss.

Recently, a different approach to fault-tolerance in the one-way model has been taken. Most quantum error correcting code-words are stabilizer states, and as we have seen, every stabilizer state is locally equivalent to a graph state. It is therefore natural to look for error correction schemes which make use of the natural error correcting properties of the graph state. It has been demonstrated that one-way quantum computation with a high degree of robustness against qubit loss errors (the most significant error source in linear optical quantum computation) can be achieved by using a graph states with a tree-like structure [49]. This scheme tolerates losing up to half of the qubits in the graph state, and can be applied to deal with photon loss errors in linear optical proposals [50].

Most recently, it was shown [51] that a three-dimensional body-centred cubic lattice cluster state has the properties of a topological surface code. By combining ideas from topological quantum computation with the observation that quantum Reed-Muller codes [52] allow fault-tolerant non-Pauli measurements of logical qubits to be implemented by local measurements, a fully fault-tolerant scheme was presented [51] with estimated error thresholds between 0.001 and 0.01.

20.6 Outlook

In this chapter, we have given an introduction to the key ideas of one-way quantum computation and some of the most useful mathematical techniques for describing and understanding it. The one-way approach has provided a new paradigm for quantum computation which is

casting many questions of quantum computation theory in a new light. It is leading to experimental implementations that are radically different from early ideas about how a quantum computer would operate. In addition, it is likely that there will be further physical systems in which the one-way model offers the most achievable path to quantum computation. Not least, the success of the one-way approach illustrates the power of novel representations of quantum information processing and should encourage us to look for other new and distinct models of quantum computation.

Acknowledgements

Dan Browne is supported by Merton College, Oxford and EPSRC's QIPIRC programme. Hans Briegel is supported by the Austrian Science Fund (FWF), the German Science Foundation (DFG), and by the European Union through projects QLAQUI and SCALA.

We would like to thank Robert Raussendorf for many insightful discussions over a number of years, which have helped to shape our perspective of one-way quantum computation. Dan would like to thank Sean Barrett, Simon Benjamin, Michael Bremner, Jens Eisert, Joe Fitzsimons, Elham Kashefi, Pieter Kok, Michael Nielsen, Terry Rudolph and Michael Varnava for some illuminating discussions about one-way quantum computation. Hans would like to thank the Kavli Institute for Theoretical Physics (KITP) for their hospitality and support while the final part of this work was completed. We would like to thank Earl Campbell for helpful comments on the manuscript.

Exercises

1. There are only two topologically distinct three-qubit graph states. In one, the qubits form a linear three qubit cluster state, in the other, the qubits are connected in a triangle. Write down the stabilizer generators for these two states and hence also the full stabilizer group for each. Now show that one can transform between these two states by a local Clifford operator.
2. Prove that, to generate the stabilizer group for a k -qubit stabilizer sub-space in an n qubit system, $(n - k)$ generators are required.
3. Consider the one-way pattern illustrated in Fig. 20.3(a) with angle ϕ set to zero. Show that after the entangling CZ operation, but before the measurement, the logical operators $\overline{X}$ and $\overline{Z}$ have physical representations $X \otimes Z$ and $Z \otimes \mathbb{1}$ respectively. Find the stabilizer and hence the full coset of each logical observable. When observable X is measured on the first qubit, how are the stabilizer and logical observables transformed? Hence verify that this pattern implements a Hadamard gate.
4. Show that one-way patterns where all input and output qubits coincide can only implement diagonal unitaries. What can one say about patterns where only some of the input and output qubits coincide?

5. Using the decomposition of an arbitrary n -qubit diagonal unitary D_n in Eq. (20.18) and by generalizing the methods in Section 20.3.8 describe a one-way pattern which implements D_n requiring a total of $n + (2^n - 1)$ qubits.
6. Verify the effect of applying the “fusion” operator $|0\rangle\langle 0|\langle 0| + |1\rangle\langle 1|\langle 1|$ to two qubits, each of which belong to separate graph states. What happens when a projection onto the even-parity sub-space $|0\rangle\langle 0|\langle 0| + |1\rangle\langle 1|\langle 1|$ is applied instead?
7. Consider a qubit that is prepared in an unknown state, and a one-dimensional cluster state. What is the effect of applying a fusion operator on the unknown qubit and the qubit at one end of the cluster state. How can the fusion operator be used to “input” externally provided states into a one-way quantum computation?

References

- [1] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1990).
- [2] A. Barenco *et al.*, Phys. Rev. A **52** 3457 (1995).
- [3] M.A. Nielsen, I. Chuang, M.A. Nielsen, and I.L. Chuang. *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).
- [4] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
- [5] R. Raussendorf, D.E. Browne and H.J. Briegel, Phys. Rev. A **68**, 022312 (2003).
- [6] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
- [7] M. Hein, J. Eisert and H.J. Briegel, Phys. Rev. A **69**, 062311 (2004).
- [8] M.A. Nielsen, e-print quant-ph/0504097, to appear in Rev. Math. Phys.
- [9] R. Jozsa, e-print quant-ph/0508124.
- [10] M. Hein *et al.*, e-print quant-ph/0602096.
- [11] R. Raussendorf and H.J. Briegel, Quant. Inf. Comp. **6**, 433 (2002); R. Raussendorf, D.E. Browne and H.J. Briegel, Journal of Modern Optics **49**, 1299 (2002).
- [12] V. Danos, E. Kashefi and P. Panangaden, eprint: quant-ph/0412135; V. Danos, E. Kashefi, and P. Panangaden Phys. Rev. A **72**, 064301 (2005).
- [13] D. Gottesman, *Stabilizer codes and quantum error correction*, quant-ph/9705052, PhD Thesis, California Institute of Technology (1997).
- [14] D. Gottesman, *The Heisenberg Representation of Quantum Computers*, Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics 32 (Cambridge, MA, International Press, 1999).
- [15] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
- [16] S. Anders and H.J. Briegel, Phys. Rev. A **73**, 022334 (2006).
- [17] C. Cohen-Tannoudji *et al.*, *Quantum Mechanics Volume 1*, (Wiley, New York, 1978).
- [18] D. Schlingemann, Quant. Inf. Comp. **2**, 307 (2002); D. Schlingemann, Quant. Inf. Comp. **4**, 287 (2004).
- [19] D. Schlingemann, e-print quant-ph/0111080; M. Grassl, A. Klappenecker, and M. Roetteler, IEEE International Symposium on Information Theory, 45 (Lausanne, 2001).
- [20] M. Van den Nest, J. Dehaene and B. De Moor, Phys. Rev. A **69**, 022316 (2004).

- [21] A. Bouchet, *Combinatorica* **11** 314 (1991).
- [22] C. Moore and M. Nilsson, *SIAM J. Comput.* **31**, 799 (2002).
- [23] W. Dür, M. Bremner and H.J. Briegel, in preparation.
- [24] D. Jaksch *et al.*, *Phys. Rev. Lett.* **82**, 1975 (1999).
- [25] M. Greiner *et al.*, *Nature (London)* **415**, 39 (2002); M. Greiner *et al.*, *Nature (London)* **419**, 51 (2002); O. Mandel *et al.*, *Phys. Rev. Lett.* **91**, 010407 (2003); O. Mandel *et al.*, *Nature (London)* **425**, 937 (2003).
- [26] S.R. Clark, C. Moura Alves and D. Jaksch, *New J. Phys.* **7**, 124 (2005); A. Kay, J.K. Pachos, and C.S. Adams, *Phys. Rev. A* **73**, 022310 (2006).
- [27] D. Gottesman and I.L. Chuang, *Nature (London)* **402**, 390 (1999).
- [28] E. Knill, R. Laflamme and G. Milburn, *Nature (London)* **409**, 46 (2001).
- [29] N. Yoran and B. Reznik, *Phys. Rev. Lett.* **91**, 037903 (2003).
- [30] M.A. Nielsen, *Phys. Rev. Lett.* **93** 040503 (2004).
- [31] D.E. Browne and T. Rudolph, *Phys. Rev. Lett.* **95** 10501 (2005).
- [32] F. Verstraete and J.I. Cirac, *Phys. Rev. A* **70**, 060302(R) (2004).
- [33] P. Walther *et al.*, *Nature (London)* **434**, 169 (2005).
- [34] A.-N. Zhang *et al.*, *Phys. Rev. A* **73**, 022330 (2006).
- [35] P. Kok *et al.*, e-print quant-ph/0512071, to appear in *Rev. Mod. Phys.*
- [36] S.D. Barrett and P. Kok, *Phys. Rev. A* **71**, 060310(R) (2005); Y.L. Lim, A. Beige and L.C. Kwek, *Phys. Rev. A* **73**, 012304 (2006); J. Cho, H.-W. Lee, *Phys. Rev. Lett.* **95**, 160501 (2005).
- [37] M.A. Nielsen, *Phys. Lett. A* **308**, 96 (2003); D. Leung, e-print quant-ph/0111122.
- [38] P. Jorrand and S. Perdrix, e-print: quant-ph/0404125.
- [39] P. Aliferis and D. W. Leung, *Phys. Rev. A* **70**, 062314 (2004).
- [40] A.M. Childs, D.W. Leung and M.A. Nielsen, *Phys. Rev. A* **71**, 032318 (2005).
- [41] I. Markov and Y. Shi, e-print quant-ph/0511069; N. Yoran and A.J. Short, *Phys. Rev. Lett.* **96**, 170503 (2006).
- [42] J. Zhang, e-print quant-ph/0501112; J. Zhang and S. Braunstein, *Phys. Rev. A* **73**, 032318 (2006).
- [43] D.L. Zhou *et al.*, *Phys. Rev. A* **68**, 062303 (2003); W. Hall, e-print quant-ph/0512130; S. Clark, *J. Phys. A: Math. Gen.* **39**, 2701 (2006).
- [44] M.S. Tame *et al.*, *Phys. Rev. A* **73**, 022309 (2006).
- [45] R. Raussendorf, PhD Thesis, Ludwig-Maximilians University, Munich (2003), online at <http://edoc.ub.unimuenchen.de/archive/00001367/>.
- [46] M. Nielsen and C. Dawson, *Phys. Rev. A* **71**, 042323 (2005).
- [47] P. Aliferis and D.W. Leung, *Phys. Rev. A* **73**, 032308 (2006).
- [48] C.M. Dawson, H.L. Haselgrove and M.A. Nielsen, *Phys. Rev. Lett.* **96**, 020501 (2006).
- [49] M. Varnava, D.E. Browne, T. Rudolph, *Phys. Rev. Lett.* **97**, 120501 (2006).
- [50] M. Varnava, D.E. Browne, T. Rudolph, in preparation (2006).
- [51] R. Raussendorf, J. Harrington and K. Goyal, e-print quant-ph/0510135.
- [52] S. Bravyi and A. Kitaev, *Phys. Rev. A* **71**, 022316 (2005).

21 Holonomic Quantum Computation

Angelo C.M. Carollo and Vlatko Vedral

A considerable understanding of the formal description of quantum mechanics has been achieved after Berry's discovery [2] of a geometric feature related to the motion of a quantum system. He showed that the wave function of a quantum object retains a memory of its evolution in its complex phase argument, which, apart from the usual dynamical contribution, only depends on the "geometry" of the path traversed by the system. Known as the *geometric phase* factor, this contribution originates from the very heart of the structure of quantum mechanics.

A renewed interest in geometric phenomena in quantum physics has been recently motivated by the proposal of using geometric phases for quantum computation. Geometric (or "Berry") phases depend only on the geometry of the path executed, and are therefore resilient to certain types of errors. The idea is to exploit this inherent robustness provided by the topological properties of some quantum systems as a means of constructing built-in fault tolerant quantum logic gates. Various strategies have been proposed to reach this goal, some of them making use of purely geometric evolutions, i.e., non-Abelian holonomies [19, 20, 29]. Others make use of hybrid strategies that combine together geometrical and dynamical evolutions [7, 11], and others yet use more topological structures to design quantum memories [5, 13]. Several proposals for geometric quantum computations have been suggested and realized in different contexts, in NMR experiments [11], ion traps [6, 10, 14, 26, 27], cavity QED experiments [23], atomic ensembles [15, 28], Josephson junction devices [8], anyonic systems [13], and quantum dots [25].

21.1 Geometric Phase and Holonomy

Suppose that a system undergoing a cyclic evolution is described by classical mechanics; it is impossible to tell from its initial and final states whether it has undergone any physical motion. The situation in quantum mechanics is quite different. The state vector of a quantum system retains the "history" of its evolution in the form of a geometric phase factor.

This deep and fundamental concept was originally discovered by Pancharatnam [21] in the context of a classical beam of polarized light and "rediscovered" in a quantum mechanical context by Berry [2]. Pancharatnam introduced the concept of *parallelism* between two states, as a criterion to compare the relative phase between two beams of light with different polarization. He recognized that a natural convention to measure the phase difference between two interfering beams is to choose a reference where the intensity has its maximum. For example, by superimposing two beams of polarizations ψ_1 and ψ_2 the intensity is pro-

portional to $I \propto 1 + |\langle \psi_1 | \psi_2 \rangle| \cos(\chi + \arg \langle \psi_1 | \psi_2 \rangle)$. The interference fringes are shifted by $\varphi = \arg \langle \psi_1 | \psi_2 \rangle$, which, following Pancharatnam's prescription, represents the phase difference between ψ_1 and ψ_2 . This idea, translated into quantum mechanics, leads to the definition of relative phase between any (nonorthogonal) states lying in a (finite or infinite) Hilbert space. When $\arg \langle \psi_1 | \psi_2 \rangle = 0$, ψ_1 and ψ_2 are called *in phase*. Pancharatnam's most important contribution was to point out that this condition is *not transitive*: If ψ_1 is in phase with ψ_2 and ψ_2 with ψ_3 , the phase between ψ_1 and ψ_3 is, in general, not zero. As in quantum mechanics states are defined up to a phase, ψ_2 can always be redefined parallel to ψ_1 . However, when a third state ψ_3 is considered, it is, in general, impossible to redefine it in phase with both ψ_1 and ψ_2 . This is due to an *irreducible* phase contribution $\chi = \arg \langle \psi_1 | \psi_2 \rangle \langle \psi_2 | \psi_3 \rangle \langle \psi_3 | \psi_1 \rangle$, called *Pancharatnam phase*, which represents the most elementary example of *geometric phase* [1, 17, 22].

If, instead of a discrete collection, we consider a continuous chain of states $|\phi(s)\rangle$ (with $s \in \{s_0 \dots s_1\}$), we can repeat a similar argument and redefine the local phases $|\phi(s)\rangle \rightarrow |\psi(s)\rangle = e^{i\alpha(s)}|\phi(s)\rangle$ to impose the phase condition between infinitely neighboring states, namely

$$\arg \langle \psi(s) | \psi(s+ds) \rangle \simeq \langle \psi(s) | \frac{d}{ds} |\psi(s)\rangle ds = 0, \quad (21.1)$$

which is known as the *parallel transport condition*. As emphasized earlier, this condition is not transitive. Therefore, although neighboring states are in phase, states far apart along the curve accumulate a finite phase difference between them. In particular, if the chain is a closed loop, i.e., $|\phi(s_0)\rangle = |\phi(s_1)\rangle$, a state “parallel-transported” around the loop experiences a phase shift

$$|\psi(s_1)\rangle = e^{i\chi_\gamma} |\psi(s_0)\rangle, \quad \chi_\gamma = \alpha(s_1) - \alpha(s_0) = i \int_{s_0}^{s_1} \langle \phi | \frac{d}{ds} | \phi \rangle ds = i \oint_\gamma \langle \phi | d\phi \rangle, \quad (21.2)$$

which is the celebrated *geometric phase*. As for the Pancharatnam phase, χ_γ is an *irreducible* phase contribution which solely depends on the closed path γ traced out by $|\psi(s)\rangle$ in the Hilbert space. It is easy to verify that neither a *local redefinition of phase*, nor a change in the *rate of traversal* affects the value χ_γ .

21.1.1 Adiabatic implementation of holonomies

A natural question to ask is how the idea of parallel transport applies to physical scenarios. It turns out that this concept plays a key role in a variety of physical contexts (see [3, 18, 24]), and, in quantum mechanics it emerges as a natural feature of adiabatically evolving systems.

Suppose that a Hamiltonian, $H(\lambda_t)$ is controlled by a set of time-dependent parameters λ_t . If the requirements for the adiabatic approximation (see [12, 16]) are satisfied, a state, initially prepared in an eigenstate $|\psi(t_0)\rangle = |\Psi_n(\lambda_{t_0})\rangle$, remains eigenstate of the instantaneous Hamiltonian, during the evolution

$$|\psi(t)\rangle = e^{i\delta(t)} |\Psi_n(\lambda_t)\rangle \quad \text{where} \quad H(\lambda_t) |\Psi_n(\lambda_t)\rangle = \epsilon_n(\lambda_t) |\Psi_n(\lambda_t)\rangle, \quad (21.3)$$

($\hbar = 1$) where $\delta(t) = -\int_{t_0}^t \epsilon_n(\lambda_t) dt$ is the usual *dynamical phase*. Under this approximation, the state $|\psi(t)\rangle$ can satisfy the Schrödinger equation only if the constraint

$\langle \Psi_n(\lambda_t) | \frac{d}{dt} | \Psi_n(\lambda_t) \rangle = 0$ is fulfilled. Hence, the state $|\Psi_n(\lambda_t)\rangle$ is parallel transported around the Hilbert space as the parameters λ 's are varied. If the latter are eventually brought back to their initial values λ_0 , and the eigenspace of $|\Psi_n\rangle$ is *nondegenerate*, the final state will be proportional to the initial one, $|\Psi(t_f)\rangle = e^{i\chi_\gamma} |\Psi(t_i)\rangle$, with an accumulated geometric phase χ_γ (which in this context is called the *Berry phase*), only dependent on the path, γ , traced in the parameter space

$$\chi_\gamma = \oint_\gamma A_i d\lambda_i, \quad A_i = i \langle \Psi_n | \partial_{\lambda_i} \Psi_n \rangle, \quad (21.4)$$

where the path integral here is explicitly expressed in terms of a vector (one-form), known as *Berry connection*. The inherently geometric nature is even more evident when the path integral in Eq. (21.4) is formulated as a surface integral, via the Stokes theorem

$$\chi_\gamma = \oint_\gamma \langle \phi | d\phi \rangle = \iint_\Sigma \mathcal{F} d\sigma, \quad (21.5)$$

where Σ is the surface enclosed within the loop traced by λ in the parameters' manifold, and $\mathcal{F}_{ij} = \partial_i A_j - \partial_j A_i$ is called the *Berry curvature*. The Berry curvature in many interesting cases (such as for *qubits*) is a slowly varying function, or even a constant. As a result of this, the geometric phase behaves as an *area* and depends almost exclusively on the *surface* enclosed by the loop. This is one of the crucial characteristic that makes the geometric phase quite appealing for the implementations of *fault-tolerant* quantum computation. A feature, like an area, which is much less dependent on the details of the time evolution, is likely to be less affected by variations of environmental conditions, and hence, *more robust*.

The prototypical example in which this *area-like* behavior is manifest, is the case of a single qubit adiabatically evolving under a generic Hamiltonian $H(t) = \vec{n}_t \cdot \vec{\sigma}$, where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli matrices, and $\vec{n}_t$ is a time-dependent vector. It is possible to show that the curvature associated with a qubit state gives rise to a very simple form of the geometric phase, namely $\chi_\gamma = \pm \frac{\Omega}{2}$ ($\pm$ depending on whether the qubit is initially aligned or against the direction of $\vec{n}$), where Ω is the solid angle spanned by the direction of the vector $\vec{n}$. The curvature in this case is constant ($\pm 1/2$) and Ω is the surface enclosed in parameter manifold (the Bloch sphere) (see Fig. 21.2.1a).

Before turning the discussion towards the implementation of quantum computation, it is important to introduce the *non-Abelian* generalization of the geometric phase, or *holonomy*. In obtaining the geometric phase for an adiabatic evolving system, the assumption that the eigenspace to which the prepared state belongs is nondegenerate was crucial. Such a condition insures that, when a loop in the parameter space is traversed, final and initial states are proportional, i.e., the net effect of the evolution is merely a phase. However, assuming a degenerate eigenspace, opens up a wider variety of possible evolutions, with a slightly more complex structure, known formally as *holonomy*.

The word holonomy refers to the set of all the closed curves, or *loops* on a manifold, starting and ending in the same point x_0 . It is easy to verify that this set has the structure of *group*.¹

¹The composition of two loops is obtained by joining the end point of one loop with the starting point of the other. The identity element is the trivial loop with only one point (x_0). The inverse of curve is the same traversed in the opposite direction. For a rigorous definition see [9, 18].

The geometric phases themselves form a *representation* of a holonomy group: any loop in the parameter space of an Hamiltonian is associated with a geometric phase factor. And clearly they form an *Abelian representation* as phases commute: $e^{i\chi_{\gamma_1}} e^{i\chi_{\gamma_2}} = e^{i\chi_{\gamma_2}} e^{i\chi_{\gamma_1}}$. This therefore implies that their non-Abelian generalization are not represented by ordinary numbers, but by matrices. This naturally emerges in adiabatic evolving systems, when eigenspaces are degenerate.

Let us write a parameter dependent Hamiltonian in the form: $H(\lambda_t) = \sum_k \epsilon_k(\lambda_t) \Pi_k(\lambda_t)$, where $\Pi_k(\lambda_t)$ are the projector operators of the instantaneous eigenspaces. As time varies, the parameters change and with them eigenvalues and eigenspaces. The latter are smoothly concatenated via a unitary transformation $O(\lambda_t)$ (the eigenspaces never change dimension, as this is forbidden by the adiabatic requirements), $\Pi_k(\lambda_t) = O(\lambda_t) \Pi_k^0 O^\dagger(\lambda_t)$, where Π_k^0 is an eigenspace at the initial time t_0 ($O(\lambda_{t_0}) = \mathbb{1}$). The unitary transformation $O^\dagger$ produces the change of picture to the frame moving rigidly with the instantaneous eigenspaces. In this frame, the evolution is governed by the Hamiltonian $\tilde{H}(\lambda_t) = \sum_k \epsilon_k \Pi_k^0 - i \frac{dO(\lambda_t)}{dt} O^\dagger(\lambda_t)$. Imposing the adiabatic approximation is equivalent to neglecting Hamiltonian terms coupling different eigenspaces (see [16]). The evolution inside each eigenspace is, then, generated by the following equation:

$$i \frac{dU_k(t)}{dt} = [\epsilon(\lambda_t) - A_k(\lambda_t)] U_k(t), \quad A_k(\lambda_t) = i \Pi_k^0 \frac{dO(\lambda_t)}{dt} O^\dagger(\lambda_t) \Pi_k^0. \quad (21.6)$$

This equation can be formally solved, and, for a closed loop of the parameters, yields the total evolution (notice that by definition $O(\lambda_{t_f}) = \mathbb{1}$):

$$U_k(t_f) = T_k(t_f) V_k^\gamma, \quad \text{with} \quad V_k^\gamma = \mathcal{P} \exp \oint_\gamma A_k(\lambda) d\lambda, \quad \text{and} \quad T_k = e^{-i \int \epsilon_k t}, \quad (21.7)$$

where T is an overall dynamical phase factor, and V_k^γ is the celebrated (*non-Abelian*) *holonomy*. In this formula $\mathcal{P}$ is the *path-ordering* operator, needed because of the noncommutativity of the operators $A(\lambda)$ for different values of the parameters. This non-Abelian phases is in general very difficult to evaluate, because of the path-ordering operation.

21.2 Application to Quantum Computation

We would like to mention potential advantages of using geometrical evolution to implement quantum gates. Firstly, there is no dynamical phase in the evolution. This is because we are using degenerate states to encode information so that the dynamical phase is the same for both states (and it factors out as it were). Also, all the errors stemming from the dynamical phase are automatically eliminated. Secondly, the states being degenerate do not suffer from any bit flip errors between the states (like the spontaneous emission). So, the evolution is protected against these errors as well. Thirdly, the size of the error depends on the area covered and is therefore immune to random noise (at least in the first order) in the driving of the evolution. This is because the area is preserved under such a noise as formally proven by DeChiara and Palma [4]. Also, by tuning the parameters of the driving field it may be possible to make

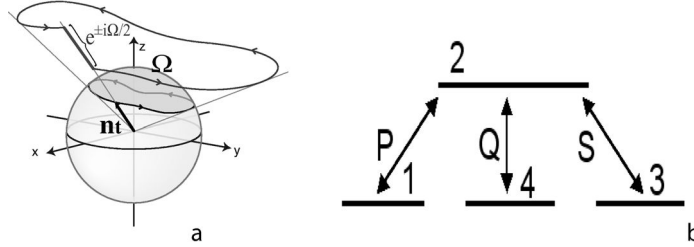


Figure 21.1. (a) The geometric phase for a single qubit is proportional to the solid angle Ω . (b) The four level system that can be used for non-Abelian quantum computation to encode one qubit of information in two degenerate levels. The method is detailed in the text.

the phase independent of the area to a large extent and make it dependent only on a singular topological feature - such as in the Aharonov–Bohm effect where the flux can be confined to a small area - and this would then make the phase resistant under very general errors.

So, in order to see how this works in practice we take an atomic system as our model implementing the non-Abelian evolution. We'll see that quantum computation can easily be implemented in this way. The question, of course, is the one about the ultimate benefits of this implementation. Although there are some obvious benefits, as listed above, there are also some serious shortcomings, and so the jury is still out on this issue.

21.2.1 Example

Let us look at the following 4 level system analyzed by Unanyan, Shore, and Bergmann [28]. They considered a four level system with three degenerate levels 1, 3, 4 and one level 2 with a different energy as in Fig. 21.2.1b. This system stores one bit of information in the levels 1 and 2 (hence there is double the redundancy in the encoding of information). We have the following Hamiltonian:

$$H(t) = \begin{pmatrix} 0 & P(t) & 0 & 0 \\ P(t) & 0 & S(t) & Q(t) \\ 0 & S(t) & 0 & 0 \\ 0 & Q(t) & 0 & 0 \end{pmatrix}$$

where P, Q, S are arbitrary functions of time. It is not difficult to find eigenvalues and eigenvectors of this matrix (exercise!). There are two degenerate eigenvectors (with the corresponding zero eigenvalue for all times) which will be implementing our qubit and they are

$$\Phi_1(t) = (\cos \theta_t, 0, -\sin \theta_t, 0) \quad \text{and} \quad \Phi_2(t) = (\sin \phi_t \sin \theta_t, 0, \sin \phi_t \cos \theta_t, -\cos \phi_t)$$

where $\tan \theta_t = P(t)/Q(t)$ and $\tan \phi_t = Q(t)/\sqrt{P(t)^2 + Q(t)^2}$. In the adiabatic limit, we can restrict ourselves to these states only. Although, in general, the Dyson equation is difficult to solve, in this special example we can write down a closed form expression [28]. The unitary

matrix representing the geometrical evolution of the degenerate states is

$$B(\eta_t) = \begin{pmatrix} \cos \eta_t & \sin \eta_t \\ -\sin \eta_t & \cos \eta_t \end{pmatrix}, \quad (21.8)$$

where $\eta_t = \int_0^t \sin \phi_\tau \frac{d\theta}{d\tau} d\tau$. This therefore allows us to calculate the non-Abelian phase for any closed path in the parametric space. After some time we suppose that the parameters return to their original value. So, at the end of the interaction we have the matrix $B(\eta_f)$ where $\eta_f = \oint_c \frac{Q}{(P^2+S^2)\sqrt{Q^2+P^2+S^2}}(SdP - PdS)$, which can be evaluated using Stokes' theorem (the phase will in general depend on the path, as explained before). So, we can have a non-Abelian phase implementing a Hadamard gate. With two systems of this type (mutually interacting) we can implement a controlled-Not gate and therefore (at least in principle) have a universal quantum computer (see [29]).

References

- [1] V. Bargmann. Note on Wigners theorem on symmetry operations. *J. Math. Phys.*, 5:862, 1964.
- [2] M. V. Berry. Quantal phase-factor accompanying adiabatic changes. *Proc. Roy. Soc. A*, 329:45, 1984.
- [3] Arno Bohm, Ali Mostafazadeh, Hiroyasu Koizumi, Qian Niu, and Joseph Zwanziger. *The Geometric Phase in Quantum Systems*. Springer, Berlin, Heidelberg, New York, 2003.
- [4] Gabriele De Chiara and G. Massimo Palma. Berry phase for a spin 1/2 particle in a classical fluctuating field. *Phys. Rev. Lett.*, 91:art. no.–090404, 2003.
- [5] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *J. Math. Phys.*, 43:4452–4505, 2002.
- [6] L. M. Duan, J. I. Cirac, and P. Zoller. Geometric manipulation of trapped ions for quantum computation. *Science*, 292:1695–1697, 2001.
- [7] A. Ekert, M. Ericsson, P. Hayden, H. Inamori, J.A. Jones, D.K.L. Oi, and V. Vedral. Geometric quantum computation. *J. Mod. Opt.*, 47:2501, 2000.
- [8] Giuseppe Falci, Rosario Fazio, G. Massimo Palma, Jens Siewert, and Vlatko Vedral. Detection of geometric phases in superconducting nanocircuits. *Nature*, 407:355, 2000.
- [9] T. Frankel. *The Geometry of Physics*. Cambridge University Press, Cambridge, 2000.
- [10] J. J. García-Ripoll, P. Zoller, and J. I. Cirac. Speed optimized two-qubit gates with laser coherent control techniques for ion trap quantum computing. *Phys. Rev. Lett.*, 91:art. no.–157901, 2003.
- [11] J.A. Jones, V. Vedral, A. Ekert, and G. Castagnoli. Geometric quantum computation using nuclear magnetic resonance. *Nature*, 403:869–871, 1999.
- [12] Tosio Kato. On the adiabatic theorem of quantum mechanics. *J. Phys. Soc. Jpn.*, 5:435–439, 1950.
- [13] A. Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Ann.*, 303:2–30, 2003.

- [14] D. Leibfried, B. De Marco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D. J. Wineland. Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate. *Nature*, 422:412 – 415, 2003.
- [15] Y. Li, P. Zhang, P. Zanardi, and C. P. Sun. Non-Abelian geometric quantum memory with atomic ensemble. 2004. Preprint, quant-ph/0403143.
- [16] A. Messiah. *Quantum Mechanics*, volume 2. North-Holland, Amsterdam, 1962.
- [17] N. Mukunda and R. Simon. Quantum kinematic approach to the geometric phase. *Ann. Phys. (NY)*, 228:205, 1993.
- [18] M. Nakahara. *Geometry, Topology and Physics*. Graduate Student Series in Physics. Adam Hilger, Bristol, New York, 1990.
- [19] J. Pachos and S. Chountasis. Optical holonomic quantum computer. *Phys. Rev. A*, 62:052318, 2000.
- [20] Jiannis Pachos, Paolo Zanardi, and Mario Rasetti. Non-Abelian Berry connections for quantum computation. *Phys. Rev. A*, 61:010305, 2000.
- [21] S. Pancharatnam. Generalized theory of interference, and its applications. *Proc. Ind. Acad. Sci. A*, 44:247, 1956.
- [22] E. M. Arvind Rabei, N. Mukunda, and R. Simon. Bargmann invariants and geometric phases: A generalized connection. *Phys. Rev. A*, 60:3397, 1999.
- [23] A. Recati, T. Calarco, P. Zanardi, J. I. Cirac, and P. Zoller. Holonomic quantum computation with neutral atoms. *Phys. Rev. A*, 66:032309, 2002.
- [24] A. Shapere and F. Wilczek, editors. *Geometric Phases in Physics*. World Scientific, Singapore, 1989.
- [25] Paolo Solinas, Paolo Zanardi, Nino Zanghì, and Fausto Rossi. Nonadiabatic geometrical quantum gates in semiconductor quantum dots. *Phys. Rev. B*, 67:art. no.–052309, 2003.
- [26] Anders Sørensen and Klaus Mølmer. Entanglement and quantum computation with ions in thermal motion. *Phys. Rev. A*, 62:art. no.–022311, 2000.
- [27] Peter Staunum, Michael Drewsen, and Klaus Mølmer. Geometric quantum gate for trapped ions based on optical dipole forces induced by Gaussian laser beams. 2004. Preprint: quant-ph/0406186.
- [28] R. G. Unanyan, B. W. Shore, and K. Bergmann. Laser-driven population transfer in four-level atoms: Consequences of non-Abelian geometrical adiabatic phase factors. *Phys. Rev. A*, 59:2910–2919, 1999.
- [29] P. Zanardi and M. Rasetti. Holonomic quantum computation. *Phys. Lett. A*, 264:94, 1999.

Part VI

Quantum Computing: Implementations

22 Quantum Computing with Cold Ions and Atoms: Theory

Dieter Jaksch, Juan José García-Ripoll, J. Ignacio Cirac, and Peter Zoller

22.1 Introduction

Systems of trapped cold ions and neutral atoms are invaluable experimental tools for the study and demonstration of elementary quantum information processing tasks. The distinguishing features are that we have (i) a detailed microscopic understanding of the Hamiltonian of the systems realized in the laboratory, and (ii) complete control of the system parameters via external fields. Atoms have many internal states that can be manipulated using laser light and can be employed as qubits with very long coherence times. In addition electric and magnetic fields or optical traps can be used to control the motion of atoms. This allows the realization of quantum registers, for e.g., by chains of trapped ions or regular patterns of neutral atoms of different dimensionality in optical lattices. In this chapter we show how such atomic qubit register can be realized and describe various methods to implement quantum gate operations on these registers.

22.2 Trapped Ions

Trapped ions constitute one of the most promising candidates to implement quantum computation [1–4]. In this section we will review the theory of quantum information processing with ions. For an overview of the remarkable experimental progress in the last years we refer the reader to the next section in this chapter.

In ion trap quantum computing qubits are stored in long-lived internal states of individual atoms. Single-qubit operations are done by coupling the qubit states with laser light for an appropriate period of time. In general, this requires to address single ions with the laser beams. Two-qubit gates, on the other hand, are performed by coupling the ions via the collective vibrational modes [1]. For some protocols this requires first cooling a particular mode to the zero phonon limit, as well as resolving individual sidebands. However, recent proposals for “hot gates” relax these restrictions [5–10]. Furthermore, the two-qubit operations can be performed either dynamically, i.e., based on the time evolution generated by a specific Hamiltonian, or *geometrically* as in holonomic quantum computing [11]. Finally, measurements are accomplished using the method of quantum jumps [12].

Even if the viability of the two-qubit gate has been demonstrated [13–15], the most important feature of trapped ions is the scalability to a large number of qubits. Indeed, while quantum computers will have interesting uses for a number of ions of around 100—for instance, to

simulate other quantum systems—current linear traps can only store a small number of ions. However, larger systems can be decomposed into a shielded quantum memory, where ions are stored, and a number of interacting regions, where single ions or pairs of ions are brought to in order to make single- and two-qubit gates. These are the ideas developed in [16, 17], and which have already been implemented in the group of Wineland at NIST. An important part of a scalable quantum computer though is the design of a robust and fast quantum gate. Such a gate should ideally be (i) insensitive to temperature, so that one does not need to cool the ions after moving them; (ii) require no addressability, in order to bring the ions very close and increase the gating speed, and finally (iii) be fast, to minimize the effect of decoherence during the realization of the gate. Although there have been some proposals for scalable two-qubit gates in [14, 16], the most promising candidate remains that of [9, 10], where an arbitrarily fast quantum gate has been designed with the help of laser coherent quantum control. Alternatively, there are other proposals which combine ion-trap quantum computing with solid-state superconducting devices to provide scalable schemes that do not require moving the ions [18].

In the following paragraphs we will start by discussing the trapping and manipulation of ions with laser light. We will then explain several proposals for implementing a two-qubit gate with ions, from the very first one in [1] to the most recent developments based on quantum control [9, 10].

22.2.1 Motional degrees of freedom

We consider N ions confined in some trapping potential and interacting with laser light. If the lasers are directed along one of the principal axes of the harmonic potential, we can neglect the motion along the transverse directions and treat the system as purely one-dimensional. The Hamiltonian for the motional degrees of freedom of this model is

$$H_0 = \sum_{i=1}^N \left[\frac{p_i^2}{2m} + V_{e,i}(x_i) \right] + \sum_{i=1}^N \sum_{j=1}^{i-1} \frac{e^2}{4\pi\epsilon_0} \frac{1}{|x_i - x_j|}. \quad (22.1)$$

In this equation, $V_{e,k}$ is the trapping potential that confines the k th ion, and it may be the same for all of them if stored in a common linear trap [1] or may change from ion to ion as in the case of microtraps [16]. If we expand the previous Hamiltonian around the equilibrium configuration, given by $(\partial H / \partial x_i)(x_1^{(0)}, \dots, x_N^{(0)}) = 0$, and find out the normal modes for the resulting system of coupled oscillators, we obtain

$$H_{0T} = \sum_{k=1}^N \left[\frac{P_k^2}{2m} + \frac{1}{2} m \nu_k^2 Q_k^2 \right] + H|_{x_k=x_k^{(0)}} = \sum_{k=1}^N \hbar \nu_k a_k^\dagger a_k + E_0. \quad (22.2)$$

The new collective coordinates, $Q_k = M_{ik}[x_i - x_i^{(0)}]$ and $P_k = M_{ik}p_i$, are defined in terms of an orthogonal transformation, $M^t = M^{-1}$, and they are usually replaced by the corresponding Fock operators $Q_k = \sqrt{1/2m\nu_k}(a_k + a_k^\dagger)$ and $P_k = i\sqrt{m\nu_k/2}(a_k^\dagger - a_k)$. For instance, for two ions in a linear Paul trap we have two modes, a center of mass mode with frequency equal to the trap frequency, $\nu_{cm} = \nu$, and a stretch mode with incommensurate frequency $\nu_r = \sqrt{3}\nu$. Finally, E_0 denotes the energy of the ions in the equilibrium configuration.

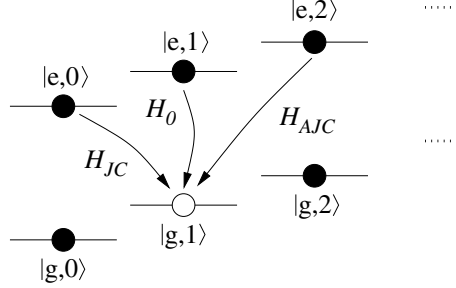


Figure 22.1. Coupling of the atom+trap levels according to the Hamiltonians (22.5), (22.6), and (22.7), respectively, in the lowest order Lamb–Dicke expansion.

22.2.2 Internal degrees of freedom and atom–laser interaction

We will model the internal electronic structure of the ion using a two level system, $|g\rangle$ and $|e\rangle$. These two long-lived levels are connected by a dipole-forbidden transition, and since they are used to store the quantum information, they are also denoted as $|0\rangle$ and $|1\rangle$. We will study what happens when a laser driving the transition $|g\rangle \rightarrow |e\rangle$ is on. If the interaction time between the atom and the laser beam is much longer than the lifetime of the state $|e\rangle$, we can neglect spontaneous emission. Then, in a frame rotating with the laser frequency the Hamiltonian modeling the process will be ($\hbar = 1$)

$$H = H_{0T} + \delta|g\rangle\langle g| + \frac{1}{2}\Omega \sin[kx_k + \phi] (|e\rangle\langle g| + |g\rangle\langle e|), \quad \text{or} \quad (22.3a)$$

$$H = H_{0T} + \delta|g\rangle\langle g| + \frac{1}{2}\Omega \{|e\rangle\langle g| \exp[\pm ikx_k] + \text{h.c.}\}, \quad (22.3b)$$

for standing-wave and traveling-wave configurations, respectively. Here, $\delta = \omega_L - \omega_{rg}$ is the laser detuning from the internal transition, Ω is the Rabi frequency, and k is the wavevector of the photons. The sign $\pm$ denotes that the laser plane wave propagates in the positive or negative x direction. Finally, ϕ depends on the position of the trap in the laser standing wave.

22.2.3 Lamb–Dicke limit and sideband transitions

In some parts of this chapter we will confine our discussion to the Lamb–Dicke limit, i.e., to the limit where the ion motion is restricted to a region much smaller than the wavelength of the light exciting a given transition [19]: $k|x_k - x_k^{(0)}| \ll 1$. This allows us to expand the Hamiltonian (22.3) up to the first order in terms of the Lamb–Dicke parameters $\eta_j = k\alpha_j$, where $\alpha_j = 1/(2m\nu_j)^{1/2}$ is the size of the ground state of j th vibrational mode. For a single trapped ion we have the first order in η

$$H = \nu a^\dagger a + \delta|g\rangle\langle g| + \frac{1}{2}\Omega_1 \{|e\rangle\langle g|[c_0 + c_\pm(a + a^\dagger) + \mathcal{O}(\eta^2)] + \text{h.c.}\}, \quad (22.4)$$

where $c_0 = 1$, $c_\pm = \pm i\eta$ and $c_0 = \sin(\phi)$, $c_\pm = \eta \cos(\phi)$ are for a traveling and standing-wave configuration, respectively.

This model can be further simplified if the laser field is sufficiently weak so that only pairs of bare atom+trap levels are coupled resonantly. Let us introduce the spin-1/2 notation $\sigma_z = |e\rangle\langle e| - |g\rangle\langle g|$, $\sigma_+ = |e\rangle\langle g|$. We denote by $|g, n\rangle$ and $|e, n\rangle$ the eigenstates of the bare Hamiltonian $H_{\text{bare}} = \nu a^\dagger a - \frac{1}{2}\delta\sigma_z$, where the internal two-level system is in the ground or excited state and n is the occupation number of the harmonic oscillator. Whenever the laser

is tuned to one of the “motional sidebands,” that is for $\delta = 0, \nu, 2\nu, \dots$, the pairs of $|g, n\rangle$ and $|e, n+k\rangle$ ($k = 0, 1, 2, \dots$) become degenerate. For example, right on atomic resonance, $\delta \simeq 0$, transitions changing the harmonic oscillator quantum number n are off-resonance and can be neglected. In this case the Hamiltonian (22.3) can be approximated by

$$H_0 = \nu a^\dagger a - \frac{1}{2}\delta_1 \sigma_z + \frac{1}{2}\Omega(c_0 \sigma_+ + \text{h.c.}). \quad (22.5)$$

On the other hand, for laser frequencies close to the lower motional sideband resonance $\delta \simeq -\nu$, only transitions decreasing the quantum number n by one are important, and (22.3) can be approximated by a Hamiltonian of the Jaynes–Cummings type:

$$H_{\text{JC}} = \nu a^\dagger a - \frac{1}{2}\delta \sigma_z + \frac{1}{2}\Omega(c_\pm \sigma_+ a + \text{h.c.}). \quad (22.6)$$

Similarly, for $\delta \sim +\nu$, only transitions increasing the quantum number n by one contribute, so that (22.3) can be approximated by the *anti*-Jaynes–Cummings Hamiltonian

$$H_{\text{AJC}} = \nu a^\dagger a - \frac{1}{2}\delta_1 \sigma_z + \frac{1}{2}\omega_1(c_\pm \sigma_+ a^\dagger + \text{h.c.}). \quad (22.7)$$

For all these approximations to be valid we require that the effective Rabi frequencies to the nonresonant states be much smaller than the trap frequency $(c_{0,\pm}\Omega/\nu)^2 \ll 1$, i.e., we must spectroscopically resolve the motional sidebands. Note, in particular, that for an ion at the node of a standing light wave, corrections to H_{JC} are of the order $(\eta\Omega/\nu)^2 \ll 1$, i.e., the conditions of validity are greatly relaxed.

22.2.4 Single-qubit operations and state measurement

The eigenstates of the Hamiltonians H_0 , H_{JC} and H_{AJC} are the dressed states familiar from cavity QED, which are obtained by diagonalizing the 2×2 matrices of nearly degenerate states, $|g, n\rangle$ and $|e, n+k\rangle$ with $k = 0, -1, +1$, respectively. Using each of these possible configurations, one can perform arbitrary rotations on these subspaces

$$\begin{aligned} |g, n\rangle_j &\longrightarrow \cos(\theta)|g, n\rangle_j - ie^{i\phi} \sin(\theta)|e, n+k\rangle_j, \\ |e, n+k\rangle_j &\longrightarrow \cos(\theta)|e, n+k\rangle_j - ie^{-i\phi} \sin(\theta)|g, n\rangle_j. \end{aligned} \quad (22.8)$$

In particular, when $\delta = k = 0$ this can be used to make any single qubit unitary transformation. However, one may also swap information from the internal degrees of freedom to the motional ones, as in $(\alpha|g\rangle + \beta|e\rangle)|0\rangle \rightarrow |g\rangle(\alpha|0\rangle + \beta|1\rangle)$ (Fig. 22.2a) or introduce conditional phases. These type of operations are the basic ingredients for many quantum gates and in particular for the gate [1] explained below.

Implementation of quantum information protocols also require measurement of the internal state of the atom. For ions this can be done with essentially 100% efficiency using the method of quantum jumps [12, 20]. The theoretical understanding of quantum jumps is based on the continuous measurement theory, and we refer to [12] for a detailed mathematical description of the underlying theory. For our purpose it suffices to summarize the results as follows. Consider a *single* ion prepared initially in a superposition state on the metastable transition, $\alpha|g\rangle + \beta|e\rangle$. Switching on a laser tuned to a strongly dissipative transition $|g\rangle \rightarrow |e_1\rangle$ involving some short-lived atomic state $|e_1\rangle$, will give with probability $|\alpha|^2$ a burst of photon emissions $|e_1\rangle \rightarrow |g\rangle$ on the time scale $1/\Gamma$ (Γ is the spontaneous emission rate), or with probability $|\beta|^2$ the appearance on an emission window on the strong line. Measuring an emission window, or no window thus corresponds to a projective measurement of $|e\rangle$ or $|g\rangle$.

22.2.5 The gate Cirac–Zoller ’95

The original two-qubit gate from Ref. [1] can be understood as the composition of two fundamental operations between the internal state of the ions and a single vibrational mode or “bus” mode. For this purpose the mediating vibrational mode (typically the center of mass) has to be cooled to the ground state [21, 22]. The first operation is labeled $U_m^{1,0}$ and it transfers a qubit from the m th ion to the bus. As described in Eq. (22.8), the activation of the bus mode is done with a π -pulse performs the swap $|e, n-1\rangle \leftrightarrow |g, n\rangle$, leaving the state $|g, 0\rangle$ untouched (Fig. 22.2a). The second operation, denoted $U_n^{2,0}$, uses the second ion which participates in the gate. This time the operation is done via a third auxiliary atomic state $|e_1\rangle$, performing a 2π rotation on the two-level system $|g, 1\rangle \leftrightarrow |e_1, 0\rangle$ (Fig. 22.2b). The result is a phase gate that changes the sign of the quantum state only when the n th ion is in the internal state g and the bus mode has one phonon. The composition of both unitaries produces a phase gate between the internal state of the ions, while leaving the bus state untouched

$$\begin{array}{ccccccc}
 & \hat{U}_m^{1,0} & & \hat{U}_n^{2,1} & & \hat{U}_m^{1,0} & \\
 |g_m, g_n, 0\rangle & \longrightarrow & |g_m, g_n, 0\rangle & \longrightarrow & |g_m, g_n, 0\rangle & \longrightarrow & |g_m, g_n, 0\rangle, \\
 |g_m, e_n, 0\rangle & \longrightarrow & |g_m, e_n, 0\rangle & \longrightarrow & |g_m, e_n, 0\rangle & \longrightarrow & |g_m, e_n, 0\rangle, \\
 |e_m, e_n, 0\rangle & \longrightarrow & -i|g_m, g_n, 1\rangle & \longrightarrow & i|g_m, g_n, 1\rangle & \longrightarrow & |e_m, g_n, 0\rangle, \\
 |e_m, r_n, 0\rangle & \longrightarrow & -i|g_m, e_n, 1\rangle & \longrightarrow & -i|g_m, e_n, 1\rangle & \longrightarrow & -|e_m, e_n, 0\rangle.
 \end{array} \quad (22.9)$$

This phase gate is more concisely written as $|\epsilon_1\rangle|\epsilon_2\rangle \rightarrow (-1)^{\epsilon_1\epsilon_2}|\epsilon_1\rangle|\epsilon_2\rangle$ ($\epsilon_{1,2} = 0, 1$) and it is equivalent to a controlled-NOT up to single-qubit rotations. Together with the single-qubit operations and measurements, these are all the ingredients required to implement small quantum computations [15].

The previous setup has several limitations. First, the bus mode has to be cooled to the zero phonon limit, a process that takes time and makes the gate sensitive to heating. Second, it requires being able to address individual ions during realization of the two-qubit gate. This limits the tightness of the traps that can be used and thus the speed. Finally, the fact that we cannot excite more than one phonon, the need to resolve a sideband (i.e., to excite only one mode and leave other untouched), and the Mössbauer effect,¹ impose severe limits in the intensity of the coupling between internal and motional degrees of freedom and make the gate slow.

The gate Cirac–Zoller ’00 While in the ion trap ’95 scheme a two-qubit gate was realized using the collective phonon mode as an auxiliary quantum degree of freedom, we now describe briefly a version on an ion-trap computer in which entanglement is achieved by designing an *internal-state dependent two-body interaction* between the ions [16, 23]. This proposal has the advantage of being conceptually simpler (e.g., there is no zero temperature requirement), and obviously scalable. The model assumes that the N ions are stored in an *array of microtraps*: independent harmonic potential wells, separated by some distance d which is large enough so that the ions can be individually addressed (Fig. 22.3a). Similar to the ion trap ’95 proposal, information is stored using long-lived internal atomic states and single qubit operations are performed by addressing individually the ions with a laser.

The two-qubit gate is then performed between neighboring ions adiabatically. One must apply a standing wave of off-resonance laser light on both ions. The dipole force exerted by

¹The coupling between the ions and the bus mode has a prefactor $(mN)^{-1/2}$, where N is the number of ions.

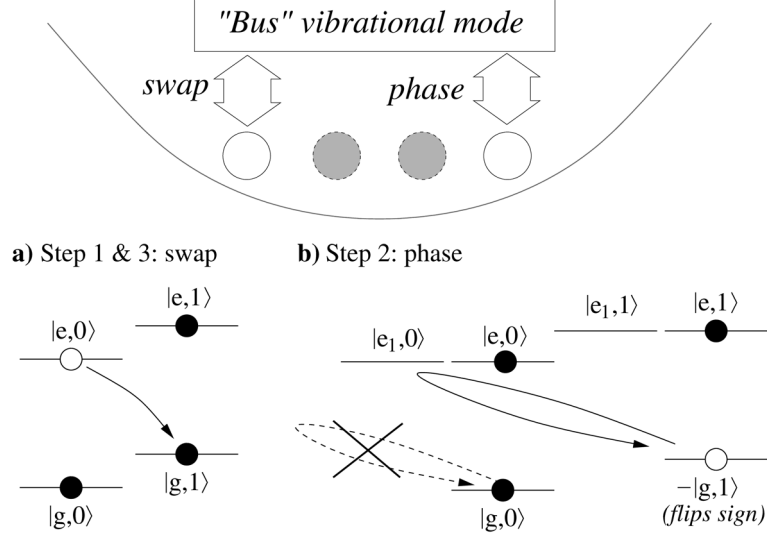


Figure 22.2. Ion trap quantum computer '95. (a) First step according to (22.9): the qubit of the first atom is swapped to the photonic data bus with a π -pulse on the lower motional sideband, (b) Second step: the state $|g, 1\rangle$ acquires a minus sign due to a 2π -rotation via the auxiliary atomic level $|e_1\rangle$ on the lower motional sideband. By combining both operations, the quantum information can be transmitted from the internal state of the ions to a vibrational mode (the "bus"). This allows selected pairs of ions to see each other and to produce a two-qubit gate.

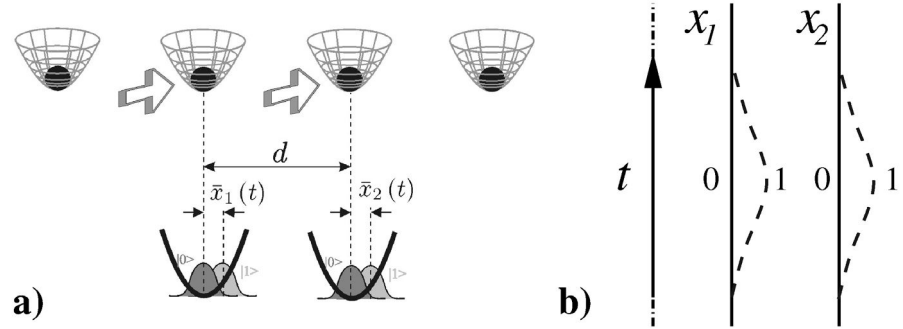


Figure 22.3. (a) Ions stored in an array of microtraps. By addressing two adjacent ions with an external field the ion wavepacket is displaced conditional to its internal state. (b) Trajectories of the qubits as a function of time. Depending on the internal state different phases are accumulated.

the light can be designed so that it only pushes ions which are on one of the qubit states, say $|1\rangle$. Switching on and off the state-dependent force is equivalent to displacing the center of the

microtraps (Fig. 22.3a), so that, depending on the internal state, the ions will approach each other or become more separated (Fig. 22.3b). If the whole process is done adiabatically, the motional state of the ions will be restored. However, according to the adiabatic theorem, the quantum state will have acquired a different phase, that depends on the Coulomb interaction experienced by the ions during the pushing. This way, by tuning the duration of the gate, we can produce a phase gate $|\epsilon_1\rangle|\epsilon_2\rangle \rightarrow e^{i\epsilon_1\epsilon_2\phi}|\epsilon_1\rangle|\epsilon_2\rangle$.

In order to analyze this in a more quantitative way, we consider two ions 1 and 2 of mass m confined by two harmonic traps of frequency ν in one dimension (Fig. 22.3a). A standing wave of off-resonance light induces an AC-Stark shift and thus a dipole force on one of the internal states, $|1\rangle$. The expression of this potential is similar to Eq. (22.3a). By placing the ions in the node of the standing wave, the force becomes approximately linear and the effective Hamiltonian can be written as $H_F = \sum_{i=1,2} -F_i(t)x_i|1\rangle\langle 1| + \mathcal{O}(x_i^3)$. The total potential experienced by the ions is

$$V = \sum_{i=1,2} \frac{1}{2}m\nu^2 (x_i - \bar{x}_i(t)|1\rangle_i\langle 1|)^2 + \frac{e^2}{4\pi\epsilon_0} \frac{1}{|d + x_2 - x_1|}, \quad (22.10)$$

where $\bar{x}_i(t) \sim F_i/m\nu^2$ is the state-dependent displacement induced by the force. We will impose that the ions do not come too close to each other, $|x_{1,2}| \ll d$, so that the Coulomb energy remains small compared to the trapping potentials, $\epsilon|x_1x_2|/a_0^2 \ll 1$. Furthermore, we will assume that the motional state of the pushed ions changes adiabatically with the potential. Expanding the Coulomb term in powers of $\hat{x}_{1,2}/d$ produces a term $-m\omega^2\epsilon x_1x_2$ in the potential (22.10). It is this term which is responsible for entangling atoms, giving rise to a conditional phase shift, which can be simply interpreted as arising from the energy shifts due to the Coulomb interactions of atoms accumulated on different trajectories according to their internal states (Fig. 22.3b),

$$\phi = -\frac{e^2}{4\pi\epsilon_0} \int_0^T dt \left[\frac{1}{d + \bar{x}_2 - \bar{x}_1} - \frac{1}{d + \bar{x}_2} - \frac{1}{d - \bar{x}_1} + \frac{1}{d} \right], \quad (22.11)$$

where the four terms are due to atoms in $|1\rangle_1|1\rangle_2$, $|1\rangle_1|0\rangle_2$, $|0\rangle_1|1\rangle_2$ and $|0\rangle_1|0\rangle_2$, respectively.

The phase acquired by the ions depends only on mean displacement of the atomic wavepacket and thus it is insensitive to the temperature (the width of the wavepacket) which will appear only in the problem in higher orders in $x_{1,2}/d$ of our expansion of the potential (22.10), or in the cases of nonadiabaticity. This feature means that this gate can be used in the type of setups considered for scalable quantum computing, because it is not required to cool the ions completely after bringing them to the interaction region. However, the fact that the gate operates in the adiabatic regime, means that it will be much slower than the period of the trap. A detailed theory of this proposal including an analysis of imperfections can be found in [23].

22.2.6 Optimal gates based on quantum control

With the number of different proposals for performing two-qubit quantum gates with ions [1, 5–8, 11, 16, 24], it remained open the question of what are the ultimate limits of quantum

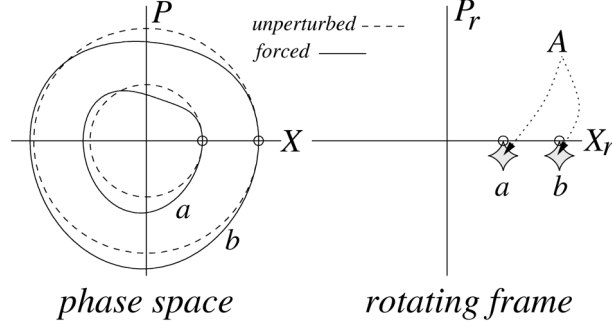


Figure 22.4. (a) Orbits in phase space of a single ion in a harmonic trap, either unforced (dashed) or subject to a time-dependent force (solid). (b) Similar picture but on a rotating frame of reference.

computing in these systems. For instance, a quick inspection of the literature reveals that most gates require a time much larger than the period of the trap, Ref. [5] being an exception. This question was answered in Ref. [9], where the main stopper of current proposals was identified to be the need of addressing a single vibrational mode. Following the ideas of Poyatos *et al* [5], this work suggests using all vibrational modes, combined with state-dependent forces to engineer a phase gate between the ions.

The background idea is very simple, and begins with a single forced ion in a harmonic trap. The model being considered is

$$H = \frac{1}{2m}p^2 + \frac{1}{2}m\nu^2 x^2 - F(t)\sigma_z x = \hbar\nu a^\dagger a - \frac{a_0}{\sqrt{2}}F(t)\sigma_z(a + a^\dagger), \quad (22.12)$$

and $F(t)\sigma_z$ represents the state-dependent force acting on the ion. This problem can be integrated exactly, and the result is that the force $F(t)$ distorts the circular orbits on phase space, (x, p) , adding some area to them (Fig. 22.4a). If the force is properly designed, the motional state of the ion will be restored (Fig. 22.4b) and the final quantum state will be

$$|\psi(t)\rangle = e^{iA\sigma_z^2} e^{i\nu a^\dagger at} |\psi(0)\rangle. \quad (22.13)$$

This unitary evolution is made of two terms: one which would even be present in the free, unforced case, plus an additional dynamical phase, e^{iA} , that depends on the area covered in the rotating frame of reference (Fig. 22.4b).

First, if we had not one ion but two, both of them coupled to a common vibrational mode, the phase would depend on the product $A\sigma_z^1\sigma_z^2$, and by tuning the area A one could produce a phase gate, $|\epsilon_1, \epsilon_2\rangle \rightarrow (-1)^{\epsilon_1\epsilon_2} |\epsilon_1, \epsilon_2\rangle$. This idea was already used experimentally in [14] to generate a two-qubit gate in an ion trap. Second and most important, the area and the phase obtained by the ions do not depend on the motional state, which is also “restored” at the end of the process, making the gate extremely robust. However, in real experiments we do not have a single vibrational mode, and implementing the previous proposal requires once more addressing a single sideband [14], what makes the gate as slow as the pushing gate.

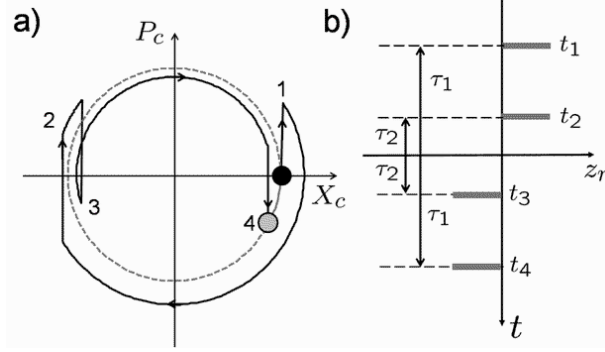


Figure 22.5. (a) Trajectory in phase space of the center-of-mass state of the ion (X_c, P_c) (where $(X_c + iP_c)/\sqrt{2} = \langle a \rangle$) during the two-qubit gate (solid line), connecting the initial state (black filled circle) to the final state (grey filled circle) at the gate time T . The time evolution consists of a sequence of kicks (vertical displacements), which are interspersed with free harmonic oscillator evolution (motion along the arcs). A pulse sequence satisfying the commensurability condition (22.14) guarantees that the final phase space point is restored to the one corresponding to a free harmonic evolution (dashed circle). The particular pulse sequence plotted corresponds to a four pulse sequence given in the text (Protocol I). (b) It shows how the laser pulses (bars) distribute in time for this scheme.

To solve the problem of speed, we put in the second ingredient, which is coherent quantum control. The goal is to achieve a certain unitary transformation using all degrees of freedom in the trapped ion system. For that we are free to design the time dependence of all controlling parameters in our experiment: which in our case are the state-dependent forces applied on the ions. Notably, the model in our hands is completely integrable [10] and the control problem is rather easy. In the case of two ions we can use a common force,² and if this force satisfies two commensurability conditions

$$\int_0^T d\tau e^{i\nu\tau} F(\tau) = \int_0^T d\tau e^{i\sqrt{3}\nu\tau} F(\tau) = 0, \quad (22.14)$$

the evolution of the ions can be decomposed into a phase operation and a global rotation

$$|\psi(t)\rangle = e^{-i\phi\sigma_z^i\sigma_z^j} e^{i\sqrt{3}\nu a_r^\dagger a_r t} e^{i\nu a_{cm}^\dagger a_{cm} t} |\psi(0)\rangle. \quad (22.15)$$

Here a_{cm} and a_r stand for the center of mass and stretch modes, and ϕ is the total phase

$$\phi = \frac{1}{2m\hbar} \int_0^T d\tau_1 \int_0^{\tau_1} d\tau_2 F(\tau_1) F(\tau_2) \left[\sin(\nu t) - \frac{1}{\sqrt{3}} \sin(\sqrt{3}\nu t) \right]_{t=\tau_2-\tau_1}. \quad (22.16)$$

²For instance, shining the same laser light standing wave on both atoms.

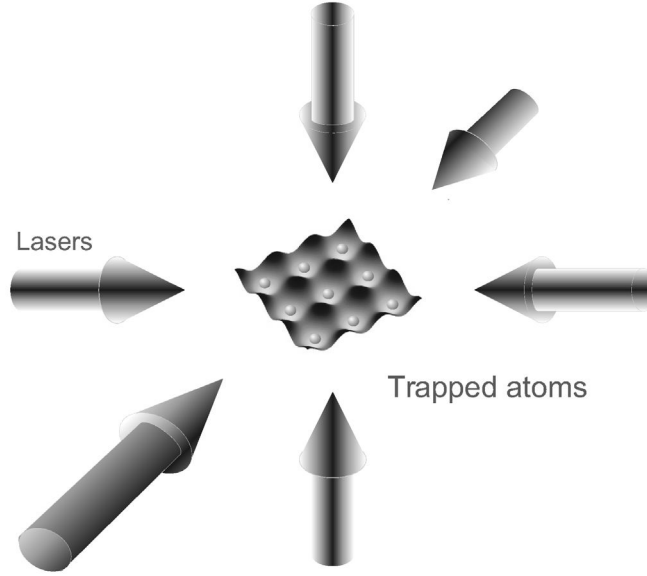


Figure 22.6. Laser setup and resulting optical lattice configuration in 3D.

In Ref. [9] it was suggested to use ultrashort laser pulses to kick the ions instantaneously, so that the forces may actually be written as a sequence of delta kicks

$$F(\tau) = \sum_{n=1}^N z_n \delta(\tau - t_n). \quad (22.17)$$

Each protocol is uniquely characterized by the intensity of the kicks, z_j , and the instant in which they are applied, t_j . This parameterization was used in Ref. [9] to design a protocol that produces a phase gate within a period of the trap, $T \sim 1/\nu$, using only four kicks (Fig. 22.5). Furthermore, a similar protocol was found that, within this simplified model, produces the phase gate as fast as wished. However, in practice, making faster gates involves also stronger forces and larger displacements of the ions. These larger displacements are then a source of error, either because the ions approach each other so much that the harmonic model (22.2) breaks down, or because there is some dissipation on the vibrational degrees of freedom which causes an exponential decay of the fidelity. For a deeper analysis of the errors, a generalization to many-ions setups and continuous forces, we refer the reader to [10].

22.3 Trapped Neutral Atoms

The creation of atomic Bose–Einstein condensates (BEC) and degenerate Fermi gases marks a milestone in the history of atomic physics. These degenerate gases enable a range of novel possibilities for applications exploiting ultracold trapped neutral atoms. One of the most promising experiments for future applications is the loading of a BEC into an optical lattice optical lattice [25–27]. Optical lattices are periodic conservative trapping potentials which are created by interference of traveling laser beams yielding standing laser waves in each direction (see Fig. 22.6). The laser light induces AC-Stark shift in atoms and thus acts as a conservative periodic potential [28]. The usage of a BEC for loading has the advantage that atoms are ultracold at temperatures very close to zero so that they practically behave as if their temperature was $T = 0$; in particular all of them occupy the lowest Bloch band. Furthermore the large density of atoms loaded from a BEC enables a filling of few particles per site $n \gtrsim 1$ while laser-cooled atoms loaded into an optical lattice typically only allow a filling factor smaller than one. The resulting competition of atom hopping between neighboring sites and repulsion of two atoms occupying the same lattice site can be used to induce a quantum phase transition from a superfluid (SF) atom state to a Mott insulator (MI) state where each site is filled by exactly one atom thus realizing a regular array of qubits. Further manipulation of atoms using external fields (e.g., laser) then allows quantum information processing on the qubits.

22.3.1 Optical lattices

In this section we present several examples of different laser-atom configurations for the realization of a variety of trapping potentials, in particular periodic optical lattices with different geometries, and even trapping potentials whose shape depends on the internal (hyperfine) state of the atom. These setups are the basis for realizing quantum memories and quantum gates. In our derivations we will neglect spontaneous emission and later establish the consistency of this approximation by giving an estimate for the rate at which photons are spontaneously emitted in a typical optical lattice setup.

Optical potentials The Hamiltonian of an atom of mass m is given by $H_A = \mathbf{p}^2/2m + \sum_j \omega_j |e_j\rangle \langle e_j|$. Here $\mathbf{p}$ is the center of mass momentum operator and $|e_j\rangle$ denotes the internal atomic states with energies ω_j (setting $\hbar \equiv 1$). We assume the atom to initially occupy a metastable internal state $|e_0\rangle \equiv |a\rangle$ which defines the point of zero energy. The atom is subject to a classical laser field with electric field $\mathbf{E}(\mathbf{x}, t) = E(\mathbf{x}, t)\epsilon \exp(-i\omega t)$, where ω is the frequency and ϵ the polarization vector of the laser. The amplitude of the electric field $E(\mathbf{x}, t)$ is varying slowly in time t compared to $1/\omega$ and slowly in space $\mathbf{x}$ compared to the size of the atom. In this situation the interaction between atom and laser is adequately described in dipole approximation by the Hamiltonian $H_{\text{dip}} = -\mu\mathbf{E}(\mathbf{x}, t) + \text{h.c.}$, where μ is the dipole operator of the atom. We assume the laser to be far detuned from any optical transition so that no significant population is transferred from $|a\rangle$ to any of the other internal atomic states via H_{dip} . We can thus treat the additional atomic levels in perturbation theory and eliminate them from the dynamics. In doing so we find the AC-Stark shift of the internal state $|a\rangle$ in the form of a conservative potential $V(\mathbf{x})$ whose strength is determined by the atomic dipole operator and the properties of the laser light at the center of mass position $\mathbf{x}$ of the atom. In particular

$V(\mathbf{x})$ is proportional to the laser intensity $|E(\mathbf{x}, t)|^2$. Under these conditions the motion of the atom is governed by the Hamiltonian $H = \mathbf{p}^2/2m + V(\mathbf{x})$.

Let us now specialize the situation to the case where the dominant contribution to the optical potential arises from one excited atomic level $|e\rangle$ only. In a frame rotating with the laser frequency the Hamiltonian of the atom is approximately given by $H_A = \mathbf{p}^2/2m + \delta |e\rangle \langle e|$, where $\delta = \omega_e - \omega$ is the detuning of the laser from the atomic transition $|e\rangle \leftrightarrow |a\rangle$. The dominant contribution to the atom–laser interaction neglecting all quickly oscillating terms (i.e., in the rotating wave approximation) is given by $H_{\text{dip}} = \Omega(\mathbf{x}) |e\rangle \langle a|/2 + \text{h.c.}$. Here $\Omega = -2E(\mathbf{x}, t) \langle e | \mu \epsilon | a \rangle$ is the so-called Rabi frequency driving the transitions between the two atomic levels. For large detuning $\delta \gg \Omega$ adiabatically eliminating the level $|e\rangle$ yields the explicit expression $V(\mathbf{x}) = |\Omega(\mathbf{x})|^2/4\delta$ for the optical potential. The population transferred to the excited level $|e\rangle$ by the laser is given by $|\Omega(\mathbf{x})|^2/4\delta^2$ and this is the reason why we require $\Omega(\mathbf{x}) \ll \delta$ for our adiabatic elimination to be valid.

Periodic lattices For creating an optical lattice potential we start by superimposing two counter propagating running wave laser beams with $E_{\pm}(\mathbf{x}, t) = E_0 \exp(\pm i k x)$ propagating in the x -direction with amplitude E_0 , wave number k and wavelength $\lambda = 2\pi/k$. They create an optical potential $V(\mathbf{x}) \propto \cos^2(kx)$ in one dimension with periodicity $a = \lambda/2$. Using two further pairs of laser beams propagating in y - and z -directions, respectively, a full three-dimensional periodic trapping potential of the form

$$V(\mathbf{x}) = V_{0x} \cos^2(kx) + V_{0y} \cos^2(ky) + V_{0z} \cos^2(kz) \quad (22.18)$$

is realized. The depth of this lattice in each direction is determined by the intensity of the corresponding pair of laser beams which is easily controlled in an experiment.

Bloch bands and Wannier functions For simplicity we only consider one spatial dimension in Eq. (22.18) and write down the Bloch functions $\phi_q^{(n)}(x)$ with q the quasi momentum and n the band index. The corresponding eigenenergies $E_q^{(n)}$ for different depths of the lattice V_0/E_R in units of the recoil energy $E_R = k^2/2m$ are shown in Fig. 22.7. Already for a moderate lattice depth of a few recoil the separation between the lowest lying bands is much larger than their extend. In this case a good approximation for the gap between these bands is given by the oscillation frequency ω_T of a particle trapped close to one of the minima x_j ($\equiv$ lattice site) of the optical potential. Approximating the lattice around a minimum by a harmonic oscillator we find $\omega_T = \sqrt{4V_0 E_R}$ [29].

The dynamics of particles moving in the lowest lying well separated bands will be described using the Wannier functions. These are complete sets of orthogonal normalized real mode functions for each band n . For properly chosen phases of the $\phi_q^{(n)}(x)$ the Wannier functions optimally localized at lattice site x_j are defined by [30]

$$w_n(x - x_j) = \Theta^{-1/2} \sum_q e^{-iqx_j} \phi_q^{(n)}(x), \quad (22.19)$$

where Θ is a normalization constant. Note that for $V_0 \rightarrow \infty$ and fixed k the Wannier function $w_n(x)$ tends toward the wavefunction of the n th excited state of a harmonic oscillator with

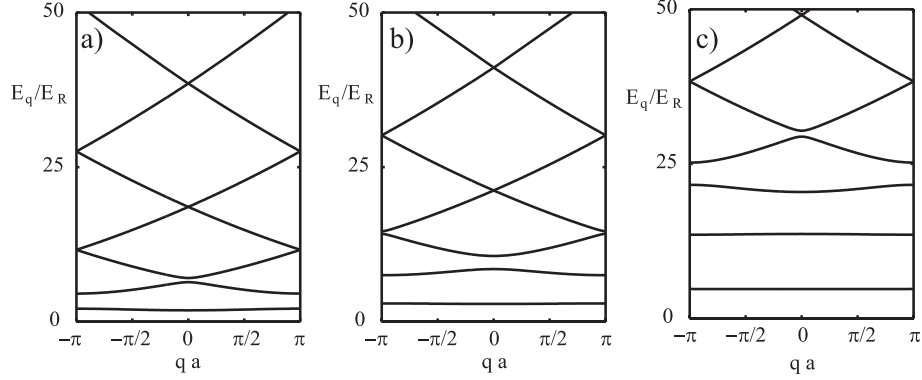


Figure 22.7. Band structure of an optical lattice of the form $V_0(x) = V_0 \cos^2(kx)$ for different depths of the potential. (a) $V_0 = 5E_R$, b) $V_0 = 10E_R$, and c) $V_0 = 25E_R$.

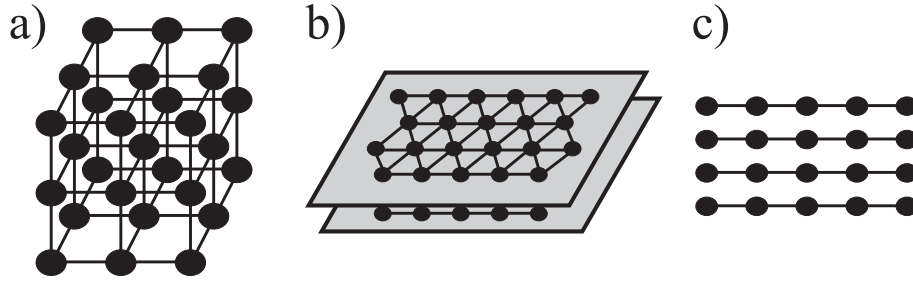


Figure 22.8. (a) Simple three-dimensional cubic lattice. (b) Sheets of a two-dimensional triangular lattices. (c) Set of one-dimensional lattice tubes. In (a)–(c) tunneling of atoms through the optical potential barriers is only possible between sites which are connected by lines.

the ground state size $a_0 = \sqrt{1/m\omega_T}$. We will use the Wannier functions to describe particles trapped in the lattice since they allow (i) to attribute a mean position x_j to the particles in a given mode and (ii) to easily account for local interactions between particles because the dominant contribution to the interaction energy arises from particles occupying the same lattice site x_j .

Lattice geometry and site offset The lattice site positions $\mathbf{x}_j$ determine the lattice geometry. For instance the above arrangement of three pairs of orthogonal laser beams leads to a simple cubic lattice (shown in Fig. 22.8a). Since the laser setup is very versatile different lattice geometries can be achieved easily. As an example consider three laser beams propagating at angles $2\pi/3$ with respect to each other in the xy -plane and all of them being polarized in the z direction. The resulting lattice potential is given by $V(\mathbf{x}) \propto 3 + 4 \cos(3kx/2) \cos(\sqrt{3}ky/2) + 2 \cos(\sqrt{3}ky)$ which is a triangular lattice in two dimensions. An additional pair of lasers in the z direction can be used to create localized

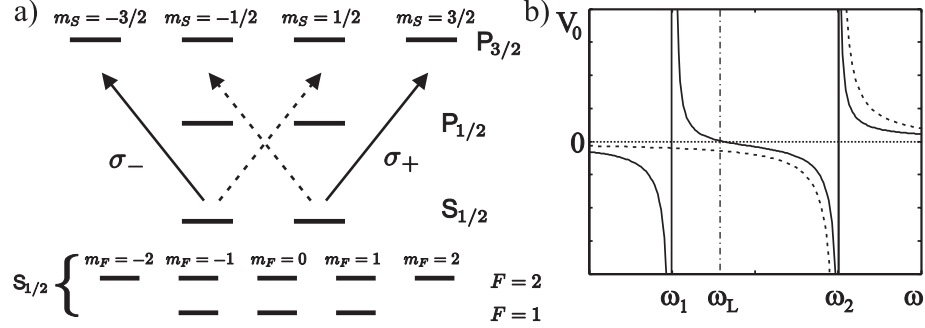


Figure 22.9. (a) Atomic fine and hyperfine structure of the most commonly used alkali atoms ^{23}Na and ^{87}Rb . (b) Schematic AC-Stark shift of the atomic level $S_{1/2}$ with $m_s = 1/2$ (dashed curve) and with $m_s = -1/2$ (solid curve) due to the laser beam σ_+ as a function of the laser frequency ω . The AC-Stark shift of the level $S_{1/2}$ with $m_s = -1/2$ can be made 0 by choosing the laser frequency $\omega = \omega_L$.

lattice sites (cf. Fig. 22.8b). Furthermore, as will be discussed later in Sec. 22.3.2, the motion of atoms can be restricted to two or even one spatial dimension by large laser intensities. As will be shown it is thus possible to create truly one- and two-dimensional lattice models as indicated in Fig. 22.8b and c. The offset of the lattice sites can be manipulated through a superimposed magnetic trapping field or Stark shifts introduced by additional lasers. In particular, regular patterns are useful for quantum computing as they exploit the inherent scalability of optical lattice setups.

State-dependent lattices As already mentioned above the strength of the optical potential crucially depends on the atomic dipole moment between the internal states involved. Thus we can exploit selection rules for optical transitions to create differing traps for different internal states of the atom [31–33]. We will illustrate this by an example that is particularly relevant in what follows. We consider an atom with the fine structure shown in Fig. 22.9a, like e.g., ^{23}Na or ^{87}Rb , interacting with two circularly polarized laser beams. The right circularly polarized laser σ^+ couples the level $S_{1/2}$ with $m_s = -1/2$ to two excited levels $P_{1/2}$ and $P_{3/2}$ with $m_s = 1/2$ and detunings of opposite sign. The respective optical potentials add up. The strength of the resulting AC-Stark shift is shown in Fig. 22.9b as a function of the laser frequency ω . For $\omega = \omega_L$ the two contributions cancel. The same can be achieved for the σ^- laser acting on the $S_{1/2}$ level with $m_s = 1/2$. Therefore, at $\omega = \omega_L$ the AC-Stark shift of the levels $S_{1/2}$ with $m_s = \pm 1/2$ are purely due to $\sigma_{\pm}$ polarized light which we denote by $V_{\pm}(x)$. The corresponding level shifts of the hyperfine states in the $S_{1/2}$ manifold (shown in Fig. 22.9a) are related to $V_{\pm}(x)$ by the Clebsch–Gordan coefficients, e.g., $V_{|F=2, m_F=2\rangle}(x) = V_+(x)$, $V_{|F=1, m_F=1\rangle}(x) = 3V_+(x)/4 + V_-(x)/4$, and $V_{|F=1, m_F=-1\rangle}(x) = V_+(x)/4 + 3V_-(x)/4$.

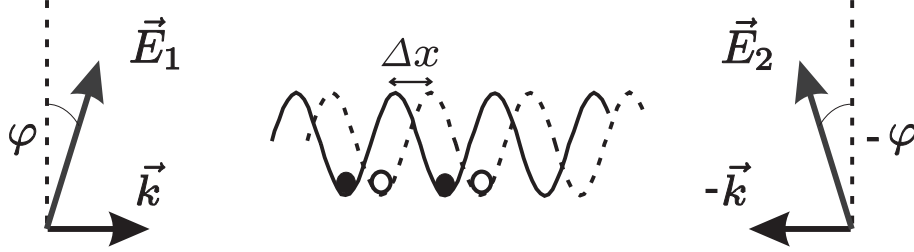


Figure 22.10. Laser configuration for a state selective optical potential. Two standing circular polarized standing waves are produced out of two counter-propagating running waves with an angle 2φ between their polarization axes. The lattice sites for different internal states (indicated by closed and open circles) are shifted by $\Delta x = 2\varphi/k$.

State selectively moving the lattice The two standing waves $\sigma_{\pm}$ can be produced out of two running counter-propagating waves with the same intensity as shown in Fig. 22.10. Moreover, it is possible to move nodes of the resulting standing waves by changing the angle of the polarization between the two running waves [31]. Let $\{e_1, e_2, e_3\}$ be three unit vectors in space pointing along the $\{x, y, z\}$ direction, respectively. The position dependent part of the electric field of the two running waves $\mathbf{E}_{1,2}$ is given by $\mathbf{E}_1 \propto e^{ikx} (\cos(\varphi)e_3 + \sin(\varphi)e_2)$, $\mathbf{E}_2 \propto e^{-ikx} (\cos(\varphi)e_3 - \sin(\varphi)e_2)$. The sum of the two electric fields is thus $\mathbf{E}_1 + \mathbf{E}_2 \propto \cos(kx - \varphi)\sigma_- + \cos(kx + \varphi)\sigma_+$, where $\sigma_{\pm} = e_2 \pm ie_3$ and the resulting optical potentials are given by

$$V_{\pm}(x) \propto \cos^2(kx \pm \varphi). \quad (22.20)$$

By changing the angle φ it is therefore possible to move the nodes of the two standing waves in the opposite directions. Since these two standing waves act as internal state dependent potentials for the hyperfine states the optical lattice can be moved in the opposite directions for different internal hyperfine states.

Validity In all of the above calculations we have only considered the coherent interactions of an atom with laser light. Any incoherent scattering processes which lead to spontaneous emission were neglected. We will now establish the validity of this approximation by estimating the mean rate Γ_{eff} of spontaneous photon emission from an atom trapped in the lowest vibrational state of the optical lattice. This rate of spontaneous emission is given by the product of the life time Γ of the excited state and the probability of the atom occupying this state. In the case of a blue detuned optical lattice (dark optical lattice) $\delta < 0$ the potential minima coincide with the points of no light intensity and we find the effective spontaneous emission rate $\Gamma_{\text{eff}} \approx -\Gamma\omega_T/4\delta$. If the lattice is red detuned (bright optical lattice) $\delta > 0$ the potential minima match the points of maximum light intensity and we find $\Gamma_{\text{eff}} \approx \Gamma V_0/\delta$. Since $V_0 > \omega_T$ the spontaneous emission in a red detuned optical lattice will always be more significant than in a blue lattice, however, as long as $V_0 \ll \delta$ spontaneous emission does not play a significant role.

Typical numerical values In a typical blue detuned optical lattice, with $\lambda = 514$ nm for ^{23}Na atoms ($S_{1/2} - P_{3/2}$ transition at $\lambda_2 = 589$ nm and $\Gamma = 2\pi \times 10$ MHz), the recoil energy is $E_R \approx 2\pi \times 33$ kHz and the detuning from the atomic resonance is $\delta \approx -2.3 \times 10^9 E_R$. A lattice with depth $V_0 = 25E_R$ leads to a trapping frequency of $\omega_T = 10E_R$ yielding a spontaneous emission rate of $\Gamma_{\text{eff}} \approx 10^{-2}/s$ while experiments are typically carried out in times shorter than one second. Therefore spontaneous emission does not play a significant role in such experiments.

22.3.2 The (Bose) Hubbard Hamiltonian

We consider a gas of interacting particles moving in an optical lattice. Starting from the full many body Hamiltonian including local two particle interactions, we first give brief derivation of the Bose–Hubbard model (BHM) [29,34] and present related models which can be realized in an optical lattice. Then we proceed by discussing adiabatic and irreversible schemes for loading the lattice with ultracold atoms. Throughout we will concentrate on bosonic atoms. Similar derivations for fermions lead to quantum registers realized by fermions [33,35].

The (Bose) Hubbard model The Hamiltonian of a weakly interacting gas in an optical lattice is

$$H_{\text{full}} = \int d^3x \hat{\Psi}^\dagger(\mathbf{x}) \left(\frac{\mathbf{p}^2}{2m} + V_0(\mathbf{x}) + V_T(\mathbf{x}) \right) \hat{\Psi}(\mathbf{x}) + \frac{g}{2} \int d^3x \hat{\Psi}^\dagger(\mathbf{x}) \hat{\Psi}^\dagger(\mathbf{x}) \hat{\Psi}(\mathbf{x}) \hat{\Psi}(\mathbf{x}) \quad (22.21)$$

with $\hat{\Psi}(\mathbf{x})$ the bosonic field operator for atoms in a given internal atomic state $|b\rangle$ and $V_T(\mathbf{x})$ a (slowly varying compared to the optical lattice $V_0(\mathbf{x})$) external trapping potential, e.g., a magnetic trap or a superlattice potential. The parameter g is the interaction strength between two atomic particles. If atoms interact via s -wave scattering only it is given by $g = 4\pi a_s/m$ with a_s the s -wave scattering length. We assume all particles to be in the lowest band of the optical lattice and expand the field operator in terms of the Wannier functions $\hat{\Psi}(\mathbf{x}) = \sum_i \hat{b}_i w^{(0)}(\mathbf{x} - \mathbf{x}_i)$, where $\hat{b}_i$ is the destruction operator for a particle in site $\mathbf{x}_i$. We find

$$H_{\text{full}} = - \sum_{i,j} J_{ij} \hat{b}_i^\dagger \hat{b}_j + \frac{1}{2} \sum_{i,j,k,l} U_{ijkl} \hat{b}_i^\dagger \hat{b}_j^\dagger \hat{b}_k \hat{b}_l,$$

where

$$J_{ij} = - \int d^3x w_0(\mathbf{x} - \mathbf{x}_i) \left(\frac{p^2}{2m} + V_0(\mathbf{x}) + V_T(\mathbf{x}) \right) w_0(\mathbf{x} - \mathbf{x}_j),$$

and

$$U_{ijkl} = g \int d^3x w_0(\mathbf{x} - \mathbf{x}_i) w_0(\mathbf{x} - \mathbf{x}_j) w_0(\mathbf{x} - \mathbf{x}_k) w_0(\mathbf{x} - \mathbf{x}_l).$$

The numerical values for the offsite interaction matrix elements U_{ijkl} involving Wannier functions centered at different lattice sites as well as tunneling matrix elements J_{ij} to sites

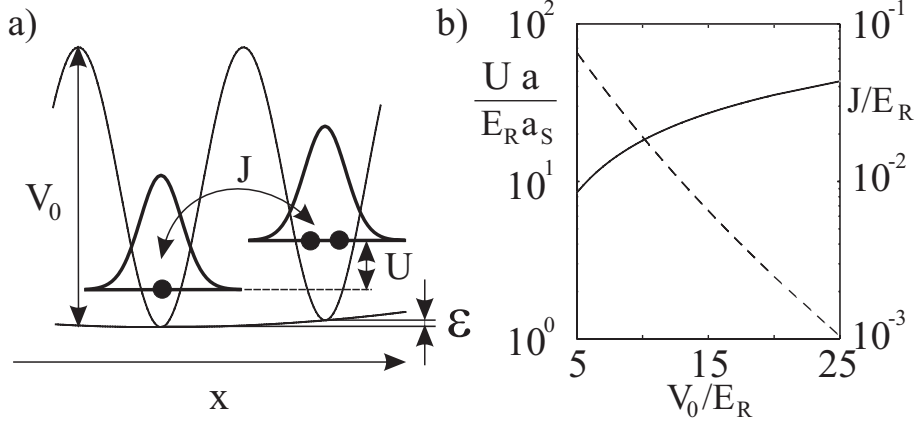


Figure 22.11. (a) Interpretation of the BHM in an optical lattice as discussed in the text. (b) Plot of scaled onsite interaction U/E_R multiplied by a/a_s ($\gg 1$) (solid line with axis on left-hand side of graph) and J/E_R (dashed line, with axis on right-hand side of graph) as a function of $V_0/E_R \equiv V_{x,y,z0}/E_R$ (for a cubic 3D lattice).

other than nearest neighbors (note that diagonal tunneling is not allowed in a cubic lattice since the Wannier functions are orthogonal) are small compared to onsite interactions $U_{0000} \equiv U$ and nearest neighbor tunneling $J_{01} \equiv J$ for reasonably deep lattices $V_0 \gtrsim 5E_R$. We can therefore neglect them and for an isotropic cubic optical lattice arrive at the standard Bose–Hubbard Hamiltonian

$$H_{\text{BH}} = -J \sum_{\langle i,j \rangle} \hat{b}_i^\dagger \hat{b}_j + \frac{U}{2} \sum_j \hat{b}_j^\dagger \hat{b}_j^\dagger \hat{b}_j \hat{b}_j + \sum_j \epsilon_j \hat{b}_j^\dagger \hat{b}_j. \quad (22.22)$$

Here $\langle i,j \rangle$ denotes the sum over nearest neighbors and the terms $\epsilon_j = V_T(\mathbf{x}_j)$ arise from the additional trapping potential. The physics described by H_{BH} is schematically shown in Fig. 22.11a. Particles gain an energy of J by hopping from one site to the next while two particles occupying the same lattice site provide an interaction energy U . An increase in the lattice depth V_0 leads to higher barriers between the lattice sites decreasing the hopping energy J as shown in Fig. 22.11b. At the same time two particles occupying the same lattice site become more compressed which increases their repulsive energy U (cf. Fig. 22.11b).

Tunneling term J In the case of an ideal gas, where $U = 0$ the eigenstates of H_{BH} are easily found for $\epsilon_i = 0$ and periodic boundary conditions. From the eigenvalue equation $E_q^{(0)} = -2J \cos(qa)$ we find that $4J$ is the height of the lowest Bloch band. Furthermore we see that the energy is minimized for $q = 0$ and therefore particles in the ground state are delocalized over the whole lattice, i.e., the ground state of N particles in the lattice is $|\Psi_{\text{SF}}\rangle \propto (\sum_i \hat{b}_i^\dagger)^N |\text{vac}\rangle$ with $|\text{vac}\rangle$ the vacuum state. In this limit the system is superfluid (SF) and possesses first order long range off diagonal correlations [29, 34].

Onsite interaction U In the opposite limit, where the interaction U dominates the hopping term J , the situation changes completely. As discussed in detail in [29, 34] a quantum phase transition takes place at about $U \approx 5.8zJ$, where z is the number of nearest neighbors of each lattice site. The long-range correlations cease to exist in the ground state and instead the system becomes Mott insulating (MI). For commensurate filling of one particle per lattice site this MI state can be written as $|\Psi_{MI}\rangle \propto \prod_j \hat{b}_j^\dagger |\text{vac}\rangle$. Using two internal long-lived states of atoms in this MI state realizes a scalable quantum register with coherence times of the order of seconds.

22.3.3 Loading schemes

Only by using atomic Bose–Einstein condensates (BEC) it has become possible to achieve large densities corresponding to a few particles per lattice site. A BEC can be loaded from a magnetic trap into a lattice by slowly turning on the lasers and superimposing the lattice potential over the trap. The system adiabatically undergoes the transition from the SF ground state of the BEC to the MI state for a deep optical lattice [29]. Experimentally this loading scheme and the SF to MI transition was realized in several experiments [36–38]. The number of defects in the created *optical crystals* were limited to approximately 10% of the sites. For applications in quantum computing it is essential to decrease these defects even further.

Defect suppressed optical lattices One method to further decrease the number of defects in the lattice was recently described in [39]. The proposed setup utilizes two optical lattices for internal states $|a\rangle$ and $|b\rangle$ with substantially different interaction strengths $U_b \neq U_a$ and identical lattice site positions $\mathbf{x}_i$. Initially atoms in $|a\rangle$ are adiabatically loaded into the lattice and brought into a MI state, where the number of particles per site may vary between $n = 1, \dots, n_{\max}$ because of defects. Then a Raman laser with a detuning varying slowly in time between δ_i and δ_f is used to adiabatically transfer exactly one particle from $|a\rangle$ to $|b\rangle$ as shown in Fig. 22.12a and b. This is done by going through exactly one avoided crossing. During the whole of this process transfer of further atoms is blocked by interactions. This scheme allows a significant suppression of defects and—with additional site offsets ϵ_i —can also be used for patterned loading [38] of the $|b\rangle$ lattice.

Irreversible loading schemes Further improvement could be achieved via irreversible loading schemes. An optical lattice is immersed in an ultracold degenerate gas from which atoms are transferred into the first Bloch band of the lattice. By spontaneous emission of a phonon [40] the atom then decays into the lowest Bloch band as schematically shown in Fig. 22.12. By atom–atom repulsion further atoms are blocked from being loaded into the lattice. This scheme can also be extended to cool atomic patterns in a lattice. In contrast to adiabatic loading schemes it has the advantage of being repeatable without removing atoms already stored in the lattice.

22.3.4 Quantum computing in optical lattices

The above methods and experiments for creating optical crystals are a very important step toward realizing theoretical ideas for implementing the basic ingredients of a quantum com-

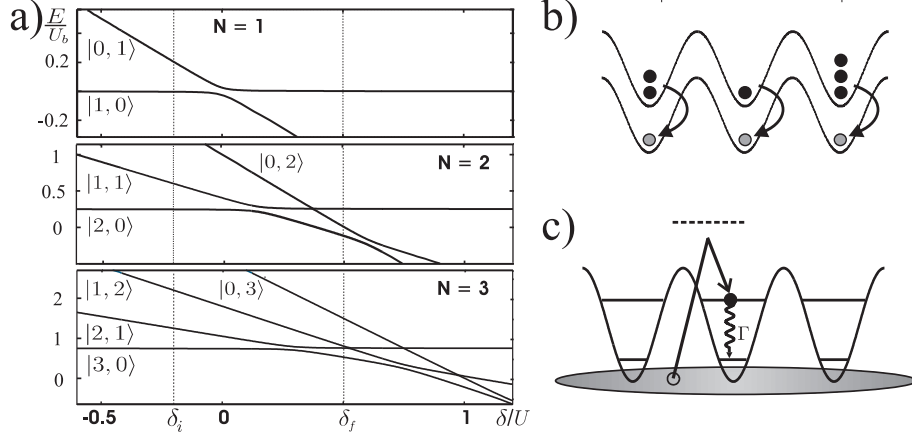


Figure 22.12. (a) Avoided crossings in the energy eigenvalues E for $n = 1, 2, 3$ (Note the variation in the vertical scale). For the chosen values of δ_i and δ_f (dotted vertical lines) only one avoided crossing is traversed transferring exactly one atom from $|a\rangle$ to $|b\rangle$ as schematically shown in (b). (c) Loading of an atom into the first Bloch band from a degenerate gas and spontaneous decay to the lowest band via emitting a phonon into the surrounding degenerate gas.

puter. We first discuss how the basic building blocks can be realized and then turn toward recently developed more sophisticated setups.

Basic building blocks of a quantum computer The SF to MI transition is used to initialize the quantum register. In the MI state each atom has a fixed position and the particle number fluctuations are very small. Using two internal states each atom can thus be used to realize a qubit. Single-qubit operations can be realized by laser interactions of atoms and light and controlled entanglement generation is achieved via interactions between atoms trapped in the lattice [31, 32, 41, 42].

Single-qubit gates In principle it is straightforward to induce single qubit gates by using Raman transitions between the two internal states $|a\rangle$ and $|b\rangle$. Raman transitions with Rabi frequency Ω_R and detuning δ are described by the Hamiltonian

$$H_R = \frac{1}{2} (\Omega_R |a\rangle \langle b| + h.c.) + \delta |b\rangle \langle b|, \quad (22.23)$$

which induce rotations of the qubit state on the Bloch sphere. The axis and angle of this rotation depend on the choice of laser parameters and can be chosen freely. The major problem in inducing single qubit operations is addressing of a single atom as it is difficult to focus a laser to spots of order of an optical wave length which is the typical separation between atoms in the lattice. Possible solutions to this difficulty are using schemes for pattern loading [29, 43], where only specific lattice sites are filled with atoms or using additional marker atoms which specify the atom the laser is supposed to interact with.

MI atoms in an optical lattice have already experimentally been used as qubits and it has been shown that they support multiparticle entangled states [44]. The robustness of these qubits is, however, limited by stray magnetic fields and spin echo techniques need to be used to perform the experiments successfully. A different approach to obtaining robust quantum memory uses a more sophisticated encoding of the qubits [45]. A 1D chain with an even number of atoms encodes a single qubit in the states $|0\rangle = |abab \cdots ab\rangle$ and $|1\rangle = |baba \cdots ba\rangle$. These states both contain the same number of atoms in internal states $|a\rangle$ and $|b\rangle$ and therefore interact with magnetic fields in exactly the same way avoiding dephasing of the quantum information stored in the chain. This and the fact that all the atoms have to flip their internal state to get from one logical state to the other make these qubits very robust against the most dominant experimental sources of decoherence. However, at the same time this robustness makes it more difficult to manipulate them. A laser pulse no longer corresponds to a simple rotation on the Bloch sphere spanned by the logical states $|0\rangle$ and $|1\rangle$ which makes the realization of a single qubit gate difficult. We will describe how these problems can be circumvented later and further details can be found in [45].

Two-qubit gates Implementing a two qubit gate is more challenging than the single qubit gates. The different schemes for two qubit gates can be classified in two categories. The first version relies on the concept of a quantum data bus; the qubits are coupled to a collective auxiliary quantum mode, like e.g., a phonon mode in an ion trap, and entanglement is achieved by swapping the qubits to excitations of the collective mode. The second concept which is the basis for two qubit gates between atoms in optical lattices deploys controllable internal-state dependent two-body interactions. Examples for different interactions are coherent cold collisions of atoms, optical dipole–dipole interactions [31, 32] and the “fast” two-qubit gate based on large permanent dipole interactions between laser excited Rydberg atoms in static electric fields [41]. Besides these dynamical schemes for entanglement creation it is also possible to generate entanglement by purely geometrical means [46]. We will now discuss the different ways to achieve two qubit operations in optical lattices.

Entanglement via coherent ground state collisions The interaction terms describing s -wave collisions between ultracold atoms in one lattice site are analogous to Kerr nonlinearities between photons in quantum optics. For atoms stored in optical lattices these nonlinear atom–atom interactions can be large [31], even for interactions between individual pairs of atoms, thus providing the necessary ingredients to implement two-qubit gates.

We consider a situation where two atoms in a superposition of internal states $|a\rangle$ and $|b\rangle$ are trapped in the ground states of two optical lattice sites (see Fig. 22.13a). Initially, at time $t = -\tau$ these wells are centered at positions sufficiently far apart so that the particles do not interact. The optical lattice potential is then moved state selectively and for simplicity we assume that only the potential for a particle in internal state $|a\rangle$ moves to the right and drags along an atom in state $|a\rangle$ while a particle in state $|b\rangle$ remains at rest. Thus the wavefunction of each atom splits up in space according to the internal superposition of states $|a\rangle$ and $|b\rangle$. When the wavefunction of the left atom in state $|a\rangle$ reaches the second atom in state $|b\rangle$ as shown in Fig. 22.13b they will interact with each other. However, any other combination of internal states will not interact and therefore this collision is conditional on the internal state. A specific laser configuration achieving this state-dependent atom transport has been analyzed

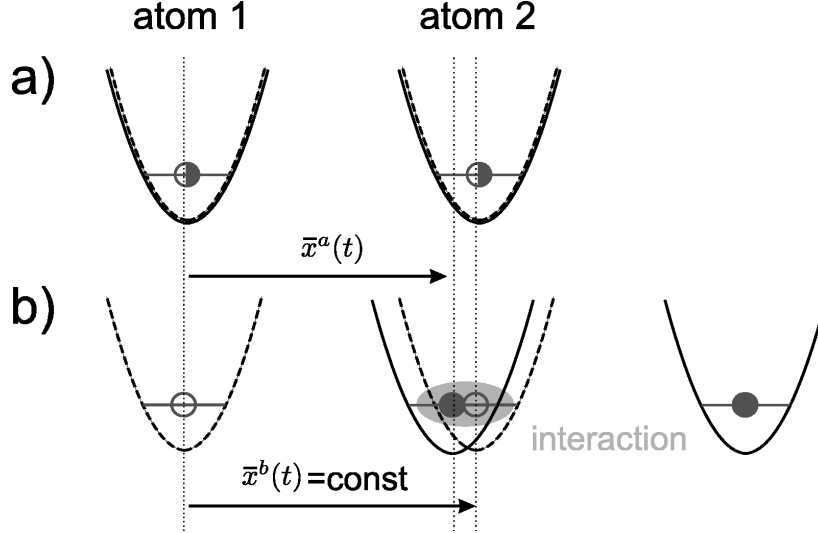


Figure 22.13. We collide one atom in the internal state $|a\rangle$ (filled circle, potential indicated by solid curve) with a second atom in state $|b\rangle$ (open circle, potential indicated by dashed curve)). In the collision the wavefunction accumulates a phase according to Eq. (22.25). (a) Configurations at times $t = \pm\tau$ and b) at time t .

in Ref. [31] for alkali atoms, based on tuning the laser between the fine structure excited p -states. The trapping potentials can be moved by changing the laser parameters. Such trapping potentials could also be realized with magnetic and electric microtraps [47].

We therefore only need to consider the situation where atom 1 is in state $|a\rangle$ and particle 2 is in state $|b\rangle$ to analyze the interactions between the two atoms. The positions of the potentials are moved along the trajectories $\bar{x}^a(t)$ and $\bar{x}^b(t) = \text{const.}$ so that the wavepackets of atoms overlap for a certain time, until they are finally restored to the initial position at the final time $t = \tau$. This situation is described by the Hamiltonian

$$H = \sum_{\beta=a,b} \left[\frac{(\hat{p}^\beta)^2}{2m} + V^\beta(\hat{x}^\beta - \bar{x}^\beta(t)) \right] + u^{ab}(\hat{x}^a - \hat{x}^b). \quad (22.24)$$

Here, $\hat{x}^{a,b}$ and $\hat{p}^{a,b}$ are the position and momentum operators, $V^{a,b}(\hat{x}^{a,b} - \bar{x}^{a,b}(t))$ describe the displaced trap potentials and u^{ab} is the atom–atom interaction term (which leads to the interaction terms in the BHM). Ideally, we want to implement the transformation from before to after the collision,

$$\psi_0^a(x^a - \bar{x}^a(-\tau))\psi_0^b(x^b - \bar{x}^b(-\tau)) \rightarrow e^{i\phi}\psi_0^a(x^a - \bar{x}^a(\tau))\psi_0^b(x^b - \bar{x}^b(\tau)), \quad (22.25)$$

where each atom remains in the ground state $\psi_0^{a,b}$ of its trapping potential and preserves its internal state. The phase $\phi = \phi^a + \phi^b + \phi^{ab}$ will contain a contribution ϕ^{ab} from the interaction (collision) and (trivial) single particle kinematic phases ϕ^a and ϕ^b . The transformation

Eq. (22.25) can be realized in the *adiabatic limit*, whereby we move the potentials slowly on the scale given by the trap frequency, so that atoms remain in their motional ground state. In this case the collisional phase shift is given by $\phi^{ab} = \int_{-\infty}^{\infty} dt \Delta E(t)/\hbar$, where $\Delta E(t)$ is the energy shift induced by the atom–atom interactions

$$\Delta E(t) = \frac{4\pi a_s \hbar^2}{m} \int dx |\psi_0^a(x - \bar{x}^a(t))|^2 |\psi_0^b(x - \bar{x}^b(t))|^2, \quad (22.26)$$

with a_s the s -wave scattering length. In addition we assume that $|\Delta E(t)| \ll \hbar\omega_T$ so that no sloshing motion is excited.

The interaction phase thus only applies when atoms are in internal state $|a, b\rangle$ but not otherwise. Carrying out the above state selective collision with a phase $\phi^{ab} = \pi$ we obtain (up to trivial phases) the mapping (as above we identify $|a\rangle \equiv |0\rangle$ and $|b\rangle \equiv |1\rangle$)

$$\begin{aligned} |0, 0\rangle &\rightarrow |0, 0\rangle \\ |0, 1\rangle &\rightarrow -|0, 1\rangle \\ |1, 0\rangle &\rightarrow |1, 0\rangle \\ |1, 1\rangle &\rightarrow |1, 1\rangle \end{aligned} \quad (22.27)$$

which realizes a two-qubit phase gate that is universal in combination with single-qubit rotations.

State-selective interaction potential An alternative possibility, for a nontrivial logical phase to be obtained, is to rely on a state-independent trapping potential, while defining a procedure where different logical states couple to each other with different energies. An example is given by the interaction between state-selectively switched electrical dipoles [41].

In each qubit, the hyperfine ground states $|a\rangle \equiv |0\rangle$ is coupled by a laser to a given Stark eigenstate $|r\rangle$ which does not correspond to a logical state. The internal dynamics is described by a model Hamiltonian

$$H_I(t, \mathbf{x}_1, \mathbf{x}_2) = \sum_{j=1,2} \left[\delta_j(t) |r\rangle_j \langle r| - \frac{\Omega_j(t, \mathbf{x}_j)}{2} (|a\rangle_j \langle r| + \text{h.c.}) \right] + u |r\rangle_1 \langle r| \otimes |r\rangle_2 \langle r|, \quad (22.28)$$

with $\Omega_j(t, \mathbf{x}_j)$ Rabi frequencies, and $\delta_j(t)$ detunings of the exciting lasers. Here, u is the dipole–dipole interaction energy between the two particles. We have neglected any loss from the excited states $|r\rangle_j$. We discuss two possible realizations of two qubit gates with this dynamics. The most straightforward way to implement a two-qubit gate is to just switch on the dipole–dipole interaction by exciting each qubit to the auxiliary state $|r\rangle$, conditioned on the initial logical state. This can be obtained by two resonant ($\delta_1 = \delta_2 = 0$) laser fields of the same intensity, corresponding to a Rabi frequency $\Omega_1 = \Omega_2 \gg u$. After a time $\tau = \varphi/u$, the gate phase φ is accumulated and the particles can be taken again to the initial internal state. However, besides φ being sensitive to the atomic distance via the energy shift u , during the gate operation (i.e., when the state $|rr\rangle$ is occupied) there are large mechanical effects, due to the dipole–dipole force, which create unwanted entanglement between the internal

and the external degrees of freedom. These problems can be overcome by assuming single-qubit addressability and by moving to the opposite regime of small Rabi frequencies $\Omega_1(t) \neq \Omega_2(t) \ll u$. The gate operation is then performed in three steps, by applying: (i) a π -pulse to the first atom, (ii) a 2π -pulse (in terms of the unperturbed states) to the second atom, and, finally, (iii) a π -pulse to the first atom. The state $|00\rangle$ is not affected by the laser pulses. If the system is initially in one of the states $|01\rangle$ or $|10\rangle$ the pulse sequence (i)-(iii) will cause a sign change in the wavefunction. If the system is initially in the state $|11\rangle$ the first pulse will bring the system to the state $i|r1\rangle$, the second pulse will be *detuned* from the state $|rr\rangle$ by the interaction strength u , and thus accumulate a *small* phase $\tilde{\varphi} \approx \pi\Omega_2/2u \ll \pi$. The third pulse returns the system to the state $e^{i(\pi-\tilde{\varphi})}|11\rangle$, which realizes a phase gate with $\varphi = \pi - \tilde{\varphi} \approx \pi$ (up to trivial single qubit phases). The time needed to perform the gate operation is of the order $\tau \approx 2\pi/\Omega_1 + 2\pi/\Omega_2$. Loss from the excited states $|r\rangle_j$ is small provided $\gamma\Delta t \ll 1$, i.e., $\Omega_j \gg \gamma$. A further improvement is possible by adopting chirped laser pulses with detunings $\delta_{1,2}(t) \equiv \delta(t)$ and *adiabatic* pulses $\Omega_{1,2}(t) \equiv \Omega(t)$, i.e., with a time variation slow on the time scale given by Ω and δ (but still larger than the trap oscillation frequency), so that the system adiabatically follows the dressed states of the Hamiltonian H_I . As found in [41], in this adiabatic scheme the gate phase is

$$\varphi(\tau) = \int_{t_0}^{t_0+\tau} dt \left[\text{sgn}(\tilde{\delta}) \frac{|\tilde{\delta}| - \sqrt{\tilde{\delta}^2 + 2\Omega^2}}{2} - \text{sgn}(\delta) \left(|\delta| - \sqrt{\delta^2 + \Omega^2} \right) \right] \quad (22.29)$$

with $\tilde{\delta} = \delta - \Omega^2/(4\delta + 2u)$ the detuning including a Stark shift. For a specific choice of pulse duration and shape $\Omega(t)$ and $\delta(t)$ we achieve $\varphi(\tau) = \pi$. To satisfy the adiabatic condition, the gate operation time τ has to be approximately one order of magnitude longer than in the other scheme discussed above. In the ideal limit $\Omega_j \ll u$, the dipole–dipole interaction energy shifts the doubly excited state $|rr\rangle$ away from resonance. In such a “dipole-blockade” regime, this state is therefore never populated during gate operation. Hence, the mechanical effects due to atom–atom interaction are greatly suppressed. Furthermore, this version of the gate is only weakly sensitive to the exact distance between atoms, since the distance-dependent part of the entanglement phase is $\tilde{\varphi} \ll \pi$. For the same reason, possible excitations in the particles’ motion do not alter significantly the gate phase, leading to a very weak temperature dependence of the fidelity.

Universal quantum simulators Building a general purpose quantum computer, which is able to run for example Shor’s algorithm, requires quantum resources which will only be available in the long term future. Thus, it is important to identify *nontrivial* applications for quantum computers with limited resources, which are available in the lab at present. Such an example is provided by *Feynman’s universal quantum simulator* (UQS) [48]. A UQS is a controlled device that, operating itself on the quantum level, efficiently reproduces the dynamics of any other many-particle system that evolves according to short-range interactions. Consequently, a UQS could be used to efficiently simulate the dynamics of a generic many-body system, and in this way function as a fundamental tool for research in many body physics, e.g., to simulate spin systems.

According to Jane *et al.* [49] the very nature of the Hamiltonian available in quantum optical systems makes them best suited for simulating the evolution of systems whose building

blocks are also two-level atoms, and having a Hamiltonian $H_N = \sum_a H^{(a)} + \sum_{a \neq b} H^{(ab)}$ that decomposes into one-qubit terms $H^{(a)}$ and two-qubit terms $H^{(ab)}$. A starting observation concerning the simulation of quantum dynamics is that if a Hamiltonian $K = \sum_{j=1}^s K_j$ decomposes into terms K_j acting in a small constant subspace, then by the Trotter formula $e^{-iK\tau} = \lim_{m \rightarrow \infty} (e^{-iK_1\tau/m} e^{-iK_2\tau/m} \dots e^{-iK_s\tau/m})^m$ we can approximate an evolution according to K by a series of short evolutions according to the pieces K_j . Therefore, we can simulate the evolution of an N -qubit system according to the Hamiltonian H_N by composing short one-qubit and two-qubit evolutions generated, respectively, by $H^{(a)}$ and $H^{(ab)}$. In quantum optics an evolution according to one-qubit Hamiltonians $H^{(a)}$ can be obtained directly by properly shining a laser beam on atoms or ions that host the qubits. Instead, two-qubit Hamiltonians are achieved by processing some given interaction $H_0^{(ab)}$ (see the example below) that is externally enforced in the following way. Let us consider two of the N qubits, that we denote by a and b . By alternating evolutions according to some available, switchable two qubit interaction $H_0^{(ab)}$ for some time with local unitary transformations, one can achieve an evolution

$$U(t = \sum_{j=1}^n t_j) = \prod_{j=1}^n V_j \exp(-iH_0^{(ab)} t_j) V_j^\dagger = \prod_{j=1}^n \exp(-iV_j H_0^{(ab)} V_j^\dagger t_j)$$

where $t = \sum_{j=1}^n t_j$, $V_j = u_j^{(a)} \otimes v_j^{(b)}$ with u_j and v_j being one-qubit unitaries. For a small time interval $U(t) \simeq 1 - it \sum_{j=1}^n p_j V_j H_0^{(ab)} V_j^\dagger + O(t^2)$ with $p_j = t_j/t$, so that by concatenating several short gates $U(t)$, $U(t) = \exp(-iH_{\text{eff}}^{(ab)} t) + O(t^2)$, we can simulate the Hamiltonian

$$H_{\text{eff}}^{(ab)} = \sum_{j=1}^n p_j V_j H_0^{(ab)} V_j^\dagger + O(t)$$

for larger times. Note that the systems can be classified according to the availability of homogeneous manipulation, $u_j = v_j$, or the availability of local individual addressing of the qubits, $u_j \neq v_j$.

Cold atoms in optical lattices provide an example where single atoms can be loaded with high fidelity into each lattice site, and where cold controlled collisions provide a way of entangling these atoms in a highly parallel way. This assumes that atoms have two internal (ground) states $|0\rangle \equiv |\downarrow\rangle$ and $|1\rangle \equiv |\uparrow\rangle$ representing a qubit, and that we have two *spin-dependent* lattices, one trapping the $|0\rangle$ state, and the second supporting the $|1\rangle$ state. An interaction between adjacent qubits is achieved by displacing one of the lattices with respect to the other as discussed in the previous subsection. In this way the $|0\rangle$ component of the atom a approaches in space the $|1\rangle$ component of the atom $a+1$, and these collide in a controlled way. Then the two components of each atom are brought back together. This provides an example of implementing an Ising $\sum_{a \neq b} H_0^{(ab)} = \sum_a \sigma_z^{(a)} \otimes \sigma_z^{(a+1)}$ interaction between the qubits, where the $\sigma^{(a)}$'s denote Pauli matrices. By a sufficiently large, relative displacement of the two lattices, also interactions between more distant qubits could be achieved. A local unitary transformation can be enforced by shining a laser on the atoms, inducing an arbitrary

rotation between $|0\rangle$ and $|1\rangle$. On the time scale of the collisions requiring a displacement of the lattice (the entanglement operation) these local operations can be assumed instantaneous. In the optical lattice example it is difficult to achieve an individual addressing of the qubits. Such an addressing would be available in an ion trap array as discussed in Ref. [50]. These operations provide us with the building blocks to obtain an effective Hamiltonian evolution by time averaging as outlined above.

As an example let us consider the ferromagnetic [antiferromagnetic] Heisenberg Hamiltonian

$$H = J \sum_{j=x,y,z} \sigma_j \otimes \sigma_j \quad (22.30)$$

where $J > 0$ [$J < 0$]. An evolution can be simulated by short gates with $H_0^{(ab)} = \gamma \sigma_z \otimes \sigma_z$ alternated with local unitary operations

$$\begin{aligned} p_1 &= \frac{1}{3}, & V_1 &= \hat{1} \otimes \hat{1} \\ p_2 &= \frac{1}{3}, & V_2 &= \frac{\hat{1} - i\sigma_x}{\sqrt{2}} \otimes \frac{\hat{1} - i\sigma_x}{\sqrt{2}} \\ p_3 &= \frac{1}{3}, & V_3 &= \frac{\hat{1} - i\sigma_y}{\sqrt{2}} \otimes \frac{\hat{1} - i\sigma_y}{\sqrt{2}} \end{aligned}$$

without local addressing, as provided by the standard optical lattice setup. The ability to perform independent operations on each of the qubits would translate into the possibility to simulate any bipartite Hamiltonians.

An interesting aspect is the possibility to simulate effectively different lattice configurations: for example, in a 2D pattern a system with nearest neighbor interactions in a triangular configuration can be obtained from a rectangular array configuration. This is achieved by making the subsystems in the rectangular array interact not only with their nearest neighbor but also with two of their next-to-nearest neighbors in the same diagonal (see Fig. 22.14).

One of the first and most interesting applications of quantum simulations is the study of quantum phase transitions [51]. In this case one would obtain the ground state of a system, adiabatically connecting ground states of systems in different regimes of coupling parameters, allowing to determine its properties.

Multiparticle maximally entangled states in optical lattices Let us assume that the Rydberg interactions between neighboring atoms are turned on all the time and that atoms are arranged in a 1D chain. Furthermore, we allow each atom to either tunnel between two adjacent wells whose ground states are denoted by $|a\rangle$ and $|b\rangle$ or to have an additional laser driving Raman transitions between two internal states (again denoted by $|a\rangle$ and $|b\rangle$). This situation is schematically shown in Fig. 22.15.

The dynamics of this setup can be understood as follows. Hopping between the two modes $|a\rangle_j$ and $|b\rangle_j$ of the j th atom is described by

$$H_h = B \sum_j \left(|a\rangle_j \langle b| + \text{h.c.} \right) \equiv B \sum_j \sigma_x^{(j)} \quad (22.31)$$

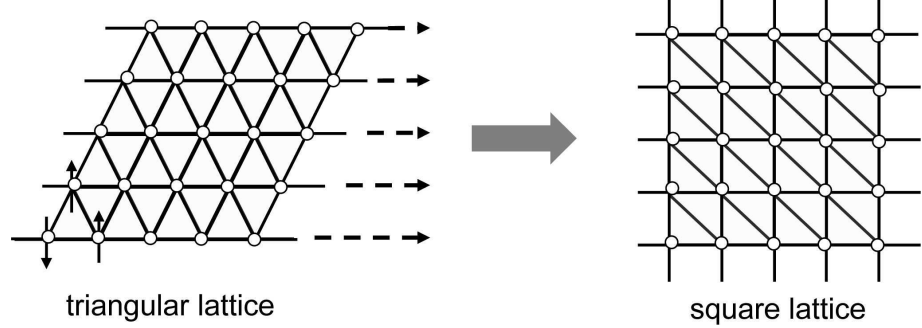


Figure 22.14. Illustrating how triangular configurations of atoms with nearest neighbor interactions may be simulated in a rectangular lattice.

with $\sigma_x^{(j)}$ the Pauli x -matrix for the two states (viewed as a spin) of the j th atom and $B > 0$ the energy associated with this process. The ground state of this Hamiltonian is obtained by putting each atom into an equal superposition of states written in spin notation as $|\downarrow_x\rangle_j = (|\uparrow_z\rangle - |\downarrow_z\rangle)/\sqrt{2}$, where $|\uparrow_z\rangle \equiv |a\rangle$ and $|\downarrow_z\rangle \equiv |b\rangle$, i.e., we find

$$|\Psi_h\rangle = |\downarrow_x \downarrow_x \downarrow_x \cdots \downarrow_x\rangle. \quad (22.32)$$

Note that this part of the Hamiltonian is identical to a spin chain in a magnetic field B along the x -axis.

The interaction between two nearest neighbors due to Rydberg interactions is given by

$$H_i = W \sum_j \sigma_z^{(j)} \sigma_z^{(j+1)} \quad (22.33)$$

accounting for the energy difference of having two adjacent particles in the same vs. different internal states. In this case the ground state depends on the sign of the interaction parameter W . For repulsive interactions $W > 0$ the interaction will be minimized by arranging the particles as

$$|\psi_{ir}\rangle = \alpha |\uparrow_z \downarrow_z \cdots \uparrow_z \downarrow_z\rangle + \beta |\downarrow_z \uparrow_z \cdots \downarrow_z \uparrow_z\rangle, \quad (22.34)$$

while for attractive interactions the ground state is

$$|\psi_{ia}\rangle = \alpha |\uparrow_z \uparrow_z \cdots \uparrow_z\rangle + \beta |\downarrow_z \downarrow_z \cdots \downarrow_z\rangle. \quad (22.35)$$

Both of these states are maximally entangled multiparticle states, i.e., extensions of the well-known GHZ states for three particles.

In the total Hamiltonian $H = H_h + H_i$ the interaction energy and the hopping energy compete with each other resulting in a quantum phase transition. When the interaction energy is kept constant and the hopping term is switched off adiabatically, as shown in Fig. 22.15 the state of the system will dynamically change from $|\Psi_h\rangle$ which is a product state to one of the

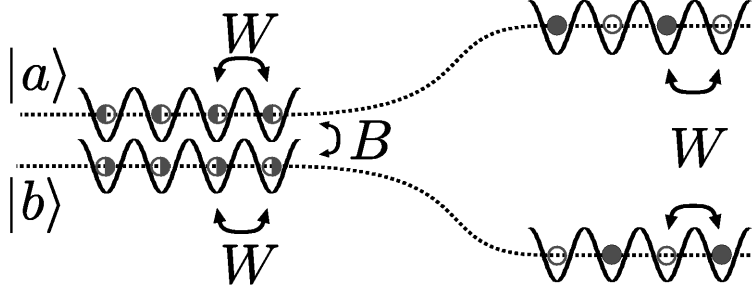


Figure 22.15. Creation of robust multiparticle entangled states in 1D beam splitter setups. Closed circles indicate an atom open circles an empty position.

two states $|\Psi_{ir}\rangle$ or $|\Psi_{ia}\rangle$ depending on the sign of the interaction. The exact values of the parameters α and β depend on the details of the dynamics and are discussed in [45]. These maximally entangled states can serve different purposes depending on the sign of W . Let us discuss the possible applications of these two kinds of maximally entangled states.

Repulsive interactions In this case both parts of the superposition state have the same number of particles in each of the two internal states and thus external stray fields act identically on both, therefore not affecting the parameters α and β . Because of this stability one can use them for storing quantum information in a robust way. Single-qubit gates can be performed by dynamically going back and forth through the quantum phase transition in the whole chain changing the parameters α and β in a controlled way.

Attractive interactions For attractive interactions the terms in the superposition of $|\psi_{ia}\rangle$ will respond to external fields very differently. Therefore, the relative phase between the parameters α and β will be very susceptible to these fields, in fact for N particles in the chain this phase will be N times larger than if there was just a single particle. The two parts of $|\psi_{ia}\rangle$ can thus be used as two arms of an entanglement enhanced atomic interferometer.

A single-atom transistor in a 1D optical lattice As a second example, we consider a spin-1/2 atomic impurity which is used to switch the transport of either a 1D Bose–Einstein Condensate (BEC) or a 1D degenerate Fermi gas initially situated to one side of the impurity [52]. In one spin state the impurity is transparent to the probe atoms, while in the other it acts as single atom mirror prohibiting transport. Observation of the atomic current passing the impurity can then be used as a quantum nondemolition measurement of its internal state, which can be seen to encode a qubit, $|\psi_q\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$. If a macroscopic number of atoms pass the impurity, then the system will be in a macroscopic superposition, $|\Psi(t)\rangle = \alpha|\uparrow\rangle|\phi_\uparrow(t)\rangle + \beta|\downarrow\rangle|\phi_\downarrow(t)\rangle$, which can form the basis for a single shot readout of the qubit spin. Here, $|\phi_\sigma(t)\rangle$ denotes the state of the probe atoms after evolution to time t , given that the qubit is in state σ (see Fig. 22.16). In view of the analogy between state amplification via this type of blocking mechanism and readout with single-electron transistors (SET) used in solid-state systems, we refer to this setup as a single-atom transistor (SAT).

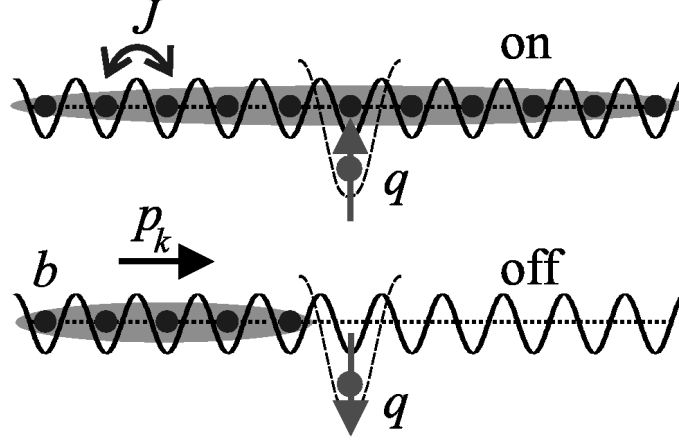


Figure 22.16. A spin 1/2 impurity q used as a switch: in one spin state it is transparent to the probe atoms “on,” but in the other it acts as a single atom mirror “off.” Probe atoms b approaching with momentum p_k are either transmitted or reflected at the impurity.

We consider the implementation of a SAT using cold atoms in 1D optical lattices: probe atoms in the state $|b\rangle$ are loaded in the lattice to the left of a site containing the impurity atom $|q\rangle$, which is trapped by a separate (e.g., spin dependent) potential (cf. Fig. 22.16). The passage of $|b\rangle$ atoms past the impurity q is then governed by the spin-dependent effective collisional interaction $H_{\text{int}} = \sum_{\sigma} U_{\text{eff},\sigma} \hat{b}_0^{\dagger} \hat{b}_0 \hat{q}_{\sigma}^{\dagger} \hat{q}_{\sigma}$. By making use of a quantum interference mechanism, we engineer complete blocking (effectively $U_{\text{eff}} \rightarrow \infty$) for one spin state and complete transmission ($U_{\text{eff}} \rightarrow 0$) for the other.

The quantum interference mechanism needed to engineer U_{eff} can be produced using an optical or magnetic Feshbach resonance [53–55], and we use the present example to illustrate Hamiltonians for impurity interactions involving Feshbach resonances and molecular interactions. For the optical case a Raman laser drives a transition on the impurity site, 0, from the atomic state $\hat{b}_0^{\dagger} \hat{q}_{\sigma}^{\dagger} |\text{vac}\rangle$ via an off-resonant excited molecular state to a bound molecular state back in the lowest electronic manifold $\hat{m}_{\sigma}^{\dagger} |\text{vac}\rangle$ (Fig. 22.17a). We denote the effective two-photon Rabi frequency and detuning by Ω_{σ} and Δ_{σ} , respectively. The Hamiltonian for our system is then given by $\hat{H} = \hat{H}_b + \hat{H}_0$, with

$$\hat{H}_b = -J \sum_{\langle ij \rangle} \hat{b}_i^{\dagger} \hat{b}_j + \frac{1}{2} U_{bb} \sum_j \hat{b}_j^{\dagger} \hat{b}_j (\hat{b}_j^{\dagger} \hat{b}_j - 1), \quad (22.36)$$

$$\begin{aligned} \hat{H}_0 = & \sum_{\sigma} \left[\Omega_{\sigma} (\hat{m}_{\sigma}^{\dagger} \hat{q}_{\sigma}^{\dagger} \hat{b}_0 + \text{h.c.}) - \Delta_{\sigma} \hat{m}_{\sigma}^{\dagger} \hat{m}_{\sigma} \right] \\ & + \sum_{\sigma} \left[U_{qb,\sigma} \hat{b}_0^{\dagger} \hat{q}_{\sigma}^{\dagger} \hat{q}_{\sigma} \hat{b}_0 + U_{bm,\sigma} \hat{b}_0^{\dagger} \hat{m}_{\sigma}^{\dagger} \hat{m}_{\sigma} \hat{b}_0 \right]. \end{aligned} \quad (22.37)$$

Here $\hat{H}_b$ is a familiar Hubbard Hamiltonian for atoms in the state $|b\rangle$; $\hat{H}_0$ describes the additional dynamics due to the impurity on site 0, where atoms in the state $|b\rangle$ and $|q\rangle$ are

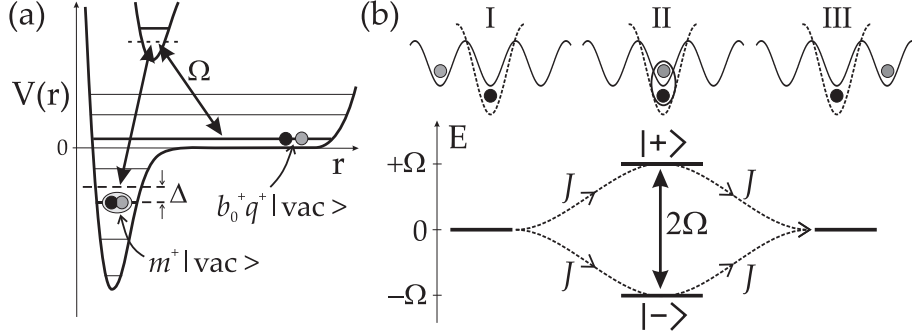


Figure 22.17. (a) The optical Feshbach setup couples the atomic state $\hat{b}_0^\dagger \hat{q}_\sigma^\dagger |\text{vac}\rangle$ (in a particular motional state quantized by the trap) to a molecular bound state of the Born–Oppenheimer potential, $m_\sigma^\dagger |\text{vac}\rangle$, with the effective Rabi frequency Ω_σ and detuning Δ_σ . (b) A single atom passes the impurity (I→III) via the two dressed states (II), $|+\rangle = \hat{b}_0^\dagger \hat{q}_\sigma^\dagger |\text{vac}\rangle + m_\sigma^\dagger |\text{vac}\rangle$ and $|-\rangle = \hat{b}_0^\dagger \hat{q}_\sigma^\dagger |\text{vac}\rangle - m_\sigma^\dagger |\text{vac}\rangle$. Quantum interference between the paths gives rise to an effective tunneling rate $J_{\text{eff},\sigma}$.

converted to a molecular state with effective Rabi frequency Ω_σ and detuning Δ_σ , and the last two terms describe background interactions, $U_{\alpha\beta,\sigma}$ for two particles $\alpha, \beta \in \{q_\sigma, b, m\}$, which are typically weak. This model is valid for $U_{\alpha\beta}, J, \Omega, \Delta \ll \omega_T$ (where ω_T is the energy separation between Bloch bands). Because the dynamics for the two spin channels q_σ can be treated independently, in the following we will consider a single spin channel, and drop the subscript σ .

To understand the qualitative physics behind the above Hamiltonian, let us consider the molecular couplings and associated effective interactions between the $|q\rangle$ and $|b\rangle$ atoms for (i) off-resonant ($\Omega \ll |\Delta|$) and (ii) resonant ($\Delta = 0$) laser driving. In the first case the effective interaction between $|b\rangle$ and $|q\rangle$ atoms is $U_{\text{eff}} = U_{qb} + \Omega^2/\Delta$, where the second term is an AC-Stark shift which plays the role of the resonant enhancement of the collisional interactions between $|b\rangle$ and $|q\rangle$ atoms due to the optical Feshbach resonance. For resonant driving ($\Delta = 0$) the physical mechanism changes. On the impurity site, laser driving mixes the states $\hat{b}_0^\dagger \hat{q}^\dagger |\text{vac}\rangle$ and $m^\dagger |\text{vac}\rangle$, forming two dressed states with energies $\varepsilon_\pm = (U_{qb})/2 \pm (U_{qb}^2/4 + \Omega^2)^{1/2}$ (Fig. 22.17b, II). Thus we have two interfering quantum paths via the two dressed states for the transport of $|b\rangle$ atoms past the impurity. In the simple case of weak tunneling $\Omega \gg J$ and $U_{qb} = 0$ second order perturbation theory gives for the effective tunneling $J_{\text{eff}} = -\frac{J^2}{\varepsilon + \Omega} - \frac{J^2}{\varepsilon - \Omega} \rightarrow 0$ ($|\varepsilon| \ll \Omega$) which shows destructive quantum interference, analogous to the interference effect underlying electromagnetically induced transparency (EIT) [56], and is equivalent to having an effective interaction $U_{\text{eff}} \rightarrow \infty$.

In Ref. [52] the exact dynamics for scattering of a single $|b\rangle$ atom from the impurity is solved exactly, confirming the above qualitative picture of EIT-type quantum interference. Furthermore, in this reference a detailed study of the time-dependent many body dynamics based on the 1D Hamiltonian (22.38) is presented for interacting many-particle systems including a 1D Tonks gas.

References

- [1] Juan Ignacio Cirac and Peter Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74:4091–4094, 1995.
- [2] A. Steane. The ion trap quantum information processor. *App. Phys. B*, 64:623, 1997.
- [3] J. I. Cirac, L. M. Duan, D. Jaksch, and P. Zoller. Quantum optical implementation of quantum information processing. In F. De Martini and C. Monroe, editors, *Proceedings of the International School of Physics “Enrico Fermi” Course CXLVIII, Experimental Quantum Computation and Information*, Amsterdam, 2002. IOS Press.
- [4] P. Zoller, J. I. Cirac, Luming Duan, and J. J. García-Ripoll. Quantum entanglement and information processing. In D. Estève, J. M. Raimond, and J. Dalibard, editors, *Proceedings of the Les Houches Summer School, Session 79*, Amsterdam, 2004. Elsevier.
- [5] J. F. Poyatos, J. I. Cirac, and P. Zoller. Quantum gates with “hot” trapped ions. *Phys. Rev. Lett.*, 81(6):1322–1325, 1998.
- [6] Klaus Molmer and Anders Sorensen. Multiparticle entanglement of hot trapped ions. *Phys. Rev. Lett.*, 82(9):1835–1838, 1999.
- [7] Anders Sorensen and Klaus Molmer. Quantum computation with ions in thermal motion. *Phys. Rev. Lett.*, 82(9):1971–1974, 1999.
- [8] G. J. Milburn, S. Schneider, and D. F. V. James. Ion-trap quantum computing with warm ions. *Fortschr. Phys.*, 48:9–11, 2000.
- [9] J. J. García-Ripoll, P. Zoller, and J. I. Cirac. Speed optimized two-qubit gates with laser coherent control techniques for ion trap quantum computing. *Phys. Rev. Lett.*, 91:157901, 2003.
- [10] J. J. García-Ripoll, P. Zoller, and J. I. Cirac. Coherent control of trapped ions using off-resonant lasers. *Phys. Rev. A*, 71:062309, 2005.
- [11] L.-M. Duan, J. I. Cirac, and P. Zoller. Geometric manipulation of trapped ions for quantum computation. *Science*, 292:1695–1697, 2001.
- [12] C. W. Gardiner and P. Zoller. *Quantum Noise*, chapter . Springer, Berlin, 1999.
- [13] B. DeMarco, A. Ben-Kish, D. Leibfried, V. Meyer, M. Rowe, B. M. Jelenkovic, W. M. Itano, J. Britton, C. Langer, T. Rosenband, and D. J. Wineland. Experimental demonstration of a controlled-NOT wavepacket gate. *Phys. Rev. Lett.*, 89(26):267901, 2002.
- [14] D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barret, J. Britton, W. M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D. J. Wineland. Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate. *Nature*, 422:412, 2003.
- [15] F. Schmidt-Kaler, Hartmut Häffner, Mark Riebe, Stephan Gulde, Gavin P. T. Lancaster, Thomas Deuschle, Christoph Becher, Christian F. Roos, Jürgen Eschner, and Rainer Blatt. Realization of the Cirac–Zoller controlled-NOT quantum gate. *Nature*, 422:408–411, 2003.
- [16] Juan Ignacio Cirac and Peter Zoller. A scalable quantum computer with ions in an array of microtraps. *Nature*, 404(6):579–581, 2000.
- [17] D. Kielpinski, C. Monroe, and D. J. Wineland. Architecture for a large-scale ion-trap quantum computer. *Nature*, 417(13), 709–711, 2002.
- [18] Lin Tian and Peter Zoller. Quantum computing with atomic Josephson junction arrays. *Phys. Rev. A*, 68:042321, 2003.

- [19] S. Stenholm. The semiclassical theory of laser cooling. *Rev. Mod. Phys.*, 58:699–739, 1986.
- [20] D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof. *Res. J. NIST*, 103:259, 1998.
- [21] B. E. King, C. S. Wood, C. J. Myatt, Q. A. Turchette, D. Leibfried, W. M. Itano, C. Monroe, and D. J. Wineland. Cooling the collective motion of trapped ions to initialize a quantum register. *Phys. Rev. Lett.*, 81:1525–1528, 1998.
- [22] C. F. Roos, D. Leibfried, A. Mundt, F. Schmidt-Kaler, J. Eschner, and R. Blatt. Experimental demonstration of ground state laser cooling with electromagnetically induced transparency. *Phys. Rev. Lett.*, 85:5547–5550, 2000.
- [23] T. Calarco, J. I. Cirac, and P. Zoller. Entangling ions in arrays of microscopic traps. *Phys. Rev. A*, 63:062304, 2001.
- [24] D. Jonathan, M. B. Plenio, and P. L. Knight. Fast quantum gates for cold trapped ions. *Phys. Rev. A*, 62:042307, 2000.
- [25] B. P. Anderson and M. A. Kasevich, *Science* 282:1686, 1998; C. Orzel, A. K. Tuchman, M. L. Fenselau, M. Yasuda, and M. A. Kasevich. *Science*, 291:2386, 2001.
- [26] W. K. Hensinger, H. Häffner, A. Browaeys, N. R. Heckenberg, K. Helmerson, C. McKenzie, G. J. Milburn, W. D. Phillips, S. L. Rolston, H. Rubinsztein-Dunlop, and B. Upcroft. *Nature*, 412:52, 2001.
- [27] M. Greiner, O. Mandel, T. Esslinger, T. W. Haensch, and I. Bloch. *Nature*, 415:39, 2002.
- [28] P. Jessen and I. Deutsch. *Adv. At. Mol. Opt. Phys.*
- [29] D. Jaksch, C. Bruder, J. I. Cirac, C. W. Gardiner, and P. Zoller. *Phys. Rev. Lett.*, 81:3108, 1998.
- [30] W. Kohn. *Phys. Rev.*, 115:809, 1959.
- [31] D. Jaksch, H. Briegel, J. Cirac, C. Gardiner, and P. Zoller. *Phys. Rev. Lett.*, 82:1999, 1975.
- [32] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch. *Phys. Rev. Lett.*, 82:1060, 1999.
- [33] W. Liu, F. Wilczek, and P. Zoller. *Phys. Rev. A*, 70:033603, 2004.
- [34] M. Fisher, P. Weichman, G. Grinstein, and D. Fisher. *Phys. Rev. B*, 40:546, 1989.
- [35] W. Hofstetter, J. I. Cirac, P. Zoller, E. Demler, and M. Lukin. *Phys. Rev. Lett.*, 89:220407, 2002.
- [36] M. Greiner, O. Mandel, T. Esslinger, T. Hänsch, and I. Bloch. *Nature*, 415:39, 2002.
- [37] T. Stöferle, H. Moritz, C. Schori, M. Köhl, and T. Esslinger. *Phys. Rev. Lett.*, 92:130403, 2004.
- [38] S. Peil, J. Porto, B. L. Tolra, J. Obrecht, B. King, M. Subbotin, S. Rolston, and W. Phillips. *Phys. Rev. A*, 67:051603, 2003.
- [39] P. Rabl, A. J. Daley, P. O. Fedichev, J. I. Cirac, and P. Zoller. *Phys. Rev. Lett.*, 91:110403, 2003.
- [40] A. J. Daley, P. O. Fedichev, and P. Zoller, *Phys. Rev. A*, 69:022306, 2004.
- [41] D. Jaksch, J. I. Cirac, P. Zoller, S. L. Rolston, R. Cote, and M. D. Lukin. *Phys. Rev. Lett.*, 85:2208, 2000.

- [42] J. K. Pachos and P.L. Knight. *Phys. Rev. Lett.*, 91:107902, 2003.
- [43] S. Peil, J. V. Porto, B. Laburthe Tolra, J. M. Obrecht, B. E. King, M. Subbotin, S. L. Rolston, and W. D. Phillips. *Phys. Rev. A*, 67:051603(R), 2003.
- [44] O. Mandel *et al.* *Nature*, 425:937, 2003.
- [45] U. Dorner, P. Fedichev, D. Jaksch, M. Lewenstein, and P. Zoller. *Phys. Rev. Lett.*, 91:073601, 2003.
- [46] L.-M. Duan, J. I. Cirac, and P. Zoller. *Science*, 292:1695, 2001.
- [47] T. Calarco, H.-J. Briegel, D. Jaksch, J. I. Cirac, and P. Zoller. *J. Mod. Opt.*, 47:2137, 2000.
- [48] S. Lloyd. *Science*, 273: 1073, 1996.
- [49] E. Jane, G. Vidal, W. Dür, P. Zoller, and J. Cirac. *Quantum Information and Computation*, 3(1):15–37, 2003.
- [50] J. I. Cirac and P. Zoller. *Physics Today*, 38–44, 2004.
URL <http://www.physicstoday.org/vol-57/iss-3/contents.html>
- [51] S. Sachdev, Quantum Phase Transitions, Cambridge University Press, Cambridge, 1999.
- [52] A. Micheli, A. Daley, D. Jaksch, and P. Zoller. *Phys. Rev. Lett.*, in press.
- [53] E. Bolda, E. Tiesinga, and P. Julienne. *Phys. Rev. A*, 013403, 2002.
- [54] M. Theis, G. Thalhammer, K. Winkler, M. Hellwig, G. Ruff, R. Grimm, and J. H. Denschlag. *Phys. Rev. Lett.*, 93:123001, 2004.
- [55] T. Calarco, U. Dorner, P. Julienne, C. Williams, and P. Zoller. *Phys. Rev. A*, 70:012306, 2004.
- [56] M. Lukin, *Rev. Mod. Phys.*, 75:457, 2003.

23 Quantum Computing Experiments with Cold Trapped Ions

Ferdinand Schmidt-Kaler

23.1 Introduction

Experiments with single trapped and laser-cooled ions started as early as 1980 when the fluorescence of *one single* laser-cooled Ba^+ ion was observed [1]. At that time, research was motivated strongly by two goals: To beat all those limitations in the spectroscopy of atomic clock transitions, and to manipulate and to observe a single but exemplary quantum mechanical system in well-controlled interaction with an optical laser field. Perhaps the most striking result of those years was the observation of quantum jumps on a single trapped ion [2, 3]. The vivid debate about the adequate interpretation of these results continued over a couple of years, and has transformed today into the reasoning about the quantum measurement process and decoherence, two mind-twisting puzzles of quantum mechanics. The fascinating spectroscopic results of those days [4] laid a basis for the astonishing precision which ion-based standards [5–7] are reaching now with fractional frequency uncertainty $\delta\nu/\nu$ of a few 10^{-15} only. Hence, laboratory experiments can be employed to test even the smallest variations of fundamental constants [8].

Thus, at that time, the scientific ground was well prepared, when in 1994 Cirac and Zoller realized that ions confined in a linear Paul trap should establish an almost ideal setting for an elementary quantum computer (QC) [9]: Each ion in a linear crystal of N ions stores one bit of quantum information (qubit) in two long-lived electronic levels, here called $|g\rangle$ and $|e\rangle$. Quantum logic operations (quantum gates) are implemented by laser–ion interactions [10]. The logic state of these qubits can thus be expressed as $\alpha|g\rangle + \beta|e\rangle$ with complex amplitudes that hold $|\alpha|^2 + |\beta|^2 = 1$. Even though the idea of quantum computing had been existing from 1980 on, pioneered by Manin [11, 12], then Feynman [13, 14], later Deutsch [15], it was known to only a small number of insiders. At the 14th International Conference on Atomic Physics Ekert [16] brought the fantastic Shor factorization algorithm [17, 18] into discussion. The hope for a clear concept of a feasible experiment in the field of quantum optics spurred the activities on the theoretical and experimental side. And precisely this first “blueprint” of a future QC was given by Cirac and Zoller.

Let me repeat here the list of specific advantages of trapped ions for QC, as listed in the seminal paper [9]:

1. In an ion trap, before a quantum algorithm starts, the quantum state of each ion in the crystal can be prepared such that the register of qubits (quantum register) is initialized.

The necessary techniques for this are laser cooling and optical pumping. Both techniques have been established long ago for the purpose of high resolution laser spectroscopy.

2. The ions are stored in a linear Paul trap which uses as a “handle” for trapping simply their positive charge interacting with electric fields. Therefore, the trapping potential might be very deep and tight, without affecting the internal electronic states—which are employed to store qubit information. Cirac and Zoller deduced therefore that in an experiment with a trapped ion crystal serving as a quantum register, the ions being held in a Paul trap under ultra-high vacuum conditions, one could avoid any unwanted coupling of this quantum register to the environment. The decoherence rate could be very low.
3. For the necessary quantum gate operations ions are coherently manipulated by laser radiation. For two-qubit gates the coupling to a common vibrational mode (as a quantum bus) is employed. Details of this method are given in Section 23.6.1 and in the previous Chapter 22. Today, various two-qubit gate operations are proposed and a number of them has been experimentally realized (see Section 23.6).
4. Fairly unique for trapped ions—as compared to other possible physical systems discussed for a QC—is the asset of a very high detection efficiency. The technique of “electron shelving” dates back to Dehmelt in 1975 [19], and allows to scatter a large number of photons off an ion (and to observe at least some fraction of them as clicks on a detector) if the ion is in the qubit state $|g\rangle$, while *no photons* are scattered if the ion is in the state $|e\rangle$. In typical experiments the rate of a few thousand counts per second allows a discrimination between both logic qubit states within at most a few milliseconds. A discrimination quality between both states of better than 99.5% is reached [20].

In 1995 the Cirac and Zoller proposal stimulated a series of experiments using trapped ions for quantum information processing. We can claim today that *the principle of a QC is proven* and that trapped ions are indeed a pioneering technique for its further development. This experimental development also helped to succeed over an initially overwhelming criticism concerning any experimental realization of a QC [21]. Future work is now dedicated mostly to the remaining two experimental demonstrations: Even advanced experiments using 3 or 4, [22–24] recently even 6 and 8 ions [25, 26] cannot yet prove the scalability of ion-based QC. Experiments in the next generation aim to coherently manipulate a few dozen ions in specifically adapted ion trapping structures. Second, the fidelity of quantum logic gate operations has—up to now—never been good enough for an active error correction scheme [27, 28] (see Chapter 7). It is of experimental and theoretical interest to improve gate schemes for this goal; leading finally to a large scale QC.

This article is organized as follows: After a discussion of linear Paul traps, and quantized eigenmodes of ion crystals in the resulting harmonic potential, I will switch to ion–laser interaction and typical qubit candidates. Then I will sketch single-qubit gate-operations and a number of different two-qubit gates. The experimental realization of the Cirac and Zoller gate is outlined. Quantum logic operations have been combined in different ways to establish quantum algorithms, and I will focus on the quantum teleportation algorithm. The work-horse for a future proof of scalability are segmented ion traps which are briefly discussed in the last section.

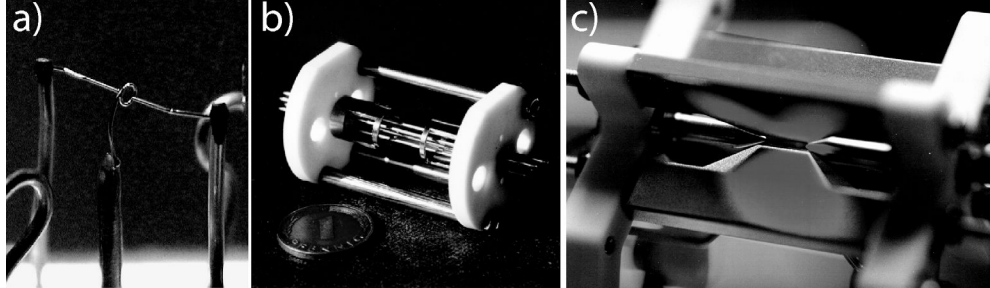


Figure 23.1. Various realizations of macroscopic ion traps: (a) Three-dimensional trap for single ion experiments with ring diameter of 1.2 mm [32]. (b) Four rod trap with ring shaped axial electrodes. The distance between the ring electrodes for axial confinement is 10 mm, the distance between the four rods for radial confinement is 2 mm [33, 34]. (c) Linear trap with four rf-electrodes in the shape of knife edges, axial electrodes in the shape of sharp tips. The free distance between two opposite knife edges is 1.5 mm, the distance between the axial confining tips is 5 mm [35, 36].

23.2 Paul Traps

Charged particles, such as atomic ions, can be confined by electromagnetic fields, either by using a combination of a static electric and magnetic field (Penning trap) or a time dependent inhomogeneous electric field (Paul trap) [29, 30]. In the latter case, a rf-electric field is generated by an appropriate electrode structure and creates a pseudo-potential confining a charged particle. The motion of a particle confined in such a field involves a fast component synchronous to the applied driving frequency (micro motion) and the slow (secular) motion in the dynamically created pseudo-potential. Figure 23.1 shows a selection of ion traps used at the Institute for Experimental Physics, Innsbruck University, Austria [31].

In order to confine the particle in a harmonic potential, we require an electric restoring force $\vec{F} = -q\vec{E}$, which increases linearly with the distance from the origin of the trap, e.g., $\vec{F} \propto -\vec{r}$. Such forces are described by a quadrupole potential $\Phi = \Phi_0(\alpha x^2 + \beta y^2 + \gamma z^2)/r_0^2$, where Φ_0 denotes a voltage applied to a quadrupole electrode configuration, r_0 is the characteristic trap size and the constants α, β, γ determine the shape of the potential, given by the solution of Laplace's equation $\Delta\Phi = 0$. For example, in the case of a *three-dimensional electric field* we find $\alpha = \beta = -2\gamma$. The potential is attractive in the x - and y -directions, but *repulsive* along the z -direction. A static electric field does not lead to three-dimensional binding. If, however, an alternating electric field is applied, the resulting potential is attractive in the x - and y -directions for the first half cycle of the field, and attractive in the z -direction for the second half. A well chosen amplitude and frequency Ω of this alternating rf-field then allows the trapping of charged particles, mass m and charge q , in all three dimensions. The three-dimensional Paul trap provides a confining force with respect to a single point in space, the node of the rf-field, and therefore is mostly used for single ion experiments or for the confinement of three-dimensional crystallized ion structures.

If we regard the electric rf-field in a *two-dimensional geometry* along x - and y -axis only, we find $\alpha = -\beta, \gamma = 0$. Now, the potential is attractive in x - and repulsive in the y -direction

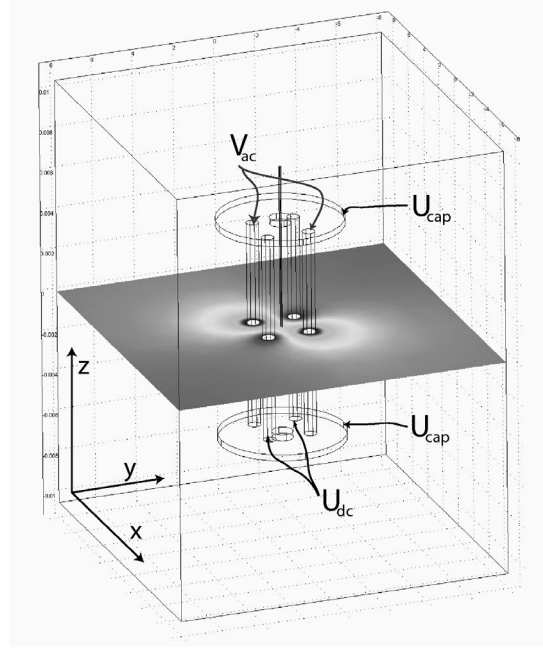


Figure 23.2. Four rod electrode arrangement with a numeric calculation of the electric field (bright: high positive field amplitude). For this example, the geometry of trap, shown in Fig. 23.1b is chosen. The trap axis is the symmetry axis in the vertical direction and is identified with the z -direction.

in the first half cycle of the rf-field, and vice versa for the second half. This property is well known from the quadrupole mass filter. Here, the confining of a charged particle works only in the (radial) x , and y -directions. See Fig. 23.2 for the potential in the (x, y) -plane in the first half cycle of the rf-field. With this, the particle is free in the axial direction (along the z -axis). If an additional dc-potential is applied in the z -direction, the particle is trapped radially and axially, and we may talk about a linear ion trap.

In order to realize a quantum register with trapped ions, a linear arrangement of the ions (i.e., ion strings) is advantageous. This geometry allows best individual observation, and individual coherent manipulation of an ion's quantum state.

23.2.1 Stability diagram of dynamic trapping

We focus here on the relevant case of a two-dimensional trap and discuss the parameter range for dynamic trapping. To confine the ions in 2D, we apply a rf-voltage $V_{ac} \cos(\Omega t)$ and an (optional) dc-voltage U_{dc} to the trap electrodes. Near the trap axis, see Fig. 23.2, for $x, y \ll r_0$, this creates a potential of the form

$$\Phi = \frac{U_{dc} + V_{ac} \cos(\Omega t)}{2r_0^2} (x^2 - y^2), \quad (23.1)$$

where r_0 denotes the distance between the trap axis and the surface of one of the electrodes. With an appropriately chosen frequency Ω , particles are trapped in the x - and y -directions.

The equations of motion resulting from (23.1) are given by the Mathieu equations,

$$\frac{d^2 u_x}{d\tau^2} + (a_x + 2q_x \cos(2\tau))u_x = 0, \quad (23.2)$$

$$\frac{d^2 u_y}{d\tau^2} + (a_y + 2q_y \cos(2\tau))u_y = 0, \quad (23.3)$$

where $a_x = -a_y = (4qU_{dc})/(m\Omega^2 r_0^2)$ and $q_x = -q_y = (2qV_{ac})/(m\Omega^2 r_0^2)$ with $\tau = \Omega t/2$. The general solution of Eqs. (23.2) and (23.3) can be described analytically as an infinite series of harmonics of the trap frequency Ω [30]. For the appropriate choice of parameters, the ion trajectory is confined in space and momentum: dynamical trapping occurs, see Fig. 23.3. If the conditions $a_i < q_i^2 \ll 1$, $i = x, y$ are fulfilled, an analytical approximate solution to the equations of motion can be given. It consists of a harmonic secular motion (macromotion) at frequencies ω_i with a superimposed micromotion at the trap's drive frequency Ω ,

$$u_i(t) = A_i \cos(\omega_i t + \varphi_i) \left[1 + \frac{q_i}{2} \cos(\Omega t) \right], \quad i = x, y.$$

The amplitude A_i and the phases φ_i depend on the initial conditions, and the secular frequencies are given by

$$\omega_i = \beta_i \frac{\Omega}{2}, \quad \beta_i \approx \left[a_i + \frac{q_i^2}{2} \right].$$

23.2.2 3D confinement in a linear Paul trap

Axial confinement is provided by an additional static potential U_{endcap} applied along the z -axis using additional axial electrodes of a ring or other shape (cf. Fig. 23.2). This creates a static harmonic well in the z -direction, which is characterized by the longitudinal trap frequency

$$\omega_z = \sqrt{2\kappa q U_{\text{endcap}} / m z_0^2}.$$

Here, z_0 is half the length between the axially confining electrodes, and κ is an empirically determined geometry factor of order unity which accounts for the specific electrode configuration. In principle, exact values of κ can be obtained either numerically or, in some cases, analytically. For the trap in Fig. 23.1c, the axial trap frequency $\omega_z/2\pi$ with $U_{\text{endcap}} = 2000$ V applied to the tips, and for the $^{40}\text{Ca}^+$ is 1.4 MHz. Under typical operation conditions, radial trap frequencies of 5 MHz are achieved.

The resulting potentials in all directions are harmonic and the motion of a trapped ion is very accurately described by a quantum harmonic oscillator with frequencies $\omega_{x,y,z}/2\pi$. It is a major advantage of linear traps that the radial and axial trap frequencies can be adjusted freely and independently by choosing the applied voltages. The micromotion completely vanishes for ions confined on the z -axis at $x = y = 0$. Further details of the calculation of the stability diagram for 3D linear traps are given in [37].

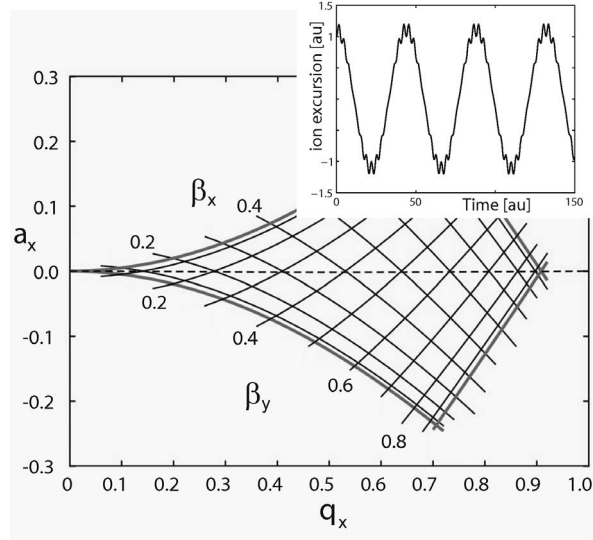


Figure 23.3. Stability diagram for a linear quadrupole configuration. Inside the red lines the ion trajectory is confined within the trap volume. A similar stability diagram exists for the y -direction. Inset: Ion trajectory as solution of the Mathieu equation plotted versus time with $a_x = 0$ and $q_x = 0.2$. The oscillation exhibits a slow macromotion at the frequency $\omega/2\pi$, superimposed the fast micromotion at the frequency $\Omega/2\pi$ of the rf-drive.

23.3 Ion crystals and their normal modes

In a linear trap, ions can be confined and optically cooled such that they form ordered structures [34, 38–40]. If the radial confinement along the x - and y -axis is strong compared to the axial confinement, with $\omega_z \ll \omega_{x,y}$, ions arrange themselves in a linear pattern along the trap axis at distances determined by the equilibrium of the Coulomb repulsion and the potential providing axial confinement. An example of a string of ions in a linear Paul trap is shown in Fig. 23.4. The average distance between two ions, in this case, is about $10 \mu\text{m}$. The exposure time for the CCD image of the ion fluorescence was 1 s, the resolution measured for the imaging system consisting of lens and CCD camera was better than $4 \mu\text{m}$.

23.3.1 Lagrangian of the ion motion in the trap

Consider N ions in a linear arrangement where the position of the n th ion is denoted by $\vec{x}_n = (x_{nx}, x_{ny}, x_{nz})$, see Fig. 23.5. The ions experience the trap potential and their mutual Coulomb repulsion. The total potential energy is given by

$$V = \frac{m}{2} \sum_{n=1}^N \sum_{j=x,y,z} \omega_j^2 x_{nj}^2 + \frac{q^2}{8\pi\epsilon_0} \sum_{n,m=1, m \neq n}^N \left\{ \sum_{j=x,y,z} (x_{nj} - x_{mj})^2 \right\}^{-\frac{1}{2}},$$



Figure 23.4. Linear crystal with ten $^{40}\text{Ca}^+$ ions imaged by a CCD system. The fluorescence light near 397 nm is observed while the ions are excited by laser light at 397 nm and 866 nm. The trap used for this experiment is shown in Fig. 23.1b.

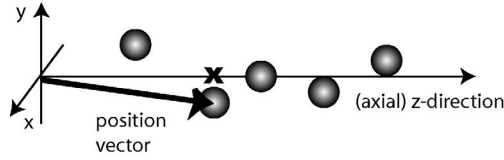


Figure 23.5. Illustration of the model for the linear crystal, position vector components (x_{nx}, x_{ny}, x_{nz}) for the n th ion, and its equilibrium position $(\bar{x}_{nx}, \bar{x}_{ny}, \bar{x}_{nz})$ as indicated by a cross (X).

where ω_z denotes the axial trap frequency and for simplicity both radial frequencies are assumed to be equal with $\omega_x = \omega_y = \omega_{x,y} = \omega_z / \sqrt{\gamma}$ and $\gamma \ll 1$ is a parameter that describes the anisotropy of the trap. We deduce the equilibrium positions of the ions in a linear crystal from the condition

$$\frac{\partial V}{\partial x_{nj}} = 0, \quad (23.4)$$

with $n = 0, 1 \dots N$ and, $j = x, y, z$. The values of equilibrium positions $\bar{x}_{nj}$ may be numerically determined and they can be described by a single parameter, the axial frequency ω_z [41, 42]. An analytic approximation for the minimum inter-ion distance in a string of N ions yields $\delta z_{\min} \cong 2 \cdot l \cdot N^{-0.57}$. It is convenient to use a dimensionless length scale where l

$$l = \left(\frac{e^2}{4\pi\epsilon_0 m \omega_z^2} \right)^{1/3}.$$

For example, at an axial frequency of $\omega_z/2\pi = 700$ kHz, the distance between two $^{40}\text{Ca}^+$ ions is 7.6 μm and shrinks to 6 μm in the case of three. Figure 23.6 shows the distances between neighboring ions in a linear crystal of 22 and 5 ions. Small oscillations of the ions about their equilibrium positions are denoted by $x_{ni}(t) = \bar{x}_{ni} + \xi_{ni}(t)$ and we will see that these motions are described in terms of *normal modes of the entire chain* vibrating at distinct

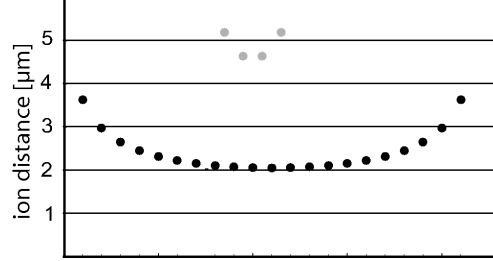


Figure 23.6. Inter-ion distances in a linear Ca^+ crystal of 22 ions (black dots) at an axial frequency of $\omega_z/2\pi = 700$ kHz. The distances vary between the minimum distance $2.05 \mu\text{m}$ and the maximum value of $3.64 \mu\text{m}$ for the outermost ions. The inter-ion distances are $5.18 \mu\text{m}$ and $4.63 \mu\text{m}$ in the case of 5 ions (grey dots).

frequencies [42, 43]. The Lagrangian describing the motion reads as:

$$L = T - V = \frac{m}{2} \sum_{n=1}^N \sum_{j=x,y,z} (\dot{\xi})_{nj}^2 - \frac{m}{2} \sum_{n=1}^N \sum_{j=x,y,z} \omega_i^2 (\bar{x}_{nj} + \xi_{nj}(t))^2 - \frac{q^2}{8\pi\epsilon_0} \sum_{n,m=1, n \neq m}^N \left\{ \sum_{j=x,y,z} [\bar{x}_{nj} + \xi_{nj}(t) - \bar{x}_{mj} - \xi_{mj}(t)]^2 \right\}^{-\frac{1}{2}}. \quad (23.5)$$

The first term describes the kinetic energy, the second the potential energy in the harmonic trap, and the third the mutual Coulomb interactions. A Taylor expansion with respect to the equilibrium positions converts the nonlinear Coulomb interaction into a linear spring constant, because higher order terms may be neglected [44]. The first row of Eq. (23.6) describes the motion along the (axial) z -axis only, while the second contains kinetic and potential energy in the (radial) x - and y -directions [45]:

$$L = \frac{m}{2} \left\{ \sum_{n=1}^N (\dot{\xi}_{nz})^2 - \omega_z^2 \sum_{m,n=1}^N \mathbf{A}_{mn} \xi_{mz} \xi_{nz} \right\} + \frac{m}{2} \sum_{j=x,y} \left\{ \sum_{n=1}^N (\dot{\xi}_{nj})^2 - \omega_{x,y}^2 \sum_{m,n=1}^N \mathbf{B}_{mn} \xi_{mj} \xi_{nj} \right\} \quad (23.6)$$

23.3.2 Eigenmodes

In the linearized model the eigenmodes and eigenvectors are found by a diagonalization of matrixes $\mathbf{A}$ and $\mathbf{B}$:

$$A_{mn} = \begin{cases} 1 + 2 \sum_{(p=1, p \neq m)}^N \frac{1}{|u_m - u_p|^3} & \text{if } m = n \\ -\frac{2}{|u_m - u_p|^3} & \text{if } m \neq n \end{cases} \quad (23.7)$$

$$B_{mn} = \left(\frac{1}{\alpha} + \frac{1}{2} \right) \delta_{mn} - \frac{1}{2} A_{mn},$$

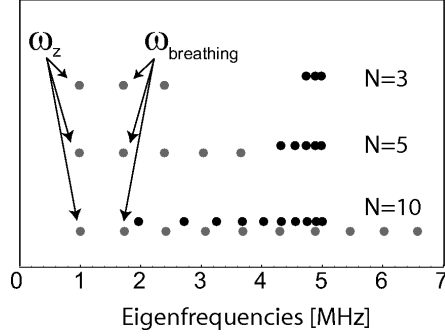


Figure 23.7. Eigenfrequencies of a $N = 3$, 5, and 10 ion crystal. Black: radial modes, grey: axial modes. The axial trap frequency $\omega_z/2\pi = 1$ MHz and the radial trap frequency $\omega_{(x,y)}/2\pi = 5$ MHz.

with the dimensionless equilibrium positions along the axial direction $u_n = \bar{x}_{n3}/l$. As an example, see Fig. 23.7 with the eigenfrequencies of a $N = 3, 5$, and 10 ion linear crystal. The figure shows that for a large number of ions the frequency differences become increasingly small. Thus, the selected quantum bus vibrational mode becomes less well separated from other modes which denotes a problem of scalability for the Cirac and Zoller 1995 quantum gate proposal (Section 23.6.1). The first axial normal mode ω_z corresponds to an oscillation of the entire chain of ions moving back and forth as if they were rigidly joined. This oscillation is also referred to as the *center-of-mass mode* (COM) of the string [42]. The second normal mode corresponds to an oscillation where the ions move in the opposite directions. More generally, this so-called *breathing mode* describes a string of N ions moving with an amplitude proportional to their mean distance from the trap center. The vibrational modes are quantized in the familiar way by introducing operators for momentum and position, together with the canonical commutation relations.

To sum up the most important results of the explicit calculation [42–44] of the normal modes (eigenmodes) and the respective eigenfrequencies of linear ion crystals: (i) Exactly N axial normal modes and normal frequencies exist. (ii) The center-of-mass mode has a frequency which is exactly equal to the frequency of a single ion. (iii) Higher order axial frequencies are almost independent of the ion number N , and are given by $\omega_z \cdot (1, 1.732, 2.412(8), 3.061(12), 3.681(22), 4.285(21), 4.874(20), \dots)$ where the numbers in brackets indicate the maximum frequency deviation as N increases from 1 to 10 ions.

Nonlinear coupling A calculation of the higher order terms of the Taylor expansion of Eq. (23.5), which have been neglected in the description so far, leads to the existence of inter-mode coupling: Vibrational quanta in one mode might undergo a decay into two quanta of other modes, mediated by a nonlinear phonon–phonon interaction [44]. Fortunately, the coupling coefficients are very small and mode mixing can be fully avoided for sufficiently small values of γ when the frequencies of x - and y - modes are much higher than those of the axial z -modes. In the following, we will therefore regard the vibrational modes of the ion crystal as stable harmonic oscillator eigenmodes.

23.4 Ion–light interaction

As the relevant theory is outlined in Chapter 22, we concentrate here on examples of carrier and sideband Rabi oscillations to demonstrate the Jaynes–Cummings dynamics given in equations (Chapter 22, Eqs. (22.4)–(22.8)). The interaction between two electronic levels $|g\rangle$ and $|e\rangle$ is driven by a light field, quantified in strength by its Rabi frequency Ω_{Rabi} and resulting in the Hamiltonian $H = (\hbar\Omega_{\text{Rabi}}/2)(|g\rangle\langle e| + |e\rangle\langle g|)$. If the laser frequency precisely fulfills the resonance condition for the bare electronic transition $\hbar\nu_{\text{laser}} = E_{|e\rangle} - E_{|g\rangle}$, the interaction is not changing the vibrational quantum number $|n\rangle$ (carrier transition) and is described by Chapter 22, Eq. (22.5). For a trapped particle, external vibrational modes can also be excited by the laser–ion interaction. The carrier Rabi frequency $\Omega_{\text{Carrier}} = \Omega_{\text{Rabi}}(1 - \eta^2(2n + 1)) \approx \Omega_{\text{Rabi}}$ remains almost unchanged for small values of the Lamb–Dicke factor¹ $\eta = k\sqrt{\hbar/2m\omega_z}$, where k denotes the k -vector of the light and n the phonon number of the vibrational mode.

However, if the laser excitation frequency is tuned to $\hbar\nu_{\text{laser}} = E_{|e\rangle} - E_{|g\rangle} - \hbar\omega_z$, at a detuning of $\delta_{\text{laser}} = -\omega_z/2\pi$ red with respect to the bare transition, we realize the Hamiltonian of the Jaynes–Cummings type Eq. (22.6) in Chapter 22. Now the sideband Rabi frequency is reduced to $\Omega_{\text{SB}} = \eta\Omega_{\text{Rabi}}\sqrt{n}$. Blue laser detuning, with $\delta_{\text{laser}} = +\omega_z/2\pi$ realizes the anti-Jaynes–Cummings Hamiltonian (22.7) in Chapter 22 with $\Omega_{\text{SB}} = \eta\Omega_{\text{Rabi}}\sqrt{n+1}$. For resolving the carrier and sideband transitions spectroscopically we require a narrow optical transition between long-lived electronic states $|e\rangle$ and $|g\rangle$.

In the experiment, one out of the vibrational modes is selected for the quantum bus mode. Criteria for this selection are a low-motion heating and decoherence rate, a large symmetry of eigenvectors, and the condition that no other mode is resonant in the close vicinity. For the experiments that illustrate the basic building blocks of quantum gates, a single ion is kept in a Paul trap and the center-of-mass mode at ω_z has been used. An experimental four-step-sequence is applied:

- (a) The ion is laser cooled to the ground state of vibration $|n = 0\rangle_{\text{com}}$.
- (b) The electronic state is initialized to the ground state $|g\rangle$ by optical pumping.
- (c) Laser light is applied with a fixed laser frequency, phase and intensity for a certain interaction time t . Thus, a superposition of electronic qubit basis states $\alpha|g\rangle + \beta|e\rangle$ is excited.
- (d) The upper state probability $|\beta|^2$ is revealed by electron shelving—exciting the ion by resonant light on a dipole transition and observing simultaneously the ion’s fluorescence. If the ion is measured in the ground state level g , fluorescence photons are observed, while the detection of no fluorescence means e .

Finally, the probability for upper state population $P_{|e\rangle}$ is revealed as the average of all measurement outcomes in the above sequence (a) to (d) for a large number of repetitions.

Figure 23.8a exemplifies single qubit (carrier) rotations denoted by $R(\theta, \phi)$ (definitions as in Chapter 22, Eq. (22.8)), where θ is varied by changing the product of pulse duration and Rabi frequency. ϕ is controlled by the phase of the laser field. The blue sideband Rabi oscillation is denoted by $R^+(\theta, \phi)$, and this operation is used to transfer the quantum information

¹The equation is modified by a prefactor $\cos(\beta)$ if the ion vibration and the $\vec{k}$ -vector include an angle β

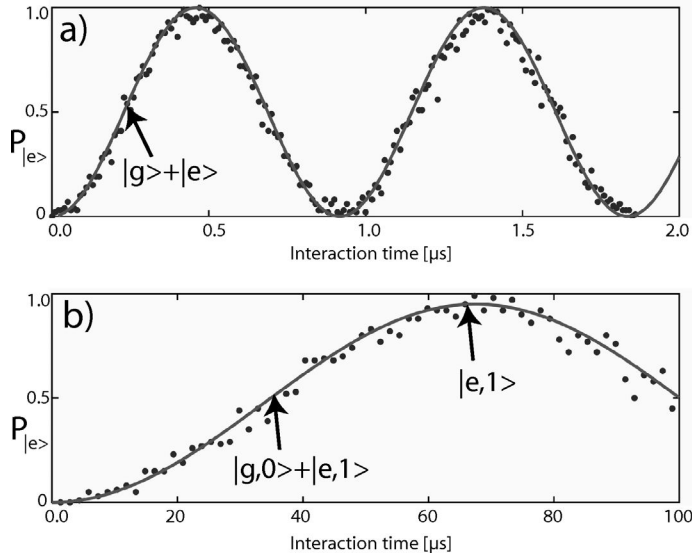


Figure 23.8. The $^{40}\text{Ca}^+ : S_{1/2}$ to $D_{5/2}$ qubit transition, see Fig. 23.9. We identify the $S_{1/2}$ state with $|g\rangle$ and the $D_{5/2}$ with $|e\rangle$. (a) Single ion Rabi oscillation on the carrier transitions. Starting from $|g, n=0\rangle$ at $t=0$ the state $|e, n=0\rangle$ is reached near $t \sim 0.5 \mu\text{s}$. After a $\theta = 2\pi$ rotation near $t \sim 0.9 \mu\text{s}$ the state $|-e, n=0\rangle$ is reached and only after a full $\theta = 4\pi$ rotation for $t \sim 1.8 \mu\text{s}$ we recover the initial quantum state $|g, n=0\rangle$. With 100 mW of laser power focused to a waist size of $30 \mu\text{m}$ a Rabi frequency of $\Omega_{\text{carrier}}/2\pi = 1.09 \text{ MHz}$ is reached. (b) Rabi oscillation on the blue sideband with a laser detuning $\delta = +\omega_z/2\pi$. The initial quantum state $|g, n=0\rangle$ evolves into a superposition $(|g, n=0\rangle + |e, n=1\rangle)/\sqrt{2}$ after an interaction time of about $40 \mu\text{s}$. The state $|e, n=1\rangle$ is reached for a π -pulse at about $t \sim 75 \mu\text{s}$. In situation (b) with 4 mW of the laser power the sideband was driven with $\Omega_{\text{sideband}}/2\pi = 7.4 \text{ kHz}$. The Rabi frequency of the sideband dynamics is slower by the Lamb–Dicke parameter η , here $\sim 4\%$, with respect to the carrier Rabi frequency. We observe a 95% perfect π -pulse [46].

out of the electronic degree of freedom into the vibrational quantum bus state, a SWAP operation. In the following section we discuss possible qubit candidates and the corresponding experimental realizations.

23.5 Levels and Transitions for Typical Qubit Candidates

Although an ion trap is deep and is capable of holding almost every kind of ion, only a few ions are favorable for QC experiments. Those ions should exhibit energy levels appropriate for the implementation of a two-level system with qubit levels $|g\rangle$ and $|e\rangle$ that show negligible decoherence by spontaneous decay, and the ion should also allow for optical cooling and efficient fluorescence detection. The “ideal ion” typically has one electron in the outermost

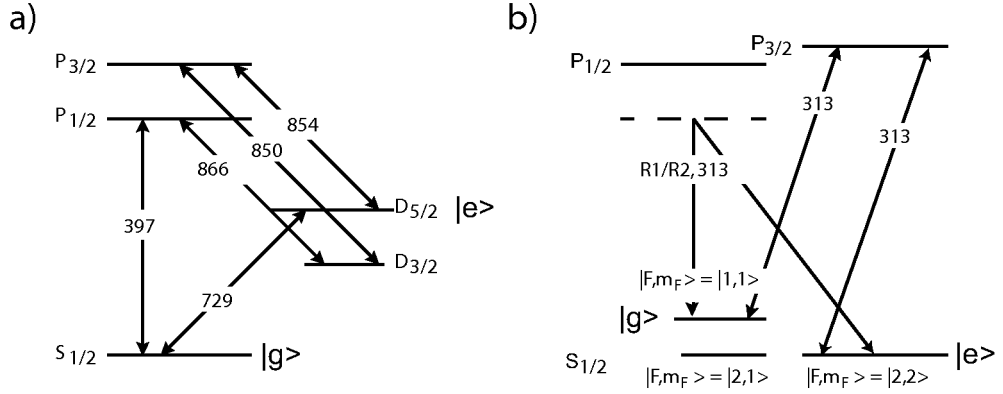


Figure 23.9. $^{40}\text{Ca}^+$ (left) and $^9\text{Be}^+$ (right) level scheme. The wavelengths of different transitions are indicated (in nm). For $^{40}\text{Ca}^+$, the lifetimes of the ion in the excited state $D_{5/2}$ is ~ 1.2 s. A laser near 729 nm serves to drive the qubit transition. In $^9\text{Be}^+$, two Raman laser beams R1 and R2 near 313 nm are used for coherent manipulation of the qubit.

shell (hydrogenic ion) and a correspondingly simple electronic level structure. The two-level system can either be provided by two hyperfine ground states, by Zeeman sublevels or by a long-lived metastable electronic state. The following discussion concentrates on $^9\text{Be}^+$, where hyperfine ground states form the two-level system, and on $^{40}\text{Ca}^+$, where the ground state and an optically excited metastable level is used. The level schemes of $^{40}\text{Ca}^+$ and $^9\text{Be}^+$ are shown in Fig. 23.9. Current activities also use the hyperfine ground states of $^{171}\text{Yb}^+$, $^{24}\text{Mg}^+$, the isotope $^{43}\text{Ca}^+$ and $^{111}\text{Cd}^+$. Qubit manipulations by Raman transitions have the advantage that both light fields R1 and R2 may be derived from one single laser source such that the differential phase fluctuations of both Raman beams can be kept very small with moderate experimental effort. If the detuning of the Raman beams from the resonance is chosen large enough, spontaneous emission from the $P_{3/2}$ and $P_{1/2}$ is largely suppressed and the coherence of the qubits is not affected [47].

23.6 Various Two-Qubit Gates

23.6.1 The Cirac and Zoller scheme 1995

A quantum gate between the internal states $\{|g\rangle, |e\rangle\}$ of any pair of ions m and n in a linear string is achieved by three successive laser pulses, addressing the m th, then the n th, and finally again the m th ion [9] (Chapter 22, Eq. (22.9)). In the original proposal, the first and last pulse are driven with a light field of orthogonal polarization with respect to the second pulse, and the second pulse is exciting an auxiliary transition. The gate operation relies on the initialization of the ion crystal in the vibrational ground state of the quantum bus mode $|n = 0\rangle$ [20, 48–50] of the quantum bus vibrational mode and individual optical addressing of

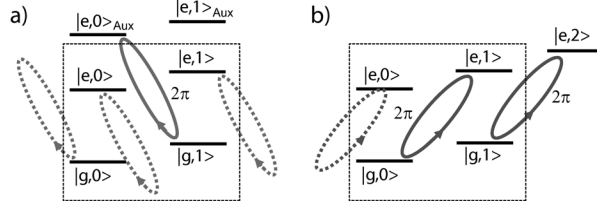


Figure 23.10. (a) Qubit level scheme and Cirac and Zoller gate 1995: A red sideband 2π -pulse on the auxiliary transition is driven and the state $|g, n = 1\rangle$ acquires a phase factor of -1 . Ellipses indicate Rabi cycles (dashed: no resonant level is available and thus no evolution is possible, solid: 2π -evolution). (b) Composite phase gate [53]. A blue sideband 2π -pulse is driven and all states acquire a phase factor of -1 except the state $|e, n = 0\rangle$. A dashed box indicates the set of computational basis states.

ions [36, 51]—technically very demanding requirements. The *beauty of this gate operation*, however, is the clear flow of quantum information in three consecutive steps:

- A first SWAP from electronic state to common vibrational state, applied to the control ion and writing the information into the vibrational mode, followed by
- A phase gate, or a controlled-NOT gate, on the target ion, conditioned upon the vibration quantum state, (see Fig. 23.10a) and finally
- A SWAP back from the common mode of vibration to the control ion's electronic state in order to leave the control qubit's quantum state unchanged.

23.6.2 Experimental realization of the Cirac and Zoller gate

Phase gate and composite laser pulses As the SWAP operations are simple $R^+(\theta = \pi, \phi)$ pulses, let us explain the central operation (step b) that is the conditional rotation of the target ion. Defining the computational subspace by $(|e, 0\rangle, |e, 1\rangle, |g, 0\rangle, |g, 1\rangle)$, this gate can be described by a diagonal matrix with the entries $(-1, 1, 1, 1)$. Unlike the original proposal which requires a 2π -rotation on an auxiliary transition, the experiment [36, 54] uses a blue-sideband excitation leading to pairwise coupling between levels $|g, n\rangle \leftrightarrow |e, n + 1\rangle$ except for the level $|e, 0\rangle$, see Fig. 23.10b.

For the phase gate we perform an *effective 2π -pulse* on the two two-level systems $(|g, 0\rangle \leftrightarrow |e, 1\rangle)$ and $(|g, 1\rangle \leftrightarrow |e, 2\rangle)$ which changes the sign of all computational basis states except for $|e, 0\rangle$ [52]. Since the Rabi frequency depends on n , we need a composite-pulse sequence [53] instead of a single blue sideband pulse. Up to an overall phase factor, this transformation yields the desired phase gate. The sequence is composed of four sideband pulses and can be described by

$$R_{\text{phase}} = R_4^+(\pi\sqrt{n+1}, 0) R_3^+(\pi\sqrt{\frac{n+1}{2}}, 0) R_2^+(\pi\sqrt{n+1}, 0) R_1^+(\pi\sqrt{\frac{n+1}{2}}, \pi/2).$$

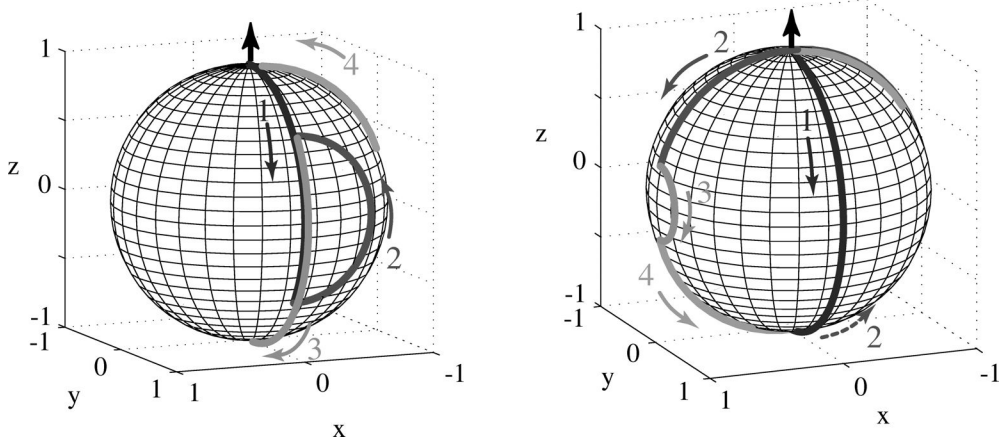


Figure 23.11. Bloch sphere trajectories for the composite phase gate, R_{phase} . Left: Bloch sphere for the quasi-two-level-system $|g, 0\rangle \leftrightarrow |e, 1\rangle$. The initial state is $|g, 0\rangle$, indicated by the black arrow. Pulse R_1^+ of the sequence rotates the state vector about the x -axis by $\pi/\sqrt{2}$. R_2^+ accomplishes a π -rotation about the y -axis. It therefore transforms the state to its mirror image about the x - y -plane. Consequently, R_3^+ rotates the state vector all the way down to the bottom of the sphere. R_4^+ represents a π -rotation about the y -axis. The final state is identical to the initial one, except the acquired phase factor -1 . Right: The same laser pulse sequence acting in the $|g, 1\rangle \leftrightarrow |e, 2\rangle$ subspace. Again, the final state is identical to the initial one, except the acquired phase factor -1 .

For an intuitive picture of R_{phase} we plot the evolution of the Bloch vector in Fig. 23.11.² This phase gate is transformed into a controlled-NOT operation if sandwiched in between two $\pi/2$ -carrier pulses on the target ion, $R_{\text{CNOT}} = R(\pi/2, 0) R_{\text{phase}} R(\pi/2, \pi)$.

Two-ion universal gate We realize this gate operation [36, 54] with a sequence of laser pulses. A blue sideband π -pulse, $R^+(\pi, 0)$, on the control ion transfers its quantum state to the bus mode. Then we apply the controlled-NOT operation R_{CNOT} to the target ion. Finally, the bus mode and the control ion are reset to their initial states by another π -pulse $R^+(\pi, \pi)$ on the blue sideband. We apply the gate to all computational basis states and follow their temporal evolution, see Fig. 23.12. The output of the gate reaches a fidelity³ of 0.71 ± 0.03 [36, 54]. If the qubits are initialized in the superposition state $|\text{control}, \text{target}\rangle = |g+e, g\rangle$, the controlled-NOT operation generates an entangled state $(|g, g\rangle + |e, e\rangle)/\sqrt{2}$.

23.6.3 The Sørensen and Mølmer scheme

Sørensen and Mølmer [55]–[57], and in a different formulation Milburn *et al.* [58], proposed a scheme for “hot” quantum gates. For successful operation it requires not the cooling to

²The Bloch vector picture does not allow to indicate the phase factor -1

³We use the overlap between ideal $|\Phi_{\text{ideal}}\rangle$ and experimentally obtained state $|\Phi_{\text{exp.}}\rangle$ for the fidelity $F = |\langle \Phi_{\text{ideal}} | \Phi_{\text{exp.}} \rangle|^2$

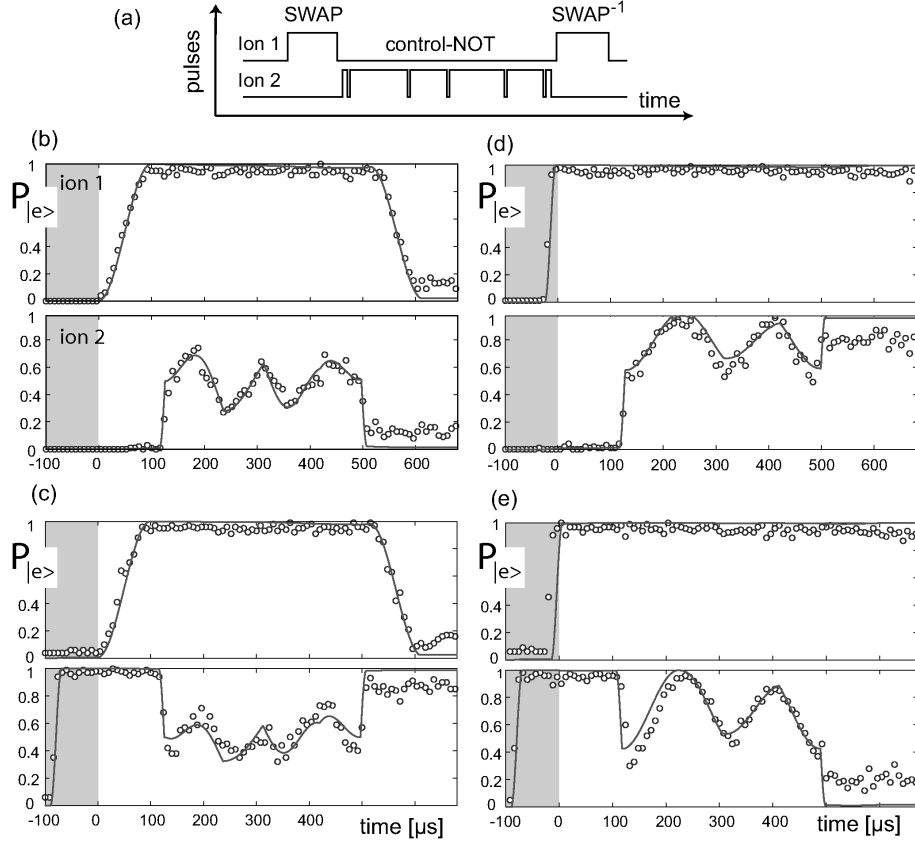


Figure 23.12. State evolution of both qubits $|\text{control}, \text{target}\rangle = |\text{ion 1}, \text{ion 2}\rangle$ under the controlled-NOT operation. For this, the pulse sequence (a) is truncated as a function of time and the $|e\rangle$ state probability $P_{|e\rangle}$ is measured ((b)–(e)). The solid lines indicate the theoretically expected behavior. Input parameters for the calculation are the independently measured Rabi frequencies on the carrier and sideband transitions and the addressing error. The initial state preparation is indicated by the shaded area and drawn in all figures for negative time values. The actual gate pulse sequence starts at $t=0$. After mapping the first ion’s state (control qubit) with a SWAP π -pulse of length $95\ \mu\text{s}$ to the bus mode, the single-ion controlled-NOT sequence (consisting of six concatenated pulses) is applied to the second ion (target qubit) for a total time of $380\ \mu\text{s}$. Finally, the control qubit (first ion) is reset by the SWAP⁻¹ to its original value with the concluding π -pulse [36].

the vibrational ground state but only the cooling of the ion crystal deep into the Lamb–Dicke regime, such that $\eta\sqrt{1 + \bar{n}_{\text{therm}}} \ll 1$, where $\bar{n}_{\text{therm}}$ is the mean thermal phonon number and η the Lamb–Dicke factor. The authors assume an even number $2N$ of ions which are equally illuminated by a *bichromatic* laser field with laser frequencies of opposite detunings close to

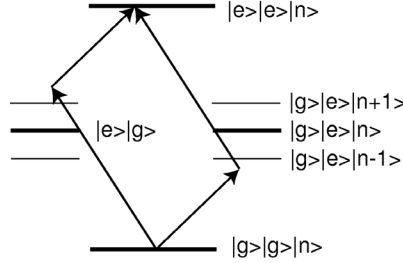


Figure 23.13. Level scheme for the Sørensen and Mølmer gate operation.

the sideband frequency $\omega_{\text{laser}} = \omega_{ge} \pm (\omega_z - \delta)$ (see Fig. 23.13). The initially prepared state $|g, g, n\rangle$ undergoes a sinusoidal Rabi oscillation to $|e, e, n\rangle$ with a modified Rabi frequency Ω_{SM} . In the weak excitation regime, with $\eta\Omega_{\text{Rabi}} \ll \omega_z - \delta$, intermediate levels with vibrational numbers other than n , namely $|g, e, n-1\rangle$ and $|e, g, n+1\rangle$, are not occupied. The modified Rabi frequency reads $\Omega_{\text{SM}} = -(\Omega_{\text{Rabi}}\eta)^2/2(\omega_z - \delta)$. It appears that the ions *only* absorb photons simultaneously from the bichromatic laser field as the ions share the same vibrational mode. While the absorption of a single photon is suppressed due to the frequency mismatch δ , the coupling of the ions to the common vibration mode allows a mutual compensation of this frequency mismatch $\pm\delta$. As a consequence, the Sørensen and Mølmer scheme works with any even number of ions in a string. If the Rabi type evolution is stopped midway, one has generated an entangled state of the electronic components of the ions only, and the vibrational quantum number $|n\rangle$ factorizes out, resulting in a transformation.

$$|g, g, n\rangle \rightarrow \frac{1}{\sqrt{2}} \{ |g, g\rangle - i |e, e\rangle \} |n\rangle. \quad (23.8)$$

The two ions are in an entangled state after the laser pulse. However, to fulfill the weak excitation regime, the Rabi frequency has to be significantly reduced, and the entanglement evolution with Ω_{SM} becomes quite slow, thus leading to an impractically long duration of typically a few ms for the entanglement operation. The corresponding result is displayed in Fig. 23.14 as a calculation of the dynamics of two density matrix elements $\rho_{gg}(t)$ and $\rho_{ee}(t)$ according to [57].

The scheme was significantly improved shortly afterwards, when Sørensen and Mølmer realized that the gate operation could also be driven much faster. However, with faster evo-

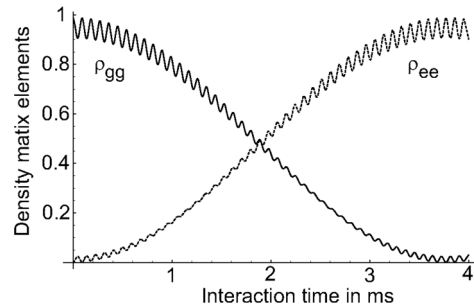


Figure 23.14. Simulation of the evolution of the density matrix elements ρ_{gg} (solid line) and ρ_{ee} (dashed) for two ions when the $^{40}\text{Ca}^+ : S_{1/2} - D_{5/2}$ transition is driven with a bichromatic laser field. Parameters are $\omega_z/2\pi = 700$ kHz, $\delta = 630$ kHz (from the carrier transition), $\Omega_{\text{Rabi}} = 70$ kHz, mean thermal number of 2, and $\eta = 10.9\%$. After an interaction time of 1.88 ms, the entangled state (23.8) is generated.

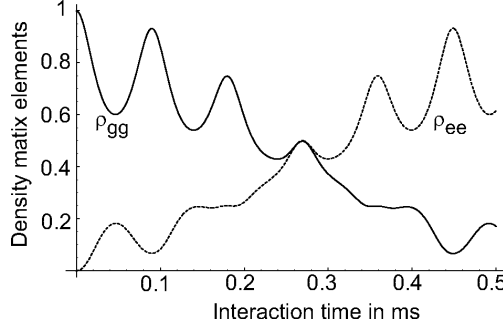


Figure 23.15. Simulation of the evolution of the density matrix elements ρ_{0000} (solid line) and ρ_{1111} (dashed) for two ions. The parameters are similar to Fig. 23.14 but the laser intensity is increased by a factor 7 to reach a Rabi frequency of $\Omega_{\text{Rabi}} = 185.5$ kHz (resulting in $k = 3$). In contrast to the situation in Fig. 23.14 it takes only 0.27 ms to generate the entangled state.

lution of ρ_{gg} and ρ_{ee} and a larger Ω_{SM} , intermediate levels with vibrational numbers $|n \pm 1\rangle$ are occupied, and in general the vibrational quantum number no longer factorizes out at the end of the evolution. The internal electronic states are therefore strongly entangled with the vibration in the course of the gate. For a successful gate operation we have to make sure that the vibrational state $|n\rangle$ returns back to the initial state at the end of the gate operation. This corresponds to a closed circle in the phase space of the ion's external degrees of freedom, momentum and position. As shown in [56, 57], the interaction time τ has to be adjusted in accordance with $\tau = \pi\sqrt{k}/\eta\Omega_{\text{Rabi}}$ with $k = 1, 2, 3, \dots$. See Fig. 23.15 for a numerical simulation of a fast two ion entanglement. Compared to the simulation in Fig. 23.14, the Rabi frequency Ω_{Rabi} is increased by 2.65 which allows the generation of an entangled state after 0.27 ms. Effects that limit the gate fidelity are discussed in [57].

The fast Sørensen and Mølmer entanglement operation was realized in the case of two $^9\text{Be}^+$ ions with a fidelity of $F = 83 \pm 1\%$ and for four ions with $F = 57 \pm 2\%$ [22]. The small mass of the $^9\text{Be}^+$ ion and the high recoil due to the Raman transition (two-photon interaction) in the UV at 313 nm are helpful for the Sørensen and Mølmer scheme: A resulting relatively high η of $0.23\text{ N}^{-1/2}$ even at a high trap frequency of 8.8 MHz speed up the operation.

23.6.4 The Jonathan, Plenio, and Knight scheme

A gate scheme proposed by Jonathan, Plenio, and Knight operates at a high laser intensity [59]: The ion string has to be cooled to the vibrational ground state prior to the gate laser pulses (cold gate). The laser frequency is chosen to be resonant with the carrier transition, and the laser intensity is increased such that the light-induced dressed states $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ are split by $2\Omega_{\text{Rabi}}$ (dynamic or ac-Stark effect). If now the laser intensity is chosen *exactly* such that $2\Omega_{\text{Rabi}}$ equals the trap frequency ω_z , the two dressed levels $|+, 0\rangle$ and $|-, 1\rangle$ with different vibration quantum number n , will become degenerate and we expect an exchange between them. As a result, the internal and vibrational states couple, which is used for the implementation of a two-bit gate. As in the other gate types, the above interaction is enclosed by several pulses to complete the controlled-NOT gate [59]. The authors point out that this quantum gate is fast and still maintains high fidelity if the laser intensity is carefully stabilized. Further calculations show that this gate can operate even at residual thermal phonon numbers [60].

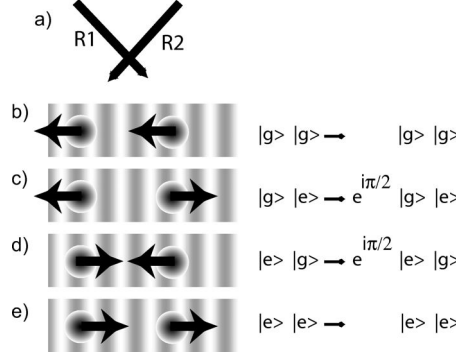


Figure 23.16. (a) Raman beam geometry: Laser beams R1 and R2 cross under an angle such that a standing wave pattern is formed. The resulting dipolar light forces onto two ion crystal for exciting the breathing mode are sketched at the left side for all computational basis states $|ion1\rangle|ion2\rangle$, from (b) to (e). For this illustration, I assume for simplicity that a force to the left-hand side acts on an ion in the state $|g\rangle$ to the right. The action of this force during the gate time results in quantum logic operations (right side). See text for details.

The gate scheme seems to be well within experimental reach, because high Rabi frequencies even with $\Omega_{\text{Rabi}} > \omega_z$ have been observed. The regime of strong excitation is reached at a modest laser power because of the tightly focused laser beam. However, no experimental attempts for the gate operation have been carried out so far.

23.6.5 Geometric phase shift gates

Holonomic quantum computing has been discussed in Chapter 21, and a proposal for single- and two-qubit phase gates exists in the case of trapped ions [61]. For the gate, a cyclic path in the phase space of the ion's external degrees is closed by an adiabatic variation of control parameters, and the enclosed area results in a Berry phase. Thus, the gate operation should be robust, because small variations of the actual path from the desired one do alter the geometric quantum phase to first order. For a discussion of the proposals by Poyatos *et al.* [62] and the kick-force proposal by Ripol *et al.* [63] I refer to Chapter 22, Eq. (22.6). Both proposals utilize geometric phases.

Geometric σ_z phase gate realization Experimentally, a geometric two-ion phase gate has been realized by the NIST Boulder group [64, 65]. Two $^9\text{Be}^+$ ions are held in a linear trap and are excited (see Fig. 23.9) by Raman beams under 45° such that the resulting difference vector $\Delta\vec{k}$ points along the axial direction [64]. Up to a small detuning δ , the frequency difference of both Raman beams is set to coincide with the breathing mode frequency $\omega_{\text{breathing}}$. This way, a standing wave along the axial direction is generated (see Fig. 23.16) which is moving to one side. If the inter-ion distance d is now chosen to fulfill the relation $\Delta k d = 2\pi n$, with $n = 1, 2, \dots$, the light field at the positions of both ions is identical. As the Raman wave acts nonresonantly via an ac-Stark shift, a dipolar force is applied to the ions. By a proper combination of polarizations and frequencies of both Raman light fields R1 and R2, the resulting force on the ions *depends* on the internal quantum state $|g\rangle$ or $|e\rangle$: forces act with equal magnitude but in the opposite direction. Therefore, when the ions are in the same internal state, the force driving each ion will be same and *no differential force* arises. Hence, the motion of the breathing mode, see Section 23.3.2, with its counter-propagating ion oscillation is not excited. On the other hand, if the ions are in different internal states a differential force exists between them, exciting this mode.

For a geometric phase the cyclic path in momentum-position phase space has to be adjusted such that the enclosed area corresponds to a differential phase of $\pi/2$. As the difference frequency of both Raman beams is chosen not to coincide exactly with the breathing mode frequency, but is off by a small frequency difference δ , the breathing mode oscillation is excited and later refocused after a time $T = 2\pi/\delta$ precisely adjustable by δ . This is analogous to a classical pendulum which is excited slightly off its eigenresonance. Its oscillation is initially growing, and the phase difference between external drive and pendulum eigenfrequency accumulates such that it is slowed down again. As a consequence the phase space diagram is a closed circle.

The gate operation does not require ground state cooling. Curves in the phase diagram close regardless of their initial vibrational quantum states (if fulfilling the Lamb–Dicke regime). The gate speed—different to Cirac and Zoller 1995—is not limited by off-resonant carrier excitations [46] which allows to perform the gate operation quickly (in the experiment 39 μ s). The measured gate fidelity of 0.97 ± 0.02 was limited in the experiment mainly by the spontaneous decay from the $P_{1/2}$ and the $P_{3/2}$ states of $^9\text{Be}^+$ [64]. Qubit operations using ions with a large fine structure splitting [66], as in the case of $^{43}\text{Ca}^+$ or $^{111}\text{Cd}^+$ may help to reduce this error source.

σ_ϕ phase insensitive qubit dynamics Recently, dipole forces have been investigated for different configurations of the Raman beams [67]. The authors re-interpret the Sørensen and Mølmer scheme as a σ_ϕ , finding that its operation is equivalent to the σ_z phase gate in a rotated basis. They analyze the susceptibility of the gate operation if the phase relationship between both Raman light beams is not strictly maintained but fluctuating as in every experimental situation. If the Sørensen and Mølmer scheme is slightly modified phase fluctuations from the optical driving field of both Raman beams cancel out. This should allow to maintain the phase coherence of qubits and to perform gate sequences beyond the coherence time of the optical field. Experiments with a single $^{111}\text{Cd}^+$ ion prove this principle [67].

ac-Stark shift gate Note that also a vibrational-state dependent light shift on an optical (quadrupole) transition has been used for gate operations [68]. Since the sideband Rabi frequency on the blue sideband reads as $\Omega_{\text{SB}} \sim \sqrt{1+n}$, the corresponding ac-light shift of a laser field which is detuned from resonance by Δ is proportional to $\Omega_{\text{SB}}^2/\Delta \sim (n+1)/\Delta$ [69], depending linearly on the vibrational quantum number $|n\rangle$ (see Fig. 23.17).

In order to realize a phase gate operation, we fix an interaction time T so that the phase shift for states with $|n = 1\rangle$ yields precisely $\pi/2$. This accomplishes a quantum gate in the two-qubit computational space composed by the states $|g, 0\rangle$, $|e, 0\rangle$, $|g, 1\rangle$ and $|e, 1\rangle$: The states $|g, 1\rangle$ and $|e, 1\rangle$ acquire phases of $e^{\pm i\pi/2} = \pm i$, respectively, while $|g, 0\rangle$ and $|e, 0\rangle$ do not acquire any phase. This phase gate operation may be converted into a controlled-NOT gate by the application of appropriate single qubit rotations. In the experiment we find transfer efficiencies with a fidelity of 0.81 ± 0.02 . Numerical simulations show that this gate may be used advantageously for the generation of multi-ion GHZ states $\{|gg\dots gg\rangle + |ee\dots ee\rangle\}/\sqrt{N}$ in a simple and efficient way [68].

23.6.6 The Mintert and Wunderlich gate proposal

For the excitation of the vibrational bus mode, in the case of the Cirac and Zoller 1995 gate, and equally for the applications of light forces in geometric quantum gates, laser light transports energy and momentum. The Lamb–Dicke parameter $\eta = k\sqrt{\hbar/2m\omega_z}$ governs the dynamics of momentum transfer to the ion crystal. In the case of microwave transitions, with almost vanishing values of k and η , we expect no direct momentum transfer, thus no coupling to vibrational modes, and no two-qubit gates to be possible. However, if a magnetic field gradient is applied along the linear crystal of ions, the situation is modified: Ions may be transferred by a microwave pulse from low-field seekers to high-field seekers, and spatially re-arrange themselves to find minimum positions of the total potential (see Eq. (23.4)). As ions move to find the optimum position, their motion is transferred by the Coulomb interaction to all other ions in the crystal, and common modes of vibration may be excited [70]. The second advantage of a high magnetic field gradient is that ions may be addressed by tuning to the position dependent frequency: addressing in frequency space.

With a coupling to common vibrational modes and a scheme for individual addressing in hands, most of the above gate schemes are in reach. The main advantage of this microwave-based approach is the high frequency stability and flexible programmability of commercial rf-sources. Commercial nuclear magnetic resonance (NMR) pulse generators fulfill the required specifications.

23.6.7 Gate proposals based on the interaction of ions with a common optical mode

In the framework of cavity-QED a large number of gate proposals exists. The asset of trapped ions compared to the situation of a neutral atom inside an optical cavity is the localization

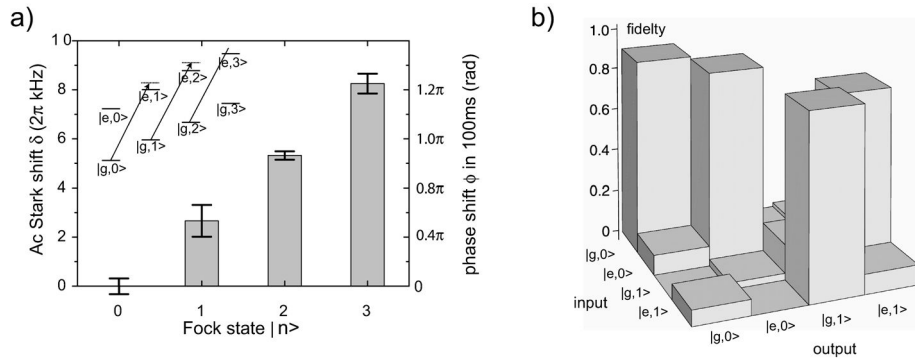


Figure 23.17. (a) The measured phase shift acquired due to the off-resonant laser interaction depends linearly on the vibrational quantum state. We find $\delta_{\text{res}}/2\pi = 2.71(6)$ kHz per phonon if the phase shifting laser is detuned from the blue axial sideband by $\Delta = 60$ kHz. Inset: relevant qubit energy levels. (b) Experimentally obtained truth table for the gate operation. The vibrational state $|n\rangle$ controls the electronic state and a fidelity of 0.81 ± 0.02 is reached.

within a small fraction of the wavelength [71]–[74]. However, experiments with a single ion inside a cavity are still hampered by the relatively weak coupling constant $g/2\pi$. A miniaturization of ion traps, together with a miniaturization of the optical cavity, will help to reduce the mode volume and to increase the coupling. For further reading we refer to Chapter 28.

23.7 Teleportation

In 2004, more than a decade after the proposal [75], deterministic quantum teleportation with matter has been demonstrated in two different laboratories [76, 77]. For the teleportation with light we refer the reader to Chapter 14. The quantum teleportation algorithm for a qubit $|\psi_{\text{Alice}}\rangle = |\psi_1\rangle = \alpha|g\rangle_1 + \beta|e\rangle_1$ from Alice to Bob is based on five consecutive steps:

- (a) An entangled pair of qubits $|\Psi^+\rangle_{2,3} = \frac{1}{\sqrt{2}}(|g\rangle_2|e\rangle_3 + |e\rangle_2|g\rangle_3)$ is created and distributed, the particle with index 2 to Alice's and the other one to Bob's side.

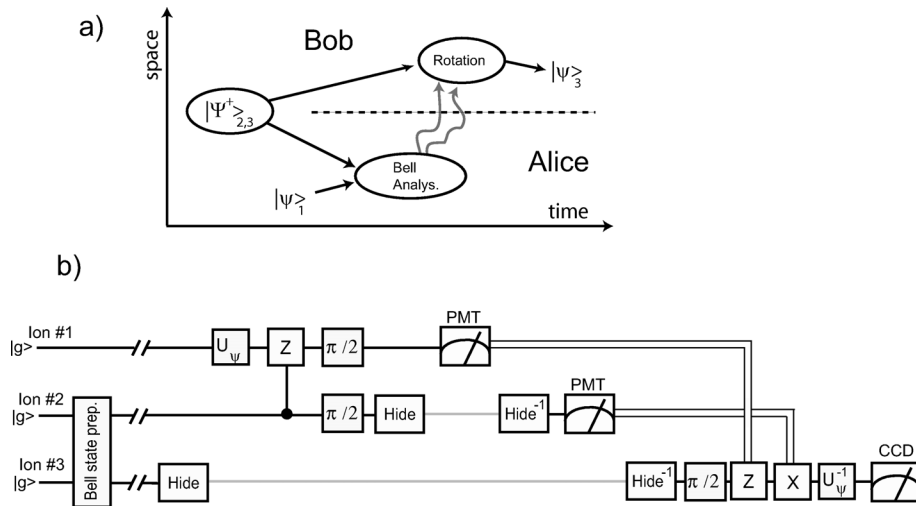


Figure 23.18. a) Space–time diagram of the quantum teleportation algorithm. A Bell state is distributed among Alice (lower part of Figure) and Bob. Alice transmits the outcome of her Bell analysis to Bob who recovers the original quantum state. (b) Protocol for teleportation from ion #1 to ion #3: Initially, a Bell state of ions #2 and #3 is prepared. The state $|\psi\rangle$ is encoded in ion #1. The Bell state analyzer consists of a controlled Z -gate followed by $\pi/2$ rotations and a state detection of ions #1 and #2. Note that this implementation uses a Bell basis rotated by $\pi/4$ with respect to the standard notation. Therefore, a $\pi/2$ rotation on ion #3 is required prior to the reconstruction operations Z and X . Grey lines indicate qubits which are protected against light scattering. Ions #1 and #2 are detected by observing their fluorescence on a PMT. Only upon a detection event $|g\rangle$ the corresponding reconstruction operation is applied to ion #3. Classical information is represented by double lines. For the fidelity analysis we apply U^{-1} and measure the quantum state of ion #3.

- (b) Alice is given an unknown quantum state in the form of a single qubit $|\psi_1\rangle$ which is to be teleported. The overall quantum state of the three-qubit system reads as the direct product $|\phi_{1,2,3}\rangle = |\psi_1\rangle \frac{1}{\sqrt{2}}(|g\rangle_2|e\rangle_3 + |e\rangle_2|g\rangle_3)$.
- (c) The overall quantum state can be written as a sum of four terms

$$|\phi_{1,2,3}\rangle = \frac{1}{2}(|\Psi^+\rangle_{1,2} |\psi\rangle_3 + |\Psi^-\rangle_{1,2} \sigma_z |\psi\rangle_3 + |\Phi^+\rangle_{1,2} \sigma_x |\psi\rangle_3 + |\Phi^-\rangle_{1,2} (-i\sigma_y) |\psi\rangle_3), \quad (23.9)$$

where the four Bell states are denoted by $|\Psi^\pm\rangle_{1,2} = \frac{1}{\sqrt{2}}(|g\rangle_1|e\rangle_2 \pm |e\rangle_1|g\rangle_2)$ and $|\Phi^\pm\rangle_{1,2} = \frac{1}{\sqrt{2}}(|g\rangle_1|g\rangle_2 \pm |e\rangle_1|e\rangle_2)$. The Pauli matrices σ describe rotations of the third qubit, see e.g. Sect. 3.2.1 for their definition. Alice performs a measurement in the Bell basis on both her qubits, particle 1 and 2. Thus, she projects her particles of $|\phi_{1,2,3}\rangle$ into one of the possible Bell states, each with 1/4 probability outcome. If Alice's measurement result is Ψ^+ , Bob's qubit is already in the desired quantum state $|\psi\rangle_3$. If she finds a different outcome, for e.g., Φ^+ , Bob has recovered the quantum state $|\psi\rangle_3$ up to a single qubit rotation σ_x in his particle with index 3.

- (d) Therefore, Alice sends the outcome of her measurement, two bits of classical information to Bob, such that
- (e) Bob is able to perform the correct single qubit rotation on his particle to obtain back the original state $|\psi\rangle_3$. Note that no quantum information is duplicated but that the entire information about the state $|\psi\rangle_1$ has fully disappeared at Alice's side.

The protocol, see Fig. 23.18b, has been realized [76] with three ions held in the linear trap shown in Fig. 23.1c. The quantum algorithms consist of more than 30 laser pulses. The outcome of the deterministic teleportation is revealed by inverse reconstruction and shows a fidelity of 75% [76]. This result has been improved to about 85% fidelity [78] and the analysis of the algorithm has been completed by applying process tomography on the teleported output state [10, 79–81].

Teleportation with a fidelity of 78% were obtained with three ions held in a linear segmented ion trap (NIST Ion Storage Group, Boulder, USA [65]). Control voltages allow to shuttle single ions or to separate single ions from a linear crystal. In this experiment, a fidelity of 78% was demonstrated [77]. For quantum gate operations among two ions, for single qubit rotations, and for the readout of single qubits without projecting the other qubits, the required ions are singled out from the linear crystal, and transported into a processor section of the ion trap where the laser–ion interaction is performed. Thus, quantum teleportation has become the first algorithm to demonstrate the assets of segmented and miniaturized Paul traps.

23.8 Segmented Traps and Future Directions

Novel fabrication methods allow to fabricate segmented traps with μm dimensions. The sketch of the two-layer geometry is shown in Fig. 23.19. Gold-coated-ceramic wafers are structured, either by laser ablation or by conventional etching techniques, and two trap chips are assembled. Figure 23.20 shows the laser fabricated ion chip. The use of fs-laser pulses improves

significantly the quality of cuts. In a second approach, semiconductor material is structured and the entire three-dimensional trapping device is thus fabricated in one step [82]. The dimensions range for a wafer spacing of 400 to 200 μm , and in the case of semiconductor-based two-layer devices down to about 5 μm . The slit width ranges from 400 down to 50 μm .

Next steps of the trap development are the investigation of planar trap geometries [83–85], **Y**- or **X**-track switches [86, 87] which direct ions into a central processor unit, or into storage segments. This development is a further step towards a scalable ion-based QC [88]. The transport of ions in segmented devices [89, 90] maintains the qubit coherence which has been proven by a Ramsey testing scheme [91]. The same holds for the splitting operation, which is essential for a successful teleportation algorithm [77]. Second, the miniaturization of ion traps will necessarily lead to a coupling of surfaces [92], or micromechanical oscillators [93, 94], with the single ion. A well controlled quantum system is then interfaced with a semiclassical system. This opens a whole field of future theoretical and experimental research [95]. A discussion of the limits of miniaturization of dynamic traps takes into account the maximum electric field strength that may be applied to the rf-electrodes avoiding electrical breakdown. The estimation [84] indicates that for trap sizes of the order of 10 nm the pseudo-potential could exhibit GHz secular frequencies, but the trap depth will decrease such that the trap would

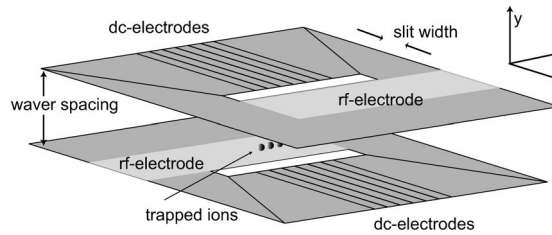


Figure 23.19. Dual layer linear ion trap. A trap is constructed by a stack of two wafers (not to scale). Ions are transported along the z -axis by controlling the dc-electrode voltages.

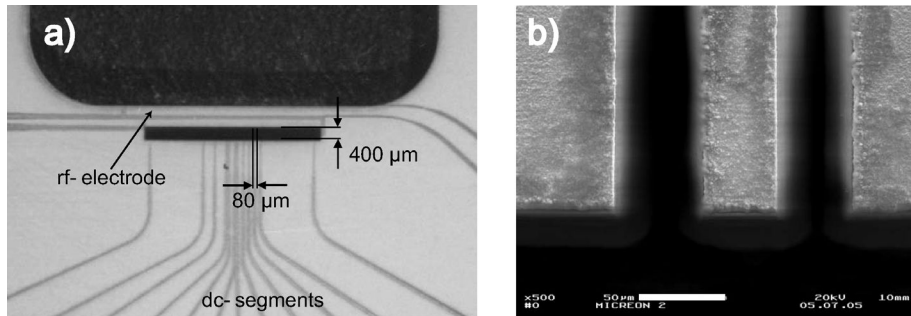


Figure 23.20. (a) An optical microscope image of the ion chip for a two layer micro trap. Gold is coated onto a ceramics carrier and structured with ns-laser pulses (Fraunhofer Inst., Dresden, Germany). Dc electrodes allow to modify the axial potential. For this example, the narrowest axial dc electrode is 80 μm wide and the radial size is 400 μm . (b) Electron microscope image of a gold/ceramics test structure with cuts fabricated by fs-laser pulses. A roughness of $\sim 5 \mu\text{m}$ is obtained. The white bare indicates a length scale of 50 μm .

confine only very few vibrational levels. In this situation, it will probably be necessary to load the nm-traps from a larger trapping structure. We expect that in future segmented microstructured ion traps will allow for a coherent manipulation of entangled states with ensembles of $N \sim 10^2$ qubits. So far, only technical, but no fundamental physical obstacles have been identified. The solution of the corresponding problems, however, is certainly a tremendous task being shared by only a relatively small number of research groups. My strong expectation is that the enforcement by technical engineers will be increasingly necessary for this advanced type of quantum engineering.

Acknowledgments My cordial thanks are to R. Blatt, Head of the Institute of Experimentalphysik at the University Innsbruck, Austria and all the members of his group. A large part of the scientific success has been due to a strong group effort and none of the measurements presented here—to illustrate the unique power of quantum information with trapped ions—would have been possible otherwise. I acknowledge stimulating atmosphere, and discussions with I. Cirac, A. Zeilinger, P. Zoller, and coworkers, and thank M. Freyberger and G. Huber for reading the manuscript. For financial support I acknowledge the Austrian FWF, the German DFG, the Landesstiftung Baden-Württemberg, and the European commission.

Exercises

1. Prove that the Laplace equation $\Delta\Phi = 0$ allows no static electric trapping of ions in three dimensions.
2. Numerically solve the Mathieu equation in one dimension in the case $a=0$:

$$\frac{d^2 u(t)}{dt^2} + 2q \cos(2t)u(t) = 0,$$

Plot $u(t)$ for $q = 0.1, 0.3, 0.7$, and 1 . What is your observation for $u(t)$? Find out the limit of stability by trying out different values of q .

3. Construct the matrix $\mathbf{A}$ for two and three ions. Find the axial eigenvectors and eigenfrequencies by diagonalizing (see Eq. (23.7)).
4. Rabi oscillations of the upper state population P_e on the blue sideband (Fig. 23.8) are described by

$$P_e = \frac{1}{2} \left[1 - \sum_n P_n \cos(\Omega_{(n+1,n)} \cdot t) \right]$$

with Rabi frequencies $\Omega_{(n+1,n)} = \eta\Omega_0\sqrt{n+1}$ that depend on the vibrational state $|n\rangle$. Assume a thermal phonon distribution $P_n = m^n/(m+1)^{n+1}$ with a mean phonon number m and plot $P_e(t)$ for $\eta=0.1$, $m=0.1$, and $m=0.5$, respectively. How differs the visibility of many Rabi oscillations in both cases? How does the fidelity of a π -rotation depends on m ?

5. Prove Eq. (23.9) for the common quantum state $|\phi_{1,2,3}\rangle$ —written in terms of Bell states—in the teleportation algorithm prior to Alice's projection into Bell basis states.

References

- [1] W. Neuhauser, M. Hohenstatt, P. E. Toschek, and H. Dehmelt, *Phys. Rev. A* **22**, 1137 (1980).
- [2] W. Nagourney, J. Sandberg, and H. Dehmelt, *Phys. Rev. Lett.* **56**, 2797 (1986).
- [3] T. Sauter, W. Neuhauser, R. Blatt, and P. E. Toschek, *Phys. Rev. Lett.* **57**, 1696 (1986).
- [4] J. J. Bollinger, J. D. Prestage, W. Itano, and D. Wineland, *Phys. Rev. Lett.* **54**, 1000 (1985).
- [5] S. A. Diddams, Th. Udem, J. C. Bergquist, E. A. Curtis, R. E. Drullinger, L. Hollberg, W. M. Itano, W. D. Lee, C. W. Oates, K. R. Vogel, and D. J. Wineland, *Science* **293**, 825 (2001).
- [6] H. S. Margolis, G. P. Barwood, G. Huang, H. A. Klein, S. N. Lea, K. Szymaniec, and P. Gill, *Science* **306**, 1355 (2004).
- [7] Th. Udem, S. A. Diddams, K. R. Vogel, C. W. Oates, E. A. Curtis, W. D. Lee, W. M. Itano, R. E. Drullinger, J. C. Bergquist, and L. Hollberg, *Phys. Rev. Lett.* **86**, 4996 (2001).
- [8] E. Peik, B. Lipphardt, H. Schnatz, T. Schneider, Chr. Tamm, and S. G. Karshenboim, *Phys. Rev. Lett.* **93**, 170801 (2004).
- [9] I. Cirac and P. Zoller, *Phys. Rev. Lett.* **74**, 4091 (1995).
- [10] *Quantum Computation and Quantum Information*, M. A. Nielsen, and I. L. Chuang, Cambridge University Press, Cambridge, (2000).
- [11] Yu. I. Manin, *Sovetskoye Radio*, Moscow (1980).
- [12] Yu. I. Manin, *Nordrhein-Westfael. Akademie der Wissenschaften* (1999), *Preprint* quant-ph/9903008.
- [13] R. Feynman, *Internat. J. Theoret. Phys.* **21**, 467 (1982).
- [14] R. Feynman, *Found. Phys.* **21**, 507 (1986).
- [15] D. Deutsch, *Proc. R. Soc. Lond. A* **425**, 73 (1989).
- [16] A. Ekert, *Atomic Physics* **14**, 450 (1994).
- [17] P. W. Shor, *Proceed. of the 35th Annual Symposium on the Foundations of Computer Science*, ed. S. Goldwasser (1994).
- [18] A. Ekert and R. Josza, *Rev. Mod. Phys.* **68**(3) (1996).
- [19] H. Dehmelt, *Bull. Am. Phys. Soc.* **20**, 60 (1975).
- [20] Ch. Roos, Th. Zeiger, H. Rohde, H. C. Nägerl, J. Eschner, D. Leibfried, F. Schmidt-Kaler, and R. Blatt, *Phys. Rev. Lett.* **83**, 4713 (1999).
- [21] S. Haroche and J. M. Raimond, *Physics Today* (1996).
- [22] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe. **404**, 256 (2000).
- [23] C. F. Roos, M. Riebe, H. Häffner, W. Hänsel, J. Benhelm, G. P. T. Lancaster, C. Becher, F. Schmidt-Kaler, R. Blatt, *Science* **304**, 1478 (2004).
- [24] D. Leibfried, M. D. Barrett, T. Schaetz, J. Britton, J. Chiaverini, W.M. Itano, J.D. Jost, C. Langer, and D.J. Wineland, *Science* **304**, 1476 (2004).
- [25] H. Häffner *et al*, *Nature* **438**, 643 (2005).
- [26] D. Leibfried *et al*, *Nature*. **438**, 639 (2005).

- [27] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
- [28] A. Steane, Proc. R. Soc. Lond. A **452**, 2551 (1996).
- [29] W. Paul, Q. Osberghaus, and E. Fischer, Forschungsberichte des Wirtschafts—und Verkehrsministeriums Nordrhein-Westfalen **415** (1958).
- [30] P. K. Ghosh, *Ion Traps*, The International Series of Monographs on Physics, 90. Oxford Science Publications (1995).
- [31] <http://heart-c704.uibk.ac.at/>
- [32] Andreas Mundt, PhD Thesis, Cavity QED with single trapped $^{40}\text{Ca}^+$ -ions, unpublished, Innsbruck (2003)
- [33] H. C. Nägerl, Ch. Roos, D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, and R. Blatt, Phys. Rev. A **61**, 023405 (2000).
- [34] H.C. Nägerl, W. Becher, J. Eschner, F. Schmidt-Kaler, R. Blatt, Appl. Phys. B **66**, 603 (1998).
- [35] Stephan Gulde, PhD Thesis, Experimental realization of quantum gates and the Deutsch–Josza algorithm with trapped $^{40}\text{Ca}^+$ -ions, unpublished, Innsbruck (2003)
- [36] F. Schmidt-Kaler, H. Häffner, S. Gulde, M. Riebe, G. P. T. Lancaster, T. Deuschle, C. Becher, W. Hänsel, J. Eschner, C. F. Roos, and R. Blatt, Appl. Phys. B: Lasers and Optics **77**, 789 (2003).
- [37] M. Drewsen and A. Broner, Phys. Rev. A **62**, 045401 (2000).
- [38] I. Waki, S. Kassner, G. Birkel, and H. Walther. Phys. Rev. Lett. **68**, 2007 (1992).
- [39] G. Birkel, S. Kassner, and H. Walther, Nature **357**, 310, (1992).
- [40] M. G. Raizen, J. M. Gilligan, J. C. Bergquist, W. M. Itano, C. Monroe, and D. J. Wineland, Phys. Rev. A **45**, 6493 (1992).
- [41] H. C. Nägerl, W. Bechter, J. Eschner, F. Schmidt-Kaler, and R. Blatt, Optics Express **3**, 89 (1998).
- [42] D. V. F. James, Appl. Phys. B **66**, 181 (1998).
- [43] A. Steane, Appl. Phys. B **64**, 632 (1997).
- [44] C. Marquet, F. Schmidt-Kaler, and D. F. V. James, Appl. Phys. B **76**, 199 (2003).
- [45] D. G. Enzer, M. M. Schauer, J. J. Gomez, M. S. Gulley, M. H. Holzscheiter, P. G. Kwiat, S. K. Lamoreaux, C. G. Peterson, V. D. Sandberg, D. Tupa, A. G. White, and R. J. Hughes, Phys. Rev. Lett. **85**, 2466 (2000).
- [46] A. Steane, C. F. Roos, D. Stevens, A. Mundt, D. Leibfried, F. Schmidt-Kaler, and R. Blatt, Phys. Rev. A **62**, 042305 (2000).
- [47] R. Ozeri, C. Langer, J. D. Jost, B. L. DeMarco, A. Ben-Kish, B. R. Blakestad, J. Britton, J. Chiaverini, W. M. Itano, D. Hume, D. Leibfried, T. Rosenband, P. Schmidt, and D. J. Wineland, Phys. Rev. Lett. **95**, 030403 (2005).
- [48] C. F. Roos, D. Leibfried, A. Mundt, F. Schmidt-Kaler, J. Eschner, and R. Blatt, Phys. Rev. Lett. **85**, 5547 (2000).
- [49] M. Barrett, B. L. DeMarco, T. Schätz, V. Meyer, D. Leibfried, J. Britton, J. Chiaverini, W. M. Itano, B. M. Jelenkovic, J. D. Jost, C. Langer, T. Rosenband, and D. J. Wineland, Phys. Rev. A **68**, 042302 (2003).
- [50] C. Monroe, D. M. Meekhof, B. E. King, S. R. Jefferts, W. M. Itano, D. J. Wineland, and P. Gould, Phys. Rev. Lett. **75**, 4011 (1995).

- [51] H. C. Nägerl, D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, and R. Blatt, *Phys. Rev. A* **60**, 145 (1999).
- [52] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, *Nature* **421**, 48 (2003).
- [53] A. M. Childs and I. L. Chuang, *Phys. Rev. A* **63**, 012306 (2000).
- [54] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner, and R. Blatt, *Nature* **422**, 408 (2003).
- [55] K. Mölmer, A. Sørensen, *Phys. Rev. Lett.* **82**, 1835 (1999).
- [56] A. Sørensen, K. Mölmer, *Phys. Rev. Lett.* **82**, 1971 (1999).
- [57] A. Sørensen and K. Mölmer, *Preprint quant-ph/0002024*.
- [58] G. J. Milburn, *Preprint quant-ph/9908037*.
- [59] D. Jonathan, M. B. Plenio, and P. L. Knight, *Phys. Rev. A* **62**, 042307 (2000).
- [60] D. Jonathan and M. B. Plenio, *Phys. Rev. Lett.* **87**, 127901 (2001).
- [61] L. M. Duan, J. I. Cirac, and P. Zoller, *Science*, **292**, 1695 (2001).
- [62] J. F. Poyatos, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 1322, (1998).
- [63] J. J. García-Ripoll, P. Zoller, and J. I. Cirac, *Phys. Rev. Lett.* **91**, 157901 (2003).
- [64] D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D. J. Wineland, *Nature* **422**, 412 (2003).
- [65] <http://tf.nist.gov/timefreq/ion/>
- [66] see discussion and Tab. 1 in D. J. Wineland, M. Barrett, J. Britton, J. Chiaverini, B. L. DeMarco, W. M. Itano, B. M. Jelenkovic, C. Langer, D. Leibfried, V. Meyer, T. Rosenband, and T. Schaetz, *Phil. Trans. Royal Soc. London A* **361**, 1349 (2003).
- [67] P. C. Haljan, K.-A. Brickman, L. Deslauriers, P. J. Lee, and C. Monroe, *Phys. Rev. Lett.* **94**, 153602 (2005).
- [68] F. Schmidt-Kaler, H. Häffner, S. Gulde, M. Riebe, G. Lancaster, J. Eschner, C. Becher, and R. Blatt, *Europhysics Letters* **65**, 587 (2004).
- [69] H. Häffner, S. Gulde, M. Riebe, G. Lancaster, C. Becher, J. Eschner, F. Schmidt-Kaler, and R. Blatt, *Phys. Rev. Lett.* **90**, 143602 (2003).
- [70] F. Mintert and C. Wunderlich, *Phys. Rev. Lett.* **87**, 257904 (2001).
- [71] A. Kreuter, C. Becher, G. P. T. Lancaster, A. B. Mundt, C. Russo, H. Häffner, C. Roos, J. Eschner, F. Schmidt-Kaler, and R. Blatt, *Phys. Rev. Lett.* **92**, 203002 (2004).
- [72] A. B. Mundt, A. Kreuter, C. Becher, D. Leibfried, J. Eschner, F. Schmidt-Kaler, R. Blatt, *Phys. Rev. Lett.* **89**, 103001 (2002).
- [73] G. R. Guthöhrlein, M. Keller, K. Hayasaka, W. Lange, and H. Walther *Nature* **414**, 49 (2001).
- [74] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther *Nature* **431**, 1075 (2004).
- [75] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [76] M. Riebe, H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James, and R. Blatt, *Nature* **429**, 734 (2004).

- [77] M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W.M. Itano, J.D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D.J. Wineland, *Nature* **429**, 737 (2004).
- [78] H. Häffner *et al*, to be published.
- [79] C. F. Roos, G. P. T. Lancaster, M. Riebe, H. Häffner, W. Hänsel, S. Gulde, C. Becher, J. Eschner, F. Schmidt-Kaler, R. Blatt, *Phys. Rev. Lett.* **92**, 220402 (2004).
- [80] J. L. O'Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White, *Phys. Rev. Lett.* **93**, 080502 (2004).
- [81] Z. Hradil *et al.*, *Lecture Notes in Physics* (ed. M.G.A. Paris, J. Rehacek), 59, Springer, Berlin (2004).
- [82] D. Stick, W. K. Hensinger, S. Olmschenk, M. J. Madsen, K. Schwab, and C. Monroe, *Nature Physics* **2**, 36 (2006).
- [83] M. J. Madsen, W.K. Hensinger, D. Stick, J.A. Rabchuk, and C. Monroe, *Appl. Phys. B* **78**, 639 (2004).
- [84] J. Chiaverini, R. B. Blakestad, J. Britton, J. D. Jost, C. Langer, D. Leibfried, R. Ozeri, D. J. Wineland, *Quantum Information and Computation* **5**, 419 (2005).
- [85] S. Seidelin, *et al*, *Phys. Rev. Lett.* **96**, 253003 (2006).
- [86] <http://monroelab2.physics.lsa.umich.edu/research/trap/index.html>
- [87] W. K. Hensinger, S. Olmschenk, D. Stick, D. Hucul, M. Yeo, M. Acton, L. Deslauriers, C. Monroe, and J. Rabchuk, *App. Phys. Lett.* **88**, 034101 (2006).
- [88] D. Kielpinski, C.R. Monroe, and D. J. Wineland, *Nature* **417**, 709 (2002).
- [89] S. Schulz, U. Poschinger, K. Singer, and F. Schmidt-Kaler, *Fortschr. Phys.* **54**, No. 8, 648 (2006).
- [90] R. Reichle, *et al*, *Fortschr. Phys.* **54**, No. 8, 666 (2006).
- [91] M. A. Rowe, A. Ben-Kish, B. DeMarco, D. Leibfried, V. Meyer, J. Beall, J. Britton, J. Hughes, W. M. Itano, B. Jelenkovic, C. Langer, T. Rosenband, and D. J. Wineland, *Quant. Inform. and Comput.* **2**, 257 (2002).
- [92] The control of quantum correlations in tailored matter, and common perspectives of mesoscopic systems and quantum gases are investigated in a German research network. Detailed information is provided by <http://www.physik.uni-stuttgart.de/TR21/>
- [93] W. K. Hensinger, D. W. Utami, H.-S. Goan, K. Schwab, C. Monroe, G. J. Milburn, *Phys. Rev. A* **72**, 041405R (2005).
- [94] D. J. Heinzen and D. J. Wineland, *Phys. Rev A* **42**, 2977 (1990).
- [95] L. Tian, P. Rabl, R. Blatt and P. Zoller, *Phys. Rev. Lett.* **92**, 247902 (2004).

24 Quantum Computing with Solid State Systems

Guido Burkard and Daniel Loss

24.1 Introduction

This chapter is intended as an introduction to the theory of solid-state quantum information processing. We do not aspire to offer a comprehensive review of all proposed solid-state schemes for quantum computing, as there are far too many to be covered here (see, e.g., [1] for a review). We will highlight some general concepts that have relevance for most proposals and only discuss the physics of two types of solid-state qubit systems in which experimental progress has been particularly strong in the past 5 years: Electron spin-based qubits in semiconductors [2] and superconducting circuits with small-capacitance Josephson junctions [3–5]. Even for these systems, we will not be able to cover everything that has been done; the interested reader is referred to more extensive reviews [6–11].

Other solid-state proposals for quantum computation include quantum Hall systems in fractional quantum Hall systems, the nuclear spin of donors in a semiconductor, electron charge degrees of freedom in quantum dots (QDs), “flying” electron spin qubits in surface acoustic waves or ballistic quantum wires, ferroelectrically coupled quantum dots, excitons, SiGe quantum dots, paramagnetic impurities in semiconductor quantum wells, Si-based solid-state NMR, and electrons on the surface of liquid He (for a list of references, see [9]).

One of the eminent features of many solid-state systems studied for quantum information processing is their *scalability*, i.e., the existence of fabrication technology that permits the making of a large number of qubits, once one such qubit has been tried and tested. Both semiconductor and superconductor samples are produced with lithographic techniques which are ideal for scaling.

Despite the fact that both semiconductor and superconductor qubits are made using solid-state materials, these two types of qubits which we discuss in this chapter are fundamentally different. The spin-based qubits are truly *microscopic* objects—in this respect they are similar to the atomic qubits in the sense that they are based on quantum objects on the atomic scale whose states $|0\rangle$ and $|1\rangle$ are distinguishable by measuring a microscopic observable, such as angular momentum of the order of Planck’s constant $\hbar$ or a magnetic dipole moment of the order of one Bohr magneton, μ_B . Electron and nuclear spin qubits, as well as the orbital state of an electron in a semiconductor quantum dot, fall under this category. Another class of qubits could be labeled *macroscopic*, for their distinguishability under measurement of a macroscopic observable, such as a current carried by a large number of electrons, the magnetic field induced by such a current, or the position of an electron charge in a system

with two macroscopically distinguishable sites. The typical examples in this category are the superconducting qubits (with exceptions).

24.2 Concepts

24.2.1 The exchange coupling

The exchange coupling between electron spins [2] is an important paradigm for most solid-state quantum computing (QC) proposals, even those where the qubit is not a real spin, but a *pseudospin*, which can be any other type of quantum two-level system. As we shall see, even the *pseudospin* in superconducting qubits is coupled via an anisotropic exchange coupling.

Let us for concreteness consider an array of semiconductor quantum dots, as shown in Fig. 24.1, with one electron occupying each of the dots, as in the original spin qubit proposal [2]. The coupling between the qubits in this case is provided by the tunneling between adjacent quantum dots, giving rise to a nearest-neighbor exchange coupling. The resulting spin Hamiltonian in this case is that of the Heisenberg model,

$$H(t) = \sum_{\langle i,j \rangle} J_{ij}(t) \mathbf{S}_i \cdot \mathbf{S}_j + \mu_B \sum_i g_i \mathbf{B}(\mathbf{r}_i) \cdot \mathbf{S}_i, \quad (24.1)$$

where $\mathbf{S}_i$ denotes the spin operator of the electron in the i th quantum dot and J_{ij} the exchange energy between spins i and j . As mentioned above, this proposal for exchange-based QC extends far beyond electron spins in quantum dots. Subsequent proposals for QC, using the nuclear spins of donor atoms buried in a silicon substrate, or using electron spins in SiGe quantum dots, electrons trapped by surface acoustic waves, and spins of paramagnetic impurities, rely on the same type of interaction [9].

The spin Hamiltonian, Eq. (24.1), also accounts for the Zeeman coupling to an external magnetic field $\mathbf{B}$ which may be spatially varying (here, the Bohr magnetic moment is denoted

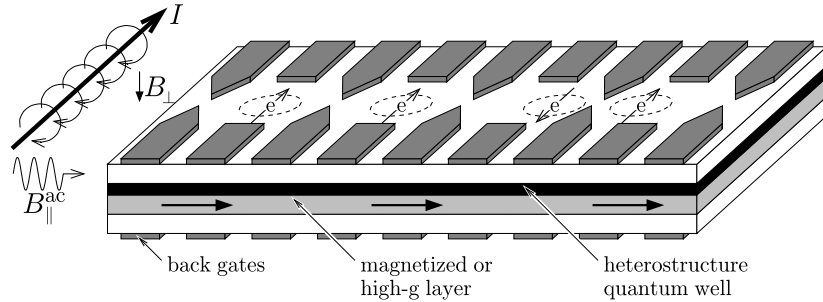


Figure 24.1. A quantum-dot array for quantum computing according to [2] (schematically). Quantum dots (dashed circles) are defined in a two-dimensional semiconductor heterostructure with metal gates (shown schematically in gray) and host one (excess) electron (e) with a spin $1/2$ each. By controlling the gate voltages, the coupling of adjacent quantum dots is switched on and off for quantum gate operations.

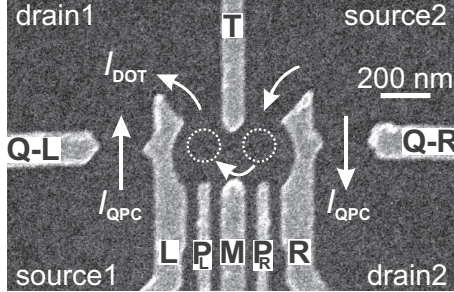


Figure 24.2. Two quantum dots in a scanning electron micrograph picture (Courtesy of J. Elzerman, TU Delft). The dots are defined by metal electrodes (bright features) on the surface of a GaAs/AlGaAs heterostructure. The charge on each of the dots is controlled in steps of single elementary charges, down to one electron per dot, by tuning the voltage applied to the plunger gates $P_{L,R}$ and is monitored by measuring the conductance of (i.e., the currents I_{QPC} through) the quantum point contacts (QPCs) Q-R and Q-L. Conductance spectroscopy was performed by measuring the current I_{dot} [12].

by μ_B). There is the possibility, in some semiconductor heterostructures, of a site-dependent Landé g -factor g_i . Two coupled quantum dots with individually tunable electron number down to one electron have been demonstrated [12], see Fig. 24.2.

In this scheme for quantum computation, the exchange coupling is switched off $J_{ij} = 0$ between all dots i and j , except when a gate operation between dots i and j takes place. Several nonoverlapping qubit pairs can be coupled simultaneously. A pulse $J_{ij}(t)$ with

$$\frac{1}{\hbar} \int J_{ij}(t') dt' = \frac{\pi}{2} \pmod{2\pi} \quad (24.2)$$

generates the square-root of SWAP gate, up to a global phase factor $e^{-i\pi/8}$ which we omit,

$$S \simeq \exp\left(\frac{i}{\hbar} \int dt' H(t')\right) = \exp\left(i\frac{\pi}{2} \mathbf{S}_i \cdot \mathbf{S}_j\right). \quad (24.3)$$

The quantum gate S can then be combined with single-spin rotations

$$U_i(\phi) = \exp(i\phi \cdot \mathbf{S}_i), \quad (24.4)$$

to produce a controlled phase flip (CPF) [2],

$$U_{CPF} = e^{-i\frac{\pi}{2}} e^{i\frac{\pi}{2} S_1^z} e^{-i\frac{\pi}{2} S_2^z} S e^{i\pi S_1^z} S, \quad (24.5)$$

which, up to a basis change, equals the quantum XOR (aka CNOT) gate

$$U_{XOR} = V U_{CPF} V^\dagger, \quad (24.6)$$

$$V = \exp(-i\pi S_2^y/2). \quad (24.7)$$

24.2.2 Anisotropic exchange

24.2.2.1 Ising and transverse (XY) coupling

In semiconductor optical cavities, the coupling between spins in quantum dots can be achieved without tunnel coupling between the dots, but instead via emission and reabsorption of virtual cavity photons [13] (see Section 24.3.3). In this case, the exchange coupling between the electron spins is no longer described by the isotropic exchange Hamiltonian (24.1), but by the XY (transverse) spin Hamiltonian,

$$H_{XY} = J \sum_{i,j} (S_i^x S_j^x + S_i^y S_j^y) = \frac{J}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (24.8)$$

where we chose the S^z basis of the two interacting qubits i and j for the matrix representation of H_{XY} . In inductively coupled superconducting qubits [5, 10] (Section 24.4), the coupling also has the XY form, Eq. (24.8), thus it is of interest whether this coupling can be used for universal quantum computing instead of the isotropic Heisenberg Hamiltonian.

In this context one should point out that any generic two-qubit Hamiltonian gives rise to a universal set of gates when combined with single-qubit operations. Here we discuss how a universal gate (CPF, XOR) can be constructed *explicitly* from anisotropic exchange interaction. In two notable cases of anisotropic spin couplings, the Ising and the XY interactions, it is known how the CPF and XOR gates can be constructed. In the case of a system described by the Ising Hamiltonian $H_I = JS_1^z S_2^z$ and a homogeneous magnetic field in the z direction, there is a particularly simple realization of the CPF gate with constant parameters, namely $U_{\text{CPF}} = \exp(i\pi(1 - 2S_1^z - 2S_2^z + 4S_1^z S_2^z)/4)$ [2]. However, a pure Ising coupling is rarely found in nature (although it has to be said that motional narrowing in liquid-state NMR leads to an *approximately* pure Ising coupling).

For the transverse spin-spin coupling of Eq. (24.8), we find that a useful two-qubit gate, such as the conditional-phase-flip (CPF) operation, can be done by combining H_{XY} with one-bit rotations. The unitary evolution operator generated by the Hamiltonian of Eq. (24.8) is

$$U_{XY}(\phi) = T \exp \left[i \int dt H_{XY} \right] = \exp [i\phi(S_i^x S_j^x + S_i^y S_j^y)], \quad (24.9)$$

where $\phi = \int dt J(t)$. The CPF gate (U_{CPF}) can be realized by the sequence [13, 14]

$$U_{\text{CPF}} = e^{i\pi/4} e^{i\pi \mathbf{n}_i \cdot \boldsymbol{\sigma}_i / 3} e^{i\pi \mathbf{n}_j \cdot \boldsymbol{\sigma}_j / 3} U_{XY}(\pi/2) e^{i\pi \sigma_z^i / 2} U_{XY}(\pi/2) e^{i\pi \sigma_y^i / 4} e^{i\pi \sigma_y^j / 4}, \quad (24.10)$$

where $\boldsymbol{\sigma}$ denotes the vector Pauli operator, $\mathbf{S} = \boldsymbol{\sigma}/2$, and $\mathbf{n}_i = (1, 1, -1)/\sqrt{3}$ and $\mathbf{n}_j = (-1, 1, 1)/\sqrt{3}$. The XOR gate can be realized by combining the CPF operation with single-qubit rotations as in Eqs. (24.6) and (24.7).

While it is impossible to generate the CNOT gate with a single use of the XY Hamiltonian [14], it is possible to generate a different universal quantum gate with the XY interaction in a single pulse; the CNOT + SWAP (CNS) gate $U_{\text{CNS}} = U_{\text{SWAP}} U_{\text{XOR}}$, is generated as [15]

$$U_{\text{CNS}} = H_1 U_{XY}(\pi) e^{-i\pi \sigma_z^i / 4} e^{-i\pi \sigma_z^j / 4} H_2, \quad (24.11)$$

where H_i is the Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ applied to qubit i .

24.2.2.2 Anisotropy due to the spin-orbit coupling

Even in the case of spins occupying tunnel-coupled sites (such as quantum dots), where the exchange is described by the isotropic Hamiltonian, Eq. (24.1), the isotropy can be broken due to spin-orbit coupling during tunneling between the sites (see [9] and references therein). Surprisingly, it turns out that the first-order effect of the spin-orbit coupling during quantum gate operations can be eliminated by using time-symmetric pulse shapes for the coupling between the spins. A related, but independent, result shows that the spin-orbit effects *exactly* cancel in the gate sequence on the right-hand side of Eq. (24.5) required to produce the quantum XOR gate, provided that the pulse form for the spin-orbit and the exchange couplings are identical. The XOR gate being universal when complemented with single-qubit operations, this result implies that the spin-orbit coupling can be dealt within any quantum computation. In any real implementation, there will be some (small) discrepancy between the pulse shapes for the exchange and the spin-orbit coupling; however, one can choose two pulse shapes which are very similar. It was shown that the cancellation still holds to a very good approximation in such a case, i.e., the effect of the spin-orbit coupling will still be strongly suppressed.

We will now discuss the cancellation of the spin-orbit effects in the sequence Eq. (24.5) required for the XOR gate in detail. The spin-orbit coupling for a conduction-band electron is given by the following Hamiltonian, being linear in the 2D momentum operator p_i , $i = x, y$ ([100] orientation of the 2D plane),

$$H_{\text{so}} = \sum_{i,j=x,y} \beta_{ij} \sigma_i p_j, \quad (24.12)$$

where the constants β_{ij} depend on the strength of the confinement in the z -direction and are of the order $(1 \div 3) \cdot 10^5$ cm/s for GaAs heterostructures. Combining the isotropic Heisenberg coupling (24.1) with the anisotropic exchange between two localized spins $\mathbf{S}_1$ and $\mathbf{S}_2$ one obtains the spin Hamiltonian

$$H(t) = J(t) (\mathbf{S}_1 \cdot \mathbf{S}_2 + \mathcal{A}(t)), \quad (24.13)$$

where the anisotropic part is given by the expression

$$\mathcal{A}(t) = \beta(t) \cdot (\mathbf{S}_1 \times \mathbf{S}_2) + \gamma(t) (\beta(t) \cdot \mathbf{S}_1) (\beta(t) \cdot \mathbf{S}_2), \quad (24.14)$$

and $\beta_i = \sum_j \beta_{ij} \langle \psi_1 | i p_j | \psi_2 \rangle$ is the spin-orbit field, $|\psi_i\rangle$ the ground state in site (quantum dot) $i = 1, 2$, and $\gamma \approx O(\beta^0)$. As discussed in Section 24.4, for $\mathcal{A} = 0$, the quantum XOR gate can be obtained by applying $H(t)$ twice, together with single-spin rotations, see Eqs. (24.5) and (24.7). Moreover, if $\mathcal{A} = 0$, then $H(t)$ commutes with itself at different times and the time-ordered exponential

$$U(\varphi) = T \exp \left(-i \int_{-\tau_s/2}^{\tau_s/2} H(t) dt \right) \quad (24.15)$$

is a function of the integrated interaction strength only, $\varphi = \int_{-\tau_s/2}^{\tau_s/2} J(t)dt$. In particular, $U(\varphi = \pi/2) = U_{\text{sw}}^{1/2} = S$ is the “square-root of swap” gate.

Let us now consider the more interesting situation where $\mathcal{A} \neq 0$. If in this case, β and γ (and thus $\mathcal{A}$) are time-independent, then $H(t)$ *still* commutes with itself at different times and one can find a fixed coordinate system in which β is parallel to the z -axis. In this basis, the anisotropic term (24.14) can be expressed as

$$\mathcal{A} = \beta(S_1^x S_2^y - S_1^y S_2^x) + \delta S_1^z S_2^z, \quad (24.16)$$

with $\delta = \gamma\beta^2$. In the singlet–triplet basis of the two spins with basis vectors $\{|T_+\rangle = |\uparrow\uparrow\rangle, |S\rangle = (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)/\sqrt{2}, |T_0\rangle = (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)/\sqrt{2}, |T_-\rangle = |\downarrow\downarrow\rangle\}$ the gate sequence Eq. (24.5), including the anisotropy, Eq. (24.14), produces the unitary operation

$$U_g = \text{diag}(ie^{-i\varphi(1+\delta)}, 1, 1, -ie^{-i\varphi(1+\delta)}), \quad (24.17)$$

where $\text{diag}(x_1, \dots, x_4)$ denotes the diagonal matrix with diagonal entries $x_1, \dots, x_4$. The pulse strength φ and the spin-orbit parameters only enter U_g in the $S^z = \pm 1$ subspaces, while the terms linear in β have canceled out exactly in U_g . By choosing $\varphi = \pi/2(1 + \delta)$, one obtains the conditional phase-flip (CPF) gate $U_g = U_{\text{CPF}} = \text{diag}(1, 1, 1, -1)$, equivalent to the XOR via the basis change equation (24.7). In conclusion, we have shown that the anisotropic terms $\mathcal{A} = \text{const.}$ in the spin Hamiltonian cancel exactly in the gate sequence (24.6) for the quantum XOR. In real systems, we can expect that the anisotropic terms in the Hamiltonian H are not exactly proportional to $J(t)$, i.e., that $\mathcal{A}(t)$ is time-dependent. It can be shown, that nevertheless, for small deviations from proportionality, the cancellation described above still holds to a good approximation (e.g., within a reasonable error-correction threshold).

24.2.3 Universal QC with the exchange coupling

Both for spin-based and superconducting qubits, there exist (in principle) methods to generate the single-qubit operations required for universal quantum computation. We assume that for some reason we can gain simplicity by trying to implement universal quantum computation with the two-qubit interaction only, without using single-qubit operations on the physical level. Let us concentrate on the isotropic interaction $J\mathbf{S}_1 \cdot \mathbf{S}_2$ —is quantum computing feasible with the exchange only? At first, this seems impossible, because the operator $\mathbf{S}_1 \cdot \mathbf{S}_2$ has too much symmetry: It commutes with the operators S^2 and S_z , where the total spin is $\mathbf{S} = \sum_{i=1}^n \mathbf{S}_i$, and therefore it can only generate transformations that leave the S , S_z quantum numbers the same. Nevertheless, a scheme has been developed in which the Heisenberg interaction alone suffices to exactly implement any quantum computer circuit by restricting the Hilbert space to a subspace with fixed S , S_z . This restriction of the Hilbert space is done by way of a suitable *encoding* (see [9] for detailed references).

24.2.3.1 Encoding

The smallest number of spins 1/2 for which two orthogonal states with identical S , S_z exist is three. The space of three-spin states with spin quantum numbers $S = 1/2$, $S_z = +1/2$ is

two-dimensional and will serve as our encoded qubit. We make the following explicit choice for the basis states of the qubit,

$$|0_L\rangle = |S\rangle|\uparrow\rangle, \quad (24.18)$$

$$|1_L\rangle = \sqrt{2/3}|T_+\rangle|\downarrow\rangle - \sqrt{1/3}|T_0\rangle|\uparrow\rangle, \quad (24.19)$$

where $|S\rangle = \sqrt{1/2}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ is the singlet state of spins 1 and 2 of the three-spin block, and $|T_+\rangle = |\uparrow\uparrow\rangle$ and $|T_0\rangle = \sqrt{1/2}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$ are triplet states of these two spins. In principle this solves the problem of exchange-only quantum computing, but in practice we would like to know what the cost in terms of qubits (for coding) and gates (for operating on encoded qubits with the exchange interaction) will be, and explicitly how a universal set of operations on the encoded qubits can be achieved.

Universal quantum computing is also possible uniquely with the anisotropic XY interaction (24.8), a result which was later generalized to large class of anisotropic exchange Hamiltonians. An encoding involving two spins per qubit has also been demonstrated for universal quantum logic starting from locally alternating g -factors and from a homogeneous magnetic field combined with anisotropic exchange interactions.

24.2.3.2 One-qubit gates

Unitary gates on a single encoded qubit (a block of three spins) are performed as follows. The exchange between code qubits 1 and 2, H_{12} , generates a rotation $U_{12} = \exp(i/\hbar \int J \vec{S}_1 \cdot \vec{S}_2 dt)$ which is a z -axis rotation (in Bloch-sphere notation) on the encoded qubit, while H_{23} produces a rotation about an axis in the x - z plane, at an angle of 120° from the z -axis. Since simultaneous application of H_{12} and H_{23} can generate a rotation around the x -axis, three steps of exchange coupling suffice to implement any one-qubit rotation using the classic Euler-angle construction; assuming nearest-neighbor coupling in a linear arrangement of the code block and allowing for parallel operations. In serial operation, i.e., if each exchange coupling is switched on after all others have been turned off, it can be found numerically that four steps are always adequate when only nearest-neighbor interactions are possible, while three steps suffice if interactions can be turned on between any pair of spins.

24.2.3.3 Two-qubit gates

It is less straightforward to understand the implementation of a two-qubit gate such as XOR using the exchange interaction on two three-spin code blocks. While the four basis states $|0_L, 1_L\rangle|0_L, 1_L\rangle$ have total spin quantum numbers $S = 1$, $S_z = +1$, the complete space with these quantum numbers for six spins is nine-dimensional. Numerical searches for the implementation of two-qubit gates using a simple minimization algorithm have resulted in an apparently optimal sequence for an encoded XOR (CNOT) operation comprising 19 exchange operations in series. (Variations of this result with other than linear arrangements of the constituent qubits and with parallel operation exist.

24.2.3.4 Spin cluster qubits

A different kind of encoded qubits, the so-called spin cluster qubits, have been suggested in order to relax the requirements for control on the single-spin level while inheriting the favorable single-spin properties such as long decoherence time and fast gate operating time. Spin cluster qubits are finite spin chains with Heisenberg or anisotropic (XY and Ising-like) antiferromagnetic exchange interaction ($J > 0$).

24.2.4 Adiabaticity

Unitary quantum gates are generated by controlling the time dependence of the parameters in the Hamiltonian, e.g., Eq. (24.1) in the case of isotropic exchange. The parameters are, e.g., $J_{ij}(t)$ and $\mathbf{B}_i(t)$ (or $g_i(t)$). In spin qubits, the exchange coupling J can depend on time via some physically controlled quantity, such as an electric gate voltage $v(t)$, i.e., $J(t) = J(v(t))$ and similarly for the effective g -factor $g(t)$. According to Eq. (24.2), only the time integral $\int_0^T J(v(t))dt$ needs to assume a certain value (modulo 2π) in order to generate the correct quantum gate, while the pulse form of $v(t)$ does not matter. However, the exchange interaction $J(t)$ needs to be switched *adiabatically* in order to avoid unwanted excitations in the system. The adiabaticity condition is [14, 16, 17] $|\dot{v}/v| \ll \delta\varepsilon/\hbar$, where $\delta\varepsilon$ is the energy scale on which excitations may occur. Here, $\delta\varepsilon$ denotes the energy-level separation of a single dot, i.e., the smaller of either the single-electron level spacing or the on-site Coulomb energy U required to add a second electron to a dot. A rectangular pulse leads to excitation of higher levels, whereas an adiabatic pulse with amplitude v_0 is, for e.g., given by $v(t) = v_0 \operatorname{sech}(t/\Delta t)$ where Δt controls the width of the pulse. We need to use a switching time $\tau_s > \Delta t$, such that $v(t = \tau_s/2)/v_0$ becomes vanishingly small. We then have $|\dot{v}/v| = |\tanh(t/\Delta t)|/\Delta t \leq 1/\Delta t$, so we need $1/\Delta t \ll \delta\varepsilon/\hbar$ for adiabatic switching. The Fourier transform $v(\omega) = \Delta t v_0 \pi \operatorname{sech}(\pi\omega\Delta t)$ has the same shape as $v(t)$ but a width of $2/\pi\Delta t$. In particular, $v(\omega)$ decays exponentially in the frequency ω , whereas it decays only with $1/\omega$ for a rectangular pulse.

24.3 Electron Spin Qubits

The spin 1/2 of the electron is a natural quantum two-state system; its two basis states “spin up” and “spin down” can be identified with the logical basis of a quantum bit (qubit),

$$|\uparrow\rangle \equiv |0\rangle, \quad |\downarrow\rangle \equiv |1\rangle. \quad (24.20)$$

The electron spin is (typically) quite well isolated from charge degrees of freedom. There is, however, not a total separation due to relativistic (spin-orbit) corrections. In bulk semiconductors, the decoherence times for extended electronic states can be very long compared to other typical time scales in these systems (particularly charge decoherence times), exceeding microseconds [18]. The situation for localized electrons is more complicated due to the role played by the nuclear spins (at least in materials like GaAs where the nuclear spins are nonzero). We will discuss this issue in some more detail in Section 24.3.4.2.

Until a few years ago, single spins in solid-state structures were far from readily available and controllable. However, recently, there has been remarkable experimental progress that has lead to QDs with controllable single-electron occupation and single-spin read-out [7, 12].

Single-qubit operations with the Hamiltonian (24.1) require a time-varying Zeeman coupling $(g\mu_B \mathbf{S} \cdot \mathbf{B})(t)$ [2, 16], which can be controlled by changing the magnetic field $\mathbf{B}$ or the g -factor g . Effective magnetic fields/ g -factors can be produced by coupling the spin via exchange to a ferromagnet [2] or to polarized nuclear spins [16]. There is also the possibility of using electron spin resonance (ESR), the electronic analog to nuclear magnetic resonance (NMR) [7, 16, 19].

24.3.1 Quantum dots

In Fig. 24.1, we schematically show a quantum register made from single electrons confined in quantum dots (QDs) that are arranged in a one-dimensional array in a semiconductor structure [2]. One can also imagine the one-dimensional array being replaced by a two-dimensional lattice. Structures in which two QDs, each containing a well-controlled number of electrons (down to a single electron), are adjacent and tunnel-coupled, have been fabricated and studied [7, 12]. An electron micrograph of a structure of the type that was used in [12] is shown in Fig. 24.2. The tunneling of electrons between the two dots gives rise to the spin-exchange coupling $J\mathbf{S}_1 \cdot \mathbf{S}_2$ in Eq. (24.1). The objective of the following section is to understand this spin-exchange mechanism within a suitable theoretical model.

24.3.2 Exchange in laterally coupled QDs

The Pauli principle demands that the ground state of two confined electrons in the absence of a magnetic field is always a spin singlet. In the presence of tunneling and the Coulomb interaction, there is a finite energy splitting J between this spin singlet ground state and the energetically higher lying spin triplets. In a two-site configuration, e.g., in a system of two coupled QDs, Fig. 24.3, this energy gap J is called the *exchange coupling* between site 1 and site 2, as it arises from virtual electron exchange between the two sites due to the interaction. The virtual electron exchanges are allowed for opposite spins (spin singlet, $S = 0$) but forbidden by the Pauli principle for parallel spins (spin triplet, $S = 1$), therefore the energy of the singlet is lowered by the interaction.

In order to understand this quantitatively, we introduce a model for the two laterally coupled QDs containing one (conduction band) electron each [16]. The two-dot system is shown schematically in Fig. 24.3. It is essential that the electrons are allowed to tunnel between the dots, and that the total wavefunction of the coupled system must be antisymmetric under particle exchange due to the Pauli principle (Fermi statistics). These ingredients are responsible for correlations between the spins via the charge (orbital) degrees of freedom. The electronic Hamiltonian in the effective-mass approximation for the coupled system is

$$H = \sum_{i=1,2} h(\mathbf{r}_i, \mathbf{p}_i) + C + H_Z = H_{\text{orb}} + H_Z. \quad (24.21)$$

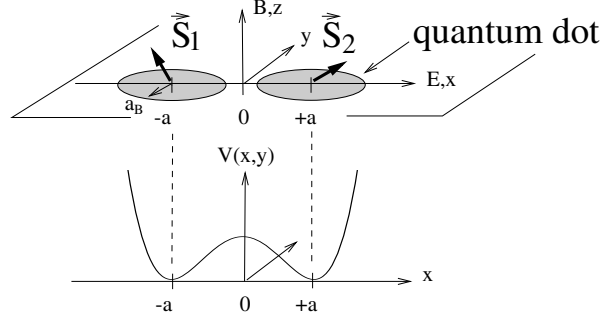


Figure 24.3. A pair of coupled quantum dots containing one electron per dot. Electrons in the semiconductor heterostructure are confined to the xy plane. The spins of the electrons in dots 1 and 2 are denoted by $\mathbf{S}_1$ and $\mathbf{S}_2$, respectively. The magnetic field B is perpendicular to the plane, i.e., along the z -axis, and the electric field E is in-plane and along the x -axis. The quartic potential is given in Eq. (24.23) and is used to model the coupling of two harmonic wells centered at $(\pm a, 0)$. The exchange coupling J between the spins is a function of B , E , and the inter-dot distance is $2a$.

We now discuss the various terms in Eq. (24.21) one by one. The single-particle Hamiltonian

$$h(\mathbf{r}_i, \mathbf{p}_i) = \frac{1}{2m} \left(\mathbf{p}_i - \frac{e}{c} \mathbf{A}(\mathbf{r}_i) \right)^2 + ex_i E + V(\mathbf{r}_i), \quad (24.22)$$

describes the electron dynamics confined to the xy -plane and $C = e^2/\kappa|\mathbf{r}_1 - \mathbf{r}_2|$ the Coulomb interaction between the two negatively charged electrons with κ denoting the dielectric constant (in GaAs, $\kappa = 13.1$). Here, the interaction can be assumed not to be screened, if the quantum dot diameter is small or comparable to the screening length. The electrons have an effective mass m ($m = 0.067 m_e$ in GaAs) and carry a spin-1/2 $\mathbf{S}_i$. We include a magnetic field $\mathbf{B} = (0, 0, B)$, applied along the z -axis and which couples to the electron charge via the vector potential $\mathbf{A}(\mathbf{r}) = \frac{B}{2}(-y, x, 0)$. We also allow for an electric field E applied in-plane along the x -direction, i.e., along the line connecting the centers of the dots. The simplest analytic model potential that correctly renders the double-well character (including tunneling) of the double-dot potential has the following quartic form:

$$V(x, y) = \frac{m\omega_0^2}{2} \left(\frac{1}{4a^2} (x^2 - a^2)^2 + y^2 \right), \quad (24.23)$$

which is reduced (for $x \approx \pm a$) to two separate harmonic wells of frequency ω_0 , one for each dot, in the limit of large inter-dot distance, i.e., for $2a \gg 2a_B$, where a is half the distance between the centers of the dots, and $a_B = \sqrt{\hbar/m\omega_0}$ is the effective Bohr radius of a single isolated harmonic well. Experimentally, the spectrum of single QDs is very well described by using a parabolic confinement potential, which justifies this form of the potential. We note that in this simplified model, increasing (decreasing) the inter-dot distance is physically equivalent to raising (lowering) the inter-dot barrier, which can be achieved experimentally by, for e.g.,

applying a gate voltage between the dots. Thus, the effect of such gate voltages is described in this model simply by a change of the inter-dot distance $2a$.

The magnetic field B also couples to the electron spins via the Zeeman term $H_Z = g\mu_B \sum_i \mathbf{B}_i \cdot \mathbf{S}_i$, where g is the effective g -factor ($g \approx -0.44$ for GaAs), and μ_B the Bohr magneton. The ratio between the Zeeman splitting and the relevant orbital energies is small for all B -values of interest here; indeed, $g\mu_B B/\hbar\omega_0 \lesssim 0.03$, for $B \ll B_0 = (\hbar\omega_0/\mu_B)(m/m_e) \approx 3.5$ T, and $g\mu_B B/\hbar\omega_L \lesssim 0.03$, for $B \gg B_0$, where $\omega_L = eB/2mc$ is the Larmor frequency, and where we used $\hbar\omega_0 = 3$ meV. Thus, we can safely ignore the Zeeman splitting when we discuss the orbital degrees of freedom and include it later into the effective spin Hamiltonian.

We will now discuss two approximations which allow us to determine the exchange coupling J from the model (24.21). First, we introduce the *Heitler–London* (HL) approximation, also known as valence orbit approximation, and then refine this approach by including hybridization as well as double occupancy in a *Hund–Mulliken* (HM) approach, which will finally lead us to an extension of the standard *Hubbard* description for electron hopping and on-site interaction on a lattice. We will see, however, that the qualitative features of J as a function of the control parameters are already captured by the simplest HL approximation.

24.3.2.1 The Heitler–London approach

The HL approximation has its origin in molecular physics: we can think of our double-dot systems as a hydrogen molecule H_2 . In the HL approach, we start from single-dot ground-state (s wave) orbital wavefunctions $\varphi(\mathbf{r})$ and combine them into the (anti-) symmetric two-particle orbital state vectors

$$|\Psi_{\pm}\rangle = \frac{|12\rangle \pm |21\rangle}{\sqrt{2(1 \pm S^2)}}, \quad (24.24)$$

the positive (negative) sign corresponding to the spin singlet (triplet) state, and $S = \langle 2|1\rangle = \int d^2r \varphi_{+a}^*(\mathbf{r})\varphi_{-a}(\mathbf{r})$ denoting the overlap of the right and left orbitals. A nonvanishing overlap implies that the electrons tunnel between the dots (see also Section 24.3.2.3). Here, $\varphi_{-a}(\mathbf{r}) = \langle \mathbf{r}|1\rangle$ and $\varphi_{+a}(\mathbf{r}) = \langle \mathbf{r}|2\rangle$ denote the one-particle orbitals centered at $\mathbf{r} = (\mp a, 0)$, and $|ij\rangle = |i\rangle|j\rangle$ are two-particle product states. The exchange energy is then obtained through $J = \epsilon_t - \epsilon_s = \langle \Psi_- | H_{\text{orb}} | \Psi_- \rangle - \langle \Psi_+ | H_{\text{orb}} | \Psi_+ \rangle$. The single-dot orbitals for harmonic confinement in two dimensions in a perpendicular magnetic field are the Fock-Darwin states which are the usual harmonic oscillator states, magnetically compressed by a factor $b = \omega/\omega_0 = \sqrt{1 + \omega_L^2/\omega_0^2}$, where $\omega_L = eB/2mc$ denotes the Larmor frequency. The ground state with energy $\hbar\omega = b\hbar\omega_0$, centered at the origin, is $\varphi(x, y) = \sqrt{m\omega/\pi\hbar} \exp[-m\omega(x^2 + y^2)/2\hbar]$. Shifting the single-particle orbitals to $(\pm a, 0)$ in the presence of a magnetic field, we obtain $\varphi_{\pm a}(x, y) = \exp(\pm iya/2l_B^2)\varphi(x \mp a, y)$, where the phase factor involving the magnetic length $l_B = \sqrt{\hbar c/eB}$ is due to the gauge transformation $\mathbf{A}_{\pm a} = B(-y, x \mp a, 0)/2 \rightarrow \mathbf{A} = B(-y, x, 0)/2$. Splitting the Hamiltonian (24.21) according to $H = \sum_i h_i^0 + W + C$, where h_i^0 is the single-electron Hamiltonian of a parabolic quantum dot at site i , we obtain [16]

$$J = \frac{2S^2}{1 - S^4} \left(\langle 12 | C + W | 12 \rangle - \frac{\text{Re} \langle 12 | C + W | 21 \rangle}{S^2} \right), \quad (24.25)$$

with the overlap integral $S = \exp(-m\omega a^2/\hbar - a^2\hbar/4l_B^4 m\omega)$. Evaluation of the matrix elements of C and W yields

$$J = \frac{\hbar\omega_0}{\sinh(2d^2(2b - \frac{1}{b}))} \left[c\sqrt{b} \left(e^{-bd^2} I_0(bd^2) - e^{d^2(b-1/b)} I_0 \left(d^2 \left\{ b - \frac{1}{b} \right\} \right) \right) + \frac{3}{4b} (1 + bd^2) \right], \quad (24.26)$$

where $d = a/a_B$ is the dimensionless distance and I_0 is the zeroth-order Bessel function. The first and second term in Eq. (24.26) are due to the Coulomb interaction C , where the exchange term enters with a minus sign. We have introduced the parameter $c = \sqrt{\pi/2}(e^2/\kappa a_B)/\hbar\omega_0$ (≈ 2.4 , for $\hbar\omega_0 = 3$ meV) as the ratio between Coulomb and confining energy. The last term in (24.26) has its origin in the confinement potential W . We plot the exchange coupling $J(B)$ in Fig. 24.4 (dashed line). As we have anticipated above, the ground state at $B = 0$ is a singlet (thus $J > 0$). However, we also see here that the singlet need not be the ground state for finite magnetic fields. In fact, in our example, $J(B)$ changes sign from positive to negative at $B = B_*^s$. This singlet–triplet crossing occurs over a wide range of parameters c and a . At $\hbar\omega_0 = 3$ meV ($c = 2.42$) and $d = 0.7$, the singlet–triplet crossing occurs at about $B_*^s = 1.3$ T. The transition from antiferromagnetic ($J > 0$) to ferromagnetic ($J < 0$) spin–spin coupling with increasing magnetic field is caused by the long-range Coulomb interaction, in particular by the negative exchange term, the second term in Eq. (24.26). As $B \gg B_0$ (≈ 3.5 T for $\hbar\omega_0 = 3$ meV), the magnetic field compresses the orbits by a factor $b \approx B/B_0 \gg 1$ and thereby reduces the overlap of the wavefunctions, $S^2 \approx \exp(-2d^2(2b - 1/b))$, exponentially strongly. Similarly, the overlap decays exponentially for large inter-dot distances, $d \gg 1$. There is a subtlety regarding this exponential suppression, however, namely that it is partly compensated by the exponentially growing exchange term $\langle 12|C|21 \rangle / S^2 \propto \exp(2d^2(b - 1/b))$. As a result, the exchange coupling J decays exponentially as $\exp(-2d^2b)$ for large b or d , as shown in Fig. 24.5b for $B = 0$ ($b = 1$). What is important for quantum gate operations is that the exchange coupling J can be tuned through zero and then suppressed to zero by a magnetic field in a very efficient way.

24.3.2.2 Limitations and extensions of the Heitler–London approach

The HL approximation breaks down explicitly (i.e., J becomes negative even when $B = 0$) for some values of the inter-dot distance if the interaction becomes too strong. For the choice of parameters made above, this happens as c exceeds ≈ 2.8 .

Several improvements of the HL method are possible—we discuss two such improvements that have been studied for the double quantum dot case.

1. *sp-hybridization*: The HL approximation can be improved by taking into account more than just the lowest single-dot orbital. Admixture of higher orbitals can be taken into account using a variational approach; the orbitals obtained in this way are termed *hybridized* orbitals, in analogy to hybridized molecular orbitals in chemistry. We plot the result of a calculation using sp-hybridized quantum dot orbitals in Fig. 24.4.

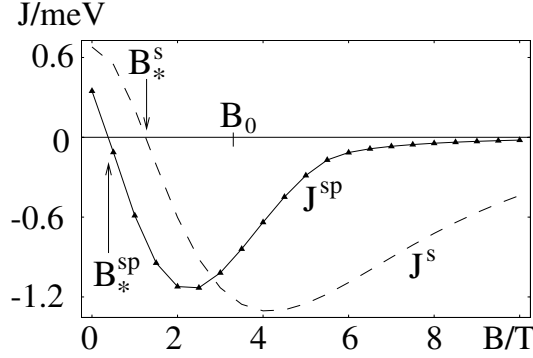


Figure 24.4. Exchange energy J (in meV) as a function of the magnetic field B (Tesla), as obtained from the s-wave Heitler–London approximation (dashed line), Eq. (24.26). Triangles: improved sp-hybridized HL approximation (with solid line). The crossover to magnetically dominated confining is denoted $B_0 = (\hbar\omega_0/\mu_B)(m/m_e)$. The parameters for these plots are $\hbar\omega_0 = 3$ meV (Coulomb parameter $c = 2.42$) and $a = 0.7 a_B$.

2. *Hund–Mulliken approximation:* The HL approximation is restricted to QDs that are occupied with a single electron. Even with a single orbital per site, the Pauli principle allows for the presence of a second electron with opposite spin on a QD orbital. This admixture of double occupancy is suppressed by the repulsive Coulomb interaction between electrons, thus justifying the HL approximation (to some degree). However, it is better to take the two doubly occupied states into account explicitly. This is done in the Hund–Mulliken (molecular orbit) approximation which we discuss in the next section.

24.3.2.3 The Hund–Mulliken approach and the Hubbard Limit

In the Hund–Mulliken (HM) or molecular orbit approximation, the HL approach is extended by including also the two doubly occupied states. Due to the Pauli principle, these additional states have to be spin singlets [16]. In this manner, we have enlarged the orbital Hilbert space from two to four dimensions. In order to write down a HM model, we first need to orthonormalize the single-particle states. This yields the states $\Phi_{\pm a} = (\varphi_{\pm a} - g\varphi_{\mp a})/\sqrt{1 - 2Sg + g^2}$, where S again denotes the overlap of φ_{-a} with φ_{+a} and $g = (1 - \sqrt{1 - S^2})/S$. Diagonalizing

$$H_{\text{orb}} = 2\epsilon + \begin{pmatrix} U & X & -\sqrt{2}t_H & 0 \\ X & U & -\sqrt{2}t_H & 0 \\ -\sqrt{2}t_H & -\sqrt{2}t_H & V_+ & 0 \\ 0 & 0 & 0 & V_- \end{pmatrix} \quad (24.27)$$

in the space spanned by $\Psi_{\pm a}^d(\mathbf{r}_1, \mathbf{r}_2) = \Phi_{\pm a}(\mathbf{r}_1)\Phi_{\pm a}(\mathbf{r}_2)$, $\Psi_{\pm}^s(\mathbf{r}_1, \mathbf{r}_2) = [\Phi_{+a}(\mathbf{r}_1)\Phi_{-a}(\mathbf{r}_2) \pm \Phi_{-a}(\mathbf{r}_1)\Phi_{+a}(\mathbf{r}_2)]/\sqrt{2}$, we obtain the eigenvalues $\epsilon_{s\pm} = 2\epsilon + U_H/2 + V_{\pm} \pm \sqrt{U_H^2/4 + 4t_H^2}$, $\epsilon_{s0} = 2\epsilon + U_H - 2X + V_+$ (singlet), and $\epsilon_t = 2\epsilon + V_-$ (triplet), where the quantities U_H , t_H ,

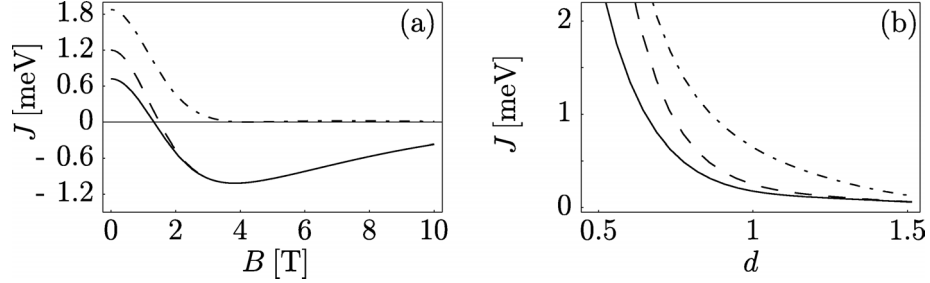


Figure 24.5. Exchange coupling J from HM (full line), Eq. (24.28), and from the extended Hubbard approximation (dashed line), Eq. (24.29). For comparison, we also plot the usual Hubbard approximation where the long-range interaction term V is omitted, i.e., $J = 4t_H^2/U_H$ (dashed-dotted line). In (a), J is plotted as a function of the magnetic field B at fixed inter-dot distance ($d = a/a_B = 0.7$), and for $c = 2.42$, in (b) as a function of inter-dot distance $d = a/a_B$ at zero field ($B = 0$), and again $c = 2.42$. For these parameter values, the s-wave HL J , Eq. (24.26), and the HM J (full line) are almost identical.

X , and $V_{\pm}$ are given in [16]. The exchange energy then becomes

$$J = \epsilon_t - \epsilon_{s-} = V - \frac{U_H}{2} + \frac{1}{2} \sqrt{U_H^2 + 16t_H^2}. \quad (24.28)$$

For short-range Coulomb interactions (and in the absence of a magnetic field), J reduces to $-U/2 + \sqrt{U^2 + 16t^2}/2$, where t denotes the hopping matrix element, and U the on-site repulsion. Thus, t_H and U_H are the generalized hopping matrix element and the on-site repulsion in an extended Hubbard model, renormalized by long-range Coulomb interactions. The remaining two singlet energies ϵ_{s+} and ϵ_{s0} are separated from ϵ_t and ϵ_{s-} by a gap of order U_H and are therefore neglected for the study of low-energy properties. Typically, the “Hubbard ratio” t_H/U_H is less than 1, e.g., if $d = 0.7$, $\hbar\omega_0 = 3$ meV, and $B = 0$, we obtain $t_H/U_H = 0.34$, and this ratio decreases with increasing B . Therefore, we are in an *extended* Hubbard limit, where J takes the form

$$J = \frac{4t_H^2}{U_H} + V. \quad (24.29)$$

The first term in Eq. (24.29) corresponds to the standard Hubbard approximation but with t_H and U_H being renormalized by long-range Coulomb interactions. The V term is of long-range Coulomb nature; it accounts for the difference in Coulomb energy between the singly occupied singlet and triplet states $\Psi_{\pm}^s$. It is the V term that makes J negative for high magnetic fields, whereas $t_H^2/U_H > 0$ for all values of B (see Fig. 24.5a). Thus, the usual Hubbard approximation (i.e., without V) would not give reliable results, neither for the B -dependence (Fig. 24.5a) nor for the dependence on the inter-dot distance a (Fig. 24.5b).

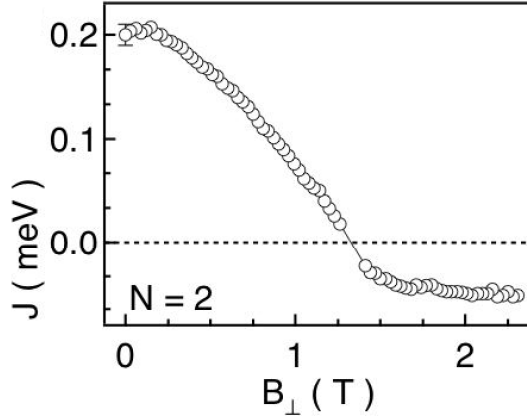


Figure 24.6. Exchange coupling J measured as a function of magnetic field $B_{\perp}$ using conductance spectroscopy in a two-electron dot system defined in a GaAs/AlGaAs heterostructure. There are signatures that due to the elongated dot shape, a double has been formed although a single dot structure was used [20]. The dot spectra appear to be consistent with a parabolic potential with harmonic energies $\hbar\omega_a = 1.2$ meV and $\hbar\omega_b = 3.3$ meV, corresponding to a spatial elongation of $\sqrt{\omega_b/\omega_a} \sim 1.6$. (Figure courtesy of Zumbühl [20]).

24.3.2.4 Numerical work

The calculations we have discussed so far take into account only the ground-state orbital in each QD, with the exception of the sp-hybridized HL, where two additional p-orbitals are included. The HM can be refined by including a number of higher QD orbitals as well. Refined calculations of this type are usually done numerically, and are very closely related to Hartree-Fock (HF) calculations. However, HF is not sufficient for the purpose of calculating a spin-exchange coupling J , because it is not capable of including entangled (quantum correlated) states such as the spin singlet or $m = 0$ triplet. This is typically remedied by invoking the so-called configuration-interaction (CI) method which includes linear superpositions of HF states. Numerical studies of the double-dot system with one and three electrons per QD showed good agreement with the somewhat more crude approximations discussed above [9].

24.3.2.5 Measurements of quantum dot exchange

Signatures of singlet-triplet crossings have been observed using transport spectroscopy in lateral GaAs quantum dot structures [20] (see Fig. 24.6). Although a single elongated dot structure was used, there are signatures that a double dot was formed in the experiment [7]. These data seem to be in rather good qualitative agreement with theory [16], bearing in mind that the absolute magnitude of the exchange coupling J strongly depends on the inter-dot distance which is a free parameter of the theory. Similar double-dot experiments with the double-dot systems shown in Fig. 24.2 are in preparation.

24.3.3 Semiconductor microcavities

The proposal for spin-based quantum computation as presented in Section 24.3 makes use of the exchange coupling which arises when electrons are allowed to tunnel from one to the adjacent quantum dot [2]. Note that this scheme is universal for quantum computing despite the locality of the physical exchange interaction. In particular, arbitrary remote pairs of spins can be coupled by using the exchange coupling to swap spins and bring two distant spins into proximity. There is a modification of this original scheme in which the proximity of two spins is not required even at a physical level, because the interaction is mediated by a resonant mode of an electromagnetic cavity [13]. The control of this interaction and single-qubit operations are achieved using focused laser fields applied to the quantum dots.

The scheme is based on doped QDs that are embedded in a semiconductor microcavity (typically of the size of $\approx \mu\text{m}$) which can reach very high quality factors nowadays ($Q > 10,000$). Because of the strong z -axis confinement, the lowest energy eigenstates of a QD in a semiconductor with zinc blende crystal structure (e.g., GaAs or InAs) consist of $|m_z = \pm 1/2\rangle$ conduction-band states and $|m_z = \pm 3/2\rangle$ valence-band states. The QDs are doped such that each QD has a full valence band and a single conduction band electron: it is assumed that a uniform magnetic field along the x -direction (B_x) is applied, so the qubit is defined by the conduction-band states $|m_x = -1/2\rangle = |\downarrow\rangle$ and $|m_x = 1/2\rangle = |\uparrow\rangle$.

24.3.3.1 Single-qubit operations

In this scheme, single-qubit operations are carried out by applying two lasers, polarized along the x - and y -directions, that exactly satisfy the Raman-resonance condition between $|\downarrow\rangle$ and $|\uparrow\rangle$. The laser fields are turned on for a short time duration that satisfies a π/r -pulse condition, where r is any real number. The process can be best understood as a Raman π/r -pulse for the *hole* in the conduction band state. The laser field polarizations should have nonparallel components to create a nonzero Raman coupling.

24.3.3.2 Two-qubit operations

The two-qubit operations are mediated by virtual photons that are emitted to and reabsorbed from the microcavity field. It is assumed that the x -polarized cavity-mode with energy ω_{cav} ($\hbar = 1$) and a y -polarized laser field establish the Raman transition between the two conduction-band states, in close analogy with the atomic cavity-QED schemes. For a single QDs, the Hamiltonian is brought into the form $H = H_0 + H_{\text{int}}$, with

$$H_0 = \sum_{\sigma=\uparrow,\downarrow,\pm 3/2} \omega_{\sigma} e_{\sigma}^{\dagger} e_{\sigma} + \omega_{\text{cav}} a_{\text{cav}}^{\dagger} a_{\text{cav}} + \omega_L a_L^{\dagger} a_L, \quad (24.30)$$

where $e_{\uparrow,\downarrow}$ annihilates an electron with spin $\uparrow, \downarrow$ along the x -direction in the conduction band and $e_{\pm 3/2}$ annihilates an electron with spin $\pm 3/2$ along the z -direction in the valence band. The light-matter interaction has the form

$$H_{\text{int}} = g \left(a_+^{\dagger} e_{-3/2}^{\dagger} e_{-1/2} - a_-^{\dagger} e_{3/2}^{\dagger} e_{1/2} + h.c. \right), \quad (24.31)$$

where g is the dipole interaction strength, $e_\sigma^\dagger$ and e_σ the electron creation and annihilation operators in the conduction and valence band, and $a_{cav,L}^\dagger$, $a_{cav,L}$ denote the cavity and laser mode photon creation and annihilation operators. All the photon and electronic degrees of freedom, except the electron spins in the conduction band can be eliminated in the case of two quasi-resonant QDs by a series of formal manipulations [9, 13], with the resulting two-spin Hamiltonian

$$H_{\text{int}}^{(2)} = \sum_{i \neq j} \tilde{g}_{ij}(t) \left[\sigma_{\uparrow\downarrow}^i \sigma_{\downarrow\uparrow}^j e^{i\Delta_{ij}t} + \sigma_{\uparrow\downarrow}^j \sigma_{\downarrow\uparrow}^i e^{-i\Delta_{ij}t} \right], \quad (24.32)$$

where $\tilde{g}_{ij}(t) = g_{\text{eff}}^i(t)g_{\text{eff}}^j(t)/\Delta_i$, $\Delta_{ij} = \Delta_i - \Delta_j$, and $\Delta_i = \omega_{\uparrow\downarrow}^i - \omega_{cav} + \omega_L^i = \Delta_j \ll \omega_{\uparrow\downarrow}^{i,j}$. We have already discussed the implementation of the CPF and the CNOT or quantum XOR gates between two spins i and j from a transversal (XY) spin coupling of the form (24.32) in Section 24.2.2. The interaction Hamiltonian $H_{\text{int}}^{(2)}$ describes the coupling of the QD spins via the following virtual process. One of the QDs emits a virtual photon into the cavity while absorbing a laser photon. The cavity photon is then reabsorbed by the other dot while a laser photon is emitted. Due to the spin splitting in the dot spectrum, this process is spin sensitive and leads to the spin–spin coupling $H_{\text{int}}^{(2)}$ between the QDs.

24.3.3.3 Measurement

Measurement of an individual quantum dot spin in the cavity QED scheme can be achieved by applying a laser field to the QD to be measured, in order to realize exact two-photon resonance with the cavity mode. If the QD spin is in state $|\downarrow\rangle$, there is no Raman coupling and no photons will be detected. If on the other hand, the spin state is $|\uparrow\rangle$, the electron will exchange energy with the cavity mode and eventually a single photon will be emitted from the cavity. A single photon detection capability is thus sufficient for detecting a single spin.

24.3.4 Decoherence

Thus so far, we have been content with showing that universal quantum computing is feasible in principle with the present physical resources. However, we cannot assume that the spin of the electron remains coherent for arbitrarily long times. The spin coherence time in semiconductors—the time over which the phase of a superposition of spin-up and spin-down states $\alpha|\uparrow\rangle + \beta|\downarrow\rangle$ is well-defined—can be much longer than the charge coherence time (the latter typically being a few nanoseconds at sufficiently low temperatures). This is of course one of the reasons for using spin as a qubit [2] rather than charge. In bulk GaAs the ensemble spin coherence time T_2^* , being a lower bound on the single-spin decoherence time T_2 , was measured using a technique called time-resolved Faraday rotation [18]. The spin decoherence time T_2 in confined systems (e.g., QDs) may actually be shorter than in extended systems, due to the absence of “motional narrowing” for localized electrons [8].

The spin relaxation time T_1 in a single-electron QD in a GaAs heterostructure was probed via transport measurements and found to approach 1 μs [21, 22]. It has been proposed to also measure the single-spin T_2 in such a structure in a transport experiment by applying electron spin resonance (ESR) techniques [19]. In this scheme, the stationary current exhibits a resonance whose line width is determined by the single-spin decoherence time T_2 .

24.3.4.1 Phonons and the spin–orbit coupling

The interaction of a confined electron spin with lattice phonons via the spin–orbit interaction can lead to transitions between different discrete energy levels (or Zeeman sublevels) in GaAs quantum dots that can cause spin flips and therefore spin decoherence (see [8, 9] and references therein). Various mechanisms are known, originating from the spin–orbit coupling, which lead to such spin flip processes. The most relevant mechanisms in 2D have to do with the broken inversion symmetry, either in the elementary crystal cell or at the heterointerface. The spin-orbit Hamiltonian for the electron in such a structure is given by Eq. (24.12). The spin relaxation rate $\Gamma = T_1^{-1}$ can be evaluated in leading perturbation order in this coupling, with and without a magnetic field. The spin–orbit coupling H_{so} mixes the spin-up and spin-down states of the electron and leads to a nonvanishing matrix element of the phonon-assisted transition between two states with opposite spins. However, the spin relaxation of electrons localized in a QD differs strongly from that of delocalized electrons. It turns out that in quantum dots (in contrast to extended 2D states), the contributions to the spin-flip rate proportional to β^2 are absent. This reduces the spin-flip rates of electrons confined to dots to a large extent. The finite Zeeman splitting in the energy spectrum also leads to contributions $\propto \beta^2$,

$$\Gamma \simeq \Gamma_0(B) \left(\frac{m\beta^2}{\hbar\omega_0} \right) \left(\frac{g\mu_B B}{\hbar\omega_0} \right)^2, \quad (24.33)$$

where $\hbar\omega_0$ is the orbital energy level splitting in the QD and $\Gamma_0(B)$ is the inelastic rate without spin flip for the transition between neighboring orbital levels.

Spin-flip transitions between Zeeman sublevels occur with a rate that is proportional to the fifth power of the Zeeman splitting,

$$\Gamma_z \simeq \frac{(g\mu_B B)^5}{\hbar(\hbar\omega_0)^4} \Lambda_p. \quad (24.34)$$

The dimensionless constant $\Lambda_p \propto \beta^2$ characterizes the strength of the effective spin–piezo-phonon coupling in the heterostructure and ranges from $\approx 7 \cdot 10^{-3}$ to $\approx 6 \cdot 10^{-2}$ depending on β . As an example, $\Gamma_z \approx 1.5 \cdot 10^3 \text{ s}^{-1}$ for $\hbar\omega_0 = 10 \text{ K}$ and at a magnetic field $B = 1 \text{ T}$. It was found that under realistic and quite general conditions, a symmetry argument leads to the conclusion that the spin decoherence time T_2 has only transverse contributions (in leading order), in other words, $T_2 = 2T_1$ for spin-orbit (phonon) related processes [8].

24.3.4.2 Nuclear spins

The hyperfine interaction between an electron spin and the spins of the surrounding atomic nuclei is another source of electron spin decoherence. A rough estimate of the strength of this effect based on perturbation theory [16] suggests that the rate of such processes can be suppressed by either polarizing the nuclear spins or by applying an external magnetic field. The suppression factor is $(B_n^*/B)^2/N$, where $B_n^* = AI/g\mu_B$ is the maximal magnitude of the effective nuclear field (Overhauser field), N the number of nuclear spins in the vicinity of the electron, and A the hyperfine coupling constant. In GaAs, the nuclear spin of both Ga and As is $I = 3/2$. The field B denotes either the external field, or, in the absence of an external

field, the Overhauser field $B = pB_n^*$ due to the nuclear spin polarization p , which can be obtained by optical pumping or by spin-polarized currents at the edge of a 2DEG. In the latter case, the suppression of the spin flip rate becomes $1/p^2N$.

A detailed calculation (see [8] for a review) shows that the electron spin decoherence time T_2 is shorter than the nuclear spin relaxation time T_{n2} determined by the dipole–dipole interaction between nuclei, and therefore the problem can be considered in the absence of the nuclear dipole–dipole interaction. Since the hyperfine interaction depends on the position via a factor $|\psi(\mathbf{r})|^2$ where $\psi(\mathbf{r})$ is the electron wavefunction, the value of the hyperfine interaction varies spatially. It turns out that this is the relevant cause of decoherence. The analysis is complicated by the fact that in a weak external Zeeman field (smaller than a typical fluctuating Overhauser field seen by the electron, ~ 100 Gauss in a GaAs QD), the perturbative treatment of the electron spin decoherence breaks down and the decay of the spin precession amplitude is not exponential in time, but either described by a power law, $1/t^{d/2}$ (for finite Zeeman fields) or an inverse logarithm, $1/(\ln t)^{d/2}$ (for vanishing fields).

The decoherence rate $1/T_2$ is thus roughly given by $A/\hbar N$, where A is the hyperfine interaction constant, and N is the number of nuclei within the dot, with N typically $\approx 10^5$. This time is of the order of several μs . However, it needs to be stressed that there is no simple exponential decay which, strictly speaking, means that decoherence cannot simply be characterized by the decay times T_1 and T_2 in this case. The case of a fully polarized nuclear spin state was solved exactly [8]. The amplitude of the precession which is approached after the decay is of the order one, while the decaying part is $1/N$, in agreement with earlier results [16]. A large difference between the values of T_2 (decoherence time for a single dot) and T_2^* (dephasing time for an ensemble of dots), i.e., $T_2^* \ll T_2$ is found and indicates that it is desirable to have direct experimental access to single spin decoherence times.

24.4 Superconducting Qubits

Superconducting (SC) qubits are quantum-coherent electric circuits. This means that it is not sufficient for the individual charge carriers to preserve phase coherence, as in coherent transport in a normal conductor; the *macroscopic* degrees of freedom, charges and fluxes, of the circuit must behave quantum mechanically. Since dissipation-free electric transport is a necessary condition for quantum phase coherence, the materials of choice are superconductors (e.g., aluminum or niobium). Linear circuits will typically give rise to harmonic behavior, i.e., a spectrum of equidistant levels. In order to obtain a two-level system whose levels are split far from higher excitations, it is necessary to add a nonlinear element. In SC qubits, this role is played by Josephson junctions in which two SC pieces are joined by a very thin oxide (non-SC) layer which still allows a SC current to flow between the two SCs. The typical size of such SC circuits with Josephson junctions is around one or a few micrometers.

24.4.1 Regimes of operation

The SC qubits can be grouped into three classes: The SC charge (charge box) qubits operating in the regime $E_C \gg E_J$, and the SC flux (persistent current) qubits operating in the regime $E_J \gg E_C$, are distinguished by their Josephson junctions' relative magnitude of charging

energy E_C and Josephson energy E_J . The SC phase qubits operate in the same regime as the flux qubit, but are represented purely by the SC phase and are not associated with any macroscopic magnetic flux or circulating current. The different SC qubit types are described in detail in a couple of excellent review articles [10, 11].

In the flux systems, the qubit is stored in the SC phase differences across the Josephson junctions in the circuit, whereas in charge systems, the qubit is stored in the presence or absence of an extra Cooper pair on a small SC island. A micrograph of the circuit for a SC flux qubit studied in [23] is shown in Fig. 24.7.

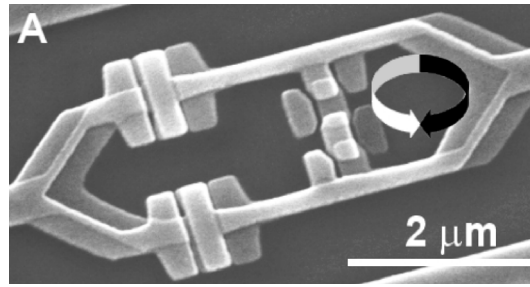


Figure 24.7. The SC flux qubit circuit studied in [23] in a scanning electron micrograph image. The logical qubit basis states correspond to circulating SC currents in the smaller loop as indicated. The bright areas are the Al wires; the double-layer structure from the shadow evaporation deposition is clearly visible. (Figure courtesy of I. Chiorescu and J. E. Mooij, TU Delft).

SC qubits can be approximately described by the pseudo-spin model [10],

$$H = \frac{\Delta}{2}\sigma_x + \frac{\epsilon}{2}\sigma_z, \quad (24.35)$$

where Δ denotes the tunnel coupling between the two qubit states $|0\rangle$ and $|1\rangle$ (eigenstates of σ_z) and ϵ the bias (asymmetry). This model is equivalent to an asymmetric double well, see Fig. 24.8. In Section 24.4.2.4, a more general model, including the full Hilbert space of a SC circuit, will be discussed.

24.4.2 Decoherence, visibility, and leakage

24.4.2.1 Decoherence

We will mostly be concerned with questions related to SC qubit decoherence here. Consider a situation where the qubit is initially prepared in state $|0\rangle$, i.e., in the left well in Fig. 24.8. As it evolves under the influence of the Hamiltonian (24.35), it will undergo free Larmor oscillations with frequency $\nu = \hbar^{-1}\sqrt{\Delta^2 + \epsilon^2}$. Ideally, the probability for finding the qubit in state $|0\rangle$ again after time t would be a cosine function $p(t) = (1 + \cos(2\pi\nu t))/2$ which is plotted as a thin dotted line in Fig. 24.8. Such a Larmor precession experiment (also known as Ramsey fringe experiment) determines to what extent the qubit is quantum phase coherent. Decoherence is a process in which the amplitude of the oscillations decays over time, as

shown by the thick solid line in Fig. 24.8 (the respective experimental data for a SC flux qubit can be found in [23]). This decay is often (but not always) exponential with a characteristic decoherence time T_2 .

All types of SC qubits suffer from decoherence that is caused by a number of sources. Decoherence in charge qubits can be understood within the spin-boson model, based on the two-level model (24.35) coupled to a bath of harmonic oscillators [10]. A systematic theory of decoherence of a qubit from such dissipative elements, based on the network graph analysis [24] of the underlying SC circuit, was developed for SC flux qubits [25], and applied to study the effect of asymmetries in a persistent-current qubit [26]. The circuit theory for SC qubits will be discussed further below in Section 24.4.2.4.

24.4.2.2 Visibility

In Fig. 24.8, we also show another type of imperfection that typically affects SC qubits: a limited visibility v . This means that the maximum range v of the read-out probability of the qubit being in state $|0\rangle$ is smaller than one. The probability $p(0)$ of measuring the qubit in state $|0\rangle$ immediately after preparation in this state is less than one. In the case of a symmetric reduction of the visibility, the relation is $p(0) = (1 + v)/2$.

24.4.2.3 Leakage

One possible mechanism leading to a reduced visibility, is *leakage*. Since the SC phase is a continuous variable as, e.g., the position of a particle, superconducting qubits (two-level

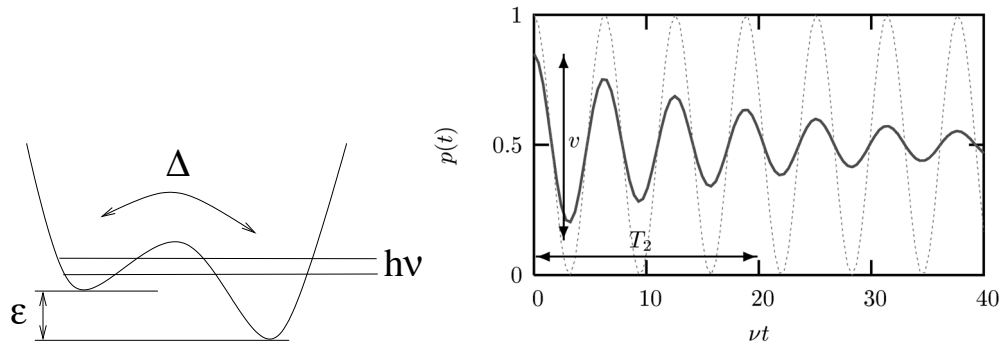


Figure 24.8. Left: The simplest model of a SC qubit consists of a biased double well with tunnel coupling Δ and asymmetry ϵ . The energy splitting of the two lowest eigenstates is then given by $h\nu = \sqrt{\Delta^2 + \epsilon^2}$. Right: Theoretical Larmor precession (Ramsey fringe) curve with decoherence time $T_2 < \infty$ and limited visibility $v < 1$ (solid thick line), compared to the ideal curve (dotted thin line). The probability $p(t)$ to find the qubit in state $|0\rangle$ is plotted as a function of the free evolution time t . The Larmor frequency of the coherent oscillations is denoted by ν . The *visibility* v is the maximum range of $p(0)$ whereas the *decoherence time* T_2 is the time over which the oscillations are damped out (in the case of an exponential decay). For this plot, we have chosen the parameters $T_2 = 20/\nu$ and $v = 70\%$.

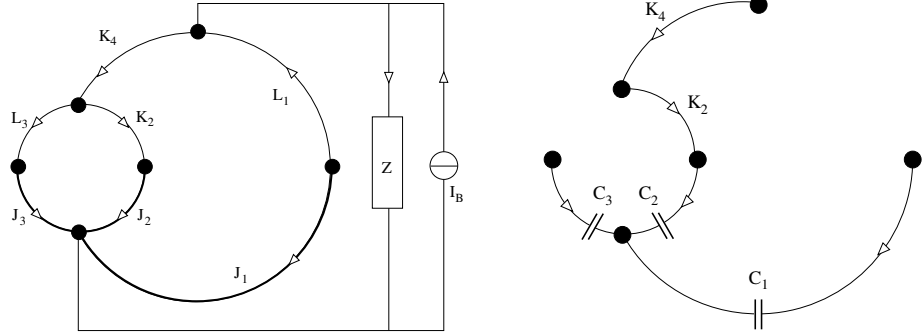


Figure 24.9. An example of a circuit graph (left) and a tree of the same graph (right). The branches represent electrical elements, such as capacitors (C), Josephson junctions (J), inductors (L, K), impedances (Z), and current sources (I_B). The tree is a subgraph containing all nodes but no closed loops.

systems) have to be obtained by truncation of an infinite-dimensional Hilbert space. This truncation is not exact for the following reasons: (i) because it may not be possible to prepare the initial state with perfect fidelity in the lowest two states, (ii) because of erroneous transitions to higher levels (leakage effects) due to imperfect gate operations on the system, and (iii) because of erroneous transitions to higher levels due to the unavoidable interaction of the system with the environment. Apparent leakage effects may also occur if the read-out process has a finite failure probability (i.e., gives the outcome 0 if the qubit was in state $|1\rangle$ and vice versa). Leakage effects due to the nonadiabaticity of externally applied fields were studied in [27]. Recent work [28] shows that leakage in microwave-driven Josephson phase qubits leading to a reduced visibility can occur, even if the microwave source is pulsed slowly.

24.4.2.4 Circuit theory

We will now discuss a theoretical description of superconducting circuits based on the network graph method that goes beyond the two-level (pseudospin) description (24.35). This method allows one to systematically find the Hamiltonian of both simple and complex SC circuits, starting from their circuit graph. Combined with a theory of dissipative quantum systems such as the Caldeira–Leggett model [29], it can then be utilized to describe decoherence in arbitrary SC circuits [25].

First, the *network graph* of the SC circuit is drawn, where each two-terminal element (Josephson junction, capacitor, inductor, external impedance, current source, etc.) is represented as a branch connecting two nodes of the graph. An example of a network graph is shown in Fig. 24.9. Then, a *tree* of the network graph needs to be specified (see Fig. 24.9). A tree of a graph is a set of branches connecting all nodes without containing any loops. Details about the graph method, including the suitable choice of a tree, can be found in [25]. The branches in the tree are called *tree branches*; all other branches are called *chords*. Each chord

is associated with exactly one the so-called fundamental loop that is obtained when adding the chord to the tree.

The purpose of the circuit graph is the systematic representation of Kirchhoff's laws

$$(\mathbb{1} \mid \mathbf{F}) \mathbf{I} = 0, \quad (24.36)$$

$$(-\mathbf{F}^T \mid \mathbb{1}) \mathbf{V} = \dot{\Phi}, \quad (24.37)$$

with the *fundamental loop matrix* $\mathbf{F}$ and the branch current and voltage vectors $\mathbf{I}$ and $\mathbf{V}$. This matrix is composed of sub-matrices (blocks) $\mathbf{F}_{XY}$ corresponding to the various branch types $X, Y = C, L, K, Z, B, J$. The loop sub-matrices $\mathbf{F}_{XY}$ have entries $+1, -1$, or 0 , and hold the information about which tree branches of type X belong to which fundamental loop associated with the chords of type Y . In order to derive the equations of motion and eventually, the Hamiltonian of the SC circuit, Kirchhoff's laws need to be combined with the current–voltage relations (CVRs) of various branch elements. Each branch type has its own CVR, most of them linear (capacitances and inductances, impedances, etc.), except the Josephson junction (J) branches which follow the nonlinear (first) Josephson relation,

$$I_J = I_c \sin(\varphi_1 - \varphi_2), \quad (24.38)$$

where I_c denotes the critical current and $\varphi_{1,2}$ the SC phase at the two nodes 1 and 2 of the circuit that are connected by the corresponding Josephson branch.

24.4.2.5 The Hamiltonian

Kirchhoff's laws and the CVRs combined are sufficient to write down the Hamiltonian of a SC circuit. In the absence of dissipative elements (impedances Z), the Hamiltonian is [25]

$$\mathcal{H}_S = \frac{1}{2} \mathbf{Q}_C^T \mathbf{C}^{-1} \mathbf{Q}_C + \left(\frac{\Phi_0}{2\pi} \right)^2 U(\varphi), \quad (24.39)$$

$$U(\varphi) = - \sum_i \frac{2\pi I_{c,i}}{\Phi_0} \cos \varphi_i + \frac{1}{2} \varphi^T \mathbf{M}_0 \varphi + \frac{2\pi}{\Phi_0} \varphi^T (\mathbf{N} \Phi_x + \mathbf{S} \mathbf{I}_B), \quad (24.40)$$

where $\mathbf{Q}_C$ are the charges conjugate to the fluxes $\Phi_J = (\Phi_0/2\pi)\varphi$, where $\varphi = (\varphi_1, \dots, \varphi_n)$ is a vector containing the SC phase differences across all Josephson branches and $\mathbf{C}$ is the capacitance matrix of the circuit. The matrices $\mathbf{M}_0$, $\mathbf{N}$, and $\mathbf{S}$ are obtained from the inductance and loop matrices $\mathbf{L}_t$ and $\mathbf{F}$ [25]. The theory can be quantized using the commutator relation

$$[\Phi_{J,i}, Q_{C;j}] = \left[\frac{\Phi_0}{2\pi} \varphi_i, Q_{C;j} \right] = i\hbar \delta_{ij}. \quad (24.41)$$

The system including dissipation, in the case of a single impedance Z , can be described using a Caldeira–Leggett model [29] of the form

$$\mathcal{H} = \mathcal{H}_S + \mathcal{H}_B + \mathcal{H}_{SB}, \quad (24.42)$$

$$\mathcal{H}_B = \frac{1}{2} \sum_{\alpha} \left(\frac{p_{\alpha}^2}{m_{\alpha}} + m_{\alpha} \omega_{\alpha}^2 x_{\alpha}^2 \right), \quad (24.43)$$

$$\mathcal{H}_{SB} = \mathbf{m} \cdot \varphi \sum_{\alpha} c_{\alpha} x_{\alpha} + \Delta U(\varphi), \quad (24.44)$$

where $\mathcal{H}_S$ is the quantized Hamiltonian Eq. (24.39), $\mathcal{H}_B$ is the Hamiltonian describing a bath of harmonic oscillators with (fictitious) position and momentum operators x_α and p_α with $[x_\alpha, p_\beta] = i\hbar\delta_{\alpha\beta}$, masses m_α , and oscillator frequencies ω_α . Finally, $\mathcal{H}_{SB}$ describes the coupling between the system and bath degrees of freedom, φ and x_α , where c_α is a coupling parameter and $\mathbf{m}$ are obtained from the inductance and loop matrices $\mathbf{L}_t$ and $\mathbf{F}$ [25]. For the case of several impedances, a Caldeira–Leggett model with more than one bath of harmonic oscillators is required in general [30].

The time evolution of the qubit (dissipation-free SC circuit) and oscillator bath (circuit impedances) is determined by the Liouville equation $\dot{\rho}(t) = -i[\mathcal{H}, \rho(t)]$ for the density matrix ρ of the combined system. The state of the SC qubit alone can be obtained by taking the partial trace over the harmonic oscillator bath to find the reduced density matrix, $\rho_S(t) = \text{Tr}_B \rho(t)$. The time evolution for $\rho_S(t)$ is the *master equation*, which in general is a complicated linear integro-differential equation [29]. In the Born–Markov approximation, the master equation for $\rho_S(t)$ can be written in the relatively simple form of the Redfield equation,

$$\dot{\rho}_{nm}(t) = -i\omega_{nm}\rho_{nm}(t) - \sum_{kl} R_{nmkl}\rho_{kl}(t), \quad (24.45)$$

where $\rho_{nm} = \langle n|\rho_S|m\rangle$ are the matrix elements of ρ_S in the eigenbasis $|n\rangle$ of $\mathcal{H}_S$ (eigenenergies ω_n), and $\omega_{nm} = \omega_n - \omega_m$, and with the Redfield tensor,

$$R_{nmkl} = \delta_{lm} \sum_r \Gamma_{nrrk}^{(+)} + \delta_{nk} \sum_r \Gamma_{lrrm}^{(-)} - \Gamma_{lmnk}^{(+)} - \Gamma_{lmnk}^{(-)}. \quad (24.46)$$

The Redfield equation (24.45) constitutes a description of the dissipative dynamics of the SC circuit in an infinite-dimensional Hilbert space. In some situations, however, it can be more useful to concentrate only on the two eigenstates of $\mathcal{H}_S$ with the lowest energy, corresponding to the qubit $|0\rangle$ and $|1\rangle$ states. Note that such a two-level approximation is sensible only if the leakage rate is small. In the two-dimensional qubit subspace, we can then define the Bloch vector $\mathbf{p} = \text{Tr}(\sigma\rho)$ where $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices. The Redfield equation (24.45) then takes the form of the Bloch equation $\dot{\mathbf{p}} = \boldsymbol{\omega} \times \mathbf{p} - R\mathbf{p} + \mathbf{p}_0$, with $\boldsymbol{\omega} = (0, 0, \omega_{01})^T$. In the secular approximation, the relaxation matrix R becomes diagonal,

$$R = \begin{pmatrix} T_2^{-1} & 0 & 0 \\ 0 & T_2^{-1} & 0 \\ 0 & 0 & T_1^{-1} \end{pmatrix}, \quad (24.47)$$

where T_1 denotes the energy relaxation, $T_2 = (1/2T_1 + 1/T_\phi)^{-1}$ the decoherence, and T_ϕ the pure dephasing time. We have already discussed the physical meaning of the decoherence time T_2 above. The relaxation time T_1 describes the exponential decay of the population of an excited state (say, $|1\rangle$) into thermal equilibrium (at zero temperature, $T = 0$, the ground state $|0\rangle$) due to energy exchange with the environment. From our circuit theory, we obtain

$$\frac{1}{T_1} = 4|\langle 0|\mathbf{m} \cdot \boldsymbol{\varphi}|1\rangle|^2 J(\omega_{01}) \coth \frac{\omega_{01}}{2k_B T}, \quad (24.48)$$

$$\frac{1}{T_\phi} = |\langle 0|\mathbf{m} \cdot \boldsymbol{\varphi}|0\rangle - \langle 1|\mathbf{m} \cdot \boldsymbol{\varphi}|1\rangle|^2 \left. \frac{J(\omega)}{\omega} \right|_{\omega \rightarrow 0} 2k_B T, \quad (24.49)$$

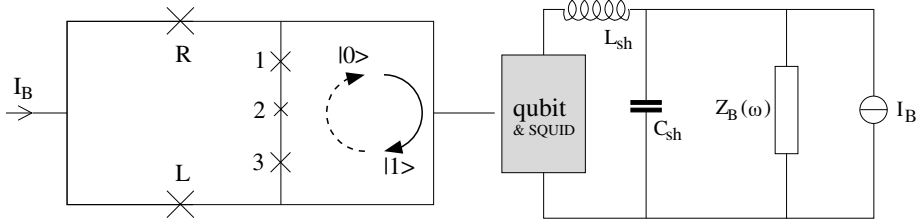


Figure 24.10. Left: Schematic of the Delft circuit, Fig. 24.7, where the crosses denote Josephson junctions. The outer loop with two junctions L and R forms a dc SQUID that is used to read out the qubit. The state of the qubit is determined by the orientation of the circulating current in the small loop, comprising the junctions 1, 2, and 3, one of which has a slightly smaller critical current than the others. A bias current I_B can be applied as indicated for read-out. Right: External circuit attached to the qubit (Fig. 24.10) that allows the application of a bias current I_B for qubit read-out. The inductance L_{sh} and capacitance C_{sh} form the *shell circuit*, and $Z_B(\omega)$ is the total impedance of the current source (I_B). The case where a voltage source is used to generate a current can be reduced to this using Norton's theorem.

where the spectral function is defined as

$$J(\omega) = \frac{\pi}{2} \sum_{\alpha} \frac{c_{\alpha}^2}{m_{\alpha} \omega_{\alpha}} \delta(\omega - \omega_{\alpha}), \quad (24.50)$$

and can be related to the impedance $Z(\omega)$. In the case of small circuit self inductances $L \ll Z(\omega)/\omega$, we find $J(\omega) \approx \omega \text{Re}(1/Z(\omega))$ (for the exact expression, see [25]). In the semiclassical approximation, T_1 and T_{ϕ} can be related to the parameters Δ and ϵ in the Hamiltonian (24.35),

$$\frac{1}{T_1} = \left(\frac{\Delta}{\omega_{01}} \right)^2 |\Delta \varphi \cdot \mathbf{m}|^2 J(\omega_{01}) \coth \frac{\omega_{01}}{2k_B T}, \quad (24.51)$$

$$\frac{1}{T_{\phi}} = \left(\frac{\epsilon}{\omega_{01}} \right)^2 |\Delta \varphi \cdot \mathbf{m}|^2 \left. \frac{J(\omega)}{\omega} \right|_{\omega \rightarrow 0}. \quad (24.52)$$

24.4.2.6 The Delft qubit

We shall now turn to a specific design of a SC flux qubit, the Delft qubit [23] which is shown in Fig. 24.7. Of course, this is one among a number of other types of SC qubits [10, 11], but it will serve as an excellent example for our purpose. The Delft qubit (Fig. 24.10) is designed to be immune against fluctuations in the current bias I_B . Due to its symmetry properties, at zero dc bias, $I_B = 0$, and independently of the applied magnetic field, a small fluctuating current $\delta I_B(t)$ caused by the finite impedance Z of the current source is divided equally into the two arms of the SQUID loop with no net current flowing through the three-junction qubit line. As a consequence, in the ideal circuit (Fig. 24.10) the qubit is protected from decoherence due to bias current fluctuations. Of course, if the symmetry is broken, the protection of the qubit

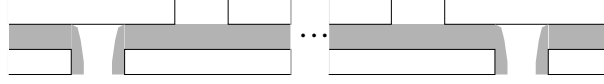


Figure 24.11. Josephson junctions produced by the shadow evaporation technique always connect the upper with the lower aluminum (Al) layer. Shaded regions represent the aluminum oxide (AlOx).

from decoherence will be lost. It turns out in this case that the symmetry is indeed broken, due to the *double layer structure* of the physical device, being an artifact of the fabrication method used to produce SC circuits with Al/AlOx junctions. Such junctions are produced using the *shadow evaporation technique* (Fig. 24.11) and always connect the top with the bottom layer.

When a circuit with an odd number of junctions in a closed loop (such as Fig. 24.10) is fabricated with this technique (Fig. 24.11), the loop must contain an additional (unintended) junction in order to connect the mismatched parts of the loop. In order to analyze the implications of the double layer structure for the circuit in Fig. 24.10, the circuit can be drawn again in Fig. 24.12a with separate upper and lower layers. Note that each piece of the upper layer is connected with the underlying piece of the lower layer via an “unintentional” Josephson junction. These extra junctions typically have large areas and therefore large critical currents; thus, their Josephson energy can often be neglected. In order to study the lowest-order effect of the double layer structure, one can obtain a minimal model (Fig. 24.12b) by approximating all unintentional junctions as shorts. It should be emphasized that the resulting circuit is dis-

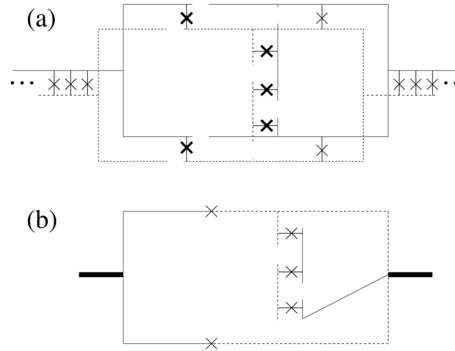


Figure 24.12. (a) Double layer structure of the Delft qubit. Dashed blue lines represent the lower, solid red lines the upper SC layer, and crosses indicate Josephson junctions. Thick crosses denote intended junctions, while thin crosses denote unintended distributed junctions due to the double-layer structure. (b) Minimal circuit model of the double layer structure. The symmetry between the upper and lower arms of the SQUID has been broken by the qubit line comprising three junctions. Thick black lines denote pieces of the SC in which the upper and lower layers are connected by large area junctions.

tinct from the “ideal” circuit (Fig. 24.10), which does not reflect the double-layer structure. In the real circuit, Fig. 24.12b, the symmetry between the two arms of the dc SQUID is broken, and thus it can be expected that bias current fluctuations cause decoherence of the qubit at zero dc bias current, $I_B = 0$.

Now, we can use the circuit theory to find the Hamiltonian of the circuit, taking into account the asymmetry. Numerically, the double-well minima φ_0 and φ_1 can be found for a range of bias currents and applied external flux. (The states localized at φ_0 and φ_1 are encoding the logical $|0\rangle$ and $|1\rangle$ states of the qubit.) Two special lines (drawn in Fig. 24.13) in the plane spanned by the bias currents and applied external flux can now be determined: (i) The line $f^*(I_B)$ on which a *symmetric* double well is predicted, $\epsilon \equiv U(\varphi_0) - U(\varphi_1) = 0$. On this line, the dephasing time T_ϕ diverges. (ii) The line on which $\mathbf{m} \cdot \Delta\varphi = 0$, where $\Delta\varphi = \varphi_0\varphi_1$ is the vector joining the two minima of the potential. Here, the environment is *decoupled* from the system, and both the relaxation and the decoherence times diverge, $T_{1,2,\phi} \rightarrow \infty$. The curve $f^*(I_B)$ agrees qualitatively with the experimentally measured symmetry line [33], but it underestimates the magnitude of the variation in flux f' as a function of I_B . The point where the symmetric and the decoupling lines intersect coincides with the maximum of the symmetric line, as can be understood from the following argument. Taking the total derivative with respect to I_B of the relation $\epsilon = U(\varphi_0; f^*(I_B), I_B) - U(\varphi_1; f^*(I_B), I_B) = 0$ on the symmetric line, and using that $\varphi_{0,1}$ are extremal points of U , we obtain $\mathbf{n} \cdot \Delta\varphi \partial f^* / \partial I_B + (2\pi/\Phi_0) \mathbf{m} \cdot \Delta\varphi = 0$ for some constant vector $\mathbf{n}$. Therefore, $\mathbf{m} \cdot \Delta\varphi = 0$ (decoupling line) and $\mathbf{n} \cdot \Delta\varphi \neq 0$ implies $\partial f^* / \partial I_B = 0$.

The relaxation and decoherence times T_1 and T_2 on the symmetric line $\epsilon = 0$, have been calculated numerically (Fig. 24.13). The agreement with the experimentally measured values [33] is good, in particular, the value of the bias current where the $T_{1,2}$ are longest is in excellent agreement with the experiment (without free fitting parameters). The lowest-order pure dephasing time T_ϕ diverges on the symmetric line; however, this divergence is cut off

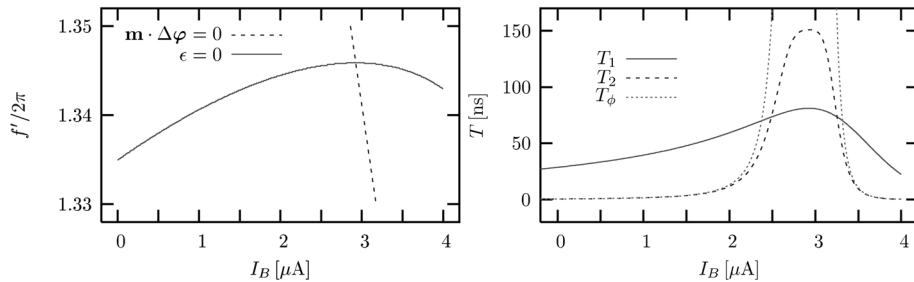


Figure 24.13. Left: Special lines in the (I_B, f') plane of the Delft qubit. The decoupling line ($\mathbf{m} \cdot \Delta\varphi = 0$) is drawn solid red whereas the symmetric line ($\epsilon = 0$) is drawn dashed blue. Here, I_B is the applied bias current and $f' = 2\pi\Phi'_x/\Phi_0$ is the dimensionless externally applied magnetic flux threading the SQUID loop. Both lines can be obtained from a numerical minimization of the potential equation (24.40). Right: Theoretical relaxation, pure dephasing, and decoherence times T_1 , T_ϕ , and T_2 as a function of the applied bias current I_B , along the symmetric line (Fig. 24.13, left).

by higher order effects. The relaxation time T_1 exhibits a divergence on the decoupling line which is cut off by residual impedances, e.g., due to the quasiparticle resistance of the junctions [26]. The asymmetry which is responsible for the reduced T_2 at zero bias $I_B = 0$ can be avoided in a SC circuit with an *even* number of junctions in the qubit loop. Such a modified circuit has been studied experimentally [33], and indeed the maxima of T_1 and T_2 in the four-junction qubit were found to be essentially at $I_B = 0$. The maximal T_1 and T_2 could be increased by over an order of magnitude.

Exercises

1. Controlled-NOT gate with the Heisenberg Hamiltonian

- Write the square-root of SWAP gate S , defined in Eq. (24.3), as a 4-by-4 matrix in the product basis $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle$. Hint: The operator $\mathbf{S}_1 \cdot \mathbf{S}_2$ is diagonal in the singlet-triplet basis (spin eigenbasis) $|T_+\rangle = |\uparrow\uparrow\rangle, |S\rangle = (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)/\sqrt{2}, |T_0\rangle = (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)/\sqrt{2}, |T_-\rangle = |\downarrow\downarrow\rangle$.
- Show that the controlled phase flip gate can be obtained from the square-root of SWAP gate S and single-qubit operations using the sequence (24.5). The controlled phase-flip gate is diagonal in the product basis, $U_{\text{CPF}} = \text{diag}(1, 1, 1, -1)$.
- Show that the local basis change in Eqs. (24.6) and (24.7) serves to transform the controlled phase flip gate into the controlled-NOT (quantum XOR) gate

$$U_{\text{XOR}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

2. Heitler-London approach

Derive the form (24.25) of the exchange energy J in the Heitler-London approximation assuming that the Hamiltonian has the form $H = \sum_{i=1,2} h_i^0 + W + C$, where h_i^0 only acts on quantum dot i .

3. Bloch equations

Show that the Redfield equation (24.45) reduces to the Bloch equation $\dot{\mathbf{p}} = \omega \times \mathbf{p} - R\mathbf{p} + \mathbf{p}_0$ for the Bloch vector $\mathbf{p} = \text{Tr}(\sigma\rho)$ with the relaxation matrix R in Eq. (24.47). Express the relaxation and decoherence times T_1 and T_2 in terms of the Redfield tensor R_{nmkl} .

References

- [1] Sam Braunstein and Hoi-Kwong Lo, editors. *Experimental Proposals for Quantum Computation*, volume 48. Wiley, Berlin, 2000. Special Focus Issue of Fortschritte der Physik.
- [2] Daniel Loss and David P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A*, 57(1):120, 1998.

- [3] D. V. Averin. *Solid State Commun.*, 105:659, 1998.
- [4] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Wal, and S. Lloyd. *Science*, 285:1036, 1999.
- [5] Y. Makhlin, G. Schön, and A. Shnirman. Josephson-junction qubits with controlled couplings. *Nature*, 398:305, 1999.
- [6] D. D. Awschalom, D. Loss, and N. Samarth, editors. *Semiconductor spintronics and quantum computation*. Nanoscience and Technology. Springer, Berlin, 2002.
- [7] Hans-Andreas Engel, L. P. Kouwenhoven, Daniel Loss, and C. M. Marcus. Controlling spin qubits in quantum dots. *Quantum Information Processing*, 3:115, 2005.
- [8] Veronica Cerletti, W. A. Coish, Oliver Gywat, and Daniel Loss. Recipes for spin-based quantum computing. *Nanotechnology*, 16:R27, 2005. Preprint, cond-mat/0412028.
- [9] Guido Burkard. Theory of solid-state quantum information processing. *Handbook of Theoretical and Computational Nanotechnology*. Vol. 3, eds. M. Rieth and W. Schommers, American Scientific Publishers, 2005.
- [10] Y. Makhlin, G. Schön, and A. Shnirman. *Rev. Mod. Phys.*, 73:357, 2001.
- [11] M. H. Devoret, A. Wallraff, and J. M. Martinis. Superconducting qubits: A short review. *Preprint cond-mat/0411174*.
- [12] J. M. Elzerman, R. Hanson, J. S. Greidanus, L. H. Willems van Beveren, S. De Franceschi, L. M. K. Vandersypen, S. Tarucha, and L. P. Kouwenhoven. *Phys. Rev. B*, 67:161308, 2003.
- [13] A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small. *Phys. Rev. Lett.*, 83:4204, 1999.
- [14] G. Burkard, D. Loss, D. P. DiVincenzo, and J. A. Smolin. *Phys. Rev. B*, 60:11404, 1999.
- [15] Norbert Schuch and Jens Siewert. Natural two-qubit gate for quantum computation using the xy interaction. *Phys. Rev. A*, 67:032301, 2003.
- [16] Guido Burkard, Daniel Loss, and David P. DiVincenzo. Coupled quantum dots as quantum gates. *Phys. Rev. B*, 59:2070–2078, 1999.
- [17] Guido Burkard, Hans-Andreas Engel, and Daniel Loss. *Fortsch. Physik*, 48:965–986, 2000. *Preprint cond-mat/0004182*.
- [18] J. M. Kikkawa, I. P. Smorchkova, N. Samarth, and D. D. Awschalom. *Science*, 277:1284, 1997.
- [19] Hans-Andreas Engel and Daniel Loss. *Phys. Rev. Lett.*, 86:4648, 2001.
- [20] D. M. Zumbühl, C. M. Marcus, M. P. Hanson, and A. C. Gossard. Cotunneling spectroscopy in few-electron quantum dots. *Phys. Rev. Lett.*, 93:256801, 2004.
- [21] R. Hanson, B. Witkamp, L. M. K. Vandersypen, L. H. Willems van Beveren, J. M. Elzerman, and L. P. Kouwenhoven. Zeeman energy and spin relaxation in a one-electron quantum dot. *Phys. Rev. Lett.*, 91:196802, 2003.
- [22] R. Hanson, J. M. Elzerman, L. H. Willems van Beveren, L. M. K. Vandersypen, and L. P. Kouwenhoven. Single-shot read-out of an electron qubit. In *Controlling Decoherence*, 2004. 330. WE-Heraeus Seminar, Bad Honnef, Germany.
- [23] I. Chiorescu, Y. Nakamura, C. J. P. M. Harmans, and J. E. Mooij. *Science*, 299:1869, 2003.

- [24] M. H. Devoret. In S. Reynaud, E. Giacobino, and J. Zinn-Justin, editors, *Quantum fluctuations, lecture notes of the 1995 Les Houches summer school*, page 351, 1997, Elsevier, The Netherlands.
- [25] Guido Burkard, Roger H. Koch, and David P. DiVincenzo. Multilevel quantum description of decoherence in superconducting qubits. *Phys. Rev. B*, 69:064503, 2004.
- [26] Guido Burkard, David P. DiVincenzo, P. Bertet, I. Chiorescu, , and J. E. Mooij. Asymmetry and decoherence in a double-layer persistent-current qubit. *Phys. Rev. B*, 71:134504, 2005.
- [27] R. Fazio, G. M. Palma, and J. Siewert. Fidelity and leakage of josephson qubits. *Phys. Rev. Lett.*, 83:5385, 1999.
- [28] Florian Meier and Daniel Loss. Reduced visibility of rabi oscillations in superconducting qubits. *Phys. Rev. B*, 71:094519, 2005.
- [29] U. Weiss. *Quantum Dissipative Systems*, 2nd edition, World Scientific, Singapore, 1999.
- [30] Guido Burkard and Frederico Brito. Non-additivity of decoherence rates in superconducting qubits. *Phys. Rev. B*, 72:054528, 2005.
- [31] T. P. Orlando, J. E. Mooij, Lin Tian, Caspar H. van der Wal, L.S. Levitov, Seth Lloyd, and J. J. Mazo. *Phys. Rev. B*, 60:15398, 1999.
- [32] C. H. van der Wal, A. C. J. ter Har, F. K. Wilhelm, R. N. Schouten, C. J. P. M. Harmans, T. P. Orlando, S. Lloyd, and J. E. Mooij. *Science*, 290:773, 2000.
- [33] P. Bertet, I. Chiorescu, G. Burkard, K. Semba, C. J. P. M. Harmans, D. P. DiVincenzo, and J. E. Mooij. Relaxation and dephasing in a persistent-current qubit. *Preprint cond-mat/0412485*, 2004.

25 Quantum Computing Implemented via Optimal Control: Theory and Application to Spin and Pseudo-Spin Systems

Thomas Schulte-Herbrüggen, A.K. Spörl, Raimund Marx, Navin Khaneja, John M. Myers, Amr F. Fahmy, and Steffen J. Glaser

25.1 Introduction

In this chapter, we discuss theoretical and experimental aspects of quantum control of spin- and pseudo-spin systems in view of realizing quantum algorithms or quantum simulations [1, 2] at minimal cost, in particular in a minimum amount of time. For example, we will see that the time required for implementing a quantum module experimentally is a most natural measure of cost, whereas the number of standard elementary gates, i.e., the network complexity, often does not allow for a simple one-to-one translation into the actual time complexity. Further typical cost functions may include relaxative losses or sensitivity to experimental imperfection. To a considerable extent, recent progress is due to combining the tools of two mature research disciplines: (i) magnetic resonance [3] with its ample arsenal of methodology [4] for manipulating quantum systems, (ii) optimal control theory [5, 6], nowadays an indispensable tool in system theory [7] and engineering [8]. Optimal control can readily be extended to quantum systems [9] and has become a field of growing interest [10–12].

Although the main source of examples presented is liquid-state nuclear magnetic resonance (NMR), the techniques shown here are in no way confined to ensemble quantum computing, but hold for single-spin solid-state quantum computing [13], electron spin resonance (ESR), as well as techniques beyond spin dynamics such as charge or flux qubits in a Josephson element [14]. The methods of geometric control on Lie groups [15] apply to all quantum systems whose dynamics are governed by finite-dimensional Lie algebras, i.e., they have to be expressible within the framework of spin- or pseudo-spin systems (at least to sufficient approximation).

Quantum computational qubit systems may be implemented with particular convenience by nuclear spins-1/2, since spin degrees of freedom are largely isolated from their environment. Moreover, the isotropic overall tumbling of the molecules in a liquid sample decouples the, say, n spins within each molecule from all their surrounding ones, and the spins can readily be represented by a density matrix. It carries the ensemble average over all molecules, each with n spins [3]. Thus the spin degrees of freedom span a Hilbert space of dimension 2^n as desired in systems of n qubits.

It is the ease of experimental control and theoretical setting that gave NMR a head start in the experimental realization of fundamental concepts in quantum computing [16–18].

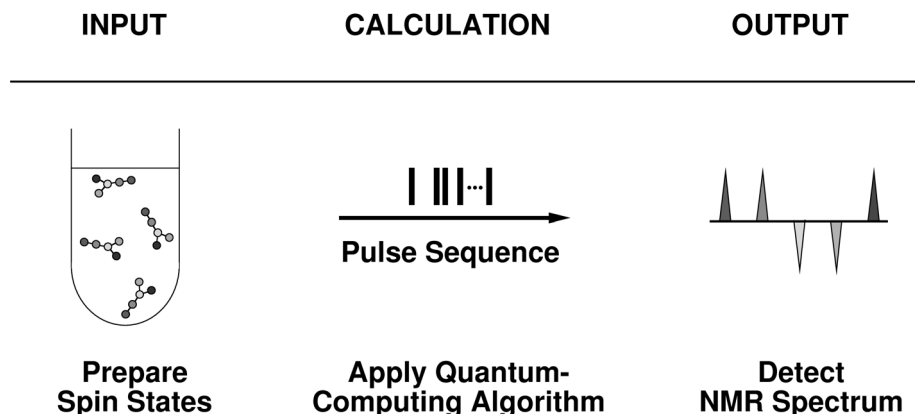


Figure 25.1. Schematic representation of a liquid state NMR experiment. The sample comprises an ensemble of about 10^{18} molecules in an external magnetic field of some 10 T. After preparing the density operator representing the nuclear spin ensemble of the molecules in an initial state, unitary transformations of a quantum algorithm are applied as a sequence of radio-frequency pulses and delays. Finally, the outcome of the experiment is deduced from an acquired NMR spectrum.

As a liquid NMR sample contains an ensemble of many spin systems of the same kind, one can neither manipulate nor detect individual ones thus precluding the preparation of pure states. Nevertheless, in order to use the usual quantum algorithms designed for initial conditions in terms of pure states, one may transcribe the density operator of a spin ensemble to a so-called pseudo-pure state [17]. Furthermore, ensemble-averaged expectation values are detected rather than observables of individual spin systems. Hence, NMR quantum computers are examples of expectation-value quantum computers (EVQC), where the outcome of a given quantum algorithm can be extracted from the resulting NMR spectra. Under mild conditions, spin-1/2 systems are fully controllable in the sense that every unitary transform can be realized experimentally (*vide infra*) and thus universal sets of elementary quantum gates [19] can be put into practice. Then the basic steps of quantum algorithms can be implemented by spin-selective radio-frequency pulses (see Fig. 25.1) and, e.g., CNOT (controlled NOT) gates. In this manner, many algorithms were carried out with NMR experiments, such as the Deutsch–Jozsa algorithm for two [20,21], three [22] and five [23] qubits, variations of Grover’s algorithm for two [24,25] and three qubits [26], the period-finding algorithm for five qubits [27] and a pioneering version of Shor’s algorithm for seven qubits [28]. So NMR quantum computing has also been extensively reviewed, see for instance [29–39].

25.2 From Controllable Spin Systems to Suitable Molecules

25.2.1 Reachability and controllability

Neglecting decoherence, a quantum system is said to be *fully controllable* [40–45] or *operator controllable* [46], if for any arbitrary initial state represented by its density operator A the entire unitary orbit $U(A) := \{UAU^{-1} | U \text{ unitary}\}$ can be reached or, in equivalent terms of control theory, if $U(A)$ is the *reachability set* to the initial state A . In systems of n qubits (e.g., spins-1/2), this is the case under the following mild conditions [45, 47, 48]: (1) the qubits have to be inequivalent, i.e., distinguishable and selectively addressable, and (2) they have to be pairwise coupled (e.g., by Ising interactions), where the coupling topology may take the form of any connected graph. This can readily be proven in equivalent algebraic terms by showing that for n qubits, the Pauli matrices $\sigma_{x,y,z}$ on every single qubit plus the weak Ising couplings $\sigma_{kz} \otimes \sigma_{\ell z}$ (with $1 \leq k < \ell \leq n$) suffice to generate the entire Lie algebra $\mathfrak{su}(2^n)$ by way of the Lie bracket. With the exponential mapping in compact connected groups being surjective, the entire Lie group $SU(2^n)$ can thus be generated by local controls on every qubit and evolutions of Ising interactions or couplings [45].

Of course, fully controllable qubit systems are equivalent to those in which at least one universal and all local quantum gates may be realized by admissible controls.

25.2.2 Molecular hardware for quantum computation

From a chemical perspective, compounds with suitable spin systems require molecules with n coupled spins-1/2. To this end, not all of the spins have to be mutually coupled, but they have to form a connected coupling topology, so there should be no working qubits without any coupling to the other ones. In particular for large qubit systems, linear spin chains with coupling topologies of nearest-neighbor interactions (L_n) are far more realistic than complete coupling topologies (K_n) as shown in Fig. 25.2. Moreover, if the spins can be controlled individually, arbitrary coupling terms can be used, such as combinations of isotropic and dipolar couplings [48].

In order to perform a large number of basic computational steps in a quantum algorithm, the time for each quantum gate must be considerably smaller than the relaxation time of the qubits. Moreover, it is highly desirable to strive for time-optimal implementations of quan-

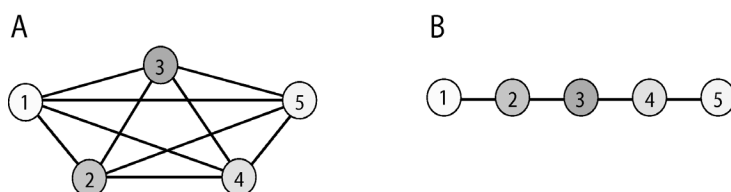


Figure 25.2. (A) Schematic representation of a system consisting of $n = 5$ mutually coupled spins-1/2 (qubits). (B) Spin chains are sufficient for an n -qubit quantum computer.

tum algorithms or their modules in order to avoid unnecessary decoherence. The particular strength of optimal control for achieving this goal will be shown in Section 25.4.

Currently used sample preparations for liquid state NMR quantum computers result in nuclear spin relaxation times of up to several seconds. Characteristic spin–spin coupling constants are of the order of 10 to 10^2 Hz, resulting in a typical duration of two-qubit quantum gates between directly coupled spins of 10^{-2} s. Hence, sequences of up to 10^2 to 10^3 two-qubit quantum gates are feasible based on current liquid state NMR technology, and even more quantum gates may be possible by increasing the spin–spin coupling constants, e.g., by using dipolar couplings in liquid crystalline media [49] and by further increasing the relaxation times. Compared to two-qubit operations, single-spin quantum gates such as NOT or Hadamard gates are very short. For example, in heteronuclear spin systems, typical single-spin gate durations are of the order of 10^{-5} s. The minimum time required for a given single-spin quantum gate not only depends on the maximum amplitude of radio-frequency pulses but also on the smallest frequency difference of the nuclear spins in a given molecule [23].

For the first NMR quantum computers with up to three qubits, readily available compounds were used, such as 2,3-dibromothiophene [16, 50], ^{13}C -chloroform [21], 2,3-dibromopropionic acid [21, 51], and $^{13}\text{C}_3$ -alanine [52]. For the realization of the first five-qubit NMR quantum computer the compound BOC-($^{13}\text{C}_2$ - ^{15}N - $^2\text{D}_2$ -Gly)-F was synthesized [23, 53] (see Fig. 25.3). If the deuterium spins are decoupled, the nuclear spins of $^1\text{H}^N$, ^{15}N , $^{13}\text{C}^\alpha$, $^{13}\text{C}'$ (i.e., C^O) and ^{19}F form a coupled spin system consisting of five spins-1/2. The ^1J coupling constants range between 13.5 Hz ($^1J_{\text{N},\text{C}^\alpha}$) and 366 Hz ($^1J_{\text{C}',\text{F}}$), and for a magnetic field of 9.4 T, the smallest frequency differences are 12 kHz ($\nu_{\text{C}'} - \nu_{\text{C}^\alpha}$). A further synthetic five-qubit system is a perfluorobutadienyl iron complex [27], an entirely homonuclear spin system consisting of five coupled ^{19}F spins. A carbon-labeled analog has been used as a seven-qubit molecule for implementing a variant of Shor's algorithm [28]. Another seven-qubit molecule suggested for NMR quantum computing applications is $^{13}\text{C}_4$ -crotonic acid [54]. The design and synthesis of molecules with suitable spin systems for 10–20 qubits is not a trivial chemical challenge. An alternative way of realizing a molecular architecture with more than 10 coupled spins is the synthesis of polymers with a repetitive unit consisting of three or more spins [55]. This approach is advantageous because only a small number of resonances

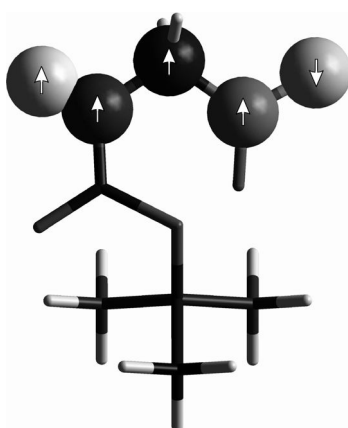


Figure 25.3. Schematic representation of BOC- $^{13}\text{C}_2$ - ^{15}N - $^2\text{D}_2$ -glycine-fluoride with the coupled five-spin system (represented schematically by white arrows) that forms the molecular basis of a five-qubit NMR quantum computer [23]. The atoms that form the spin system of interest are shown as spheres. The rest of the molecule is shown in a stick representation.

have to be addressed selectively. However, in such an architecture the implementation of quantum algorithms will require an additional overhead, which poses new challenges for the efficient implementation of quantum gates.

25.3 Scalability

25.3.1 Scaling problem with pseudo-pure states

The density operator of a spin system at thermal equilibrium is proportional to $\exp(-\frac{\mathcal{H}}{kT})$, where $\mathcal{H}$ is the spin Hamiltonian of the n -spin molecule used as a quantum register, k is Boltzmann's constant, and T is the temperature. As the usual magnetic fields in NMR are of the order of 10 T, the so-called high-temperature approximation is valid above temperatures of some 10 mK and the thermal density operator can be given by the first two terms in the Taylor expansion

$$\rho_{\text{eq}} = 2^{-n} \left(\mathbb{1} - \frac{\mathcal{H}}{kT} \right) \approx 2^{-n} \left(\mathbb{1} - \frac{\hbar}{kT} \sum_j \omega_j I_z^j \right), \quad (25.1)$$

where ω_j is the angular frequency of the j th nucleus, and I_z^j is defined by a tensor product over all n spins in which all the factors are unit operators except for $\frac{1}{2}\text{diag}(1, -1)$ as the j th factor of the tensor product.

Although highly mixed, this state can be transformed into a so-called pseudo-pure state [16, 17], resulting in an initial density operator of the form

$$\rho_{\text{pps}} = 2^{-n} (1 - \epsilon) \mathbb{1} + \epsilon |\psi\rangle\langle\psi| \quad (25.2)$$

for some (usually small) coefficient ϵ . With the identity operator $\mathbb{1}$ being invariant under any similarity transform and all spin observables being traceless, pseudo-pure states form handy starting points for NMR implementations of quantum algorithms. However, this convenience comes at a high cost: the coefficient ϵ decreases exponentially with the number of qubits n [56]. Hence the spectroscopic signal decreases as well and severe signal-to-noise problems are expected for experiments with more than about 10 qubits.

The exponential signal loss is often thought to impose a fundamental limit on the scalability of liquid state NMR [57]. Fortunately, this problem can be circumvented by several approaches avoiding pseudo-pure states altogether.

25.3.2 Approaching pure states

The first approach is to prepare the sample not in a mixed state corresponding to the thermal equilibrium density operator at high temperature, but in a pure state corresponding to a low temperature close to 0 K. However, if simply the actual sample temperature was cooled down close to absolute zero, every sample would ultimately freeze thus precluding any NMR experiments in the liquid state. Fortunately it is possible to cool down only the spin temperature by increasing the nuclear spin polarization well beyond the thermal extent, while leaving the sample at room temperature. Several spin polarization techniques are available for decreasing

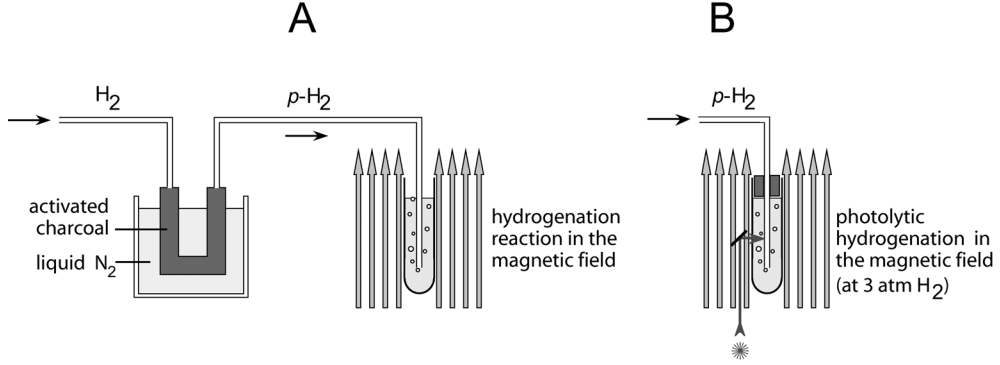


Figure 25.4. Set-ups for experimental NMR quantum computation with almost pure states (estimated purity up to > 0.9). Hydrogen gas (H_2) is converted to *para*-hydrogen gas ($p-H_2$) at low temperature before reacting with host molecules in the magnetic field. (A) original concept [58] and (B) continuation [59–64] to purities over 90% by laser-photolytic onset of the *para*-hydrogenation reaction.

the spin temperature. So far, the largest polarizations achieved experimentally have exploited the spin order of *para*-hydrogen, see Fig. 25.4. Already the original concept with the spin order at liquid-nitrogen temperatures (77 K) allowed applications to a simple quantum computing algorithm [58]. By preparing *para*-hydrogen at even lower temperatures (20 K) and using a photolytic onset of the *para*-hydrogenation reaction in high-pressure samples [59], the purity of the quantum state can be further increased [60–64], so that experimental NMR quantum computing with states of over 90 % purity can be put into practice. In this setting, a Deutsch–Jozsa algorithm [61] as well as a Grover search [62] have been performed.

Other techniques for polarization enhancement may be based on the use of laser-polarized xenon [65]. Although promising, these techniques also pose a number of technical problems that currently limit their practical use in scaling up the number of qubits.

25.3.3 Scalable quantum computing on thermal ensembles

An attractive alternative approach avoiding pure or pseudo-pure states altogether is to design ensemble quantum computing algorithms based on the thermal density operator instead of a pure state. A premier example of this approach is a new scalable version of the Deutsch–Jozsa algorithm [66]. At the expense of an extra qubit and a modified oracle, balanced functions can be distinguished from constant ones using an initial state obtained merely by a hard 90° y -pulse applied to the thermal state. This requires neither pseudo-pure states of Eq. (25.2) nor temporal averaging. Let $N = 2^n$ denote the number of levels in an n -qubit system. Then, for an Oracle of a function $f : \mathbb{Z}_{N/2} \rightarrow \mathbb{Z}_2$, one implements a substitute $U_{f'}$ for $f' : \mathbb{Z}_N \rightarrow \mathbb{Z}_2$ instead of U_f . To this end, relate f' to f by

$$f'(j) := \begin{cases} f(j) & \text{for } 0 \leq j \leq N/2 - 1 \\ 0 & \text{for } N/2 \leq j \leq N - 1 \end{cases}.$$

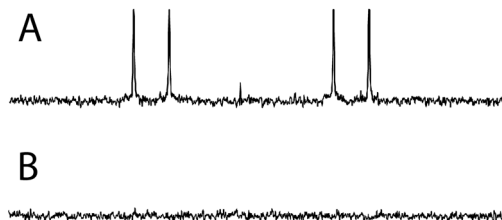


Figure 25.5. Experimental spectra [67] representing the result of the new version of the Deutsch–Jozsa algorithm [66] based on the thermal density operator for a constant (A) and a balanced (B) test function.

Given the Oracle $U_{f'}$, a scalable NMR quantum computer can readily discriminate balanced functions from constant ones. Note that resolving the output spectra [66] does not build upon any demands growing exponentially with the number of qubits. For example, for the constant function $f_0(x_1, x_2, x_3) = 0$ and the balanced function $f_b(x_1, x_2, x_3) = x_1 \oplus x_2 x_3$, the scalable version of the Deutsch–Jozsa algorithm requires an additional qubit (x_0) and the implementation of $U_{f'_0}$ for $f'_0(x_0, x_1, x_2, x_3) = \bar{x}_0 f_0(x_1, x_2, x_3) = 0$ and of $U_{f'_b}$ for $f'_b(x_0, x_1, x_2, x_3) = \bar{x}_0 f_b(x_1, x_2, x_3) = \bar{x}_0 x_1 \oplus \bar{x}_0 x_2 x_3$. For the five-qubit system BOC- ($^{13}\text{C}_2$ - ^{15}N - $^2\text{D}_2^\alpha$ -Gly)-F [23, 53], the resulting spectra [67] of x_0 are shown in Fig. 25.5A and B for $U_{f'_0}$ and $U_{f'_b}$, respectively. Constant and balanced functions can be easily distinguished by the presence or absence of the signals.

It is important to note that for this version of the algorithm, the number of molecules in the ensemble does *not* have to increase exponentially with the number of qubits n within the molecule. These favorable scaling properties are at variance to a previous alternative ensemble implementation of the Deutsch–Jozsa algorithm [68, 69].

However, with an increasing number of qubits, not only the synthetic requirements grow, but also the demands with respect to NMR instruments and pulse-sequence design, in order to control experimental imperfections (such as rf-inhomogeneity) or relaxation.

25.4 Control Theory for Spin- and Pseudo-Spin Systems

Although one can decompose any quantum computing algorithm into a series of single-spin operations and two-spin gates between directly coupled spins, some fundamental questions remain: they are of both theoretical and practical interest. What is the minimum time required to realize a given unitary transformation in a given coupling topology of a spin system? Which controls (pulse sequences) achieve the task in minimal time? Control theory [70–73] provides powerful tools to address these issues numerically. Moreover, one may characterize time-optimal pulse sequences algebraically by geometric optimal control [15] showing that the problem reduces to finding geodesics (i.e., shortest paths) between cosets [70], as will be demonstrated below in Section 25.5.1.3.

In this section, we discuss gradient-flow based methods for solving the following three fundamental problems of quantum control:

- I Given the unitary orbit UAU^{-1} of Hamiltonian quantum evolution of some initial state A of a quantum system, what is the utmost projection onto a given final state C ?
- II What are the fastest ways of steering a given initial quantum state into maximal overlap with a desired final state by admissible experimental controls?

- III What are the fastest decompositions of a given unitary quantum gate or algorithmic module into a sequence of evolutions under experimentally admissible controls?

I. Maximizing coherence transfer

In spectroscopy the signal-relevant components of a density operator are may be conveniently collected in arbitrary finite complex matrices $A, C \in \text{Mat}_N(\mathbb{C})$. Define $f : U(N) \rightarrow \mathbb{C}$ by $f(U) := \text{tr}\{UAU^{-1}C\}$. In this setting, there are two geometric optimization tasks of particular practical relevance as they determine maximal signal intensity in coherent spectroscopy [47, 74]:

1. *Minimize the Euclidean distance between $C^\dagger$ and the unitary orbit of A !*
Clearly, the distance $\|UAU^{-1} - C^\dagger\|_2^2 = \|A\|_2^2 + \|C\|_2^2 - 2\text{Re } \text{tr}\{UAU^{-1}C\}$ is minimum if the overlap $\Phi_1 := \text{Re } f(U)$ is maximum.
2. *Minimize the angle $\text{mod}(\pi)$ between $C^\dagger$ and the unitary orbit of A !* With the complex scalar product, define $\cos^2(\angle\{UAU^{-1}, C^\dagger\}) = |\text{tr}\{UAU^{-1}C\}|^2 \cdot \|A\|_2^{-2} \cdot \|C\|_2^{-2}$. Then UAU^{-1} and $C^\dagger$ are closest to collinear for maximal $\Phi_2 := |f(U)|^2$.

Extending concepts of Brockett [75, 76] from the orthogonal to the unitary group and expressing differentials in terms of the Fréchet derivatives one obtains the gradient flows of Φ_ν for either case ($\nu = 1, 2$) reading [45, 47, 77],

$$\begin{aligned} \nabla\Phi_\nu(iHU) &= \text{tr}\{G^{(\nu)} iH\}, \quad \text{where} \\ G^{(1)} &:= \frac{1}{2} \{[A_t, C] - [A_t, C]^\dagger\} \\ G^{(2)} &:= [A_t, C] f(U)^* - [A_t, C]^\dagger f(U), \end{aligned}$$

and $A_t := UAU^{-1}$. The critical points are characterized by $\nabla\Phi_\nu(iHU) = 0$. Following the gradient flow by recursive unitary transformations

$$U_{r+1}^{(\nu)} = e^{-\alpha_r^{(\nu)} G_r^{(\nu)}} \cdot U_r^{(\nu)} \quad \text{till} \quad \|\nabla\Phi_\nu(iHU_{r+1}^{(\nu)})\|_2 \rightarrow 0$$

then drives $U_{r+1}AU_{r+1}^{-1}$ into the final state attaining the extrema of the quality functions Φ_ν in the settings $\nu = 1, 2$.

II. Time-optimal transfer of quantum states

Once having established the limits of unitary coherence transfer, it is natural to ask (i) how to achieve these maxima by experimentally available controls, and (ii) what the minimal time for doing so actually is in a given experimental setting. To this end, write the unitary propagators involved as

$$U(T) = e^{-it_M H^{(M)}} \dots e^{-it_k H^{(k)}} \dots e^{-it_1 H^{(1)}} \quad \text{with} \quad H^{(k)} = H_d + \sum_j u_j^{(k)} H_j^{(k)},$$

where $\{H^{(k)}\}$ are the piecewise constant Hamiltonians and H_d is the drift term resulting from free evolution, while the $\{H_j\}$ denote experimentally available controls “switched on” with the amplitudes u_j during each time interval $t_1, t_2, \dots, t_k, \dots, t_M \equiv T$.

In NMR spin dynamics [3], for instance, the local controls of qubit ℓ are represented by a linear combination of the Pauli matrices $\{\sigma_{\ell x}, \sigma_{\ell y}\}$. And in the rotating frame [3], the drift term is governed by the Ising-type weak scalar couplings

$$H_d = \pi \sum_{\ell < m} J_{\ell m} \frac{1}{2} \sigma_{\ell z} \otimes \sigma_{m z},$$

provided the couplings between spins are much smaller than the difference between the eigenfrequencies of the respective spins: this is the case in heteronuclear spin systems, and for quantum control even the homonuclear ones can be designed [78] such as to meet this simplifying approximation.

Allowing again for non-Hermitian operators A, C collecting the signal-relevant terms and with the one-parameter group of time dependence $U(t) = e^{-itH}$, one may optimize the quality functionals

$$\Phi_1 := \operatorname{Re} \operatorname{tr}\{U(t)AU^{-1}(t)C\} \quad \text{and} \quad \Phi_2 := |\operatorname{tr}\{U(t)AU^{-1}(t)C\}|^2 \quad (25.3)$$

subject to the equation of motion $\dot{A}(t) = -i[H, A(t)]$. Standard control theory introduces an analogous adjoint system $\dot{\lambda}(t) = -i[H, \lambda(t)]$ and scalar-valued Hamiltonian functions, e.g.,

$$h_1(U) := \operatorname{Re} \operatorname{tr}\{\lambda^\dagger(t) [-i(H_d + \sum_j u_j H_j), A(t)]\},$$

where $h_2(U)$ is the squared absolute value of the same arguments. Then, Pontryagin's maximum principle [5] requires

$$\frac{\partial h_1(U)}{\partial u_j} \equiv -\operatorname{Re} \operatorname{tr}\{\lambda^\dagger [-iH_j, A(t)]\} \stackrel{!}{=} 0$$

and an analogous identity for $\frac{\partial h_2(U)}{\partial u_j}$ [73] thus allowing to implement again gradient-flow based recursions as in the previous section. For the amplitude of the j th control in iteration $r + 1$ at time interval t_k one finds with a step size α

$$u_j(t_k^{(r+1)}) = u_j(t_k^{(r)}) + \alpha \frac{\partial h_j}{\partial u_j} \Big|_{t=t_k^{(r)}}. \quad (25.4)$$

The procedure is then repeated with decreasing final times T up to a minimal time τ still allowing to get full coherence transfer (see [9–11, 73, 79] and the GRAPE algorithm [73] described below).

III. Time-optimal implementation of quantum gates

Next we focus on quantum gate control [9, 73, 80–82]. In order to control a quantum system of n qubits (spins-1/2) such as to realize a quantum gate or module of some quantum algorithm given by the unitary propagator $U_G \in U(2^n)$ in minimal time, one has to decompose

$$U_G \sim U(T) = e^{-it_M H^{(M)}} \dots e^{-it_k H^{(k)}} \dots e^{-it_1 H^{(1)}}$$

into a *time-optimal sequence* ($T := \sum_k t_k \stackrel{!}{=} \min$) of evolutions under piecewise constant Hamiltonians where H_d is again the drift term of free evolution, while the $\{H_j\}$ denote experimentally available controls “switched on” with the amplitudes u_j during t_k . For the system to be *fully controllable* in the sense outlined above, $\{H_d\} \cup \{H_j\}$ has to form a generating set of the Lie algebra $\mathfrak{su}(N)$ by way of commutation.

The control problem can be put into two distinct settings, one that explicitly carries the phase while the other one automatically absorbs it as desired. So for a given unitary quantum gate U_G and propagators $U = U(t)$ describing the evolution of the quantum system, there are two geometric tasks:

- (1) *minimize the distance* $\|U - U_G\|_2$ *by maximizing* $\Phi_3 := \text{Re tr}\{U_G^\dagger U\}$
- (2) *minimize the angle* $\angle(U, U_G) \bmod(\pi)$ *by maximizing* $\Phi_4 := |\text{tr}\{U_G^\dagger U\}|^2$.

(1) In terms of control theory, the first task is to maximize the quality functional $\Phi_3[U(t)] = \text{Re tr}\{U_G^\dagger U(T)\}$ with $0 \leq t \leq T$ subject to the equation of motion $\dot{U}(t) = -iHU(t)$ (with $H = H_d + \sum_j u_j H_j$) and the initial condition $U(0) = \mathbb{1}$, whereas the final condition $U(T)$ is free at an appropriately fixed final time T (*vide infra*). The problem is readily solved by introducing the operator-valued Lagrange multiplier $\lambda(t)$ satisfying $\dot{\lambda}(t) = -iH\lambda(t)$ and a scalar-valued Hamiltonian function

$$h(U) = \text{Re tr}\{\lambda^\dagger(t)(-i(H_d + \sum_j u_j H_j))U(t)\}.$$

Then, Pontryagin’s maximum principle [5] may be exploited in a quantum setting [9, 73] to require

$$\frac{\partial h(U)}{\partial u_j} \equiv -\text{Im tr}\{\lambda^\dagger H_j U\} \stackrel{!}{=} 0$$

as well as the final condition for the adjoint system

$$\lambda(T) = -\frac{\partial \Phi_3(T)}{\partial U(T)} = -U_G \quad (25.5)$$

thus allowing to implement again a gradient-flow-based recursion as in the previous section. For the amplitude of the j th control in iteration $r + 1$ at time interval t_k one finds with α as a suitably chosen step size

$$u_j(t_k^{(r+1)}) = u_j(t_k^{(r)}) + \alpha \frac{\partial h}{\partial u_j} \Big|_{t=t_k^{(r)}}. \quad (25.6)$$

The procedure is then repeated for a set of decreasing final times T up to a minimal time τ still allowing to get sufficient fidelity.

(2) The second task amounts to maximizing $\Phi_4[U(t)] = |\text{tr}\{U_G^\dagger U(T)\}|^2$, which translates to the square of the trace fidelity and is easy to handle by gradient flow methods. This problem, however, readily reduces to task (1): let $U \in SU(N)$, then $\tilde{U} := U^* \otimes U$ is a representation of the *projective special unitary group* $PSU(N) \stackrel{\text{iso}}{=} SU(N)/\mathbb{Z}_N \stackrel{\text{iso}}{=} U(N)/U(1)$ embedded in $SU(N^2)$. Though highly reducible, this representation is very convenient, because

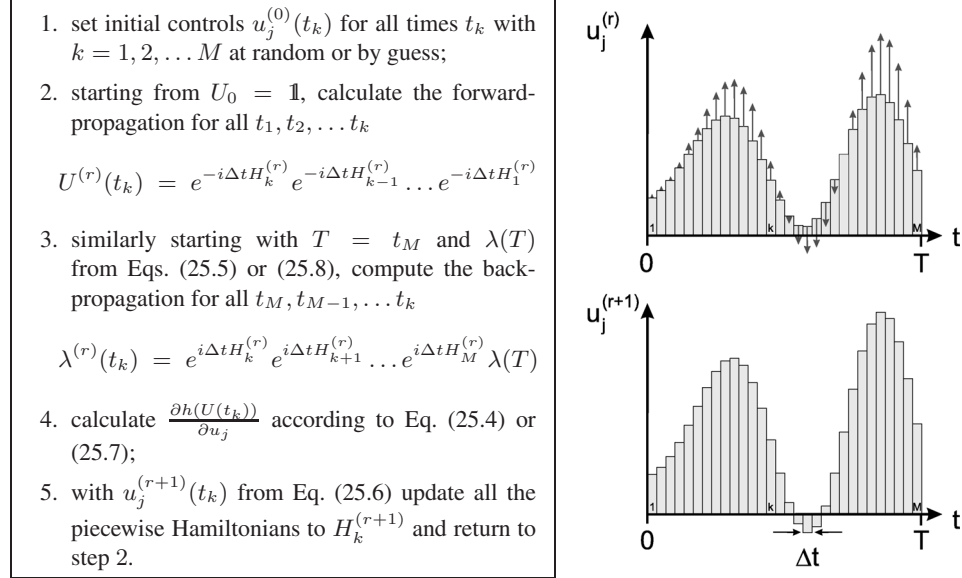


Figure 25.6. Left: the GRAPE algorithm [73] as given in the text. Right: at each of the time steps $t_1, \dots, t_k, \dots, t_M$ the iteration $r + 1$ provides the new controls $u_j^{r+1}(t_k)$ obtained from the old ones $u_j^r(t_k)$ and the gradients. For simplicity, here all the time steps are of equal length $\Delta t = t_k - t_{k-1}$.

$\Phi_3[\hat{U}(t)] = \text{Re tr}\{\hat{U}_G^\dagger \hat{U}(T)\} = |\text{tr}\{U_G^\dagger U(T)\}|^2 = \Phi_4[U(t)]$. Hence one may adopt the previous results to obtain the gradient flow on $PSU(N)$ [82] as the maximum principle likewise requires

$$\frac{\partial h(\hat{U})}{\partial u_j} \equiv -2 \text{Im} \left(\text{tr}\{U^\dagger(t) H_j \lambda(t)\} \cdot \text{tr}\{\lambda(t)^\dagger U(t)\} \right) \stackrel{!}{=} 0, \quad (25.7)$$

thus allowing a gradient flow to be implemented as above (Eq. (25.6) with $\frac{\partial h(\hat{U})}{\partial u_j}$), where the final condition of the adjoint system reads

$$\hat{\lambda}(T) = -\frac{\partial \Phi_3[\hat{U}(T)]}{\partial \hat{U}(T)} = -\hat{U}_G = -U_G^* \otimes U_G. \quad (25.8)$$

Embedding $PSU(N)$ in $SU(N^2)$ enforces a global phase of zero in $\Phi_3[U(t)]$. Therefore the final condition of the adjoint system does not require any prior knowledge or screening of the global phase ultimately giving the fastest implementation as has been the case in previous settings, e.g., [83] thus cutting the number of runs in n -qubit systems by a factor $N = 2^n$. Having reduced task (2) to task (1) also saves all the convergence and step-size considerations [77] from $SU(N^2)$ to apply to $PSU(N)$. With the Hamiltonians H_k in the iterations r of Eq. (25.6) one arrives at the gradient-ascent pulse engineering scheme (GRAPE) described in Fig. 25.6; for more details see [73].

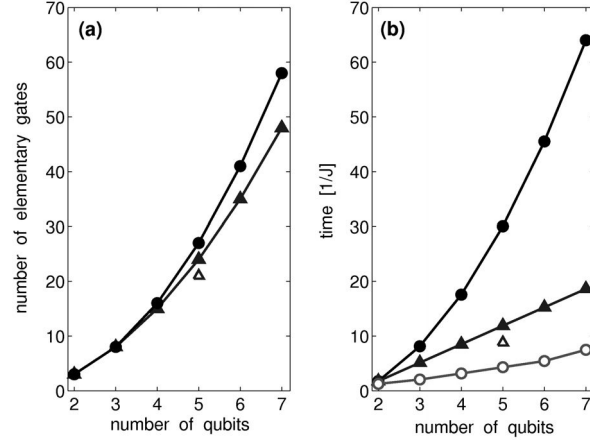


Figure 25.7. The QFT in linear coupling topologies L_n : (A) gate complexity by standard-gate decomposition (●) [86] and optimized scalable gate decomposition (▲) [87]; (B) time complexity of the QFT. Upper traces give analytical times associated with the decompositions of part (A): standard-gate decompositions (●) [86] and optimized scalable gate decompositions (▲) [87]; (△) gives a special (i.e., nonscalable) five-qubit decomposition into standard gates obtained by simulated annealing [87]. Lowest trace: fastest realizations [82] currently obtained by numerical time-optimal control (rounded to $0.01 J^{-1}$) giving trace fidelities > 0.99999 (○) and > 0.9975 for the last point.

25.5 Applied Quantum Control

25.5.1 Regime of fast local controls: the NMR limit

Firstly, we choose the limit of fast local controls (by strong pulses), the time scale of which can safely be neglected as compared to the time-limiting coupling interactions of the Ising type. Not only is this regime typical of NMR with weak scalar couplings, it also lends itself for a theoretical understanding in Lie-algebraic terms. Here, the J -couplings are assumed to be uniform in the following examples thus allowing to express the time required in units of J^{-1} . However, the numerical algorithms are of course general and can cope with coupling types and strengths directly matching the experimental settings, and even finite times for local controls can be dealt with as shown in Section 25.5.2.

25.5.1.1 The quantum Fourier transform

The quantum Fourier transform (QFT) is in the core of all quantum algorithms of *Abelian hidden subgroup type* [84, 85] such as, e.g., the algorithms of Deutsch–Jozsa’s, Simon’s, and Shor’s. In order to speed up quantum modules and minimize decoherence, the QFT should be implemented in the fastest way. Clearly, the time required for realizing the QFT in n -qubit systems depends on the coupling topology and the interaction type and strength of the per-

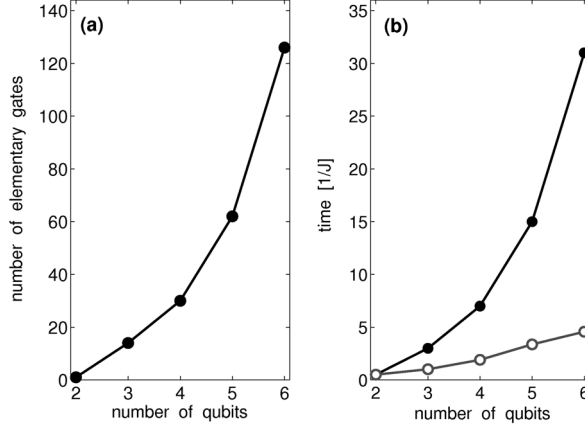


Figure 25.8. The C^{n-1} NOT gate on complete coupling topologies K_n : (A) network complexity [88]; (B) time complexity. Upper trace: analytical times for decomposition into standard gates (●) [88]. Lowest trace: fastest realizations [82] currently obtained by numerical time-optimal control (rounded to $0.01 J^{-1}$) giving trace fidelities > 0.99999 (○) and > 0.999 for the last point.

periment experimental setting. Figure 25.7 demonstrates how in linear spin chains (L_n) with the nearest-neighbor Ising interactions, numerical time-optimal control provides a decomposition of the QFT that is much faster than the corresponding decomposition into standard gates would impose: in six qubits, for instance, the speed-up is more than eightfold and in seven qubits approximately ninefold.

25.5.1.2 Multiply controlled NOTs

Analogously the C^{n-1} NOT-gate can be decomposed in a time-optimized way. Interestingly, in a complete coupling topology of n qubits, the algorithmic complexity was described by Barenco *et al.* [88] as growing exponentially up to six qubits, whereas the increase from seven qubits onwards was said to be quadratic. Again, time-optimal control provides a dramatic speed-up in this case, see Figure 25.8.

25.5.1.3 Geometry of time-optimal gates

In NMR, the markedly different time scales for fast local controls (pulses) vs slow coupling evolutions lend themselves for making use of Cartan decomposition of real semisimple Lie algebras $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ (where $[\mathfrak{k}, \mathfrak{k}] \subseteq \mathfrak{k}$; $[\mathfrak{k}, \mathfrak{p}] = \mathfrak{p}$; $[\mathfrak{p}, \mathfrak{p}] \subseteq \mathfrak{k}$). The goal of time-optimal realizations then reduces to finding constrained shortest paths in the cosets G/K . For $n = 2$ spins-1/2, $G = SU(2^n)$, $K = (SU(2))^{\otimes n}$ and the coset G/K takes the form of a Riemannian symmetric space. Thus time-optimal trajectories between points in G correspond to Riemannian geodesics. For $n > 2$, the cosets G/K are no longer Riemannian symmetric spaces, so the time-optimal trajectories in G denote sub-Riemannian geodesics.

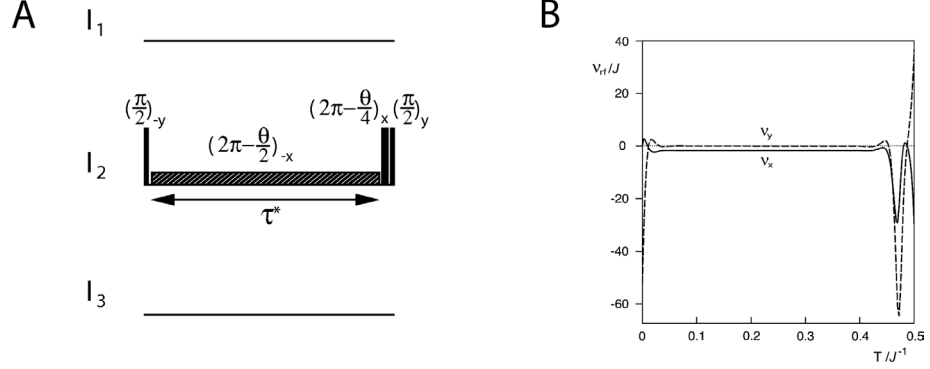


Figure 25.9. Time-optimal pulse sequences for synthesizing the propagator $U_{zzz}(\kappa) = \exp\{-i\theta I_{1z}I_{2z}I_{3z}\}$ with $\theta = 2\pi\kappa$. (A) In the scheme for time-optimal (geodesic) pulse sequence derived on algebraic grounds, the radio-frequency amplitude ν_{rf} of the hatched pulse is $(2 - \kappa)J/\sqrt{\kappa(4 - \kappa)}$ [89]. (B) Pulse sequence found by numerical optimal control for $\kappa = 0.25$. Only the I_2 channel is used, amplitudes on the other spins are of negligible amplitude thus matching the theoretically predicted controls in (A).

Yet, in the sub-Riemannian geometry of three spins, there is a first example that can be fully understood: the time-optimal simulation of three-spin-interaction Hamiltonians of the form $\mathcal{H}_{\alpha\beta\gamma} = 2\pi J_{\text{eff}} I_{1\alpha}I_{2\beta}I_{3\gamma}$ where α, β, γ can be x, y or z and J_{eff} is an effective trilinear coupling constant. We considered a linear coupling topology consisting of a chain of three heteronuclear spins-1/2 with the coupling constants $J_{12} = J_{23} = J$, $J_{13} = 0$ and the coupling term $\mathcal{H}_{\text{coup}} = 2\pi J I_{1z}I_{2z} + 2\pi J I_{2z}I_{3z}$. Here, the time-optimal realization of the trilinear coupling term $\mathcal{H}_{\alpha\beta\gamma}$, see Fig. 25.9, can be derived by means of geometric optimal control [89].

Compared to conventional approaches [90], the time-optimal synthesis of effective three-spin propagators of the form $\mathcal{U}_{\alpha\beta\gamma}(\kappa) = \exp\{-i\kappa 2\pi I_{1\alpha}I_{2\beta}I_{3\gamma}\}$ has a duration of only $\sqrt{\kappa(4 - \kappa)}/2J$ [89] compared to the duration $(2 + \kappa)/2J$ of conventional implementations [90] and hence provides significant time savings as shown in Fig. 25.10.

25.5.2 Regime of finite local controls: beyond NMR

25.5.2.1 CNOT and TOFFOLI gates for charge qubits

Clearly the optimal control methods presented thus far can be generalized such as to hold for systems with finite times for local controls as long as one has finite degrees of freedom allowing for a pseudo-spin formulation in terms of closed Lie algebras. Suffice it to mention that the standard CNOT-gate can be realized in two coupled charge qubits of a solid-state Josephson device some five times faster than in the pioneering setting of Nakamura [91]. As will be shown elsewhere, one easily obtains a trace fidelity beyond 0.99999. With the same fidelities one finds realizations of the TOFFOLI-gate in three linearly coupled charge qubits

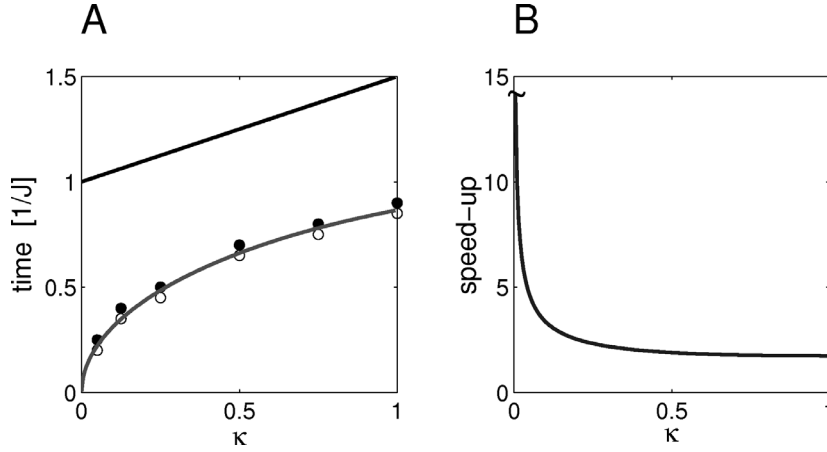


Figure 25.10. (A) Times required for simulating the trilinear coupling Hamiltonian $\mathcal{H}_{zzz} = 2\pi J_{\text{eff}} I_{1z}I_{2z}I_{3z}$ in the conventional and the time-optimal way [89]. In the lower trace, the solid line (—) is calculated on algebraic grounds, while numerical results [73] are inserted point-wise: full circles (●) represent times achieving full trace fidelity, while empty ones (○) denote times giving trace fidelities between 0.9985 and 0.99998. The time resolution for the numerical calculations was $0.05 J^{-1}$. (B) The speed-up factors are most prominent for small flip angles κ .

that are some nine times faster than by standard-gate decomposition, and approximately 13 times faster than one would infer from the CNOT in Ref. [91].

25.6 Conclusions

25.6.1 Ensemble quantum computing

At low temperatures and using *in situ* reactions with *para*-hydrogen, ensemble states of high purity can be obtained for pure-state NMR quantum computing.

However, even thermal ensemble states may be used for *scalable* NMR implementations of quantum algorithms: e.g., the Deutsch–Jozsa algorithm can be modified by introducing a single ancilla qubit (independent of the n working qubits) in order to turn into a scalable variant. It does *not* require an exponential growth of the ensemble with increasing number of qubits and thus should in fact be regarded as proper quantum information processing [57, 92].

25.6.2 From gate-complexity to time-complexity by optimal control

On a quite general scale, gradient flows can be used to determine the sharp upper bound to quality functions in Hamiltonian quantum dynamics. Exploiting gradient-flow based quantum control, here we have left the usual approach of decomposing quantum modules into sets of discrete building blocks, such as elementary universal quantum gates thus expressing the cost as algorithmic network complexity. Instead we proposed to refer to *time complexity* as the

experimentally relevant cost: it allows for exploiting the continuous differential geometry of the unitary Lie-groups as well as the power of quantum control for getting constructive upper bounds to the time complexity perfectly matching the experimental setting [82].

Clearly, in the generic case, there is no simple one-to-one relation between time complexity and network complexity, because typically (1) not all the elementary gates are of the same time cost, but each experimental implementation comes with its characteristic ratio of times required for local vs nonlocal (coupling) operations; (2) not all the elementary gates have to be performed sequentially, but can be rearranged so that some of the commuting operations (e.g., controlled phase gates between several qubits) or operations in disjoint subspaces can be parallelized; (3) the coupling topology between the qubits does not have to form a complete graph (K_n) but may be just a connected subgraph, and each graph comes with a specific potential of parallelizing timewise costly interactions; (4) the experimental setting with its specific type and individual strengths of coupling interaction (e.g., Ising or Heisenberg- XY or XYZ type) related to the choice of universal gates for the network decomposition may introduce some arbitrariness.

It is for these very reasons that time complexity is the more realistic measure of the experimentally relevant cost than network complexity is [82].

25.6.3 Beyond NMR spin systems

Geometric optimal quantum control is a most powerful tool for optimizing experimental implementations of quantum computing, whenever the quantum degrees of freedom can be described in closed Lie-algebraic form. This means, the quantum system in question can be treated as a spin- or pseudo-spin system as, e.g., the charge qubits in Josephson devices. Therefore, we anticipate the tools sketched here await broad application. Extrapolating the results to some 20 qubits, network decompositions of quantum modules will often become impractical, while time-optimal control may easily accelerate experimental implementations by one to two orders of magnitude.

Acknowledgements

This work was supported in part by the integrated EU-programme QAP as well as by DFG (*Deutsche Forschungsgemeinschaft*) in the incentive QIV.

Exercises

1. Spin Polarization

- (a) Set $\beta := 1/(kT)$. Verify for a single spin-1/2 that at $T = 300$ K and a magnetic field $B_0 = 20$ T no more than roughly 1 in 10000 spins of an ensemble contributes to the spin polarization. (Hint: use $\rho_{\text{eq}} := e^{-\beta H} / \sum_{j=1}^2 e^{-\beta E_j}$, where $H = -\hbar\gamma B_0 \sigma_z$ and $\gamma/(2\pi) = 42.5759$ MHz/T, $k = 1.3807 \times 10^{-23}$ J/K, $\hbar = 1.0546 \times 10^{-34}$ J s.)
- (b) Show that the “high-temperature” approximation Eq. (25.1) holds for $T \gg 10$ mK. Give the population difference $p(|0\rangle\langle 0|) - p(|1\rangle\langle 1|)$ at $T = 77$ K and 300 K.

2. von Neumann Entropy of Spin Ensembles

Using results from (1) show that at almost all practical temperatures

- (a) in von Neumann’s entropy $S(\rho)$ one finds $-\text{tr}\{\rho \ln \rho\} \approx 1 - \|\rho\|_2^2$;
- (b) for σ near $\frac{1}{N}\mathbb{1}$, the relative entropy becomes $S(\rho, \sigma) := \text{tr}\{\rho \ln \sigma\} \approx \|\rho\|_2^2 - \text{tr}\{\rho \sigma\}$;
- (c) $S(\rho, \sigma) + S(\sigma, \rho) \approx \|\rho - \sigma\|_2^2$ for both ρ, σ near $\frac{1}{N}\mathbb{1}$.

(Hint: use $-\text{tr}\{\rho \ln \rho\} = \text{tr}\left\{\sum_{n=1}^{\infty} \sum_{k=0}^n (-1)^k \frac{1}{n} \binom{n}{k} \rho^{k+1}\right\}$ to first order and set $0 \ln 0 := 0$ for the expansion to hold even for eigenvalues $0 \leq \lambda_i(\rho) \leq 2$).

3. Unitary Equivalence versus Entropy Conservation

Show that for two density operators to be unitarily similar, conservation of von Neumann’s entropy is a necessary but *not* a sufficient condition. (Hint: use the moments $\langle \rho^k \rangle := \text{tr}\{\rho^{k+1}\}$ and the series of Exercise (2).) Give a sufficient condition. What is the maximum of Φ_1 in Eq. (25.3) for A, C Hermitian and $U(t) \in U(N)$ arbitrary [74]?

4. Lie Algebras in Quantum Dynamics

A Lie algebra is a vector space L over some field F endowed with a mapping $[\cdot, \cdot] : L \times L \rightarrow L$, $(X, Y) \mapsto [X, Y]$, where

$$[\cdot, \cdot] \text{ is linear, i.e., } [X, aY + bZ] = a[X, Y] + b[X, Z], \forall a, b \in F$$

$$[\cdot, \cdot] \text{ is antisymmetric, i.e., } [Y, X] = -[X, Y]$$

$$[\cdot, \cdot] \text{ obeys Jacobi's identity: } [X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0$$

Show that

- (a) the Pauli matrices $(\{\sigma_x, \sigma_y, \sigma_z\}, [\cdot, \cdot])$ generate a Lie algebra (this is $\mathfrak{su}(2)$);
- (b) $(\mathbb{R}^3, \times)$ is a Lie algebra isomorphic to $\mathfrak{su}(2)$; interpret the relation between the Bloch equation $\dot{\vec{M}} = \vec{M} \times \vec{B}$ and the Liouville equation $\dot{\rho} = -i[H, \rho]$;
- (c[#]) the quaternions $q := q_0\mathbb{1} + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$ (with $\mathbf{i}\mathbf{j} = \mathbf{k}$, $\mathbf{j}\mathbf{k} = \mathbf{i}$, $\mathbf{k}\mathbf{i} = \mathbf{j}$, $q_\nu \in \mathbb{R}$ and $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbb{1}$) give rise to a group $SL(1, q)$ that is isomorphic to $SU(2)$;
- (d) the Heisenberg algebra $\{P, Q, \mathbb{1}\}$ and the oscillator algebra $\{P, Q, H, \mathbb{1}\}$, where $H := \frac{1}{2}(P^2 + Q^2)$ are Lie algebras; (NB[#]: quantum dynamics expressible by finite-dimensional Lie algebras can often be solved algebraically, see R.M. Wilcox, *J. Math. Phys.* **8** (1967), 962 or D.H. Sattinger and O.L. Weaver, *Lie Groups and Algebras with Applications to Physics, Geometry and Mechanics*, Springer, 1986);

- (e) in n spins-1/2, the entire Lie algebra $\mathfrak{su}(2^n)$ can be generated by commutation of the Pauli matrices on each spin and Ising terms $J_{k\ell} \sigma_{kz} \otimes \sigma_{\ell z}$ if the nonvanishing $J_{k\ell} \in \mathbb{R}$ can be represented as vertices of an arbitrary connected graph;
- (f) (e) is equivalent to saying that a system of n spins-1/2 is fully controllable and there is a universal set of quantum gates that can be realized (compare Section 25.2.1).

5.[#] *Spin: Recommended Further Reading on Foundations*

In proper terms, the spin is defined as *the quantum angular momentum S that has to be added to the orbital angular momentum $L := Q \times P$ so that the total angular momentum $J = L + S$ is invariant under Lorentzian—and already Galilean!—transformations.*

Convince yourself of these facts by reading:

- (a) a first simplified introduction in W. Greiner, *Theoretical Physics* Vol. 4 (Chap. 13) to see that spin arises naturally from linearising the equation of motion;
- (b) the famous originals of P.A.M. Dirac, *Proc. Royal Soc. Lond. A* **117** (1927), 610 and **118** (1928), 351 for the Lorentz invariance;
- (c) J.M. Lévy-Leblond, *Commun. Math. Phys.* **6** (1967), 286 and V.S. Varadarajan, *Geometry of Quantum Theory*, Springer 1985, (Chap. IX.8) for Galilei invariance;
- (d) the amusing story on Bohr's train trip to Leiden in December 1925 where he discussed spin-orbit coupling with Einstein and Ehrenfest (in: A. Pais, *The Genius of Science*, Cambridge University Press (2000), p 303 f).

Do you now see why spin already follows from Galilei invariance, whereas spin-orbit coupling requires Lorentz invariance?

References

- [1] R.P. Feynman, *Int. J. Theo. Phys.* **21**, 467 (1982).
- [2] R.P. Feynman, *Feynman Lectures on Computation*, Perseus Books, Reading, 1996.
- [3] R.R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*, Clarendon Press, Oxford, 1987.
- [4] *Encyclopedia of Nuclear Magnetic Resonance*, Vols I–IX, D.M. Grant and R.K. Harris, Eds., Wiley, Chichester, 1996.
- [5] L.S. Pontryagin, V.G. Bol'tanskii, R.S. Gamkrelidze, and E.F. Mischenko, *The Mathematical Theory of Optimal Processes*, Pergamon Press, New York, 1964.
- [6] E.B. Lee and L. Markus, *Foundations of Optimal Control Theory*, Wiley, New York, 1967.
- [7] S. Sastry, *Non-Linear Systems: Analysis, Stability and Control*, Springer, New York, 1999.
- [8] *The Control Handbook*, W.S. Levine, Ed., CRC Press, Boca Raton, FL, 1996.
- [9] A.G. Butkovskiy and Yu.I. Samoilenko, *Control of Quantum-Mechanical Processes and Systems*, Kluwer, Dordrecht, 1990.
- [10] D.J. Tannor and S.A. Rice, *J. Chem. Phys.* **83**, 5013 (1985).

- [11] S. Shi and H. Rabitz, *J. Chem. Phys.* **92**, 364 (1989).
- [12] [special volume on optimal control in chemical physics] *Chem. Phys.* **267**, (2001).
- [13] B.E. Kane, *Nature (London)* **393**, 133 (1998).
- [14] Yu. Makhlin, G. Schön, and A. Shnirman, *Rev. Mod. Phys.* **73**, 357 (2001).
- [15] V. Jurdjevic, *Geometric Control Theory*, Cambridge University Press, Cambridge, 1997.
- [16] D.G. Cory, A.F. Fahmy, and T.F. Havel, *Proc. of the 4th Workshop on Physics and Computation* (New England Complex Systems Institute, Boston, MA, 1996), pp. 87–91.
- [17] D. G. Cory, A. F. Fahmy, and T.F. Havel, *Proc. Natl. Acad. Sci. USA* **94**, 1634 (1997).
- [18] N. A. Gershenfeld and I.L. Chuang, *Science* **275**, 350 (1997).
- [19] D. Deutsch, *Proc. Royal Soc. London A* **400**, 97 (1985).
- [20] J.A. Jones and M. Mosca, *J. Chem. Phys.* **109**, 1648 (1998).
- [21] I.L. Chuang, L.M.K. Vandersypen, X.L. Zhou, D.W. Leung, and S. Lloyd, *Nature (London)* **393**, 143 (1998).
- [22] N. Linden, H. Barjat, and R. Freeman, *Chem. Phys. Lett.* **296**, 61 (1998).
- [23] R. Marx, A.F. Fahmy, J.M. Myers, W. Bermel, and S.J. Glaser, *Phys. Rev. A* **62**, 012310 (2000).
- [24] I.L. Chuang, N. Gershenfeld, and M.G. Kubinec, *Phys. Rev. Lett.* **80**, 3408 (1998).
- [25] J.A. Jones, M. Mosca, and R.H. Hansen, *Nature (London)* **393**, 344 (1998).
- [26] L.M.K. Vandersypen, M. Steffen, M.H. Sherwood, C.S. Yannoni, G. Breyta, I.L. Chuang, *Appl. Phys. Lett.* **76**, 468 (2000).
- [27] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, R. Cleve, and I.L. Chuang, *Phys. Rev. Lett.* **85**, 5452 (2000).
- [28] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, *Nature (London)* **414**, 883 (2001).
- [29] M. Mehring, *Appl. Magn. Reson.* **17**, 141 (1999).
- [30] J.A. Jones, *Fortschr. Physik* **48**, 909 (2000).
- [31] D.G. Cory, R. Laflamme, E. Knill, L. Viola, T.F. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, C. Negrevergne, M. Pravia, Y. Sharf, G. Teklemariam, Y.S. Weinstein, and W.H. Zurek, *Fortschr. Physik* **48**, 875 (2000).
- [32] T.F. Havel, S.S. Somaroo, C.H. Tseng, and D.G. Cory, *Appl. Algebra Eng. Comm.* **10**, 339 (2000).
- [33] J.A. Jones, *Prog. NMR Spectrosc.* **38**, 325 (2001).
- [34] J.A. Jones, *Phys. Chem. Comm.* **11**, 11 (2001).
- [35] S.J. Glaser, *Angew. Chem.* **113**, 151 (2001); *Angew. Chem. Int. Ed.* **40**, 147 (2001).
- [36] L.M.K. Vandersypen, C.S. Yannoni, and I.L. Chuang, *Preprint quant-ph/0012108* (2001).
- [37] T.F. Havel, D.G. Cory, S. Lloyd, N. Boulant, E.M. Fortunato, M.A. Pravia, G. Teklemariam, Y.S. Weinstein, A. Bhattacharyya, and J. Hou, *Am. J. Phys.* **70**, 345 (2002).
- [38] C. Ramanathan, N. Boulant, Z. Chen, D.L. Cory, I.L. Chuang, and M. Steffen, *Quant. Inf. Process.* **3**, 15 (2004).
- [39] L.M.K. Vandersypen and I.L. Chuang, *Rev. Mod. Phys.* **76**, 1037 (2004).
- [40] H. Sussmann and V. Jurdjevic, *J. Diff. Equat.* **12**, 95 (1972).

- [41] V. Jurdjevic and H. Sussmann, *J. Diff. Equat.* **12**, 313 (1972).
- [42] R.W. Brockett, *SIAM J. Control* **10**, 265 (1972).
- [43] R.W. Brockett, *SIAM J. Appl. Math.* **25**, 213 (1973).
- [44] W.M. Boothby and E.N. Wilson, *SIAM J. Control Optim.* **17**, 212 (1979).
- [45] T. Schulte-Herbrüggen, *Aspects and Prospects of High-Resolution NMR*, PhD Thesis, Diss-ETH 12752, Zürich, 1998.
- [46] F. Albertini and D. D'Alessandro, *IEEE Trans. Automat. Control* **48**, 1399 (2003).
- [47] S.J. Glaser, T. Schulte-Herbrüggen, M. Sieveking, O. Schedletsky, N.C. Nielsen, O.W. Sørensen, and C. Griesinger, *Science* **280**, 421 (1998).
- [48] T. Schulte-Herbrüggen, K. Hüper, U. Helmke, and S.J. Glaser, "Geometry of Quantum Computing by Hamiltonian Dynamics of Spin Ensembles", in: *Applications of Geometric Algebra in Computer Science and Engineering*, L. Dorst, C. Doran, and J. Lasenby, Eds., Birkhäuser, Boston, pp. 271–283 (2002).
- [49] C.S. Yannoni, M.H. Sherwood, D.C. Miller, I.L. Chuang, L.M.K. Vandersypen, and M.G. Kubinec, *Appl. Phys. Lett.* **75**, 3563 (1999).
- [50] D.G. Cory, M.D. Price, and T.F. Havel, *Physica D* **120**, 82 (1998).
- [51] Z.L. Mádi, R. Brüschweiler, and R.R. Ernst, *J. Chem. Phys.* **109**, 10603 (1998).
- [52] D.G. Cory, W. Mass, M. Price, E. Knill, R. Laflamme, W.H. Zurek, T.F. Havel, and S.S. Somaroo, *Phys. Rev. Lett.* **81**, 2152 (1998).
- [53] R. Marx, A.F. Fahmy, J.M. Myers, W. Bermel, and S.J. Glaser, in *Quantum Computing*, E. Donkor and A. R. Pirich, Eds., Proceedings of SPIE Vol. 4047, pp. 131–138 (2000).
- [54] E. Knill, R. Laflamme, R. Martinez, and C.H. Tseng, *Nature (London)* **404**, 368 (2000).
- [55] S. Lloyd, *Science* **261**, 1569 (1993).
- [56] W.S. Warren, *Science* **277**, 1688 (1997).
- [57] S.L. Braunstein, C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, *Phys. Rev. Lett.* **83**, 1054 (1999).
- [58] P. Hübler, J. Bargon, and S.J. Glaser, *J. Chem. Phys.* **113**, 2056 (2000).
- [59] C. Godard, P. Callaghan, J.L. Cunningham, S.B. Duckett, J.A.B. Lohmann, and R.N. Perutz, *Chem. Commun.* **2002**, 2836 (2002).
- [60] M.S. Anwar, D. Blazina, H.A. Carteret, S.B. Duckett, T.K. Halstead, J.A. Jones, C.M. Kozak, and R.J.K. Taylor, *Phys. Rev. Lett.* **93**, 040501 (2004).
- [61] M.S. Anwar, J.A. Jones, D. Blazina, S.B. Duckett, and H.A. Carteret, *Phys. Rev. A* **70**, 032324 (2004).
- [62] M.S. Anwar, D. Blazina, H.A. Carteret, S.B. Duckett, and J.A. Jones, *Chem. Phys. Lett.* **400**, 94 (2004).
- [63] J.P. Dunne, D. Blazina, S. Aiken, H.A. Carteret, S.B. Duckett, J.A. Jones, R. Poli, and A.C. Whitwood, *Dalton Trans.* **2004**, 3616 (2004).
- [64] D. Blazina, S.B. Duckett, T.K. Halstead, C.M. Kozak, R.J.K. Taylor, M.S. Anwar, J.A. Jones, and H.A. Carteret, *Magn. Res. Chem.* **43**, 200 (2005).
- [65] A.S. Verhulst, O. Liivak, M. Sherwood, H.M. Vieth, and I.L. Chuang, *Appl. Phys. Lett.* **79**, 2480 (2001).
- [66] J.M. Myers, A.F. Fahmy, S.J. Glaser, and R. Marx, *Phys. Rev. A* **63**, 032302 (2001).

- [67] R. Marx, *Anwendungen der NMR-Spektroskopie: von der Strukturaufklärung bis zum Quanten Computing*, PhD Thesis, University of Frankfurt, 2001.
- [68] F.M. Woodward and R. Brüschweiler, *Preprint quant-ph/0006024* (2000).
- [69] Arvind and D. Collins, *Phys. Rev. A* **68**, 052301 (2003).
- [70] N. Khaneja, R. Brockett, and S.J. Glaser, *Phys. Rev. A* **63**, 032308 (2001).
- [71] N. Khaneja and S.J. Glaser, *Chem. Phys.* **267**, 11 (2001).
- [72] T.O. Reiss, N. Khaneja, and S.J. Glaser, *J. Magn. Reson.* **154**, 192 (2002).
- [73] N. Khaneja, T.O. Reiss, C. Kehlet, T. Schulte-Herbrüggen, and S.J. Glaser, *J. Magn. Reson.* **172**, 296 (2005).
- [74] O.W. Sørensen, *Prog. NMR Spectrosc.* **21**, 503 (1989).
- [75] R.W. Brockett, in: *Proceedings of the IEEE Conference on Decision and Control, Austin, Texas 1988*, pp. 779–803 (1988).
- [76] U. Helmke and J.B. Moore, *Optimisation and Dynamical Systems*, Springer, Berlin, 1994.
- [77] U. Helmke, K. Hüper, J.B. Moore, and T. Schulte-Herbrüggen, *J. Global Optim.* **23**, 283 (2002).
- [78] R. Marx, A.F. Fahmy, J.M. Myers, W. Bermel, and S.J. Glaser, *Phys. Rev. A* **62**, 012310 (2000).
- [79] Y. Ohtsuki, G. Turinici, and H. Rabitz, *J. Chem. Phys.* **120**, 5509 (2004).
- [80] J.P. Paolo and R. Kosloff, *Phys. Rev. Lett.* **89**, 188301 (2002).
- [81] S.E. Sklarz and D.J. Tannor, *Chem. Phys.* **322**, 87 (2006).
- [82] T. Schulte-Herbrüggen, A.K. Spörl, N. Khaneja, and S.J. Glaser, *Phys. Rev. A* **72**, 042331 (2005).
- [83] J. Wesenberg, *Phys. Rev. A* **69**, 042323 (2004) [see in particular Eq. 14 in the previous version, *Preprint quant-ph/0312076*]
- [84] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
- [85] G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, and A. Zeilinger, *Quantum Information: an Introduction to Basic Concepts and Experiments* (Springer Tracts in Modern Physics Vol. 173), Springer, Heidelberg, 2000.
- [86] A. Saito, K. Kioi, Y. Akagi, N. Hashizume, and K. Ohta, *Preprint quant-ph/0001113* (2000).
- [87] A. Blais, *Phys. Rev. A* **64**, 022312 (2001).
- [88] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, *Phys. Rev. A* **52**, 3457 (1995).
- [89] N. Khaneja, S.J. Glaser, and R. Brockett, *Phys. Rev. A* **65**, 032301 (2002).
- [90] C.H. Tseng, S. Somaroo, Y. Sharf, E. Knill, R. Laflamme, T.F. Havel, and D.G. Cory, *Phys. Rev. A* **61**, 012302 (2000).
- [91] T. Yamamoto, Yu.A. Pashkin, O. Astaviev, Y. Nakamura, and J.S. Tsai, *Nature (London)* **425**, 941 (2003).
- [92] R. Laflamme, D.G. Cory, C. Negrevergne, and L. Viola, *Preprint quant-ph/0110029* (2001).

Part VII

Transfer of Quantum Information Between Different Types of Implementations

26 Quantum Repeater

Wolfgang Dür, Hans-J. Briegel, and Peter Zoller

26.1 Introduction

The reliable transmission of quantum information over noisy quantum channels is one of the major problems of quantum communication and quantum information processing. One of the main obstacles for high-fidelity transmission over large distances is the exponential scaling of channel noise and absorption with the distance. Since quantum signals can neither be cloned [1] nor amplified [2], standard techniques from classical communication technology (such as amplification of signals or the usage of repeater stations) cannot be directly applied.

In principle, methods developed in the context of quantum error correction can be used to protect a quantum signal against the influence of noise during transmission. One may for example use redundant encoding, i.e., encoding of each logical qubit into a number of physical qubit, using a concatenated error correction code [3]. This provides a method where the required resources (overhead) only scale polynomially with the distance. However, the requirements on measurements, local control operations, and channel noise are rather stringent. Before the influence of noise becomes too big (channel error rate must not exceed about 10^{-2}), error correction needs to be performed. That is, one needs to split the channel into small segments, where at intermediate local nodes error correction is applied. The small tolerable error rates limit the distance between such local nodes. In addition, the acceptable error rates for local operations (required to perform the error correction) are at the order of 10^{-5} – 10^{-4} , far below experimentally achievable accuracies with present day technology.

There exists an alternative approach, based on entanglement purification [4, 5] and teleportation [6]. The problem of transmitting *arbitrary, unknown quantum* states over a noisy channel is replaced by the task to establish a maximally entangled pair (or a pair with high fidelity) between two communication partners. This pair is then used for teleportation [6], thereby allowing for high-fidelity transmission of arbitrary quantum states, or for quantum key distribution [7]. In this case, the state to be prepared (a maximally entangled pair) is *fixed and known*, which makes this task potentially easier to be performed. By sending parts of maximally entangled states through a noisy quantum channel, one can obtain several copies of nonmaximally entangled states, which can then postprocessed (using an entanglement purification protocol) to obtain a smaller number of entangled pairs with enhanced fidelity.

In the limit of perfect local control operations, the distillation of perfect maximally entangled pure states is possible [4, 5]. Hence, faithful transmission over noisy quantum channels can be achieved. However, the acceptable channel noise such that entanglement purification

can be successfully applied, is limited. In particular, the channel should be such that one can still produce entangled pairs. For instance, for depolarizing channels this implies that the fidelity of output pairs has to be larger than $1/2$. The exponential distance dependence of noise and losses limit the maximal length of the channel. However, substantially larger distances than in the case when relying on quantum error correction techniques are possible.

For long-distance communication, one should split up the channel into segments of sufficiently small length (and hence sufficiently small channel noise). Then, maximally entangled pairs across each of the segments can be established. Finally, one can use entanglement swapping [8, 9], i.e., the teleportation of an already entangled qubit, to create maximally entangled pairs over larger distances.

However, the procedure described so far only works if maximally entangled pairs are available. When considering also imperfect local operations, as it is necessary in realistic scenarios, it is no longer possible to create maximally entangled pure states by means of entanglement purification. One can, however, still increase the fidelity and hence the amount of entanglement of the states. The maximal reachable fidelity thereby depends on the specific entanglement purification protocol and, more importantly, on the fidelity of local operations. A remarkable robustness of certain entanglement purification protocols under the influence of noisy local operations has been shown [10, 11]. In particular, errors of the order of several percent can be tolerated, while the fidelity of the entangled pairs can still be increased. For short-distance quantum communication, this already provides a way to achieve the desired goal, that is high-fidelity quantum communication.

For long-distance quantum communication, one may try to straightforwardly apply the scheme sketched above, i.e., use entanglement swapping to create far distant entangled pairs. In this case, however, the fidelity of the resulting long-distance pair will depend on the fidelity of the small-distance pairs, and will in fact decrease exponentially with the number of connected pairs. In particular, it might happen that the resulting pair is no longer entangled, and hence cannot be used for faithful teleportation. The solution to this problem is the *quantum repeater* [10, 11], which we discuss in this chapter. The basic idea is to connect only a few short-distance pair with fidelity F_0 , thereby decreasing the fidelity only slightly, and purifying these longer distance pairs to the initial fidelity F_0 . By using a nested scheme described below, one can generate entangled pairs over arbitrary distances with only polynomial overhead in the distance. In addition, such a protocol shows essentially the same robustness against local noise as standard entanglement purification protocols, i.e., large-distance quantum communication is feasible even for error rates of the order of percent. We emphasize that quantum repeaters cannot only deal with *any* kind of channel noise, but also with absorption and losses. The exponential scaling of noise and absorption with the distance can be overcome, and can be translated into only polynomial overhead in resources.

We remark that the generation of long-distance entanglement is not only useful in the context of quantum communication and quantum key distribution, but may also find applications in distributed quantum computation, for scalable quantum computation, or even for fault-tolerant quantum computation to improve error thresholds. In this context, high-fidelity entangled states—created by means of entanglement purification, or more generally by quantum repeaters—are used to implement nonlocal two-qubit gates between distant qubits [12–14].

26.2 Concept of the quantum repeater

Entanglement purification and connection of entangled pairs via a process known as entanglement swapping [8, 9] or teleportation [6] are the main tools required for a quantum repeater. While entanglement purification is discussed in detail in a separate chapter (see Chapter 11), we will briefly review the connection of nonmaximally entangled pairs here. Having these tools available, we proceed by introducing in detail the nested purification loop, the key ingredient of the quantum repeater. Required resources, in particular the polynomial scaling with the distance, will be discussed. We also show how to translate the polynomial overhead in spatial resources (i.e., qubits to be stored at repeater stations) into temporal resources.

26.2.1 Entanglement purification

Entanglement purification protocols are discussed in detail in Chapter 11. What is important in the present context is that one can generate entangled pairs with fidelity F_1 , starting from pairs with some initial fidelity F_0 , if (i) $F_1 < F_{\max}$, i.e., the required fidelity is smaller than the maximal reachable fidelity of the entanglement purification protocol and (ii) $F_0 > F_{\min}$, i.e., the initial fidelity is larger than the minimal required fidelity. The purification range of the entanglement purification protocol is given by the interval $(F_{\min}, F_{\max})$. On average, a certain number of elementary pairs, specified by the yield D_{ϕ^+, F_1} , will be required to achieve this aim. We call the inverse of this number M in the following. Typically, only a few (say 3–4) purification steps will be required, and hence M will be reasonable small (typically 20–30). In any case, M can be treated as a constant in the following.

26.2.2 Connection of elementary pairs

Given two maximally entangled pairs, one may connect them by means of a Bell measurement. That is, given pairs $A-C_1$ and C'_1-B , one can teleport the particle C_1 using the pair C'_1-B , where a Bell measurement on particles $C_1 C'_1$ is performed. The resulting state is a maximally entangled pair shared between A and B . That is, the entanglement is swapped and now shared between A and B , and hence this process is sometimes also called entanglement swapping [8, 9]. If $A-C_1$ and C'_1-B are short-distance entangled pairs shared between $A-C_1$ and C'_1-B , where C_1 might be some intermediate location between A and B , the resulting state a long-distance entangled pair, now shared between A and B (where we dispose the entangled pair shared between $C_1 C'_1$ here). In a similar way, one may connect L of these elementary pairs and obtain a maximally entangled pair of distance Ll_0 , where l_0 is the distance of elementary pairs. The connection of L pairs may be done (i) sequentially or, more practically, (ii) in parallel. Regarding (i), one first connects at location C_1 , then C_2 etc., where $L-1$ connections are required. In (ii), one first connect simultaneously the neighboring pairs at $C_1, C_3, \dots, C_{L-1}$. This leaves us with longer pairs $(A-C_2), (C_2-C_4), \dots, (C_{N-2}-B)$. Then one connect simultaneously these longer pairs at $C_2, C_6, \dots, C_{N-2}$, and so on, until we get a final pair between A and B .

However, if the elementary pairs are nonmaximally entangled, but have some fidelity $F < 1$, the resulting state after the connection procedure will not be maximally entangled either. This is already clear from the teleportation picture, as a nonmaximally entangled state

used for teleportation corresponds to imperfect transmission. For instance, if the elementary pairs are Werner states [15],

$$\rho_W(x) = x|\Phi_{00}\rangle\langle\Phi_{00}| + (1-x)/4\mathbb{1}_{AB}, \quad (26.1)$$

one obtains that the resulting state after L connections (and subsequent depolarization), is again a Werner state $\rho_W(x_L)$ with reduced fidelity x_L .¹ One finds

$$x_L = x^L, \quad (26.2)$$

and one may derive a similar formula when taking into account also noisy operations. Let us illustrate the influence of errors by considering the simple error model used in Chapter 11. Imperfect two-qubit operations are in this case modeled by first applying local white noise (depolarizing channels $\mathcal{M}$) to the individual qubits, followed by the perfect operation, $\mathcal{E}_{kl}\rho = U_{kl}[\mathcal{M}_k\mathcal{M}_l\rho]U_{kl}^\dagger$ with $\mathcal{M}_k\rho = p\rho + (1-p)/4\sum_{j=0}^3\sigma_j^{(k)}\rho\sigma_j^{(k)}$. The action of such a single-qubit depolarizing channel on one qubit of a Werner state $\rho_W(x)$ leads again to a Werner state, $\rho_W(px)$, with reduced fidelity. It follows that the imperfect connection of L Werner states leads, after depolarization, again to a Werner state with reduced fidelity

$$x_L = p^{2(L-1)}x^L, \quad (26.3)$$

where the exponent $2(L-1)$ of p can be understood from the fact that $L-1$ connection processes (Bell measurements) are required. Similar expressions can be obtained taking into account more general errors (correlated noise, errors in measurement and depolarization) [11], leading essentially to the same behavior.

26.2.3 Nested purification loops

We are now in a position to introduce (nested) entanglement purification, the basic notion of a quantum repeater [10, 11]. Our aim is to create an entangled pair between two distant locations A – B , which are connected by a noisy quantum channel. Due to exponential scaling of channel noise and absorption losses with the distance l , any quantum signal sent through the channel will be absorbed with large probability, and even if it finds its way through the channel it will be completely corrupted. To overcome this limitation, we divide the long channel into N smaller segments of length $l_0 = l/N$, where l_0 is chosen in such a way that entangled pairs with sufficiently high fidelity $F > F_{\min}$ can be created. Several of these pairs are then purified to constitute elementary pairs of length l_0 with some working fidelity F .

Given several copies of such elementary pairs of length l_0 and fidelity F , one creates by (i) the connection of L such pairs and (ii) the repurification to the working fidelity F new pairs of length Ll_0 , again with fidelity larger or equal F . The connection of L pairs reduces the fidelity, while entanglement purification restores the fidelity to the initial value. In order that such a process can work, one needs that the fidelity after the connection of L pairs is still larger than $F_{\min}$, the minimum required fidelity for entanglement purification, and that the working fidelity F is smaller than $F_{\max}$, the maximum reachable fidelity of entanglement distillation. Such an elementary *purification loop* is illustrated in Fig. 26.1.

The requirement that one always needs to stay within the purification regime of the entanglement purification protocol limits the number L of pairs that can be connected before

¹To be precise, x_L is related to the fidelity via $F_L = (3x_L + 1)/4$.

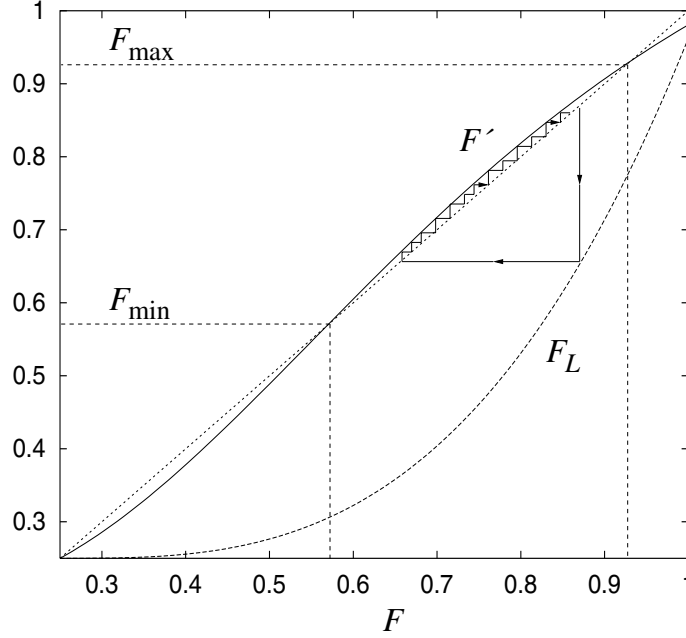


Figure 26.1. Purification loop: Connection of L elementary pairs and repurification to initial fidelity F . Figure taken from Ref. [10].

repurification. Hence, one needs a *nested procedure* to generate entanglement over a large distance. After one such purification loop, one has pairs of length Ll_0 , again with fidelity F . That is, one has an equivalent situation as at the beginning, but now the length of elementary pairs (at nesting level 1) is Ll_0 . Performing again a purification loop with these elementary pairs at nesting level 1, one ends up with pairs of distance L^2l_0 and fidelity F which now serve as elementary pairs at nesting level 2. Proceeding in the same way, we have that after n nesting levels, the distance of the pairs is L^n , i.e., only a logarithmic number $n = \log_L N$ of nesting levels is required to cover the distance $l = l_0 N$.

26.2.4 Resources

The logarithmic number of required nesting levels translates into a polynomial number of total resources (see Fig. 26.2).

At nesting level 1, one needs in total LM elementary pairs, as L pairs are connected, and M copies are required on average for repurification. At nesting level 2, blocks of the size LM now play the role of elementary pairs at nesting level 1. In total, L such blocks are connected and again M copies are required for repurification. Hence, at nesting level 2, the total number of resources is given by $(LM)LM = (LM)^2$. Hence, the total number R of elementary pairs

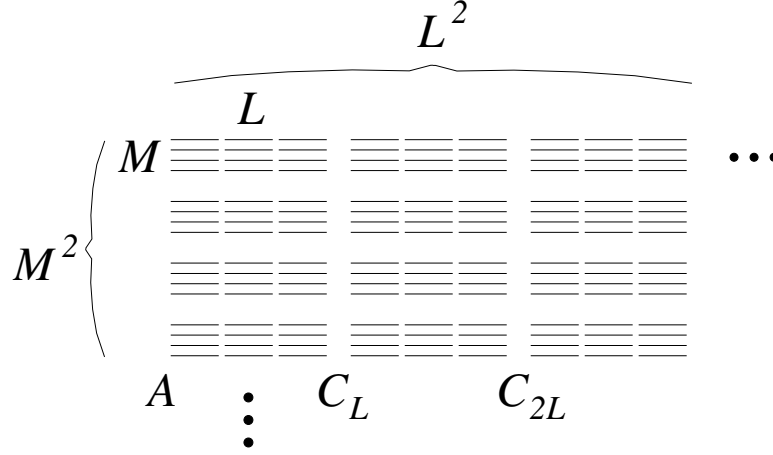


Figure 26.2. Nested purification with an array of elementary EPR pairs. Figure taken from Ref. [10].

will be $(LM)^n$. This result can be re-expressed as

$$R = N^{\log_L M + 1}, \quad (26.4)$$

which shows that the resources grow *polynomially* with the distance N .

The number of parallel channels required between the repeater stations is given by $M^n = M^{\log_L N} = N^{\log_L M}$ when using recurrence protocols of Refs. [4, 5], where all pairs are purified simultaneously. As shown in Refs. [10, 11], one can translate the polynomial overhead in spatial resources (i.e., number of required parallel channels, or, equivalently, the number of particles to be stored at each local node) into a *logarithmical* overhead in spatial resources and a *polynomial* overhead in temporal resources. That is, the required number of particles that need to be stored at local nodes is at most $n + 1$, while the temporal resources (i.e., the time required to obtain a long distant entangled pair with high fidelity) grows polynomially. This translation of the vertical axes in Fig. 26.2 to a temporal axis is achieved by using *entanglement pumping* rather than recurrence schemes of Refs. [4, 5] (see Chapter 11 for details). In the case of entanglement pumping, only two particles need to be stored at each site. Elementary pairs need to be sequentially generated, and are used to purify a second pair. This leads to the polynomial overhead in temporal resources. One additional particle needs to be stored at each nesting level, as one pair corresponding to this nesting level needs to be stored, while all other particles are already involved in the generation of elementary pairs at this nesting level. This results into a total of $n + 1 = \log_L N + 1$ number of particles that need to be stored at certain repeater stations (the end points). In all other repeater stations—which are used at lower nesting levels—the required spatial resources are smaller.

A further improvement in the required spatial resources has been achieved in Ref. [16]. In this scheme, only a constant number of qubits (namely two) need to be stored at each site. The basic idea is to make use of entanglement pumping, however once a pair over distance Ll_0 between sites C_1 and C_L is generated, one attempts to generate a new elementary pair

of distance Ll_0 by generating and purifying a pair of distance $(L - 2)l_0$ between the two *neighboring* sites C_2 and C_{L-1} . This is possible, since all intermediate repeater stations are not occupied with storage of another qubit, only sites C_1 and C_2 are. Finally, short-distance pairs between $C_1 - C_2$ and $C_{L-1} - C_L$ are generated and connected with the pair $C_2 - C_{L-1}$ to form a new elementary pair of distance Ll_0 , which is used to purify the initial pair. This scheme avoids the logarithmical increase of spatial resources with the distance, while leading to slightly more stringent error thresholds.

In the schemes described above, it is assumed that memory errors can be neglected at timescales required for the generation of long-distance entangled pairs. That is, entangled pairs need to be reliably stored until additional pairs required for entanglement purification are available. For the schemes with reduced spatial but increased temporal resources, this becomes challenging for larger distances as entangled pairs are created sequentially. The times to generate long-distance entangled pairs (and hence the required storage times) on an intercontinental scale have been estimated to be of the order of seconds. This implies that a reliable quantum memory with sufficiently long decoherence times is a necessary ingredient of a quantum repeater.

It is also worth mentioning that arbitrary channel errors, including absorption and losses, can be handled and overcome by the quantum repeater. In the case of absorption, one can devise schemes to detect the absence of a traveling qubit (e.g., a photon) [17]. The detection of such absorption errors is sufficient to guarantee that the standard quantum repeater scheme—with respective polynomial resources—can be applied. This scheme can at the same time overcome arbitrary additional channel noise, provided that absorption and error probability are not too big (which can always be achieved by choosing channel segments sufficiently short).

26.3 Proposals for Experimental Realization

A quantum repeater requires two main ingredients: (i) the possibility to generate entanglement over relatively short distances and (ii) the possibility to store and manipulate a few qubits at each repeater station to perform entanglement swapping and entanglement purification. The requirements on physical qubits for (i) and (ii) differ. While (i) is achieved by transmission of entangled qubits, and hence photons are ideal candidates to perform this task, (ii) is based on controlled manipulation and storage of qubits, where long coherence times and strong interactions between qubits are required. Since photons are in general difficult to store and interact only weakly, atomic qubits or solid-state-based qubits seem to be more suitable in the case of (ii). This implies that interfaces between flying qubits (e.g., photons) and qubits required for storage and manipulation (e.g., trapped atoms or ions) are desirable. In fact, theoretical proposals for such interfaces have been put forward [18], for example, based on atoms surrounded by a cavity. In the following, we will briefly discuss theoretical proposals for the implementation of quantum repeaters.

26.3.1 Photons and cavities

An implementation of a quantum repeater, based on atomic qubits for storage and manipulation, and photonic qubits for transportation was proposed in Ref. [17]. In this scheme, atoms are embedded in high finesse optical cavities which are connected by optical fibers. Atomic and photonic states are mapped onto each other using the interface proposed in [18]. The usage of auxiliary atoms in each of the cavities allows one to design a scheme that can detect and correct photon losses (absorption) which may occur during transmission. That is, the usage of a “back-up atom” allows one to check whether the transmission of the photon was successful or not, while maintaining the coherence (and possible entanglement) of the transmitted quantum information. In case of unsuccessful transmission (absorption of the photon), the process can simply be repeated. Also additional errors arising due to nonstationary environment—which leads to phase noise—can be corrected using a purification protocol [17]. This finally allows for the design of a quantum repeater that can generate entangled states over large distances.

26.3.2 Atomic ensembles

A scheme for a quantum repeater based on atomic ensembles interacting with light was proposed in [19]. Details of this scheme can be found in Chapter 27.

26.3.3 Quantum dots

The implementation of a quantum repeater in a solid-state architecture has been proposed recently [20]. In this case, the primary goal is to establish high-fidelity entangled pairs within a single solid-state device. That is, the quantum repeater is there not a tool to achieve high-fidelity quantum communication, but rather a source for distant entangled pairs within in the device. These entangled pairs can, for e.g., be used to implement two-qubit gates between distant qubits in a quantum processor.

The solid-state architecture in question consists of quantum dots, where spin degrees of freedom of trapped electrons are used for quantum processing. Rather than using single electron spins directly, each (logical) qubit consists of two spins, where $|0\rangle_L = |\Psi^-\rangle$, $|1\rangle_L = |\Psi^+\rangle$ with $|\Psi^\pm\rangle = 1/\sqrt{2}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$. That is, a (dynamical) decoherence free subspace is used, thereby suppressing most dominant noise sources and increasing coherence times by several orders of magnitude. Entanglement is generated between logical qubits, and hence both entanglement purification and connection have to be adopted accordingly. Locally generated entangled states are distributed by moving electrons—which is achieved by charge manipulation of trapping potentials—and eventually purified and connected following the standard repeater scheme. Based on directly available operations in such a set-up (partial Bell measurement, exchange interaction), a novel entanglement purification scheme and connection scheme for entangled states of logical qubits was designed [20]. The resulting purification map within the logical subspace is exactly the same as that for the recurrence protocol of Ref. [5]—also discussed in Chapter 11. In addition, all leakage errors, i.e., errors leading outside the logical subspace, are also corrected. The proposed scheme provides a valuable tool to generate distant entanglement in such quantum dot devices, which may, e.g., be used as a basic resource in scalable quantum computation architectures.

26.4 Summary and Conclusions

A quantum repeater is a fundamental tool for long-distance quantum communication, with potential applications also in scalable quantum computation design. While an experimental realization of a fully operating quantum repeater has not been reported so far, important parts required for a quantum repeater have already been experimentally demonstrated. These demonstration experiments include the *generation of entangled pairs* over a few tens of kilometers, *entanglement swapping* [8,9] and *entanglement purification* [21]. These experiments have been performed with entangled photons. Given the moderate error thresholds of the order of a percent, reliable creation of long-distance entanglement on demand seems feasible.

Acknowledgments

This work has been supported by the Austrian Science Foundation (FWF), the European Union (IST-2001-38877, -39227, OLAQUI, SCALA), the Österreichische Akademie der Wissenschaften through project APART (W.D.), and the Deutsche Forschungsgemeinschaft (DFG).

References

- [1] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982).
- [2] R. J. Glauber, in *Frontiers in Quantum Optics*, (eds. E. R. Pike & S. Sarkar), pp. 534–582. Bristol: Adam Hilger.
- [3] E. Knill and R. Laflamme, quant/ph-9608012. See also D. Aharonov and M. Ben-Or, Proc. 29th Annual ACM Symposium on Theory of Computing, ACM, New York, pp. 176 (1997), E-print quant-ph/9611025; C. Zalka, quant-ph/9612028.
- [4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996). C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [5] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).
- [6] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, Peres, and A. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [7] A. K. Ekert, *Phys. Rev. Lett.* **70**, 661 (1991).
- [8] M. Zukowski, A. Zeilinger, M. A. Horne, and A. Ekert, *Phys. Rev. Lett.* **71**, 4287 (1993); S. Bose, V. Vedral, and P. L. Knight, *Phys. Rev. A* **57**, 822 (1998).
- [9] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.* **80**, 3891 (1998);
- [10] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).
- [11] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, *Phys. Rev. A* **59**, 169-181 (1999).
- [12] D. Gottesman, quant-ph/9807006.
- [13] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, *Phys. Rev. Lett.* **86**, 544 (2001).
- [14] W. Dür and H.-J. Briegel, *Phys. Rev. Lett.* **90**, 067901 (2003).

- [15] R.F. Werner, *Phys. Rev. A* **40**, 4277 (1989).
- [16] L. Childress, J. M. Taylor, A. S. Sorensen, and M. D. Lukin, E-print quant-ph/0410123 and quant-ph/0502112.
- [17] S.J. Enk, J. I. Cirac, and P. Zoller, *Science* **279**, 205 (1998); S. J. van Enk, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **78**, 4293 (1997).
- [18] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, *Phys. Rev. Lett.* **78**, 3221 (1997).
- [19] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature* **414**, 413 (2001).
- [20] J. M. Taylor, W. Dür, P. Zoller, A. Yacoby, C. M. Marcus, and M. D. Lukin, *Phys. Rev. Lett.* **94**, 236803 (2005).
- [21] J.W. Pan, C. Simon, C. Brukner, and A. Zeilinger, *Nature* **409**, 1067 (2001).

27 Quantum Interface Between Light and Atomic Ensembles

Eugene S. Polzik and Jaromír Fiurášek¹

27.1 Introduction

Light–atoms quantum interface is an important component of a quantum network. Whereas light is a natural long-distance information carrier, it is difficult to keep information encoded in light for an extended period of time due to decoherence associated with its propagation. In the best case scenario, light at an optimal telecom wavelength propagating in a fiber loses half of its photons in 100 μ sec. Longer storage times for a quantum state of light require a faithful transfer onto an atomic quantum state where coherence and storage times can be much longer. Even stronger motivation for light–atoms interface is provided by the need to interconnect distant atomic nodes of a quantum network. One example of such connection is long-distance teleportation of atomic states discussed in this chapter. Another example is a two-step transfer of a quantum state: First from atomic sample A to light and then from the light onto a distant atomic sample B.

The light–atoms interface considered in this chapter can be characterized as deterministic. That is the result of it is not conditioned on probabilistic events, such as detecting a photon in a specific mode. The probabilistic type of light–atom interaction, though being another important ingredient of quantum information processing, cannot alone achieve the above-stated goals for communication and storage.

In this chapter, we shall concentrate on the quantum interface via free-space interaction of light with an atomic ensemble. This approach is a powerful alternative to the interface of light with a single atom. The latter approach, developed within the framework of cavity quantum-electrodynamics, requires strong coupling of an atom to a high-finesse optical cavity. With multiatom ensembles strong coupling to light can be achieved in the absence of a cavity, due to the fact that the interaction with a collective mode of an ensemble grows as the square root of the number of atoms. As shown in this chapter, the effective “figure of merit” of the light–atomic ensemble quantum interface is the resonant optical density of the atomic sample.

The light–atomic ensembles quantum interface considered in this chapter provides an example of a link between discrete and continuous quantum variables. Although most of the discussion in this chapter is formulated in the language of canonical operators x and p , which are usually associated with continuous variables, the interface we are discussing often works

¹This work was supported by EU under the projects COVAQIAL (FP6-511004) and Integrated Project QAP, by the Czech Ministry of Education under the project Information and Measurement in Optics (MSM 6198959213) and by Danish National Research Foundation.

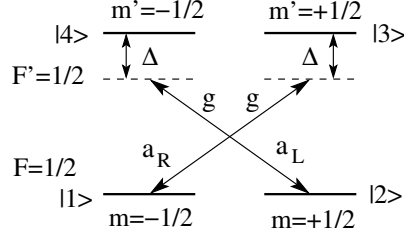


Figure 27.1. A level structure of the model atoms with total angular momentum $F = \frac{1}{2}$. (After Ref. [2]).

for an arbitrary single-mode state of light, which means that it also works for a qubit encoded into a state of a single photon.

27.2 Off-Resonant Interaction of Light with Atomic Ensemble

In this section we shall describe the basic physics behind the light matter interface and derive the effective Hamiltonian that governs the evolution of the system [1–3]. Consider a polarized light beam propagating along the z -axis through an ensemble of N_A spin- $\frac{1}{2}$ atoms with two degenerate ground states $|g, m_z = -\frac{1}{2}\rangle \equiv |1\rangle$ and $|g, m_z = \frac{1}{2}\rangle \equiv |2\rangle$ and two excited states $|e, m_z = -\frac{1}{2}\rangle \equiv |4\rangle$ and $|e, m_z = \frac{1}{2}\rangle \equiv |3\rangle$. The level structure is depicted in Fig. 27.1 and the geometry of the experiment is shown in Fig. 27.2.

As imposed by the selection rules, the left-hand (L) and right-hand (R) circularly polarized light modes couple to the transitions $|2\rangle \rightarrow |4\rangle$ and $|1\rangle \rightarrow |3\rangle$, respectively. The light frequency ω_L is strongly detuned from the atomic transition frequency ω_A , and the detuning $\Delta = \omega_L - \omega_A$ satisfies $|\Delta| \gg \gamma$ where γ is the spontaneous emission decay rate from excited to ground states. Due to the large detuning, only a tiny fraction of atoms gets excited in the course of evolution and most atoms remain in their ground states. The light–atoms interaction becomes dispersive and the light in each circularly polarized mode experiences a refraction index which depends on the number of atoms in state $|1\rangle$ or $|2\rangle$. If the populations of these two levels are slightly unbalanced, then the atomic medium exhibits a circular birefringence closely resembling a Faraday effect. The back-action of the light on the atoms results in the Stark shift of the frequency of the atomic transition $|1\rangle \rightarrow |3\rangle$ ($|2\rangle \rightarrow |4\rangle$) proportional to the intensity of the light beam in mode R (L).

Large detuning of light from atomic resonance helps in several respects. Alkali atoms used in experiments have the total angular momentum F in the ground state higher than $1/2$, e.g., $F = 4$ for cesium. Nevertheless, the simplified four-level model faithfully captures all the essential features of the interaction between atoms and light when the detuning is large compared to the hyperfine detuning of the excited state. Another experimental advantage brought about by the off-resonant character of the interaction is the insensitivity to the Doppler motion of atoms at detunings much larger than the Doppler width which allows using atomic gases at room temperature.

The effective Hamiltonian for a circularly polarized light beam propagating in a medium with refraction index n is $H_{\text{eff}} = \hbar(n-1)\omega a_j^\dagger a_j$, where a_j , $j = L, R$, denotes the annihilation operator of the light mode. The unitary transformation corresponding to the beam propagation

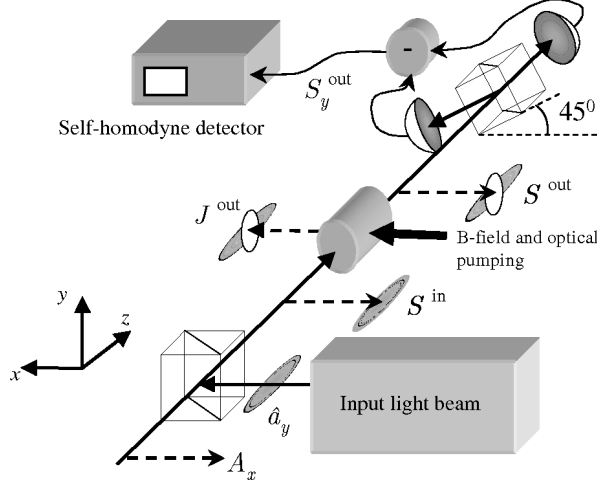


Figure 27.2. Geometry of the experimental setup. A weak quantum light beam linearly polarized along the y -axis is combined on a polarizing beam splitter with a strong coherent beam linearly polarized along the x -axis. The light propagates along the z -axis, passes through the atomic ensemble and impinges on a self-homodyne detector that measures a Stokes component of the light beam. (After Ref. [4]).

through the medium is $U = \exp[-ik_L \int (n(z) - 1) dz a_j^\dagger a_j]$, where $k_L = \omega_L/c$. In our case the refraction indices n_L and n_R for the two modes L and R may differ and $\int (n_R - 1) dz = \beta \Sigma_{11}$ and $\int (n_L - 1) dz = \beta \Sigma_{22}$, where $\Sigma_{\mu\nu} = \sum_{j=1}^{N_A} |\mu\rangle_j \langle \nu|$ are the collective atomic operators and we assume equal coupling strength of all atoms to the light beam. The resulting unitary $U = \exp(-iH_{\text{int}}/\hbar)$ where the total effective interaction Hamiltonian reads

$$\begin{aligned} H_{\text{int}} &= \hbar k_L \beta (\Sigma_{11} a_R^\dagger a_R + \Sigma_{22} a_L^\dagger a_L) \\ &= \hbar \frac{a}{4} (\Sigma_{22} - \Sigma_{11}) (a_R^\dagger a_R - a_L^\dagger a_L) - \hbar \frac{a}{4} N_A N_L. \end{aligned} \quad (27.1)$$

Here we introduced new coupling constant $a = -2k_L \beta$, $N_A = \Sigma_{11} + \Sigma_{22}$ and $N_L = a_L^\dagger a_L + a_R^\dagger a_R$. Since the total number of photons and atoms N_L and N_A is constant during the evolution, the term in the Hamiltonian (27.1) proportional to $N_A N_L$ can be dropped.

It is helpful to introduce the components of the collective atomic spin operator $\mathbf{J}$,

$$J_x = \frac{1}{2}(\Sigma_{12} + \Sigma_{21}), \quad J_y = \frac{1}{2i}(\Sigma_{21} - \Sigma_{12}), \quad J_z = \frac{1}{2}(\Sigma_{22} - \Sigma_{11}), \quad (27.2)$$

which satisfy the angular-momentum commutation relations $[J_j, J_k] = i\epsilon_{jkl} J_l$. Similarly we define the components of the Stokes vector $\mathbf{S}$ describing the polarization properties of the light beam,

$$S_1 = \frac{1}{2}(a_R^\dagger a_L + a_L^\dagger a_R), \quad S_2 = \frac{1}{2i}(a_R^\dagger a_L - a_L^\dagger a_R), \quad S_3 = \frac{1}{2}(a_R^\dagger a_R - a_L^\dagger a_L). \quad (27.3)$$

It holds that $[S_j, S_k] = i\epsilon_{jkl}S_l$. In terms of the operators $\mathbf{J}$ and $\mathbf{S}$, the effective interaction Hamiltonian (27.1) can be rewritten as

$$H_{\text{int}} = \hbar a J_z S_3. \quad (27.4)$$

Following closely Ref. [2], we shall now outline a more rigorous derivation of the effective interaction (27.4) which provides an explicit expression for the coupling constant a . The light beam is described by the field operators $a(z, t)$ satisfying the equal time commutation relations $[a_j(z, t), a_k^\dagger(z', t)] = \delta_{jk}\delta(z - z')$, $j, k = L, R$. It is convenient to formally define continuous atomic operators $\sigma_{\mu\nu}(z, t) = \lim_{\Delta z \rightarrow 0} \frac{1}{\rho A \Delta z} \sum_j^{z \leq z_j \leq z + \Delta z} |\mu\rangle_j \langle \nu|$ which satisfy

$$[\sigma_{\mu\nu}(z, t), \sigma_{\mu'\nu'}(z', t)] = \frac{1}{\rho A} \delta(z - z') (\delta_{\nu\mu'} \sigma_{\mu\nu'} - \delta_{\mu\nu'} \sigma_{\mu'\nu}). \quad (27.5)$$

Here A denotes the transverse area of the atomic ensemble and ρ is the number density of atoms, $\int_0^L \rho A dz = N_A$, and L is the length of the ensemble.

The interaction of light with the atoms is governed by the Jaynes–Cummings Hamiltonian,

$$\begin{aligned} H = & \hbar \int_0^L \sum_{j=1,2} \Delta \sigma_{j+2,j+2}(z, t) \rho A dz - i\hbar c \sum_{j=R,L} \int a_j^\dagger(z, t) \frac{\partial}{\partial z} a_j(z, t) dz \\ & + \hbar \int_0^L [g e^{ik_L z} a_R(z, t) \sigma_{31}(z, t) + g e^{ik_L z} a_L(z, t) \sigma_{42}(z, t) + \text{h.c.}] \rho A dz, \end{aligned}$$

where the coupling constant $g = d\sqrt{\omega_L/(2\hbar\epsilon_0 A)}$ and d is the dipole moment of the atomic transition. In the Heisenberg picture, the atomic and field operators evolve according to $\dot{X} = -i\hbar^{-1}[X, H]$, and we neglect the spontaneous decay. Since the interaction is off-resonant, the populations of the excited states are negligible and the atomic coherences σ_{13} and σ_{24} adiabatically follow the field operators,

$$\sigma_{13}(z, t) \approx -\frac{g}{\Delta} e^{ik_L z} a_R(z, t) \sigma_{11}(z, t), \quad \sigma_{24}(z, t) \approx -\frac{g}{\Delta} e^{ik_L z} a_L(z, t) \sigma_{22}(z, t).$$

Within this approximation, the ground-state populations $\sigma_{11}(z, t)$ and $\sigma_{22}(z, t)$ as well as the field intensities $a_j^\dagger(z, t) a_j(z, t)$, $j = L, R$, are constants of motion and the coupled Maxwell–Bloch equations for a_j and $\sigma_{\mu\nu}$ simplify to

$$\frac{\partial}{\partial z} a_R(z, \tau) = i \frac{2|g|^2 \rho A \sigma_{11}(z)}{\Delta c} a_R(z, \tau), \quad \frac{\partial}{\partial z} a_L(z, \tau) = i \frac{2|g|^2 \rho A \sigma_{22}(z)}{\Delta c} a_L(z, \tau), \quad (27.6)$$

where $\tau = t - z/c$ is the retarded time and

$$\frac{\partial}{\partial \tau} \sigma_{12}(z, \tau) = \frac{i2|g|^2}{\Delta} [a_L^\dagger(z, \tau) a_L(z, \tau) - a_R^\dagger(z, \tau) a_R(z, \tau)] \sigma_{12}(z, \tau). \quad (27.7)$$

The differential equations (27.6) and (27.7) can be solved by a straightforward integration. The resulting transformation for the elements of the total Stokes vector of the whole pulse,

$S_1 = \frac{c}{2} \int_0^T (a_R^\dagger(z, \tau) a_L(z, \tau) + \text{h.c.}) d\tau$, etc., is

$$\begin{aligned} S_1^{\text{out}} &= S_1^{\text{in}} \cos(aJ_z) - S_2^{\text{in}} \sin(aJ_z), \\ S_2^{\text{out}} &= S_2^{\text{in}} \cos(aJ_z) + S_1^{\text{in}} \sin(aJ_z), \\ S_3^{\text{out}} &= S_3^{\text{in}}, \end{aligned} \quad (27.8)$$

and similar formulas hold for the elements of the total atomic spin operator $\mathbf{J}$ at time T when the light beam passed through the ensemble,

$$\begin{aligned} J_x(T) &= J_x(0) \cos(aS_3) - J_y(0) \sin(aS_3), \\ J_y(T) &= J_y(0) \cos(aS_3) + J_x(0) \sin(aS_3), \\ J_z(T) &= J_z(0). \end{aligned} \quad (27.9)$$

These expressions coincide with the formulas obtained by solving the Heisenberg equations of motion induced by the effective Hamiltonian (27.4). The physical meaning of Eqs. (27.8) and (27.9) is that the light Stokes vector $\mathbf{S}$ is rotated along the z -axis by the angle proportional to J_z and, simultaneously, $\mathbf{J}$ is rotated by an angle proportional to S_3 . The coupling constant

$$a = \frac{4|g|^2}{\Delta c} = \frac{2\omega_L |d|^2}{\hbar \epsilon_0 A \Delta c} = \frac{3\gamma \lambda^2}{2\pi A \Delta}, \quad (27.10)$$

where λ is the wavelength and we used the relationship between the dipole moment d and the spontaneous decay rate, $\gamma = \omega_L^3 |d|^2 / (3\pi \epsilon_0 \hbar c^3)$.

In order to enhance the coupling between atoms and light, the atomic ensemble is prepared in a coherent spin state (CSS) with all atoms oriented along the x -axis. The ensemble can be polarized by optical pumping with a right-hand circularly polarized laser propagating along the x -axis. As a result, the J_x component of the collective atomic spin attains a macroscopic value and the operator can be replaced with a c -number, $J_x \approx N_A/2$. Under these conditions we can introduce effective quadratures for the atomic system, $x_A = J_y/\sqrt{J_x}$ and $p_A = J_z/\sqrt{J_x}$, which satisfy the canonical commutation relations $[x_A, p_A] = i$. This approximation can be visualized as follows. The atomic ensemble in a CSS with all atoms polarized along the x -axis can be pictured as a vector pointing to the north pole of the Bloch sphere. In the experiment, the state always remains close to the north pole and the Bloch sphere can be locally approximated by a tangent plane whose geometry is that of the phase space of a particle with momentum p_A and position x_A . Analogously, the light beam should contain a strong coherent component linearly polarized along the x -axis with mean number of photons N_L . The operator S_1 can be approximated by a c -number, $S_1 \approx N_L/2$, and we can define the light quadratures $x_L = S_2/\sqrt{S_1}$ and $p_L = S_3/\sqrt{S_1}$ and we have $[x_L, p_L] = i$. Note that the quadratures x_L and p_L can be interpreted as the quadratures of the optical mode linearly polarized along the y -axis.

Assuming $aS_3 \ll 1$ and $aJ_z \ll 1$, the transformations (27.8) and (27.9) can be linearized and we obtain the resulting effective linear canonical transformations for the light and atomic quadrature operators,

$$\begin{aligned} x_A^{\text{out}} &= x_A^{\text{in}} + \kappa p_L^{\text{in}}, & p_A^{\text{out}} &= p_A^{\text{in}}, \\ x_L^{\text{out}} &= x_L^{\text{in}} + \kappa p_A^{\text{in}}, & p_L^{\text{out}} &= p_L^{\text{in}}. \end{aligned} \quad (27.11)$$

The coupling constant $\kappa = a\sqrt{N_L N_A}/2$ can be written as $\kappa^2 = \alpha_0 \eta$, where

$$\eta = N_L \frac{\sigma}{A} \frac{\gamma^2}{\Delta^2}, \quad \alpha_0 = N_A \frac{\sigma}{A}, \quad (27.12)$$

η is the atomic depumping rate due to the absorption of light, α_0 is the optical density of the atomic sample on resonance, and $\sigma \propto \lambda^2$ is the atomic cross-section on resonance.

For such quantum information protocols as quantum memory (see below) the coupling constant κ should be of the order of unity. Simultaneously, the decoherence and losses which are proportional to the depumping rate η should remain as low as possible. This means that the optical density of the atomic sample should be high, $\alpha_0 \gg 1$. This condition can be marginally satisfied with atomic vapor at room temperature stored in a paraffin-coated glass cell, where $\alpha \approx 5$ has been observed. For other protocols, such as the generation of strongly entangled states, the coupling should be as strong as possible, $\kappa \geq 1$. High optical densities, required for satisfying this condition, can be achieved with cold atomic samples held in a magneto-optical trap and, in particular, with Bose–Einstein condensates, where α_0 can be of the order of 10^2 to 10^3 .

The linear canonical transformation (27.11) is often referred to as the quantum nondemolition (QND) interaction and is well known from the theory of quantum nondemolition measurements. Indeed, the x quadrature of light stores information about the p quadrature of atoms, while the p_A quadrature is a constant of motion and the noise associated with the measurement of p_A is fed to the conjugate quadrature x_A in the form of the term κp_L . In particular, if $\kappa = 1$ then we recover the so-called continuous-variable controlled NOT gate [5]. In addition to the two-mode gate (27.11), it is also experimentally feasible to apply arbitrary single-mode phase-space rotations. The light quadratures can be rotated by sending the beam through a wave plate and the rotation of atomic quadratures can be accomplished by illuminating the ensemble with strong coherent far-detuned laser beams. Alternatively, it is also possible to switch between the coupling to the p_A and x_A quadratures by sending the light beam through the atomic sample either along the z or y axes, respectively.

The light Stokes vector components (i.e., the x_L or p_L quadratures) can be measured by sending the light through a wave plate and a polarizing beam splitter which spatially separates two linear orthogonally polarized beams; see Fig. 27.2. The power of these two beams is measured with the high efficiency linear photodiodes and the two powers are subtracted. The x_L quadrature is proportional to the difference of the power of two linear polarizations oriented at $+45^\circ$ and -45° with respect to the x -axis. The p_L quadrature is proportional to the difference of the power of two circular polarizations. If the S_1 component is in a strong coherent state then this scheme becomes equivalent to self-homodyning where one polarization mode plays the role of the local oscillator while the orthogonal mode is the signal whose quadrature is detected. In quantum information applications, we require that the measurement is shot-noise limited, and the detected quadrature variance should be proportional to the mean number of photons N_L in the strong beam.

Experimental realization of quantum information protocols described here requires achieving the level of quantum fluctuations for both the light pulse and the atomic collective spin variables. The relative size of the quantum noise (the shot noise for light and the projection noise for atoms) is of the order of $1/\sqrt{N}$, where N is the number of photons per pulse or the number of atoms in the samples, respectively. It is possible to reduce technical noise to

the level much lower than this quantum limit with dc detection provided that $N_L \leq 10^8$ in current experiments. In order to achieve sufficiently strong κ for gasses at room temperature, it is necessary to go to a higher number of atoms, and correspondingly to a higher number of photons per pulse. Quantum limited noise for such a high number of particles can be achieved with the help of ac detection at frequency Ω of few hundred of kHz or higher. This approach allows us to suppress technical noise by several orders of magnitude and quantum-limited measurements can be carried out with up to $N_L = 10^{12}$. However, the light sidebands at the frequency $\pm\Omega$ around the carrier frequency ω_L do not couple to the atoms. This problem is resolved by placing the atoms into a constant magnetic field B oriented along the x -axis. The atomic spins precess with Larmor frequency Ω which should coincide with the frequency of the detected light sidebands.

The application of the magnetic field resolves the problems with the technical noise but it significantly alters the light–matter coupling. At each time instant t the atomic quadrature $x_A(t)$ stores information about $S_3(t)$. However, after some time the rotation exchanges x_A and p_A , the information about $S_3(t)$ is fed to the light Stokes operator $S_2(t + \Delta t)$ and the QND character of the interaction is lost. The evolution of the collective atomic spin operators is governed by the Heisenberg–Langevin equations

$$\begin{aligned}\dot{J}_y(t) &= -\Omega J_z(t) - \Gamma J_y(t) + aJ_x S_3(t) + \mathcal{F}_y(t), \\ \dot{J}_z(t) &= \Omega J_y(t) - \Gamma J_z(t) + \mathcal{F}_z(t),\end{aligned}\quad (27.13)$$

where Γ is the decay rate of the atomic coherence and $\mathcal{F}$ are the quantum Langevin stochastic forces. The input–output relations for the light Stokes vector components at time t can be written as

$$S_2^{\text{out}}(t) = S_2^{\text{in}}(t) + aS_1(t)J_z(t), \quad S_3^{\text{out}}(t) = S_3^{\text{in}}(t). \quad (27.14)$$

The validity of this description has been confirmed in an experiment where a cw polarization squeezed state of light has been sent through the atomic ensemble and the noise spectrum of S_2^{out} was measured [4]. In this experiment, the pumping and repumping beams were simultaneously applied to the sample which resulted in decay to the coherent spin state, i.e., to the vacuum state in the Gaussian approximation. Thus the decay Γ has to be taken into account. Equations (27.13) can be solved by performing a Fourier transformation and the resulting noise spectrum of S_2^{out} normalized to the shot noise can be expressed as

$$\Phi(\omega) = V_{S_2} + \frac{\frac{1}{2}\kappa^2}{(\Omega - \omega)^2 + \Gamma^2} \left[\frac{\kappa^2}{2} V_{S_3} + 2\Gamma \right]. \quad (27.15)$$

The first term V_{S_2} represents the S_2^{in} variance in shot-noise units. The second term in the brackets, 2Γ , represents the quantum noise of the atomic ensemble recorded in the light beam. Most interesting is the first term in the brackets, proportional to the variance of S_3 . This term represents the quantum noise of S_3 that was recorded in the atomic ensemble and subsequently transferred again back to the light beam to the S_2 component of the Stokes vector.

With ac detection and a single atomic sample placed in a magnetic field, it is more difficult to recover the QND-type coupling (27.11), which would be desirable for applications in quantum information processing. Remarkably, the QND coupling can be recovered if *two*

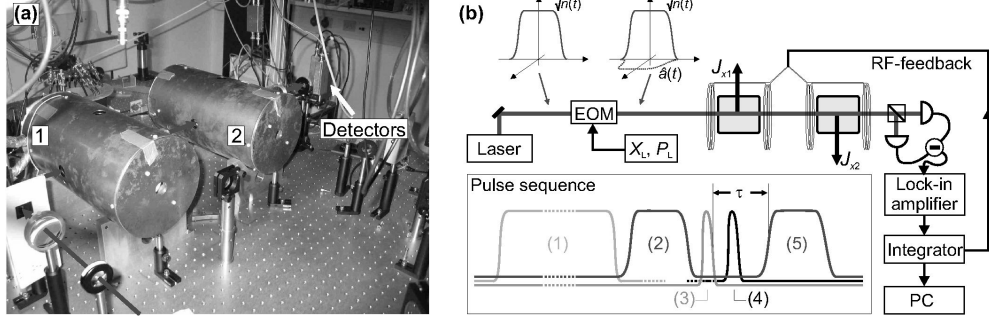


Figure 27.3. Experimental setup. (a) Two cesium samples in glass cells at approximately room temperature are placed inside magnetic shields 1, 2. The path of the light pulses interacting with atomic ensembles is shown with arrows. (b) The simplified layout of the experiment. Cesium atoms are optically pumped into $|F = 4, m_x = 4\rangle$ ground state in the first cell and into $|F = 4, m_x = -4\rangle$ in the second cell to form coherent spin states oriented along the $+x$ -axis for cell 1 and along $-x$ for cell 2. Coherent input state of light with the desired displacements x_L, p_L can be generated with the electro-optic modulator (EOM). The inset shows the pulse sequence. Pulse 1 is the optical pumping, pulse 2 is the input light pulse which entangles the two atomic ensembles. Pulse 3 is the magnetic feedback pulse. Pulse 4 is the magnetic $\pi/2$ pulse used for the read out of one of the atomic operators. Pulse 5 is the probe optical pulse that reads the state of the atomic ensembles. This pulse sequence can be used to entangle the two atomic ensembles or to store the quantum state of the input light beam into atomic memory. (After Ref. [7]).

atomic ensembles 1 and 2 polarized in opposite directions and both placed in a magnetic field are used as a single unit and the light passes through both ensembles in series [6, 7]. This approach has the added bonus that the effective atomic quadratures that couple to the light are nonlocal, i.e., balanced superpositions of the quadratures of atomic ensembles 1 and 2. This can be explored to create entanglement of two distant macroscopic atomic clouds as discussed below.

Suppose that by means of optical pumping the atomic spins are aligned along the x -axis and the two ensembles 1 and 2 are polarized in the opposite directions, $\langle J_{x1} \rangle = -\langle J_{x2} \rangle = J_x$; see Fig. 27.3. The formulas relating the input and output components of the Stokes vector that describes the polarization of the light beam are a direct generalization of Eq. (27.14) and we have

$$S_2^{\text{out}}(t) = S_2^{\text{in}}(t) + aS_1(t)[J_{z1}(t) + J_{z2}(t)], \quad S_3^{\text{out}}(t) = S_3^{\text{in}}(t). \quad (27.16)$$

The Heisenberg equations of motion for the y and z components of the collective atomic spin vectors can be formulated as follows:

$$\begin{aligned} \dot{J}_{z1}(t) &= \Omega J_{y1}, & \dot{J}_{z2}(t) &= \Omega J_{y2}(t), \\ \dot{J}_{y1}(t) &= -\Omega J_{z1}(t) + aJ_x S_3(t), & \dot{J}_{y2}(t) &= -\Omega J_{z2}(t) - aJ_x S_3(t). \end{aligned} \quad (27.17)$$

We define atomic operators in the frame rotating with frequency Ω ,

$$\tilde{J}_{y1,2}(t) = J_{y1,2} \cos(\Omega t) + J_{z1,2} \sin(\Omega t), \quad \tilde{J}_{z1,2}(t) = J_{z1,2} \cos(\Omega t) - J_{y1,2} \sin(\Omega t).$$

It is also helpful to introduce the “nonlocal” operators that are superpositions of the collective spin operators of atomic clouds 1 and 2,

$$\tilde{J}_{y\pm} = \frac{1}{\sqrt{2}}(\tilde{J}_{y1} \pm \tilde{J}_{y2}), \quad \tilde{J}_{z\pm} = \frac{1}{\sqrt{2}}(\tilde{J}_{z1} \pm \tilde{J}_{z2}). \quad (27.18)$$

The solution of the Heisenberg equations of motion (27.17) reads

$$\begin{aligned} \tilde{J}_{y+}(t) &= \tilde{J}_{y+}(0), & \tilde{J}_{y-}(t) &= \tilde{J}_{y-}(0) + \sqrt{2}aJ_x \int_0^t S_3(\tau) \cos(\Omega\tau) d\tau, \\ \tilde{J}_{z+}(t) &= \tilde{J}_{z+}(0), & \tilde{J}_{z-}(t) &= \tilde{J}_{z-}(0) - \sqrt{2}aJ_x \int_0^t S_3(\tau) \sin(\Omega\tau) d\tau. \end{aligned} \quad (27.19)$$

Note that the “plus” operators in the rotating frame are constants of motion while the information about the light is fed to the “minus” operators. Using the commutation relations $[J_{y1}, J_{z1}] = iJ_x$ and $[J_{y2}, J_{z2}] = -iJ_x$ one can derive the commutation relations for the nonlocal operators in the rotating frame,

$$[\tilde{J}_{y+}, \tilde{J}_{z+}] = 0, \quad [\tilde{J}_{y-}, \tilde{J}_{z+}] = iJ_x, \quad [\tilde{J}_{y-}, \tilde{J}_{z-}] = 0, \quad [\tilde{J}_{y+}, \tilde{J}_{z-}] = iJ_x.$$

It follows from these relations that the quadrature operators of two effective atomic modes A and B should be defined as follows:

$$x_A = \frac{\tilde{J}_{y-}}{\sqrt{J_x}}, \quad p_A = \frac{\tilde{J}_{z+}}{\sqrt{J_x}}, \quad x_B = \frac{\tilde{J}_{y+}}{\sqrt{J_x}}, \quad p_B = \frac{\tilde{J}_{z-}}{\sqrt{J_x}}. \quad (27.20)$$

These operators satisfy the canonical commutation relations $[x_j, p_k] = i\delta_{jk}$.

In terms of the nonlocal atomic operators in rotating frame the input–output transformations for the Stokes operators read

$$S_2^{\text{out}}(t) = S_2^{\text{in}}(t) + a\sqrt{2}S_1(t)[\tilde{J}_{z+} \cos(\Omega t) + \tilde{J}_{y+} \sin(\Omega t)], \quad S_3^{\text{out}}(t) = S_3^{\text{in}}(t). \quad (27.21)$$

The quadrature operators of light sidebands with modulation $\cos(\Omega t)$ and $\sin(\Omega t)$ can be defined as properly normalized Stokes operators,

$$\begin{aligned} x_L &= \sqrt{\frac{2}{S_1}} \int S_2(t) \cos(\Omega t) dt, & p_L &= \sqrt{\frac{2}{S_1}} \int S_3(t) \cos(\Omega t) dt, \\ x_M &= \sqrt{\frac{2}{S_1}} \int S_2(t) \sin(\Omega t) dt, & p_M &= \sqrt{\frac{2}{S_1}} \int S_3(t) \sin(\Omega t) dt, \end{aligned} \quad (27.22)$$

where the integration is carried over the whole pulse and $S_1 = \int S_1(t) dt$. These quadratures satisfy canonical commutation relations provided that the pulse duration is much larger than $2\pi/\Omega$. This condition is satisfied in the present experiments where $\Omega = 330$ kHz and the pulse is approximately 1 ms long.

On inserting the definitions of the atomic and light quadrature operators in Eqs. (27.19) and (27.21) we finally obtain two decoupled systems of linear canonical transformations. Coupling of the modes A and L is governed by the transformations (27.11) and the atomic mode

B couples to the light mode M according to

$$\begin{aligned} x_B^{\text{out}} &= x_B^{\text{in}}, & p_B^{\text{out}} &= p_B^{\text{in}} - \kappa p_M^{\text{in}}, \\ p_M^{\text{out}} &= p_M^{\text{in}}, & x_M^{\text{out}} &= x_M^{\text{in}} + \kappa x_B^{\text{in}}. \end{aligned} \quad (27.23)$$

The coupling constant $\kappa = a\sqrt{S_1 J_x}$ as it would have been for two atomic samples without the magnetic field. We have thus shown that the QND-type interaction can be recovered if a pair of atomic ensembles with oppositely polarized spins is utilized. In the following sections, we shall illustrate various applications of the QND coupling (27.11) for quantum information processing. For the sake of presentation simplicity, below we will use the term “an atomic ensemble” although depending on the particular implementation the basic unit interacting with light may actually comprise two ensembles polarized in opposite directions.

27.3 Entanglement of Two Atomic Clouds

The basic application of the QND interaction (27.11) is to measure the atomic quadrature in a nondestructive way. This measurement reduces the uncertainty of the quadrature p_A and if the atomic ensemble was initially in a coherent state, then the measurement reduces the fluctuations of p_A below the shot-noise level and the atomic ensemble is prepared in a squeezed state. The squeezed state is generally not centered on vacuum but is displaced by an amount that is proportional to the value of the measured light quadrature x_L . If the atomic state is displaced in such a way that this off-set is canceled then the ensemble is unconditionally prepared in a pure squeezed vacuum state. The displacement can be accomplished by a tiny rotation of the atomic spin along the y -axis, which couples the operators J_x and J_z . For small rotation angles ϵ , we have $J_z^{\text{new}} \approx J_z^{\text{old}} + \epsilon J_x$ and the quadrature is displaced by the amount $\epsilon\sqrt{J_x}$. In the system consisting of two atomic ensembles, the displacement has to be applied simultaneously and symmetrically to both ensembles so that the appropriate symmetric nonlocal quadrature is displaced.

The optimal classical gain g in the applied displacement can be determined by minimizing the noise of the displaced quadrature

$$p'_A = p_A - g(x_L + \kappa p_A) = (1 - g\kappa)p_A - gx_L. \quad (27.24)$$

Assuming that both atoms and light are initially in coherent states, then $\langle(\Delta x_L)^2\rangle = \langle(\Delta p_A)^2\rangle = 1/2$ and the optimum gain is given by $g_{\text{opt}} = \kappa/(1 + \kappa^2)$. The variance of the atomic quadrature p'_A is reduced below the shot-noise level $1/2$,

$$\langle(\Delta p'_A)^2\rangle = \frac{1}{2} \frac{1}{1 + \kappa^2}, \quad (27.25)$$

and 3 dB squeezing is reached already for $\kappa = 1$. The great advantage of the light–atom interaction is that it may be experimentally feasible to achieve $\kappa \gg 1$ which would result in very strong squeezing of the atomic ensemble. For instance, with $\kappa = 5$ we would obtain 14 dB of squeezing, which is much higher than the squeezing of light achievable in optical parametric processes. In practice, the maximum amount of squeezing would be mainly limited by the

losses, spontaneous emission, and other decoherence effects. As shown in [8], when spontaneous emission is taken into account, the achievable degree of squeezing scales approximately as $1/\sqrt{\alpha_0}$ for large α_0 .

In the setting with two atomic ensembles, the quadrature that is squeezed is a balanced combination of the quadratures of the two atomic ensembles 1 and 2, $p_A = (p_1 + p_2)/\sqrt{2}$. In this way, none of the two ensembles is prepared in a squeezed state separately, but the two ensembles are in an entangled Gaussian state. Moreover, in addition to detecting x_L , we can also measure the quadrature x_M and squeeze the atomic mode B in the quadrature $x_B = (x_1 - x_2)/\sqrt{2}$. In this way, the two atomic ensembles are prepared in a two-mode squeezed vacuum state. Such state is an implementation of the Einstein–Podolsky–Rosen entangled state introduced by these authors in 1935 in their famous paper on completeness of quantum mechanics [9].

The entanglement of two distant macroscopic atomic clouds has been demonstrated experimentally [6]. The vapor of Cs atoms at room temperature was contained in two glass cells coated from inside with a special paraffin coating to reduce the Cs spin decoherence due to collisions with walls. In order to inhibit the depolarization of spin states, each atomic cell was protected from the external spurious magnetic fields by careful shielding. Initially, the atoms are prepared in a coherent spin state (CSS) by polarizing along the x -axis by optical pumping. The close proximity of the prepared state to CSS is checked by observing the linear dependence of the variance of the measured Stokes components on the size of the collective spin J_x . An independent measurement via magneto-optical resonance yielded the degree of spin polarization better than 99%. The linear dependence combined with experimentally verified almost perfect spin polarization proves that the ensemble is very close to CSS. Then, the pumping lasers are switched off and the first (entangling) beam is sent through the two atomic cells. At the output, the cos and sin components at frequency Ω of the Stokes operator S_2 are measured simultaneously, i.e., x_L^{ent} and x_M^{ent} are detected. This prepares the atomic ensemble in an entangled state. To verify the presence of entanglement after time t , a second strong coherent verifying pulse is sent through the atoms and the two light quadratures $x_L^{\text{ver}} = x_{L,0}^{\text{ver}} + \kappa p_A^{\text{ent}}$ and $x_M^{\text{ver}} = x_{M,0}^{\text{ver}} + \kappa x_B^{\text{ent}}$ are measured. This provides information about the two squeezed nonlocal quadratures of the entangled atomic ensembles. In this experiment, it is not necessary to physically displace the atomic state after the entangling pulse, instead, one can displace the measured quadratures of the verifying pulse and the atomic squeezing can be inferred from the fluctuations of the difference operators $\Delta X = x_L^{\text{ver}} - g x_L^{\text{ent}}$ and $\Delta P = x_M^{\text{ver}} - g x_M^{\text{ent}}$. In a later experiment, a deterministic entangled state of atoms was achieved by applying to atoms the displacement conditioned on the result of the first measurement.

The entanglement was tested using the Duan criterion [10] which states that the two-mode state is entangled if the condition

$$\Delta_{\text{EPR}}^2 \equiv \langle (\Delta p_A^{\text{ent}})^2 \rangle + \langle (\Delta x_B^{\text{ent}})^2 \rangle < 1 \quad (27.26)$$

is satisfied. The variances appearing in the criterion can be inferred from the variances of ΔX and ΔP , respectively. Since the verifying light beam is in a coherent state, we have $\langle (\Delta X)^2 \rangle = 1/2 + \kappa^2 \langle (\Delta p_A^{\text{ent}})^2 \rangle$ and $\langle (\Delta P)^2 \rangle = 1/2 + \kappa^2 \langle (\Delta x_B^{\text{ent}})^2 \rangle$. In terms of the measured variances, the entanglement criterion can be thus rephrased as

$$\langle (\Delta X)^2 \rangle + \langle (\Delta P)^2 \rangle < 1 + \kappa^2. \quad (27.27)$$

In the experiment, the minimum observed EPR variance was $\Delta_{\text{EPR},\text{min}}^2 \approx 0.65$ which confirms that an entangled state has been prepared. The entanglement survived for the time 0.5 ms which was the delay between the entangling and verifying pulses.

27.4 Quantum Memory for Light

One of the major goals of quantum information processing is the development of a reliable deterministic quantum memory for light, where the quantum state of light could be stored for some time period T and retrieved at a later stage. The quantum memory for light is a key element of the envisioned quantum communication networks, where the quantum repeaters should allow distribution of entanglement over arbitrary long distances. The quantum memory is also required for other applications such as scalable quantum computing with linear optics. Note that a conditional atomic state generated upon detection of a photon emitted by an atom is also sometimes referred to, as quantum memory. Such protocols usually work in a probabilistic way. As opposed to such approaches, here we discuss the deterministic memory for an unknown, externally provided state of light. The criteria for the quantum memory for light can be summarized as follows:

1. The memory should work for a class of independently prepared quantum states of light.
2. The storage should provide the fidelity higher than the fidelity for a classical storage protocol which involves measurement and reparation and sends and stores only classical information.
3. The stored state should be readable.

The off-resonant interaction of light with an atomic ensemble provides a natural interface between light and atoms. The QND interaction entangles the atoms with the light beam and this entanglement can be exploited to transfer the state of the light beam onto the state of the atomic ensembles.

The simplest memory storage protocol consists of sending the light beam through the atomic ensembles, measuring the quadrature of the output light beam, and applying an appropriate feedback to the atoms. This protocol has been already implemented experimentally, and storage of coherent light states with fidelity exceeding the maximum fidelity that can be achieved by measure-and-prepare protocols has been demonstrated [7]. Consider the light and atomic quadratures after the QND interaction (27.11). If the light quadrature x_L is measured and the atomic quadrature p_A is displaced by an amount $-gx_L$, then the resulting atomic quadratures read

$$x_A^{\text{mem}} = x_A^{\text{in}} + \kappa p_L^{\text{in}}, \quad p_A^{\text{mem}} = (1 - g\kappa)p_A^{\text{in}} - gx_L^{\text{in}}. \quad (27.28)$$

In particular, if $\kappa = 1$ and $g = 1$, then the light quadrature x_L is perfectly stored in the atomic quadrature p_A . The conjugate light quadrature p_L was stored in the atomic quadrature x_A during the QND interaction due to the feedback of light on atoms. The storage of p_L is only imperfect due to the noise stemming from the original atomic quadrature x_A^{in} . This noise can be suppressed by preparing the atomic ensembles in a squeezed state before the memory

protocol is applied. In the limit of infinite squeezing, we obtain in theory an ideal transfer of the light state onto atoms, $x_A^{\text{mem}} = p_L^{\text{in}}$ and $p_A^{\text{mem}} = -x_L^{\text{in}}$.

Note that the above conclusion is reached on the basis of Heisenberg equations of motion which are state independent. This means that an arbitrary single mode input state can be perfectly mapped onto an atomic ensemble state. This input state should be in a form of a linearly polarized light pulse. This pulse is then mixed on a polarizing beam splitter with an orthogonally polarized strong pulse in a coherent state. The two pulses must have a common spatio-temporal mode. Under these conditions, and provided that the atomic sample is initially in a perfectly squeezed state, the quantum memory protocol should work for a qubit state of light, or any other state. The only limitation is that the mean photon number of this state must be much smaller than the mean photon number of the strong coherent pulse which drives the interaction. In the case of less than perfect squeezing of the initial atomic state, or even for the coherent initial state of atoms, the memory protocol can still provide the fidelity of mapping for a light qubit which is better than the fidelity for classical mapping. This subject is beyond the scope of the present article and will be considered in detail elsewhere [11].

The experimental demonstration of quantum memory for light has been carried out for a class of weak coherent states with mean photon number in the range between zero and a few. In the experiment a pair of atomic ensembles in glass cells placed in external magnetic field and polarized in the opposite directions served as the memory unit; see Fig. 27.3. The initial coherent states of light at the Ω sidebands were prepared by an electro-optical modulator. The weak horizontally polarized coherent state and the strong coherent vertically polarized beam with identical spatio-temporal profiles were sent through the atoms and the quadrature x_L^{out} was detected in a self-homodyne detector consisting of a polarizing beam splitter, two photodiodes, a lock-in amplifier and an integrator. The atoms were then displaced by applying a radio-frequency magnetic pulse conditioned on the measurement result. The success of the quantum memory storage was verified by the read-out pulse that was sent through the atoms after a variable delay τ . From the measurement of the read-out quadrature $x_L^{\text{ro}} = x_L^{\text{ro, in}} + \kappa p_A^{\text{mem}}$ we can determine the gain of the storage for the x_L quadrature, $g_x = -\kappa^{-1} \langle x_L^{\text{ro}} \rangle / \langle x_L^{\text{in}} \rangle$, and the variance $\sigma_x^2 = [\langle (\Delta x_L^{\text{ro}})^2 \rangle - 1/2] / \kappa^2$.

The conjugate quadrature x_A in this scheme does not directly couple to the light. In order to probe this quadrature, in another series of measurements, a magnetic $\pi/2$ pulse converting x_A to x_B is applied to the atoms. The quadrature x_B is then measured as the $\sin(\Omega t)$ component of the signal. The gain g_p as well as the variance σ_p^2 are determined similarly as for the x_L quadrature. The fidelity of the mixed Gaussian state stored in the memory with the initial pure coherent state $|\alpha\rangle$ is given by

$$F(\alpha) = \frac{2}{\sqrt{(1 + 2\sigma_x^2)(1 + 2\sigma_p^2)}} \exp \left[-\frac{(1 - g_x)^2}{1 + 2\sigma_x^2} \langle x_L^{\text{in}} \rangle^2 - \frac{(1 - g_p)^2}{1 + 2\sigma_p^2} \langle p_L^{\text{in}} \rangle^2 \right]. \quad (27.29)$$

Note that for nonunit gains g_x and g_p , the fidelity depends on α . In the experiment, coherent states with mean number of photons $0 < |\alpha|^2 < 8$ were stored in the memory. In this case the optimal gain is actually slightly less than one and the gains used in the experiment $g_x = 0.80$ and $g_p = 0.84$ were close to the optimum. The mean storage fidelity obtained by averaging (27.29) over the ensemble of the input coherent states was determined from the experimental data as $F_{\text{exp}} = 66.7 \pm 1.7\%$, which substantially exceeds the maximum

benchmark fidelity $F_{\text{meas}} = 55.4\%$ that can be obtained by any classical measurement and reparation protocol [12]. The maximum memory time over which the fidelity was still larger than F_{meas} was $\tau_{\text{max}} = 4$ ms.

The full retrieval of the quantum memory, i.e., the transfer of the quantum state of the atoms onto light can, in principle, be performed in a similar way as the storage. Indeed, the QND interaction is fully symmetric so one simply exchanges the role of the atoms and light. The protocol goes as follows. First, a read-out pulse is sent through the atoms. Then, a second, measurement, pulse is sent through the atomic ensembles in order to measure the quadrature $x'_A = x_A^{\text{in}} + \kappa p_L^{\text{in}}$. This measurement is not perfect since it is partially disturbed by the noise of the measurement pulse. Assuming for simplicity that the coupling strength κ is the same for both light beams, the measured quadrature reads $x_L^{\text{meas,in}} + \kappa x'_A$. The p_L quadrature of the first beam is displaced by the amount $g x_L^{\text{meas}}$ and the final quadratures of the read-out beam are

$$x_L^{\text{out}} = x_L^{\text{in}} + \kappa p_A^{\text{in}}, \quad p_L^{\text{out}} = (1 - g\kappa^2)p_L^{\text{in}} - g\kappa x_A^{\text{in}} - g x_L^{\text{meas,in}}. \quad (27.30)$$

In contrast to the memory storage protocol, here both quadratures contain some extra noise even if $g = \kappa = 1$, since the measurement of the atomic quadrature x'_A is indirect and noisy. A perfect memory retrieval is possible only with very strongly squeezed light beams such that $\langle (\Delta x_L^{\text{in}})^2 \rangle = \langle (\Delta x_L^{\text{meas,in}})^2 \rangle \rightarrow 0$. However, even with vacuum light beams and with unity gains the fidelity of transfer of coherent states from the memory to light is $F = 2/3$ which is much higher than the maximum classical fidelity $F = 0.5$. The above memory retrieval protocol implies that the retrieval light pulse does not travel too far away before the second pulse measuring on the atoms has completed its job. This means, in practice, that this retrieval protocol is limited to rather short pulses of light.

27.5 Multiple Passage Protocols

The great practical advantage of the entanglement generation and memory storage protocols is that each light beam has to pass through the atomic ensembles only once and is immediately measured afterward. This is crucial for the experimental feasibility of these schemes, because in current experiments the duration of each pulse is about 1 ms, and the corresponding length is 300 km, so it is impossible to store the pulse, e.g., in a fiber and send it through the atomic samples several times. This problem would complicate the experimental demonstration of the memory read-out, where one would ideally like to displace the read-out beam before detection, which would require to keep this beam somewhere while the atomic quadrature is being measured.

The experiments where the light beam traverses through the atomic ensembles several times could provide much more flexibility and allow us to generate entanglement and squeezing and transfer the state of light onto atoms and vice versa in a unitary way, without resorting to measurements and feedback. Note that in the multipass protocols discussed below, it is crucial that the second passage of the light beam through the atoms begins only after the end of the first passage, i.e., the head of the pulse could be sent again onto the atoms only when the tail of the pulse already cleared through. Otherwise the various parts of the pulse would couple simultaneously to the ensemble which would invalidate the simple single-mode description.

Schemes with several passages of light may become experimentally feasible if cold trapped atoms are employed, which could allow us to reduce the pulse duration to a few ns, making the pulse length compatible with table-top experiments.

The main advantage of schemes with several passages is that it is possible to modify the coupling between the two subsequent passages by applying local phase shifts to atoms and light. For instance, it is possible to switch between the effective QND unitary transformations $U_I(\kappa) = \exp(-i\kappa p_L x_A)$ and $U_{II}(\kappa) = \exp(-i\kappa x_L p_A)$ [13]. If these two unitaries are applied in sequence, then the resulting unitary will no longer correspond to QND coupling. In addition, it is also in principle possible to modify the coupling strength κ between two passages, for e.g., by changing the focusing of the light beam, although this would be experimentally challenging. It is insightful to consider the limit of a weak coupling, when $\kappa \ll 1$. In this case we can write

$$U_{II}(\kappa_2)U_I(\kappa_1) \approx \exp[-i(\kappa_1 p_L x_A + \kappa_2 x_L p_A)] = U_{\text{tot}}, \quad (27.31)$$

and the effective Hamiltonian generating U_{tot} is a sum of the effective Hamiltonians $\kappa_1 p_L x_A$ and $\kappa_2 x_L p_A$. In particular, if $\kappa_1 = \kappa_2 = \kappa$ then U_{tot} describes the two-mode squeezer with squeezing constant κ while if $\kappa_1 = -\kappa_2 = \kappa$ then U_{tot} represents a beam splitter with mixing angle κ . By repeating the sequence (27.31) many times, the total squeezing constant or mixing angle increases linearly with the number of passages n .

A more realistic evaluation of the schemes with multiple passages requires taking into account the losses and decoherence during the interaction [8]. The resulting evolution corresponding to a single passage of light through the ensemble is a Gaussian completely positive map. Let $v = (x_A, p_A, x_L, p_L)$ denote the vector of quadrature operators. The first moments $d = \langle v \rangle$ and the covariance matrix $\gamma_{jk} = \langle \Delta v_j \Delta v_k + \Delta v_k \Delta v_j \rangle$ which comprises the second moments transform according to

$$d \rightarrow DS(\kappa)d, \quad \gamma \rightarrow DS(\kappa)\gamma S^T(\kappa)D^T + G. \quad (27.32)$$

The symplectic matrix $S(\kappa)$ describes the QND coupling between atoms and light while the matrix D accounts for the damping due to losses and atomic depumping and G is the noise stemming from losses and decoherence. A simple model predicts that

$$D = \begin{pmatrix} \sqrt{1-\eta} & 0 & 0 & 0 \\ 0 & \sqrt{1-\eta} & 0 & 0 \\ 0 & 0 & \sqrt{1-\epsilon} & 0 \\ 0 & 0 & 0 & \sqrt{1-\epsilon} \end{pmatrix}, \quad G = \begin{pmatrix} 2\eta & 0 & 0 & 0 \\ 0 & 2\eta & 0 & 0 \\ 0 & 0 & \epsilon & 0 \\ 0 & 0 & 0 & \epsilon \end{pmatrix}.$$

Here η is the atomic depumping rate introduced earlier in Section 27.2 and ϵ is the fraction of light lost due to the absorption, reflection from the glass cells, etc. Note the factor of 2 in the atomic part of the noise matrix G . This additional noise arises because the atoms which decohere are still present in the atomic ensemble and contribute to the noise. Moreover, the damping decreases the coupling constant κ , because $\kappa \propto \sqrt{J_x S_1}$ and after n passages we have $\kappa_n = [(1-\eta)(1-\epsilon)]^{n/2} \kappa$. The net effect of the multiple passages can be evaluated by iterating the map (27.32) with properly chosen $S(\kappa_n)$ for each passage. It has been shown that as the total number of passages n increases, the amount of generated entanglement grows and can be

arbitrarily high even in the presence of losses and decoherence. To achieve good performance, it is necessary to optimize η which is connected with coupling strength via $\kappa^2 = \eta\alpha_0$. The optimal η decreases with increasing n and the value of η can be tuned experimentally, e.g., by changing the detuning Δ .

It has been shown that various important two-mode linear canonical transformations can be implemented with three passages of light through the atoms, provided that κ can be set independently for each passage [14]. The resulting effective unitary operation is given by

$$U = U_I(\kappa_3)U_{II}(\kappa_2)U_I(\kappa_1). \quad (27.33)$$

The two-mode squeezing transformation $U_{\text{TMS}} = \exp[-ir(x_{\text{A}}p_{\text{L}} + p_{\text{A}}x_{\text{L}})]$ with squeezing constant r is applied to light and atoms if

$$\kappa_1 = \tanh \frac{r}{2}, \quad \kappa_2 = \sinh r, \quad \kappa_3 = \tanh \frac{r}{2}. \quad (27.34)$$

Similarly, it is possible to implement a beam splitter-type interaction $U_{\text{BS}} = \exp[-i\phi(x_{\text{L}}p_{\text{A}} - p_{\text{L}}x_{\text{A}})]$ by choosing

$$\kappa_1 = \tan \frac{\phi}{2}, \quad \kappa_2 = -\sin \phi, \quad \kappa_3 = \tan \frac{\phi}{2}. \quad (27.35)$$

In particular, for $\phi = \pi/2$ we get a beam splitter that swaps the state of atoms and light which can be used for quantum memory storage and retrieval. The advantage of this approach is that it does not require any measurement and feedback and the transfer of the quantum state from light onto atoms is in principle perfect even if the atomic ensemble is not initially squeezed. Importantly, at $\phi = \pi/2$ the absolute values of all three coupling constants κ_j coincide, $|\kappa_j| = 1$, and it is not therefore necessary to change the strength of coupling between the subsequent passages but only apply local phase shifts to atoms and light.

Let us consider the three steps of the unitary quantum-state swapping in more detail. In the first step, a unitary $U_1 = \exp(-ix_{\text{A}}p_{\text{L}})$ is applied and we have

$$x'_{\text{A}} = x_{\text{A}}^{\text{in}}, \quad p'_{\text{A}} = p_{\text{A}}^{\text{in}} - p_{\text{L}}^{\text{in}}, \quad x'_{\text{L}} = x_{\text{L}}^{\text{in}} + x_{\text{A}}^{\text{in}}, \quad p'_{\text{L}} = p_{\text{L}}^{\text{in}}. \quad (27.36)$$

Next follows the unitary $U_2 = \exp(ip_{\text{A}}x_{\text{L}})$ which results in

$$x''_{\text{A}} = -x_{\text{L}}^{\text{in}}, \quad p''_{\text{A}} = p_{\text{A}}^{\text{in}} - p_{\text{L}}^{\text{in}}, \quad x''_{\text{L}} = x_{\text{L}}^{\text{in}} + x_{\text{A}}^{\text{in}}, \quad p''_{\text{L}} = p_{\text{A}}^{\text{in}}. \quad (27.37)$$

The state transfer is finished by sending the light through the atoms for the third time after local phase shifts such that $U_3 = \exp(-ix_{\text{A}}p_{\text{L}})$ is effectively applied, and we obtain

$$x_{\text{A}}^{\text{out}} = -x_{\text{L}}^{\text{in}}, \quad p_{\text{A}}^{\text{out}} = -p_{\text{L}}^{\text{in}}, \quad x_{\text{L}}^{\text{out}} = x_{\text{A}}^{\text{in}}, \quad p_{\text{L}}^{\text{out}} = p_{\text{A}}^{\text{in}}, \quad (27.38)$$

and the states of light and atoms have been mutually exchanged.

It is also possible to squeeze the state of the atoms in a unitary way by sending the light beam through the atomic ensemble several times. If we restrict ourselves to the sequence of unitaries $U_I(\kappa_j)$ and $U_{II}(\kappa_k)$, then the single-mode squeezing of atoms $U_{\text{SMS}} =$

$\exp(-i\frac{r}{2}x_A p_A)$ requires four passages of light, and the coupling constants depend on r as follows,

$$\kappa_2 = \frac{e^r - 1}{\kappa_1}, \quad \kappa_3 = -\kappa_1 e^{-r}, \quad \kappa_4 = \frac{e^r}{\kappa_1}(1 - e^r), \quad (27.39)$$

and κ_1 can be arbitrary. After this sequence of operations, the atomic ensemble is squeezed irrespective of the initial state of light and the scheme is thus robust against noise in the light beam.

27.6 Atoms-light teleportation and entanglement swapping

Quantum teleportation is a process for a disembodied transmission of a quantum state between two distant locations via dual quantum and classical channels. The quantum channel consists of an entangled state shared by the sender and receiver. The sender carries out a joint measurement in the basis of maximally entangled states (the so-called Bell measurement) on her part of the entangled state and on the state she wants to teleport. The measurement result is transmitted to the receiver via a classical channel, and the receiver then applies an appropriate unitary transformation to his part of the entangled state. Under ideal conditions, when the two partners share maximally entangled state and the Bell measurement is perfect, the state is exactly transferred to the receiver.

The quantum teleportation has been originally proposed for finite-dimensional systems but it has been later extended to the realm of continuous variables [15, 16]. Here, the entanglement is provided by the two-mode squeezed vacuum state, which approximates the (unphysical) maximally entangled EPR state. The continuous-variable Bell measurement on two modes 1 and 2 consists of simultaneously measuring two commuting quadrature operators $x_+ = x_1 + x_2$ and $p_- = p_1 - p_2$. For two optical modes, this measurement can be accomplished by mixing the two modes on a balanced beam splitter and measuring the x and p quadratures on the first and second outputs, respectively.

However, the beam splitter is not the only option, and it can be replaced by the QND-type coupling $U = \exp(-i\kappa x_A p_L)$ with properly chosen coupling constant $\kappa = 1$. The atom and light quadratures after the interaction, $x_L^{\text{out}} = x_L^{\text{in}} + x_A^{\text{in}}$ and $p_A^{\text{out}} = p_A^{\text{in}} - p_L^{\text{in}}$ are exactly the balanced superpositions of the quadratures required for CV Bell measurement. The light quadrature can be measured directly while an auxiliary probe light beam has to be employed to measure the atomic quadrature p_A^{out} similarly as in the protocol for atomic memory read-out discussed in the preceding section.

The Bell measurement can be explored to teleport the quantum state of light beam onto atoms and vice versa [3]. Consider first the teleportation of an atomic state onto light. Two light beams L and M are prepared in a two-mode squeezed vacuum state with reduced fluctuations of the quadratures $x_+ = x_L + x_M$ and $p_- = p_L - p_M$, $\langle(\Delta x_+)^2\rangle = \langle(\Delta p_-)^2\rangle = e^{-2r}$. The horizontally polarized mode L is combined with a strong coherent vertically polarized coherent beam and sent through the atomic ensemble A. The output quadrature $x_L^{\text{out}} = x_L^{\text{in}} + x_A^{\text{in}}$ is measured and then an auxiliary beam K probes the atomic p -quadrature, and $x_K^{\text{out}} = x_K^{\text{in}} + \kappa(p_A^{\text{in}} - p_L^{\text{in}})$ is measured. The measurement results are communicated to the receiver who possesses the light beam M and displaces the quadratures according to

$x_M \rightarrow x_M + x_L^{\text{out}}, p_M \rightarrow p_M + \kappa^{-1} x_K^{\text{out}}$. The resulting quadratures of the mode M read

$$x_M^{\text{out}} = x_A^{\text{in}} + x_M^{\text{in}} + x_L^{\text{in}}, \quad p_M^{\text{out}} = p_A^{\text{in}} + p_M^{\text{in}} - p_L^{\text{in}} + \kappa^{-1} x_K^{\text{in}}. \quad (27.40)$$

This describes the unity-gain teleportation and the mean values of the quadratures of mode M after teleportation are equal to the mean values of the initial atomic quadratures. The process of teleportation is imperfect and adds some noise to the two quadratures. In the present case, this noise is unequally distributed since in the Bell measurement one quadrature is detected directly while the other only indirectly using the auxiliary beam K . The quality of the teleportation is often quantified by the fidelity of teleportation of coherent states. Assuming vacuum probe K and pure two-mode squeezed vacuum in modes L and M , we obtain

$$F = \sqrt{2} [(1 + e^{-2r})(2 + 2e^{-2r} + \kappa^{-2})]^{-1/2}. \quad (27.41)$$

The teleportation of the state of light onto the atoms proceeds in a similar way. The atomic ensembles have to be first prepared in an entangled state following the procedure described in Section 27.3. Then the light beam is sent through one of the ensembles and the output light quadrature is measured. An auxiliary beam then probes the atomic ensemble and its quadrature is measured. The second ensemble is displaced according to the measurement results by tiny rotations of the collective spin over the y and z axes. The relationship between the final atomic quadratures and the initial light quadratures is formally identical to Eq. (27.40), where the role of atoms and light should be interchanged.

One particularly interesting and useful application of quantum teleportation is the entanglement swapping, i.e., a teleportation of one part of entangled state. In this way, the quantum entanglement can be distributed over quantum communication network. Consider three nodes, A , B , and C . Suppose that A and B share an entangled state of two atomic ensembles 1 and 2. Simultaneously, nodes B and C share an entangled state of two other atomic ensembles 3 and 4. The ensemble 1 is at A , the ensembles 2 and 3 at B and the ensemble 4 at C . The middle partner B can teleport the state of the atomic ensemble 2 to C by performing the Bell measurement on the pair of ensembles 2 and 3. This can be accomplished using the same procedure that was used to entangle a pair of ensembles. It is advantageous to carry out this experiment with atomic ensembles placed in an external magnetic field since then the Bell measurement can be performed in a single run by detecting the sin and cos modulation at Ω sidebands of the output light beam.

The whole procedure of the entanglement swapping would involve four light beams. First, two beams are used to entangle the pairs of atomic ensembles 1, 2 and 3, 4, as described in Section 27.3. Next, the third beam is sent through ensembles 2 and 3 and measured, which establishes an entanglement between two atomic ensembles 1 and 4 that never directly interacted. Finally, the presence of the entanglement should be verified by sending a probe beam through the ensembles 1 and 4 and measuring it.

27.7 Quantum Cloning into Atomic Memory

Due to the linearity of quantum mechanics, an unknown quantum state cannot be copied, the transformation $|\psi\rangle \rightarrow |\psi\rangle|\psi\rangle$ is forbidden in quantum mechanics. It is, nevertheless, possible

to perform approximate copying of quantum states. In the context of continuous variables, particular attention has been paid to copying of coherent states, because the optimal cloning machines can be used as an efficient eavesdropping on quantum key distribution protocols based on coherent states and homodyne detection.

By exploiting the QND interaction between atoms and light it is possible to combine the optimal Gaussian quantum cloning of coherent states with the storage of the clones into quantum memory and accomplish a direct quantum cloning into atomic memory [17]. The cloning requires two passages of the light beam L through the two atomic ensembles A and B. During the first passage the information about the x quadrature of light is transferred to atoms by engineering the effective interaction $U_1 = \exp[-i(p_A + p_B)x_L]$. After the first passage of light through the ensembles we obtain

$$\begin{aligned} x'_A &= x_A^{\text{in}} + x_L^{\text{in}}, & p'_A &= p_A^{\text{in}}, \\ x'_B &= x_B^{\text{in}} + x_L^{\text{in}}, & p'_B &= p_B^{\text{in}}, \\ x'_L &= x_L^{\text{in}}, & p'_L &= p_L^{\text{in}} - p_A^{\text{in}} - p_B^{\text{in}}. \end{aligned} \quad (27.42)$$

In the next step, the information about the quadrature p_L is written to atoms by sending the light beam through the ensembles again. Before this, local phase shifts are applied to atoms and light which change the effective interaction to $U_2 = \exp[i(x_A + x_B)p_L]$. After the second passage the quadratures are transformed to

$$\begin{aligned} x_A^{\text{out}} &= x_L^{\text{in}} + x_A^{\text{in}}, & p_A^{\text{out}} &= p_L^{\text{in}} - p_B^{\text{in}}, \\ x_B^{\text{out}} &= x_L^{\text{in}} + x_B^{\text{in}}, & p_B^{\text{out}} &= p_L^{\text{in}} - p_A^{\text{in}}, \\ x_L^{\text{out}} &= -x_L^{\text{in}} - x_A^{\text{in}} - x_B^{\text{in}}, & p_L^{\text{out}} &= p_L^{\text{in}} - p_A^{\text{in}} - p_B^{\text{in}}. \end{aligned} \quad (27.43)$$

If the atomic ensembles are initially in a vacuum state (i.e., CSS with all atoms pointing along the x -axis), then the ensembles A and B contain two optimal Gaussian clones of the coherent state $|\alpha\rangle$ of the light beam L [18], each with fidelity $F = 2/3$.

In current experiments with hot atomic ensembles, it would be impossible to accomplish the second passage of light through the atoms because the light pulse has to be several hundred kilometers long. Luckily, the second passage of the light beam through the atoms can be avoided and replaced by the measurement of the quadrature p'_L followed by the displacement of the atomic quadratures conditioned on the measurement outcome,

$$p'_A \rightarrow p'_A + p'_L, \quad p'_B \rightarrow p'_B + p'_L. \quad (27.44)$$

The resulting atomic quadratures coincide with those in Eq. (27.43). This renders the cloning experimentally feasible and the whole procedure closely resembles the protocol for the quantum memory storage. The protocol can be also generalized to optimal asymmetric Gaussian quantum cloning where the two clones exhibit different fidelities. The asymmetric cloning is achievable by a suitable preprocessing of the atomic ensembles, by preparing them in a squeezed state with reduced fluctuations of quadratures x_A and p_B . By varying the amount of squeezing, the whole one-parametric class of optimal Gaussian asymmetric cloning machines for coherent states can be obtained.

27.8 Summary

We have described a quantum interface between a single-mode light and atomic ensemble(s). The basis of this interface is an off-resonant dipole interaction which leads to a phase shift (polarization rotation) of light and Stark shift (rotation of the collective Bloch vector) of atoms. Combined with the quantum measurement and feedback, this interaction provides a wide range of operations useful for quantum information processing, such as long-distance quantum teleportation of atomic states, quantum memory for light, and quantum cloning of light onto atoms.

References

- [1] A. Kuzmich, N. P. Bigelow, and L. Mandel, Atomic quantum non-demolition measurements and squeezing, *Europhys. Lett.* **42** (1998), 481–486.
- [2] L. M. Duan, J. I. Cirac, P. Zoller, and E. S. Polzik, Quantum Communication between Atomic Ensembles Using Coherent Light, *Phys. Rev. Lett.* **85** (2000), 5643–5646.
- [3] A. Kuzmich and E. S. Polzik, Atomic Quantum State Teleportation and Swapping, *Phys. Rev. Lett.* **85** (2000), 5639–5642.
- [4] C. Schori, B. Julsgaard, J. L. Sørensen, and E. S. Polzik, Recording Quantum Properties of Light in a Long-Lived Atomic Spin State: Towards Quantum Memory, *Phys. Rev. Lett.* **89** (2002), 057903.
- [5] S. L. Braunstein, Error Correction for Continuous Quantum Variables, *Phys. Rev. Lett.* **80** (1998), 4084–4087.
- [6] B. Julsgaard, A. Kozhekin, and E. S. Polzik, Experimental long-lived entanglement of two macroscopic objects, *Nature (London)* **413** (2001), 400–403.
- [7] B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, Experimental demonstration of quantum memory for light, *Nature (London)* **432** (2004), 482–486.
- [8] K. Hammerer, K. Mølmer, E. S. Polzik, and J. I. Cirac, Light-matter quantum interface, *Phys. Rev. A* **70** (2004), 044304.
- [9] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, *Phys. Rev.* **47** (1935), 777–780.
- [10] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Inseparability Criterion for Continuous Variable Systems, *Phys. Rev. Lett.* **84** (2000), 2722–2725.
- [11] J. Sherson, A.S. Sørensen, J. Fiurasek, K. Mølmer, and E.S. Polzik, Light qubit storage and retrieval using macroscopic atomic ensembles, *Phys. Rev. A* **74** (2006), 011802(R).
- [12] K. Hammerer, M. M. Wolf, E. S. Polzik, and J. I. Cirac, Quantum Benchmark for Storage and Transmission of Coherent States, *Phys. Rev. Lett.* **94** (2005), 150503.
- [13] B. Kraus, K. Hammerer, G. Giedke, and J. I. Cirac, Entanglement generation and Hamiltonian simulation in continuous-variable systems, *Phys. Rev. A* **67** (2003), 042314.
- [14] J. Fiurášek, Unitary-gate synthesis for continuous-variable systems, *Phys. Rev. A* **68** (2003), 022304.
- [15] S.L. Braunstein and H.J. Kimble, Teleportation of Continuous Quantum Variables, *Phys. Rev. Lett.* **80** (1998), 869–872.

- [16] A. Furusawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Unconditional quantum teleportation, *Science* **282** (1998), 706–709.
- [17] J. Fiurášek, N. J. Cerf , and E. S. Polzik, Quantum Cloning of a Coherent Light State into an Atomic Quantum Memory, *Phys. Rev. Lett.* **93** (2004), 180501.
- [18] N. J. Cerf, A. Ipe, and X. Rottenberg, Cloning of Continuous Quantum Variables, *Phys. Rev. Lett.* **85** (2000), 1754–1757.

28 Cavity Quantum Electrodynamics: Quantum Information Processing with Atoms and Photons

Jean-Michel Raimond and Gerhard Rempe

The simplest model in quantum optics deals with a single two-level atom interacting with a single mode of the radiation field. This ideal situation is implemented in cavity quantum electrodynamics experiments, using high-quality microwave or high-finesse optical cavities as photon boxes. It provides a fruitful test bench for fundamental quantum processes and a promising ground for quantum information processing.

28.1 Introduction

Most experiments in atomic and optical physics dealing with light–matter interactions involve a large number of atoms interacting with laser fields made up of a large number of photons. The simplest situation, however, involves a single atom interacting with one or just a few photons. Achieving this situation and making it available for applications is the aim of cavity quantum electrodynamics (cavity QED).

The history of cavity QED started, about 50 years ago, with a seminal remark by Purcell [1]. He realized that the radiation properties of an atom are not a fundamental property of the atom itself. Instead, they can be changed by controlling the boundary conditions of the electromagnetic field with mirrors or cavities. Cavity QED experiments initially measured modifications of spontaneous emission rates or spatial patterns in low-quality cavities. They evolved to higher and higher atom–cavity couplings and photon storage times. Most of them are now in the so-called regime of “strong coupling,” in which the coherent interaction of a single atom with one photon stored in a very-high-quality cavity, a modern equivalent of Einstein’s photon box, overwhelms the incoherent dissipative processes. The most prominent effect in this regime is that a photon emitted into the cavity can be reabsorbed by the atom. The usually irreversible process of spontaneous emission therefore becomes reversible—a remarkable cavity QED effect!

In principle, cavity QED experiments implement a situation so simple that their results can be cast in terms of the fundamental postulates of quantum theory. They are thus appropriate for tests of basic quantum properties: quantum superposition, complementarity or entanglement. In the context of quantum information processing, the atom and the cavity are long-lived qubits, and their mutual interaction provides a controllable entanglement mechanism—an essential requirement for quantum computing or teleportation applications. Cavity QED is therefore a fertile ground for quantum information processing. In addition, the ability to

manipulate mesoscopic fields, containing a few to a few tens of photons, made it possible to explore the fuzzy boundary between the quantum and the classical worlds, unveiling the decoherence mechanisms that confine the quantum weirdness at a microscopic scale.

Cavity QED comes in two flavors: microwave and optical. The novel regime of strong coupling was first reached in microwave cavities, but is now also achieved in optical cavities. Although both situations share a similar underlying physics, they are nevertheless quite different and, in fact, have complementary features. In the microwave domain, highly excited “Rydberg” states interact with rather large superconducting millimeter-wave cavities. Dissipation is extremely low, and the pace of the atom–field entanglement process is slow. An exquisite degree of control is reached, making it possible to tailor complex multiqubit entangled states. In the optical domain, low-lying atomic levels interact with submillimeter-sized optical cavities at room temperature. The interaction is much faster, as is the dissipation. This, however, turns out to be an asset: optical photons can efficiently be coupled in or out of the cavity. Optical cavity QED thus provides a natural and essential interface between flying photonic qubits for the transmission of quantum information and stationary atomic qubits for the storage of quantum information.

This chapter gives a brief introduction into cavity QED, both microwave and optical. It highlights the basic properties, discusses some selected achievements and mentions a few perspectives for quantum information processing. It does not aim to give full account of all experimental developments and theoretical concepts. Instead, it concentrates mainly on some recent experimental work performed at ENS and MPQ. More information can be found in broader reviews [2–5] and popular accounts [6].

28.2 Microwave Cavity Quantum Electrodynamics

In order to reach the strong coupling regime, a cavity QED experiment must combine large atom–field couplings with long atomic and field lifetimes. The longest photon storage times, in the 1 ms to 1 s range, are obtained in the millimeter-wave domain (few tens of GHz) with photon boxes made of superconducting materials cooled down to cryogenic temperatures. They have sizes comparable to the wavelength and provide a high field confinement, essential to increase the atom–field coupling. The ideal tools for cavity–field manipulations are Rydberg atoms [7]. Here, the valence electron of an alkali atom is promoted to a very excited level, with a large principal quantum number N . The diameter of these giant atoms is 0.2 μm for $N = 50$, the typical size of a large virus or of a small bacteria! Such atoms are huge antennas, strongly coupled to the millimeter-wave fields. The “circular” atoms, realizing Bohr model’s circular orbits, are particularly interesting due to their very long lifetimes (30 ms for $N = 50$). These levels can be counted with a large efficiency by field-ionization. This detection is moreover state-selective, measuring with precision the final quantum number.

Figure 28.1 presents the scheme of a cavity QED experiment using circular Rydberg atoms. For a review and additional information, see [8]. Laser and microwave excitation of an atomic beam, effusing from oven O , prepares in box B one of the states $|e\rangle$ or $|g\rangle$ ($N=51$ or $N=50$). A reasonable approximation of single-atom samples is obtained by preparing much less than one atom on the average. When an atom is finally detected, it was most probably travelling alone. Before entering B , the atoms are velocity-selected by standard laser tech-

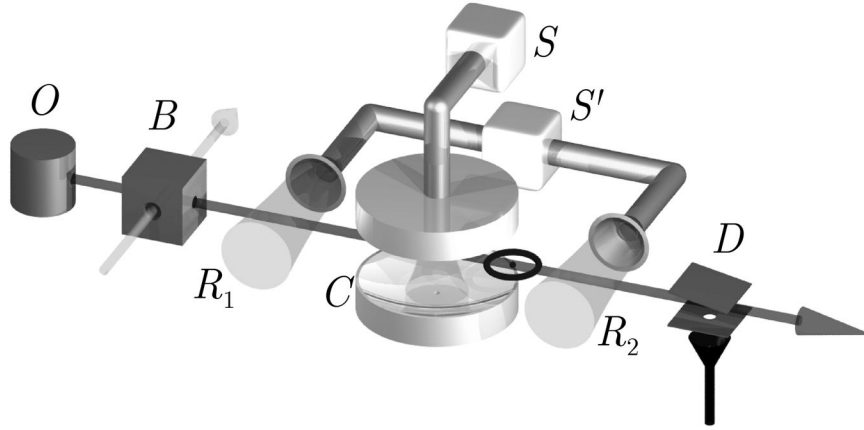


Figure 28.1. A cavity QED setup using circular Rydberg atoms, prepared in box B out of a rubidium atomic beam effusing from oven O, and a superconducting millimeter-wave cavity C. The atoms are counted downstream by the field-ionization detector D. Their state can be manipulated in the classical field zones R_1 and R_2 sandwiching C.

niques. The state preparation being pulsed and performed at a precise location, the position of an atom at any time during its 20 cm transit through the apparatus is well determined. Selective transformations can thus be applied at will on all atoms crossing the setup during an experimental sequence. This individual addressing is essential for quantum information processing experiments. The atoms, very sensitive to microwave fields, are in a cryogenic environment, cooled below 1 K and shielded from the room-temperature blackbody background. They interact with the superconducting cavity C , nearly resonant with the transition between $|e\rangle$ and $|g\rangle$ at 51 GHz. An electric field is applied across the cavity mirrors. It can be used to tune, via the Stark effect, the atomic frequency in or out of resonance with the cavity mode, with an excellent time resolution. The atom–field evolution can be “frozen” suddenly by a large field. With moderate field amplitudes, the interaction can be tuned at will from the resonant to the dispersive regimes. The atoms are finally detected in the field-ionization counter D, whose efficiency, greater than 80%, provides a nearly ideal qubit readout [9]. A classical source S , coupled to C , can be used to fill the cavity with a mesoscopic quasi-classical field, with a well-controlled phase. Its amplitude can be adjusted from a microscopic value, corresponding to a fraction of a photon on average, to a macroscopic one, with few tens of photons. The resonant interaction of the atom with classical fields in the zones R_1 and R_2 , sandwiching C and fed by the source S' , realizes single-qubit gates in quantum information terms. The atom can thus be prepared in any state before entering C . The detection by D , in the $\{|e\rangle, |g\rangle\}$ basis, after the gate operation performed by R_2 , amounts to measuring the atomic qubit in a completely adjustable basis. This provides a full analysis of the final atomic state, an essential ingredient to assess the fidelity of the quantum processes taking place in C .

Most quantum entanglement manipulations realized so far with this setup rely on the resonant atom–cavity interaction. The simplest situation is an atom in the upper state, $|e\rangle$, entering

the empty resonant cavity (vacuum state $|0\rangle$). The initial quantum state $|e, 0\rangle$ is degenerate with $|g, 1\rangle$ representing an atom in the lower state with one photon in C . The atom–field dipole interaction couples these states and the atom–cavity system thus oscillates between them in a “vacuum Rabi oscillation.” Note that no evolution takes place when the initial state is $|g, 0\rangle$ (atom in the ground state and empty cavity) since there is no excitation to exchange. Figure 28.2 presents an experimental vacuum Rabi oscillation. The probability P_e for detecting the atom in $|e\rangle$ is plotted as a function of the atom–cavity interaction time, t_i . The observation of four 20 μs periods shows that the coherent atom–cavity interaction dominates dissipative processes, fulfilling the strong coupling condition. This oscillation is a reversible spontaneous emission process. The atom in $|e\rangle$ emits a photon. When the emission occurs in free space, the photon escapes at light velocity and is lost. Ordinary spontaneous emission is irreversible. Here, the emitted photon remains trapped in C , ready to be absorbed again by the atom. In the strong coupling regime, spontaneous emission is a reversible process!

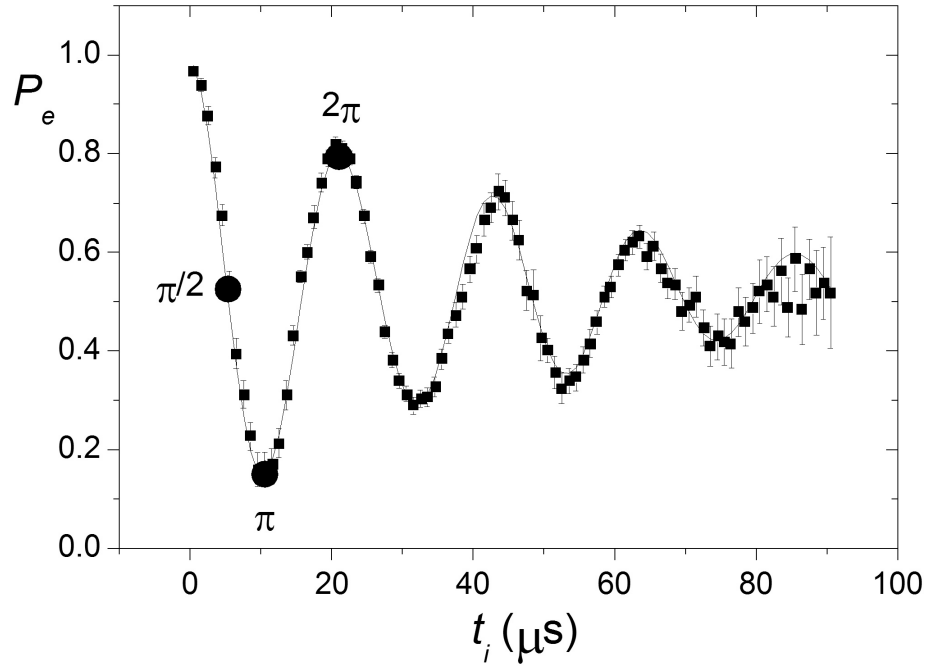


Figure 28.2. Experimental quantum Rabi oscillation. The probability for finding the atom in the upper state $|e\rangle$, P_e , is plotted as a function of the atom–cavity interaction time t_i . The quantum Rabi pulses used for quantum information processing experiments are marked with black solid circles.

Oscillatory spontaneous emission is at the heart of an interesting quantum device, studied mostly in Munich: the micromaser (see the chapter by Raithel et al. in [2] and [10–12]). A continuous stream of single Rydberg atoms crosses the cavity. The competition between cumulative atomic emissions and cavity damping results in the build-up of a mesoscopic field,

containing up to a few tens of photons. The cavity damping time is so long that the maser action is sustained, close to threshold, even though the average time interval between atoms is much greater than their transit time through C . The micromaser operates thus with much less than a single excited atom at a time, a regime in which quantum effects are of paramount importance [13, 14]. The Rydberg atom–cavity coupling is so large that these remarkable micromasers can even operate on a two-photon transition, a rather exotic kind of quantum oscillator [15].

The vacuum Rabi oscillation provides elementary stitches to knit complex entangled states. Three atom–cavity interaction times are particularly interesting. They are depicted by black circles in Fig. 28.2. After a quarter of a period ($\pi/2$ pulse), the atom and the cavity are in a coherent superposition of $|e, 0\rangle$ and $|g, 1\rangle$ with equal weights. This is an entangled state, similar to the one of the spin pair used to discuss the EPR (Einstein–Podolski–Rosen) situation illustrating quantum nonlocality. The atom–cavity entanglement lives as long as the photon, about a millisecond. This time is much longer than the mere 5 μs required for the entanglement creation, making complex entanglement-knitting sequences possible. Half a period of the quantum Rabi oscillation (π pulse) corresponds to an atom–cavity state exchange. An atom entering the empty cavity in a superposition of its energy states always ends up in $|g\rangle$, leaving in C a coherent superposition of the zero- and one-photon states. In quantum information terms, the qubit carried by the atom is copied onto the cavity. The process is reversible. An atom entering C in the lower level $|g\rangle$ for a half-period interaction takes away the quantum information stored in the cavity, which is left in the vacuum state. This operation does not create atom–cavity entanglement, but is essential since the cavity field is not directly accessible in these experiments, in contrast to optical cavity QED situations (see below). The cavity mode is initialized with the help of properly prepared atoms. All the information on the cavity mode is retrieved by probe atoms. Finally, a full Rabi oscillation period (2π pulse) drives the atom–cavity system back to its initial state, albeit with a state-sign change, reminiscent of the π -phase shift experienced by a spin-1/2 system undergoing a 2π rotation in real space. The same phase shift occurs when the initial state is $|g, 1\rangle$, the atom transiently absorbing the photon and releasing it. Note again that $|g, 0\rangle$ remains invariant. The state phaseshift is thus conditioned on the states of the atom and the cavity. The 2π pulse implements a conditional dynamics, the building block for a quantum gate.

Combining these transformations, it is now possible to realize quantum information processing sequences of increasing complexity [8]. In a quantum memory experiment [16], a qubit carried by a first atom is copied onto C by a π quantum Rabi pulse, stored for a while as a superposition of zero- and one-photon states, and later taken away by a second atom undergoing another π -pulse. An EPR atomic pair is created by entangling a first atom with C ($\pi/2$ quantum Rabi pulse). The cavity state and, hence, its entanglement with the first atom is then copied onto a second atom by a π -pulse. Quantum correlations observed between the atomic states for different detection basis settings assess the coherence of the process [17]. Two nondegenerate modes of the cavity are entangled in a similar way, through their successive resonant interactions with a single atom [18]. A full-fledged quantum gate uses the full Rabi period [19]. The atomic qubit is coded onto the transition between $|g\rangle$ and another level $|i\rangle$ (circular level with $N = 49$). When the system is initially in $|g, 1\rangle$, it undergoes a π -phase shift. All other levels are unchanged ($|i\rangle$ is not resonant with the cavity and $|g, 0\rangle$ does not evolve). This is the truth table of a quantum phase gate acting on the atom and the field mode.

Two single-qubit gates performed in R_1 and R_2 transform it into a CNOT gate, conditioning the atomic state on the cavity mode. In this interesting situation, the outgoing atomic state reveals the presence of a single photon in the cavity. When the photon is “seen” by the atom, it stays in the cavity (it is first absorbed by the atom, but then re-emitted). This quantum nondemolition detection [20] is quite different from a standard photodetection in which the photon is destroyed. In other words, the same photon can be detected twice or more!

The most complex quantum information sequence realized so far is the creation of a three-qubit entangled state [21]. The cavity is entangled with a first atom, as in the first step of the EPR pair generation above. A second atom then enters the mode and realizes a quantum phase-gate operation, instead of a cavity mode readout. This atom gets entangled with C and, hence, with the first one, completing the three-qubit entanglement. The quantum correlations between these qubits are then measured. A third atom is involved, which reads out the field state. Altogether, the production and analysis of this entanglement involves four qubits, three one-qubit gates and three two-qubit ones. It is still among the most complex sequences realized with individually addressed qubits.

In these experiments, the entanglement fidelity is mainly limited by cavity damping, reaching 54% for the three-qubit entanglement. A promising quantum gate gets rid of this limitation [22]. Two atoms, one in $|e\rangle$ and one in $|g\rangle$, interact simultaneously with the nonresonant cavity. The first atom virtually emits a photon in C , which is immediately absorbed by the other. This cavity-induced coherent “collision,” reminiscent of the resonant van der Waals interaction in free space, creates a two-atom entangled state and provides the conditional dynamics of a quantum gate. Since the photon is only virtually stored in C , the gate fidelity is, to first order, impervious to cavity losses or residual thermal photons. This scheme is thus very promising for the implementation of simple quantum algorithms [23] with moderate-quality cavities at finite temperatures.

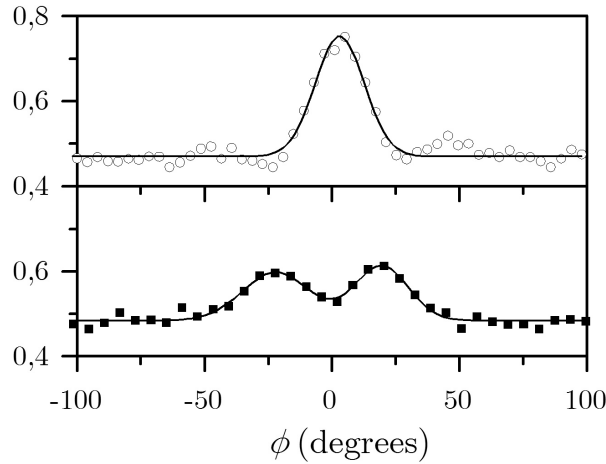


Figure 28.3. A single resonant atom prepares a coherent superposition of two large fields with different phases. Phase distribution of the initial 29 photons coherent field (above) and of the final field state (below). The separation in two phase components is conspicuous.

Another remarkable feature of these experiments is the ability to manipulate in C mesoscopic fields, made up of a few to a few tens of photons, which are useful tools to explore the quantum-classical boundary. These mesoscopic objects can be entangled with a single atom crossing the cavity, as the famous Schrödinger cat gets entangled with a single radioactive atom. A nonresonant atom, in the dispersive regime, cannot absorb or emit a photon but is a piece of transparent dielectrics, whose index of refraction transiently shifts the cavity frequency. The atom-cavity interaction results then in a classical phaseshift for the cavity field, with opposite values for an atom in level $|e\rangle$ or $|g\rangle$. An atom in a state superposition then prepares a mesoscopic superposition state involving two field phases *at the same time*, a situation closely linked with the Schrödinger cat, suspended between life and death in quantum limbs. The slow relaxation of the cavity makes it possible to study in “real time” the decoherence mechanism [8] transforming this quantum superposition into a probabilistic alternative, the transition being faster and faster when the cat’s size increases.

The resonant atom-field coupling also involves such bizarre states. An atom interacting with a very large field undergoes a trivial Rabi oscillation between levels $|e\rangle$ and $|g\rangle$ and leaves the field unchanged. In a mesoscopic field, containing only a few tens of photons, the situation is much more interesting. The photon number graininess results then in an atom-field phase entanglement [24, 25]. The field is separated in two phase components, rotating in opposite directions. A phase distribution measurement, based on a homodyne method, directly reveals this separation (see Fig. 28.3). In other words, an atom at resonance is in a quantum superposition of two states with very large refractive indices, an utterly nonclassical result (the index of refraction of a classical charged oscillator at resonance is 1). The resonant interaction prepares large coherent cat states, which will be fantastic tools for new decoherence studies. They are important for fundamental quantum mechanics issues and also because decoherence is the most serious obstacle on the road toward practical quantum computation. The direct determination of the cavity-field Wigner function [26], which provides a complete and pictorial insight into the cavity-field quantum state, will make it possible to put our understanding of decoherence under close scrutiny.

28.3 Optical Cavity Quantum Electrodynamics

All cavity QED experiments are characterized by three physically distinct time scales. One is the period of the oscillatory exchange of a single energy quantum between the atom and the cavity, the vacuum Rabi time; see Fig. 28.2. A second time is the transit time of the atom through the cavity. The third time comes from the coupling of the combined atom-cavity system to the environment and is determined by the photon lifetime inside the cavity and the atomic lifetime due to spontaneous emission into directions not supported by the cavity.

In principle, these three time scales can be arbitrary, making the description of an experiment rather tedious. Cavity QED, however, achieves the ideal situation in which these time scales can differ by several orders of magnitude. The distinct hierarchy is the key ingredient for coherently controlling the system at the level of single atomic and photonic quanta. In the microwave domain, it ensures that different atoms passing the cavity one after the other interact with essentially the same cavity field, thereby “seeing” the previous atom. In the optical domain, the time scales follow a different hierarchy. While in the regime of strong coupling

the vacuum-Rabi period is still shorter than the lifetimes of both the cavity and the atom, the transit time can now be many orders of magnitude longer, in particular when laser-cooled slow atoms are employed. It follows that a single atom can interact with literally thousands and even millions of photons one after the other. This provides an excellent opportunity to make real-time measurements on a single atom by observing the photons emitted from the cavity. In fact, the rate of information one can achieve from a single intracavity atom can significantly exceed the corresponding rate from a free-space atom, for essentially two reasons: one is the more or less “one-dimensional” radiation environment, with the cavity effectively covering the full solid angle. The other reason is the fast time scale provided by the short vacuum-Rabi period in the regime of strong coupling. The loss of photons is therefore a highly useful ingredient of optical cavity QED experiments.

It follows that atoms and photons play opposite roles in microwave and optical cavity QED. This can also be understood when comparing the kind of excitation that is typically employed to drive the atom–cavity system in the two domains. In most microwave experiments, energy is provided by atoms entering the cavity in the excited state, quickly depositing a photon into the cavity. In the optical domain, atoms tend to be in their ground state, and excitation of the system is provided by an external laser. Two configurations are possible: Firstly, the laser illuminates the system from the side, driving the atom which then emits a photon into the cavity, again by virtue of the short vacuum-Rabi time in the strong coupling regime. Secondly, laser light is coupled into the cavity whose transmission is modified by the presence of the atom. In both configurations, accurate knowledge about the atom can be obtained by observing with unprecedented time resolution the photons that escape the cavity through one (or both) of its mirrors.

Let us now look at a typical cavity QED experiment as displayed in Figs. 28.4. Here, the cavity is of the Fabry–Perot type and consists of two concave dielectric mirrors facing each other at a distance of at most a few 100 μm . The cavity supports a standing-wave mode with a focus at its center. An essential requirement for achieving strong coupling is to have both the waist of the cavity mode and the distance between the two mirrors small. In this case, the electric field of a single photon confined to a small volume in space is large, typically a few 100 V/m for the above dimensions, making the dipole interaction between the atom and the photon large, too. The small mirror spacing, however, has a pronounced disadvantage: the photon lifetime is also small. To compensate this decrease of the cavity lifetime, the reflectivity of the mirrors must be as high as possible. The best commercially available mirrors feature transmission, absorption and scattering losses down to about 1:1 000 000 each, a value several 10 000 times smaller than that of metallic mirrors. This makes it possible to realize cavities with a finesse exceeding 1 000 000 [27]. In such a good cavity, single photons are reflected to and fro between the mirrors several 100 000 times.

Single atoms are now sent between the two mirrors, either dropped from above or injected from below in fountain geometry. The velocity of the atoms is reduced to a very small value by standard laser-cooling techniques. In the simplest situation, these atoms just pass the cavity in free fall, in which case transit times of the order of a few 10 μs are achieved with atoms moving with a speed of a few m/s. Such a setup has the advantage that the mechanical influence of the cavity field on the atomic trajectory can largely be neglected. But the atoms can also be trapped inside the cavity by means of an auxiliary laser field (not shown in Fig. 28.4). This field can either be weak and near-resonant with the atom [28, 29], or strong and far-detuned from the

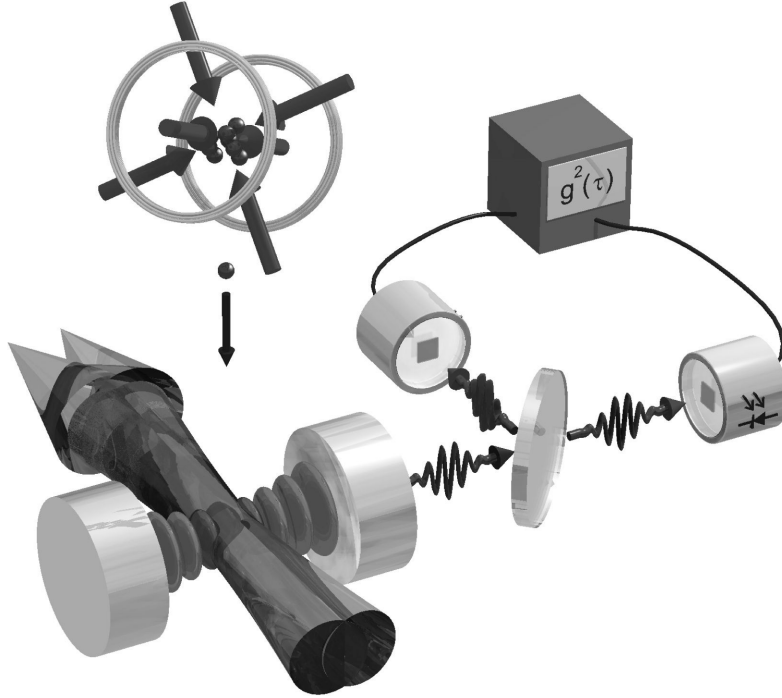


Figure 28.4. Experimental setup of an optical cavity QED experiment: Cold atoms dropped through (or stored in) a high-finesse optical cavity are illuminated with laser beams from the side (or through one of the mirrors). The photons emitted from the cavity are recorded with single-photon counters. The use of a beam splitter in front of the two detectors allows one to measure the photon statistics of the emitted light.

atom [30–34]. In the first case, trapping can be achieved with single photons in the cavity on average, but trapping times are severely limited by spontaneous emission events and quantum fluctuations of both the atomic dipole and the cavity field. In the latter case, single atoms have been observed to stay inside the cavity for several 10 s [34], limited either by collisions with atoms of the background gas in a nonperfect vacuum or, ultimately, by the cavity-enhanced momentum diffusion in the far-detuned dipole trap. Compared to experiments with freely falling atoms, the extended cavity dwell time for a trapped atom comes at the expense of a dramatically more complex protocol of capturing, trapping and cooling the intracavity atom. The precise control of the atomic motion between closely spaced, highly reflecting mirrors is subject of intense investigations in several laboratories worldwide.

Systems such as that described here have been used to perform a plethora of cavity QED experiments in the optical domain during the last few years. These include the observation of single atoms in realtime [35–38], the realization of an atom–cavity microscope [29] and an atomic kaleidoscope [39–41] to track the motion of individual atoms with high spatial and temporal resolution, the counter-intuitive vacuum-stimulated generation of photons with sin-

gle laser-cooled atoms freely falling through the cavity one after the other [42, 43], the optical feedback on the atomic motion based on a measurement of the atom's velocity with the goal to increase the dwell time of the atom inside the cavity [44], the cooling of the atomic motion by means of a novel technique which makes use of the atom's coupling to the dissipative cavity instead of its spontaneous emission [33, 34, 45–47], the realization of a continuously operated single-atom light source exhibiting a nonclassical photon statistics [48], the repeated optical transport of single (or a short string of) atoms through a high-finesse cavity with submicron precision [38, 49], and last but not least the spectroscopic investigation of the energy-level structure of the strongly-coupled bound atom–cavity system with its characteristic vacuum-Rabi splitting, representing in the frequency domain the time-dependent vacuum-Rabi oscillation already known from Fig. 28.2 [50, 51]. While all these experiments were performed with one (laser-cooled) atom in the cavity, other experiments employed an atomic beam, with atoms passing through the cavity at thermal speed. As mentioned above, such experiments do not require the complex trapping and cooling protocol of the single-atom experiments. In one beam experiment, the optical analogue of the micromaser, a microlaser, with atoms prepared in a metastable excited state was demonstrated [52]. In other beam experiments, novel quantum effects demonstrating the nonclassical photon statistics of the light transmitted through the cavity were observed [53–55], and the conditional state of the cavity field (produced by a measurement) was stabilized by means of feedback on the driving laser [56]. Moreover, the transition from photon antibunching to photon bunching occurring when the average number of fluorescing atoms inside the cavity is increased from a value well below 1 to much larger than 1 [57] was investigated. But arguably most interesting from the point of view of quantum information processing is the demonstration of a novel light source emitting single photons on demand. These experiments make full use of the unique potential offered by cavity QED concepts, as will be described in some detail now [58–63].

A remarkable feature of this new light source is that it generates photons without spontaneous emission. In particular, the emitting atom is at no time promoted to an excited state. Instead, the atom is always in a so-called dark state: By slowly varying the parameters of the system, a stimulated Raman process transfers the atom adiabatically from one ground state to another ground state (another hyperfine or Zeeman level) while depositing a photon into the initially empty cavity [64]. Experimentally, the adiabatic passage is performed by slowly increasing the intensity of the laser driving the atom to a level where its Rabi frequency exceeds the vacuum-Rabi frequency associated with a single intracavity photon. For continuous driving, this can be achieved by displacing the laser focus downstream from the cavity axis with respect to the free atomic motion. In such a counter-intuitive configuration, the photon is produced while the atom is leaving the cavity, entering the drive laser. For pulsed driving, the decrease of the atom–cavity coupling can be replaced by cavity decay. Here, the escape of the photon from the cavity finishes the adiabatic passage. In the latter case, the atom can be pumped back to the initial state and the whole process can be repeated as long as the atom resides in the cavity. In this way, a bit stream of single-photon pulses is generated. The stimulated adiabatic transfer process has the distinctive advantage that it is intrinsically reversible and thus ideal to interconnect flying and stationary qubits, i.e., photons and atoms, respectively. It also allows one to control the time-dependent amplitude and frequency of the emitted photon by using a suitably tailored laser pulse.

Figure 28.5 shows data from the very first experiment with atoms falling through the cavity at such a low rate that the probability of having two or more atoms in the cavity is negligible [60]. The figure displays the intensity correlation function of the emitted photon stream as measured with the Hanbury Brown and Twiss setup of Fig. 28.4. The pronounced peaks reflect the pulsed nature of the light source and occur at times determined by the repetition rate of the pump laser, about 200 kHz in this particular experiment. The missing peak at zero delay time proves that single photons are emitted, because single photons cannot hit simultaneously the two photon detectors behind the beam splitter. The decay of the peak height for increasing delay time comes from the finite atom–cavity transit time in this first experiment. The decay was largely suppressed in similar experiments performed recently with a trapped atom or ion [62, 63].

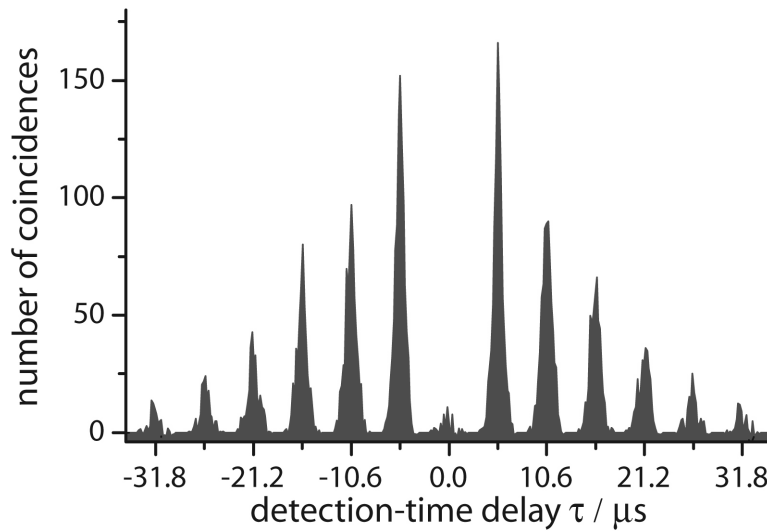


Figure 28.5. Photon statistics of a deterministic single-photon source [60]. The comb-like structure is due to the pulsed driving. Strong photon antibunching as characterized by the missing peak at zero detection-time delay is observed. The decrease of the peak height for larger delays is due to the finite atom–cavity interaction time for a freely moving atom.

Interesting results were also obtained in an experiment in which two cavity QED photons generated one-after-the-other were appropriately delayed and superimposed on a beam splitter [65,66]. Although these two photons were produced by means of the same atom, they were truly independent because after the emission of the first photon optical excitation in combination with spontaneous emission was required to pump the atom back to the initial state before the generation of the second photon. Consider now the situation in which the two photons have identical polarizations and frequencies and, hence, are indistinguishable. In this case it is well known that the photons coalesce, i.e., they leave the beam splitter as a pair through one of the two output ports. This effect occurs only for single-photon fields and has been observed in countless experiments with photon pairs produced by parametric fluorescence in a nonlinear

crystal. It lies at the heart of quantum computing with linear optics. But what happens when the two incoming photons have different frequencies? As the two photons are distinguishable now, the effect of photon coalescence is expected to disappear. However, it can be restored in a time-resolved experiment with photon detectors having a response time much shorter than the duration of the single-photon pulses. In fact, the experiment (see Fig. 28.6) shows that no coincidences at the two output ports are observed for zero detection-time delay. It is remarkable, that two different single photons impinging simultaneously on a beam splitter do not produce simultaneous “clicks” in the two detectors at the two output ports, provided that the time resolution of the detectors is better than the inverse of the frequency separation of the two photons. In addition to this observation, a novel interference effect occurs that can be described as a quantum-beat phenomenon between the two incoming single-photon fields. The beat arises because a photon detected behind the beam splitter could equally come from either of the two input ports. The detection event therefore projects the incoming product state onto an entangled state containing one or the other photon with equal probability in one or the other input port, respectively. The relative phase of this superposition state evolves in time with the frequency difference of the two photons, leading to a beat signal. Its duration depends on the coherence time of the two incoming photons. The effect can therefore be used to characterize the coherence properties of single-photon wave packets or, more general, the coherence properties of the single-photon source.

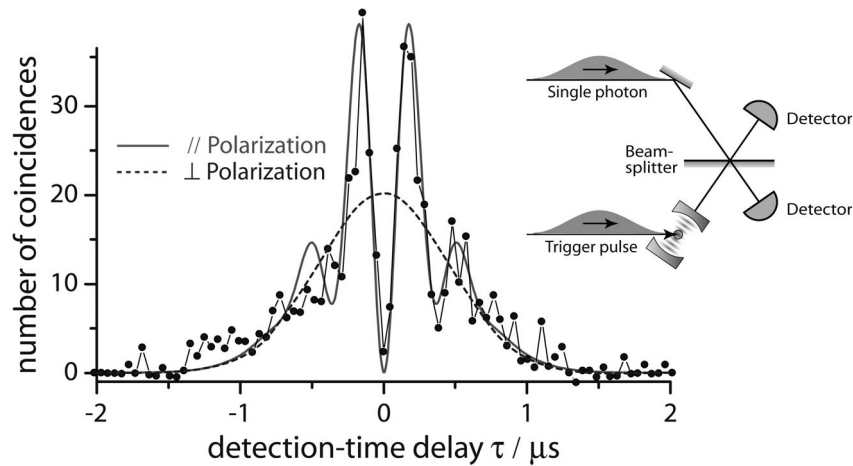


Figure 28.6. Time-resolved quantum-beat experiment with two single-photon pulses impinging simultaneously on a beam splitter [66]. Photon-detection times are recorded with fast counters at the two output ports of the beam splitter. The distribution of the time intervals between detection events displays a central minimum, demonstrating the absence of simultaneous detection events. The oscillatory behaviour comes from the frequency difference (3 MHz) of the two 450 ns long incoming photons. The damping time of the oscillation reflects the coherence time of the photons. The dashed line obtained for orthogonal polarization of the two photons serves as a reference.

It is remarkable that already in these first experiments a very good control over flying photonic wave packets has been achieved, demonstrating the truly impressive progress in the relatively young research field of optical cavity QED. It should be noted, however, that the experimental techniques required to control both the internal and external degrees of freedom of single strongly coupled atoms are quite demanding, making the experiments a real challenge. From the theoretical side, the dissipative coupling to the environment makes the description of optical experiments difficult. An additional challenge is to properly take into account the atomic motion and the effect of the light force on the atomic trajectory and, hence, on the precise value of the atom–cavity coupling [45–47, 67, 68]. This force arises from the recoil kicks the atom experiences when absorbing or emitting a photon. The inclusion of the light force leads to a complex interplay between the motion of the atom, its internal dynamics and the dynamics of the cavity field [69, 70]. No general solutions of the problem of a driven, open system are known even for one intracavity atom.

28.4 Conclusions and Outlook

Both in the microwave and the optical domains, more experiments in the same league as those mentioned above are now in progress or planned. For example, it will be possible to repeatedly move trapped atoms in and out of the strong-coupling region in the near future, enabling one to address individual or pairs of qubits of an atomic quantum register with a high-finesse cavity. First experiments in this direction, with atoms localized in a standing-wave dipole-force trap which can be displaced perpendicular to the cavity axis, have already been reported [38, 49]. It therefore seems possible to create in a deterministic way an entanglement of one stationary atom (individually selected from a string of several atoms) and a flying photon. Alternatively, two atoms strongly coupled by the cavity could be used for scalable quantum computation [71, 72]. Experiments with many atoms coupled to the cavity would also allow one to exploit collective radiation effects like superradiance. The collective emission of light from the atomic ensemble automatically generates a large entangled state involving all the intracavity atoms. The basic idea here is that photons are simultaneously emitted from all atoms, making it impossible to tell, even in principle, from which atom the photon is emitted.

In another line of experiments, setups with two spatially separated cavities are presently under construction. They will offer a much greater flexibility and new possibilities for quantum information processing. For example, photons could be exchanged between two atom–cavity systems, allowing one to transfer the quantum state of one atom to another. Using the single-photon technique described above, entanglement between two remote locations could thus be generated [73]. The technology of individually addressable atom–cavity systems is intrinsically scalable so that a large network with stationary atoms as quantum memories and flying photons as quantum messengers could be formed [74]. In such a network the state of an atom could be teleported over a macroscopic distance like several meters or even many kilometers [75, 76]. Moreover, nonlocal Schrödinger cat states residing simultaneously in separated cavities could be created and studied. Such states are a completely new species of quantum monsters, allowing us to advance our understanding of decoherence and nonlocality.

It is even possible to envision experiments blending cavity QED and atom chip concepts. In the latter technology, atoms are manipulated with magnetic and/or electric fields gener-

ated by the wires of a microfabricated chip. On-chip conveyor belts can be used to transport atoms along the surface of the chip and move them into on-chip transmission-line cavities. Micrometer-sized cavities between the tips of two optical fibers are presently tested in several laboratories around the world. Such integrated experiments provide a scalable architecture for quantum information processing. Coherence preserving traps can be tailored for Rydberg atoms, holding them over superconducting chips, which block their only decay, spontaneous emission [77]. In addition, the on-chip atoms could be coupled with superconducting qubits also integrated on-chip, opening a wealth of new possibilities. Similarly, superconducting Cooper pair boxes (instead of Rydberg atoms) coupled to microwave strip-line resonators (instead of Fabry–Perot resonators) offer an interesting solid-state alternative to atom-based cavity QED [78, 79]. Last but not least, the recent advances in nanotechnology will allow one to design novel wavelength-sized optical cavities, e.g., with photonic band-gap materials. The very strong coupling that can theoretically be achieved in such small cavities could dramatically boost the speed of quantum gates or the rate of single photons delivered on demand. A first step into this direction has already been done with the achievement of strong coupling in systems with artificial atoms, i.e., quantum dots [80, 81].

The countless avenues cavity QED opens up for quantum information processing makes research with individual atoms and photons in confined space increasingly exciting even 50 years after the first ideas were formulated!

References

- [1] E.M. Purcell, Spontaneous emission probabilities at radio frequencies, *Phys. Rev.* **69**, 681 (1946).
- [2] P.R. Berman (Ed.), Cavity Quantum Electrodynamics, in *Advances in Atomic, Molecular and Optical Physics*, supplement 2, Academic Press, New York, (1994).
- [3] F. De Martini and C. Monroe (Eds.), Experimental Quantum Computation and Information, in *Proceedings of the International School of Physics “Enrico Fermi,”* IOS Press, Amsterdam, (2002).
- [4] H. Mabuchi and A.C. Doherty, Cavity quantum electrodynamics: Coherence in context, *Science* **298**, 1372 (2002).
- [5] K.J. Vahala, Optical microcavities, *Nature* **424**, 839 (2003).
- [6] G. Rempe, Quantum mechanics with single atoms and photons, *Phys. World* **13**, (12), 37 (2000).
- [7] T.F. Gallagher, Rydberg atoms, Cambridge University Press, Cambridge (1994).
- [8] J.-M. Raimond, M. Brune, and S. Haroche, Colloquium: Manipulating quantum entanglement with atoms and photons in a cavity, *Rev. Mod. Phys.* **73**, 565 (2001).
- [9] P. Maioli, T. Meunier, S. Gleyzes, A. Auffeves, G. Nogues, M. Brune, J.-M. Raimond, and S. Haroche, Nondestructive Rydberg atom counting with mesoscopic fields in a cavity, *Phys. Rev. Lett.* **94**, 113601 (2005).
- [10] M. Weidinger, B.T.H. Varcoe, R. Heerlein, and H. Walther, Trapping states in the micro-maser, *Phys. Rev. Lett.* **82**, 3795 (1999).
- [11] B.T.H. Varcoe, S. Brattke, M. Weidinger, and H. Walther, Preparing pure photon number states of the radiation field, *Nature* **403**, 743 (2000).

- [12] S. Brattke, B.T.H. Varcoe, and H. Walther, Generation of photon number states on demand via cavity quantum electrodynamics, *Phys. Rev. Lett.* **86**, 3534 (2001).
- [13] G. Rempe, A. Walther, and N. Klein, Observation of quantum collapse and revival in a one-atom maser, *Phys. Rev. Lett.* **58**, 353 (1987).
- [14] G. Rempe, F. Schmidt-Kaler, and H. Walther, Observation of sub-Poissonian photon statistics in a micromaser, *Phys. Rev. Lett.* **64**, 2783 (1990).
- [15] M. Brune, J.-M. Raimond, P. Goy, L. Davidovich, and S. Haroche, Realization of a two-photon maser oscillator, *Phys. Rev. Lett.* **59**, 1899 (1987).
- [16] X. Maitre, E. Hagley, G. Nogues, C. Wunderlich, P. Goy, M. Brune, J.-M. Raimond, and S. Haroche, Quantum memory with a single photon in a cavity, *Phys. Rev. Lett.* **79**, 769 (1997).
- [17] E. Hagley, X. Maitre, G. Nogues, C. Wunderlich, M. Brune, J.-M. Raimond, and S. Haroche, Generation of Einstein–Podolsky–Rosen pairs of atoms, *Phys. Rev. Lett.* **79**, 1 (1997).
- [18] A. Rauschenbeutel, P. Bertet, S. Osnaghi, G. Nogues, M. Brune, J.-M. Raimond, and S. Haroche, Controlled entanglement of two field modes in a cavity quantum electrodynamics experiment, *Phys. Rev. Lett.* **64**, 050301 (2001).
- [19] A. Rauschenbeutel, G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.-M. Raimond, and S. Haroche, Coherent operation of a tunable quantum phase gate in cavity QED, *Phys. Rev. Lett.* **83**, 5166 (1999).
- [20] G. Nogues, A. Rauschenbeutel, S. Osnaghi, M. Brune, J.-M. Raimond, and S. Haroche, Seeing a single photon without destroying it, *Nature* **400**, 239 (1999).
- [21] A. Rauschenbeutel, G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.-M. Raimond, and S. Haroche, Step-by-step engineered multiparticle entanglement, *Science* **288**, 2024 (2000).
- [22] S. Osnaghi, P. Bertet, A. Auffeves, P. Maioli, M. Brune, J.-M. Raimond, and S. Haroche, Coherent control of an atomic collision in a cavity, *Phys. Rev. Lett.* **87**, 037902 (2001).
- [23] F. Yamaguchi, P. Milman, M. Brune, J.-M. Raimond, and S. Haroche, Quantum search with two atom collisions in cavity QED, *Phys. Rev. A* **66**, 010302 (2002).
- [24] A. Auffeves, P. Maioli, T. Meunier, S. Gleyzes, G. Nogues, M. Brune, J.M. Raimond, and S. Haroche, Entanglement of a mesoscopic field with an atom induced by photon graininess in a cavity, *Phys. Rev. Lett.* **91**, 230405 (2003).
- [25] T. Meunier, S. Gleyzes, P. Maioli, A. Auffeves, G. Nogues, M. Brune, J.M. Raimond, and S. Haroche, Rabi oscillations revival induced by time reversal: A test of mesoscopic quantum coherence, *Phys. Rev. Lett.* **94**, 010401 (2005).
- [26] P. Bertet, A. Auffeves, P. Maioli, S. Osnaghi, T. Meunier, M. Brune, J.M. Raimond, and S. Haroche, Direct measurement of the Wigner function of a one-photon Fock state in a cavity, *Phys. Rev. Lett.* **89**, 200402 (2002).
- [27] G. Rempe, R.J. Thompson, H.J. Kimble, and R. Lalezari, Measurement of ultralow losses in an optical interferometer, *Opt. Lett.* **17**, 363 (1992).
- [28] P.W.H. Pinkse, T. Fischer, P. Maunz, and G. Rempe, Trapping an atom with single photons, *Nature* **404**, 365 (2000).
- [29] C.J. Hood, T.W. Lynn, A.C. Doherty, A.S. Parkins, and H.J. Kimble, The atom-cavity microscope: Single atoms bound in orbit by single photons, *Science* **287**, 1447 (2000).

- [30] J. Ye, D.W. Vernooy, and H.J. Kimble, Trapping of single atoms in cavity QED, *Phys. Rev. Lett.* **83**, 4987 (1999).
- [31] J. McKeever, J.R. Buck, A.D. Boozer, A. Kuzmich, H.C. Nägerl, D.M. Stamper-Kurn, and H.J. Kimble, State-insensitive cooling and trapping of single atoms in an optical cavity, *Phys. Rev. Lett.* **90**, 133602 (2003).
- [32] J. McKeever, J.R. Buck, A.D. Boozer, and H.J. Kimble, Determination of the number of atoms trapped in an optical cavity, *Phys. Rev. Lett.* **93**, 143601 (2004).
- [33] P. Maunz, T. Puppe, I. Schuster, N. Syassen, P.W.H. Pinkse, and G. Rempe, Cavity cooling of single atoms, *Nature* **428**, 50 (2004).
- [34] S. Nußmann, K. Murr, M. Hijkema, B. Weber, A. Kuhn, and G. Rempe, Vacuum-stimulated cooling of single atoms in three dimensions, Preprint, quant-ph/0506067, 2005.
- [35] H. Mabuchi, Q.A. Turchette, M.S. Chapman, and H.J. Kimble, Realtime detection of individual atoms falling through a high-finesse optical cavity, *Opt. Lett.* **21**, 1393 (1996).
- [36] C.J. Hood, M.S. Chapman, T.W. Lynn, and H.J. Kimble, Realtime cavity QED with single atoms, *Phys. Rev. Lett.* **80**, 4157 (1998).
- [37] P. Münstermann, T. Fischer, P.W.H. Pinkse, and G. Rempe, Single slow atoms from an atomic fountain observed in a high-finesse optical cavity, *Opt. Commun.* **159**, 63 (1999).
- [38] J.A. Sauer, K.M. Fortier, M.S. Chang, C.D. Hamley, and M.S. Chapman, Cavity QED with optically transported atoms, *Phys. Rev. A* **69**, 051804 (2004).
- [39] P. Horak, H. Ritsch, T. Fischer, P. Maunz, T. Puppe, P.W.H. Pinkse, and G. Rempe, Optical kaleidoscope using a single atom, *Phys. Rev. Lett.* **88**, 043601 (2002).
- [40] P. Maunz, T. Puppe, T. Fischer, P.W.H. Pinkse, and G. Rempe, The emission pattern of an atomic dipole in a high-finesse optical cavity, *Opt. Lett.* **28**, 46 (2003).
- [41] T. Puppe, P. Maunz, T. Fischer, P.W.H. Pinkse, and G. Rempe, Single-atom trajectories in higher order transverse modes of a high-finesse optical cavity, *Phys. Scr.* **T112**, 7 (2004).
- [42] M. Hennrich, T. Legero, A. Kuhn, and G. Rempe, Vacuum-stimulated Raman scattering based on adiabatic passage in a high-finesse optical cavity, *Phys. Rev. Lett.* **85**, 4872 (2000).
- [43] M. Hennrich, T. Legero, A. Kuhn, and G. Rempe, Counter-intuitive vacuum-stimulated Raman scattering, *J. Mod. Opt.* **50**, 935 (2003).
- [44] T. Fischer, P. Maunz, P.W. H. Pinkse, T. Puppe, and G. Rempe, Feedback on the motion of a single atom in an optical cavity, *Phys. Rev. Lett.* **88**, 163002 (2002).
- [45] P. Horak, G. Hechenblaikner, K.M. Gheri, H. Stecher, and H. Ritsch, Cavity-induced atom cooling in the strong coupling regime, *Phys. Rev. Lett.* **79**, 4974 (1997).
- [46] V. Vuletic and S. Chu, Laser cooling of atoms, ions, or molecules by coherent scattering, *Phys. Rev. Lett.* **84**, 3787 (2000).
- [47] P. Domokos, A. Vukics, and H. Ritsch, Anomalous Doppler-effect and polariton-mediated cooling of two-level atoms, *Phys. Rev. Lett.* **92**, 103601 (2004).
- [48] J. McKeever, A. Boca, A.D. Boozer, J.R. Buck, and H.J. Kimble, Experimental realization of a one-atom laser in the regime of strong coupling, *Nature* **425**, 268 (2003).
- [49] S. Nußmann, M. Hijkema, B. Weber, F. Rohde, G. Rempe, and A. Kuhn, Nanopositioning of single atoms in a micro-cavity, Preprint, quant-ph/0506088, 2005.

- [50] A. Boca, R. Miller, K.M. Birnbaum, A.D. Boozer, J. McKeever, and H.J. Kimble, Observation of the vacuum Rabi spectrum for one trapped atom, *Phys. Rev. Lett.* **93**, 233603 (2004).
- [51] P. Maunz, T. Puppe, I. Schuster, N. Syassen, P.W.H. Pinkse, and G. Rempe, Normal-mode spectroscopy of a single bound atom–cavity system, *Phys. Rev. Lett.* **94**, 033002 (2005).
- [52] K. An, J.J. Childs, R.R. Dasari, and M.S. Feld, Microlaser—A laser with one atom in an optical resonator, *Phys. Rev. Lett.* **73**, 3375 (1994).
- [53] S.L. Mielke, G.T. Foster, and L.A. Orozco, Nonclassical intensity correlations in cavity QED, *Phys. Rev. Lett.* **80**, 3948 (1998).
- [54] H.J. Carmichael, H.M. Castro-Beltran, G.T. Foster, and L.A. Orozco, Giant violations of classical inequalities through conditional homodyne detection of the quadrature amplitudes of light, *Phys. Rev. Lett.* **85**, 1855 (2000).
- [55] G.T. Foster, L.A. Orozco, H.M. Castro-Beltran, and H.J. Carmichael, Quantum state reduction and conditional time evolution of wave-particle correlations in cavity QED, *Phys. Rev. Lett.* **85**, 3149 (2000).
- [56] W.P. Smith, J.E. Reiner, L.A. Orozco, S. Kuhr, and H.M. Wiseman, Capture and release of a conditional state of a cavity QED system by quantum feedback, *Phys. Rev. Lett.* **89**, 133601 (2002).
- [57] M. Hennrich, A. Kuhn, and G. Rempe, Transition from antibunching to bunching in cavity QED, *Phys. Rev. Lett.* **94**, 053604 (2005).
- [58] C.K. Law and H.J. Kimble, Deterministic generation of a bit-stream of single-photon pulses, *J. Mod. Opt.* **44**, 2067 (1997).
- [59] A. Kuhn, M. Hennrich, T. Bondo, and G. Rempe, Controlled generation of single photons from a strongly coupled atom–cavity system, *Appl. Phys. B* **69**, 373 (1999).
- [60] A. Kuhn, M. Hennrich, and G. Rempe, Deterministic single-photon source for distributed quantum networking, *Phys. Rev. Lett.* **89**, 067901 (2002); see also *Phys. Rev. Lett.* **90**, 249802 (2003).
- [61] M. Hennrich, T. Legero, A. Kuhn, and G. Rempe, Photon statistics of a non-stationary periodically driven single-photon source, *New J. Phys.* **6**, 86 (2004).
- [62] J. McKeever, A. Boca, A.D. Boozer, R. Miller, J.R. Buck, A. Kuzmich, and H.J. Kimble, Deterministic generation of single photons from one atom trapped in a cavity, *Science* **303**, 1992 (2004).
- [63] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, Continuous generation of single photons with controlled waveform in an ion-trap cavity system, *Nature* **431**, 1075 (2004).
- [64] A. Kuhn and G. Rempe, Optical Cavity QED: Fundamentals and Application as a Single-Photon Light Source, in Ref. [3].
- [65] T. Legero, T. Wilk, A. Kuhn, and G. Rempe, Time-resolved two-photon quantum interference, *Appl. Phys. B* **77**, 797 (2003).
- [66] T. Legero, T. Wilk, M. Hennrich, G. Rempe, and A. Kuhn, Quantum beat of two single photons, *Phys. Rev. Lett.* **93**, 070503 (2004).

- [67] S.J. van Enk, J. McKeever, H.J. Kimble, and J. Ye, Cooling of a single atom in an optical trap inside a resonator, *Phys. Rev. A* **64**, 013407 (2001).
- [68] K. Murr, On the suppression of the diffusion and the quantum nature of a cavity mode. Optical bistability: Forces and friction in driven cavities, *J. Phys. B: At. Mol. Opt. Phys.* **36**, 2515 (2003).
- [69] P. Münstermann, T. Fischer, P. Maunz, P.W.H. Pinkse, and G. Rempe, Dynamics of single-atom motion observed in a high-finesse cavity, *Phys. Rev. Lett.* **82**, 3791 (1999).
- [70] P. Münstermann, T. Fischer, P. Maunz, P.W.H. Pinkse, and G. Rempe, Observation of cavity-mediated long-range light forces between strongly coupled atoms, *Phys. Rev. Lett.* **84**, 4068 (2000).
- [71] T. Pellizzari, S.A. Gardiner, J.I. Cirac, and P. Zoller, Decoherence, continuous observation, and quantum computing: A cavity QED model, *Phys. Rev. Lett.* **75**, 3788 (1995).
- [72] L.M. Duan and H.J. Kimble, Scalable photonic quantum computation through cavity-assisted interactions, *Phys. Rev. Lett.* **92**, 127902 (2004).
- [73] D.E. Browne, M.B. Plenio, and S.F. Huelga, Robust creation of entanglement between ions in spatially separate cavities, *Phys. Rev. Lett.* **91**, 067901 (2003).
- [74] J.I. Cirac, P. Zoller, H.J. Kimble, and H. Mabuchi, Quantum state transfer and entanglement distribution among distant nodes in a quantum network, *Phys. Rev. Lett.* **78**, 3221 (1997).
- [75] S. Bose, P.L. Knight, M.B. Plenio, and V. Vedral, Proposal for teleportation of an atomic state via cavity decay, *Phys. Rev. Lett.* **83**, 5158 (1999).
- [76] S. Lloyd, M.S. Shahriar, J.H. Shapiro, and P.R. Hemmer, Long distance unconditional teleportation of atomic states via complete Bell-state measurements, *Phys. Rev. Lett.* **87**, 167903 (2001).
- [77] P. Hyafil, J. Mozley, A. Perrin, J. Tailleur, G. Nogues, M. Brune, J.M. Raimond, and S. Haroche, Coherence-preserving trap architecture for long-term control of giant Rydberg atoms, *Phys. Rev. Lett.* **93**, 103001 (2004).
- [78] I. Chiorescu, P. Bertet, K. Semba, Y. Nakamura, C.J.P.M. Harmans, and J.E. Mooij, Coherent dynamics of a flux qubit coupled to a harmonic oscillator, *Nature* **431**, 159 (2004).
- [79] A. Wallraff, D.I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S.M. Girvin, and R.J. Schoelkopf, Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics, *Nature* **431**, 162 (2004).
- [80] J.P. Reithmaier, G. Sek, A. Löffler, C. Hofmann, S. Kuhn, S. Reitzenstein, L.V. Keldysh, V.D. Kulakovskii, T.L. Reinecke, and A. Forchel, Strong coupling in a single quantum dot-semiconductor microcavity system, *Nature* **432**, 197 (2004).
- [81] T. Yoshie, A. Scherer, J. Hendrickson, G. Khitrova, H.M. Gibbs, G. Rupper, C. Ell, O.B. Shchekin, and D.G. Deppe, Vacuum Rabi splitting with a single quantum dot in a photonic crystal nanocavity, *Nature* **432**, 200 (2004).

29 Quantum Electrodynamics of a Qubit

Gernot Alber and Georgios M. Nikolopoulos

A detailed understanding of the basic physical laws governing the exchange of quantum information, as well as the interaction between material qubits and the quantized electromagnetic field, is of central importance for realizing quantum information networks and for suppressing decoherence due to spontaneous emission of photons. In this section, some basic physical aspects of this interaction are explored in the special case of a single material qubit.

The energy exchange between a material qubit interacting with the electromagnetic field is dominated by the absorption and emission of photons [1]. Whereas absorption and stimulated emission of photons is conditioned on photons which are already present in the electromagnetic field, spontaneous emission of photons occurs randomly and even if the electromagnetic field is in its ground state (vacuum) [2]. It is this random and uncontrollable feature of this latter process which causes spontaneous decay and decoherence of qubits. Therefore, suppressing its undesired and uncontrollable features is one of the major challenges in the context of quantum information processing. For this purpose powerful error correction methods have been designed recently [3–5]. Alternatively, spontaneous decay of qubits can also be suppressed at least partially by an appropriate engineering of their coupling to the electromagnetic field.

The quantum dynamics of a material qubit interacting with the electromagnetic field depend significantly on the structure of the field modes. If a qubit is coupled to a single-field mode only, its quantum state can be transferred to the field mode and back again in a reversible way as described by the Jaynes–Cummings–Paul model [6, 7]. This reversible energy exchange manifests itself in vacuum Rabi oscillations of the qubit between its excited state and its ground state, for example [7]. But with increasing number of interacting field modes this reversible character of the qubit–field dynamics is lost gradually [8–11]. In particular, in the limit of a continuum of accessible field modes the reversibility of the state exchange between qubit and field is lost completely. Typically, under such circumstances an initially excited qubit decays to its ground state spontaneously [12]. As a result, a controllable and reversible transfer of the quantum state of such a qubit to the electromagnetic field and back again becomes impossible. In general, the spontaneous decay rate of the qubit depends on the density of field modes it is coupled to. For purposes of processing quantum information, for example, this latter dependence can be exploited for suppressing spontaneous decay process by an appropriate engineering of the mode structure of the electromagnetic field [13]. Photonic crystals [14] are particularly well suited for this purpose.

In this section, we discuss basic physical aspects of the interaction between a single qubit and the electromagnetic field. In particular, we focus on the following main questions: How

does the interaction of a qubit with the electromagnetic field depend on the structure and the density of states of field modes? How does the reversible dynamics of the coupling to a single mode of the radiation field change to an irreversible energy transfer to the electromagnetic field as the number of interacting field modes is increased and the continuum limit is approached? What is the characteristic time evolution of the spontaneous decay of a qubit embedded in a photonic crystal? How do bandgaps influence this decay? Is it possible to form bound qubit–field states within a photonic crystal?

In order to address these questions in Section 29.1 we first of all analyze the dynamics of the spontaneous decay of a single qubit which is assumed to be located at the center of a spherically symmetric metallic cavity. The spherical symmetry of the electromagnetic field modes the qubit is coupled to allows us to address many aspects of this problem even analytically. Within this model system we can explore the influence of the cavity size on the dynamics of the spontaneous decay process of the qubit. The continuum limit of this model is achieved in the limit of an infinitely large cavity. Basic aspects of the dynamics of spontaneous decay of a qubit in a photonic crystal, the influence of photonic bandgaps on this decay process, and the possibility of forming bound qubit–field states are explored in Section 29.2.

29.1 Quantum Electrodynamics of a Qubit in a Spherical Cavity

In this section we discuss the spontaneous emission of a photon by a single (infinitely heavy) qubit which is assumed to be located at the center of a spherically symmetric metallic cavity. With the help of a semiclassical path representation valid for highly excited field modes, the probability amplitude of observing the qubit in its initially excited state at any later time is expressed as a sum of probability amplitudes which are associated with repeated returns of the spontaneously emitted photon to the center of the cavity where it interacts again with the qubit [10]. In this way we obtain a unified description of the spontaneous emission process which, in the spirit of the Feynman path integral approach [15], sheds light onto the underlying elementary physical processes involved in the gradual transition from reversible to irreversible energy exchange between a single qubit and the electromagnetic field.

29.1.1 The model

We consider a single qubit, i.e. a quantum mechanical two-level system with (bare) energy eigenstates $|g\rangle$ and $|e\rangle$ of well-defined parity and corresponding energies $E_g = 0$ and $E_e > 0$, interacting with the electromagnetic radiation field in a spherical cavity. The field-modes are identified by the mode indices $l \in I$ and ω_l are their frequencies. This two-level system is assumed to be localized at the center of a spherical cavity, say at position $\mathbf{x} = \mathbf{0}$, and the spatial extension of its charge distribution is assumed to be much smaller than the wave lengths of the electromagnetic field modes it is coupled to significantly. Furthermore, this qubit is supposed to be infinitely heavy so that its center of mass motion is not affected by momentum transfer from the electromagnetic field to the qubit. Thus, in the dipole approximation [1] the

Hamiltonian of this quantum system is given by

$$\hat{H} = \hbar\bar{\omega}_0\hat{b}_0^\dagger\hat{b}_0 + \sum_{l \in I} \hbar\omega_l\hat{a}_l^\dagger\hat{a}_l - \hat{\mathbf{d}} \cdot \hat{\mathbf{E}}(\mathbf{x} = 0) \quad (29.1)$$

with the dipole operator of the two-level system

$$\hat{\mathbf{d}} = \hat{b}_0\langle g|\hat{\mathbf{d}}|e\rangle + \hat{b}_0^\dagger\langle e|\hat{\mathbf{d}}|g\rangle \quad (29.2)$$

and with the atomic ladder operators $\hat{b}_0 = |g\rangle\langle e|$ and $\hat{b}_0^\dagger = |e\rangle\langle g|$. The position of the qubit is denoted by $\mathbf{x}$ while its (bare) excitation energy is given by $\hbar\bar{\omega}_0 \equiv (E_e - E_g)$. The creation and annihilation operators of mode $l \in I$ of the electromagnetic field are denoted by $\hat{a}_l^\dagger$ and $\hat{a}_l$, respectively. Correspondingly, the expansion of the electric field operator $\hat{\mathbf{E}}(\mathbf{x})$ in terms of the orthonormal set of mode functions $\mathbf{u}_l(\mathbf{x})$ is given by

$$\hat{\mathbf{E}}(\mathbf{x}) = -i \sum_l \sqrt{\frac{\hbar\omega_l}{2\epsilon_0}} \{ \mathbf{u}_l^*(\mathbf{x})\hat{a}_l^\dagger - \mathbf{u}_l(\mathbf{x})\hat{a}_l \} \quad (29.3)$$

with ϵ_0 denoting the dielectric constant of the vacuum. In Eq. (29.1) only the interaction of the two-level system with the almost resonantly coupled modes ($l \in I$) of the electromagnetic field is taken into account. To a good degree of approximation these couplings can be described approximately by the rotating-wave approximation [1]. Thereby, the interaction operator $-\hat{\mathbf{d}} \cdot \hat{\mathbf{E}}(\mathbf{x} = 0)$ is approximated by the expression

$$i\langle g|\hat{\mathbf{d}}|e\rangle\hat{b}_0 \sum_l \sqrt{\frac{\hbar\omega_l}{2\epsilon_0}} \mathbf{u}_l^*(\mathbf{x} = 0)\hat{a}_l^\dagger - i\langle e|\hat{\mathbf{d}}|g\rangle\hat{b}_0^\dagger \sum_l \sqrt{\frac{\hbar\omega_l}{2\epsilon_0}} \mathbf{u}_l(\mathbf{x} = 0)\hat{a}_l.$$

The couplings to all other modes ($l \notin I$) which are not taken into account by the dipole and rotating-wave approximation can be treated at a later stage perturbatively. These modes give rise to a radiative level shift, i.e. $\bar{\omega}_0 \rightarrow \omega_0$, where $\hbar\omega_0$ denotes the physically observed energy difference of the qubit-system considered [compare with the discussion following Eq. (29.13)]. In the case of a realistic atom these radiative energy shifts are the well-known Lamb shifts [16,17]. It is worth mentioning that for a proper treatment of the influence of these off-resonant modes the dipole approximation is no longer applicable [18].

Within this model we aim at describing the influence of the mode structure of the cavity onto the spontaneous emission of photons by the qubit. Thus, we want to restrict ourselves to an initial condition in which the two-level system is prepared in its excited state $|e\rangle$ and the electromagnetic field is in its vacuum state $|\{0\}\rangle$. Due to the coupling between the two systems the two-level system will exchange its excitation predominantly with the resonantly coupled modes of the electromagnetic field with $\omega_l \approx \omega_0$. As long as we restrict ourselves to this particular initial condition we can replace the two-level system also by a harmonic oscillator by interpreting the operators $\hat{b}_0^\dagger$ and $\hat{b}_0$ of Eqs. (29.1) and (29.2) as the creation- and destruction-operators of a harmonic oscillator. This is possible because by energy conservation in this case only the ground and first excited state of this harmonic oscillator participate in the dynamical evolution. Such a replacement offers advantages because the dynamical evolution of the qubit interacting with the electromagnetic field reduces effectively to the diagonalization of a system of coupled harmonic oscillators.

29.1.2 Mode structure of the free radiation field in a spherical cavity

Before addressing this diagonalization let us first of all determine the mode structure of the free electromagnetic radiation field in a spherical cavity with ideal metallic boundary conditions.

In the Coulomb gauge [1] the electromagnetic field can be decomposed into two parts, namely an instantaneous Coulomb interaction between charged particles and the transverse radiation field. Thus, in the Schrödinger picture the radiation field is described by a vector potential $\hat{\mathbf{A}}(\mathbf{x})$ which fulfills the transversality condition $(\nabla \cdot \hat{\mathbf{A}})(\mathbf{x}) = 0$. This vector potential can always be decomposed into complete orthonormal sets of mode functions $\mathbf{u}_l(\mathbf{x})$ according to

$$\hat{\mathbf{A}}(\mathbf{x}) = \sum_l \sqrt{\frac{\hbar}{2\epsilon_0\omega_l}} \{ \mathbf{u}_l(\mathbf{x}) \hat{a}_l + \mathbf{u}_l^*(\mathbf{x}) \hat{a}_l^\dagger \}.$$

These mode functions are orthonormal solutions of the Helmholtz equation

$$(\nabla^2 + (\omega_l/c)^2) \mathbf{u}_l(\mathbf{x}) = 0 \quad (29.4)$$

fulfilling the appropriate boundary conditions.

In order to generate such a complete system of mode functions for a spherical cavity with ideal metallic boundary conditions the tangential component of $\mathbf{u}_l(\mathbf{x})$ and the normal component of $(\nabla \wedge \mathbf{u}_l)(\mathbf{x})$ have to vanish on the surface of the spherical boundary. The resulting solutions $\mathbf{u}_l(\mathbf{x})$ of Eq. (29.4) determine the discrete set of all possible eigenfrequencies ω_l . Thereby the mode index l identifies all possible mode functions. Thus, in the Schrödinger picture the electric and magnetic field operators are given by Eq. (29.3) and by

$$\hat{\mathbf{B}}(\mathbf{x}) = \sum_l \sqrt{\frac{\hbar}{2\epsilon_0\omega_l}} \{ (\nabla \wedge \mathbf{u}_l)(\mathbf{x}) \hat{a}_l + (\nabla \wedge \mathbf{u}_l)^*(\mathbf{x}) \hat{a}_l^\dagger \}.$$

In particular, in the case of a spherical cavity of radius R with ideal metallic boundary conditions one may choose two different classes of mode functions, namely

$$\begin{aligned} \mathbf{U}_{nLM}(\mathbf{x}) &= \mathcal{N}_{nL} j_L(k_{nL}r) \mathbf{X}_{LM}(\mathbf{x}/|\mathbf{x}|), \\ \mathbf{V}_{nLM}(\mathbf{x}) &= \mathcal{N}_{nL} \frac{i}{k_{nL}} \nabla \wedge j_L(k_{nL}r) \mathbf{X}_{LM}(\mathbf{x}/|\mathbf{x}|) \end{aligned}$$

with the vector spherical harmonics [19]

$$\mathbf{X}_{LM}(\mathbf{x}/|\mathbf{x}|) = -\frac{i}{\sqrt{L(L+1)}} \mathbf{x} \wedge \nabla Y_L^M(\mathbf{x}/|\mathbf{x}|),$$

and with the (ordinary) spherical harmonics $Y_L^M(\mathbf{x}/|\mathbf{x}|)$ ($L \in \mathbb{N}_0, -L \leq M \in \mathbb{Z} \leq L$). The wave numbers of the mode functions are denoted by $k_{nL} \equiv \omega_{nL}/c$. Furthermore, $j_L(kr)$ is the regular spherical Bessel function [20] with the asymptotic behavior

$$\frac{(kr)^L}{(2L+1)!!} \xrightarrow{kr \rightarrow 0} j_L(kr) \xrightarrow{kr \gg 1} \frac{\sin(kr - L\pi/2)}{kr},$$

and with $(2L + 1)!! = (2L + 1)(2L - 1)(2L - 3) \cdots 5 \cdot 3 \cdot 1$. The normalization constants $\mathcal{N}_{nL}$ are given by

$$\mathcal{N}_{nL} = \left\{ \int_0^R dr r^2 j_L^2(k_{nL}r) \right\}^{-1/2} \xrightarrow{n \gg 1} k_{nL} \sqrt{\frac{2}{R}}.$$

The eigenvalues ω_{nL} of the mode functions $\mathbf{U}_{nLM}$ and $\mathbf{V}_{nLM}$ are determined by the conditions $j_L(k_{nL}R) = 0$ and $d(j_L(x))/dx|_{x=k_{nL}R} = 0$, respectively. In the case of highly excited modes, i.e. $k_{nL}R \gg 1$, we find

$$k_{nL}R \xrightarrow{k_{nL}R \gg 1} \pi n + (L + 1)\pi/2 \quad (29.5)$$

so that the density of states is constant, i.e. $dn/d(\hbar\omega_{nL}) = R/(\pi\hbar c)$ with c denoting the speed of light in vacuum. For these highly excited modes only the mode functions $\mathbf{V}_{nL=1M=0}(\mathbf{x})$ are nonvanishing at the center of the cavity where the qubit is located. Therefore, in the dipole approximation the coupling between the qubit and the electromagnetic radiation field is dominated by these particular modes.

29.1.3 Dynamics of spontaneous photon emission

From the considerations of the previous sections, it is apparent that in the dipole and rotating-wave approximations the spontaneous decay of a qubit located at the center of a spherical cavity with ideal metallic boundary conditions can be described by the Hamiltonian

$$\hat{H} = \hbar\omega_0 \hat{b}_0^\dagger \hat{b}_0 + \sum_{l \in I} \hbar\omega_l \hat{a}_l^\dagger \hat{a}_l + \sum_{l \in I} \{ \alpha_l \hat{b}_0 \hat{a}_l^\dagger + \alpha_l^* \hat{b}_0^\dagger \hat{a}_l \} \equiv \sum_{k, m \in \{0\} \cup I} \hat{B}_k^\dagger h_{km} \hat{B}_m \quad (29.6)$$

with $\hat{B}^T = (\hat{b}_0, \hat{a}_1, \hat{a}_2, \dots)$ and with the Hermitian matrix

$$h_{km} = \begin{pmatrix} \hbar\omega_0 & \alpha_1^* & \alpha_2^* & \cdots \\ \alpha_1 & \hbar\omega_1 & 0 & \cdots \\ \alpha_2 & 0 & \hbar\omega_2 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \quad (29.7)$$

In cases in which the approximately resonantly coupled modes $l \in I$ are highly excited, i.e. $k_l R \gg 1$, the coupling constants α_l are given by

$$\alpha_l = i \langle g | \hat{\mathbf{d}} | e \rangle \cdot \mathbf{u}_l^*(\mathbf{x} = 0) \sqrt{\frac{\hbar\omega_l}{2\epsilon_0}}. \quad (29.8)$$

The matrix (29.7) can be diagonalized by a unitary transformation $\mathcal{U}$, i.e.

$$\hat{H} = \sum_{k \in \{0\} \cup I} \hat{P}_k^\dagger \Lambda_k \hat{P}_k$$

with $\hat{B}_k = \sum_m \mathcal{U}_{km} \hat{P}_m$ and $\sum_{mn} \mathcal{U}_{km}^\dagger h_{mn} \mathcal{U}_{nr} = \Lambda_k \delta_{kr}$. The operators $\hat{P}_k^\dagger$ and $\hat{P}_k$ are the creation and destruction operators of the “quasi particles” which describe the dressing of

the qubit by the radiation field. The eigenvalues Λ_r (dressed energies) are determined by the condition [10]

$$f(\Lambda) \equiv \hbar\bar{\omega}_0 - \Lambda - \sum_{l \in I} \frac{|\alpha_l|^2}{\hbar\omega_l - \Lambda} = 0 \rightarrow \Lambda_r. \quad (29.9)$$

For the elements $\mathcal{U}_{kr}$ of this unitary transformation we obtain the relations

$$\mathcal{U}_{kr} \equiv \mathcal{U}_k(\Lambda_r) = \begin{cases} \left(1 + \sum_{l \in I} \frac{|\alpha_l|^2}{|\hbar\omega_l - \Lambda_r|^2}\right)^{-1/2}, & k = 0 \\ -\alpha_k(\hbar\omega_k - \Lambda_r)^{-1} \mathcal{U}_{0r}, & k \in I \end{cases}. \quad (29.10)$$

As a result of this diagonalization of the Hamiltonian (29.6), the time evolution of any coherent state $|\beta_0, \beta_1, \beta_2, \dots\rangle \equiv |\{\beta_i\}\rangle$ with $\hat{b}_0|\{\beta_i\}\rangle = \beta_0|\{\beta_i\}\rangle$, $\hat{a}_l|\{\beta_i\}\rangle = \beta_l|\{\beta_i\}\rangle$ ($l \in I$; $\beta_0, \beta_l \in \mathbb{C}$) is given by

$$\hat{U}(t)|\{\beta_i\}\rangle = |\{\beta_i(t)\}\rangle \quad \text{with} \quad \beta_i(t) = \sum_{k, m \in \{0\} \cup I} \mathcal{U}_{ik} e^{-i\Lambda_k t/\hbar} (\mathcal{U}^\dagger)_{km} \beta_m,$$

and $\hat{U}(t) \equiv e^{-i\hat{H}t/\hbar}$. Thus, if initially, at $t = 0$, the qubit is prepared in its excited state $|e\rangle$ and no photons are present in the radiation field, the probability $P(t)$ of observing the qubit again in its excited state at a later time t is given by

$$P(t) = |f_0(t)|^2 \quad \text{with} \quad f_0(t) = \sum_{r \in \{0\} \cup I} |\mathcal{U}_{0r}|^2 e^{-i\Lambda_r t/\hbar}. \quad (29.11)$$

In the subsequent discussion we concentrate on cases in which the approximately resonant modes of the spherical cavity are highly excited so that the coupling constants are given by Eq. (29.8). If the radius R of the spherical cavity is very large, many cavity modes are significantly coupled to the qubit. In this case many dressed energies Λ_r contribute to the sum of Eq. (29.11) so that an analysis in terms of dressed states of the interacting system is not very practical. In such cases considerable physical insight can be obtained by a semiclassical path representation [10] of the probability amplitude $f_0(t)$ which applies to the cases in which the relevant cavity modes are highly excited, i.e. $k_l R \gg 1$ with $k_l \approx \omega_0/c$. In such a semiclassical path representation $f_0(t)$ is represented by a sum of probability amplitudes which are associated with repeated returns of the spontaneously emitted photon to the center of the cavity where it interacts repeatedly with the qubit. Assuming that all cavity modes which are significantly coupled to the qubit are highly excited [compare with Eq. (29.5)], Eq. (29.11) can be rewritten in the form

$$\begin{aligned} f_0(t) &= -\frac{1}{2\pi i} \int_{-\infty+i0}^{\infty+i0} d\Lambda e^{-i\Lambda t/\hbar} \sum_{r \in \{0\} \cup I} \frac{|\mathcal{U}_{0r}|^2}{\Lambda - \Lambda_r} \\ &= -\frac{1}{2\pi i} \int_{-\infty+i0}^{\infty+i0} d\Lambda e^{-i\Lambda t/\hbar} \frac{|\mathcal{U}_0(\Lambda)|^2}{f(\Lambda)} \frac{df}{d\Lambda}(\Lambda) \end{aligned} \quad (29.12)$$

with the characteristic function $f(\Lambda)$ of Eq. (29.9) being approximately given by

$$f(\Lambda) \rightarrow \hbar\omega_0 - \Lambda + \hbar \frac{\Gamma}{2} \cot\left(\frac{\Lambda R}{\hbar c}\right). \quad (29.13)$$

Thereby, the summation over all highly excited cavity modes has been performed with the help of contour integration. The parameter

$$\Gamma = \left[\frac{2}{\hbar} |\alpha_l|^2 \frac{R}{\hbar c} \right]_{\hbar\omega_l=\Lambda} \equiv \left[\frac{\omega_l^3}{3\pi\epsilon_0\hbar c^3} |\langle e|\hat{\mathbf{d}}|g\rangle|^2 \right]_{\hbar\omega_l=\Lambda}$$

of Eq. (29.13) is a smooth function of Λ and in the spirit of a Mittag-Leffler expansion [21] all singularities of $f(\Lambda)$ are contained in the cotangent function. For $\Lambda = \hbar\omega_0$, the value of Γ is equal to the spontaneous decay rate which according to Fermi's Golden rule describes the spontaneous decay $|e\rangle \rightarrow |g\rangle$ of the qubit in the infinite cavity limit $R \rightarrow \infty$. In our subsequent treatment we shall assume that Γ is independent of Λ and that it is equal to this spontaneous decay rate. This corresponds to the flat-continuum approximation [22] in the infinite cavity limit. Furthermore, we have incorporated an approximately Λ -independent frequency shift into the renormalized physically observable transition frequency ω_0 of the qubit system. It is assumed that this renormalized transition frequency includes also the radiative corrections of the off-resonant modes ($l \notin I$).

With the help of Eqs. (29.12) and (29.13) $f_0(t)$ can be written in an equivalent form as

$$f_0(t) = e^{-i\omega_0 t - \Gamma t/2} + \frac{\hbar\Gamma}{2\pi} \int_{-\infty+i0}^{\infty+i0} d\Lambda \frac{e^{-i\Lambda t/\hbar} e^{iW(\Lambda)}}{(\Lambda - \hbar\omega_0 + i\hbar\Gamma/2)^2} \sum_{M=1}^{\infty} \left[e^{iW(\Lambda)} \chi(\Lambda) \right]^{M-1} \quad (29.14)$$

or

$$f_0(t) = e^{-i\omega_0 t - \Gamma t/2} + \sum_{M=1}^{\infty} \sum_{r=0}^{M-1} \Theta\left(t - \frac{2R}{c}M\right) \binom{M-1}{r} \times e^{-i(\omega_0 - i\Gamma/2)(t - 2RM/c)} \frac{[-\Gamma(t - 2RM/c)]^{1+r}}{(1+r)!} \quad (29.15)$$

with the Θ -function defined by $\Theta(x) = 1$ for $x \geq 0$ and $\Theta(x) = 0$ for $x < 0$. In the spirit of a Feynman path integral approach [15] $f_0(t)$ is represented as a sum of probability amplitudes which are associated with $M \geq 1$ returns of the spontaneously emitted photon to the center of the spherical cavity. Equations (29.14) and (29.15) correspond to a semiclassical limit of such a Feynman path integral representation as they apply for highly excited cavity modes only. According to the first terms of Eqs. (29.14) and (29.15) the spontaneous emission of a photon is characterized by an exponential decay of the qubit with the spontaneous decay rate Γ . Each time the photon returns to the center of the spherical cavity it interacts again with the qubit. These successive qubit-photon interactions are turned on at multiples of the classical photon return time $T = 2R/c$, and are described by the probability amplitudes of Eqs. (29.14) and (29.15) with $M \geq 1$. Due to the spherical symmetry of the cavity the probability amplitudes of all possible photon paths interfere constructively at the center of the cavity. In spite of this constructive interference the initial-state probability $P(t)$ does not rise again to its initial value of unity at times $t \approx 2R/c$. Physically speaking this is due to the fact that the re-excitation of the qubit takes a time of the order of $1/\Gamma$. However, during this time the qubit can also re-emit this photon again spontaneously. The resulting characteristic time evolution of this

competition between re-excitation and re-emission is described by the first term of the sum of Eq. (29.15) with $M = 1$.

At its subsequent returns to the center of the cavity the photon already contains information about its previous time evolution. In particular, according to Eq. (29.14), each one of the photonic returns contributes to $f_0(t)$ with an additional phase of magnitude

$$W(\Lambda) = \frac{2\Lambda R}{\hbar c}.$$

Moreover, the scattering matrix element

$$\chi(\Lambda) = 1 - \frac{i\hbar\Gamma}{\Lambda - \hbar\omega_0 + i\hbar\Gamma/2} \equiv \frac{\Lambda - \hbar\omega_0 - i\hbar\Gamma/2}{\Lambda - \hbar\omega_0 + i\hbar\Gamma/2}$$

describes scattering of the photon during its returns to the center of the cavity. So, during its first return to the center of the cavity, for example, the photon is either not scattered at all or it is scattered by the qubit due to absorption and subsequent spontaneous emission. These two possibilities manifest themselves in the terms of Eq. (29.15) with $M = 2, r = 0$ and $M = 2, r = 1$, for example. In particular, if the photon was not scattered during its first return the qubit can be excited at the photon's second return already at time $t = 4R/c$. If the photon was scattered during its first return it experiences a time delay thus leading to a corresponding later excitation of the qubit at time $t \approx 4R/c$. The terms of Eq. (29.15) which are associated with higher returns of the photon to the center of the cavity can be interpreted in an analogous manner with M enumerating the number of returns and the index r enumerating the number of previous scattering processes. In particular, the binomial coefficient $\binom{M-1}{r}$ counts the indistinguishable possibilities to scatter r times during $(M - 1)$ previous returns.

According to Eqs. (29.14) and (29.15) the dynamics of the qubit depend significantly on the number of cavity modes which are coupled resonantly to the qubit by the spontaneous energy exchange.

1. *The large cavity limit.* In this case, the number of cavity modes significantly participating in the spontaneous decay process is large, i.e. $\Gamma dn/d\omega_{nL=1} \equiv \Gamma R/(c\pi) \gg 1$. Thus, the spontaneous emission time $1/\Gamma$ is much shorter than the time $T = 2R/c$ required by a photon to travel from the center of the spherical cavity to its boundary and back again. The resulting short interaction times between the qubit and the spontaneously emitted photon imply that the contributions to $f_0(t)$ of subsequent returns of the photon are well separated in time at least for sufficiently small numbers of returns. A typical time dependence of the initial-state probability $P(t)$ for such a case is depicted in Fig. 29.1(a). Apart from the initial approximately exponential decay for times $0 \leq t < T$, one also notices the contributions of $M \geq 1$ repeated returns which lead to an increase of $P(t)$. Nevertheless, for the reasons discussed above, the initial-state probability does not rise again to a value of unity at the first return ($M = 1$) of the spontaneously emitted photon to the center of the cavity. Furthermore, the contribution of the M -th return is split into M distinct peaks which are associated with all possible previous scatterings of the photon at the center of the cavity. According to Eq. (29.15) each of these scatterings leads to a time delay and a resonant phase shift of magnitude π so that these peaks are always separated by zeros of $P(t)$. Eventually, for sufficiently large values of M contributions

of repeated returns overlap in time thus giving rise to a complicated interference pattern of the quantum probability amplitude.

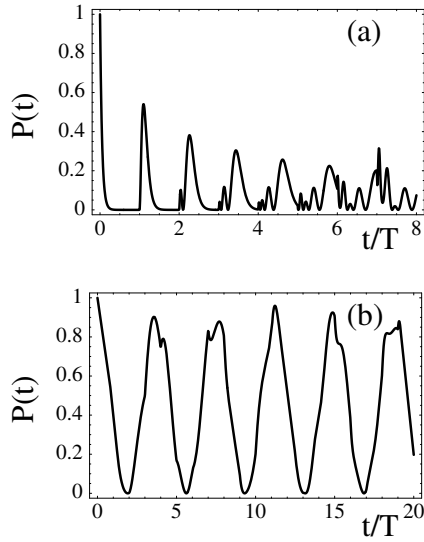


Figure 29.1. Initial-state probability $P(t)$ as a function of time t in units of the photon period $T = 2R/c$ in a spherical metallic cavity of radius R . (c is the speed of light in vacuum.) The spontaneous decay rates (in the infinite cavity limit) are given by $\Gamma = 20/T$ (a) and $\Gamma = 0.75/T$ (b). The transition between the large (a) and small (b) cavity limit is apparent.

2. *The small cavity limit.* In this opposite limit, only one cavity mode is significantly coupled to the qubit, i.e. $\Gamma dn/d\omega_{nL=1} \equiv \Gamma R/(c\pi) \ll 1$. Thus the spontaneous decay time $1/\Gamma$ is much larger than the time $T = 2R/c$ which is required for a photon to travel from the center of the spherical cavity to its boundary and back again. In this case, the contributions of numerous repeated returns in Eq. (29.15) overlap in time and an analysis of the spontaneous decay process in terms of the semiclassical path representations of Eqs. (29.14) and (29.15) is no longer practical. However, a straightforward evaluation of the probability amplitude $f_0(t)$ is still possible in the framework of the dressed-state representation of Eq. (29.11). In fact, there are only two relevant dressed energies, namely $\Lambda_{\pm} = \hbar(\bar{\omega}_0 + \omega_C)/2 \pm \sqrt{\hbar^2(\bar{\omega}_0 - \omega_C)^2/4 + \hbar^2 c\Gamma/(2R)}$, where ω_C denotes the frequency of the almost resonant cavity mode. So, in this limiting case one obtains from Eq. (29.11) the corresponding results of the Jaynes–Cummings–Paul model, i.e.

$$f_0(t) = e^{-i(\bar{\omega}_0 + \omega_C)t/2} \left\{ \frac{\Omega - (\omega_C - \bar{\omega}_0)/2}{2\Omega} e^{-i\Omega t} + \frac{\Omega + (\omega_C - \bar{\omega}_0)/2}{2\Omega} e^{i\Omega t} \right\}$$

with the detuning-dependent vacuum Rabi frequencies $\Omega = \sqrt{(\omega_C - \bar{\omega}_0)^2/4 + c\Gamma/(2R)}$.

29.2 Suppression of Radiative Decay of a Qubit in a Photonic Crystal

In this section, we discuss basic physical aspects of the radiative decay of a single qubit which is embedded in a photonic crystal [23, 24]. Inside a photonic bandgap, the small density of states of the electromagnetic field modes may lead to a significant suppression of spontaneous decay of such a qubit even in the continuum limit. Furthermore, the possibility of forming bound qubit–field states is discussed for which the electromagnetic field is localized around the position of the qubit.

29.2.1 Photonic crystals and associated density of states

Nowadays it is possible to engineer materials in such a way that the possible modes of the electromagnetic field propagating in such a medium exhibit bandgaps in their frequency spectrum. Such materials are referred to as photonic bandgap (PBG) materials, PBG crystals, or photonic crystals (PCs). Typically, the density of states (DOS) of the electromagnetic field inside such a PBG material is singular. The original idea of PCs is due to John and Yablonovitch, who both suggested independently that materials with periodic variation in the dielectric constant could influence the properties of photons in much the same way as semiconductors affect the properties of electrons [14]. In contrast to semiconductors, however, PCs do not exist naturally and therefore need to be fabricated. More precisely, one has to create a periodic lattice of dielectric matter with periodicity on the scale of the wavelengths of light. Typically this dielectric matter involves rods, spheres, slabs, etc. which are sometimes also referred to as “dielectric atoms.” As a result, under appropriate conditions a complete PBG may arise so that for frequencies inside this gap regime electromagnetic wave propagation of any polarization is forbidden in any direction.

It is also possible to create *point defects* in a PC by destroying the periodicity of the lattice of the crystal locally. Such imperfections may involve changes of the dielectric constant (or equivalently of the refractive index) of one of the “dielectric atoms.” Alternatively, they may also arise from a modification of the size or even from the removal of a “dielectric atom” from the lattice of the crystal. By destroying the perfect periodicity such a point defect can then “pull” a mode (or a group of modes) inside an otherwise forbidden bandgap. The resulting photonic state known as *defect mode* is strongly localized and decays exponentially in the bulk, while its frequency and symmetry can be controlled. The crystal surrounding a defect acts as a highly reflecting mirror. Clearly, if losses can be controlled, a high- Q microcavity (with a size of the order of the cubic wavelength of light λ^3) can be obtained. Moreover, this microcavity may operate at optical or even near-infrared wavelengths, where ordinary cavities which are used in typical quantum optical experiments are already very lossy. Alternatively, instead of a point defect one can also introduce *line defects* in an otherwise perfect photonic crystal structure which may act as a “lossless” waveguide. Finally, combining both line and point defects, the creation of channel-drop filters and other components necessary for the construction of all-optical circuits is possible. A thorough and rather readable account of the fabrication and the optical properties of PCs can be found in [25, 26], for example.

Let us now focus on the ability of photonic crystals to suppress the spontaneous emission of photons. The discussion of quantum optical phenomena, such as spontaneous emission, in PCs requires a suitable DOS incorporating all the essential physical features associated with these materials. Neglecting the vectorial nature of electromagnetic waves one may obtain a simple isotropic model where a propagating photon experiences the same periodic potential, irrespective of its polarization or direction of propagation [27, 28]. Thus, the propagation of an electromagnetic wave in such an ideal structure can be described by a scalar one-dimensional wave equation. The dispersion relation of this electromagnetic wave exhibits forbidden gaps and allowed bands. Typically, for frequencies close to the upper band-edge frequency ω_e the dispersion relation can be approximated by the effective-mass dispersion relation i.e., $\omega_k \approx \omega_e + A(k - k_e)^2$, where A is a material-specific constant and k_e is the wave-vector corresponding to ω_e . Accordingly, the isotropic DOS $\rho_I(\omega)$ ($\equiv dn/d\omega$) for frequencies close to ω_e is approximately given by

$$\rho_I(\omega) = \frac{V}{(2\pi)^3} \frac{k_e^2}{2\sqrt{A}} \frac{\Theta(\omega - \omega_e)}{\sqrt{\omega - \omega_e}} \quad (29.16)$$

where $\Theta(\omega - \omega_e)$ is the unit step function indicating that there is a frequency gap below ω_e and V is the volume. In a finite one-dimensional PC, however, the singular behavior of Eq. (29.16) is smoothened [29, 30]. This effect can be incorporated into the isotropic model by an appropriate smoothing parameter in Eq. (29.16) [31, 32].

Band-structure studies have shown that the vectorial nature of electromagnetic waves has to be taken into account in order to achieve good agreement with experiments. Quantum optical phenomena, however, are expected to depend mainly on the local DOS (LDOS), i.e., the DOS in the neighborhood of the relevant embedded qubit, rather than on the global DOS. Furthermore, according to band-structure calculations, even if a PC does not possess a complete PBG, its LDOS may exhibit pseudogaps as well as Van-Hove singularities for which an isotropic DOS is a good local approximation [33, 34]. Finally, it is worth noting that a highly peaked behavior analogous to that of Eq. (29.16) appears also in an ideal waveguide close to its fundamental frequency [13].

Besides the isotropic model, also an anisotropic one has been proposed [28] which preserves the vectorial nature of electromagnetic waves. The corresponding dispersion relation close to the upper band-edge frequency is of the form $\omega_k = \omega_e + A(\mathbf{k} - \mathbf{k}_e)^2$, while the associated DOS differs from Eq. (29.16) as the square-root factor now appears in the numerator instead of the denominator, i.e. $\rho_A(\omega) \sim \sqrt{\omega - \omega_e} \Theta(\omega - \omega_e)$. Although the anisotropic model is closer to realistic three-dimensional PCs, it is mainly the isotropic DOS of Eq. (29.16) which has been used in quantum-optical problems so far.

What should be kept in mind is that both isotropic and anisotropic models are valid for frequencies around the band-edge and for relatively large gaps. This is apparent from the fact that none of these models exhibits the correct behavior for relatively large frequencies i.e., none of them approaches the open-space value for $\omega \gg \omega_e$. Moreover, in a realistic PBG material the gap does not necessarily mean a true zero but a range of frequencies over which the DOS is several orders of magnitude smaller than that of open space. The essential point therefore is that, an appropriate model of DOS for the description of a PBG continuum must exhibit a dip over a range of frequencies and also it has to tend to the open-space DOS as

the frequency becomes much larger or much smaller than the midgap frequency. A rather simple model of such a DOS is an inverted Lorentzian of higher order (p), such as given by the expression

$$\rho_L(\omega) = \rho_o(\omega) \left[1 - \frac{\mathcal{K}^p}{(\omega - \omega_c)^p + \mathcal{K}^p} \right], \quad (29.17)$$

where ω_c is the midgap frequency, $\mathcal{K}$ is the width of the gap and $\rho_o(\omega)$ denotes the open-space DOS which is a smooth function of ω [32, 35–38].

29.2.2 “Photon + atom” bound states

Let us consider an initially excited qubit which is placed in a material exhibiting gaps in the spectrum of the electromagnetic field it supports [31, 39, 40]. Such a qubit may be realized by an atom which is placed inside a PC or by an appropriate “dielectric atom,” for example. Clearly, for transition frequencies of this qubit around the band edge of the PC, i.e. ($\omega_0 \sim \omega_e$), for both isotropic and anisotropic models we have an unconventional DOS which is not a smoothly varying function of frequency. In fact, the Fourier transforms (memory kernels) of the isotropic and anisotropic DOS, i.e. $G_{I(A)}(\tau) = \int_{-\infty+i0}^{\infty+i0} d\omega \rho_{I(A)}(\omega) \exp[-i\omega\tau]$, reflect long-range correlations in time of the form $G_I(\tau) \sim \tau^{-1/2}$ and $G_A(\tau) \sim \tau^{-3/2}$ for $\tau > 0$, respectively [41].

For the sake of illustration let us focus on the spontaneous emission by such a qubit embedded in a PC which can be described by the isotropic model. In terms of the resolvent operator of this system, i.e. $\mathcal{G}(z) = \int_0^{\infty+i0} dt \exp(izt) \hat{U}(t)$, the probability amplitude $\mathcal{A}_e(t) \equiv \langle e | \hat{U}(t) | e \rangle$ of observing the qubit at time t after its preparation in its excited state (and the electromagnetic field in its ground state again) is determined by the matrix element [39]

$$\mathcal{G}_{ee}(z) = \frac{\sqrt{z - \omega_e}}{(z - \omega_0) \sqrt{z - \omega_e} + iC}. \quad (29.18)$$

The constant C represents the strength of the coupling between the qubit and the continuum of field modes of the electromagnetic field. For the isotropic model it is given by

$$C = \frac{|\langle e | \hat{\mathbf{d}} | g \rangle|^2 k_e^2 \omega_e}{12\pi\epsilon_0 \sqrt{A}}.$$

One can easily verify that the expression for $\mathcal{G}_{ee}(z)$ has three poles. Whether they are complex- or real-valued will be determined by the detuning $\delta = \omega_0 - \omega_e$. In general, the poles with positive imaginary parts fall outside the contour of integration which is relevant for determining the time evolution of the system. Poles with negative imaginary parts describe the irreversible spontaneous decay of the qubit and purely real-valued poles are responsible for asymptotic long-time oscillations of the probability amplitude $\mathcal{A}_e(t)$. These latter oscillations may be associated with stable bound states of the atom–field system within the PC.

In Fig. 29.2, the time evolution of the atomic population $|\mathcal{A}_e(t)|^2$ is depicted for the isotropic model and for various detunings $\delta = \omega_0 - \omega_e$ of the transition frequency of the qubit ω_0 from the band-edge frequency ω_e . As expected for transition frequencies well inside the

bandgap, i.e. $\delta = -10C^{2/3} \ll 0$, the qubit remains in the excited state forever. The periodically modulated dielectric host prevents the energy exchange between the qubit and the modes of the electromagnetic field inside the PC. Thus a significant part of the spontaneously emitted radiation remains localized close to the position of the qubit. Typically, such localized photonic states may extend over many wavelengths around the qubit [28]. As a result of the strong interaction between the atom and its own localized radiation the population $|\mathcal{A}_e(t)|^2$ exhibits oscillations for $\delta < 0$, while in the long-time limit we have the formation of a “*photon + atom*” *bound state*. This bound state consists of an excited-state and a ground-state component of the qubit and of an electromagnetic field component which cannot propagate in the PC. The possibility of formation of such “photon + atom” bound states in PCs has already been predicted in the early 1970s by Bykov [42]. For transition frequencies sufficiently outside the bandgap, i.e. $\delta = 10C^{2/3} \gg 0$, the dynamics of the coupling to the electromagnetic field is governed by an exponential decay of the initially excited qubit. However, the decay rate Γ depends on the detuning from the band edge, i.e. $\Gamma \sim C/\sqrt{\delta}$. This is due to the fact that the isotropic DOS does not approach its open-space value even for detunings $\delta \gg 0$.

In the language of dressed states, the coupling of the atom to the strongly modified radiation reservoir causes a strong vacuum Rabi splitting which is reflected by the vacuum Rabi oscillations in the atomic populations. One of the two components of the doublet created by the splitting is pushed inside the gap, where it is protected against spontaneous decay, while the other one is pushed outside where it decays. Depending on the magnitude and the sign of δ , the relative magnitude of the two components changes. This relative magnitude determines which fraction of the initial excitation remains trapped at the position of the qubit in the long-time limit.

As depicted in Fig. 29.2, in the isotropic model the qubit exhibits a nonzero steady-state population even for moderate positive detunings. This, however, is an artifact originating from the divergence of the isotropic DOS as described in Eq. (29.16). For the anisotropic model and for the DOS of Eq. (29.17) the component of the doublet outside the bandgap decays much faster. Thus, even for small positive detunings the “photon + atom” bound state decays and the asymptotic oscillations in the population are not so pronounced. In general, the dynamics of a qubit coupled to a PBG continuum depend mainly on the width of the gap (as compared with the atomic linewidth) as well as on the “band-edge” behavior of the continuum. In addition, they slightly depend on the particular profile of the DOS one may adopt (see, for instance, Fig. 29.3).

Finally, in contrast to the decay rate, the Lamb shift of an atom which is embedded in a PC is not affected by the unconventional radiation reservoirs significantly [43]. This is due to the fact that the Lamb shift originates from virtual photons of all frequencies up to an effective cut off of the order of the rest mass energy of an electron [18]. Compared to this huge frequency regime, a PC modifies the spectrum of the electromagnetic field in a small frequency interval only.

29.2.3 Beyond the two-level approximation

Besides single-photon spontaneous emission also other quantum optical phenomena involving collections of two-level systems and few-level systems have been addressed in the context of PBG continua. For an extensive review see [23], for example. In general, as long as the

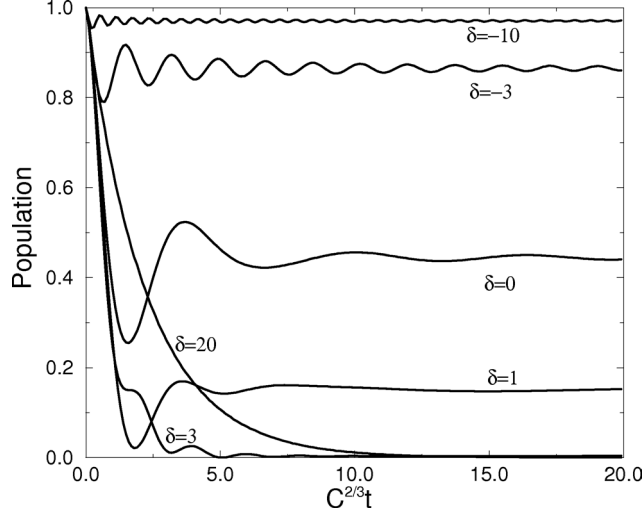


Figure 29.2. Spontaneous decay of an initially excited qubit embedded in a PC (isotropic model of DOS): The time evolution of the population of the excited state of the qubit is plotted for various detunings $\delta \equiv \omega_0 - \omega_e$ of the transition frequency of the qubit from the band-edge frequency. All the detunings are in units of $C^{2/3}$.

problem under consideration involves the exchange of a single photon between the embedded system and the PC-continuum, it can be handled in a straightforward way by direct solution of the appropriate time-dependent Schrödinger equation. Nevertheless, the direct extension of this approach to situations involving more than one photon in a PBG continuum of an arbitrary DOS does not seem tractable. On the other hand, in view of the non-smooth frequency dependences of typical DOS standard tools of quantum optics, such as Markovian master equations and quantum Monte Carlo wavefunctions, are not able to describe the essential physical effects involved. The description of such cases has been attracting increasing interest recently as problems of this kind keep emerging also in other branches of physics. As a result a number of new techniques applicable to strongly interacting dissipative systems have been developed during the last years [36, 44–48].

29.2.4 Exercises

1. *Hamiltonian diagonalization.* Diagonalize the Hamiltonian for spontaneous emission (29.6). In particular show that the elements of the related unitary transformation are given by Eq. (29.10), whereas the dressed energies are determined by Eq. (29.9).
2. *Excitation probability.* Show that the probability for an initially ($t = 0$) excited qubit to be excited also at time t is given by (29.11). Assuming that the cavity modes significantly coupled to the qubit are highly excited, derive Eq. (29.12). Finally, derive Eqs. (29.14) and (29.15) from Eq. (29.12).

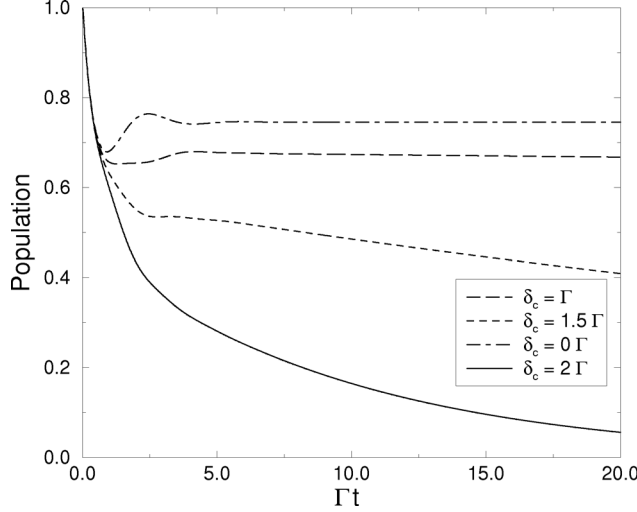


Figure 29.3. Spontaneous decay of an initially excited qubit embedded in a PC (inverted-Lorentzian profile of DOS for $p = 8$ and $\mathcal{K} = 2\Gamma$): The time evolution of the population of the excited state of the qubit is plotted for various detunings $\delta_c \equiv \omega_0 - \omega_c$ of the transition frequency of the qubit from the midgap frequency.

3. *Resolvent operator.* The resolvent of a Hamiltonian $\hat{H}$ is defined by $\mathcal{G}(z) = (z - \hat{H})^{-1}$. Consider a system with a total Hamiltonian $\hat{H} = \hat{H}_0 + \hat{V}$, where $\hat{H}_0$ and $\hat{V}$ are the unperturbed part and the interaction, respectively. Let also $\mathcal{S} \equiv \{|a\rangle, |b\rangle, |c\rangle, \dots\}$ be the set of eigenstates of $\hat{H}_0$ with respective energies $\omega_a, \omega_b, \omega_c, \dots$, in units with $\hbar = 1$. Show that, if initially the system is in state $|a\rangle$, the matrix elements $\mathcal{G}_{aa}$ and $\mathcal{G}_{ab}$ are determined by

$$(z - \omega_a)\mathcal{G}_{aa} = 1 + \sum_{j \in \mathcal{S}} \hat{V}_{aj}\mathcal{G}_{ja},$$

$$(z - \omega_b)\mathcal{G}_{ba} = \sum_{j \in \mathcal{S}} \hat{V}_{bj}\mathcal{G}_{ja}.$$

4. *Spontaneous emission in the resolvent-operator formalism.* Let $\hat{H}$ be given by Eq. (29.6) and $|a\rangle = |e\rangle \otimes |\{0\}\rangle$, $|b\rangle = |g\rangle \otimes |1_l\rangle$ with respective energies $\omega_a = \omega_0$, $\omega_b = \omega_l$. Thereby, l is an index running over all the field modes and $|1_l\rangle$ denotes an one-photon state. Show that

$$\mathcal{G}_{aa} = \left(z - \omega_0 - \sum_l \frac{|\alpha_l|^2}{z - \omega_l} \right)^{-1}.$$

Starting from this equation, derive Eq. (29.18), using the density of states (29.16).

References

- [1] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, Cambridge, 1995.
- [2] E. A. Power, *Introductory Quantum Electrodynamics*, American Elsevier, New York, 1964.
- [3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
- [4] H. Mabuchi and P. Zoller, Phys. Rev. Lett., **76** (1996) 3108.
- [5] G. Alber, Th. Beth, Ch. Charnes, A. Delgado, M. Grassl, and M. Mussinger, Phys. Rev. Lett., **86** (2001) 4402; G. Alber, Th. Beth, Ch. Charnes, A. Delgado, M. Grassl, and M. Mussinger, Phys. Rev. A, **68** (2003) 012316.
- [6] E. T. Jaynes and F. W. Cummings, Proc. IEEE, **51** (1963) 89; H. Paul, Ann. Phys. (Leipzig), **11** (1963) 411.
- [7] W. P. Schleich, *Quantum Optics in Phase Space*, Wiley-VCH, Weinheim, 2001.
- [8] Some early references dealing with the radiative coupling between atoms and a finite number of cavity modes are
E. P. Wigner, Z. Phys., **63** (1930) 54; J. Hamilton, Proc. Phys. Soc. London, **59** (1947) 917; S. Swain, J. Phys. A: Math. Gen. **5** (1972) 1592; M. Bixon, J. Jortner, and Y. Dothan, Mol. Phys., **17** (1969) 109; P. Milonni, J. R. Ackerhalt, H. W. Gailbraith, and M. L. Shih, Phys. Rev. A, **28** (1983) 32.
- [9] J. Parker and C. R. Stroud, Phys. Rev. A, **35** (1987) 4226.
- [10] G. Alber, Phys. Rev. A, **46** (1991) R5338.
- [11] H. Gießen, J. D. Berger, G. Mohs, and P. Meystre, Phys. Rev. A, **53** (1996) 2816.
- [12] H. J. Carmichael, *Statistical Methods in Quantum Optics*, Springer, Berlin, 2003.
- [13] see, e.g., E. M. Purcell, Phys. Rev., **69** (1946) 681; J. Kleppner, Phys. Rev. Lett., **47** (1981), 233.
- [14] S. John, Phys. Rev. Lett., **58** (1987) 2486; E. Yablonovitch, Phys. Rev. Lett., **58** (1987) 2059.
- [15] L. S. Schulman, *Techniques and Applications of Path Integration*, Wiley, New York, 1996; C. Grosche and F. Steiner, *Handbook of Feynman Path Integrals*, Springer, Berlin, 1998.
- [16] H. Bethe, Phys. Rev., **72** (1947) 339.
- [17] C. Itzykson and J. B. Zuber, *Quantum Field Theory*, McGraw-Hill, New York, 1966.
- [18] For a consistent theoretical treatment of the Lamb shift within the framework of nonrelativistic quantum electrodynamics without the introduction of an ad-hoc energy cut-off for the field modes, see e.g., C.-K. Au and G. Feinberg, Phys. Rev. A, **9** (1974) 1794; J. Seke, Physica A, **187** (1992) 625; J. Seke, Physica A, **196** (1993) 441; J. Seke, Physica A, **203** (1994) 284.
- [19] L. C. Biedenharn and J. D. Louck, *Angular Momentum in Quantum Physics—Theory and Applications*, Addison-Wesley, Reading, MA, 1981.
- [20] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions*, Natl. Bur. Stand. Appl. Math. Ser. No. **55**, USGPO, Washington, DC, 1964.

- [21] G. B. Arfken and H. J. Weber, *Mathematical Methods for Physicists*, Academic Press, San Diego, 2001.
- [22] C. Chohen-Tannoudji, B. Diu, and F. Laloe, *Quantum Mechanics*, Wiley, New York, 1977.
- [23] P. Lambropoulos, G. M. Nikolopoulos, T. R. Nielsen, and S. Bay, Rep. Prog. Phys., **63** (2000) 455.
- [24] D. G. Angelakis, P. L. Knight, and E. Paspalakis, Contemp. Phys., **45** (2004) 303.
- [25] J. D. Joannopoulos, *Photonic Crystals: Molding the Flow of Light*, Princeton University Press, Princeton, 1995.
- [26] K. Sakoda, *Optical Properties of Photonic Crystals*, Springer, Berlin, 2001.
- [27] S. John and J. Wang, Phys. Rev. Lett., **64** (1990) 2418–2421.
- [28] S. John and J. Wang, Phys. Rev. B, **43** (1991) 127772.
- [29] I. S. Fogel, J. M. Bendickson, M. D. Tocci, M. J. Bloemer, M. Scalora, C. M. Bowden, and J. P. Dowling, Pure Appl. Opt., **7** (1998) 393.
- [30] J. M. Bendickson, J. P. Dowling, and M. Scalora, Phys. Rev. E, **53** (1996) 4107.
- [31] A. G. Kofman, G. Kurizki, and B. Sherman, J. Mod. Opt., **41** (1994) 353.
- [32] M. Lewenstein, J. Zakrezewski, and T. W. Mossberg, Phys. Rev. A, **38** (1988) 808.
- [33] K. Busch and S. John, Phys. Rev. E, **58** (1998) 3869.
- [34] R. Sprik, B. A. van Tiggelen, and A. Lagendijk, Europhys. Lett., **35** (1996) 265.
- [35] S. Bay, P. Lambropoulos, and K. Molmer, Phys. Rev. A, **57** (1998) 3065.
- [36] B. M. Garraway, Phys. Rev. A, **55** (1997) 2290.
- [37] R. F. Nabiev, P. Yeh, and J. J. Sanchez-Mondragon, Phys. Rev. A, **47** (1993) 3380.
- [38] G. M. Nikolopoulos, and P. Lambropoulos, Phys. Rev. A, **61** (2000) 053812.
- [39] S. Bay, P. Lambropoulos, and K. Molmer, Phys. Rev. A, **55** (1997) 1485.
- [40] S. John and T. Quang, Phys. Rev. A, **50** (1994) 1764.
- [41] N. Vats and S. John, Phys. Rev. A, **58** (1998) 4168.
- [42] V. P. Bykov, Sov. Phys. JETP, **35** (1999) 269.
- [43] Z. Y. Li and Y. Xia, Phys. Rev. B, **63** (2001) 121305.
- [44] A. Imamoglu, Phys. Rev. A, **50** (1994) 3650.
- [45] G. M. Nikolopoulos and P. Lambropoulos, Phys. Rev. A, **60** (1999) 5079.
- [46] H. P. Breuer, B. Kappler, and F. Petruccione, Phys. Rev. A, **59** (1999) 1633.
- [47] M. W. Jack, M. J. Collet, and D. F. Walls, J. Opt. B, **1** (1999) 452.
- [48] W. T. Strunz, L. Diosi, and N. Gisin, Phys. Rev. Lett., **82** (1999) 1801.

Part VIII

Towards Quantum Technology Applications

30 Quantum Interferometry

Oliver Glöckl, Ulrik L. Andersen, and Gerd Leuchs

30.1 Introduction

The concept of quantum interference is one of the most basic foundations of quantum physics and appears in many areas. It for example demonstrates the wave nature of massive particles more than anything else. Young's double slit experiment with electrons and electron diffraction on a crystal surface by Davisson and Germer [1] have been first experimental proofs. Recently, similar diffraction was observed even for much larger particles [2]. The impact of quantum physics on light experiments is associated with the quantization of the field where the energy of a light mode is quantized to be multiples of a basic unit, the photon energy. For light, quantum effects become apparent, for e.g., when performing experiments with single photons. The Hong–Ou–Mandel interference [3] is a striking example where two photons simultaneously impinging on a beam splitter one each in the two input ports, will never result in one photon at each of the two output ports. In general one can say that it is the field statistics, i.e. the higher moments of observables, which are modified or even dominated by quantum effects. The field statistics is crucial for understanding the basic sensitivity limitation of interferometers [4] even when operating at high intensity levels.

It was only in 1980 that Caves established a link between Heisenberg's position and momentum uncertainty of an interferometer mirror mass, the photon counting statistics and the light pressure uncertainty caused by the light incident on the interferometer mirrors [5]. Shortly after this, Loudon provided a qualitative analysis using the higher moments of the field quadratures [6]. According to this approach, the best sensitivity is reached for an operating light power for which the contributions of the photon counting statistics and the light pressure uncertainty lead to an overall minimum of the variance (2nd moment) of the amplitude quadrature. Yuen, however, showed [7] that for any pair of conjugate variables such as momentum and position such considerations hold only if the uncertainties of these variable are not correlated. In a lecture at a summer school in 1981 in the franconian town Bad Windsheim Unruh [8] argued that correlating the two stochastic contributions to the output amplitude variance would make the standard quantum limit obsolete. His work went largely unnoticed until the matter was picked up again by Jaekel and Reynaud [9] and Luis and Sanchez-Soto [10]. The sensitivity enhancement is achieved by providing nonclassical light such as appropriately squeezed light at the interferometer input. By now, by-passing the standard quantum limit is well established in the plans for improving the sensitivity of large scale laser interferometers for gravitational wave detection [11]. Another interesting development in this context is

that the interferometer itself modifies the photon statistics of the light passing through. This is called ponderomotive squeezing [12] and relies on the formal mathematical equivalence between a Kerr medium and the response of the interferometer to the light pressure on its mirrors.

In this lecture we will discuss in more detail the operation of an interferometer with intense and nonclassical light. A pictorial approach will be used as well as a mathematical description.

30.2 The Interferometer

Probably the most famous two-beam interferometer is the Mach–Zehnder interferometer, depicted in Fig. 30.1. A beam is divided into two different spatial paths using a beam splitter. The beams run through different arms of the interferometer and finally recombine at a second beam splitter. The interferometer is thus a four-port device since fields can enter through two different ports of the first beam splitter and leave through two different ports of the second beam splitter. Relative phase changes between the two optical paths in the interferometer can be extracted by measuring the intensity in one or in both of the output ports. To realize that this is indeed the case, suppose a coherent light beam enters the interferometer. If the two paths have exactly equal lengths, the interference at the second beam splitter creates a dark and a bright output, that is all photons leave one output only. A relative phase change, however, results in a division of the photons among the two output, the exact fraction being related to the relative phase shift in the interferometer. Therefore by measuring the intensity in the two-output ports knowledge about the relative phase can be gained. However, this phase estimation process will inevitably be influenced by some noise which in turn gives rise to a statistical error. The precision by which the interferometer phase can be estimated depends on the states injected into the first beam splitter ($|\psi\rangle_1$ and $|\psi\rangle_2$ in Fig. 30.1) and the measurement strategy used to detect the phase changes.

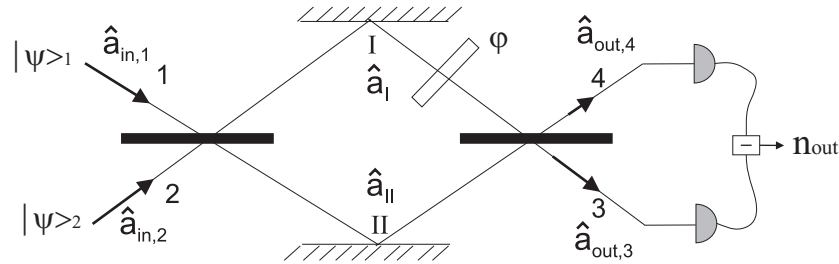


Figure 30.1. Schematic diagram of a Mach–Zehnder interferometer.

The two-beam splitters are the working horses of the interferometer. The beam splitter has two input and two output ports, each port being associated with a mode of the quantized electromagnetic field. If we denote these field operators as $\hat{a}_{in1}$, $\hat{a}_{in2}$, $\hat{a}_{out1}$, and $\hat{a}_{out2}$, the input–output relations for a beam splitter are

$$\hat{a}_{out1} = t\hat{a}_{in1} + ir\hat{a}_{in2} \quad (30.1)$$

$$\hat{a}_{out2} = ir\hat{a}_{in1} + t\hat{a}_{in2} \quad (30.2)$$

where the transmission and reflection coefficients t and r are real values and the complex i 's are included to satisfy the commutation relation for the various fields involved [13, 14]. A particular important beam splitter for interferometry is the one which splits a beam into equal portions, namely the 50/50 beam splitter with $t = r = 1/\sqrt{2}$. Let us now address the sensitivity of interferometers.

30.2.1 Sensitivity

Heisenbergs uncertainty relation for the phase and photon number is

$$\Delta\phi\Delta n \geq 1, \quad (30.3)$$

where $\Delta\phi$ and Δn are the standard deviations of the noise for the phase and the photon number, respectively. For shot-noise limited light where $\Delta n = \sqrt{\langle n \rangle}$ the optimum phase resolution is

$$\Delta\phi = \frac{1}{\sqrt{\langle n \rangle}}. \quad (30.4)$$

From this expression, it is clear that with an unlimited amount of energy, we can obtain phase measurements with an arbitrary accuracy, since by increasing the power the phase resolution becomes smaller. In practice, however, the amount of energy is finite and a certain resolution limit will be attained. Furthermore at very high powers, radiation pressure on the interferometer mirrors and heating induced effects add additional noise which eventually will limit the overall performance of the interferometer. Therefore, the following analysis of the resolution of interferometers will be made under the power constraint assumption, i.e. only a limited amount of photons is available. But can we still improve the sensitivity with this power constraint? The answer is “yes,” the above limit can indeed be surpassed. Quantum mechanics does not put any restriction on further improvements, and it has been found that the ultimate precision in phase measurements is the so-called Heisenberg limit [15], given by

$$\Delta\phi = \frac{1}{\langle n \rangle}. \quad (30.5)$$

This is a great improvement, since the number of photons needed to achieve the same sensitivity as the shot-noise limited interferometers is greatly reduced. As we will show in the following sections, this limit can in principle be reached by using manifestly nonclassical states of the light field.

To compute the sensitivity of an interferometer in a given setting, a careful quantum mechanical analysis of the interferometer must be carried out. The sensitivity of the Mach–Zehnder interferometer depends basically on two things—the prepared input states and the measurement strategy. In this chapter, we consider the measurement strategy outlined above (where the intensity difference of the outputs is measured) while considering various input states. We begin the analysis by deriving a simple input–output relation for the Mach–Zehnder interferometer in the Heisenberg picture. Two arbitrary modes $\hat{a}_{1,\text{in}}$ and $\hat{a}_{2,\text{in}}$, enter via the two input ports of the first beam splitter, the modes interfere at the 50:50 beam splitter and the

corresponding output modes are given by

$$\hat{a}_I = \frac{1}{\sqrt{2}}(i\hat{a}_{1,\text{in}} + \hat{a}_{2,\text{in}}e^{i\theta}), \quad (30.6)$$

$$\hat{a}_{II} = \frac{1}{\sqrt{2}}(\hat{a}_{1,\text{in}} + i\hat{a}_{2,\text{in}}e^{i\theta}). \quad (30.7)$$

We allow for an arbitrary phase shift θ between the two input modes. After the introduction of a relative phase shift of φ , both modes interfere at a second beam splitter. To simplify the resulting expression, we consider a phase shift in both arms equal to $\varphi/2$ but with opposite signs yielding the overall phase shift φ :

$$\hat{a}_{\text{out},3} = \frac{1}{\sqrt{2}}(\hat{a}_I e^{-i\varphi/2} + i\hat{a}_{II} e^{i\varphi/2}), \quad (30.8)$$

$$\hat{a}_{\text{out},4} = \frac{1}{\sqrt{2}}(i\hat{a}_I e^{-i\varphi/2} + \hat{a}_{II} e^{i\varphi/2}). \quad (30.9)$$

Rewriting these expressions in terms of the input states by inserting (30.6) and (30.7) in (30.8) and (30.9), we find, up to some global phase factor, the general input–output relation of a Mach–Zehnder interferometer

$$\hat{a}_{\text{out},3} = a_{1,\text{in}} \cos(\varphi/2) - a_{2,\text{in}} e^{i\theta} \sin(\varphi/2), \quad (30.10)$$

$$\hat{a}_{\text{out},4} = a_{1,\text{in}} \sin(\varphi/2) + a_{2,\text{in}} e^{i\theta} \cos(\varphi/2). \quad (30.11)$$

It is interesting to note that these two input–output relations are similar to the beam splitter equations in which the beam splitting ratio is controlled by the relative phase change between the two optical paths in the interferometer. These simplified equations make the analysis simple and the effect on changing the input states can easily be computed.

Information about the phase change is now extracted by detecting the intensities of the output beams, $\hat{n}_3 = \hat{a}_{\text{out},3}^\dagger \hat{a}_{\text{out},3}$ and $\hat{n}_4 = \hat{a}_{\text{out},4}^\dagger \hat{a}_{\text{out},4}$, and subsequently generating the difference of the photocurrents:

$$\begin{aligned} \hat{n}_{\text{out}} &= \hat{a}_{\text{out},3}^\dagger \hat{a}_{\text{out},3} - \hat{a}_{\text{out},4}^\dagger \hat{a}_{\text{out},4} \\ &= (\hat{a}_{\text{in},1}^\dagger \hat{a}_{\text{in},1} - \hat{a}_{\text{in},2}^\dagger \hat{a}_{\text{in},2}) \cos \varphi - (\hat{a}_{\text{in},1}^\dagger \hat{a}_{\text{in},2} e^{i\theta} + \hat{a}_{\text{in},1} \hat{a}_{\text{in},2}^\dagger e^{-i\theta}) \sin \varphi. \end{aligned} \quad (30.12)$$

The noise variance that is associated with measurements of the difference signal is calculated as follows:

$$(\Delta n_{\text{out}})^2 = \langle \hat{n}_{\text{out}}^2 \rangle - \langle \hat{n}_{\text{out}} \rangle^2, \quad (30.13)$$

where $\langle \rangle$ indicates the quantum-mechanical expectation value taken over the two input states $|\psi\rangle_1 |\psi\rangle_2$. Operators with index “1” act only on mode $|\rangle_1$, those with index “2” on $|\rangle_2$.

The accuracy of the phase measurements can then be estimated using the calculus of error propagation:

$$\delta\phi = \frac{\Delta n_{\text{out}}}{\partial \langle \hat{n} \rangle / \partial \varphi} = \frac{\sqrt{\langle \hat{n}_{\text{out}}^2 \rangle - \langle \hat{n}_{\text{out}} \rangle^2}}{\partial \langle \hat{n} \rangle / \partial \varphi}. \quad (30.14)$$

Inserting (30.12) in (30.14) we find the statistical error in estimating a phase change when using the above-mentioned measurement strategy and employing two arbitrary input states, $|\psi\rangle_1$ and $|\psi\rangle_2$.

30.3 Interferometer with Coherent States of Light

The first scenario that we will consider is when a coherent state enters through one input port and a vacuum state enters through the other input port. In this simple case, the expectation values have to be taken over these two states. For the standard deviation we find

$$\Delta n_{\text{out}} = \sqrt{{}_1\langle\alpha|{}_2\langle 0|\hat{n}_{\text{out}}^2|0\rangle_2|\alpha\rangle_1 - ({}_1\langle\alpha|{}_2\langle 0|\hat{n}_{\text{out}}|0\rangle_2|\alpha\rangle_1)^2} \quad (30.15)$$

$$= |\alpha|, \quad (30.16)$$

and the partial derivative of the mean photon number is

$$\frac{\partial\langle\hat{n}\rangle}{\partial\phi} = |\alpha|^2. \quad (30.17)$$

The phase resolution is thus

$$\Delta\varphi_{\text{class}} = 1/\sqrt{n} \quad (30.18)$$

as expected for a coherent input state.

30.3.1 Geometrical visualization

We now introduce a pictorial description of the propagation of noise in an interferometer. Such a visualization tool is helpful in understanding the various noise transforming mechanisms inside an interferometer [16], and it has also been shown to facilitate the understanding of the generation of intense quantum entangled light beams [17]. For a general introduction, see e.g., Leuchs [18]. We closely follow the description presented in [19].

In quantum optics, the field operator of a mode can be written as a superposition of a classical mean field and an operator describing the field uncertainty,

$$\hat{a} = \alpha + \delta\hat{a}, \quad (30.19)$$

with $\langle\delta\hat{a}\rangle = 0$. The state is best visualized in a phase space diagram (see Fig. 30.2). The classical amplitude of the field is represented by the “stick” α , the optical phase is given by its orientation in phase space φ . Hence, in this diagram the imaginary part of the field is plotted versus the real part. The fluctuations $\delta\hat{a}$ lead to a region of uncertainty which can be considered as the contour of the Wigner function [20]. For a field in a coherent state, the uncertainties in amplitude and phase direction are the same and the contour is circular as shown in Fig. 30.2. The noise that contributes to signals in direct detection corresponds to the projection of the noise arrows onto the direction along the classical excitation. In the figure, this corresponds to the arrow $\delta\bar{a}$, which represents the amplitude fluctuations, while the perpendicular arrow $\delta\bar{b}$ represents the phase noise.

These two arrows, which describe stochastic variables, span the circular region of uncertainty of the field. For the coherent state there will be no correlation between the two stochastic variables. The action of a beam splitter will be to transfer each arrow from an input port to both output ports with reduced amplitudes. In the model, we have to properly take into account the beam splitter relations. If the same stochastically varying input arrow contributes to two output ports one may expect correlations between these two partial output fields.

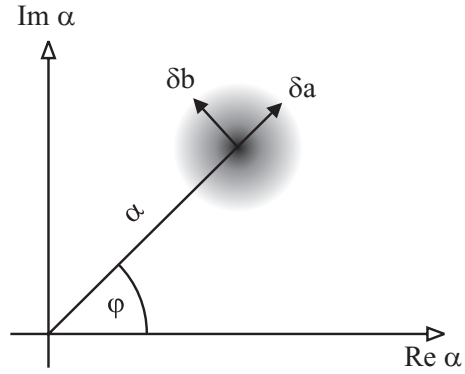


Figure 30.2. Phase diagram representing a light field.

Let us now use this pictorial approach to understand the function of the interferometer. A coherent state enters through one input port and the other input mode is not excited and, therefore, in a vacuum state (Fig. 30.3). Coherent and vacuum states have a circular region of uncertainty in phase space and as a result all four stochastic arrows describing the two coherent states have the same variance.

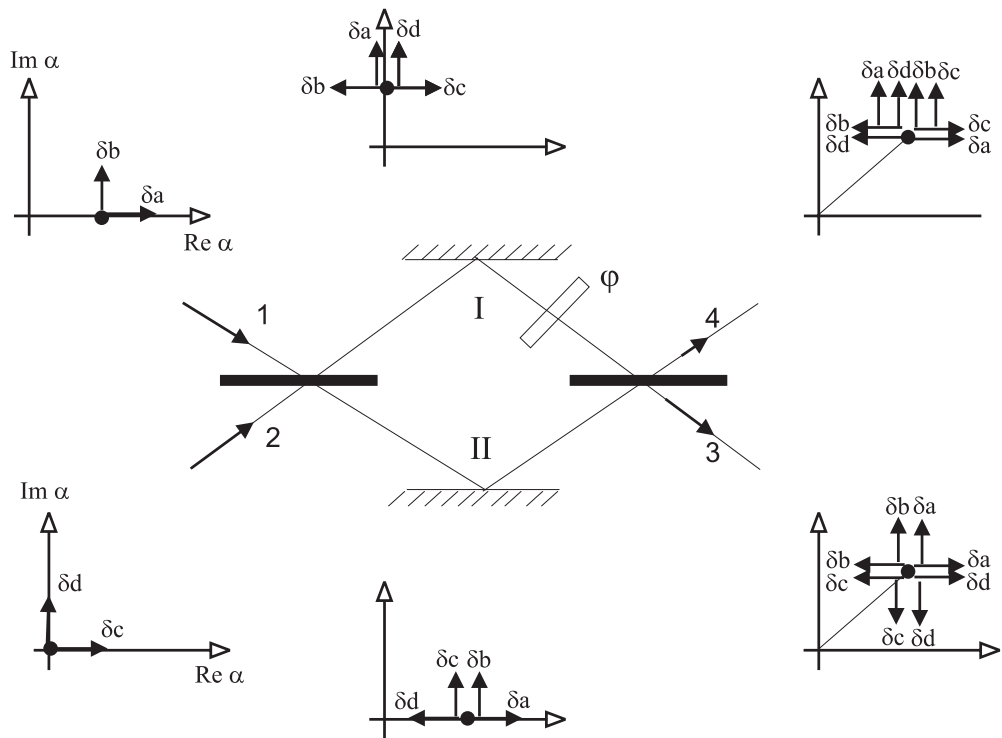


Figure 30.3. An interferometer with a coherent and a vacuum input state.

The beam splitter relations are obeyed by associating a 90° phase shift with each reflection, i.e. the factor i , and 0° phase shift to each transmission. The amplitude reduction is not shown, for simplicity. The four input arrows δa , δb , δc , and δd determine the field uncertainties in the two output ports I and II right after the first beam splitter. The amplitude uncertainty in output I is determined by the projections of all arrows onto the amplitude direction: $\delta a + \delta d$. Each arrow would then still have to be multiplied with its individual stochastic coefficient. Likewise the amplitude uncertainty at output II is determined by $\delta a - \delta d$.

Before going to the second beam splitter we now introduce a $-\pi/2$ phase shift (i.e. 90° clockwise). This is done, e.g., by introducing a path length difference between the two arms. It ensures that both output ports are at half fringe height, i.e., that they are equally intense. At the outputs 3 and 4, again following the rules introduced above, we now have altogether eight arrows. Two arrows marked with the same letter derive from one and the same stochastic input variable so they can be added vectorially. As can be seen in Fig. 30.3, arrows δa contribute to correlated amplitude uncertainties in the two outputs 3 and 4, arrows δb to correlated phase, arrows δc to anticorrelated amplitude, and arrows δd to anticorrelated phase uncertainties. Another way to say this is that the amplitudes in output ports 3 and 4 are given by $\delta a + \delta c$ and $\delta a - \delta c$ respectively. Although the uncertainties in both output ports are governed by the same four arrows they are not correlated. The reason for this lack of correlation can be traced back to the sum of two statistically independent stochastic variables and their difference being again statistically independent. Due to this uncorrelation the interferometer performs measurements at the shot-noise limit and the resolution is limited by $1/\sqrt{n}$ as expected. In the next section, we will show how this limit can be crossed.

30.4 Interferometer with Squeezed States of Light

Carefully designed interferometers can beat the shot-noise limit, e.g. by injecting squeezed states into the interferometer. We will consider three different scenarios: (1) Input ports 1 and 2 are illuminated with a coherent state and vacuum squeezed state, respectively ($|\psi\rangle_1|\psi\rangle_2 = |\alpha\rangle_1|0, \xi\rangle_2$). (2) Both ports are illuminated with bright squeezed states ($|\psi\rangle_1|\psi\rangle_2 = |\alpha, \xi\rangle_1|\alpha, \xi\rangle_2$). (3) A bright squeezed state and a squeezed vacuum state are injected into the interferometer ($|\psi\rangle_1|\psi\rangle_2 = |\alpha, \xi\rangle_1|0, \xi\rangle_2$). In the following we will see that all these realizations beat the shot-noise limit. However, only one of them reaches the Heisenberg limit.

30.4.1 Interferometer operating with a coherent state and a squeezed vacuum state

In our analysis, we assume that mode one is in a coherent state $|\alpha\rangle_1$ while mode two is a vacuum state that is squeezed $|0, \xi\rangle_2$, where ξ is the complex squeeze parameter $\xi = se^{i\vartheta}$. The strength of the squeezing is given by the parameter s and the orientation of the squeezing

ellipse is given by ϑ . Basic expectation values required for the calculation are [21]

$$\begin{aligned}\langle \alpha | \hat{n} | \alpha \rangle &= |\alpha|^2, \\ \langle 0, \xi | \hat{n} | 0, \xi \rangle &= \sinh^2 s, \\ \langle \alpha | \hat{n}^2 | \alpha \rangle &= |\alpha|^4 + |\alpha|^2, \\ \langle 0, \xi | \hat{n}^2 | 0, \xi \rangle &= 3 \sinh^4 s + 2 \sinh^2 s.\end{aligned}\tag{30.20}$$

Again, the operators labeled with index “1” act only on mode one while the index “2” acts on the second mode and $\hat{n} = \hat{a}^\dagger \hat{a}$ denotes the photon number operator. The amplitude of the coherent state is assumed to be real (see Fig. 30.2), as only the relative phase θ between the input modes matters. Using these relations, the noise of the photon number difference of the output modes can be calculated as

$$\begin{aligned}(\Delta n_{\text{out}}) &= \sqrt{{}_1\langle \alpha | {}_2\langle 0, \xi | \hat{n}_{\text{out}}^2 | 0, \xi \rangle {}_2| \alpha \rangle {}_1 - ({}_1\langle \alpha | {}_2\langle 0, \xi | \hat{n}_{\text{out}} | 0, \xi \rangle {}_2| \alpha \rangle {}_1)^2} \\ &= \sqrt{[\alpha^2 + 2 \sinh^2 s (\sinh^2 s + 1)] \cos^2 \varphi + [\alpha^2 e^{-2s} + \sinh^2 s] \sin^2 \varphi}.\end{aligned}$$

The orientation of the squeezing ellipse is $\vartheta = 0$, corresponding to an amplitude squeezed vacuum mode. The resolution of the mean photon number is

$$\frac{\partial \langle n_{\text{out}} \rangle}{\partial \varphi} = (|\alpha|^2 - \sinh^2 s) \sin \varphi.\tag{30.21}$$

By choosing the phase $\varphi = \pi/2$, we maximize the resolution while minimizing the noise. The error is then found to be

$$\Delta \varphi = \sqrt{\frac{ne^{-2s} + \sinh^2 s}{(n - \sinh^2 s)^2}},\tag{30.22}$$

where n denotes the number of classical photons in the interferometer. Let us discuss this result in detail. With no squeezing ($s = 0$), expression (30.22) reduces to $\Delta \varphi = 1/n^{1/2}$, in agreement with the result of the previous section (30.18). For quite moderate squeezing where the number of “squeezed” photons, $\sinh^2 s$, is negligible compared to the photons of the bright input mode, $n \gg \sinh^2 s$, Eq. (30.22) is reduced to

$$\Delta \varphi = e^{-s}/n^{1/2}.\tag{30.23}$$

This expression also follows from the linearized approach [22]. However, for very strong squeezing, the number of photons due to squeezing $\sinh^2 s$ becomes comparable to ne^{-2s} while we still may assume $n \gg \sinh^2 s$. With this approximation (30.22) can be rewritten as

$$\Delta \varphi = \sqrt{\frac{ne^{-2s} + 1/4e^{2s}}{n^2}}.\tag{30.24}$$

Using the approximate solution, one can easily find the squeezing level at which the phase resolution is optimized. For a squeezing value of $e^{2s} = 2n^{1/2}$, Eq. (30.24) has a minimum, therefore the statistical error is

$$\Delta \varphi = 1/n^{3/4}.\tag{30.25}$$

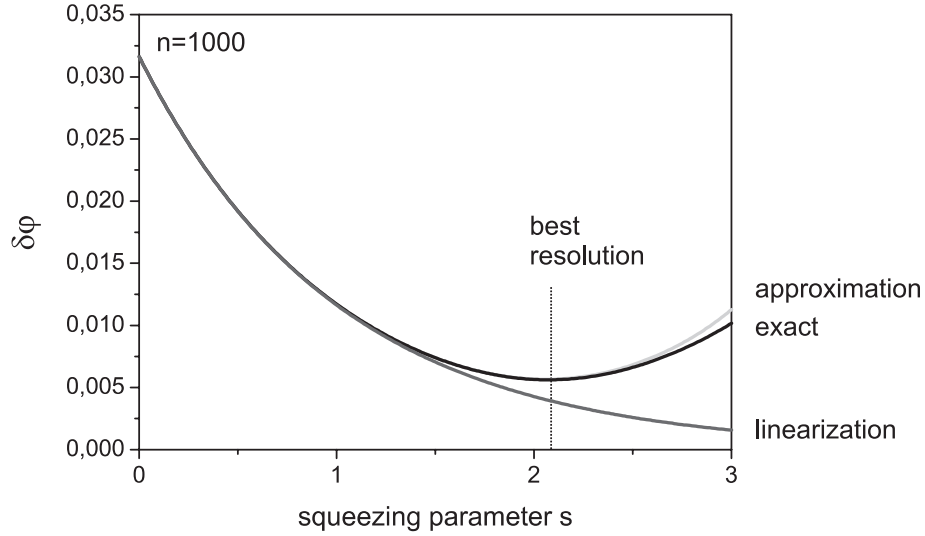


Figure 30.4. Phase resolution of interferometer with bright coherent input and a phase squeezed vacuum input as a function of s . We assume $n = 1000$ photons for the coherent beam. The exact (30.22) and the approximate (30.24) solution are plotted together with the result one would obtain using the linearization approach (30.23). Best resolution is achieved for $s \approx 2.07$, i.e. the number of squeezed photons is still negligible in this regime, the limit $1/n^{3/4}$ is reached.

This result should be compared with $\Delta\varphi = 1/n^{1/2}$, the case where no squeezing was present in the scheme. Squeezing the vacuum into the setup may significantly enhance the phase resolution properties, however, quite high squeezing $s > 1$ is required to reach the optimum. These results are summarized in Fig. 30.4, where the exact solution is plotted together with the approximate calculation and the results from the linearization.

The sensitivity improvement by using a squeezed vacuum was first proposed by Caves [23] and later the effect of imperfections of the interferometer such as losses and nonunity fringe visibility were discussed by Gea-Banacloche et al. [24]. The idea has also been experimentally demonstrated several times. Xiao et al. [25] and Grangier et al. [26] demonstrated a sensitivity improvement of a standard Mach–Zehnder interferometer, and recently McKenzie et al. [27] and Schnabel et al. [28] have demonstrated an improvement in a power-recycled and a signal- and power-recycled interferometer, respectively. These last experiments were predicted in Ref. [29].

The improvement of the interferometer sensitivity by the use of squeezed vacuum states can also be easily understood from the geometrical representation introduced in the previous section. Let us return to Fig. 30.3, but now we consider the case where the input vector $\bar{\delta}c$ is suppressed due to the squeezing of the input field in input port 2. Recalling that the amplitude uncertainties of output ports 3 and 4 are governed by $\bar{\delta}a + \bar{\delta}c$ and $\bar{\delta}a - \bar{\delta}c$, respectively, we clearly see that the two outputs both are proportional to $\bar{\delta}a$ (and thus correlated) while reducing $\bar{\delta}c$. When measuring the difference of the intensities at the two output ports, one finds

a quantum noise suppressed signal and hence an improvement in the sensitivity for measuring arm length differences.

In the above discussion, we assumed a $\pi/2$ phase shift in one of the interferometer arms in order to maximize the signal for the given measurement strategy. If instead we set the phase shift to be zero, one output will be dark and the other one will be bright. In this case, the interferometer can attain the same resolution as before, however another measurement strategy must be employed: homodyne detection in the dark port or a modulation technique [11]. Again the pictorial argument can be made for the noises and again one finds a sensitivity improvement by quantum noise reduction. Again $\delta\bar{c}$ has to be suppressed at input port 2 at the expense of increasing $\delta\bar{d}$ which in turn does not affect the close to zero amplitude at port 4. The bright output beam at port 3 recovers the noise properties of input 1 and it can be recycled, i.e. reinjected into the interferometer to enhance the total power inside the interferometer.

We have seen that the sensitivity of an interferometer can be increased by suppressing the noise in the dark input port. In the next two sections, we will address the question whether the sensitivity can be increased further by squeezing the other input state.

30.4.2 Interferometer operating with two bright squeezed states

The expectation values of the photon number and the photon number squared (as needed to determine the phase resolution) for two bright input squeezed states can be determined by making use of the squeezing operators, $\hat{S}$, (to squeeze the vacuum) and the displacement operator, $\hat{D}$, (to displace the the squeezed vacuum) both acting on the vacuum state $|\alpha, \xi\rangle = \hat{D}\hat{S}|0\rangle$. Using this relation and the fact that $\hat{D}\hat{S}\hat{S}^\dagger\hat{D}^\dagger = 1$, the basic expectation values required for the analysis of this type of interferometer can be calculated. For example, we have

$$\begin{aligned}\langle\alpha, \xi|\hat{a}^{\dagger 2}|\alpha, \xi\rangle &= \langle 0|\hat{S}^\dagger\hat{D}^\dagger\hat{a}^\dagger\hat{D}\hat{S}\hat{S}^\dagger\hat{D}^\dagger\hat{a}^\dagger\hat{D}\hat{S}|0\rangle \\ &= e^{-2i\theta}\langle 0|(\hat{a}^\dagger \cosh s - \hat{a}e^{-i\vartheta} \sinh s + \alpha)^2|0\rangle \\ &= e^{-2i\theta}(-e^{i\vartheta} \sinh s \cosh s + |\alpha|^2),\end{aligned}\quad (30.26)$$

and

$$\begin{aligned}\langle\alpha, \xi|\hat{a}|\alpha, \xi\rangle &= |\alpha|e^{i\theta} \\ \langle\alpha, \xi|\hat{a}^\dagger\hat{a}|\alpha, \xi\rangle &= \sinh^2 s + |\alpha|^2 \\ \langle\alpha, \xi|\hat{a}\hat{a}^\dagger|\alpha, \xi\rangle &= \cosh^2 s + |\alpha|^2 \\ \langle\alpha, \xi|\hat{a}^\dagger\hat{a}\hat{a}^\dagger\hat{a}|\alpha, \xi\rangle &= |\alpha|^2(e^{2s}\sin^2(\theta - \frac{1}{2}\vartheta) + e^{-2s}\cos^2(\theta - \frac{1}{2}\vartheta)) \\ &\quad + 2\sinh^2 s(\sinh^2 s + 1) + |\alpha|^4 + \sinh^4 s + 2|\alpha|^2 \sinh^2 s.\end{aligned}\quad (30.27)$$

We allowed for an arbitrary phase θ of mode $\hat{a}$ and used $\langle\hat{U}^\dagger\hat{a}\hat{U}\rangle = e^{-i\theta}\langle\hat{a}^\dagger\rangle$ where $\hat{U}$ is the phase shifting operator. With these relations at hand and assuming (a) that the two input states are equally amplitude squeezed (described by the parameter s), (b) the excitation of the two inputs are identical, denoted as α , (c) the relative phase shift between them is $\theta = \pi/2$, and (d) there is a zero relative phase shift between the two arms in the interferometer ($\varphi = 0$), we

can calculate the following photon number uncertainty:

$$\begin{aligned}\Delta n_{\text{out}} &= \sqrt{{}_1\langle\alpha, \xi|_2\langle\alpha, \xi|\hat{n}_{\text{out}}^2|\alpha, \xi\rangle_2|\alpha, \xi\rangle_1 - ({}_1\langle\alpha, \xi|_2\langle\alpha, \xi|\hat{n}_{\text{out}}|\alpha, \xi\rangle_2|\alpha, \xi\rangle_1)^2} \\ &= \sqrt{2|\alpha|^2 e^{-2s} + 4 \sinh^2 s (\sinh^2 s + 1)}\end{aligned}\quad (30.28)$$

The partial derivative of the average photon number with respect to the phase φ is $\partial\langle n\rangle/\partial\varphi = 2|\alpha|^2$ and the statistical error in phase estimation is

$$\Delta\varphi = \sqrt{\frac{ne^{-2s} + 2 \sinh^2 s (\sinh^2 s + 1)}{2n^2}}. \quad (30.29)$$

From this expression, we see that there are two competitive terms in the denominator. The first term reduced the error in phase estimation while the second term increases this error. The latter term is a function of the number of “squeezed” photons and thus relatively small for low degrees of squeezing. However for high squeezing degrees this term might dominate, hereby deteriorating the performance of the interferometer. Again, we find the minimum for the phase resolution via an approximate solution with $ne^{-2s} \approx \sinh^2 s$ but $n \ll \sinh^2 s$:

$$\Delta\varphi = \sqrt{\frac{ne^{-2s} + \frac{1}{8}e^{4s}}{2n^2}}. \quad (30.30)$$

The optimum squeezing where the phase resolution is optimized is then given by $e^{-2s} = (4n)^{-1/3}$. Inserting this into Eq. (30.30), we find that the optimal sensitivity for this scenario is given by approximately $0.69/n^{2/3} \propto 1/n^{2/3}$. It is therefore better to use a squeezed vacuum state and a coherent state at the input, since in this case the statistical error was $1/n^{3/4}$ which is indeed smaller than the result above.

30.4.3 Interferometer operating with a bright squeezed state and a squeezed vacuum state

Now we consider the last scenario where one input state is bright squeezed whereas the other input state is vacuum squeezed. To simplify the derivation on the phase resolution we assume the two input states to be equally squeezed in the same quadrature, their relative phase shift θ to be $\pi/2$ and the biased phase shift in the interferometer φ to be $\pi/2$. With these choices and using Eq. (30.27), we find the uncertainty

$$\begin{aligned}\Delta n &= \sqrt{{}_1\langle\alpha, \xi|_2\langle 0, \xi|\hat{n}_{\text{out}}^2|0, \xi\rangle_2|\alpha, \xi\rangle_1 - ({}_1\langle\alpha, \xi|_2\langle 0, \xi|\hat{n}_{\text{out}}|0, \xi\rangle_2|\alpha, \xi\rangle_1)^2} \\ &= \sqrt{-2n \cosh s \sinh s + n + 2n \sinh^2 s},\end{aligned}\quad (30.31)$$

and $\partial\langle n\rangle/\partial\varphi = |\alpha|^2$. The phase resolution is then

$$\Delta\varphi_{(\text{sqz}, \text{sqz})} = \sqrt{\frac{-2n \cosh s \sinh s + n + 2n \sinh^2 s}{n^2}} = \frac{e^{-s}}{\sqrt{n}}, \quad (30.32)$$

which is plotted in Fig. 30.5.

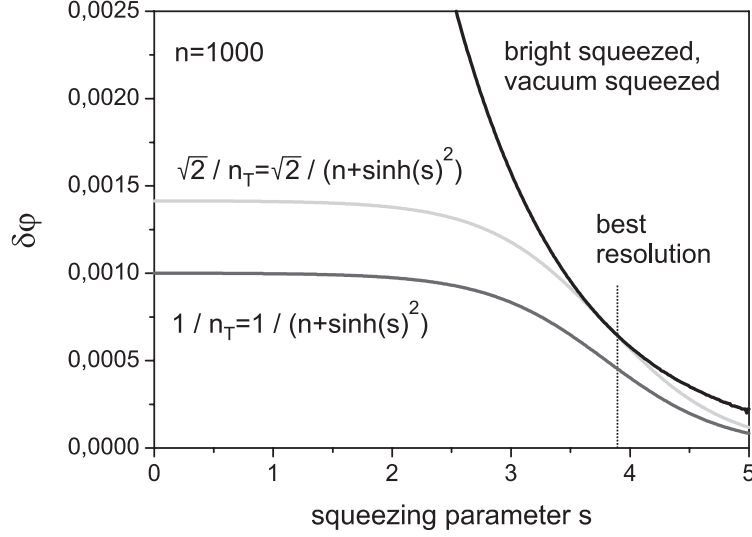


Figure 30.5. Comparison of the phase resolution for a bright squeezed and a vacuum squeezed input into the interferometer. We assume $n = 1000$ for the classical photon number. In addition to $\delta\varphi_{(\text{sqz}, \text{sqz})}$ we plot $\delta\varphi_{\text{Heis}}$ and $\sqrt{2}\varphi_{\text{Heis}}$.

Is this resolution approaching the Heisenberg limit? We answer this question by comparing expression (30.32) with the Heisenberg limit given by the total number of photons n_T in the interferometer for a certain squeezing parameter s

$$\Delta\varphi_{\text{Heis}} = \frac{1}{n_T} = \frac{1}{n + 2 \sinh^2 s}. \quad (30.33)$$

We maximize $\varphi_{\text{Heis}}/\delta\varphi_{(\text{sqz}, \text{sqz})}$ with respect to the squeezing parameter s under the assumption that $n \gg 1$ and using $2 \sinh^2 s \approx e^{2s}/2$. Hence for $s_{\text{max}} = (1/2) \ln(2n)$ the best resolution is achieved and we find from (30.32) the limit

$$\Delta\varphi_{(\text{sqz}, \text{sqz})} \approx \frac{1}{\sqrt{2n}}. \quad (30.34)$$

We compare this expression with the Heisenberg limit for s_{max} which is found to be

$$\Delta\varphi_{\text{Heis}} = \frac{1}{n_T} \approx \frac{1}{2n}, \quad (30.35)$$

i. e. we do not reach the Heisenberg limit exactly, but we find $\Delta\varphi_{(\text{sqz}, \text{sqz})} \approx \sqrt{2}/n_T$. This situation is displayed in Fig. 30.5: The phase resolution $\Delta\varphi_{(\text{sqz}, \text{sqz})}$ for $n = 1000$ is plotted together with the Heisenberg limit φ_{Heis} and $\sqrt{2}\varphi_{\text{Heis}}$. Best resolution is achieved for a certain squeezing value s_{max} .

We have now discussed various schemes with which the shot-noise limit for interferometers can be surpassed. However, in the above descriptions two realizations with squeezed

light were missing, namely the cases where a bright squeezed input beam is mixed with vacuum and the case where a coherent beam is mixed with a bright squeezed beam. The former realization reaches a sensitivity identical to the shot-noise limit, i.e. $\Delta\varphi = 1/\sqrt{n_T}$ with the total photon number $n_T = n + \sinh^2 s$. In the latter case, we get the general solution: $\Delta\varphi = \sqrt{n \exp(-2s) + 2 \sinh^2 s (\sinh^2 s + 1) + n + \sinh^4 s / \sqrt{4n^2}}$, and an approximative solution for the minimum is $\Delta\varphi = \sqrt{\frac{n(16/6*n)^{-1/3} + 3/16*(16/6*n)^{2/3} + n}{4n^2}}$. This solution is rather complex; however, by comparing it to the previous strategies, we conclude that this strategy is in general worse.

30.5 Summary and Discussion

In the previous sections, we have shown that the application of squeezed states in interferometry may enhance the phase sensitivity. The results of our analysis are displayed in Fig. 30.6 in which we compare the phase sensitivity $\delta\varphi$ for the different scenarios discussed above. We clearly see that all the schemes employing squeezed states at the input surpasses the shot-noise limit for interferometer. It is also evident that for high squeezing values the strategy where a bright squeezed state is mixed with a vacuum squeezed state is superior and eventually approaches the Heisenberg limit. The optimal phase resolution for the various schemes are summarized in Table 30.1.

Many other procedures that achieves the Heisenberg limit have been proposed. It has been shown that the usage of the maximally entangled state $|\varphi\rangle = \frac{1}{\sqrt{2}}(|n, 0\rangle + e^{in\varphi}|0, n\rangle)$, also

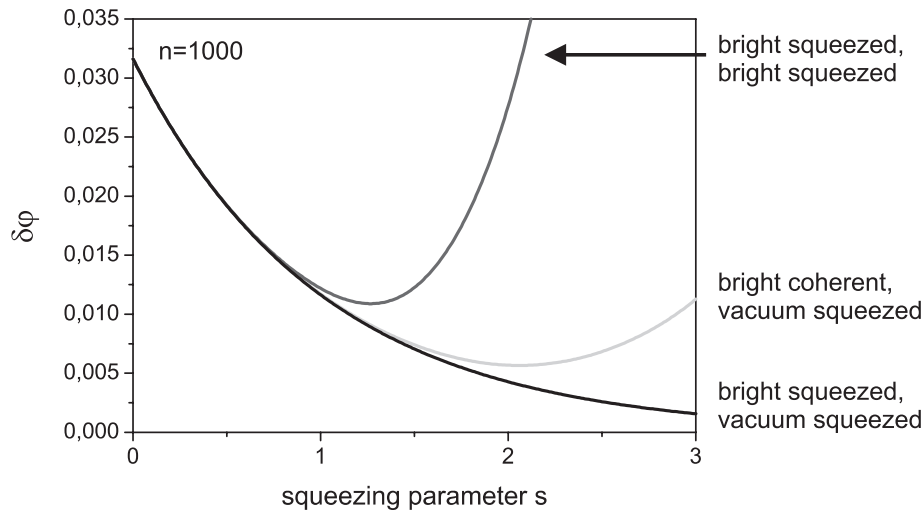


Figure 30.6. Phase resolution in quantum interferometry for different input states. We always $|\alpha|^2 = 1000$, thus for the case of two bright squeezed input modes, we considered 500 photons for each mode. Note that the number of total photons increases as the squeezing parameter is increased.

Table 30.1. Summary of various scenarios for driving a quantum interferometer and the respective phase sensitivities $\Delta\varphi$. (*): $\sqrt{\frac{n(16/6*n)^{-1/3} + 3/16*(16/6*n)^{2/3} + n}{4n^2}}$

Input port 1 2nd input port	Bright coherent	Bright squeezed	Fock state
Coherent vacuum	$1/\sqrt{n}$	$1/\sqrt{n + \sinh^2 s}$	
squeezed vacuum	$1/n^{3/4}$	$1/(\sqrt{2}n)$	
Bright squeezed	*	$\propto 1/n^{2/3}$	
Fock state			$1/n$ [31]

called the noon state, will enable quantum interferometry at the Heisenberg limit. Various different experimental realizations have been proposed. For example, Yurke proposed [32] to use fermions prepared in a so-called Yurke state in order to reach the Heisenberg limit, and latter on a similar scheme was proposed for bosons [30,33]. Another realization was proposed by Holland and Burnett [31]. They suggested to use two Fock states at the input to the Mach–Zehnder interferometer to achieve Heisenberg-limited interferometry. Bollinger et al. showed that optimal interferometry can be achieved by the use of maximally entangled states of a certain form [34], and finally Jacobson et al. showed that the limit can also be reached by measuring the de Broglie wavelength of radiation [35].

Exercises

- Derive Eq. (30.23) by using the linearization approach Hint: The annihilation operator can be decomposed into two terms: $\hat{a} = \alpha + \hat{\delta}a$ where α is the classical steady-state field and $\hat{\delta}a$ is an operator associated with the quantum noise. Derive Eq. (30.14) assuming that the minimum resolvable signal-to-noise ratio is unity.
- (a) Use the expansion of coherent states $|\alpha\rangle$ in terms of Fock states

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_n \frac{\alpha^n}{(n!)^{1/2}} |n\rangle \quad (30.36)$$

to derive the mean photon number $\bar{n} = \langle\alpha|\hat{n}|\alpha\rangle$ (see Eq. (1.20)) and its fluctuations $(\Delta n)^2 = \langle\alpha|\hat{n}^2|\alpha\rangle - \langle\alpha|\hat{n}|\alpha\rangle^2$. Hint: $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$, $\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$, $[\hat{a}, \hat{a}^\dagger] = 1$.

- Use the relations $\hat{S}^\dagger \hat{a} \hat{S} = \hat{a} \cosh s - \hat{a}^\dagger \exp(i\theta) \sinh s$ and $\hat{S}^\dagger \hat{a}^\dagger \hat{S} = \hat{a}^\dagger \cosh s - \hat{a} \exp(-i\theta) \sinh s$ where $\hat{S}$ is the squeeze operator $\hat{S}|0\rangle = |0, \xi\rangle$ to derive $\langle 0, \xi | \hat{n} | 0, \xi \rangle$ and $\langle 0, \xi | \hat{n}^2 | 0, \xi \rangle$. Show that $(\Delta n)^2$ for a squeezed state yields $2\langle\hat{n}\rangle(\langle\hat{n}\rangle + 1)$

References

- [1] C. J. Davisson and L. H. Germer, *Phys. Rev.* **30**, 705 (1927).
- [2] M. Arndt, O. Nairz, J. Voss-Andreae, C. Keller, G. van der Zouw, and A. Zeilinger, *Nature* **401**, 680 (1999).
- [3] C. K. Hong, Z. Y. Ou, and L. Mandel, *Phys. Rev. Lett.* **59**, 2044 (1987).
- [4] V. B. Braginsky, *Sov. Phys.—JETP* **26**, 831 (1968).
- [5] C. M. Caves, *Phys. Rev. Lett.* **45**, 75 (1980).
- [6] R. Loudon, *Phys. Rev. Lett.* **47**, 815 (1981).
- [7] H. P. Yuen, *Phys. Rev. Lett.* **51**, 719 (1983).
- [8] W. G. Unruh, ‘Quantum Noise in the interferometer Detectort’, in *Quantum Optics, Experimental Gravitation, and Measurement Theory*, ed. by P. Meystre, M. O. Scully (Plenum Press, New York, 1983) pp. 647–660.
- [9] M. T. Jaekel and S. Reynaud, *Europhys. Lett.* **13**, 301 (1990).
- [10] A. Luis and L. L. Sánchez-Soto, *Opt. Commun.* **89**, 140 (1992).
- [11] G. Leuchs, K. Maischberger, A. Rüdiger, R. Schilling, L. Schnupp, and W. Winkler, ‘Proposal for the Construction of a Large Laser Interferometer for the Measurement of Gravitational Waves’, Max Planck Institute for Quantum Optics, report No. MPQ-131 (1987), K. Danzmann, H. Lück, A. Rüdiger, R. Schilling, M. Schrepel, W. Winkler, J. Hough, G. P. Newton, N. A. Robertson, H. Ward, A. M. Campbell, J. E. Logan, D. I. Robertson, K. A. Strain, J. R. J. Bennett, V. Kose, M. Kühne, B. F. Schutz, D. Nicholson, J. Shuttleworth, H. Welling, P. Aufmuth, R. Rinkleff, A. Tünnermann, and B. Willke: ‘GEO 600. Proposal for a 600 m Laser-Interferometric Gravitational Wave Antennat’, Max Planck Institute for Quantum Optics, report No. MPQ-190 (1994).
- [12] V. B. Braginsky and A. B. Manukin, *Zh. Eksp. Teor. Fiz.* **52**, 987 (1967).
- [13] G. G. Stokes, *Cambridge and Dublin Math. J.* IV, 1 (1849)
- [14] M. W. Hamilton, *Am. J. Phys.* **68**, 186 (2000)
- [15] Z. Y. Ou, *Phys. Rev. A*, **55**, 2598 (1997).
- [16] W. Winkler, G. Wagner, and G. Leuchs, ‘Interferometric detection of gravitational radiation and nonclassical light’, in *Fundamentals of Quantum Optics II*, ed. by F. Ehlotzky, (Springer, Berlin, Heidelberg, 1987) pp. 92–108; G. Leuchs, *Contemp. Phys.* **29**, 299 (1988).
- [17] G. Leuchs, T. C. Ralph, C. Silberhorn, and N. Korolkova, *J. Mod. Optics* **46**, 1927 (1999).
- [18] G. Leuchs, ‘Photon statistics, anti-bunching, and squeezed states’, in *Frontiers of Non-Equilibrium Statistical Physics*, ed. by G. T. Moore and M. O. Scully, (Plenum Press, New York, London, 1986) pp. 329–360.
- [19] G. Leuchs, in *Laser physics at the limit* ed. by H. Figger, D. Meschede, and C. Zimmermann, (Springer, Berlin, Heidelberg, 2002) pp. 209.
- [20] W. Schleich, *Quantum Optics in Phase Space* (Wiley-VCH, Heidelberg, New York, 2000).
- [21] R. Loudon, *The Quantum Theory of Light*, (Oxford University Press, Oxford, 2000).

- [22] S. Inoue, G. Björk, and Y. Yamamoto, *Proc. SPIE* **2378**, 99 (1995); N. Korolkova, C. Silberhorn, O. Glöckl, S. Lorenz, C. Marquardt, and G. Leuchs, *Eur. Phys. J. D* **18**, 229, (2002).
- [23] C. M. Caves, *Phys. Rev. D* **23**, 1693 (1981).
- [24] J. Gea-Banacloche and G. Leuchs, *J. Mod. Optics* **34**, 793 (1987); J. Gea-Banacloche and G. Leuchs, *J. Opt. Soc. Am. B* **4**, 1667 (1987); J. Gea-Banacloche and G. Leuchs, *J. Mod. Opt.* **36**, 1277 (1989).
- [25] M. Xiao, L.-A. Wu, and H. J. Kimble, *Phys. Rev. Lett.* **59**, 278 (1987).
- [26] P. Grangier, R. E. Slusher, B. Yurke, and A. LaPorta, *Phys. Rev. Lett.* **59**, 2153 (1987).
- [27] K. McKenzie, D. A. Shaddock, D. E. McClelland, B. C. Buchler, and P. K. Lam, *Phys. Rev. Lett.* **88**, 231102 (2002).
- [28] R. Schnabel, H. Vahlbruch, S. Chelkowski, B. Hage, A. Franzen, N. Lastzka, and K. Danzmann, Abstract p. 155, 9th International Conference on Squeezed States and Uncertainty Relations, Besancon, France (2005).
- [29] A. Brillet, J. Gea-Banacloche, G. Leuchs, C. N. Man, and J.Y. Vinet, 'Advanced techniques: recycling and squeezing' in 'Detection of Gravitational Waves' pp. 369–405, ed. by D. Blair, (Cambridge University Press, Cambridge University, 1991)
- [30] B. Yurke, S. L. McCall, and J. R. Klauder, *Phys. Rev. A* **33**, 4033(1986).
- [31] M. J. Holland and K. Burnett, *Phys. Rev. Lett.* **71**, 1355 (1993); T. Kim, O. Pfister, M. J. Holland, J. Noh, and J. L. Hall, *Phys. Rev. A* **57**, 4004 (1998) and references therein.
- [32] B. Yurke, *Phys. Rev. Lett.* **56**, 1515 (1986).
- [33] H. P. Yuen, *Phys. Rev. Lett.* **56**, 2176 (1986).
- [34] J. J. Bollinger, W. M. Otano, D. J. Wineland, and D. J. Heinzen, *Phys. Rev. A* **54**, R4649 (1996).
- [35] J. Jacobson, G. Björk, I. Chuang, and Y. Yamamoto, *Phys. Rev. Lett.* **74**, 4835 (1995).

31 Quantum Imaging

Claude Fabre and Nicolas Treps¹

31.1 Introduction

For more than two decades now, techniques have been designed and experimentally implemented enabling physicists to get rid of, or at least to reduce, quantum fluctuations in optical measurements. The same techniques lead also to the production of strong quantum correlations and entanglement in light. This domain has recently been successfully developed in the direction of quantum information processing and is presented extensively in the present book.

So far the quantum noise reduction, or the correlations, were effective when the *total intensity of light beams* was recorded. But there is another part of optics which presents a great interest from the point of view of information: The domain of *optical images*, which are a privileged medium to convey a great quantity of information in a parallel way. “Pixellized” detectors (such as CCD cameras or detectors arrays) are used to record such information, either in the photon counting regime or with macroscopic intensities. Due to the quantum nature of light, this information is inevitably affected by uncontrolled fluctuations, the “quantum noise” or shot noise, which limits the reliability of the information extraction from the image, or the ultimate resolution for the detection of small details in the image. In these optical measurements, the fluctuations that come into play are the *local spatial quantum fluctuations*.

Researches made in the last decade at the theoretical level showed that it was possible to tailor these local spatial quantum fluctuations of light (of course within the constraint imposed by Heisenberg inequalities), and also to produce *spatial quantum entanglement*, i.e. to create strong quantum correlations in the measurements performed at different points of the optical image. Quantum techniques have the potentiality to improve the sensitivity of measurements performed in images and to increase the optical resolution beyond the wavelength limit, not only at the single photon counting level, but also with macroscopic beams of light. These new techniques could then be of interest in many domains where light is used as a tool to convey information in very delicate physical measurements, such as ultraweak absorption spectroscopy or atomic force microscopy. Detecting details in images smaller than the wavelength has obvious applications in the fields of microscopy and pattern recognition, and also in optical data storage, where it is now envisioned to store bits on areas much smaller than the square of the wavelength. Furthermore, spatial entanglement leads to completely novel

¹Laboratoire Kastler Brossel, of the Ecole Normale Supérieure and the University P.M. Curie, associated with the Centre National de la Recherche Scientifique. This work was supported by the European Commission in the frame of the QUANTIM project (IST-2000-26019).

and fascinating effects, such as two-photon imaging, in which the camera is illuminated by light which did not interact with the object to image, or “quantum microlithography”, where the quantum entanglement is able to act upon matter at a scale smaller than the wavelength. Finally, there is a natural extension of quantum information protocols to multimode quantum information and computing using images that is still in its very early days.

This kind of study forms a newly emerging subject of quantum optics, and few pioneer experimental demonstrations have been already performed. The investigations made so far concern mainly the ways of producing and characterizing spatially entangled nonclassical light and also first simple implementations of applications, which showed that it is possible using such concepts to improve information extraction from images. To illustrate these somewhat abstract considerations, we will give in the following a short description of several achievements obtained in the domain, and conclude by mentioning some perspectives and open problems which seem promising and deserve therefore more investigations in the future. Readers interested in more details can find them in some review articles [1].

31.2 The Quantum Laser Pointer

Experiments have demonstrated that the sensitivity of optical measurements performed on the global intensity of a light beam, or on its global phase, can be improved by using *single mode nonclassical states of light*, such as sub-Poissonian or squeezed states. This is no longer true for measurements performed in optical images, in which one monitors a variation of the transverse distribution of the light and not of the total intensity. One needs in this case more complex nonclassical beams, which are superpositions of different transverse modes, i.e. *multimode nonclassical states of light*.

The simplest of these measurements is that of the position of the center of a beam, which is obtained using a quadrant detector (Fig. 31.1): If the four partial intensities are equal, the beam is exactly centered on the detector, and any imbalance between the four signals gives information about the transverse displacement of the beam. This is actually a highly sensitive measurement, at the nanometer scale. But as all optical measurements, it is limited by the standard quantum noise, or shot noise, present on the four parts of the quadrant detector. It was first shown theoretically [2] that the pointing sensitivity can be improved beyond such a standard quantum limit by using, instead of a usual laser beam, the superposition of a single-mode squeezed beam with a coherent beam having its two halves in the transverse plane shifted with each other by π . This curious mixing actually creates a perfect quantum correlation between the intensities measured on the halves of the total beam, and therefore on the photocurrents detected on the corresponding pixels of the detector.

This effect has been recently experimentally demonstrated [3]: The two transverse displacements of the beam center were measured with a sensitivity better than the standard quantum limit. In order to measure *simultaneously* the two transverse coordinates below shot noise, one needs a three-mode nonclassical state of light, consisting of the superposition of two squeezed states and a coherent state, each transverse mode having appropriate π phase shifts in the four quadrants of the transverse plane corresponding to the four detection regions (Fig. 31.1).

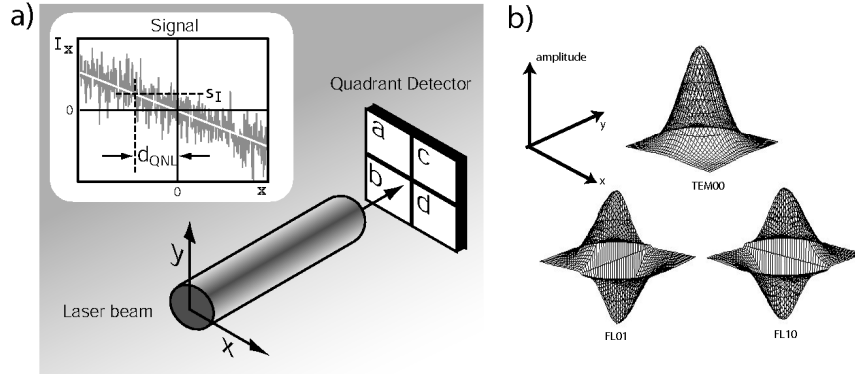


Figure 31.1. Measuring the pointing direction of a laser beam with a quadrant detector: (a) Quantum fluctuations limit the ultimate accuracy of the positioning measurement; (b) transverse modes to be considered in order to go beyond the standard quantum noise limit in two-dimension positioning.

Transverse displacement is the simplest measurement that can be performed with a multi-pixel detector, but there are many other parameters that can be extracted from an image: The motion of a very small scattering object, a very weak spatial modulation, the presence or absence of small holes carrying digitized information, for example in CDs used in optical storage of information. The extraction of such an information is made through “image processing”, which consists in most cases in computing linear combinations of the local intensities measured by the different pixels. This problem has been analyzed in detail at the theoretical level [4]. The transverse mode responsible for the noise in this kind of image processing has been identified for any linear processing. By reducing the noise in this specific mode, one improves the determination of the corresponding information. This kind of technique may improve many image processing and analysis functions, such as pattern recognition, image segmentation, or wavefront analysis.

On the quantum information side, techniques have recently been theoretically proposed for producing *spatially entangled beams* [5], which constitute an extension to the problem of transverse measurements of the entangled state proposed by Einstein, Podolsky and Rosen for the measurement of X and P . In these “EPR-entangled beams”, the measurements of the transverse position x of two light beams are perfectly correlated, whereas measurements of the angular tilt θ with respect to the optical axis are perfectly anti-correlated. In the transverse plane, x and θ are indeed the quantum-conjugate quantities which are analogous of X and P for a particle.

31.3 Manipulation of Spatial Quantum Noise

The experiment described in the previous section shows that it is possible to manipulate the *transverse distribution of temporal quantum fluctuations* in light. But in an image, there is

also a “pure” spatial quantum noise, i.e. the *pixel-to-pixel fluctuations of the light intensity when it is integrated over the total duration of a single light pulse*. It concerns only spatial averages, and no longer time averages.

Measuring pixel-to-pixel fluctuations at the quantum level is a new experimental challenge, and novel and delicate experimental techniques had to be developed in order to reach the shot noise level for spatial fluctuations. In particular it is necessary to make a very precise calibration of each pixel of the detector, so that the intensity measured on each one can be properly normalized [6]. It is only after all these technical problems have been solved that it was possible to observe the two specific spatial quantum effects that are described in the two following subsections.

31.3.1 Observation of pure spatial quantum correlations in parametric down conversion

It is well known that parametric down conversion produces “twin photons” which are perfectly correlated at the quantum level, not only temporally (they are produced at the same time) but also spatially (they are produced in symmetric directions). This effect has been extensively used in beautiful landmark experiments at the photon counting level. When the pump intensity is raised by a large factor, many twin photons are produced, and they can no longer be counted individually. One now obtains patterns, or “images” on the signal and idler beams which are still temporally and spatially correlated at the quantum level. As can be seen in Fig. 31.2 each image has large pixel-to-pixel fluctuations, but almost identical intensity values on pixels symmetrical with respect to the center of the figure.

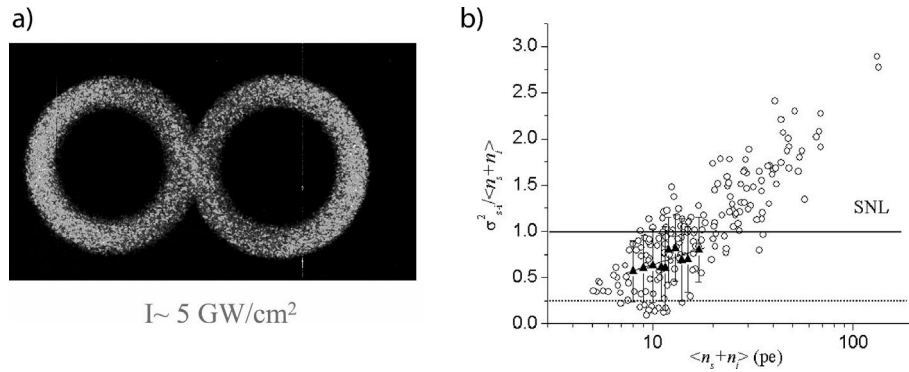


Figure 31.2. a) Light emitted by the process of spontaneous parametric down-conversion when it is pumped at very high intensities I , so that many photons arrive simultaneously at the same point; (b) intensity noise difference between two symmetric pixels, averaged over all pixels, as a function of the gain. The horizontal solid line is the standard quantum limit.

The experiment [7] has been performed with an intense pulse laser as the pump of the spontaneous down-conversion process. The parametric gain is high in such a regime (10 to 1000), and roughly 10 to 100 photons were recorded on average on each pixel. A pixel to

pixel quantum correlation was found between the intensity distributions of the signal and idler transverse patterns recorded after a single pump laser shot. More precisely, the variance of the difference between the intensities recorded on the signal and idler modes on symmetrical pixels, averaged over the different points of the transverse plane, was measured to be well below the standard quantum limit, which is in this case the spatial shot noise corresponding to the total intensities measured on the photodetectors. The best spatial noise reduction observed was about 50% below the standard quantum limit. For very high gain, the quantum correlation turns out to disappear. This quantum-to-classical transition from the quantum to the classical regime is due to the spatial narrowing of the signal or idler beams generated by the nonlinear crystal with increased gain, which lead, through diffraction, to an extension of the zone in which the twin photons are distributed. The quantum spatial correlation that has been observed can now be used to improve information processing in images, for example to improve the sensitivity in the detection of faint images below the standard quantum limit.

31.3.2 Noiseless image parametric amplification

Optical amplification is one of the key techniques in the handling of optical information. Quantum theory shows that the amplification process induces inevitably a degradation of the signal to noise ratio by at least a factor 2 when oscillating signals are amplified in a way independent of the phase of the oscillation. In contrast the amplification can be noiseless in the phase-sensitive configuration. It is known that parametric amplification, in the frequency degenerate configuration, can operate in such a phase sensitive way. It can thus amplify an optical signal without degrading it.

This important property of degenerate parametric amplifiers had been demonstrated for the total intensities of the amplified signal beam in a pulsed parametric amplifier. It also holds for image amplification. The experimental demonstration of noiseless image amplification has been the first experimental demonstration of a quantum imaging effect. It concerned the temporal fluctuations measured at the different points of an image [8]. The effect was also recently demonstrated for the pure pixel to pixel spatial fluctuations of an image amplified by a pulsed optical parametric amplifier and recorded on a pump laser single shot [9]. In a very delicate experiment the spatial noise figures were determined in the phase-sensitive and phase insensitive schemes, and it was shown that in the low gain regime the phase sensitive amplifier does not add noise, while the phase insensitive amplifier leads to the degradation of the signal to noise ratio by a factor 2 (Fig. 31.3). Amplification of faint images without degradation of their quality is obviously a domain which may have important applications.

31.4 Two-Photon Imaging

Two-photon imaging, sometimes labeled as “ghost imaging”, is a striking effect based on the spatial correlations of light. It was demonstrated for the first time by using the spatial quantum correlations existing between the signal and idler twin photons produced by spontaneous parametric down-conversion [10]. Its principle is the following (see Fig. 31.4): One inserts in the signal arm an object that one intends to observe. The image of this object is obtained in a rather paradoxical way, without using a pixellized detector but instead a nonimaging “bucket”

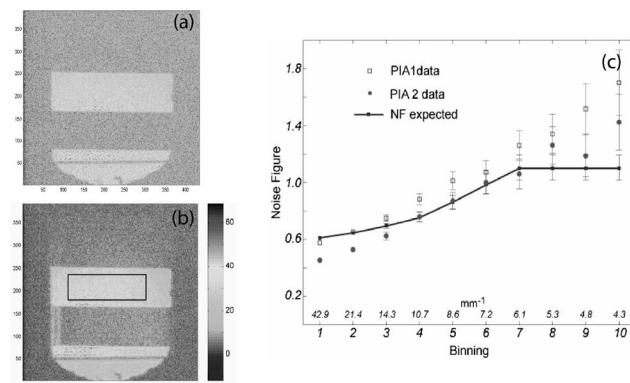


Figure 31.3. (a) Image without amplification, (b) amplified image in a phase insensitive amplifier, and (c) effective noise figure (ratio between the noises of the amplified and nonamplified image divided by the gain) versus the number of neighboring pixels used to determine the noise

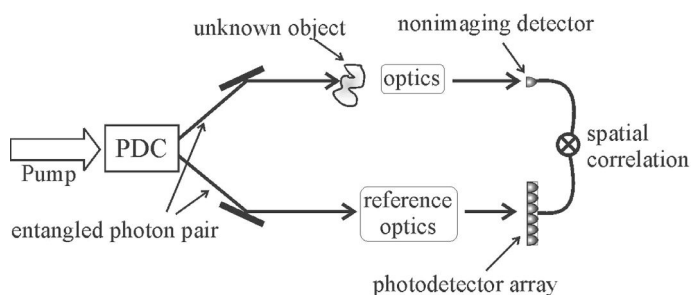


Figure 31.4. Two-photon imaging of an unknown object: Light going through the object is detected with a bucket detector, whereas the correlated beam is detected with a photodetector array.

detector on the signal beam, which measures only the total intensity transmitted through the object. On the other hand, one inserts a pixellized detector (i.e. a CCD camera) in the idler arm where there is no object. The image of the object is obtained by retaining the information on the CCD camera only when it is coincident with a photon measured by the “bucket” detector. This technique was implemented at the photon counting level in a number of beautiful experiments in the mid nineties, and was generally considered as the perfect example of a specific use of spatial quantum correlations in the photon-counting regime.

It was then showed that the effect could be also observed using the same kind of imaging setup, but in the intense light produced in the high gain regime of parametric amplification. More precisely the image appears on the correlation existing between the total intensity of the signal beam and the spatially resolved intensity distribution of the idler beam. It was also predicted that both the image itself (often called “near field image”) and its Fourier transform (obtained for example through diffraction in the far-field regime, and called “far field image”)

could be determined in the same experimental setup. As these two quantities play a role having some similarity with the conjugate variables position and momentum, this property was considered as being related to the EPR character of the spatial correlation between the signal and idler beams.

In a recent experiment [11], it was shown that a near-field image could be obtained by the same technique using classically correlated beams produced by a beam-splitter, and not twin photons. A lively worldwide discussion started on the precise assignment of classical and quantum features in “two-photon imaging”: It was in particular discovered, and experimentally demonstrated [12], that the same imaging technique could provide both the near-field and the far-field images using a thermal beam divided into two parts on a beam-splitter, instead of quantum correlated beams. Only some quantitative features, such as the contrast of the image are improved when one uses quantum correlated beams instead of classical correlations. From the point of view of applications, the fact that the mysterious “ghost imaging” can be realized using a simple beam-splitter and a thermal lamp instead of twin beams produced by a complex setup is positive in terms of cost and simplicity: This shows that there is some practical interest in precisely assigning what is classical and what is quantum in a given phenomenon, a discussion which is generally considered as purely academic.

31.5 Other Topics in Quantum Imaging

Among the numerous problems that are currently studied under the general name of quantum imaging, the investigations concerning the quantum limits on optical resolution have a special importance, as they may lead to new concepts in microscopy and optical data storage. “Super-resolution techniques” have been studied for a long time at the classical level in the perspective of beating the Rayleigh limit of resolution, on the order of the wavelength. In principle, deconvolution techniques are likely to extract the shape of a very small object from its image, even if it is completely blurred by diffraction. But the noise present in the image, and ultimately the quantum noise, will prevent such a perfect reconstruction procedure. It will reduce the quantity of information that can be obtained about the small object shape. This procedure of object reconstruction was recently revisited at the quantum level [13]. It was shown that it was in principle possible to improve the performance of super-resolution techniques by injecting nonclassical light in very specific transverse modes, namely the eigenmodes of the propagation through the imaging system. The precise generation scheme of such a multi-mode nonclassical light was also obtained. The simplicity of the proposed scheme brings confidence that quantum-enhanced super-resolution technique can effectively be implemented in an actual experiment.

Transverse solitons are potential candidates for the role of spatial q-bits, and soliton arrays for the role of q-registers. The theoretical study of their quantum features has been recently undertaken in different configurations: Free propagating solitons through planar Kerr media [14], and cavity solitons appearing in degenerate parametric oscillators [15]. As a first step in the investigation in the direction of quantum information processing, the existence of local noise reduction and spatial correlations has been predicted in such devices.

Nonlinear media have been used for a long time to process images. For example, up-conversion of optical images from the infrared to the visible has been proposed and realized

in order to take advantage of the higher quality of CCD detectors in the visible. This domain was also recently investigated at the quantum level in second harmonic generation: It has been shown that there existed configurations where the up-conversion of any image to the second harmonic field was possible without adding quantum noise to the initial image [16].

It is also interesting to investigate how the now “classical” protocols of quantum information on global variables, such as teleportation or cryptography, could be extended into the domain of images, and in which respect the intrinsic parallelism peculiar to imaging could be used in these protocols. The quantum teleportation of images was particularly studied in detail [17]. The proposed scheme has indeed a lot of similarities with the usual holographic technique, with the advantage that, in the quantum teleportation scheme, no quantum noise is added by the image reproduction device.

31.6 Conclusion and Perspectives

Microscopy, wavefront correction, image processing, optical data Storage, and optical measurements in general constitute a very important domain of our present day technologies. They can benefit in various ways from the researches on quantum imaging, which is currently studied by a growing number of teams throughout the world.

Optical technologies can directly benefit from the improvements brought by quantum effects and demonstrated by laboratory experiments, but their present complexity is an obstacle to such applications. At a less ambitious level, but perhaps more realistic, many optical technologies could be significantly improved by using the highly sophisticated methods developed in quantum optics laboratories to reach, and go beyond, the level of quantum noise in images. A great deal of research work remains indeed to be done, on the experimental side, to improve the light sources and the detectors in order to obtain high levels of quantum spatial entanglement and, but also on the theoretical side, to find more practical applications of spatial entanglement to information technologies. A promising direction of research is certainly the use of orbital angular momentum of light to convey and process quantum information. So far, the spatial quantum effects are somewhat on the edges of quantum computing, as they have been essentially used in the domain of metrology and information storage. No proposition has been made up to now to use the parallelism of optical imaging in quantum computing algorithms. This subject is obviously a very difficult one, but undoubtedly interesting. It requires collaborative work between the quantum computing and quantum imaging communities.

References

- [1] For a review of the subject, see for example: M. Kolobov, *Rev. Mod. Phys.* **71**, 1539 (1999); L.A. Lugiato, A. Gatti, and E. Brambilla *Quantum imaging*, *J. Opt. B: Quantum Semiclass. Opt.* **4**, S183 (2002), and the book to be published “Quantum Imaging” (Springer, Berlin 2005).
- [2] C. Fabre, J.B. Fouet, and A. Maitre, *Opt. Lett.* **25**, 76 (2000)
- [3] N. Treps, N. Grosse, C. Fabre, H. Bachor, and P.K. Lam, *Science* **301**, 940 (2003)
- [4] N. Treps, V. Delaubert, A. Maitre, J.M. Courty, and C. Fabre, *Phys. Rev.A* **71**, 013820 (2005)

- [5] M. Hsu, W. Bowen, N. Treps, and P.K. Lam, arXiv:quant-Ph/0501144, 2005
- [6] Y. Jiang, O. Jedrkiewicz, S. Minardi, P. Di Trapani, A. Mosset, E. Lantz, and F. Devaux, *Eur. Phys. J. D* **22**, 521 (2003)
- [7] O. Jedrkiewicz, Y.K. Jiang, E. Brambilla, A. Gatti, M. Bache, L. Lugiato, and P. Di Trapani, *Phys. Rev. Lett.* **93**, 243601 (2004)
- [8] SK Choi, M. Vasilyev, and P. Kumar, *Phys. Rev. Lett.* **83**, 1938 (1999)
- [9] A. Mosset, F. Devaux, and E. Lantz, “Experimental demonstration of noiseless amplification of images,” Preprint
- [10] D. V. Strekalov, A.V. Sergienko, D. N. Klyshko, and Y.H. Shih, *Phys. Rev. Lett.* **74**, 3600 (1995)
- [11] R.S. Bennink, S.J. Bentley, R.W. Boyd, and J.C. Howell, *Phys. Rev. Lett.* **92**, 033601 (2004)
- [12] A. Gatti, E. Brambilla, M.Bache, and L.A. Lugiato, *Phys. Rev. Lett.* **93**, 093602 (2004)
- [13] M. Kolobov and C. Fabre, *Phys. Rev. Lett.* **85**, 3789 (2000)
- [14] E. Lantz, T. Sylvestre, H. Maillotte, N. Treps, and C. Fabre, *J. Opt. B* **6**, S295 (2004)
- [15] I. Rabbiosi, A.J. Scroggie, and G.L. Oppo, *Eur. Phys. J. D* **22**, 453 (2003)
- [16] P. Scotto, P. Colet, and M. San Miguel, *Opti. Lett.* **28**, 1695 (2003)
- [17] I.V.Sokolov, M.I.Kolobov, A.Gatti, and L. A. Lugiato, *Opt. Commun.*, **193**, 175 (2001)

Index

- $N \rightarrow M$ purification protocol 190
- $T - V$ diagram 267
- π -pulse 541
- $\pi/2$ pulse 541
- para*-hydrogen 486, 495
- 2π pulse 541
- absorption 505
- Active transformations 46
- additivity 170
- adiabatic approximation 382, 384
- adiabatic computation 100
- adiabaticity 458
- alphabet 315
- Anti-Jaynes–Cummings Hamiltonian 394
- asymmetric cloning 67
- asymptotic continuity 168
- atom chip 549
- atom-cavity microscope 545
- atomic ensemble 516
- atomic kaleidoscope 545
- atomic spin operator 517
- atomic trajectory 544
- attenuated laser pulses 278
- authentication 275
- base norm 172
- BB84 protocol (Bennett-Brassard) 272
- BBPSSW protocol 187
- beam splitter 151, 153, 300, 321, 547, 576
- Bell
 - measurement 350
- Bell basis 186
- Bell Inequality 135
- Bell measurement 531
- Bell state 186, 257, 260
 - basis 258
 - measurement, BSM 260, 262
- Bell States 337
- Berry phase 383
- bipartite mixed states 125
- bipartite pure states 123
- bipartite system 179
- biseparable 244
- bit-flip error 110
- Bloch ball 40
- Bloch band 402
- Bloch equation 474
- Bloch sphere 360, 436
- Bloch vector 40
- block code 10
- Boolean Function
 - Conjunction 345
 - Disjunction 345
- Boolean function 315
- bound entangled 155
- bound entanglement: bipartite 183
- bound entanglement: multipartite 193
- bound state
 - photon+atom 567
- branch 472
- breeding 191
- bright squeezed states 584
- BSC 8
- Bures distance 165
- bus mode 395
- Caldeira–Leggett model 473
- Calderbank–Shor–Steane code(CSS) 276
- Canonical commutation relations 43
- canonical transformations 530
- Cartan decomposition 493
- cavity 512, 544
- cavity lifetime 544
- Cavity QED 375

- cavity QED 466
- Cavity QED with ions 442
- CD-decomposition of unitary operators 373
- channel
 - binary symmetric 8
 - dephasing 106
 - depolarizing 106
 - discrete 4
 - noiseless 4
 - noisy 4
 - product 107
- channel capacity
 - discrete memoryless 8
 - discrete noiseless 4
 - quantum 108
- channel noise 275, 505
- Characteristic function 44
- characteristic function 150
- charge qubit 481, 494, 496
- charge-box qubit 469
- chord 472
- Cirac–Zoller ’95 395
- Cirac–Zoller gate 436
- circuit theory 472
- Classical Gaussian noise 48
- Clauser, Horne, Shimony, and Holt (CHSH)
 - inequality 136
- Clifford 249
- Clifford group 370
- Cluster state 249, 360
- cluster state 194
- CNOT gate 494, 495, 542
- code
 - block 10
 - CSS 116
 - dual 13
 - Hamming 14
 - quantum 108
 - rate 10
 - repetition 10
 - stabilizer 117
- coherent attack 277
- coherent quantum control 399
- coherent spectroscopy 488
- coherent spin state 519, 525
- Coherent state 43
- coherent state 579
- Coherent states 45
- coherent superposition 542
- coincidence(s) 261
- collective attack 277
- Coloring 25
- commutation relation 150, 298
- commutation relations
 - angular momentum 517
- commutator 154
- Complete positivity 42
- completely positive map
 - Gaussian 529
- composability 275
- Composite phase gate 435
- composite system 256
- Compositeness 24
- Composition 42
- Concurrence 247
- conditional entropy 7, 169
- conditional variance 267
- configuration interaction (CI) 465
- connection 507
- continuous variable quantum communication
 - 297
- continuous variables 147, 297
- continuous variables, CV 263, 264
- control theory 487, 490
- controlled phase flip (CPF) 453, 454, 456, 467
- controlled–not operation 187
- convex roof construction 170
- Cooper pair boxes 550
- correlation matrix 150
- correlation operator 186, 194
- coset 487, 493
- coset leader 15
- Coulomb interaction 458–460, 462–464
- coupling topology 492–494, 496
- criterion 154
 - Duan’s inseparability 154, 155
 - npt 156
 - partial transpose 155
 - Peres-Horodecki 156
 - Simon’s inseparability 157
- cross norm 173
- cryogenic environment 539
- cryptography 30
- CSIGN (controlled Sign gate) 357
- CSS code 116
- current fluctuations 475
- current–voltage relations (CVRs) 473

- Decoherence 323
- decoherence 529, 538, 543
- decoherence time T_2 458, 467, 469, 470, 474
- defect mode 564
- DEJMPS protocol 188
- Delft qubit 475
- dense-codeable (DC) states 141
- density operator 485
 - thermal 485
- dephasing channel 106
- depolarization 186
- depolarizing channel 106
- depumping rate 520
- Deutsch's algorithm 88
- Deutsch–Josza Algorithm 90
- Deutsch–Jozsa algorithm 482, 486, 487, 492, 495
- dipole approximation 556
- dipole–dipole interaction 412
- dipole-blockade 413
- discrete log 97
- discrete variables, DV 264
- Displacement operator 44
- displacer 302
- distillability 197
- distillable entanglement 165, 181
 - Rains' bound 172
- distillation 177
- divide-and-conquer 20
- double layer structure 476
- drift term 488
- dual code 13
- dual-homodyne detector 303
- dual-rail encoding 352
- Duan separability criterion 525
- dynamical trapping, Paul trap 425
- eavesdropping 68, 272, 277
- efficiency 259
- eigenvalue 331
- eigenvector 331
- Einstein locality assumption 136
- Einstein Podolsky Rosen argument 135
- Einstein–Podolski–Rosen 541
- electromagnetic field
 - in photonic crystal 564
 - in spherical cavity 558
- Electron shelving 424
- electron spin resonance 481
- electron spin resonance (ESR) 459, 467
- element distinctness 100
- encoded operator 113
- encoding 456
- Energy constraint 39
- ensemble quantum computing 481, 486, 495
- ensemble states 495
- entangled state 123, 525
 - of atomic ensembles 525
- entanglement 67, 147, 177, 256
 - bipartite 147
 - two-party 147
 - witness 154
- entanglement cost 165
- entanglement criteria 125
- entanglement fidelity 107
- entanglement measures
 - additivity 170
 - additivity on pure states 168
 - asymptotic continuity 168
 - axioms for 167
 - convex roof construction 170
 - cross norm measure 173
 - distillable entanglement 165
 - entanglement cost 165
 - entanglement monotones 167
 - entanglement of formation 169
 - entropy of entanglement 166, 168
 - extremality of distillation and cost 169
 - logarithm of the negativity 171
 - norm based monotones 172
 - ordering of 168
 - regularization 169, 170
 - relative entropy of entanglement 170
 - robustness of entanglement 172
 - squashed entanglement 173
 - uniqueness on pure states 168
- Entanglement monotones 246
- entanglement of distillation 181
- entanglement of formation 169
 - additivity 170
 - strong superadditivity 170
- entanglement pumping 188
- entanglement purification 177
- entanglement swapping 507, 532
- Entanglement witness 245
- entanglement witness
 - decomposable 129
 - nondecomposable (nd-EW) 129

- entanglement witness (EW) 129
- entanglement-based QKD 290
- entropy
 - conditional 7
 - entropy of entanglement 166, 168
 - joint 7
 - Shannon 5
- entropy function 9
- entropy of entanglement 166, 180
- EPR 147, 152
 - pair 255, 258, 260
 - particle 258
- EPR entangled state 525
- error
 - bit-flip 110
 - sign-flip 110
- error basis 109
- error model 198
- error operator 106
- error syndrome 13
- error threshold 204
- error weight 109
- Eulerian path 18
- exchange coupling J 452, 456, 459, 462, 464
 - anisotropic 454
 - antiferromagnetic 458, 462
 - ferromagnetic 462
 - Ising 454
 - transverse (XY) 454
- exchange-only quantum computing 457
- expectation-value quantum computer 482
- experimental control 488, 496
- extension field 11

- Fabry-Perot 544
- factoring 93
- Factorization 29
- Fast Fourier transform 94
- feed forward 303
- Fermi's Golden rule 561
- fiber-based QKD. 286
- fidelity 186, 259–260, 542
 - entanglement 107
- field
 - extension 11
 - prime 11
- field-ionization 539
- filtering 184
- Filtering operation 239

- five-qubit NMR quantum computer 484
- flat-continuum approximation 561
- flux qubit 469, 475, 481
- Free-space QKD 289
- full controllability 482, 483
- fully entangled 240
- fully separable 243
- fundamental loop 473
- Fusion operations on graph states 375

- gate complexity 492
- Gaussian operations 151
- Gaussian states 45, 147, 149, 151
- Gaussian transformations 300
- generator matrix 13
- geodesic 487, 494
- geodesics
 - Riemannian 493
 - sub-Riemannian 493
- geometric control 481, 487, 494
- Geometric measure of entanglement 247
- geometric phase 382
- Geometric phase gate 440
- GHZ state 181
- Global entanglement 247
- global fidelity 55
- Gottesman/Chuang trick 349
- gradient flow 487–491, 495
- GRAPE algorithm 489, 491
- graph 472
- Graph Isomorphism 30
- graph isomorphism 97
- Graph state 360
- graph state 194
- Grover's Algorithm 98
- Grover's search 98

- Hadamard gate 88
- Hahn–Banach theorem 128
- Hamiltonian path 22
- Hamming code 14
- Hamming distance 10
- Hamming weight 10
- Hanbury Brown and Twiss 547
- Hartree-Fock 465
- hashing 190, 196, 201
- hashing inequality 169
- Heisenberg limit 577
- Heisenberg model 452

- Heisenberg picture 518
- Heisenberg–Langevin equations 521
- Heitler–London approximation 461
- hidden subgroup problem 97, 492
 - abelian 492
- hidden translation problem 97
- hidden variables 136
- high-finesse cavity 549
- Hilbert space 128
- History of quantum computing 423
- Holevo bound 138
- holonomy 383
- homodyne detection 151, 303
- homodyne method 543
- Hubbard model 406, 461, 464
 - derivation 406
 - extended 464
 - Mott insulator 401
 - offsite interaction 406
 - onsite interaction 408
 - superfluid 401
 - tunneling 407
 - tunneling matrix elements 406
- Huffman coding 6
- Hund–Mulliken approximation 461
- hybridization 461, 462, 465
- hyperplane 129
- Identity 316
- IIIa: def:3 127
- impedance $Z(\omega)$ 472, 475
- incomparable states 164
- individual attack 277
- inseparability 155
- inseparable 154
- instance 17
- intensity correlation 547
- interaction phase 411
- Interference 323
- interferometer 576
- ion
 - delta kick 400
 - internal states 393
 - motional states 392
 - phase gate 395
 - quantum control gate 397
 - single qubit gate 394
 - state dependent interaction 395
 - trapping 391
 - two-qubit gate 395
- Ising interaction 483, 489, 492, 493, 496
- Jamiołkowski isomorphism 134
- Jaynes principle 47
- Jaynes–Cummings Hamiltonian 518
- Jaynes–Cummings–Paul model 555, 563
- joint entropy 7
- Josephson device 481, 494, 496
- Josephson junction 469
 - unintended 476
- k-SAT 27
- Königsberg bridges 17
- kinematic phases 411
- Kirchhoff’s laws 473
- KLM scheme (Knill–Laflamme–Milburn) 349
- Kraus operator 239
- Kraus operators 106
- Lamb shift 557, 567
- Lamb–Dicke factor 432
- Lamb–Dicke limit 393
- Landau symbols 19
- Langevin stochastic forces 521
- laser-cooling 544
- leakage 471
- Lie algebra 483, 490, 493, 494, 496
- Lie-algebra 492
- light force 549
- light source 546
- light–atoms interface 515
- line defect 564
- Linear ion crystal 429
- Linear ion trap 427
- linear map 131
- Linear optical quantum computation 375
- linear optics 352
- linear spin chain 493
- local oscillator 520
- Localizable entanglement 241
- LOCC 161, 162, 179
 - asymptotic transformations 164
 - single copy transformations 163
- logarithm of the negativity 171
- logical Heisenberg picture 366
- logical qubit 112
- long distance communication 308

- Lossy channel 48
- lossy channel 278
- Mach–Zehnder interferometer 323, 576
- macroscopic 451, 469
- macroscopic superposition 417
- magnetic resonance 481
- majorization 127, 163
- majorization criterion 127
- map 131
 - completely positive 132
 - positive (PM) 131
- master equation 474
- Matrices
 - Pauli 332
 - Stochastic 316, 325
- matrix
 - generator 13
 - parity check 13
- Maximal connectedness 241
- maximally entangled states 162
- Maxwell–Bloch equations 518
- Measurement 334
- measurement
 - decoherence in flux qubit 477
 - exchange 465
 - single spin 467
 - spin decoherence time 458, 467
 - spin relaxation time 467
- Metrology 249
- microcavities 466
- micromaser 540
- microscopic 451
- millenium problems 29
- minimum distance 10
 - quantum 113
- Minimum Spanning Tree 32
- mixed state entanglement 181
- Mixing 40
- modes 148
 - bosonic 147
 - optical 148
- momentum 148, 151
- Monogamy of entanglement 241
- motional sideband 394
- multipartite pure state entanglement 180
- multiparty entanglement purification 194
- multiply-controlled NOT gate 493
- mutual information 7
- negative partial transposition (NPT) 126
- negativity 171
- network complexity 481, 493, 495, 496
- network graph 472
- NMR quantum computer 484, 487
- NMR quantum computing 495
- no-cloning theorem 53, 109
- node 472
- noiseless coding theorem 6
- noisy apparatus 197
- noisy coding theorem 8
- noisy operation 198
- Non Abelian Quantum Fourier transform 97
- non-Gaussian transformations 303
- noncloning theorem 259
- nondeterministic polynomial 22
- nonlocality 257, 541
- nonunity gain teleportation 267
- Normal mode decomposition 47
- NP 22
 - NP-complete 28
 - NP-hard 34
- NPT 183
- NSS (nonlinear-sign-shift gate) 357
- Number states 43
- occupation-number qubit 351
- one-time pad 271
- one-way function 30
- One-way quantum computation 359
- open system 549
- operator 148
 - annihilation 148
 - creation 148
 - density 149, 154
 - Hermitian 154
 - symmetrized 149
- operator $>$ super 131
- operator controllability 483
- optical density 520
- optical experiments 544
- optical Feshbach resonance 418
- Optical lattice 374
- optical lattice 401
 - blue detuning 405
 - controlled coherent collision 410
 - geometry 403
 - impurity 417
 - loading 408

- defect suppression 408
 - irreversible scheme 408
- maximally entangled state 415
- red detuning 405
- single qubit gate 409
- site offset 403
- spontaneous emission 405
- state dependence 404
- state dependent interaction 412
- state selective movement 405
- two qubit gate 410
- optical parametric amplification 148
- optical potential 401
- optical qubits 351
- optimal control 494, 495
- optimal control theory 481
- optimization 31
- Overhauser field 468
- parabolic confinement 460
- parallel transport 382
- parametric down-conversion 261
- parametric fluorescence 547
- parity check matrix 13
- partial transposition 125, 171, 183
- partial transposition criterion 126
- Passive transformations 46
- Paul trap, stability diagram 427
- Pauli group 116, 248
- Pauli principle 459, 463
- PBG materials *see* photonic crystals 564
- period finding 93
- Phase conjugation 49
- phase covariant cloning 62
- phase distribution 543
- phase insensitive amplifier 300
- phase qubit 470
- phase sensitivity 577
- phase shifter 300
- Phase space 43
- phase space 579
- phase-space 149, 155
 - displacements 150
 - variables 149
- phonons 468
- photon 512
- photon antibunching 546
- photon bunching 546
- photon number 148, 152
- photon number basis 148
- photon statistics 546
- photon-number splitting attack 278
- photonic band-gap 550
- photonic bandgap materials *see* photonic crystals 564
- photonic crystals 564
 - anisotropic model 565
 - isotropic model 565
 - Lorentzian models 566
- physical qubit 112
- point defect 564
- polynomial reduction 27
- Pontryagin's maximum principle 489–491
- position 148, 151
- positive partial transposition (PPT) 126
- PPT 183
- Prim's algorithm 32
- Primality 24
- prime field 11
- privacy amplification 276
- probabilistic cloning 68
- probabilistic gates 356
- Probability
 - Amplitudes 323, 325
 - Axioms 317
- product channel 107
- Product states 240
- projective special unitary group 490, 491
- Proof Checking 30
- Proof Existence 31
- pseudo-pure state 482, 485, 486
- pseudo-spin system 481, 494, 496
- pseudospin 452, 470
- pure dephasing time T_ϕ 474
- pure state 485, 495
- pure state entanglement 179
- Pure states 40
- purification loop 508
- purification step 185
- QECC 108
- QND interaction 520
- quadratic interactions 147
- quadrature components 298
- quadrature operators 519
 - of atomic ensemble 519
- quadrature-phase amplitudes 264
- quadratures 148, 152

- quantum 147
 - harmonic oscillator 148
 - information applications 147
- Quantum algorithm for binary search 87
- Quantum algorithm for graph problems 87
- Quantum channel 41
- quantum channel 505
- quantum channel capacity 108
- quantum cloning 532
 - coherent states 533
 - into atomic memory 533
- quantum code 108
- quantum communication 178, 202, 505
- Quantum computation
 - Heisenberg picture 366
 - Linear optical 375
 - Measurement-based 359
 - One-way 359
- quantum control 481, 489, 495, 496
- quantum cryptography 286
- quantum dense coding 138, 292, 305
- quantum dot 512
- quantum dots 451, 452, 459
- quantum error correction code (QECC) 275
- Quantum Fourier sampling 92
- Quantum Fourier transform 93, 492
- quantum gate
 - local 483
 - universal 483
- quantum interface 538
- Quantum Interferometry 575
- quantum key distribution 275, 306
- quantum memories 549
- quantum memory 526
 - retrieval 528
 - storage protocol 526
- quantum messengers 549
- quantum noise 520
- quantum non demolition 542
- quantum nondemolition measurements 520
- Quantum operation 41
- quantum phase gate 541
- quantum repeater 505
- quantum repeaters 526
- quantum state detection 424
- quantum teleportation 531
 - of light onto atoms 531
- quantum walks (discrete and continuous) 100
- quantum-beat 548
- Quasifree states 45
- qubit 256, 259
 - atomic 255
 - logical 112
 - material(atomic)
 - embedded in photonic crystal 566
 - embedded in spherical cavity 556
 - quantum electrodynamics of 555
 - physical 112
- Rabi
 - frequency 563
 - oscillations 555, 563
- Rabi frequency 432, 546
- Rabi frequency, Carrier 432
- Rabi frequency, sideband 432
- Rabi pulse 541
- Rains'bound 172
- Raman process 546
- Raman transition 434
- Ramsey experiment 470
- reachability set 483
- realtime measurements 544
- receiver 4
- recoil kicks 549
- recurrence protocol 185, 187, 188, 194
- Redfield equation 474
- reduction 27
- reduction criteria 184
- reduction from factoring to period finding 93
- regularization 169, 170
- relative entropy
 - of entanglement 170
 - regularized 171
 - subadditivity 171
- Relative entropy of entanglement 247
- relaxation time T_1 467, 474
- repeater 505
- resolvent operator 566
- resources 509
- retarded time 518
- reversible classical computation 88
- Reversible Computation 317
- Riemannian symmetric space 493
- Robustness 241
- robustness of entanglement 172
- rotating-wave approximation 557
- RSA 30
- Rydberg atoms 538

- Satisfiability 27
- scalability 451, 485–487, 492, 495
- Schmidt decomposition 124, 148, 152, 179
- Schmidt measure 240, 246
- Schmidt normal form 238
- Schmidt rank 246
- Schrödinger cat 543
- Schrödinger cat state 299
- secure state distribution 203
- Segmented ion trap 444
- self-adjoint map 131
- self-homodyning 520
- separability class 243
- separable 154
- separable state 125
- separable states 162
- Shannon entropy 5
- Shannon's Theorem 347
- Shor's algorithm 94
- shrinking factor 60, 66
- sidebands 521
- sifting 274
- sign-flip error 110
- signal transfer 267
- Simon's algorithm 92
- single-atom transistor 417
- single-mode squeezer 300
- single-photon source 548
- singlet–triplet crossing 462
- special unitary group 490, 491
- spectral function $J(\omega)$ 475
- spin
 - decoherence time 467, 469
 - electron 452, 458
 - nuclear 468
 - relaxation time 467
- spin cluster qubits 458
- spin–orbit coupling 455, 458, 468
- spin-1/2 541
- Split 240
- split 243
- spontaneous emission 540, 546, 555
 - in photonic crystals 566
 - in spherical cavities 556
- square-root of SWAP gate 453, 456
- squashed entanglement 173
- squeezed state 151, 524
 - of atomic ensemble 524
 - one-mode 151, 153
 - two-mode 147, 152, 153, 155, 157
- squeezed states 581
- squeezed vacuum state 299
- squeezed vacuum states 581
- squeezing 148, 151, 152
- stabilizer code 117
- Stabilizer Formalism 365
- stabilizer group 116, 248
- standard array 15
- standard form 153, 157
- Stark effect 539
- Stark eigenstate 412
- state estimation 64
- State space 40
- state transformation 179
- state-dependent cloning 54
- States 40
- Stokes vector 517
- strip-line resonators 550
- strong coupling 544
- strong phase reference pulse 281
- super additivity 108
- superconducting 538
- superconducting qubit 469
- superradiance 549
- supporting hyperplane 245
- symplectic matrix 150
- tangle 247
- technical noise 520
- Teleportation 443
- teleportation 255–268
 - unconditional 262
- Teleportation algorithm 443
- tensor product 318, 343
- thermal stat 495
- thermal state 152, 485, 486
- threshold 200
- time complexity 481, 492, 493, 495, 496
- time-optimal 483, 487, 492–496
- time-symmetric pulses 455
- Toffoli 342
- TOFFOLI-gate 494
- trace distance 165
- transformations 151
 - active 151
 - Gaussian unitary 151
 - linear 151
 - passive 151

- symplectic 151
- transmitter 4
- Traveling Salesman Problem 33
- tree 472
- Two qubit quantum gate 434
- two-colorable graph 194
- two-level system 556
- two-mode squeezer 300
- two-mode squeezing 530
- uncertainty relation 150
 - N -mode 150
 - Heisenberg 150
- unconditional security 277
- Unitarity 325, 331
 - Special 331
- Unitary operation 41
- unitary orbit 483, 487, 488
- unity gain teleportation 267
- universal cloning 63
- universal gate 496
- universal gate set 87, 454, 455, 457, 466
- universal quantum simulators 413
 - Heisenberg Hamiltonian 415
 - Ising interaction 414
 - one-qubit term 414
 - quantum phase transition 416
- two-qubit term 414
- vacuum Rabi oscillation 541
- vacuum state 299
- vacuum-Rabi frequency 546
- vacuum-Rabi period 544
- vacuum-Rabi splitting 546
- Vernam cipher 271
- Vibrational eigenmodes of an ion crystal 430
- visibility 471
- von Neumann entropy 152
- Wannier function 402
- Werner state 187
- Weyl correspondence 149, 150
- Weyl operator 44
- Wigner function 44, 148, 149, 152, 155, 298, 543
- words
 - ϵ -typical 6
- worst case 19
- XOR gate 453, 455, 457, 467
- yield 182, 197
- Zeeman coupling 452, 459, 461, 468, 469
- Zeeman level 546

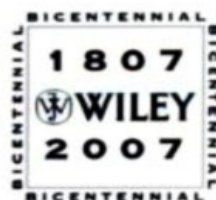
Quantum Information Processing is a young and rapidly growing field of research at the intersection of physics, mathematics, and computer science. Its ultimate goal is to harness quantum physics to conceive - and ultimately build - "quantum" computers that would dramatically overtake the capabilities of today's "classical" computers. One example of the power of a quantum computer is its ability to efficiently find the prime factors of a large integer, thus shaking the supposedly secure foundations of standard encryption schemes. This comprehensive textbook on the rapidly advancing field introduces readers to the fundamental concepts of information theory and quantum entanglement, taking into account the current state of research and development. It thus covers all current concepts in quantum computing, both theoretical and experimental, before moving on to the latest implementations of quantum computing and communication protocols. With its series of exercises, this is ideal reading for students and lecturers in physics and informatics, as well as experimental and theoretical physicists, and physicists in industry.



Dagmar Bruff graduated at RWTH University Aachen, Germany, and received her PhD in theoretical particle physics from the University of Heidelberg in 1994. As a research fellow at the University of Oxford she started to work in quantum information theory. Another fellowship at ISI Torino, Italy, followed. While being a research assistant at the University of Hannover she completed her habilitation. Since 2004 Professor Bruff has been holding a chair at the Institute of Theoretical Physics at the Heinrich-Heine-University Düsseldorf, Germany.



Gerd Leuchs studied physics and mathematics at the University of Cologne, Germany, and received his PhD in 1978. After two research visits at the University of Colorado in Boulder, USA, he headed the German gravitational wave detection group from 1985 to 1989. He then became technical director at Nanomach AG in Switzerland. Since 1994 Professor Leuchs has been holding the chair for optics at the Friedrich-Alexander-University of Erlangen-Nuremberg, Germany. His fields of research span the range from modern aspects of classical optics to quantum optics and quantum information. Since 2003 he has been Director of the Max Planck Research Group for Optics, Information and Photonics at Erlangen.



ISBN 978-3-527-40527-5



ISBN-10: 3-527-40527-5

www.wiley-vch.de

9 783527 405275