

QUANTUM INFORMATION WITH CONTINUOUS VARIABLES

Quantum Information with Continuous Variables

Edited by

SAMUEL L. BRAUNSTEIN

*School of Informatics,
University of Wales, Bangor, United Kingdom*

and

ARUN K. PATI

*Institute of Physics, Orissa, India
and
Theoretical Physics Division,
BARC, Mumbai, India*



KLUWER ACADEMIC PUBLISHERS
DORDRECHT / BOSTON / LONDON

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN 978-90-481-6255-0

Published by Kluwer Academic Publishers,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

Sold and distributed in North, Central and South America
by Kluwer Academic Publishers,
101 Philip Drive, Norwell, MA 02061, U.S.A.

In all other countries, sold and distributed
by Kluwer Academic Publishers,
P.O. Box 322, 3300 AH Dordrecht, The Netherlands.

ISBN 978-90-481-6255-0
DOI 10.1007/978-94-015-1258-9

ISBN 978-94-015-1258-9 (eBook)

Printed on acid-free paper

Cover illustration:
reprinted with permission from Nature [Nature 413, 400–403 (2001)]
Copyright (2001) Macmillan Publishers Ltd.
Softcover reprint of the hardcover 1st edition 2001

All Rights Reserved
© 2003 Kluwer Academic Publishers and copyright holders
as specified on appropriate pages within.
No part of this work may be reproduced, stored in a retrieval system, or transmitted
in any form or by any means, electronic, mechanical, photocopying, microfilming, recording
or otherwise, without written permission from the Publisher, with the exception
of any material supplied specifically for the purpose of being entered
and executed on a computer system, for exclusive use by the purchaser of the work.

*Dedicated to
Netta, Rashmi
and our parents*

Contents

Preface	xi
About the Editors	xiii
Part I Quantum Computing	
1. Quantum computing with qubits <i>Samuel L. Braunstein and Arun K. Pati</i>	3
2. Quantum computation over continuous variables <i>Seth Lloyd and Samuel L. Braunstein</i>	9
3. Error correction for continuous quantum variables <i>Samuel L. Braunstein</i>	19
4. Deutsch-Jozsa algorithm for continuous variables <i>Arun K. Pati and Samuel L. Braunstein</i>	31
5. Hybrid quantum computing <i>Seth Lloyd</i>	37
6. Efficient classical simulation of continuous variable quantum information processes <i>Stephen D. Bartlett, Barry C. Sanders, Samuel L. Braunstein and Kae Nemoto</i>	47
Part II Quantum Entanglement	
7. Introduction to entanglement-based protocols <i>Samuel L. Braunstein and Arun K. Pati</i>	59
8. Teleportation of continuous quantum variables <i>Samuel L. Braunstein and H. Jeffrey Kimble</i>	67

9. Experimental realization of continuous variable teleportation <i>Akira Furusawa and H. J. Kimble</i>	77
10. Dense coding for continuous variables <i>Samuel L. Braunstein and H. Jeffrey Kimble</i>	95
11. Multipartite Greenberger-Horne-Zeilinger paradoxes for continuous variables <i>Serge Massar and Stefano Pironio</i>	105
12. Multipartite entanglement for continuous variables <i>Peter van Loock and Samuel L. Braunstein</i>	111
13. Inseparability criterion for continuous variable systems <i>Lu-Ming Duan, Géza Giedke, J. Ignacio Cirac and Peter Zoller</i>	145
14. Separability criterion for Gaussian states <i>Rajiah Simon</i>	155
15. Distillability and entanglement purification for Gaussian states <i>Géza Giedke, Lu-Ming Duan, J. Ignacio Cirac and Peter Zoller</i>	173
16. Entanglement purification via entanglement swapping <i>Steven Parker, Sugato Bose and Martin B. Plenio</i>	193
17. Bound entanglement for continuous variables is a rare phenomenon <i>Pawel Horodecki, J. Ignacio Cirac and Maciej Lewenstein</i>	211

Part III Continuous Variable Optical-Atomic Interfacing

18. Atomic continuous variable processing and light-atoms quantum interface <i>Alex Kuzmich and Eugene S. Polzik</i>	231
---	-----

Part IV Limits on Quantum Information and Cryptography

19. Limitations on discrete quantum information and cryptography <i>Samuel L. Braunstein and Arun K. Pati</i>	269
20. Quantum cloning with continuous variables <i>Nicolas J. Cerf</i>	277
21. Quantum key distribution with continuous variables in optics <i>Timothy C. Ralph</i>	295
22. Secure quantum key distribution using squeezed states <i>Daniel Gottesman and John Preskill</i>	317

23. Experimental demonstration of dense coding and quantum cryptography with continuous variables <i>Kunchi Peng, Qing Pan, Jing Zhang and Changde Xie</i>	357
24. Quantum solitons in optical fibres: basic requisites for experimental quantum communication <i>G. Leuchs, Ch. Silberhorn, F. König, P. K. Lam, A. Sizmann and N. Korolkova</i>	379
Index	423

Preface

Quantum information has become a flagship of interdisciplinary research in recent years, sweeping physicists from a variety of disciplines, as well as computer scientists and mathematicians. It all started with the realization that the principles of quantum theory open new avenues of information processing capabilities which are unavailable in the classical world. Primarily, the discovery that quantum entanglement can be put to use has led to a watershed of activity towards the eventual implementation of quantum computation and quantum cryptography. This was naturally accompanied by efforts to place fundamental quantum limits on information processing. Today, real-world applications of quantum-information technologies seem closer and more tangible than ever.

The field of quantum information has typically concerned itself with the manipulation of discrete systems such as quantum bits, or “qubits.” However, many quantum variables, such as position, momentum or the quadrature amplitudes of electromagnetic fields, are continuous. Quantum information processing with continuous variables is the subject of this volume.

Initially, quantum information processing with continuous variables seemed daunting at best, ill-defined at worst. The first real success came with the experimental realization of quantum teleportation for optical fields. This was soon followed by a flood of activity, to understand the strengths and weaknesses of this type of quantum information and how it may be processed. The next major breakthrough was the successful definition of a notion of universal quantum computation over continuous variables, suggesting that such variables are as powerful as conventional qubits for any class of computation.

In some ways continuous-variable computation may not be so different than qubit-based computation. In particular, limitations due to finite precision make quantum floating-point operations, like their classical counterparts, effectively discrete. Thus we might expect a continuous-variable quantum computer to perform no better than a discrete quantum computer. However, for some tasks continuous-variable quantum computers are nonetheless more efficient. Indeed,

in many protocols, especially those relating to communication, they only require *linear* operations together with classical feed-forward and detection. This together with the large bandwidths naturally available to continuous (optical) variables appears to give them the potential for a significant advantage.

Noise is the Achilles' heel of quantum computation, and continuous variables are even more susceptible to noise than discrete variables. Since an uncountably infinite number of things can go wrong with a continuous variable, error correction protocols might be expected to require infinite redundancy. Fortunately, continuous-variable error correction routines exist and require no greater redundancy than protocols for discrete variables. With the problem of noise potentially reduced to manageable proportions, many other hurdles persist, and many more exciting questions remain open. Quantum information with continuous variables continues to be a dynamic and exciting field of ongoing research and development.

In this volume we present important developments in the area of quantum information theory for continuous-variable systems from various leading researchers in the field. Several introductory chapters lay out some of the basics of quantum information theory in terms of the more usual qubits. Each introduction is followed by generalizations to continuous variables. In addition to chapters on quantum computation and quantum teleportation, we have included work on quantum dense coding, quantum error correction, some simple attempts at generalizing quantum algorithms and technologically promising work on quantum cryptography and quantum memory. These results apply to any collection of continuous variables, including phonons, photons, Josephson Junction circuits, Bose-Einstein condensates, etc. Finally, the underlying nature of continuous quantum information is investigated in chapters on quantum cloning and quantum entanglement.

At this juncture, we express our gratitude to Kluwer Academic for allowing us to bring this work to light. We hope that this book offers the reader a rigorous introduction to continuous-variable quantum information and some thought-provoking snapshots of recent developments. We sincerely thank all the authors for their contributions. A.K.P. would especially like to express his thanks to Prof. R. K. Choudhury, Director of the Institute of Physics, in Orissa, India, for his encouragement. Finally, both authors appreciate the support provided by the University of Wales, Bangor, throughout this endeavor.

SAMUEL L. BRAUNSTEIN

ARUN K. PATI

About the Editors

Samuel L. Braunstein is a Professor at the University of Wales, Bangor, where he has taught since 1997. He is a recipient of the prestigious Royal Society-Wolfson Research Merit Award and was awarded the honorary title of 2001 Lord Kelvin Lecturer. Before joining the University of Wales, he held a German Humboldt Fellowship (spent at the University of Ulm). He is editor of two books *Quantum Computing* and *Scalable Quantum Computing* and serves on the editorial board of the journal *Fortschritte der Physik*. He has initiated and is a Founding Managing Editor of *Quantum Information and Computation* – the first journal dedicated specifically to this field.

Arun K. Pati is a Visiting Scientist in the Institute of Physics, Bhubaneswar, Orissa, India since 2001. He has been a Scientific Officer in the Theoretical Physics Division, BARC, Mumbai since 1989. His research interests include Quantum Theory, Foundations, and Quantum Information and Computation. He is a recipient of the Indian Physics Association NSS Memorial Award for the year 2000 and the Indian Physical Society Award for Young Physicists for the year 1996. He was an Associate of the Indian Academy of Science, Bangalore from 1998-2001. Presently he is an Associate at the Center for Philosophy and Foundation Science, New Delhi and an Honorary Research Fellow at the University of Wales, Bangor, United Kingdom.

I

QUANTUM COMPUTING

Chapter 1

QUANTUM COMPUTING WITH QUBITS

Samuel L. Braunstein

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

Arun K. Pati

Institute of Physics, Bhubaneswar-751005, Orissa, INDIA

Theoretical Physics Division, BARC, Mumbai, INDIA

akpati@iopb.res.in

Abstract We briefly give an introduction to quantum computing with qubits.

This book will introduce the reader to the area of quantum information processing with continuous variables. However, to put it into some context with the “conventional” approach to quantum computing with qubits we shall give a brief introduction to its basic principles skipping all details. Briefly, we will touch on notions of bits, qubits, quantum parallelism, and quantum algorithms such as the Deutsch-Jozsa, the Shor factoring problem, and the Grover quantum search.

Quantum information theory is a marriage between two scientific pillars of modern science, namely, quantum theory and classical information theory. Quantum theory as developed by Planck, Einstein, Schrödinger, Dirac, Heisenberg and many others in the early part of the last century is one of the finest theories that explains phenomena ranging from molecules to electrons, protons, neutrons and other microscopic particles. The mathematical theory of classical information was put forth by Shannon in the mid part of the last century. Whatever revolution in information technology we see at present is partly due to the ground breaking work by Shannon, Turing, Church and others.

When the ideas from information theory are carried over to quantum theory there emerges a revolution in our ability to process information. Ultimately, the basic ways of expressing and manipulating information require physical states

and processes. In quantum theory we know that physical processes are fundamentally different than those of classical physics. Therefore manipulation of information based on quantum physical processes has also to be fundamentally different than their classical counterparts. It was first realised by Feynman that simulating quantum systems on a classical computer would be very inefficient [1]. However, if one utilizes quantum systems than one can do much more. For this reason, quantum information is distinguished from conventional classical information.

1. QUANTUM COMPUTATION

The physics of information and computation are intimately related. Information is encoded in the state of a physical system, whereas computation involves the processing of this information through actions on the physical system. This processing must obey physical law. Therefore, the study of information and computation are linked through the study of underlying physical processes. If the physical processes obey the rules of classical physics, the corresponding computation is dubbed “classical.” If on the other hand, the underlying processes are subjected to quantum mechanical rules, the resulting computation will be called “quantum computation.” The logic that lies at the heart of conventional computers and quantum computers is therefore fundamentally different. Quantum computation is a particular way of processing information which utilizes the principles of the linearity of quantum mechanics, out of which comes quantum superposition, quantum entanglement and quantum parallelism. This was first suggested by Deutsch [2].

In a conventional computer information is stored as binary digits (bits) usually (logically) labeled 0 and 1. To represent a bit, one may use any physical system that one likes provided it allows two distinct states. Two bits of information can be stored in any system allowing $2^2 = 4$ possible distinct states. Similarly, n bits of information may be represented in any system capable of providing 2^n distinct states. In each case, there is only *one* configuration at a time of the logical bits (e.g., 110 for 3 bits). Information stored in these binary digits can be manipulated using elementary logic gates that obey Boolean algebra. For example, in a conventional classical computer one can manipulate information using sequence of logical operations such as AND, OR, NOT, and XOR gates. These gates may be built into circuits constructing any possible Boolean functions [3].

1.1 QUBITS

Let us represent a bit, 0 or 1, by saying that the spin of a neutron is up or down, or we could say an atom is in ground or in an excited state, or a photon is horizontally or vertically polarized. All these systems are examples

of two-state quantum systems because the two states are orthogonal and hence logically distinct from each other. When a quantum system is in a given basis state it may be said to carry classical information. However, quantum theory also allows states which are in linear superpositions of these basis states. If we use the logical label for each of the basis states then the most general pure quantum state for a “two-state” system is given by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle , \quad (1.1)$$

for some complex numbers α and β which satisfy $|\alpha|^2 + |\beta|^2 = 1$. According to Dirac a quantum state ψ is denoted by a “ket” $|\psi\rangle \in \mathcal{H} = \mathbb{C}^2$ (a two-dimensional Hilbert space). Such a system contains a quantum bit or “qubit” of information [4].

A single qubit allows two inputs to be stored (and possibly processed) simultaneously. As we add more qubits the number of simultaneous possibilities grows very quickly. For example, for two qubits, which have logically distinct states labeled by 00, 01, 10 and 11 the most general state may be written as a superposition of these four possibilities

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \in \mathcal{H} = \mathbb{C}^4 . \quad (1.2)$$

For n qubits with 2^n possible distinct logical basis states the most general pure state will take the form of a simultaneous superposition of this exponential number of possibilities, such as

$$\sum_{x=0}^{2^n-1} c_x|x\rangle . \quad (1.3)$$

This ability for quantum states to simultaneously represent (and process) an exponential number of “logical states” demonstrates the fundamental difference between classical and quantum computers.

In the case of a composite system of two or more qubits (or any kind of subsystems) as seen in Eq. (1.3), the result of this superposition can give rise to *quantum entanglement* (inter-twinedness). If a pure composite state cannot be written as a product of individual states for each subsystem then it is an entangled state. The word entanglement neatly encapsulates the novel non-classical correlations accessible to quantum systems, yet which cannot be described within any local realistic model since they allow for the violation of Bell inequalitiesinequality,Bell [5]. What this means is that one cannot attribute definite properties to the individual subsystems of an entangled state. Charlie Bennett’s metaphor for a pair of entangled particles is that they are to be likened to a pair of lovers. If a pair of particles are entangled, then a measurement of one, will, in some sense, instantaneously affect the other no matter how far apart they lie.

2. QUANTUM PARALLELISM AND ALGORITHMS

It is possible to design new types of logic gates, generalizing those that work for classical bits, that act on qubits. These quantum gates may also be combined into circuits in such a way as to allow the most general (unitary) transformations between quantum states. We may think of these circuits as performing particular quantum algorithms for a given input. Because more general transformations than simple Boolean functions are available, quantum superpositions may be created using these quantum circuits. This allows for the ability of quantum computers to perform many computational tasks in parallel. Further, because the potential amount of parallelism grows exponentially with the number of qubits, this feature cannot be efficiently simulated in any conventional computer, no matter how parallel its architecture.

To illustrate quantum parallelism, imagine that we had access to a black box that computes a given function $f(x)$ from an input x of n qubits ($x = 0, 1, \dots, 2^n$). Quantum mechanically because one can create a superposition of all inputs, one could perform all $N = 2^n$ function evaluations in a single go. Classically, this would require the N separate function evaluations. In particular, one can start by preparing a “register” of n qubits in an equal superposition of all possible bit strings given by

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle . \quad (1.4)$$

Further, we suppose that the function f is evaluated by some unitary operation U_f acting via [2]

$$U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle , \quad (1.5)$$

on any given input x , with the input located in the first register and the output stored in a second register. Then by the linearity of quantum mechanics, the action of U_f on the equal superposition of the input register plus an extra output register will produce

$$U_f : \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle . \quad (1.6)$$

That is, all possible function evaluations have been done in a single step. This massive parallelism comes for free if one could ever build a quantum computer.

Unfortunately, we are unable to extract all this information in a single observation of the resulting quantum state. Instead, we will only be able to *probabilistically* extract the information encoded in a single “branch” or term in this superposition. Naively then the quantum parallelism is all lost at the

stage of measurement. Fortunately, this need not be the case. Instead, by performing a further unitary transformation before the final measurement one may extract some information of this parallel information. Thus, typically algorithms performed on a quantum computer are probabilistic in nature.

Although a quantum computer cannot solve any problem a conventional computer fails at, there are a number of problems that they can solve far more efficiently. Efficiency of a computation is measured by the *computational complexity* which, roughly speaking, is how many steps are required to solve a given problem as a function of the size of the input (specifying the problem). For example, if an input is specified by a single number N , then the size of the input corresponds to the length of this number $L = \log N$. If the computation runs in a number of steps which is a polynomial in L , then the problem is considered tractable. If the number of steps grows exponentially, the problem is considered hard. In recent years there have been three important quantum computational algorithms discovered: the Deutsch-Jozsa algorithm, Shor's algorithm and Grover's algorithm. (For details of these algorithms see Ref. [9].)

- **Deutsch-Jozsa algorithm:** Here one aims to determine some “global” information about a binary function $f(x)$. In particular, we are given a promise that either the function yields a constant (0 or 1) for all inputs, or the function is balanced, with exactly half the outputs 0. We wish to determine whether the function is constant or balanced. For inputs consisting of n bits, $x \in \{0, 1, 2, \dots, 2^n - 1\}$, a conventional computer would take $O(2^n)$ steps to decide. But on a quantum computer, the Deutsch-Jozsa algorithm can tell us the answer in a single evaluation of the function [6]! Thus, to determine the global nature of such a function precisely could be achieved with an exponential speed-up in a quantum computer (however, this exponential gap vanishes if we allow classically probabilistic algorithms).
- **Shor's algorithm:** Here one aims to factorize a composite number x . In general this is believed to be computationally intractable. On a conventional computer the currently best known algorithm takes essentially an exponential number of steps $O(\exp[2L^{1/3}(\log L)^{2/3}])$, $L = \log x$. Shor discovered that a quantum computer can do the job in a polynomial number $O(L^3)$ [7]. For example, to factor a number with 250 decimal digits, an estimate of around 800,000 years has been suggested as required for a large network of currently available classical computers. By contrast, on a quantum computer, this could be done in seconds to hours depending on the computer's clock speed. Shor's landmark work generated wide interest in the field for physicists, computer scientists and mathematicians alike.

- **Grover's algorithm:** In this algorithm one aims to find one particular item from a large unsorted (virtual) database containing N items. Classically, one needs to query $O(N)$ times from the database in order to find a specific marked item. Quantum mechanically, on the other hand, one can complete the search in $O(\sqrt{N})$ steps [8]. More precisely, one models a database by a virtual table or function $f(x)$, $x \in \{0, 1, \dots, N - 1\}$. We are told that $f(x) = 1$ for a single $x = y$ and 0 for all other values. The problem is to find this y . Grover proved that quantum mechanics helps to find the desired item from the virtual database in $O(\sqrt{N})$ steps. This corresponds to a square-root speed-up. Since unstructured searches are so ubiquitous throughout computation, Grover's algorithm has a potentially important role.

These discoveries herald radically new ways of thinking about computation, information, and programming in general. It is worth mentioning that all three of these algorithms have been implemented (though some might say merely simulated) on primitive quantum computers. There have been various proposals for building a quantum computer but a full scale machine appear to be far off. The experimental proposals include isolating and manipulating qubits in ion traps, solid state based devices such as SQUIDS, quantum dots, NMR techniques and many more (see for example Ref. [10]). In part I of this book we shadow many of the developments found in qubit-based quantum computers with analogous work based on quantum continuous variables.

References

- [1] R. Feynman, Found. of Physics **16**, 507 (1986).
- [2] D. Deutsch, Proc. R. Soc. London. A, **400**, 97 (1985).
- [3] G. Boole, *An Investigation of The Laws of Thought* reprinted as (Dover, New York, 1958).
- [4] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
- [5] J. Bell, *Speakables and Unspeakables in Quantum Theory* (Oxford University Press).
- [6] D. Deutsch and R. Jozsa, Proc. R. Society (London) A **439**, 553 (1992).
- [7] P. Shor, in *Proc 35th Annual Symp. on Found. of Comp. Sci.* (IEEE Computer Society Press, 1994).
- [8] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
- [9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
- [10] H. K. Lo and S. L. Braunstein (Eds), *Scalable Quantum Computers* (Wiley-VCH Verlag, Berlin, 2001).

Chapter 2

QUANTUM COMPUTATION OVER CONTINUOUS VARIABLES*

Seth Lloyd

*MIT Department of Mechanical Engineering
MIT 3-160, Cambridge, Mass. 02139, USA
slloyd@mit.edu*

Samuel L. Braunstein

*Informatics, Bangor University, Bangor LL57 1UT, United Kingdom
schmuel@sees.bangor.ac.uk*

Abstract This paper provides necessary and sufficient conditions for constructing a universal quantum computer over continuous variables. As an example, it is shown how a universal quantum computer for the amplitudes of the electromagnetic field might be constructed using simple linear devices such as beam splitters and phase shifters, together with squeezers and nonlinear devices such as Kerr-effect fibers and atoms in optical cavities. Such a device could in principle perform “quantum floating point” computations. Problems of noise, finite precision, and error correction are discussed.

Quantum computation has traditionally concerned itself with the manipulation of discrete systems such as quantum bits, or “qubits” [1, 2]. Many quantum variables, such as position and momentum or the amplitudes of electromagnetic fields, are continuous. Although noise and finite precision make precise manipulations of continuous variables intrinsically more difficult than the manipulation of discrete variables, because of the recent developments in quantum error correction [3, 4, 5] and quantum teleportation [6, 7] of continuous quantum variables, it is worthwhile addressing the question of quantum computation over continuous variables.

*S. Lloyd and S. L. Braunstein, Physical Review Letters **82**, 1784-1787 (1999).
Copyright (1999) by the American Physical Society.

At first it might seem that quantum computation over continuous variables is an ill-defined concept. First consider quantum computation over discrete variables. A universal quantum computer over discrete variables such as qubits can be defined to be a device that can by local operations perform any desired unitary transformation over those variables [1, 2, 8]. More precisely, a universal quantum computer applies “local” operations that effect only a few variables at a time (such operations are called quantum logic gates): by repeated application of such local operations it can effect any unitary transformation over a finite number of those variables to any desired degree of precision. Now consider the continuous case. Since an arbitrary unitary transformation over even a single continuous variable requires an infinite number of parameters to define, it typically cannot be approximated by any finite number of continuous quantum operations such as, for example, the application of beam splitters, phase shifters, squeezers, and nonlinear devices to modes of the electromagnetic field. It is possible, however, to define a notion of universal quantum computation over continuous variables for various subclasses of transformations, such as those that correspond to Hamiltonians that are polynomial functions of the operators corresponding to the continuous variables: A set of continuous quantum operations will be termed universal for a particular set of transformations if one can by a finite number of applications of the operations approach arbitrarily closely to any transformation in the set.

This paper provides necessary and sufficient conditions for universal quantum computation over continuous variables for transformations that are polynomial in those variables. Such a continuous quantum computer is shown to be capable in principle of performing arithmetical manipulations of continuous variables in a “quantum floating point” computation. In principle, a continuous quantum computer could perform tasks that a discrete quantum computer cannot. In practice, noise and finite precision make quantum floating point operations, like their classical counterparts, effectively discrete. A quantum computer that uses continuous variables cannot therefore perform a task that a discrete quantum computer cannot. However, continuous quantum computers may still be able to perform some tasks *more efficiently* than their discrete counterparts. The results derived here apply to any collection of continuous variables, including phonons, photons, Josephson Junction circuits, Bose-Einstein condensates, etc. To be concrete, as results are derived they will be expressed both in terms of abstract continuous variables and in the familiar context of quadrature amplitudes of the electromagnetic field.

Consider a single continuous variable corresponding to an operator X . Let P be the conjugate variable: $[X, P] = i$. For example, X and P could correspond to quadrature amplitudes of a mode of the electromagnetic field (the quadrature amplitudes are the real and imaginary parts of the complex electric field). First investigate the problem of constructing Hamiltonians that correspond to

arbitrary polynomials of X and P . It is clearly necessary that one be able to apply the Hamiltonians $\pm X$ and $\pm P$ themselves. In the Heisenberg picture, applying a Hamiltonian H gives a time evolution for operators $\dot{A} = i[H, A]$, so that $A(t) = e^{iHt}A(0)e^{-iHt}$. Accordingly, applying the Hamiltonian X for time t takes $X \rightarrow X, P \rightarrow P - t$, and applying P for time t takes $X \rightarrow X + t, P \rightarrow P$: the Hamiltonians X and P have the effect of shifting the conjugate variable by a constant. In the case of the electromagnetic field, these Hamiltonians correspond to linear displacements or translations of the quadrature amplitudes.

A simple geometric construction allows one to determine what Hamiltonian transformations can be constructed by the repeated application of operations from some set. Apply the Hamiltonian A for time δt , followed by $B, -A, -B$, each for the same time. Since

$$e^{iA\delta t}e^{iB\delta t}e^{-iA\delta t}e^{-iB\delta t} = e^{(AB-BA)\delta t^2} + O(\delta t^3), \quad (2.1)$$

in the limit that $\delta t \rightarrow 0$, the result is the same as if one had applied the Hamiltonian $i[A, B]$ for time δt^2 . In general, if one can apply a set of Hamiltonians $\{\pm H_i\}$, one can construct any Hamiltonian that is a linear combination of Hamiltonians of the form $\pm i[H_i, H_j], \pm [H_i, [H_j, H_k]]$, etc. [9, 10, 11, 12, 13], and no other Hamiltonians. That is, one can construct the Hamiltonians in the algebra generated from the original set by commutation. This key point, originally derived in the context of quantum control and discrete quantum logic, makes it relatively straightforward to determine the set of Hamiltonians that can be constructed from simpler operations.

Now apply this result to the continuous variables introduced above. Since $[X, P] = i$, the application of the translations $\pm X$ and $\pm P$ for short periods of time clearly allows the construction of any Hamiltonian $aX + bP + c$ that is linear in X and P ; this is all that it allows. To construct more complicated Hamiltonians one must also be able to perform operations that are higher order polynomials in X and P . Suppose now that one can apply the quadratic Hamiltonian $H = (X^2 + P^2)/2$. Since $\dot{P} = i[H, P] = X, \dot{X} = i[H, X] = -P$, application of this Hamiltonian for time t takes $X \rightarrow \cos tX - \sin tP, P \rightarrow \cos tP + \sin tX$. If X and P are quadrature amplitudes of a mode of the electromagnetic field, then H is just the Hamiltonian of the mode (with frequency $\omega = 1$) and corresponds to a phase shifter. Hamiltonians of this form can be enacted by letting the system evolve on its own or by inserting artificial phase delays. Note that since e^{iHt} is periodic with period $1/4\pi$, one can effectively apply $-H$ for a time δt by applying H for a time $4\pi - \delta t$. The simple commutation relations between H, X and P imply that the addition of $\pm H$ to the set of operations that can be applied allows the construction of Hamiltonians of the form $aH + bX + cP + d$.

Suppose that in addition to translations and phase shifts one can apply the quadratic Hamiltonian $\pm S = \pm(XP + PX)/2$. S has the effect $\dot{X} = i[S, X] = X$, $\dot{P} = i[S, P] = -P$, i.e., applying $+S$ takes $X \rightarrow e^t X$, $P \rightarrow e^{-t} P$: S “stretches” X and “squeezes” P by some amount. Similarly $-S$ squeezes X and stretches P . In the case of the electromagnetic field, S corresponds to a squeezer operating in the linear regime. It can easily be verified that $[H, S] = i(X^2 - P^2)$. Looking at the algebra generated from X, P, H and S by commutation, one sees that translations, phase shifts, and squeezers allow the construction of any Hamiltonian that is quadratic in X and P , and of no Hamiltonian of higher order.

To construct higher order Hamiltonians, nonlinear operations are required. One such operation is the “Kerr” Hamiltonian $H^2 = (X^2 + P^2)^2$, corresponding to a χ^3 process in nonlinear optics. This higher order Hamiltonian has the key feature that whereas commuting the previous Hamiltonians, X, P, H, S with some polynomial in X and P resulted in a polynomial with the same or lower order, commuting H^2 with a polynomial in X and P typically *increases* its order. By evaluating a few commutators, e.g., $[H^2, X] = i(X^2 P + P X^2 + 2P^3)/2$, $[H^2, P] = -i(P^2 X + X P^2 + 2X^3)/2$, $[X, [H^2, S]] = P^3$, $[P, [H^2, S]] = X^3$ one sees that the algebra generated by X, P, H, S and H^2 by commutation includes all third order polynomials in X and P . A simple inductive proof now shows that one can construct Hamiltonians that are arbitrary Hermitian polynomials in any order of X and P . Suppose that one can construct any polynomial of order M or less, where M is of degree at least 3. Then since $[P^3, P^m X^n] = iP^{m+2} X^{n-1} +$ lower order terms, and $[X^3, P^m X^n] = iP^{m-1} X^{n+2} +$ lower order terms, one can by judicious commutation of X^3 and P^3 with monomials of order M construct any monomial of order $M + 1$. Since any polynomial of order $M + 1$ can be constructed from monomials of order $M + 1$ and lower, by applying linear operations and a single nonlinear operation a finite number of times one can construct polynomials of arbitrary order in X and P to any desired degree of accuracy. Comparison with similar results for the discrete case [14] shows that the number of operations required grows as a small polynomial in the order of the polynomial to be created, the accuracy to which that polynomial is to be enacted, and the time over which it is to be applied.

The use of the Kerr Hamiltonian H^2 was not essential: any higher order Hamiltonian will do the trick. Note that commutation of a polynomial in X and P with X and P themselves (which have order 1) always reduces the order of the polynomial by at least 1, commutation with H and S (which have order 2) never increases the order, and commutation with a polynomial of order 3 or higher typically increases the order by at least 1. Judicious commutation of X, P, H and S with an applied Hamiltonian of order 3 or higher therefore

allows the construction of arbitrary Hermitian polynomials of any order in X and P .

The above set of results shows that simple linear operations, together with a single nonlinear operation, allow one to construct arbitrary polynomial Hamiltonian transformations of a single quantum variable. Let us now turn to more than one variable, e.g., the case of an interferometer in which many modes of the electromagnetic field interact. Suppose now that there are many variables, $\{X_i, P_i\}$, on each of which the simple single-variable operations described above can be performed. Now let the variables interact with each other. For simplicity, we assume that we can apply interaction Hamiltonians of the form $\pm B_{ij} = \pm(P_i X_j - X_i P_j)$: a more complicated interaction Hamiltonian can always be used to generate interactions of this form by combining it with single-variable operations. Since $\dot{X}_i = i[B_{ij}, X_i] = X_j \dot{X}_j = i[B_{ij}, X_j] = -X_i$, $\dot{P}_i = i[B_{ij}, P_i] = P_j$, $\dot{P}_j = i[B_{ij}, P_j] = -P_i$, this operation has the effect of taking $A_i \rightarrow \cos tA_i + \sin tA_j$, $A_j \rightarrow \cos tA_j - \sin tA_i$, for $A_i = X_i, P_i$, $A_j = X_j, P_j$. For the electromagnetic field, B_{ij} functions as a beam splitter, linearly mixing together the two modes i and j . By repeatedly taking commutators of B_{ij} with polynomials in X_i, P_i , for different i , it can be easily seen by the same algebraic arguments as above that it is possible to build up arbitrary Hermitian polynomials in $\{X_i, P_i\}$.

This concludes the derivation of the main result: simple linear operations on continuous variables, together with any nonlinear operation and any interaction between variables suffice to enact to an arbitrary degree of accuracy Hamiltonian operators that are arbitrary polynomials of the set of continuous variables. In the case of modes of the electromagnetic field, linear operations such as translations, phase shifts, squeezers, and beam splitters, combined with some nonlinear operation such as a Kerr nonlinearity, allow one to perform arbitrary polynomial transformations on those modes. Note that in contrast to the case of qubits, in which a nonlinear coupling between qubits is required to perform universal quantum computation, in the continuous case only *single variable* nonlinearities are required, along with linear couplings between the variables.

In analog with information over classical continuous variables, which is measured in units of “nats” (1 nat = $\log_2 e$ bits), the unit of continuous quantum information will be called the “qunat.” Two continuous variables in the pure state $|\psi\rangle_{12}$ possess $-\text{tr}\rho_1 \ln \rho_1$ qunats of entanglement, where $\rho_1 = \text{tr}_2 |\psi\rangle_{12} \langle \psi|$. For two squeezed vacua (squeezed by an amount e^{-r}) entangled using a beam splitter as in Refs. [5-7] the entropy so computed from the approximate EPR state is given by

$$S(\rho) = (1 + \bar{n}) \ln(1 + \bar{n}) - \bar{n} \ln \bar{n} \quad \text{qunats} \quad (2.2)$$

with $\bar{n} = e^r \sinh r$. For example, $e^{2r} = 10$ gives 10 dB of squeezing in power, corresponding to $r = 1.15129$. By Eq. (2.2), two continuous variables entan-

gled using a 10 dB squeezer then possess 2.607 77 qunats of shared, continuous quantum information, equivalent to 3.762 21 qubits of discrete quantum information. This is comparable to the degree of entanglement currently available using ion-trap quantum computers.

Quantum computation over continuous variables can be thought of as the systematic creation and manipulation of qunats. Universal quantum computation for polynomial transformations of continuous variables effectively allows one to perform quantum floating point manipulations on those variables. For example, it is clearly possible using linear operations alone to take the inputs X_1, X_2 and to map them to $X_1, aX_1 + bX_2 + c$. Similarly, application of the three-variable Hamiltonian $X_1X_2P_3$ takes $X_1 \rightarrow X_1, X_2 \rightarrow X_2, X_3 \rightarrow X_3 + X_1X_2t$: that is, this operation allows one to multiply X_1 and X_2 and place the result in the “register” X_3 . A wide variety of quantum floating point operations are possible. Any polynomial transformation of the continuous variables is clearly possible, as is any transformation that can be infinitesimally represented by a convergent power series. Just as classical computation over continuous variables in principle allows one to solve problems more rapidly than is possible digitally [14], it is interesting to speculate that quantum computation over continuous variables might in principle allow the solution of problems more rapidly than is possible using a “conventional,” discrete quantum computer. Continuous variable computation has its own set of problems that might be sped up by the application of continuous quantum computation: For example, such a continuous quantum computer might be used to investigate continuous NP -complete problems such as the four-feasibility problem, that is, the problem of deciding whether or not a real degree 4 polynomial in n variables has a zero [15]. In practice, of course, due to finite precision a continuous quantum computer will effectively be able to solve the same set of problems that a conventional discrete quantum computer can, although it may be able to perform some operations more efficiently.

The ability to create and manipulate qunats depends crucially on the strength of squeezing and of the nonlinearities that one can apply. 10 dB squeezers (6 dB after attenuation in the measurement apparatus) currently exist [16]. High Q cavity quantum electrodynamics can supply a strong Kerr effect in a relatively lossless context, and quantum logic gates constructed for qubits could be used to provide the nonlinearity for continuous quantum variables as well [17]. Here the fact that only single-mode nonlinearities are required for universal quantum computation simplifies the problem of effecting continuous quantum logic. Nonetheless, the difficulty of performing repeated nonlinear operations in a coherent and loss-free manner is likely to limit the possibilities for quantum computation over the amplitudes of the electromagnetic field. Vibrational modes of ions in traps or excitations of a Bose-Eistein condensate

might provide the long-lived, lossless states required for quantum computation over continuous variables.

Noise poses a difficult problem for quantum computation [18, 19, 20], and continuous variables are more susceptible to noise than discrete variables. Since an uncountably infinite number of things can go wrong with a continuous variable, it might at first seem that continuous error correction routines would require infinite redundancy. In fact, continuous quantum error correction routines exist and require no greater redundancy than conventional routines [3, 4, 5]. Such routines are capable of correcting for noise and decoherence in principle: In practice, measurement noise, losses, and the lack of perfect squeezing will lead to imperfect error correction [5]. Surprisingly, continuous quantum error correction routines are in some sense easier to enact than discrete quantum error correction routines, in that the continuous routines can be implemented using only *linear* operations together with classical feedback [5]. The relative simplicity of such routines suggests that robust, fault-tolerant quantum computation may in principle be possible for continuous quantum variables as well as for qubits. (A scheme for quantum computation is fault-tolerant if quantum computations can be carried out even in the presence of noise and errors [21, 22]. A fault-tolerant scheme that allows for arbitrarily long quantum computations to be carried out is said to be robust [23].) If this is indeed the case then quantum computation over continuous variables, despite its intrinsic difficulties, may be an experimentally viable form of quantum information processing. Continuous variables might be used to simulate continuous quantum systems such as quantum field theories. Even in the absence of fault tolerance, the large bandwidths available to continuous quantum computation make it potentially useful for quantum communications and cryptography [24].

S.L. would like to thank H. Haus and H. J. Kimble for useful discussions. This work was supported by DARPA under the QUIC initiative.

References

- [1] D. DiVincenzo, Science **270**, 255 (1995).
- [2] S. Lloyd, Sci. Am. **273**, 140 (1995).
- [3] S. Lloyd and J. J.-E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).
- [4] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
- [5] S. L. Braunstein, Nature (London) **394**, 47 (1998).
- [6] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
- [7] A. Furusawa, *et al*, Science **282**, 706 (1998).
- [8] This definition of quantum computation corresponds to the normal “circuit” definition of quantum computation as in, e.g., D. Deutsch, Proc.

- R. Soc. London A, **425**, 73 (1989); A. C.-C. Yao, in *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser, (IEEE Computer Society, Los Alamitos, CA, 1995), pp. 352-361. The works of M. Reck *et al.*, Phys. Rev. Lett. **73**, 58 (1994), and N. J. Cerf, C. Adami, and P. G. Kwiat, Phys. Rev. A **57**, R1477 (1998), showing how to perform arbitrary unitary operators using only linear devices such as beam splitters, though of considerable interest and potential practical importance, does not constitute quantum computation by the usual definition. Reck *et al.* and Cerf *et al.* propose performing arbitrary unitary operations on N variables not by acting on the variables themselves but by expanding the information in the variables into an interferometer with $O(2^N)$ arms and acting in this exponentially larger space. Local operations on the original variables correspond to highly nonlocal operations in this “unary” representation: To flip a single bit requires one to act on half [$O(2^{N-1})$] of the arms of the interferometer. Actually to perform quantum computation on qubits using an interferometer requires nonlinear operations as detailed in Y. Yamamoto, M. Kitagawa, and K. Igeta, in *Proceedings of the 3rd Asia-Pacific Physics Conference*, edited by Y. W. Chan, A. F. Leung, C. N. Yang, K. Young (World Scientific, Singapore, 1988), pp. 779-799; G. J. Milburn, Phys. Rev. Lett. **62** 2124 (1989).
- [9] G. M. Huang, T. J. Tarn, J. W. Clark, J. Math. Phys. (N.Y.) **24**, 2608-2618 (1983).
 - [10] *Differential Geometric Control Theory*, edited by R. W. Brockett, R. S. Millman and H. J. Sussman, (Birkhauser, Boston, 1983); *Nonholonomic Motion Planning*, edited by Z. Li and J. F. Canney (Kluwer Academic, Boston, 1993).
 - [11] V. Ramakrishna, M. V. Salapaka, M. Dahleh, H. Rabitz and A. Peirce, Phys. Rev. A **51**, 960-966 (1995).
 - [12] S. Lloyd, Phys. Rev. Lett. **75**, 346-349 (1995).
 - [13] D. Deutsch, A. Barenco and A. Ekert, Proc. R. Soc. London A **449**, 669-677 (1995).
 - [14] S. Lloyd, Science **273**, 1073 (1996).
 - [15] L. Blum, M. Shub and S. Smale, Bull. Am. Math. Soc. **21**, 1-46 (1989).
 - [16] L. A. Wu *et al.*, Phys. Rev. Lett. **57**, 2520 (1986).
 - [17] Q. A. Turchette, *et al.*, Phys. Rev. Lett. **75**, 4710-4713 (1995).
 - [18] R. Landauer, Nature (London) **335**, 779-784 (1988).
 - [19] R. Landauer, Phys. Lett. A **217**, 188-193 (1996).
 - [20] R. Landauer, Phil. Trans. R. Soc. London A **335**, 367-376 (1995).

- [21] P. Shor, *Proceedings of the 37th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, 1996), pp. 56-65.
- [22] D. P. DiVincenzo and P. W. Shor, Phys. Rev. Lett. **77**, 3260-3263 (1996).
- [23] R. Laflamme, M. Knill and W.H. Zurek, Science **279**, 342 (1998); D. Aharonov and Ben-Or, quant-ph; J. Preskill, Proc. R. Soc. London A **454**, 385 (1998).
- [24] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, (IEEE Press, New York, 1984), pp. 175-179. A. K. Ekert, *et al*, Phys. Rev. Lett. **69**, 1293 (1992); P. D. Townsend, J. G. Rarity and P. R. Tapster, Electronics Letters **29**, 1291 (1993); R. J. Hughes, *et al*, in *Advances in Cryptology: Proceedings of Crypto 96*, (Springer-Verlag, New York, 1997), pp. 329-343; A. Muller *et al*. Appl. Phys. Lett. **70**, 793 (1997).

Chapter 3

ERROR CORRECTION FOR CONTINUOUS QUANTUM VARIABLES*

Samuel L. Braunstein

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

Abstract We propose an error correction coding algorithm for continuous quantum variables. We use this algorithm to construct a highly efficient 5-wave-packet code which can correct arbitrary single wave-packet errors. We show that this class of continuous variable codes is robust against imprecision in the error syndromes. A potential implementation of the scheme is presented.

Quantum computers hold the promise for efficiently factoring large integers [1]. However, to do this beyond a most modest scale they will require quantum error correction [2]. The theory of quantum error correction is already well studied in two-level or spin- $\frac{1}{2}$ systems (in terms of qubits or quantum bits) [2, 3, 4, 5, 6, 7]. Some of these results have been generalized to higher-spin systems [8, 9, 10, 11]. This work applies to discrete systems like the hyperfine levels in ions but is not suitable for systems with continuous spectra, such as unbound wave packets. Simultaneously with this paper, Lloyd and Slotine present the first treatment of a quantum error correction code for continuous quantum variables [12], demonstrating a 9-wave-packet code in analogy with Shor's 9-qubit coding scheme [2]. Such codes hold exciting prospects for the *complete* manipulation of quantum systems, including both discrete and continuous degrees of freedom, in the presence of inevitable noise [13].

In this Letter we consider a highly efficient and compact error correction coding algorithm for continuous quantum variables. As an example, we construct a 5-wave-packet code which can correct arbitrary single-wave-packet errors. We show that such continuous variable codes are robust against imprecision in

*S. L. Braunstein, Physical Review Letters **80**, 4084-4087 (1998).
Copyright (1998) by the American Physical Society.

the error syndromes and discuss potential implementation of the scheme. This paper is restricted to one-dimensional wave-packets which might represent the wave function of a nonrelativistic one-dimensional particle or the state of a single polarization of a transverse mode of electromagnetic radiation. We shall henceforth refer to such descriptions by the generic term wave packets [14].

Rather than starting from scratch we shall use some of the theory that has already been given for error correction on qubits. In particular, Steane has noted that the Hadamard transform,

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad (3.1)$$

maps phase flips into bit flips and can therefore be used to form a class of quantum error correction codes that consist of a pair of classical codes, one for each type of “flip” [3]. This mapping between phase and amplitude bases is achieved with a rotation about the y -axis by $\pi/2$ radians in the Bloch sphere representation of the state. In analogy, the position and momentum bases of a continuous quantum state may be transformed into each other by $\pi/2$ rotations in phase-space. This transition is implemented by substituting the Hadamard rotation in the Bloch sphere by a Fourier transform between position and momentum in phase-space. This suggests that we could develop the analogous quantum error correction codes for continuous systems [15].

We shall find it convenient to use a units-free notation where

$$\begin{aligned} \text{position} &= x \times (\text{scale length}) \\ \text{momentum} &= p / (\text{scale length}), \end{aligned} \quad (3.2)$$

where x is a scaled length, p is a scaled momentum and we have taken $\hbar = \frac{1}{2}$. (We henceforth drop the modifier “scaled.”) The position basis eigenstates $|x\rangle$ are normalized according to $\langle x'|x\rangle = \delta(x' - x)$ with the momentum basis given by

$$|x\rangle = \frac{1}{\sqrt{\pi}} \int dp e^{-2ixp} |p\rangle. \quad (3.3)$$

To avoid confusion we shall work in the position basis throughout and so define the Fourier transform as an active operation on a state by

$$\hat{\mathcal{F}}|x\rangle = \frac{1}{\sqrt{\pi}} \int dy e^{2ixy} |y\rangle, \quad (3.4)$$

where both x and y are variables in the position basis. Note that Eqs. (3.3) and (3.4) correspond to a change of representation and a physical change of the state, respectively.

In addition to the Fourier transform we shall require an analog to the bit-wise exclusive-OR (XOR) gate for continuous variables. The XOR gate has many interpretations including controlled-NOT gate, addition modulo 2 and parity associated with it. Of these interpretations the natural generalization to continuous variables is addition without a cyclic condition, which maps

$$|x, y\rangle \rightarrow |x, x + y\rangle . \quad (3.5)$$

By removing the cyclic structure of the XOR gate we have produced a gate which is no longer its own inverse. Thus, in addition to the Fourier transform and this generalized XOR gate we include their inverses to our list of useful gates. This generalized XOR operation performs translations over the entire real line, which are related to the infinite additive group on \mathbb{R} . The characters χ of this group satisfy the multiplicative property $\chi(x + y) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{R}$ and obey the sum rule

$$\frac{1}{\pi} \int_{-\infty}^{\infty} dx \chi(x) = \delta(x) , \quad (3.6)$$

where $\chi(x) = e^{2ix}$. Interestingly, this sum rule has the same form as that found by Chau in higher-spin codes [10]. Once we have recognized the parallel, it is sufficient to take the code of a spin- $\frac{1}{2}$ system as a basis for our continuous-variable code.

Based on these parallel group properties, we are tempted to speculate a much more general and fundamental relation: We conjecture that n -qubit error correction codes can be paralleled with n -wave-packet codes by replacing the discrete-variable operations (Hadamard transform and XOR gate) by their continuous-variable analogs (Fourier transform, generalized-XOR and their inverses). As a last remark before embarking on the necessary substitutions (in a specific example), we point out that the substitution conjecture is only valid for qubit codes whose circuits involve only these (\hat{H} and XOR) elements. We shall therefore restrict our attention to this class of codes.

An example of a suitable 5-qubit code was given by Laflamme et al. [16]. We show an equivalent circuit in Fig. 3.1 [17]. As we perform the substitutions, we must determine which qubit-XOR gates to replace with the generalized-XOR and which with its inverse. To resolve this ambiguity, two conditions are imposed. First, we demand that the code retain its properties under the parity operation (on each wave packet). We conclude that either gate may be chosen for the first operation on initially zero-position eigenstates. Ambiguity remains for the last four XOR substitutions. As a second step, the necessary and sufficient condition for quantum error correction [5, 6],

$$\langle x'_{\text{encode}} | \hat{\mathcal{E}}_\alpha^\dagger \hat{\mathcal{E}}_\beta | x_{\text{encode}} \rangle = \delta(x' - x) \lambda_{\alpha\beta} , \quad \forall \alpha, \beta , \quad (3.7)$$

must be met. Here $|x_{\text{encode}}\rangle$ encodes a single wave-packet's position eigenstate in a multi-wave-packet state, $\hat{\mathcal{E}}_\alpha$ is a possible error that can be handled by the code and $\lambda_{\alpha\beta}$ is a complex constant independent of the encoded states. [Condition (3.7) says that correctable errors do not mask the orthogonality of encoded states.]

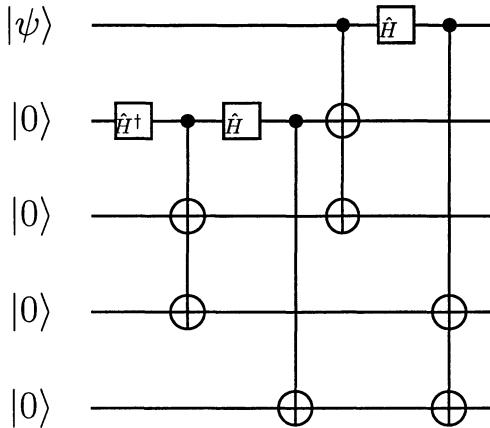


Figure 3.1 Quantum error correction circuit from [17]. The qubit $|\psi\rangle$ is rotated into a 5-particle subspace by the unitary operations represented by the operations shown in this circuit. Note that the 3-qubit gates are simply pairs of Xors.

In the case of a single wave-packet error, for our 5-wave-packet code, it turns out that amongst the conditions of Eq. (3.7) only $\langle x'_{\text{encode}} | \hat{\mathcal{E}}_{4\alpha}^\dagger \hat{\mathcal{E}}_{5\beta} | x_{\text{encode}} \rangle$, having errors on wave packets 4 and 5, is affected by the ambiguity (see detail below). An explicit calculation of *all* the conditions shows that the circuit of Fig. 3.2 yields a satisfactory quantum error correction code (as do variations of this circuit due to the extra freedom with respect to the choice of operator acting on wave-packets 1-3). By analogy with the results for higher-spin codes, we know that this code is optimal (though not perfect) and that no four-wave-packet code would suffice [10]. The code thus constructed has the form

$$\begin{aligned} |x_{\text{encode}}\rangle = \frac{1}{\pi^{3/2}} \int dw dy dz e^{2i(wy+xz)} \\ \times |z, y+x, w+x, w-z, y-z\rangle. \end{aligned} \quad (3.8)$$

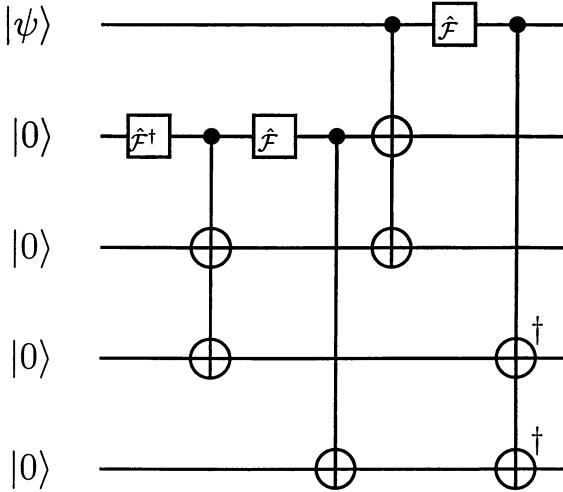


Figure 3.2 This ‘‘circuit’’ unitarily maps a one-dimensional single-wave-packet state $|\psi\rangle$ into a 5-wave-packet error correction code. Here the auxiliary wave packets $|0\rangle$ are initially zero-position eigenstates. For degrees-of-freedom larger than qubits the ideal XOR is not its own inverse; here the daggers on the XOR gates represent the inverse operation.

Let us demonstrate the calculation of one of the conditions specified by Eq. (3.7):

$$\begin{aligned}
 & \langle x'_{\text{encode}} | \hat{\mathcal{E}}_{4\alpha}^\dagger \hat{\mathcal{E}}_{5\beta} | x_{\text{encode}} \rangle \tag{3.9} \\
 = & \frac{1}{\pi^3} \int dw' dy' dz' dw dy dz e^{2i(wy+xz-w'y'-x'z')} \\
 & \times \delta(z' - z) \delta(y' - y + x' - x) \delta(w' - w + x' - x) \\
 & \times \langle w' - z' | \hat{\mathcal{E}}_\alpha^\dagger | w - z \rangle \langle y' - z' | \hat{\mathcal{E}}_\beta | y - z \rangle \\
 = & \frac{e^{-2i(x'-x)^2}}{\pi^3} \int dw dy dz e^{2i(x'-x)(w+y-z)} \\
 & \times \langle w - x' + x - z | \hat{\mathcal{E}}_\alpha^\dagger | w - z \rangle \langle y - x' + x - z | \hat{\mathcal{E}}_\beta | y - z \rangle.
 \end{aligned}$$

Making the replacements $w \rightarrow w + z$ and $y \rightarrow y + z$ in this last expression we obtain

$$\begin{aligned}
 = & \frac{e^{-2i(x'-x)^2}}{\pi^3} \int dw dy dz e^{2i(x'-x)(w+y+z)} \\
 & \times \langle w - x' + x | \hat{\mathcal{E}}_\alpha^\dagger | w \rangle \langle y - x' + x | \hat{\mathcal{E}}_\beta | y \rangle \tag{3.10} \\
 = & \frac{\delta(x' - x)}{\pi^2} \int dw dy \langle w | \hat{\mathcal{E}}_\alpha^\dagger | w \rangle \langle y | \hat{\mathcal{E}}_\beta | y \rangle \equiv \delta(x' - x) \lambda_{\alpha\beta}.
 \end{aligned}$$

For the other cases we find by explicit calculation, for wave-packets $j \neq k$, that

$$\langle x'_{\text{encode}} | \hat{\mathcal{E}}_{j\alpha}^\dagger \hat{\mathcal{E}}_{k\beta} | x_{\text{encode}} \rangle = \delta(x' - x) \lambda_{\alpha\beta}. \quad (3.11)$$

For $j = k$ this constant is found to be

$$\lambda_{\alpha\beta} = \frac{C}{\pi^2} \int dw \langle w | \hat{\mathcal{E}}_\alpha^\dagger \hat{\mathcal{E}}_\beta | w \rangle, \quad (3.12)$$

where C is formally infinite.

We shall argue that this infinity vanishes when the syndrome is read with only finite precision, which is always going to be the real situation. However, this requires us to demonstrate that our codes are robust: that for a sufficiently good precision we may correct single-wave-packet errors to any specified accuracy. In order to understand how the error syndromes are measured, let us consider a simpler code, namely, the continuous version of Shor's original 9-qubit code,

$$\begin{aligned} |x_{\text{encode}}\rangle &= \frac{1}{\pi^{3/2}} \int dw dy dz e^{2ix(w+y+z)} \\ &\quad \times |w, w, w, y, y, y, z, z, z\rangle, \end{aligned} \quad (3.13)$$

where parity alone removes all ambiguity. (This code has been independently obtained by Lloyd and Slotine [12].) Since this 9-wave-packet code corrects position errors and momentum errors separately, it is sufficient to study the subcode

$$|x_{\text{encode}}\rangle = |x, x, x\rangle, \quad (3.14)$$

designed to correct position errors on a single wave packet. The most general position error (on a single wave packet) is given by some function of the momentum of that system $\hat{\mathcal{E}}(\hat{p})$ and need not be unitary on the code subspace [Eq. (3.7)]. The action of such an error on a wave packet may be written in the position basis as

$$\hat{\mathcal{E}}(\hat{p})|x\rangle = \frac{1}{\pi} \int dy dp e^{2ip(y-x)} \mathcal{E}(p)|y\rangle = \int dy \tilde{\mathcal{E}}(y)|x-y\rangle, \quad (3.15)$$

where $\tilde{\mathcal{E}}(x)$ is the Fourier transform of $\mathcal{E}(p)$. Thus the most general position error looks like a convolution of the wave packet's ket with some unknown (though not completely arbitrary) function. Suppose this error occurs on wave packet 1 in the repetition code (3.14). Further, let us use auxiliary wave-packets (so-called ancillae) and compute the syndrome as shown in Fig. 3.3, then the resulting state may be written as

$$\int dy \tilde{\mathcal{E}}(y)|x-y, x, x, -y, 0, y\rangle. \quad (3.16)$$

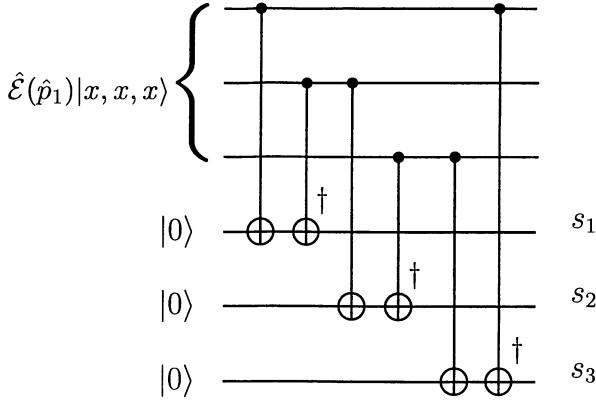


Figure 3.3 Syndrome calculation and measurement: A state with a single-wave-packet position error (here on wave packet 1) enters and the differences of each pair of positions is computed. The syndrome $\{s_1, s_2, s_3\}$ may now be directly measured in the position basis.

Everything up till now has been unitary and assumed ideal. Now measure the syndrome: Ideally it would be $\{-y, 0, y\}$ collapsing the wave packet for a specific y . Correcting the error is now easy, because we know the location, value and sign of the error. Shifting the first wave packet by the amount y retrieves the correctly encoded state $|x, x, x\rangle$. Note that this procedure uses only very simple wave-packet-gates: The comparison stage is done *classically*, in contrast to the scheme of Lloyd and Slotine, where the comparison is performed at the amplitude level and involves significantly more complicated interactions [12].

It is now easy to see what imprecise measurements of the syndromes will do. Suppose each measured value of a syndrome s'_j is distributed randomly about the true value s_j according to the distribution $p_{\text{meas}}(s'_j - s_j)$. We find two conditions for error-correction to proceed smoothly. First, $p_{\text{meas}}(x)$ must be narrow compared to any important length scales in $\hat{\mathcal{E}}(x)$. This guarantees that the chance for “correcting” the wrong wave packet is negligible and reduces the position-error operator to an uninteresting prefactor. If the original unencoded state had been $\int dx \psi(x)|x\rangle$ then after error correction we would obtain the mixed state

$$\int dx' dx dz \psi(x) \psi^*(x') p_{\text{meas}}(z) |x - z, x, x\rangle \langle x' - z, x', x'| . \quad (3.17)$$

Thus, unless $p_{\text{meas}}(x)$ is *also* narrow compared to any important length scales in $\psi(x)$, decoherence will appear in the off-diagonal terms for wave packet 1 of the corrected state (3.17). This second condition is also seen in the quantum teleportation of continuous variables due to inaccuracies caused by measure-

ment [13]. These conditions roughly match those described by Lloyd and Slotine [12]. We note that any syndrome imprecision will degrade the encoded states, though this precision may be improved by repeated measurements of the syndromes. For our 5-wave-packet example (3.8), syndromes consist of sums of two or more wave-packet positions or momenta and are measured similarly.

It should be noted that Chau's higher-spin code [10] could have been immediately taken over into a quantum error correction code for continuous quantum variables in accordance with our substitution procedure. However, we have produced an equivalent code with a more efficient circuit prescription: Whereas Chau gives a procedure for constructing his higher-spin code using 9 generalized XOR operations, the circuit in Fig. 3.2 requires only 7 such gates or their inverses. In fact, we could run this substitution backwards to obtain a cleaner 5-particle higher-spin code based on Eq. (3.8).

In order to consider potential implementations of the above code let us restrict our attention to a situation where the wave packets are sitting in background harmonic-oscillator potentials. By the virial theorem the form of a wave packet in such a potential is preserved up to a trivial rotation in phase-space with time. The two operations required may be implemented simply as follows: The rotation in phase-space, Eq. (3.4), may be obtained by delaying the phase of one wave packet relative to the others, and the XOR operation, Eq. (3.5), should be implemented via a quantum non-demolition (QND) coupling. There exists extensive experimental literature on these operations both for optical fields and for trapped ions [13, 18, 19, 20, 21].

The conjecture put forth in this Letter leads to a simple, 2-step design of error correction codes for continuous quantum variables. According to this conjecture, any qubit code, whose circuit operations include only a specific Hadamard transformation, its inverse and the ideal XOR, may be translated to a continuous quantum-variable code, by substituting these operators with their continuous analogs and then imposing two criteria – parity invariance and the error-correction condition – which remove any ambiguities in the choice of operators. We demonstrate the success of this coding procedure in two examples (one based on Shor's 9-qubit code [2], and a second based on a variation of the Laflamme et al. 5-qubit code [16, 17]). The 5-wave-packet code presented here is the optimal continuous encoding of a single one-dimensional wave packet that protects against arbitrary single-wave-packet errors. We show that this code (and in fact the entire class of codes derived in this manner) are robust against imprecision in the error syndromes. The potential implementation of the proposed class of circuits in optical-field and ion-trap set-ups is an additional incentive for further investigation of the robust manipulation of continuous quantum variables.

This work was funded in part by EPSRC grant GR/L91344. The author appreciated discussions with N. Cohen, H. J. Kimble, D. Gottesman and S. Schneider.

Appendix: Addendum

The above work demonstrates that an error correction code may be designed, though for implementation it requires some kind of QND couplings. Soon after this work was complete the author realized that much of the same work could be done with straight linear optics, in particular coupling based upon beam splitter operations [22].

First, consider two light fields $|x\rangle$ and $|y\rangle$ incident on an “ideal” (phase-free) beam splitter. The output light fields are given by

$$\hat{\mathcal{B}}_{12}(\theta)|x, y\rangle = |x \cos \theta - y \sin \theta, y \cos \theta + x \sin \theta\rangle, \quad (3.A.1)$$

where the subscripts 12 refer to the wave packets acted upon. From these ideal beam splitters we construct a 3-port device called a *tritter* [23]

$$\hat{\mathcal{T}}_{123} \equiv \hat{\mathcal{B}}_{23}(\pi/4) \hat{\mathcal{B}}_{12}(\cos^{-1} \frac{1}{\sqrt{3}}), \quad (3.A.2)$$

from which we may construct the three wave-packet subcode of Shor’s 9-wave-packet code via

$$\hat{\mathcal{T}}_{123}|x, 0, 0\rangle = |\frac{1}{\sqrt{3}}x, \frac{1}{\sqrt{3}}x, \frac{1}{\sqrt{3}}x\rangle. \quad (3.A.3)$$

In fact, the only difference between this code and the “ideal” version of it $|x, x, x\rangle$ is a simple common scaling in each of the code’s wave packets.

Finally, we combine these elements together with this freedom to scale, in order to produce our encoding device out of linear optics. A suitable choice for the 9-wave-packet code is a 9-port beam-splitter, which we call a *nona-splitter*

$$\hat{\mathcal{N}}_{1-9} \equiv \hat{\mathcal{T}}_{789}\hat{\mathcal{T}}_{456}\hat{\mathcal{T}}_{123}\hat{\mathcal{F}}_7\hat{\mathcal{F}}_4\hat{\mathcal{F}}_1\hat{\mathcal{T}}_{147}. \quad (3.A.4)$$

This device could be implemented as a series of *eight* ordinary beam splitters or as a single (mass-produced) integrated-optics element [22].

More recently, a more robust set of quantum error-correcting codes over continuous variables have been constructed which protect the state of a finite dimensional quantum system from decoherence [24]. The advantage of this variation over those described in this chapter are that they allow the effective protection against small “diffusive” errors [24], which are closer to typical realistic loss mechanisms. In the codes studied above, small errors comparable or smaller than readout errors cannot be corrected and are additive with each “protective” operation.

References

- [1] P. W. Shor in *Proc. 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, California, 1994), p.124.
- [2] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
- [3] A. M. Steane, Proc. Roy. Soc. London **452**, 2551 (1996).
- [4] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
- [5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [6] E. Knill and R. Laflamme, Phys. Rev. A, **55**, 900 (1997).
- [7] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
- [8] E. Knill, LANL report LAUR-96-2717, preprint quant-ph/9608048.
- [9] H. F. Chau, Phys. Rev. A **55**, R839 (1997).
- [10] H. F. Chau, Phys. Rev. A **56**, R1 (1997).
- [11] E. M. Rains, LANL preprint quant-ph/9703048.
- [12] S. Lloyd and J.-J. E. Slotine, LANL preprint quant-ph/9711021.
- [13] S. L. Braunstein and H. J. Kimble, “Teleportation of continuous quantum variables,” Phys. Rev. Lett., submitted; S. L. Braunstein, H. J. Kimble, Y. Sorensen, A. Furusawa and N. Ph. Georiades, “Teleportation of continuous quantum variables,” IQEC 1998, abstract submitted.
- [14] Although we consider multi-wave-packet states as one-dimensional we would not want them to physically overlap so they could, for example, be displaced one from another in an orthogonal direction.
- [15] An example using as few as 7 qubits to correct an arbitrary single-qubit error in a 1-qubit encoded state can be found in [3].
- [16] R. Laflamme, C. Miquel, J. P. Paz and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
- [17] S. L. Braunstein and J. A. Smolin, Phys. Rev. A **55**, 945 (1997).
- [18] S. F. Pereira, Z. Y. Ou and H. J. Kimble, Phys. Rev. Lett. **72**, 214 (1994).
- [19] K. Bencheikh, j. A. Levenson, P. Grangier and O. Lopez, Phys. Rev. Lett. **75**, 3422 (1995).
- [20] R. L. de Matos Filho and W. Vogel, Phys. Rev. Lett. **76**, 4520 (1996).
- [21] R. Bruckmeier, H. Hansen and S. Schiller, Phys. Rev. Lett. **79**, 1463 (1997).
- [22] S. L. Braunstein, Nature (London) **394**, 47 (1998).

- [23] M. Zukowski, *Laser Phys.* **4**, 690 (1994).
- [24] D. Gottesman, A. Kitaev and J. Preskill, “Encoding a qubit in an oscillator,” quant-ph/0008040.

Chapter 4

DEUTSCH-JOZSA ALGORITHM FOR CONTINUOUS VARIABLES

Arun K. Pati

Institute of Physics, Bhubaneswar-751005, Orissa, INDIA

Theoretical Physics Division, BARC, Mumbai, INDIA

Samuel L. Braunstein

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

Abstract We present an idealized quantum continuous variable analog of the Deutsch-Jozsa algorithm which can be implemented on a perfect continuous variable quantum computer. Using the Fourier transformation and XOR gate appropriate for continuous spectra we show that under ideal operation to infinite precision that there is an infinite reduction in number of query calls in this scheme.

In principle, quantum computers can have remarkable computational powers which classical computers cannot [1, 2]. In the last few years it has been shown that it is possible for quantum computers to perform certain computational tasks faster than any classical computer [3, 4, 5, 6, 7, 8, 9]. Quantum computation exploits quantum interference and entanglement to outperform its classical counterparts. The first algorithm promising benefits from quantum parallelism was discovered by Deutsch and Jozsa [6]. Soon after this Shor discovered [10] his now famous algorithm for factoring large numbers [11]. Subsequently, a fast quantum search algorithm was discovered by Grover [12, 13]; in addition, the time-dependent generalization of Grover's algorithm and its stability under unitary perturbation has been studied [14].

It may be mentioned that all these algorithms are usually designed for qubits. However, in nature there are other classes of quantum systems whose observables form, for example, continuous spectra. Usually a continuous variable can be anything, e.g., position, momentum, energy (unbounded), the amplitudes of the electromagnetic field, etc. It is important to know how these algorithms can

be generalized to continuous quantum variables. By learning how, we might make progress towards discovering new algorithms which are perhaps more naturally formulated using continuous variables.

Recently continuous quantum information has played an important role in teleportation [15] and even error-correction codes [16, 17] with a possible implementation using linear devices [18]. Moreover, quantum computation over continuous variables has also been studied. It was found that the universal continuous variable quantum computation can be effected using simple non-linear operations with coupling provided solely by linear operations [19]. Just as standard quantum computation can be thought of as the coherent manipulation of two-level systems (qubits), continuous quantum computation can be thought of as the manipulation of “qunats.”

The first algorithm to have been studied for potential implementation using continuous quantum variables was the Grover virtual database search [20]. Here, we go on to generalize the Deutsch-Jozsa algorithm to continuous variables. This scheme naively gives an infinite speed-up over classical function evaluation.

To start with, let us recall the standard Deutsch-Jozsa algorithm for qubits. In this case we are given a number $i \in \{0, \dots, 2^n - 1\} \equiv B^n$ and a “black box” or “oracle query” that computes a binary function $f(i) : B^n \rightarrow B$. Further, the function f which only takes values 0 or 1 is *promised* to be either constant or balanced (with an equal number of each type of outcome over all input strings). The aim is to determine this property for f , i.e., whether it is constant or balanced. On a classical computer in the worst case the oracle query requires $O(2^n)$ function evaluations. However, if one calculates the function using reversible quantum operations then only a single function evaluation is required to achieve the goal [6, 21].

In the continuous variable setting we pose the problem in the following way. Suppose there is a particle located somewhere along the x -axis. Since $x \in \mathbb{R}$ is a continuous variable it can take value from $-\infty$ to $+\infty$ (in practice it may be from $-L$ to L , where L is some length scale involved, but still the number of possible values of x is infinite). Suppose there are two persons Alice and Bob playing a game [22]. Alice tells Bob a value of x and Bob calculates some function $f(x)$ which takes values 0 or 1. Further, Bob has promised Alice that he will use a function which is either constant or balanced. A constant function is 0 or 1 for all values of $x \in (-L, +L)$. For a balanced function, $f(x) = 0$ or 1 for exactly half of the cases. One can define the balanced function more precisely in the following manner. Imagine that the interval for the continuous variable x has been divided into n sub-intervals. Let μ be the Lebesgue measure on \mathbb{R} . A function $f(x)$ is balanced provided the Lebesgue measure of the support for where the function is zero is identical to the Lebesgue measure of the support for where the function is one, i.e.,

$\mu(\{x \in \mathbb{R} | f(x) = 0\}) = \mu(\{x \in \mathbb{R} | f(x) = 1\})$. Now, Alice wants to know whether Bob has chosen a constant or balanced function. In the classical scenario since there are an infinite number of possibilities for x Alice needs to ask Bob (who has the oracle) an infinite number of times! However, we can show if we use a perfect continuous variable quantum computer and unitary operators that can be implemented on them, then a single function evaluation is required to know this global property of the function.

Let us consider a continuous variable system whose Hilbert space is infinite dimensional and spanned by a basis state $|x\rangle$ satisfying the Dirac orthogonality condition $\langle x|x'\rangle = \delta(x-x')$. In a continuous variable scheme a basic operation is the Fourier transformation between position and momentum variables in phase space (analog to the Walsh-Hadamard transformation for qubits). We can define the Fourier transformation as an active operation on a qunat state $|x\rangle$ as

$$\mathcal{F}|x\rangle = \frac{1}{\sqrt{\pi}} \int dy e^{2ixy}|y\rangle , \quad (4.1)$$

where both x and y are in the position basis. This has been used in developing error correction codes [16, 18] and Grover's algorithm for continuous variables [20]. This Fourier transformation can be easily applied in physical situations. For example, when $|x\rangle$ represents quadrature eigenstate of a mode of the electromagnetic field, $\mathcal{F}|x\rangle$ is simply an eigenstate of the conjugate quadrature produced by a $\pi/2$ phase delay.

Another useful gate on a continuous variable quantum computer is XOR gate (analogous to the controlled NOT gate for qubits but without the cyclic condition) defined as [18]

$$|x\rangle|y\rangle \rightarrow |x\rangle|x+y\rangle . \quad (4.2)$$

Further, we assume that given a classical circuit for computing $f(x)$ there is a quantum circuit which can compute a unitary transformation U_f on a continuous variable quantum computer. If a quantum circuit exists that transforms

$$|x\rangle|y\rangle \rightarrow |x\rangle|y + f(x)\rangle , \quad (4.3)$$

then by linearity it can also act on any superposition of qunat states. For example, if we evaluate the function on a state (4.1) along with another qunat state $|z\rangle$, we have

$$\mathcal{U}_f(\mathcal{F}|x\rangle|z\rangle) = \frac{1}{\sqrt{\pi}} \int dy e^{2ixy}|y\rangle|z + f(y)\rangle . \quad (4.4)$$

This shows that using quantum parallelism for idealized qunat computers one can evaluate all possible values of a function simultaneously with one application of \mathcal{U}_f .

Now, we present the Deutsch-Jozsa algorithm for a continuous variable quantum computer. The set of instructions for deciding the constant or balanced nature of function $f(x)$ are given below (and is illustrated as a quantum circuit in Fig. 4.1):

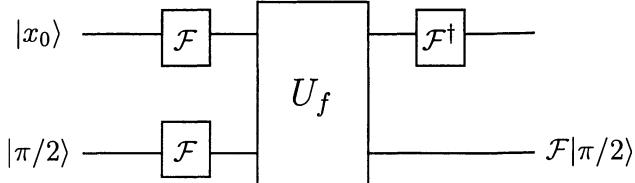


Figure 4.1 Quantum circuit for the continuous-variable Deutsch-Jozsa algorithm.

(i) Alice stores her query in a qunat register prepared in an ideal position eigenstate $|x_0\rangle$ and attaches another qunat in a position eigenstate $|\pi/2\rangle$. So the two qunts are in the state $|x_0\rangle|\pi/2\rangle$

(ii) She creates superpositions of qunat states by applying the Fourier transformation to the query qunat and the target qunat. The resulting state is given by

$$\mathcal{F}|x_0\rangle\mathcal{F}|\pi/2\rangle = \frac{1}{\pi} \int dx dy e^{2ix_0x+i\pi y}|x\rangle|y\rangle. \quad (4.5)$$

(iii) Bob evaluates the function using the unitary operator \mathcal{U}_f . The state transforms as

$$\frac{1}{\sqrt{\pi}} \int dx e^{2ix_0x+i\pi f(x)}|x\rangle\mathcal{F}|\pi/2\rangle. \quad (4.6)$$

Here, the key role is played by the ancilla qunat state $|\pi/2\rangle$. To see how the function evaluation takes place consider the intermediate steps given by

$$\mathcal{U}_f(|x\rangle\mathcal{F}|\pi/2\rangle) = \frac{1}{\sqrt{\pi}} \int dy e^{i\pi y}\mathcal{U}_f(|x\rangle|y\rangle) = (-1)^{f(x)}|x\rangle\mathcal{F}|\pi/2\rangle. \quad (4.7)$$

If the function $f(x) = 0$ there is no sign change and if $f(x) = 1$ there is a sign change. After the third step performed by Alice, she has a qunat state in which the result of Bob's function evaluation is encoded in the amplitude of the qunat superposition state given in (4.6). To know the nature of the function she now performs an inverse Fourier transformation on her qunat state.

(iv) The qunat states after the inverse Fourier transform is given by

$$|q\rangle = \frac{1}{\pi} \int dx dx' e^{2ix(x_0-x')}(-1)^{f(x)}|x'\rangle\mathcal{F}|\pi/2\rangle. \quad (4.8)$$

(v) Alice measures her qunat by projecting onto the original position eigenstate $|x_0\rangle$. In an ideal continuous variable scheme the correct projection operator is defined as [23]

$$P_{\Delta x_0} = \int_{x_0 - \Delta x_0/2}^{x_0 + \Delta x_0/2} dy |y\rangle\langle y| . \quad (4.9)$$

As has been explained in [20, 23] if the observable has a continuous spectrum then the measurement cannot be performed precisely but must involve some spread Δx_0 . Therefore, the action of projection onto the qunat state after step (iv) is given by

$$P_{\Delta x_0}|q\rangle = \frac{1}{\pi} \int dx \int_{x_0 - \Delta x_0/2}^{x_0 + \Delta x_0/2} dy e^{2ix(x_0-y)} (-1)^{f(x)} |y\rangle \mathcal{F}|\pi/2\rangle . \quad (4.10)$$

Now consider two possibilities. If the function is constant then the above equation reduces to $\pm|x_0\rangle\mathcal{F}|\pi/2\rangle$. [In simplifying we need to use the Dirac delta function $(1/\pi) \int dx e^{2ix(x_0-y)} = \delta(x_0 - y)$.] This means that if Alice measures $|x_0\rangle$ she is sure that $f(x)$ is definitely constant. In the other case, i.e., when the function is balanced she will not get the measurement outcome to be $|x_0\rangle$. In fact, in the balanced case the outcome is orthogonal to the constant case as the result gives zero. Therefore, a single function evaluation (followed by a measurement onto $|x_0\rangle$) in a qunat quantum computer can decide whether the promised function is constant or balanced. Unlike the qubit case, in the *idealized* continuous variable case the reduction in the number of query calls is from infinity to one.

In conclusion, we have generalised the primitive quantum algorithm (Deutsch-Jozsa algorithm) from the discrete case to the *idealized* continuous case. It may be worth mentioning that as in error correction codes for continuous-variablees [16], if one replaces the Hadamard transform and XOR gate by their continuous-variable analogs in original Deutsch-Jozsa algorithm for qubit case, then the idealized algorithm works perfectly. This theoretically demonstrates the power of quantum computers to exploit the superposition principle giving an infinite speed up compared to classical scenario. This idealized analysis has not considered the affects of finite precision in measurement or state construction and so whether it may be implemented remains an open question for further study. Part of the difficulty in extending this work in this direction is that defining an oracle for continuous variables appears to be a difficult task, one that we have carefully avoided here. An alternate way forward might be to consider some sort of “hybrid” approach involving both qunats and qubits. This is precisely what Seth Lloyd considers in the following chapter.

AKP thanks P. van Loock and R. Simon for useful feedback. AKP also thanks G. Giedke for discussions during Benasque Science Center-2000 in Spain on defining balanced function for continuous variables.

References

- [1] S. Lloyd, *Science*, **261**, 1569 (1993).
- [2] S. Lloyd, *Science*, **273**, 1073 (1996).
- [3] P. Benioff, *Phys. Rev. Lett.* **48**, 1581 (1982).
- [4] R. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).
- [5] D. Deutsch, *Proc. R. Soc. London A* **400**, 97 (1985).
- [6] D. Deutsch and R. Jozsa, *Proc. R. Soc. London, A* **439**, 553 (1992).
- [7] E. Bernstein and U. Vazirani, in *Proc. of the 25th Annual Symposium on the Theory of Computing* (ACM Press, New York, 1993), p. 11-20.
- [8] D. R. Simon, in *Proc. of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 116-123.
- [9] D. DiVincenzo, *Science*, **270**, 255 (1995).
- [10] P. W. Shor, in *Proceedings of the 37th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1996), pp. 56-65.
- [11] A. Ekert and R. Jozsa, *Rev. Mod. Phys.* **68**, 733 (1996).
- [12] L. K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).
- [13] L. K. Grover, *Phys. Rev. Lett.* **80**, 4329 (1998).
- [14] A. K. Pati, “Grover’s algorithm, time-dependent search and unitary perturbation” (preprint), (1999).
- [15] S. L. Braunstein and H. J. Kimble, *Phys. Rev. Lett.* **80**, 869 (1998).
- [16] S. L. Braunstein, *Phys. Rev. Lett.* **80**, 4084 (1998).
- [17] S. Lloyd and J.-J. E. Slotine, *Phys. Rev. Lett.* **80**, 4088 (1998).
- [18] S. L. Braunstein, *Nature (London)* **394**, 47 (1998).
- [19] S. Lloyd and S. L. Braunstein, *Phys. Rev. Lett.* **82**, 1784 (1999).
- [20] A. K. Pati, S. L. Braunstein and S. Lloyd, quant-ph/0002082.
- [21] R. Cleve, A. Ekert, C. Macciavello and M. Mosca, *Proc. R. Soc. London A* **454**, 339 (1998).
- [22] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, 2000).
- [23] C. Cohen-Tannoudji, B. Diu and F. Laloë, *Quantum mechanics* (John Wiley & Sons, New York, 1977).

Chapter 5

HYBRID QUANTUM COMPUTING

Seth Lloyd

*d'Arbeloff Laboratory for Information Systems and Technology
Department of Mechanical Engineering
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139
slloyd@mit.edu*

Abstract Necessary and sufficient conditions are given for the construction of a hybrid quantum computer that operates on both continuous and discrete quantum variables. Such hybrid computers are shown to be more efficient than conventional quantum computers for performing a variety of quantum algorithms, such as computing eigenvectors and eigenvalues.

Quantum computers are devices that process information in a way that preserves quantum coherence [1, 2, 3, 4, 5, 6, 8, 9, 10, 11]. The most common model of quantum computation deals with coherent logical operations on two-state quantum variables known as qubits. Quantum computation can also be performed on variables with three or more states, and is well-defined even when the underlying degrees of freedom are continuous [12, 13, 14, 15]. This paper investigates hybrid quantum computers that operate on both discrete and continuous quantum variables. It is shown that a simple set of operations (hybrid quantum logic gates) can be used to approximate arbitrary tranformations of the variables. Hybrid versions of quantum algorithms are discussed and a hybrid version of an algorithm for finding eigenvalues and eigenvectors is presented. Hybrid quantum algorithms can have a number of advantages over conventional quantum algorithms, including lower computational complexity and an enhanced resistance to noise and decoherence.

The primary reason for investigating hybrid quantum computers is that nature contains both discrete quantum variables such as nuclear spins, photon polarizations, and atomic energy levels, and continuous variables such as position, momentum, and the quadrature amplitudes of the electromagnetic field. In conventional quantum computation, continuous variables are something of a

nuisance: either they figure as sources of noise and decoherence, as in the case of environmental baths of harmonic oscillators, or they must be restricted to a discrete set of states by cooling, as in the case of the oscillatory modes of ions in ion-trap quantum computers. In hybrid quantum computation, by contrast, the full range of continuous quantum variables can be put to use.

The basic model for performing quantum computation using a hybrid of continuous and discrete variables follows the normal model for performing quantum computation using discrete or continuous variables on their own [7, 15]. Assume that one has the ability to ‘turn on’ and ‘turn off’ the members of a set Hamiltonian operators $\{\pm H_j\}$, corresponding to the ability to apply unitary transformations of the form $e^{\pm iH_j t}$. The set of transformations that can be constructed in this fashion is the set of transformations of the form e^{-iHt} where H is a member of the algebra generated from the H_j via commutation: i.e., since $e^{iH_2 t} e^{iH_1 t} e^{-iH_2 t} e^{-iH_1 t} = e^{-[H_1, H_2]t^2} + O(t^3)$, the ability to turn on and turn off $\pm H_1$ and $\pm H_2$ allows one effectively to turn on and off $H = \pm i[H_1, H_2]$, etc. Transformations of the form e^{-iHt} for non-infinitesimal t can then be built up from infinitesimal transformations to any desired degree of accuracy.

For the sake of ease of exposition, concentrate here on discrete variables (qubits) that are spins, characterized by the usual Pauli operators $\sigma_x, \sigma_y, \sigma_z$ and to continuous variables (qunats) that are harmonic oscillators characterized by the usual annihilation and creation operators a, a^\dagger ($[a, a^\dagger] = 1$), and by the ‘position’ and ‘momentum’ operators $X = (a + a^\dagger)/2, P = (a - a^\dagger)/2i$, ($[X, P] = i$). It is convenient to think of the harmonic oscillators as modes of the electromagnetic field with X and P proportional to the quadrature amplitudes of the mode. The generalization to discrete variables with more than two states and to other forms of continuous variable is straightforward and will be discussed below.

To perform quantum computations one must be able to prepare one’s variables in a desired state, perform quantum logic operations, and read out the results. Assume that it is possible to prepare the discrete variables in the state $|0\rangle \equiv |\uparrow\rangle_z$, and the continuous variables in the vacuum state $|0\rangle$: $a|0\rangle = 0$. Assume that it is possible to measure σ_z for the discrete variables and X for the continuous variables.

Now look at performing transformations of the variables. Begin with just a pair — one spin and one oscillator. Suppose that one can turn on and turn off the Hamiltonians

$$\{\pm \sigma_x X, \pm \sigma_z X, \pm \sigma_z P\}, \quad (5.1)$$

As will now be seen, the ability to turn on and off Hamiltonians from this set allows one to enact Hamiltonians that are arbitrary polynomials of the σ ’s, X and P . Note that these Hamiltonians all represent interactions between qubits and oscillators: this is physically realistic in the sense that transformations on

physical spins or atoms are accomplished by making the spins interact with the electromagnetic field, and *vice versa*. In physically realizable situations, such as the ion traps and optical cavities discussed below, the interactions in 5.1 are turned on and off by applying laser or microwave pulses to couple discrete to continuous degrees of freedom.

Now investigate what can be accomplished by turning on and off these interactions. If the spin is prepared in the state $|0\rangle$, then turning on the Hamiltonian $\sigma_z P$ is equivalent to turning on the Hamiltonian P for the oscillator on its own. The Hamiltonian X can be turned on in a similar fashion. In order to apply this Hamiltonian for a finite amount of time, the spin must be constantly reprepared in the state $|0\rangle$ or new spins in this state must be supplied. This operation allows the construction of coherent states of the oscillator.

Now start constructing effective Hamiltonians by the method of commutation above. Since $i[P, \sigma_x X] = \sigma_x$, we can effectively turn on the Hamiltonian σ_x . Similarly for the Hamiltonian $\pm i[P, \sigma_z X] = \pm \sigma_z$. And since $i[\sigma_z, \sigma_x] = 2\sigma_y$, any single qubit transformation $e^{-i\sigma t} \in SU(2)$ can be enacted by turning on and off Hamiltonians in the set. Since $i[\sigma_z P, \sigma_z X] = 2$, an arbitrary overall phase can also be turned on and off. That is, we can enact arbitrary single qubit transformations.

Now systematically build up higher order transformations. Since $i[\sigma_z X, \sigma_x X] = 2\sigma_y X^2$, and $i[\sigma_y X^2, \sigma_x X] = 2\sigma_z X^3$, etc., we can effectively turn on and off Hamiltonians of the form σX^n , for arbitrary σ, n . Similarly, we can turn on and off Hamiltonians of the form σP^n . By preparing the spin in the state $|0\rangle$ and turning on and off the Hamiltonians $\sigma_z X^m, \sigma_z P^n$, we can enact single oscillator transformations corresponding to Hamiltonians that are arbitrary Hermitian polynomials in X and P . (Not all such Hamiltonians are bounded. Nonetheless, one can build up infinitesimal versions of such Hamiltonians and apply them for finite time to states for which they are bounded.)

So the simple set of Hamiltonians above allows the construction of arbitrary single qubit transformations and arbitrary polynomial transformations of the continuous variable, along with arbitrary interactions between the spin and the oscillator. Let us now look at more than one spin and one oscillator.

Since $i[\sigma_z^1 P, \sigma_z^2 X] = \sigma_z^1 \sigma_z^2$, we can turn on the interaction Hamiltonian $\sigma_z^1 \sigma_z^2$ between two spins 1 and 2 by making them both interact with the same oscillator. But the ability to turn on this Hamiltonian together with the ability to turn on arbitrary single-spin Hamiltonian translates into the ability to perform arbitrary transformations on sets of spins: that is, one can perform arbitrary quantum logic operations on the qubits alone.

Similarly, since $i[\sigma_y X_1, \sigma_x X_2] = 2\sigma_z X_1 X_2$, the ability to make two oscillators interact with the same spin, initially in the state $|0\rangle$, allows one to turn on the Hamiltonian $X_1 X_2$ between the two oscillators 1 and 2. But this ability, together with the ability to turn on single oscillator Hamiltonians that

are arbitrary Hermitian polynomials in X and P , translates into the ability to turn on Hamiltonians that are arbitrary Hermitian polynomials of X_i, P_i for all the oscillators together. So one can perform universal quantum computation on the continuous variables on their own.

Continuing with constructing Hamiltonians via commutation, the ability to prepare the $|0\rangle$ states for spins and oscillators, together with the ability to turn on and off the simple set 5.1 of Hamiltonians given above, allows one to effectively turn on and off Hamiltonians that are arbitrary Hermitian polynomials in $1, \sigma_x^j, \sigma_y^j, \sigma_z^j, X_k^m, P_k^n$. That is, one can perform universal quantum computation on the hybrid quantum computer.

How might such a hybrid quantum computer be realized? As it turns out, many existing designs for quantum computers are easily modified to perform hybrid quantum computation. For example, ion trap quantum computers [8, 10] operate by coupling together the internal states of ions in an ion trap (qubits) via their motional state (harmonic oscillators). Existing schemes for performing quantum computation using ion traps only use the ground and first excited state of the oscillator corresponding to the fundamental mode of the ions in the trap, effectively treating the oscillator as a qubit. But the same methods that are used to couple the ions to the oscillator can just as well be used to apply the Hamiltonians in the set 5.1 above. An ion trap with many ions has many modes, each of which can be used as a continuous variable in the hybrid quantum computation. Similarly, the Pellizzari scheme for coupling together trapped atoms (qubits) via a cavity mode of the electromagnetic field can readily be altered to use the quadrature amplitudes of the modes of the cavity, rather than simply using the lowest two energy eigenstates of a mode as a qubit [11]. Other potential continuous variables that might be used for hybrid quantum computation are the translational states of atoms in a Bose condensate, the continuum states of electrons in semiconductors, or the state of a Josephson junction circuit. Essentially any hybrid system that affords precise control over the interactions between discrete and continuous variables is a good candidate for a hybrid quantum computer.

An important concern in the construction of hybrid quantum computers is the problem of noise and decoherence. At first it might seem that continuous variables are likely to be more susceptible to noise than discrete variables. It is indeed true that more things can go wrong with a continuous variable than with a discrete variable. However, quantum error correction routines for continuous variables have been developed and require no greater overhead than those for discrete variables [12, 13, 14, 16]. Although these routines are not yet technologically practical on existing devices, it may well be that improved versions of these routines combined with existing discrete quantum error correction routines will allow efficient quantum error correction for hybrid devices. In addition, as noted above, hybrid devices have the advantage that

they include in the computation states and degrees of freedom that would normally be sources of noise, decoherence, and loss.

Now turn to applications of hybrid quantum computers. Where does the ability to perform manipulations of continuous variables as well as qubits give an advantage? The first point to note in constructing hybrid algorithms is that we must be careful to assume physically reasonable uses of hybrid variables—i.e., uses that do not require infinite or exponentially high precision. Even in the classical case, the use of continuous variables can give remarkable computational speed ups (the ability to solve NP-complete problems in polynomial time, the ability to find the answer to uncomputable problems in finite time, etc.) if one allows arbitrary precision in manipulating and measuring continuous variables. By giving an explicit construction of the operations that can be used to perform continuous variable and hybrid quantum computation, however, we have implicitly avoided the use of infinite or excessive precision: all such operations would require infinite or excessive computational resources to construct, manipulate, and measure the desired over-precise states.

With this caveat in mind, turn to the operations that are relatively easy to perform using continuous quantum variables. A particularly useful subroutine in a variety of quantum algorithms is the quantum Fourier transform: $|x\rangle \rightarrow \sum_{y=1}^q e^{ixy}|y\rangle$. In the case of discrete quantum variables the quantum Fourier transform on N qubits takes on the order of N quantum logic operations to perform. Although this is an efficient algorithm it is nonetheless difficult at present to perform quantum Fourier transforms on more than a few qubits (the current record is three) [17]. By contrast, in the case of the continuous quantum variables X and P , the quantum Fourier transform is trivial. If the eigenstates of X with eigenvalue x are written $|x\rangle$, then the eigenstates of P with eigenvalue p can be written $|p\rangle = (1/\sqrt{2\pi}) \int_{-\infty}^{\infty} e^{ipx}|x\rangle dx$. That is, the eigenstates of P are the quantum Fourier transform of the eigenstates of X . Coupling to P instead of X then allows immediate access to the Fourier transformed variable. The quantum Fourier transform on a continuous variable is accomplished by a zero-step operation. The ease of performing the quantum Fourier transform on continuous variables suggests that in devising algorithms for hybrid quantum computers we look for problems in which the quantum Fourier transform plays a central role.

Perhaps the best known quantum algorithm in which the quantum Fourier transform plays a central role is Shor's algorithm for factoring large numbers [4]. Setting aside the difficulty of performing the other operations in this algorithm (such as modular exponentiation), it is immediately clear that using a continuous variable as the register on which to perform the quantum Fourier transform in Shor's algorithm would require an exponentially high precision in the preparation and manipulation of the continuous variable. (Hybrid quantum

computation might still be used to speed up some aspects of Shor's algorithm; this possibility will be investigated elsewhere.)

A second problem in which the quantum Fourier transform plays a key role is that of simulating the dynamics of quantum systems [1, 18, 19, 20, 21]. Comparison with [18] shows that the ability of hybrid quantum computers to turn on and off simple Hamiltonians involving a few discrete and a few continuous variables at a time translates into the ability to perform efficient quantum simulations of hybrid systems.

A particularly valuable type of quantum simulation is one that allows the computation of spectra: using methods developed in [22, 23, 20] Abrams and Lloyd have developed algorithms for computing eigenvalues and eigenvectors of quantum systems and for obtaining improved estimates of the ground state [21]. In its original discrete form, the algorithm is somewhat involved. However, the fact that quantum Fourier transforms are straightforward to perform on continuous variables makes the Abrams-Lloyd algorithm particularly simple in the case of hybrid quantum computation. Here we show how to perform a quantum computation that computes the eigenvectors of a hybrid system and that writes the eigenvalues of the system onto a register consisting of a single continuous variable. The algorithm is a hybrid version of the discrete algorithms proposed in [22, 23, 20, 21] and is closest in form to the discrete algorithm proposed in [20] for simulating von Neumann measurements on a quantum computer. Independently, Travaglione and Milburn [24] have shown how methods of hybrid quantum computation can be used to compute the eigenvectors of a continuous system and write the eigenvalues onto a discrete register.

First, prepare a single continuous variable such as a mode of the electromagnetic field in the squeezed state $|x = 0\rangle = (1/\sqrt{2\pi}) \int_{-\infty}^{\infty} |p\rangle dp$. In any practical experiment, of course, such perfectly squeezed states are unavailable. Imperfectly squeezed or unsqueezed states will also work, however. As discussed below, the effect of imperfect squeezing is to decrease the resolution to which the spectrum can be obtained. Prepare a second system in the state $|\psi\rangle$ whose decomposition into energy eigenstates $|\psi\rangle = \sum_i \psi_i |E_i\rangle$ one wishes to obtain. Here we assume that the system is discrete; in general, however, system may be continuous, discrete, or a hybrid of continuous and discrete variables.

Next, using the methods of hybrid quantum computation described above, couple the system to the continuous variable via the coupling Hamiltonian HP , where H is the Hamiltonian whose eigenvalues and eigenvectors are to be obtained. For H to be efficiently simulatable, it must be equal to $\sum_k H_k$, where each H_k acts on only a few variables at a time. Since $HP = \sum_k H_k P$, if H is efficiently simulatable, so is HP , by the methods of hybrid quantum computation described above. Writing $H = \sum_j E_j |E_j\rangle\langle E_j|$, the time evolution of the

state of the system and the continuous variable is

$$\begin{aligned}
 & |\psi\rangle|x=0\rangle \\
 \rightarrow & e^{-iHPt}|\psi\rangle|x=0\rangle \\
 = & e^{-i\sum_j E_j|E_j\rangle\langle E_j|Pt} \sum_j \psi_j|E_j\rangle|x=0\rangle \\
 = & \sum_j e^{-iE_j t P} \psi_j|E_j\rangle|x=0\rangle \\
 = & \sum_j \psi_i|E_j\rangle|x=E_j t\rangle,
 \end{aligned} \tag{5.2}$$

since $e^{-iPt}|x\rangle = |x+t\rangle$. Clearly, at this point, a measurement of the variable X on the continuous variable will yield the result $x = tE_i$ with probability ψ_i , leaving the system in the state $|E_i = x/t\rangle$. That is, one can sample the spectral decomposition of $|\psi\rangle$, obtaining the eigenvalues E_i together with their corresponding weights $|\psi_i|^2$ and eigenvectors $|E_i\rangle$. The process is highly efficient, requiring only the ability to prepare the initial squeezed state $|x=0\rangle$ and to apply the Hamiltonian HP .

The hybrid eigenvalue and eigenvector finding algorithm using a continuous variable to register the eigenvalue is more efficient than the corresponding algorithm using qubits to register the eigenvalue. Since the quantum Fourier transform is performed implicitly in the continuous register, fewer steps are required in the hybrid algorithm. In addition, unlike the conventional version of the algorithm, the hybrid version is insensitive to approximate decoherence of the register in the course of the computation: measuring the value x of the register in the course of the coupling does not affect the ability of the algorithm to find eigenvectors and eigenvalues.

The requirement that the initial state of the continuous variable be perfectly squeezed can also be relaxed. Suppose that the initial state is in a Gaussian state $\int e^{-\beta x^2/2}|x\rangle dx$. For example, $\beta = 1$ gives the unsqueezed $n = 0$ vacuum state, while $\beta > 1$ gives partial squeezing in X . With this initial state for the continuous variable, after the algorithm has been run, the continuous variable and the system are in the state

$$\sum_j \int e^{-\beta x^2/2}|E_j\rangle|x+E_j t\rangle dx. \tag{5.3}$$

That is, the eigenvalues and eigenvectors are resolved to within an accuracy $1/t\sqrt{\beta}$. By coupling the system to the continuous variable for a sufficiently long time, the eigenvectors and eigenvalues of H may be determined to an arbitrary degree of accuracy, even when the initial state is unsqueezed. Note that resolving the eigenvalues of a system with an exponentially large number of states requires exponential squeezing of the pointer state. But as noted in [21], this algorithm still provides a potentially exponential speedup over classical

algorithms even when the eigenvalues are not determined to an exponential degree of accuracy.

Hybrid quantum computers are devices that perform quantum computations using both discrete variables such as spins and continuous variable such as position and momentum, or the quadrature amplitudes of the electromagnetic field. Hybrid quantum computation represents a natural extension of quantum computation using quantum bits alone: as the example of finding eigenvalues and eigenvectors presented here shows, hybrid quantum computations can be more efficient and less sensitive to noise and decoherence than conventional quantum computations. Nature supplies us with both discrete and continuous quantum variables: it is advantageous to use them.

This work was supported by DARPA/ARO under the QUIC initiative.

References

- [1] R. P. Feynman, Optics News **11**, 11 (1985); reprinted in Found. Phys. **16**, 507 (1986).
- [2] D. Deutsch, Proc. R. Soc. London A **400**, 97-117 (1985).
- [3] S. Lloyd, Science **261**, 1569-1571 (1993).
- [4] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser, (IEEE Computer Society, Los Alamitos, CA, 1994), pp. 124-134.
- [5] S. Lloyd, Sci. Am. **273**, 140-145 (1995).
- [6] D. Divincenzo, Science **270**, 255-261 (1995).
- [7] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
- [8] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091-4094 (1995).
- [9] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi and H. J. Kimble, Phys. Rev. Lett. **75**, 4710-4713 (1995).
- [10] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano and D. J. Wineland, Phys. Rev. Lett. **75**, 4714-4717 (1995).
- [11] T. Pellizzari, S. A. Gardiner, J. I. Cirac and P. Zoller, Phys. Rev. Lett. **75**, 3788-3791 (1995).
- [12] S. Lloyd and J. J.-E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).
- [13] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
- [14] S. L. Braunstein, Nature **394**, 47 (1998).
- [15] S. Lloyd, S. L. Braunstein, Phys. Rev. Lett. **82**, 1784-1787 (1999).
- [16] J. Preskill and A. Kitaev, to be published.
- [17] Y. Weinstein, S. Lloyd and D. Cory, quant-ph/9906059.

- [18] S. Lloyd, *Science* **273**, 1073 (1996).
- [19] S. Wiesner, quant-ph/9603028.
- [20] C. Zalka, *Proc. R. Soc. London A* **454**, 313-322 (1998).
- [21] D. Abrams and S. Lloyd, *Phys. Rev. Lett.* **83**(24), 5162 (1999).
- [22] A. Yu. Kitaev, quant-ph/9511026.
- [23] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, *Proc. R. Soc. London A* **454** (1969), 339 (1998).
- [24] B. C. Travaglione and G. J. Milburn, ‘Generation of eigenstates using the phase estimation algorithm,’ to be published.

Chapter 6

EFFICIENT CLASSICAL SIMULATION OF CONTINUOUS VARIABLE QUANTUM INFORMATION PROCESSES*

Stephen D. Bartlett and Barry C. Sanders

Department of Physics and Centre for Advanced Computing

– Algorithms and Cryptography

Macquarie University

Sydney, New South Wales 2109, Australia

Samuel L. Braunstein and Kae Nemoto

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

Abstract

We obtain sufficient conditions for the efficient simulation of a continuous variable quantum algorithm or process on a classical computer. The resulting theorem is an extension of the Gottesman-Knill theorem to continuous variable quantum information. For a collection of harmonic oscillators, any quantum process that begins with unentangled Gaussian states, performs only transformations generated by Hamiltonians that are quadratic in the canonical operators, and involves only measurements of canonical operators (including finite losses) and suitable operations conditioned on these measurements can be simulated efficiently on a classical computer.

Quantum mechanics allows for information processing that could not be performed classically. In particular, it may be possible to perform an algorithm efficiently on a quantum computer that cannot be performed efficiently on a classical one. Significant effort is now underway to construct quantum algorithms and processes that yield such a speedup. The Gottesman-Knill (GK)

*S. D. Bartlett, B. C. Sanders, S. L. Braunstein and K. Nemoto, Physical Review Letters **88**, 097904/1-4 (2002).

Copyright (2002) by the American Physical Society.

theorem [1] for discrete-variable (qubit) quantum information provides a valuable tool for assessing the classical complexity of a given process. Essentially, it states that any quantum algorithm that initiates in the computational basis and employs only a restricted class of gates (Hadamard, phase, CNOT, and Pauli gates), along with projective measurements in the computational basis, can be efficiently simulated on a classical computer. (For a precise formulation and proof of this remarkable theorem, see [2], page 464.) The GK theorem reveals that a large class of quantum algorithms do not provide a speedup over classical processes. In fact, recent work has placed even stronger constraints on the potential speedup of fermionic quantum computers [3].

In addition to the successes of qubit-based algorithms, quantum information over continuous variables (CV) has yielded many exciting advances, both theoretically and experimentally, in fields such as quantum teleportation [4, 5], quantum cryptography [6, 7, 8, 9], and potentially quantum computation [10]. CV algorithms could also perform computational tasks more efficiently than is possible classically. To assess the computational complexity of these tasks, it is necessary to develop an extension of the GK theorem: What continuous variable processes can be efficiently simulated on a classical computer? As a CV quantum information process involves coupled canonical systems, this question of efficient classical simulation is related to asking under what conditions a quantum mechanical system can be modeled by a classical one. As noted by Feynman [11], a key advantage of a quantum computer is its ability to simulate quantum systems that cannot be efficiently simulated classically.

The issue of efficient classical simulation of a CV process is more involved than for the discrete case. One notable difference is that the quantum states and the unitary transformations involved are described by real-valued (as opposed to integer-valued) parameters, and these parameters must be described on a discrete classical computer with some assumption of error or limited precision. Also, the states used in CV experiments are approximations to the idealized computational basis. These basis states are infinitely squeezed states whereas any experimental implementation will involve finitely squeezed states thus deviating from their idealized form [10]. A good classical simulation must be robust against such deviations. Measurements are part of the quantum computation and, even in the computational basis, are subject to experimental constraints (such as photodetection efficiency). Classical simulation must also incorporate these measurements.

Despite these complications, we prove in the following an extension of the GK theorem for continuous variables; i.e., we present a set of sufficient conditions for a CV quantum information process which, if satisfied, ensure that it can be efficiently simulated on a classical computer. To prove this theorem, we employ the techniques of stabilizers [2] that are used for qubits. Using the stabilizer formalism, it is often possible to simulate a quantum information

process by following the evolution of a set of operators, the Pauli operators, rather than the evolution of quantum states. For CV processes, we show that it is more natural to analyze stabilizers in terms of the *algebras* (i.e., Hamiltonians) that generate them, rather than the groups themselves. We define analogs of the Pauli and Clifford algebras and groups for CV and construct sets of gates (as unitary transformations) that can efficiently simulate any arbitrary transformation in these groups. Any algorithm or process constructed out of these Clifford group transformations can be efficiently modeled by following the evolution of the Pauli operators rather than the states of the system.

The standard Pauli group \mathcal{G}_n for CV quantum computation on n coupled oscillator systems is the Heisenberg-Weyl group [HW(n)], which consists of phase-space displacement operators for the n oscillators. Unlike the discrete Pauli group for qubits, the group HW(n) is a continuous (Lie) group, and can therefore only be generated by a set of continuously-parameterized operators. The algebra hw(n) that generates this group is spanned by the $2n$ canonical operators $\hat{q}_i, \hat{p}_i, i = 1, \dots, n$, along with the identity operator \hat{I} , satisfying the commutation relations $[\hat{q}_i, \hat{p}_j] = i\hbar\delta_{ij}\hat{I}$. For a single oscillator, the $n = 1$ algebra is spanned by the canonical operators $\{\hat{q}, \hat{p}, \hat{I}\}$ which generate the single oscillator Pauli operators

$$X(q) = e^{-\frac{i}{\hbar}q\hat{p}}, \quad Z(p) = e^{\frac{i}{\hbar}p\hat{q}}, \quad (6.1)$$

with $q, p \in \mathbb{R}$. The Pauli operator $X(q)$ is a position-translation operator (translating by an amount q), whereas $Z(p)$ is a momentum boost operator (kicking the momentum by an amount p). These operators are non-commutative and obey the identity

$$X(q)Z(p) = e^{-\frac{i}{\hbar}qp}Z(p)X(q). \quad (6.2)$$

On the computational basis of position eigenstates $\{|s\rangle; s \in \mathbb{R}\}$ [10, 12, 13], the Pauli operators act as

$$X(q)|s\rangle = |s + q\rangle, \quad Z(p)|s\rangle = \exp\left(\frac{i}{\hbar}ps\right)|s\rangle. \quad (6.3)$$

Note that it is conventional to use highly squeezed states to approximate position eigenstates; these states satisfy the orthogonality relation $\langle s|s'\rangle = \delta(s - s')$ in the limit of infinite squeezing.

The Pauli operators for one system can be used to construct a set of Pauli operators $\{X_i(q_i), Z_i(p_i); i = 1, \dots, n\}$ for n systems (where each operator labeled by i acts as the identity on all other systems $j \neq i$). This set generates the Pauli group \mathcal{G}_n . Note that the Pauli group is only a subgroup of all possible unitary transformations. It is not possible to construct an arbitrary unitary transformation using only the Pauli operators $X(q)$ and $Z(p)$; the Pauli group

only describes transformations generated by Hamiltonians that are linear in the canonical variables.

For issues of classical simulation, we will be interested in transformations that lie in the *Clifford group*. The Clifford group $N(\mathcal{G}_n)$ is the group of transformations, acting by conjugation, that preserves the Pauli group \mathcal{G}_n ; i.e., it is the normalizer of the Pauli group in the (infinite-dimensional) group of all unitary transformations.

Theorem 1: *The Clifford group $N(\mathcal{G}_n)$ for continuous variables is the semidirect product group $[\text{HW}(n)]\text{Sp}(2n, \mathbb{R})$, consisting of all phase-space translations along with all one-mode and two-mode squeezing transformations. This group is generated by inhomogeneous quadratic polynomials in the canonical operators.*

Proof: The most straightforward method to identify the Clifford group will be to identify its algebra. The Clifford algebra consists of all Hamiltonian operators \hat{H}_c satisfying $[\hat{H}_{\text{hw}}, \hat{H}_c] \in \text{hw}(n)$ for all $\hat{H}_{\text{hw}} \in \text{hw}(n)$. This algebra must obviously include the algebra $\text{hw}(n)$, and thus $\text{hw}(n)$ is a subalgebra of the Clifford algebra. In addition, this algebra includes all homogeneous quadratic polynomials in the canonical operators $\{\hat{q}_i, \hat{p}_i; i = 1, \dots, n\}$. This algebra of quadratics consists of Hamiltonians that generate one-mode squeezing transformations [for example, the Hamiltonian $\hat{H}_S = \frac{1}{2}(\hat{q}\hat{p} + \hat{p}\hat{q})$], and also interaction Hamiltonians that generate two-mode squeezing transformations (for example, the interaction Hamiltonian $\hat{H}_{\text{int}} = \hat{q}_1 \otimes \hat{p}_2$). The algebra of homogeneous quadratic polynomials in the canonical operators is known as the linear symplectic algebra $\text{sp}(2n, \mathbb{R})$.

Together, the algebras $\text{hw}(n)$ and $\text{sp}(2n, \mathbb{R})$ form a larger algebra, consisting of *inhomogeneous* quadratic Hamiltonians in the canonical operators $\{\hat{q}_i, \hat{p}_i; i = 1, \dots, n\}$. This algebra is the semidirect sum algebra $[\text{hw}(n)]\text{sp}(2n, \mathbb{R})$, with $\text{hw}(n)$ as an ideal. The group generated by this algebra is the semidirect product group $[\text{HW}(n)]\text{Sp}(2n, \mathbb{R})$. This group includes phase-space displacements (the Pauli group), as well as the squeezing transformations (both single- and two-mode) of quantum optics [14]. (QED)

In order to describe a quantum information process as a circuit, it is necessary to find a set of transformations (gates) that generate the Clifford group; these gates will serve as building blocks for arbitrary Clifford group transformations. Following the derivation by Gottesman *et al.* [15], a set of gates will be defined in terms of the elements of the Clifford algebra (i.e., the Hamiltonians) that generate the transformations.

The SUM gate is the CV analog of the CNOT gate and provides the basic interaction gate for two oscillator systems 1 and 2; it is defined as

$$\text{SUM} = \exp\left(-\frac{i}{\hbar}\hat{q}_1 \otimes \hat{p}_2\right). \quad (6.4)$$

This gate is an interaction gate operation on the Pauli group \mathcal{G}_2 for two systems. Referring to the definition (6.1) for the Pauli operators for a single system, the action of this gate on the \mathcal{G}_2 Pauli operators is given by

$$\begin{aligned} \text{SUM} : X_1(q) \otimes I_2 &\rightarrow X_1(q) \otimes X_2(q), \\ Z_1(p) \otimes I_2 &\rightarrow Z_1(p) \otimes I_2, \\ I_1 \otimes X_2(q) &\rightarrow I_1 \otimes X_2(q), \\ I_1 \otimes Z_2(p) &\rightarrow Z_1(p)^{-1} \otimes Z_2(p). \end{aligned} \quad (6.5)$$

This gate describes the unitary transformation used in a backaction evasion or quantum nondemolition process [14].

The Fourier transform F is the CV analog of the Hadamard transformation. It is defined as

$$F = \exp\left(\frac{i}{\hbar}\frac{\pi}{4}(\hat{q}^2 + \hat{p}^2)\right), \quad (6.6)$$

and the action on the Pauli operators is

$$\begin{aligned} F : X(q) &\rightarrow Z(q), \\ Z(p) &\rightarrow X(p)^{-1}. \end{aligned} \quad (6.7)$$

The “phase gate” $P(\eta)$ is a squeezing operation for CV, defined by

$$P(\eta) = \exp\left(\frac{i}{2\hbar}\eta\hat{q}^2\right), \quad (6.8)$$

and the action on the Pauli operators is

$$\begin{aligned} P(\eta) : X(q) &\rightarrow e^{\frac{i}{2\hbar}\eta q^2} X(q)Z(\eta q), \\ Z(p) &\rightarrow Z(p). \end{aligned} \quad (6.9)$$

[The operator $P(\eta)$ is called the phase gate, in analogy to the discrete-variable phase gate P [15], because of its similar action on the Pauli operators.]

For discrete variables, it is possible to generate the Clifford group using only the SUM, F , and P gates [15]. However, for the CV definitions above, the operators SUM, F , and $P(\eta)$ are all elements of $\text{Sp}(2n, \mathbb{R})$; they are generated by homogeneous quadratic Hamiltonians only. Thus, they are in a subgroup of the Clifford group. In order to generate the entire Clifford group, one requires a continuous HW(1) transformation [i.e., a linear Hamiltonian, that generates a one-parameter subgroup of HW(1)] such as the Pauli operator $X(q)$. This set $\{\text{SUM}, F, P(\eta), X(q); \eta, q \in \mathbb{R}\}$ generates the Clifford group.

We now have the necessary components to prove the main theorem of this paper regarding efficient classical simulation of a CV process. We employ the stabilizer formalism used for discrete variables and follow the evolution of the

Pauli operators rather than the states. To start with, let us consider the ideal case of a system with an initial state in the computational basis of the form $|q_1, q_2, \dots, q_n\rangle$. This state may be fully characterized by the eigenvalues of the generators of n Pauli operators $\{\hat{q}_1, \hat{q}_2, \dots, \hat{q}_n\}$. Any continuous variable process or algorithm that is expressed in terms of Clifford group transformations can then be modeled by following the evolution of the generators of these n Pauli operators, rather than by following the evolution of the states in the Hilbert space $\mathcal{L}^2(\mathbb{R}^n)$. The Clifford group maps linear combinations of Pauli operator generators to linear combinations of Pauli operator generators (each \hat{q}_i and \hat{p}_i is mapped to sums of $\hat{q}_j, \hat{p}_j, j = 1, \dots, n$ in the Heisenberg picture). For each of the n generators describing the initial state, one must keep track of $2n$ real coefficients describing this linear combination. To simulate such a system, then, requires following the evolution of $2n^2$ real numbers.

In the simplest case, measurements (in the computational basis) are performed at the end of the computation. An efficient classical simulation involves simulating the statistics of linear combinations of Pauli operator generators. In terms of the Heisenberg evolution, the \hat{q}_j are described by their initial eigenvalues, and the \hat{p}_j in the sum by a uniform random number. This prescription reproduces the statistics of all multi-mode correlations for measurements of these operators.

Measurement in the computational basis plus feed-forward *during* the computation may also be easily simulated for a sufficiently restricted class of feed-forward operations; in particular, operations corresponding to feed-forward displacement (not rotation or squeezing, though this restriction will be dropped below) by an amount proportional to the measurement result. Such feed-forward operations may be simulated by the Hamiltonian that generates the SUM gate with measurement in the computational basis delayed until the end of the computation. In other words, feed-forward from measurement can be treated by employing conditional unitary operations with delayed measurement [2], thus reducing feed-forward to the case already treated.

In practice, infinitely squeezed input states are not available. Instead, the initial states will be of the form

$$\hat{S}_1(r_1) \otimes \hat{S}_2(r_2) \otimes \cdots \otimes \hat{S}_n(r_n) |0, 0, \dots, 0\rangle, \quad (6.10)$$

where $|0\rangle$ is a vacuum state and $\hat{S}(r)$, $r \in \mathbb{R}$ is the squeezing operation which can be expressed directly in terms of elements of the Clifford group. Now the vacuum states may *also* be described by stabilizers $\{\hat{q}_1 + i\hat{p}_1, \hat{q}_2 + i\hat{p}_2, \dots, \hat{q}_n + i\hat{p}_n\}$ which are complex linear combinations of the generators. Combining the initial squeezing operators into the computation, a classical simulation requires following the evolution of $4n^2$ numbers (twice that of infinitely squeezed inputs due to the real and imaginary parts). Measurements in the computational basis are again easily simulated in terms of this Heisenberg

evolution, by treating each of the q_i and p_i as random numbers independently sampled from a Gaussian distribution with widths described by the vacuum state. Simulation of measurement plus feed-forward follows exactly the same prescription as before.

The condition for ideal measurements can be relaxed. Finite efficiency detection can be modeled by a linear loss mechanism [16]. Such a mechanism may be described by quadratic Hamiltonians and hence simulated by the Clifford group. Note that the Clifford group transformations are precisely those that preserve Gaussian states; i.e., they transform Gaussians to Gaussians; this observation allows us to remove our earlier restriction on feed-forward gates and allow for classical feed-forward of any Clifford group operation. Note that non-Gaussian components to the states cannot be modeled in this manner.

Finally, it should be noted that modeling the evolution requires operations on real-valued (continuous) variables, and thus must be discretized when the simulation is done on a discrete (as opposed to analog) classical computer. The discretization assumes a finite error, which will be bounded by the smaller of the initial squeezing or the final detector “resolution” due to finite efficiency, and this error must remain bounded throughout the simulation. As only the operations of addition and multiplication are required, the discretization error can be kept bounded with a polynomial cost to efficiency.

Thus, we have proved the extension of the GK theorem for continuous variables:

Theorem 2 (efficient classical simulation): *Any continuous variable quantum information process that initiates with Gaussian states (products of squeezed displaced vacuum states) and performs only (i) linear phase-space displacements (given by the Pauli group), (ii) squeezing transformations on a single oscillator system, (iii) SUM gates, (iv) measurements in position- or momentum-eigenstate basis (measurements of Pauli group operators) with finite losses, and (v) Clifford group $[\text{HW}(n)]\text{Sp}(2n, \mathbb{R})$ operations conditioned on classical numbers or measurements of Pauli operators (classical feed-forward), can be efficiently simulated using a classical computer.*

We could summarize the conditions (i-iii) by simply stating *(i-iii) transformations generated by Hamiltonians that are inhomogeneous quadratics in the canonical operators $\{\hat{q}_i, \hat{p}_i; i = 1, \dots, n\}$* , which is equivalent. Thus, any circuit built up of components described by one- or two-mode quadratic Hamiltonians [such as the set of gates SUM, F , $P(\eta)$, and $X(q)$], that initiates with finitely squeezed states and involves only measurements of canonical variables may be efficiently classically simulated.

As with the discrete-variable case, these conditions do not mean that entanglement between the n oscillator systems is not allowed; for example, starting with (separable) position eigenstates, the Fourier transform gate combined with the SUM gate can lead to entanglement. Thus, algorithms that produce entan-

lement between systems may still satisfy the conditions of the theorem and thus may be simulated efficiently on a classical computer; included are those used for CV quantum teleportation [4], quantum cryptography [6, 7, 8, 9], and error correction for CV quantum computing [12, 13]. Although these processes are of a fundamentally quantum nature and involve entanglement between systems, this theorem demonstrates that they do not provide any speedup over a classical process. Thus, our theorem provides a valuable tool in assessing the classical complexity of simulating these quantum processes.

As shown in [10], in order to generate all unitary transformations given by an arbitrary polynomial Hamiltonian (as is necessary to perform universal CV quantum computation), one must include a gate described by a Hamiltonian other than an inhomogeneous quadratic in the canonical operators, such as a cubic or higher-order polynomial. Transformations generated by these Hamiltonians do not preserve the Pauli group, and thus cannot be described by the stabilizer formalism. Moreover, *any* such Hamiltonian is sufficient [10]. One example would be to include an optical Kerr nonlinearity [17], but there is a lack of sufficiently strong nonlinear materials with low absorption. Alternatively, it has recently been proposed that a measurement-induced nonlinearity (using ideal photodetection) could be used in an optical scheme without the need for nonlinear materials in the computation [15, 18]. The physical realization of such nonlinearities is an important quest for quantum information theory over continuous variables. These nonlinear transformations can be used in CV algorithms that do not satisfy the criteria of this theorem, and which may provide a significant speedup over any classical process.

This project has been supported by an Australian Research Council Large Grant. S.L.B. and K.N. are funded in part under project QUICOV as part of the IST-FET-QJPC programme.

References

- [1] D. Gottesman, in *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney *et al.*, (International Press, Cambridge, MA, 1999), p. 32.
- [2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000), p. 464.
- [3] E. Knill, quant-ph/0108033; B. M. Terhal and D. P. DiVincenzo, quant-ph/0108010.
- [4] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
- [5] A. Furusawa *et al.*, Science **282**, 706 (1998).
- [6] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (2000).

- [7] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
- [8] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
- [9] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
- [10] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
- [11] R. P. Feynman, Found. Phys. **16**, 507 (1986).
- [12] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
- [13] S. L. Braunstein, Nature (London) **394**, 47 (1998).
- [14] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).
- [15] D. Gottesman *et al.*, Phys. Rev. A **64**, 012310 (2001).
- [16] H. P. Yuen and J. H. Shapiro, IEEE Trans. Inf. Theory **26**, 78 (1980).
- [17] G. J. Milburn and D. F. Walls, Phys. Rev. A **28**, 2065 (1983).
- [18] S. D. Bartlett and B. C. Sanders, Phys. Rev. A **65**, 042310 (2002).

II

QUANTUM ENTANGLEMENT

Chapter 7

INTRODUCTION TO ENTANGLEMENT-BASED PROTOCOLS

Samuel L. Braunstein

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

Arun K. Pati

Institute of Physics, Bhubaneswar-751005, Orissa, INDIA

Theoretical Physics Division, BARC, Mumbai, INDIA

akpati@iopb.res.in

Abstract We give a brief introduction to entanglement, teleportation, entanglement swapping and purification protocols for finite-dimensional Hilbert space systems, primarily for qubits.

1. INTRODUCTION

Quantum entanglement was first introduced by Schrödinger and explored by Einstein-Podolsky-Rosen (EPR) in their famous paper on the incompleteness of quantum theory [1]. As Schrödinger put it, the phenomenon of *entanglement* is one of the quintessential features in quantum mechanics that has no analogue in classical physics. Typically, when two quantum systems interact, the wavefunction of one can get intertwined with the wavefunction of other. The combined wavefunction of the composite system can show strong correlations even though they may be widely separated. In an attempt to understand these correlations Bell constructed an inequality that must be satisfied for all local realistic models [2]. Surprisingly, he noted that entangled states violate such inequalities. Thus demonstrating that indeed entanglement resists any classical explanation.

Over the last decade it has been realised that quantum entanglement is an important resource in quantum information and computation. In particular,

there are numerous quantum communication protocols that require shared entanglement between a pair of parties, Alice and Bob. Utilizing this shared resource together with local operations and classical communication (LOCC), Alice and Bob can perform various feats: Alice can teleport an unknown state to Bob using an entangled pair and two classical bits [3]; dense coding of classical information is possible with shared entanglement between sender and receiver [4]; and one may create entanglement between a pair of systems that have never interacted in the past, called entanglement swapping [5].

For these protocols to work perfectly one requires ideal EPR pairs. This is a problem since such states are highly prone to errors during transportation or storage. The resulting imperfect EPR pairs behave like a noisy channel in the above protocols and no longer work in an ideal manner. Fortunately, there is yet another protocol that is capable of purifying such imperfect EPR pairs (provided they are still entangled). In purification, two parties start with a given number of imperfect pairs and by performing LOCC operations they produce a smaller number of more highly entangled pairs. This process may be repeated, provided the resource has not been exhausted, until the EPR pairs are sufficiently ideal for carrying out the desired protocol.

In this article we briefly discuss entanglement, teleportation, entanglement swapping and purification protocols for finite-dimensional systems (especially for qubits). We hope this will motivate readers for the continuous variable generalizations discussed in the following chapters.

2. QUANTUM ENTANGLEMENT

Entanglement is always a property of a composite system *viewed as a system consisting of subsystems*. If the whole system is always viewed as a single object then we would not bother about the role of entanglement. Entanglement is a feature of states in Hilbert spaces which have been given a tensor product structure. In the case of a composite system consisting of *two subsystems A and B* (called a bipartite system) the combined state lives in $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. If such a system can be described by a state which can be written as

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B , \quad (7.1)$$

where $|\psi\rangle_A$ and $|\phi\rangle_B$ are states of the subsystems *A* and *B*, respectively, then the state is not entangled (which is synonymous with it being separable). If one cannot assign a definite pure state to each sub-system then it is entangled. This defines entanglement for pure states.

If the dimensions of \mathcal{H}_A is N_A and of \mathcal{H}_B is N_B then an arbitrary entangled state may be written as

$$|\Psi\rangle_{AB} = \sum_{i,j}^{N_A, N_B} c_{ij} |x_i\rangle_A |y_j\rangle_B , \quad (7.2)$$

where $\{|x_i\rangle\}$ and $\{|y_j\rangle\}$ are orthonormal basis states in the Hilbert space \mathcal{H}_A and \mathcal{H}_B , respectively. Now the Schmidt decomposition theorem tells us that by performing a singular-value decomposition of the complex matrix (c_{ij}) , we may write *any arbitrary bipartite state* as [6]

$$|\Psi\rangle_{AB} = \sum_i^{\min(N_A, N_B)} \sqrt{p_i} |i\rangle_A |i'\rangle_B , \quad (7.3)$$

where $|i\rangle_A$ and $|i'\rangle_B$ are the singular-value transformed bases and the p_i 's are non-zero eigenvalues of the reduced density matrices of the subsystem A or B . We note the $\sqrt{p_i}$ are called Schmidt numbers and $\sum_i p_i = 1$. One can see then that for pure states if there is more than one Schmidt number, then the state is entangled. It should be remembered that the Schmidt decomposition theorem holds only for a bipartite system and does not hold for tripartite systems or higher. (However, there are special conditions under which Schmidt decomposition theorem may be found for tripartite systems [7].)

More generally, states of a composite system need not be pure. If the composite system is described by a mixed state, then we need a different definition for entanglement. In general, we say that a state ρ_{AB} is separable (not entangled) on $\mathcal{H}_A \otimes \mathcal{H}_B$ if it can be written as [8]

$$\rho_{AB} = \sum_i q_i \rho_A^{(i)} \otimes \rho_B^{(i)} , \quad (7.4)$$

where $\rho_A^{(i)}$ and $\rho_B^{(i)}$ are states in \mathcal{H}_A and \mathcal{H}_B , respectively and the q_i are non-negative real weights. Such states display only classically correlations. This is because two parties may always prepare such states from locally created states plus classical communication.

One may ask how much entanglement such states contain. But to answer this question we must define a *measure of entanglement*. It has been proposed that any measure of entanglement $E(\rho)$ for a state ρ (whether ρ is pure or mixed) should satisfy three conditions [9]:

1. $E(\rho)$ should be zero if and only if ρ is separable.
2. $E(\rho)$ should be invariant under local unitary operations. This means that if $\rho \rightarrow (U_A \otimes U_B)\rho(U_A \otimes U_B)^\dagger = \rho'$, then $E(\rho) = E(\rho')$.

3. On average, entanglement cannot increase under general local measurements, local unitary operations and classical communication (LOCC) and post-selection. Mathematically, we may write this condition as

$$\sum_i \text{tr}(\rho_i) E(\rho_i / \text{tr}(\rho_i)) \leq E(\rho) , \quad (7.5)$$

where $\rho_i = A_i \rho A_i^\dagger$ and the A_i are local Kraus operators [11] satisfying $\sum_i A_i^\dagger A_i = 1$.

One universally accepted measure of entanglement for pure bipartite systems is the von Neumann entropy of either of the reduced density matrices ρ_A or ρ_B [10] which is given by

$$E(|\Psi\rangle_{AB}) = -\text{tr}(\rho_A \log \rho_A) = -\text{tr}(\rho_B \log \rho_B) = -\sum_i p_i \log p_i , \quad (7.6)$$

and has units of entangled bits or “ebits.” This can reach maximum value when all the p_i are equal. Hence the maximum amount of entanglement in this system is $\log N$ assuming $N = \min(N_A, N_B)$. One can define a maximally entangled state $|\Psi_{\max}\rangle_{AB}$ to be

$$|\Psi_{\max}\rangle_{AB} = \frac{1}{\sqrt{N}} \sum_{i=1}^N |i\rangle_A |i'\rangle_B , \quad (7.7)$$

in $\mathcal{H}^A \otimes \mathcal{H}^B$ which is a state in a space of dimension N^2 .

For two qubits, EPR pairs are the most widely studied states in quantum information theory. As an example, one canonical EPR state is given by

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) , \quad (7.8)$$

with $|0\rangle, |1\rangle$ being the computational basis states for qubits. One can easily check that if we adopt the measure of entanglement as the von Neumann entropy given in Eq. (7.6), then an EPR state contains exactly 1 ebit of entanglement which is the maximum amount of entanglement that any 2×2 -dimensional Hilbert space can admit. Hence, this EPR pair is also a maximally entangled state of two-qubits. It may be worth observing that, if we have a bipartite state in an $N \times N$ -dimensional Hilbert space with $N = 2^n$, then the state $|\Psi_{\max}\rangle$ is equivalent to n (qubit-based) EPR pairs.

We now consider a number of communication protocols that may be achieved with shared entanglement.

3. QUANTUM TELEPORTATION

Suppose that Alice and Bob are at widely separated locations. Alice wants to send an *unknown* qubit to Bob without physically sending it! How is it possible?

Let Alice and Bob share an EPR pair $|\text{EPR}\rangle_{12}$ and have access to particles 1 and 2, respectively. If Victor gives a qubit to Alice (whose identity is unknown to her) of the form

$$|\psi\rangle_a = \alpha|0\rangle_a + \beta|1\rangle_a , \quad (7.9)$$

then the combined state of the input and EPR pair is just $|\psi\rangle_a \otimes |\Psi^-\rangle_{12}$. This may be expressed in terms of a basis of “Bell-states” for particles a and 1 as

$$\begin{aligned} |\psi\rangle_a \otimes |\text{EPR}\rangle_{12} &= \frac{1}{2} \left(|\Phi^+\rangle_{a1} \otimes R^{(1)}|\psi\rangle_2 + |\Phi^-\rangle_{a1} \otimes R^{(2)}|\psi\rangle_2 \right. \\ &\quad \left. + |\Psi^+\rangle_{a1} \otimes R^{(3)}|\psi\rangle_2 - |\Psi^-\rangle_{a1} \otimes R^{(4)}|\psi\rangle_2 \right) , \end{aligned} \quad (7.10)$$

where $R^{(1)} = i\sigma_y$, $R^{(2)} = \sigma_x$, $R^{(3)} = \sigma_z$ are Pauli matrices and $R^{(4)} = \mathbb{I}$. Here the states $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$ are the canonical Bell-states first introduced in Ref. [12] as

$$\begin{aligned} |\Phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle) \\ |\Psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle) . \end{aligned} \quad (7.11)$$

We can see that if Alice now performs a joint measurement on particles a and 1 in this Bell-basis she will obtain one of four possible outcomes $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$, corresponding to two classical bits of information. Then Alice sends these two bits to Bob, who applies the appropriate unitary operation to his half of the entangled state. This converts it into the original unknown state supplied by Victor. For example, if the outcome is $|\Phi^+\rangle$ then after receiving this classical information Bob will apply $R^{(1)\dagger} = -i\sigma_y$ in order to “recreate” the original state on particle 2 at his location. This completes the quantum teleportation of a single unknown qubit. This protocol works for any of the four possible outcomes of Alice’s measurements and so it is successful every time. It should be noted that in the process the original state that was handed to Alice is destroyed and is “recreated” at Bob’s location. Hence, it does not violate the no-cloning theorem. Finally, we note that neither the quantum channel (the shared EPR pair) nor the classical communication channel provide any information about the state to be teleported. It is only when these two channels are combined that the unknown state may be transferred to Bob.

One can easily generalize quantum teleportation to higher-dimensional quantum systems (say for an N -dimensional Hilbert space). In this case the shared entangled resource is a maximally entangled state in the $N \times N$ -dimensional Hilbert space. A similar protocol to the above allows Alice to send her unknown state to Bob with the use of a classical communication channel. In this case, the communication cost is $2 \log_2 N$ classical bits or “cbits” of information.

4. DENSE CODING

Usually, from a transmitted qubit one can extract only one classical bit upon measurement. However, if the sender and receiver share prior entanglement then sending a suitably modulated version of the shared half (corresponding to one qubit) to receiver, one can now extract two classical bits of information. This doubling of classical capacity of quantum channel (with the assistance of entanglement) is called dense coding or sometimes super dense coding.

Let us imagine that Alice and Bob share a canonical Bell-state

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2) . \quad (7.12)$$

One important property of the Bell-states is that one can convert any one of them to any other by acting locally on one half of the system. In particular, Alice can apply a set of local unitary operations giving:

$$\begin{aligned} |\Phi^+\rangle_{12} &= I \otimes I |\Phi^+\rangle_{12} \\ |\Phi^-\rangle_{12} &= \sigma_z \otimes I |\Phi^+\rangle_{12} \\ |\Psi^+\rangle_{12} &= \sigma_x \otimes I |\Phi^+\rangle_{12} \\ |\Psi^-\rangle_{12} &= i\sigma_y \otimes I |\Phi^+\rangle_{12} . \end{aligned} \quad (7.13)$$

After applying any of these four local operations, Alice sends her particle to Bob. Then, by performing a Bell-measurement Bob can distinguish each case thus, extracting two classical bits of information. It may be noted that dense coding is closely related to quantum teleportation. In teleportation, one sends a single qubit via two cbits plus shared entanglement, whereas in dense coding one sends two cbits via one qubit plus shared entanglement.

5. ENTANGLEMENT SWAPPING

Entanglement swapping is a method to create entanglement between two independent particles that have never interacted in the past. Though at first glance this sounds strange, it is indeed possible in the quantum world [5].

Let us consider two independent sources each emitting an EPR pair 1, 2 and 3, 4, respectively. This means particles 1 and 2 are entangled and similarly for particles 3 and 4. However, neither 1 and 4 nor 2 and 3 are entangled. Let Alice

take particle 1, Charlie take particle 4 and Bob, the man in the middle, will take particles 2 and 3. The combined state of the system can then be written as

$$\begin{aligned} |\Psi^-\rangle_{12}|\Psi^-\rangle_{34} &= \frac{1}{2} \left(|\Psi^+\rangle_{14}|\Psi^+\rangle_{23} - |\Psi^-\rangle_{14}|\Psi^-\rangle_{23} \right. \\ &\quad \left. - |\Phi^+\rangle_{14}|\Phi^+\rangle_{23} + |\Phi^-\rangle_{14}|\Phi^-\rangle_{23} \right). \end{aligned} \quad (7.14)$$

We can now see that if Bob performs a Bell-measurement on particles 2 and 3 that he will obtain one of four possible outcomes. For instance, if the outcome of Bob's projection is the state $|\Phi^\pm\rangle_{23}$ then Alice and Charlie are found to share the entangled state $|\Phi^\pm\rangle_{14}$. Similarly for all of Bob's measurement outcome this leaves Alice and Charlie in one of the maximally entangled Bell-states. If two of the particles are subjected to a Bell-measurement then the remaining halves become entangled, despite their never having interacted.

Further, if Bob communicates to Alice and Charlie (or even to one is sufficient) which of the four Bell-states he found, then they may convert their now entangled state into any standard maximally entangled state. In a sense the entanglement has been “swapped” between the partners to the pair that Bob measured. Interestingly, this protocol can also be simply viewed as just the teleportation of an entangled state. By performing a Bell-measurement on the particles 2 and 3 Bob is able to teleport the entanglement to either (or equivalently both) recipients.

6. ENTANGLEMENT PURIFICATION

As we have already noted, in practice ideal EPR pairs may undergo decoherence and become mixed entangled states. In the absence of a maximally entangled resource one can no longer faithfully perform teleportation, dense coding or entanglement swapping. This suggests that it would be useful if we could improve the quality of imperfect EPR pairs through some other protocol. Fortunately, this is possible through “entanglement purification” [13]. Since we wish to restrict this protocol to LOCC operations we will not be able to win on average. However, provided we have some entanglement there is still the possibility of probabilistically purifying our imperfect EPR pairs.

Suppose Alice and Bob share multiple copies of an imperfectly entangled EPR pair of the form

$$\rho_{AB}(f) = f |\Psi^-\rangle_{AB}\langle\Psi^-| + \frac{1-f}{3} \left(\mathbb{I} - |\Psi^-\rangle_{AB}\langle\Psi^-| \right). \quad (7.15)$$

This state is a Werner mixture with the spin-singlet appearing with probability f . This mixture is entangled provided $f > \frac{1}{2}$ [13]. The simplest protocol works on pairs of such imperfect states at a time. By performing suitable LOCC operations [13] Alice and Bob will be able to post-select a single pair

having the form $\rho_{AB}(f')$ with $f' > f$ provided $f > \frac{1}{2}$. This process only occurs with a finite probability, however, every time it works a higher quality entangled resource is purified out of several lesser quality states. Provided pairs are available, this process may be repeated until a suitably high quality EPR pair is created. In principle, the fidelity relative to an ideal EPR can approach unity.

7. CONCLUSION

We have briefly touched on basic concepts of quantum entanglement and its utility in quantum information processing. (More details may be found in Refs. [11, 14].) Of these protocols, only entanglement purification does not straightforwardly go over to continuous variable schemes, as we shall see in the following chapters.

References

- [1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935)
- [2] J. S. Bell, Physics **1**, 195 (1964)
- [3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
- [5] M. Zukowski, A. Zeilinger, M. A. Horne and E. Ekert, Phys. Rev. Lett. **71**, 4278 (1993).
- [6] A. Peres, *Quantum Theory: Concepts and Method* (Kluwer Academic Publisher, 1995).
- [7] A. K. Pati, Phys. Lett. A **278**, 118 (2000), and references therein.
- [8] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [9] V. Vedral and M. Plenio, Phys. Rev. A **57**, 1619 (1998).
- [10] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997).
- [11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, England, 2000).
- [12] S. L. Braunstein, A. Mann and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).
- [13] C. H. Bennett, H. J. Bernstein, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
- [14] J. Preskill, *Lecture Notes*, available at
<http://www.theory.caltech.edu/people/preskill/ph229>

Chapter 8

TELEPORTATION OF CONTINUOUS QUANTUM VARIABLES*

Samuel L. Braunstein

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

H. J. Kimble

Norman Bridge Laboratory of Physics 12-33

California Institute of Technology

Pasadena, CA 91125

Abstract

Quantum teleportation is analyzed for states of dynamical variables with continuous spectra, in contrast to previous work with discrete (spin) variables. The entanglement fidelity of the scheme is computed, including the roles of finite quantum correlation and nonideal detection efficiency. A protocol is presented for teleporting the wave function of a single mode of the electromagnetic field with high fidelity using squeezed-state entanglement and current experimental capability.

Quantum mechanics offers certain unique capabilities for the processing of information, whether for computation or communication [1]. A particularly startling discovery by Bennett *et al.* is the possibility for teleportation of a quantum state, whereby an *unknown* state of a spin- $\frac{1}{2}$ particle is transported by “Alice” from a sending station to “Bob” at a receiving terminal by conveying 2 bits of classical information [2]. The enabling capability for this remarkable process is what Bell termed the irreducible nonlocal content of quantum mechanics, namely that Alice and Bob share an entangled quantum state and exploit its nonlocal characteristics for the teleportation process. For spin- $\frac{1}{2}$

*S. L. Braunstein and H. J. Kimble, Physical Review Letters **80**, 869-872 (1998).
Copyright (1998) by the American Physical Society.

particles, this entangled state is a pair of spins in a Bell state as in Bohm's version of the Einstein, Podolsky, and Rosen (EPR) paradox [3] and for which Bell formulated his famous inequalities [4].

Beyond the context of dichotomic variables, Vaidman has analyzed teleportation of the wave function of a one-dimensional particle in a beautiful variation of the original EPR paradox [5]. In this case, the nonlocal resource shared by Alice and Bob is the EPR state with perfect correlations in both position and momentum. The goal of this Letter is to extend Vaidman's analysis to incorporate finite (nonsingular) degrees of correlation among the relevant particles and to include inefficiencies in the measurement process. The "quality" of the resulting protocol for teleportation is quantified with the first explicit computation of the fidelity of entanglement for a process acting on an infinite dimensional Hilbert space. We further describe a realistic implementation for the quantum teleportation of states of continuous variables, where now the entangled state shared by Alice and Bob is a highly squeezed two-mode state of the electromagnetic field, with the quadrature amplitudes of the field playing the roles of position and momentum. Indeed, an experimental demonstration of the original EPR paradox for variables with a continuous spectrum has previously been carried out [6, 7], which when combined with our analysis, forms the basis of a realizable experiment to teleport the complete quantum state of a single mode of the electromagnetic field.

Note that up until now, all experimental proposals for teleportation have involved dichotomic variables in $SU(2)$ [2, 8, 9, 10, 11] with optical schemes accomplishing the Bell-operator measurement with low efficiency. Indeed, the recent report of teleportation via parametric down conversion [12] succeeds only *a posteriori* with rare post-selected detection events. By contrast, our scheme employs linear elements corresponding to operations in $SU(1, 1)$ [13] for Bell-state detection and thus should operate at near unit absolute efficiency, enabling *a priori* teleportation as originally envisioned in Ref. [2].

As shown schematically in Fig. 8.1, an unknown input state described by the Wigner function $W_{in}(\alpha)$ is to be teleported to a remote station, with the teleported (output) state denoted by $W_{out}(\alpha)$. In analogy with the previously proposed scheme for teleportation of the state of a spin- $\frac{1}{2}$ particle, Alice (at the sending station) and Bob (at the receiving terminal) have previously arranged to share an entangled state which is sent along paths 1 and 2. Within the context of our scheme in $SU(1, 1)$, the entangled state distributed to Alice and Bob is described by the Wigner function $W_{EPR}(\alpha_1, \alpha_2)$ [4]

$$\begin{aligned} W_{EPR}(\alpha_1; \alpha_2) &= \frac{4}{\pi^2} \exp\{-e^{-2r}[(x_1 - x_2)^2 + (p_1 + p_2)^2] \\ &\quad - e^{+2r}[(x_1 + x_2)^2 + (p_1 - p_2)^2]\} \\ &\rightarrow C \delta(x_1 + x_2) \delta(p_1 - p_2), \end{aligned} \tag{8.1}$$

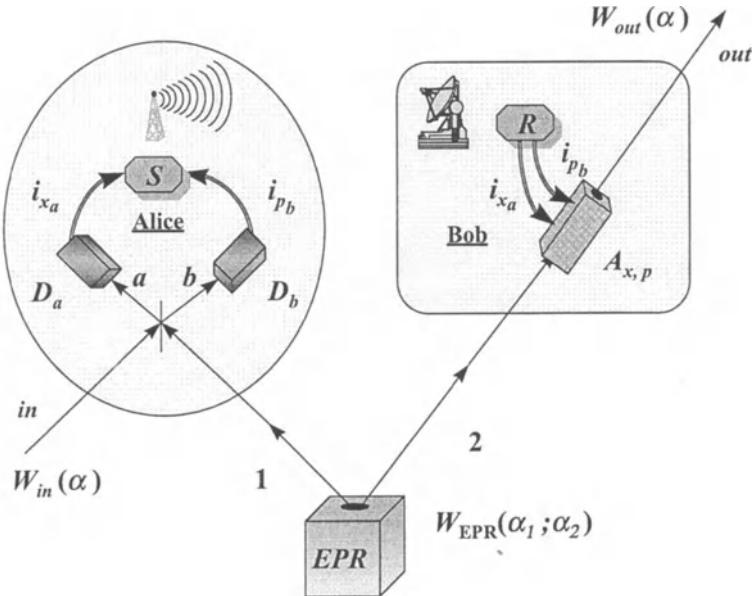


Figure 8.1 Scheme for quantum teleportation of an (unknown) input state $W_{in}(\alpha)$ from Alice's sending station S to Bob's remote receiving terminal R , resulting in the teleported output state $W_{out}(\alpha)$.

where $\alpha_j = x_j + ip_j$. Here, the real quantities (x_j, p_j) correspond to canonically conjugate variables for the relevant pathways and describe, for example, position and momentum for a massive particle, and quadrature amplitudes for the electromagnetic field. Note that for $r \rightarrow \infty$, the state described by Eq. (8.1) becomes precisely the EPR state of Ref. [3] employed by Vaidman [5] and provides an ideal entangled “pair” shared between the teleportation sending and receiving stations, albeit with divergent energy in this limit.

As for the protocol itself, the first step in teleporting the (unknown) state $W_{in}(\alpha_{in})$ is to form new variables $\beta_{a,b}$ along paths (a, b) which are linear superpositions of those of the initially independent pathways in and 1 at the sending station S of Fig. 8.1, namely $\beta_{a,b} = \frac{1}{\sqrt{2}}(\alpha_1 \pm \alpha_{in})$. The resulting Wigner function in the variables $(\beta_a; \beta_b; \alpha_2)$ exhibits “entanglement” between the paths (a, b) and the remote path 2. Step 2 at S is then to measure the observables corresponding to $\text{Re } \beta_a = \frac{1}{\sqrt{2}}(x_1 + x_{in}) \equiv x_a$ and $\text{Im } \beta_b = \frac{1}{\sqrt{2}}(p_1 - p_{in}) \equiv p_b$ at the detectors (D_a, D_b) shown in Fig. 8.1, with the resulting classical outcomes denoted by (i_{x_a}, i_{p_b}) , respectively. We define ideal measurement of (x_a, p_b) to be that for which the distribution $P_{ab}(i_{x_a}; i_{p_b})$ is identical to the associated Wigner function $W_{ab}(x_a; p_b)$. With the entangled

state of paths (1, 2) given by Eq. (8.1), we find

$$\begin{aligned} P_{ab}(i_{x_a}; i_{p_b}) &= 2 \int d^2\alpha W_{in}(\alpha) G_\nu[\sqrt{2}(i_{x_a} - i i_{p_b}) - \alpha] \\ &\equiv 2[W_{in} \circ G_\nu][\sqrt{2}(i_{x_a} - i i_{p_b})] , \end{aligned} \quad (8.2)$$

with \circ denoting convolution and G_ν as a complex Gaussian distribution with variance $\nu = \cosh 2r/2$. Note that such ideal detectors provide “perfect” information about (x_a, p_b) via (i_{x_a}, i_{p_b}) , while all information about $(p_a, x_b) \equiv (\text{Im } \beta_a = \frac{1}{\sqrt{2}}(p_1 + p_{in}), \text{Re } \beta_b = \frac{1}{\sqrt{2}}(x_1 - x_{in}))$ is lost. Furthermore, although (i_{x_a}, i_{p_b}) contains a small amount of information about the fiducial state $W_{in}(\alpha) = W_{in}(x_{in}, p_{in})$, this information goes to zero for $r \rightarrow \infty$. Nonetheless, the third and final step at the sending station is to transmit this *classical* information to the receiving terminal.

As illustrated in Fig. 8.1, receipt of (i_{x_a}, i_{p_b}) allows Bob to construct the teleported state $W_{out}(\alpha_2)$ from component 2 of the EPR state. That this resurrection is possible can be understood by examining the (unnormalized) Wigner function for the system obtained by integrating out (p_a, x_b) in correspondence to Alice’s detection of (x_a, p_b) , namely

$$G_\nu(\alpha_2) [W_{in} \circ G_\tau](\sqrt{2}(i_{x_a} - i i_{p_b}) + \tanh 2r \alpha_2) , \quad (8.3)$$

where the variance $\tau = \text{sech}2r/2$. Note that as $r \rightarrow \infty$, $G_\tau(\alpha)$ quickly approaches a delta-function, while $G_\nu(\alpha)$ describes a broad background state. Thus, for large r , the reduced state of mode 2 is described by a broad pedestal with negligible probability upon which sits a randomly located peak at $\alpha_2 \approx \sqrt{2}(i_{x_a} - i i_{p_b})$ closely mimicing the incoming state $W_{in}(\alpha)$. The location of this random “displacement” is distributed according to Eq. (8.2), and is the classical information that Alice sends to Bob.

By way of the actuator $A_{x,p}$ shown in Fig. 8.1, Bob thus performs linear displacements of the real and imaginary components of the complex amplitude α_2 to produce $\alpha_{out} = \alpha_2 + \sqrt{2}(i_{x_a} - i i_{p_b})$, where the quantities (i_{x_a}, i_{p_b}) are scaled to (x_a, p_b) . Integrating out i_{x_a} and i_{p_b} yields the ensemble description of states produced at the output of the teleportation device on an ensemble of input states W_{in} , namely

$$W_{out} = W_{in} \circ G_\sigma , \quad (8.4)$$

where $\sigma = e^{-2r}$ is the variance of the complex Gaussian G_σ , thus completing the teleportation process.

Clearly, for $r \rightarrow \infty$ the teleported state of Eq. (8.4) reproduces the original unknown state W_{in} [5]. However, note that as $r \rightarrow 0$, W_{out} also mimics W_{in} , now with *two* extra units of vacuum noise (i.e., $\sigma = \frac{1}{2} + \frac{1}{2}$). One of these

noise contributions arises from Alice's attempt to measure both (x_{in}, p_{in}) [14], while the second comes from Bob's use of this necessarily noisy information to generate a coherent state at $\sqrt{2}(i_{x_a} - i_{p_b})$. In this way *quantum mechanics extracts two tariffs* (one at each instance of the border crossing between quantum and classical domains), each of which we term the quantum duty (or *quduty*). Note that the limit $r = 0$ corresponds to what might be considered "classical" teleportation for which the "best measurement" of the coherent amplitude of the unknown state is made [14] and sent to the receiving station, where it is used to produce a coherent state of that classical amplitude. For any $r > 0$, our quantum teleportation protocol beats this classical scheme.

Before calculating an actual figure of merit for our protocol, we now specialize from general continuous variables to the case of a single mode of the electromagnetic field and thereby to actual physical implementations of the various transformations shown in Fig. 8.1. Beginning with the EPR state itself, we note that such a state can be generated by nondegenerate parametric amplification with the quantities (x_j, p_j) as the quadrature-phase amplitudes of the field [6], as has been experimentally confirmed via Type II down-conversion [7]. The linear transformation $\beta_{a,b} = \frac{1}{\sqrt{2}}(\alpha_1 \pm \alpha_{in})$ is accomplished by the simple superposition of modes *in* and 1 at a 50/50 beam splitter. The detectors (D_a, D_b) of Fig. 8.1 are now just balanced homodyne detectors with the phases of their respective local oscillators set to record (x_a, p_b) in the observed photocurrents (i_{x_a}, i_{p_b}) . Note that for unit efficiency, homodyne detection provides an ideal quantum measurement of the quadrature amplitudes required for our protocol [15, 16, 17].

Non-ideal detectors, each having (amplitude) efficiency η , may be modeled by using a pair of auxiliary beam splitters at (D_a, D_b) to introduce noise from a pair of vacuum modes described by annihilation operators $(\hat{c}_{a,b}, \hat{d}_{a,b})$ [15, 18]. It is then convenient to introduce annihilation operators corresponding to the "modes" of the photocurrents described by

$$\hat{i}_{a,b} = \eta \hat{\beta}_{a,b} + \sqrt{\frac{1 - \eta^2}{2}} (\hat{c}_{a,b} + \hat{d}_{a,b}), \quad (8.5)$$

where these fictitious objects allow us to apply an analog of the Wigner-function formalism to the photocurrents and to incorporate the effects of nonideal photodetection in a straightforward fashion. For example, loss in the response of Alice's detectors [Eq. (8.2)] leads to the convolution

$$\bar{P}_{ab}(i_{x_a}, i_{p_b}) = \frac{1}{\eta^2} [P_{ab} \circ G_\zeta]((i_{x_a} + i_{p_b})/\eta), \quad (8.6)$$

where G_ζ has variance $\zeta = (1 - \eta^2)/2\eta^2$, which goes to zero for $\eta \rightarrow 1$ in correspondence with the ideal character of homodyne detection. Substituting

for P_{ab} from Eq. (8.2) then gives

$$\bar{P}_{ab}(i_{x_a}, i_{p_b}) = \frac{2}{\eta^2} [W_{in} \circ G_{\bar{\nu}}] \left(\frac{\sqrt{2}}{\eta} (i_{x_a} - i i_{p_b}) \right), \quad (8.7)$$

where $\bar{\nu} = \frac{1}{2} \cosh 2r + (1 - \eta^2)/\eta^2$.

Within the context of the electromagnetic field, Bob can efficiently perform the required phase-space displacement of mode 2 based upon the classical information (i_{x_a}, i_{p_b}) received from Alice by combining the field of mode 2 with a (classical) coherent state of mean amplitude E/t , where $E = \sqrt{2} (i_{x_a} - i i_{p_b})/\eta$, at a highly reflecting mirror of transmissivity $t \rightarrow 0$. The mean state after this shift is the final teleported state, namely

$$W_{out} = W_{in} \circ G_{\bar{\sigma}}, \quad (8.8)$$

where $G_{\bar{\sigma}}(\alpha) = \frac{1}{\pi \bar{\sigma}} \exp(-|\alpha|^2/\bar{\sigma})$ with $\bar{\sigma} = e^{-2r} + (1 - \eta^2)/\eta^2$.

The teleportation evolution described by Eq. (8.8) may be written in density matrix form as

$$\hat{\rho}_{out} = \int d^2\xi G_{\bar{\sigma}}(\xi) \hat{D}(i\xi) \hat{\rho}_{in} \hat{D}^\dagger(i\xi), \quad (8.9)$$

where $\hat{\rho}_{in}$ is the original state being teleported and $\hat{D}(\alpha)$ is the displacement operator. The dynamics associated with Eq. (8.9) were first studied by Glauber [19] and Lachs [20] for an “incoming” vacuum state $\hat{\rho} = |0\rangle\langle 0|$ and for squeezed vacuum by Vourdas and Weiner [21]. The detailed behavior of the photocount statistics under this dynamics was investigated by Musslimani *et al.* [22]. These references also relate the development of the convolutional formalism used here (see also Refs. [23, 24]).

To illustrate the protocol, consider teleportation of the coherent superposition state

$$|\psi\rangle \propto |+\alpha\rangle + e^{i\phi}|-\alpha\rangle, \quad (8.10)$$

with corresponding Wigner function $W_{in}(\alpha)$ illustrated in Fig. 8.2(a). The teleported Wigner function $W_{out}(\alpha)$ as computed from Eq. (8.8) is shown in Fig. 8.2(b) for parameters corresponding to -10 dB of squeezing (i.e., $r = 1.15$) with efficiency $\eta^2 = 0.99$, which should be compared to the parameters of Ref. [25] [namely squeezing $r = 0.69$ (i.e., 6 dB of squeezing), and detectors with absolute quantum efficiency $\eta^2 = 0.99 \pm 0.02$]. Note that the quantum character of the state survives teleportation, including negative values for W_{out} associated with quantum interference for the off-diagonal components of $\hat{\rho}_{in}$. For comparison, note that for classical teleportation (i.e., $r = 0$), W_{out}^{cl} consists of the (incoherent) superposition of two distributions centered at $\pm\alpha$, each of which is broadened by the *qudity*.

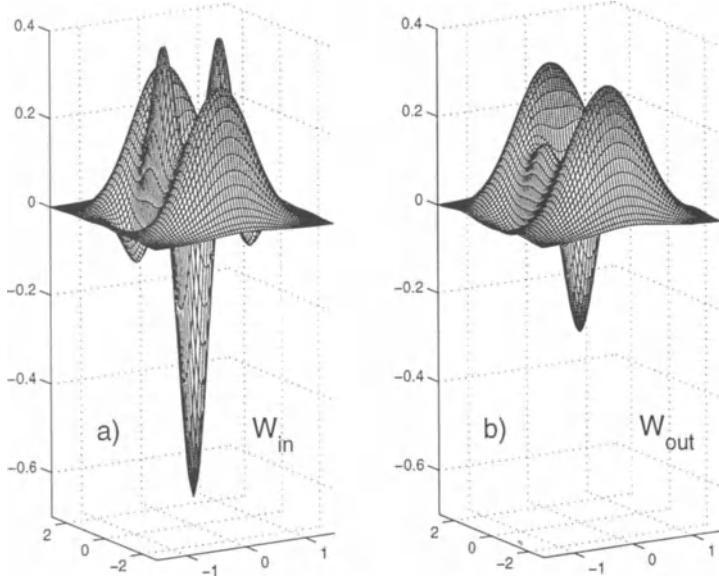


Figure 8.2 (a) Wigner function $W_{in}(\alpha)$ for the input state of Eq. (8.10) with $\alpha = 1.5i$ and $\phi = \pi$. (b) Teleported output state $W_{out}(\alpha)$ for $r = 1.15$ and $\eta^2 = 0.99$.

To provide a quantitative measure of the “quality” of the output state, we note that the strongest measure of fidelity of a teleported state relative to the input state is given by the *entanglement fidelity* [26]. For processes described by Eq. (8.9), it is given by

$$F_e = \int d^2\xi G_{\bar{\sigma}}(\xi) |\chi_{W_{in}}(\xi)|^2, \quad (8.11)$$

where $\chi_{W_{in}}(\xi) = \text{tr } \hat{D}(i\xi) \hat{\rho}_{in}$ is the characteristic function for the incoming state’s Wigner function.

For the coherent superposition of Eq. (8.10) direct substitution yields a fidelity of entanglement F_e of

$$\frac{1}{1 + \bar{\sigma}} - \frac{1 + e^{-4|\alpha|^2} - \exp\left(\frac{-4\bar{\sigma}|\alpha|^2}{1 + \bar{\sigma}}\right) - \exp\left(\frac{-4|\alpha|^2}{1 + \bar{\sigma}}\right)}{2(1 + \bar{\sigma})(1 + e^{-2|\alpha|^2} \cos \phi)^2}. \quad (8.12)$$

For the state shown in Fig. 8.2(b) this fidelity is 0.6285 for $r = 1.15$ and $\eta^2 = 0.99$ compared to 0.2487 for $r = 0$ and the same detector efficiency. This latter fidelity precludes observation of any quantum features in the classically teleported state, while the former case yields observable quantum characteristics as seen in Fig. 8.2.

Beyond any one particular state, let us now concentrate on high fidelity teleportation in general. In this case the Gaussian weighting described by $G_{\bar{\sigma}}$ is sufficiently narrow so that only the lowest terms in an expansion about $\xi = 0$ of $\chi_{W_{in}}$ will contribute. That is, $|\chi_{W_{in}}(\xi)|^2$ may be approximated by

$$1 - \xi^{*2}(\Delta\alpha)^2 - \xi^2(\Delta\alpha^*)^2 - 2|\xi|^2|\Delta\alpha|^2, \quad (8.13)$$

where $|\Delta\alpha|^2 \equiv \langle |\alpha|^2 \rangle - |\langle \alpha \rangle|^2$ averaged over $W_{in}(\alpha)$. Thus, the condition for high fidelity teleportation (i.e., $1 - F_e \ll 1$) becomes $1/|\Delta\alpha|^2 \gg \bar{\sigma}$. Now $|\Delta\alpha|^2$ is just the number of photons (plus $\frac{1}{2}$) in the incoming state *after* it has been shifted so as to have *no* coherent amplitude. Roughly speaking it is the maximal rms spread of the Wigner function of the unknown quantum state being teleported and so its reciprocal bounds the size of “important” small scale features in that state, though there can indeed be smaller features. Apparently then the condition for high entanglement fidelity says that features in the Wigner function smaller than $1/|\Delta\alpha|$ do not give a significant contribution to the state’s identity.

In conclusion, our analysis suggests that existing experimental capabilities should suffice to teleport manifestly quantum or nonclassical states of the electromagnetic field with reasonable fidelity. For such experiments, extensions of our analysis to the teleportation of broad bandwidth information must be made and will be discussed elsewhere. In qualitative terms, our scheme should allow efficient teleportation every inverse bandwidth, in sharp contrast to relatively rare transfers for proposals involving weak down conversion for spin degrees of freedom. Although our analysis is the first to obtain explicitly the fidelity of entanglement on an infinite dimensional Hilbert space, an unresolved issue is whether or not our protocol is “optimum,” either with respect to this measure or with regard to other criteria in the area of quantum communication (e.g., the ability to teleport optimally an “alphabet” $\{j\}$ of orthogonal states W_{in}^j). More generally, the work presented here is part of a larger program to extend classical communication with complex amplitudes into the quantum domain.

S.L.B. was funded in part by EPSRC Grant No. GR/L91344 and a Humboldt Fellowship. H.J.K. acknowledges support from DARPA via the QUIC Institute administered by ARO, from the Office of Naval Research, and from the National Science Foundation. Both appreciate the hospitality of the Institute for Theoretical Physics under National Science Foundation Grant No. PHY94-07194.

References

- [1] A. Steane, LANL Report No. quant-ph/9708022; A. S. Holevo, LANL Report No. quant-ph/9708046.
- [2] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [3] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
- [4] J. S. Bell, in *Speakable and Unspeakable in Quantum Mechanics* (Cambridge Univ. Press, 1988), p. 196.
- [5] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
- [6] M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988); M. D. Reid, Phys. Rev. A **40**, 913 (1989).
- [7] (a) Z. Y. Ou, S. F. Pereira, H. J. Kimble and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992); (b) Appl. Phys. B **55**, 265 (1992).
- [8] L. Davidovich, N. Zagury, M. Brune, J. M. Raimond and S. Haroche, Phys. Rev. A **50**, R895 (1984).
- [9] J. I. Cirac and A. S. Parkins, Phys. Rev. A **50**, R4441 (1994).
- [10] T. Sleator and H. Weinfurter, Ann. N. Y. Acad. Sci. **755**, 715 (1995).
- [11] S. L. Braunstein and A. Mann, Phys. Rev. A **51**, R1727 (1995); **53**, 630(E) (1996).
- [12] D. Boumeester *et al.*, Nature (London) **390**, 575 (1997).
- [13] B. Yurke, S. L. McCall and J. R. Klauder, Phys. Rev. A **33**, 4033 (1986).
- [14] E. Arthurs and J. L. Kelly Jr., Bell. Syst. Tech. J. **44**, 725 (1965).
- [15] H. P. Yuen and J. H. Shapiro, IEEE Trans. Inf. Theory **26**, 78 (1980).
- [16] S. L. Braunstein, Phys. Rev. A **42**, 474 (1990).
- [17] Z. Y. Ou and H. J. Kimble, Phys. Rev. A **52**, 3126 (1995).
- [18] K. Banaszek and K. Wódkiewicz, Phys. Phys. A **55**, 3117 (1997).
- [19] R. J. Glauber, Phys. Rev. **131**, 2766 (1963).
- [20] G. Lachs, Phys. Rev. **138**, B1012 (1965).
- [21] A. Vourdas and R. M. Weiner, Phys. Rev. A **36**, 5866 (1987).
- [22] Z. H. Musslimani, S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. A **51**, 4967 (1995).
- [23] M. S. Kim and N. Imoto, Phys. Rev. A **52**, 2401 (1995).
- [24] K. Banaszek and K. Wódkiewicz, Phys. Rev. Lett. **76**, 4344 (1996).
- [25] E. S. Polzik, J. Carri and H. J. Kimble, Phys. Rev. Lett. **68**, 3020 (1992); (b) Appl. Phys. B **55**, 279 (1992).
- [26] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).

Chapter 9

EXPERIMENTAL REALIZATION OF CONTINUOUS VARIABLE TELEPORTATION

Akira Furusawa

*Department of Applied Physics, University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

H. J. Kimble

*Norman Bridge Laboratory of Physics
California Institute of Technology, mc12-33
Caltech, Pasadena, CA91125, USA*

1. INTRODUCTION

Quantum teleportation is a method of quantum state transportation with a classical channel and a quantum channel [1]. In this technique, the “information” contained in a quantum state is transferred from a sending station (Alice) to a receiving station (Bob), with the original quantum state thereby reconstructed at Bob’s place with the received information and previously shared entanglement. Note that it is impossible to perform the state transformation represented by quantum teleportation only with a classical channel, which can be qualitatively explained as follows. If one attempts to obtain complete information with some particular measurement on an unknown quantum state of motion, for example, then both position and momentum (canonically conjugate variables) must be determined simultaneously with negligible error, which is of course impossible [2]. It is thus impossible for Alice to obtain complete information on the unknown quantum state, so that she certainly cannot send enough information for the reconstruction of the state to Bob. He then is unable to reconstruct the complete state at his place. By contrast, in quantum teleportation, Alice and Bob neatly circumvent constraints that would otherwise be imposed on Alice’s state measurement and Bob’s state generation, and are thereby able to reconstruct the original state at Bob’s place.

The essential character for this trick is quantum entanglement. For the case of continuous quantum variables, the quantum entanglement is that discussed by Einstein, Podolsky, and Rosen, in now the famous “EPR paradox” [3]. The sharing of quantum entanglement between Alice and Bob is the critical resource employed to enable the kind of quantum information transfer implicit in quantum teleportation.

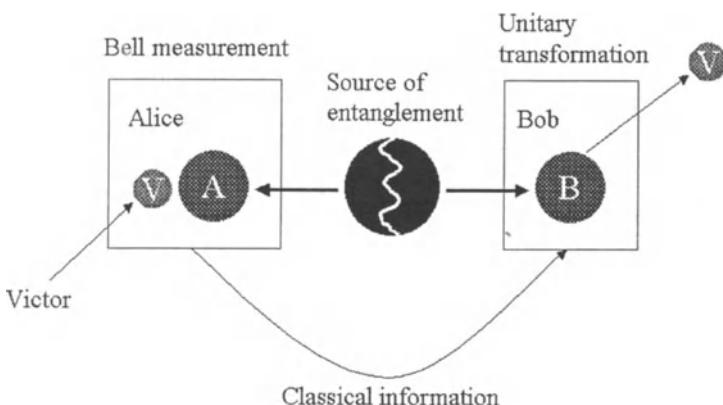


Figure 9.1 Quantum teleportation.

In general terms, teleportation protocols proceed as follows. Alice and Bob must first share two components of an entangled state. Alice makes a joint “measurement” (generalized Bell-state measurement) of an unknown state $|\psi\rangle$ (which is to be teleported) together with her component of the EPR pair. For the purpose of verifying the protocol, $|\psi\rangle$ is created by Victor (the “verifier”). Conditioned upon Alice’s measurement, the overall state “collapses” into a state for which Bob’s component of EPR state is related to $|\psi\rangle$ by a simple unitary transformation, which is however unknown to Bob. Fortunately, receipt of the measurement result (classical information) from Alice enables Bob to perform an appropriate (unitary) transformation of his component of the original EPR state to obtain a “recreation” of the original state $|\psi\rangle$ at his place, as can then be verified by Victor for the output from Bob’s station. In some sense, Alice and Bob share “quantum uncertainty” and subtract it at Bob’s place to reconstruct $|\psi\rangle$.

Quantum teleportation was originally proposed by Bennett et al. [1], with two-dimensional systems (e.g., the states of spin $\frac{1}{2}$ particles) having received the greatest attention. Initial experiments were directed toward the polarization states of single photons [4, 5]. However, the nature of the down conversion process used for the generation of the initial state and of the quantum entanglement together with the overall low efficiencies precluded these experiments from crossing the boundary between classical and quantum teleportation [6, 7, 8, 9]. An essential difficulty was the lack of ability to perform a complete set of Bell-state measurements, which for spin $\frac{1}{2}$ particles (or photon polarization) requires simple (but as yet unattainable) quantum logic between Alice's component of the entangled Bell pair and the unknown state.

On a different front, quantum teleportation with continuous variables in an infinite dimensional Hilbert space was first proposed by Vaidman [10]. His proposal was further investigated theoretically by Braunstein and Kimble, who introduced a teleportation scheme with non-singular squeezed-state entanglement [11]. This latter scheme was experimentally demonstrated by the Quantum Optics group at Caltech in 1998 [12]. Somewhat remarkably, in this scheme complete Bell-state measurements can be performed by way of quadrature-phase measurements with homodyne techniques whose detection efficiency can be close to unity. The high detection efficiency of this scheme together with the EPR entanglement generated via summing of independent squeezed beams enabled the boundary between the classical and quantum teleportation to be crossed for the first time. More specifically, a teleportation fidelity of 0.58 ± 0.02 was obtained for the teleportation of coherent states, where the relevant quantum-classical boundary is 0.50 for this experiment [8, 9]. "Bona fide" quantum teleportation was thus realized for the first time in this experiment with continuous variables, which we discuss in more detail in this chapter.

2. EXPERIMENTAL REALIZATION OF CONTINUOUS VARIABLE TELEPORTATION

2.1 EPR CORRELATION

The quantum entanglement relevant to our continuous variable teleportation experiment is the EPR correlation as in the original 1935 paper [3], which relates to the canonically conjugate position and momentum variables. As was originally pointed out by Reid and Drummond [13], the EPR *gedanken* experiment can be realized via the quadrature-phase amplitudes of a single-mode of the electromagnetic field, since these variables are also canonically conjugate in direct correspondence to position and momentum. Indeed, the first realization of the EPR experiment was accomplished by way of the quadrature-phase amplitudes using nondegenerate parametric down-conversion process

with type-II phase matching [14]. An equivalent EPR state can also be produced with type-I phase matching and a half beam splitter [12]. This state is called a two-mode squeezed vacuum. In the Heisenberg representation, the quadrature-phase amplitude operators (\hat{x}_j, \hat{p}_j) are transformed as follows [15, 16].

$$\begin{aligned}\hat{x}_1 &= \frac{1}{\sqrt{2}}e^r\hat{\tilde{x}}_1^{(0)} + \frac{1}{\sqrt{2}}e^{-r}\hat{\tilde{x}}_2^{(0)}, \\ \hat{p}_1 &= \frac{1}{\sqrt{2}}e^{-r}\hat{\tilde{p}}_1^{(0)} + \frac{1}{\sqrt{2}}e^r\hat{\tilde{p}}_2^{(0)}, \\ \hat{x}_2 &= \frac{1}{\sqrt{2}}e^r\hat{\tilde{x}}_1^{(0)} - \frac{1}{\sqrt{2}}e^{-r}\hat{\tilde{x}}_2^{(0)}, \\ \hat{p}_2 &= \frac{1}{\sqrt{2}}e^{-r}\hat{\tilde{p}}_1^{(0)} - \frac{1}{\sqrt{2}}e^r\hat{\tilde{p}}_2^{(0)},\end{aligned}\quad (9.1)$$

where $\hat{a}_j = \hat{x}_j + i\hat{p}_j$ (\hat{a}_j : annihilation operator), a superscript (0) denotes initial vacuum modes, r is the squeezing parameter, and path 1, 2 correspond to the pathways to Alice and Bob, respectively. Here, for $r \rightarrow \infty$ the state becomes the ideal EPR state: $(\hat{x}_1 - \hat{x}_2) \rightarrow 0, (\hat{p}_1 + \hat{p}_2) \rightarrow 0$. Note that r is certainly not infinite in any real experiment; however, entanglement exists for any finite value of $r > 0$ (even infinitesimal r and even in the presence of loss). [17, 18]

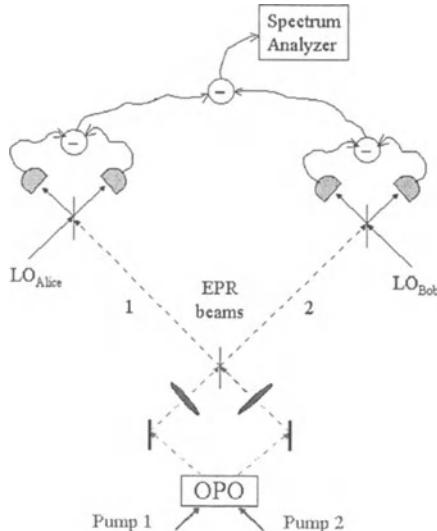


Figure 9.2 Experimental setup for the test of the EPR correlation of continuous variables.

Figure 9.2 shows the experimental setup for the realization of EPR correlation of continuous variables [12, 14]. Two squeezed vacuum beams are created by parametric down conversion in a subthreshold optical parametric oscillator (OPO). The OPO consists of a ring cavity and a potassium niobate $KNbO_3$ crystal and has two independent opposite circulations. Two pump beams (430nm) drive the OPO in the opposite directions; these pump beams are created by way of second harmonic generation with another $KNbO_3$ crystal in an external buildup cavity which is itself driven by the fundamental 860nm-output of a titanium:sapphire $Ti : Al_2O_3$ laser. The two squeezed vacuum beams are combined with a half beam splitter, where the relative phases of the input squeezed vacuum beams are locked to be $\frac{\pi}{2}$ with respect to each other. The beams emerging from the beam splitter are in a two-mode squeezed vacuum, thereby realizing entangled EPR beams. One of the EPR beams goes to Alice's station and the other beam goes to Bob's station. Alice and Bob's stations consist in the first instance of homodyne detectors which enable us to confirm the correlation (and hence entanglement [17, 18]) between the beams by way of the difference of the photocurrent from the detectors. This difference signal corresponds to $(\hat{x}_1 - \hat{x}_2)$ or $(\hat{p}_1 + \hat{p}_2)$ depending upon the relative phase chosen between Alice and Bob's local oscillators (LO_{Alice}, LO_{Bob}) [14].

Operationally speaking, the electromagnetic fields employed in experiments such as these are not single-mode but rather have finite bandwidth. The single-mode treatment must be generalized to the case of multimode fields of finite bandwidth, as discussed in detail in Ref. [14]. In this situation, the relevant quantities are the spectral components $(\hat{x}(\Omega), \hat{p}(\Omega))$ of the quadrature-phase amplitudes, where a general quadrature-phase amplitude at phase δ is defined by

$$\hat{z}(\Omega, \delta) \equiv \frac{1}{2} \int_{\Omega-\Delta\Omega}^{\Omega+\Delta\Omega} d\Omega' [\hat{a}(\Omega') \exp(-i\delta) + \hat{a}^\dagger(-\Omega') \exp(+i\delta)] \quad (9.2)$$

with $\hat{a}(\hat{a}^\dagger)$ as the annihilation (creation) operator for the field at offset Ω from the optical carrier, with $(\hat{x}(\Omega), \hat{p}(\Omega)) = (\hat{z}(\Omega, 0), \hat{z}(\Omega, \pi/2))$, and with the integration extending over a small interval $\Delta\Omega$ about Ω . Then, the spectral density of photocurrent fluctuations $\Psi(\Omega)$ obeys the following relation,

$$\Psi(\Omega)\Delta\Omega \sim \langle \hat{z}^2(\Omega, \delta) \rangle. \quad (9.3)$$

In simple terms, the overall treatment for the multimode case remains essentially unchanged from the single-mode case. However, now the relevant state describes the electromagnetic field at frequency offset $\pm\Omega$ within a bandwidth $\Delta\Omega$ about the carrier ω_L (laser frequency); that is to say, AM and FM modulation sidebands.

Figure 9.3 shows an experimental result for the setup shown in Figure 9.2. In Figure 9.3, the horizontal axis corresponds to the relative phase between

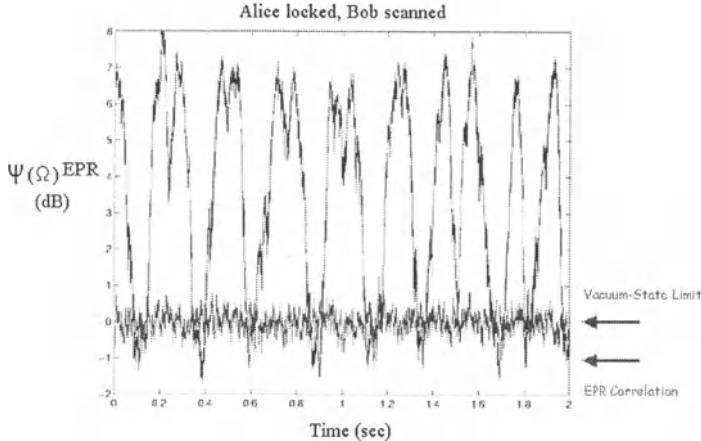


Figure 9.3 EPR correlation for Alice and Bob beyond the vacuum-state limit.

Alice and Bob's local oscillators. Actually the phase of Alice's local oscillator (LO) is locked to the phase of the EPR beam, and the phase of Bob's LO is scanned. The vertical axis represents the photocurrent fluctuation $\Psi(\Omega)^{EPR}$ for the difference output between Alice and Bob's photocurrents. Note that $\Psi(\Omega)^{EPR} = 0\text{dB} \equiv \Psi_0$ corresponds to the classical limit of the difference output without quantum correlation. It is determined experimentally without inputs to Alice and Bob's homodyne detectors (i.e., with vacuum inputs to their detectors), and is the level arising from uncorrelated vacuum fluctuations at each of the balanced detectors (i.e., two units of vacuum noise). Most importantly is to examine the minima for $\Psi_{\min}(\Omega)^{EPR}$, which corresponds to a quantum correlation between Alice and Bob's output $[(\hat{x}_1 - \hat{x}_2) \text{ or } (\hat{p}_1 + \hat{p}_2)]$ if and only if $\Psi_{\min} < \Psi_0$, which is indeed the case in Figure 9.3. In fact, the work of Refs. [17, 18] ensures that the observation $\Psi_{\min} < \Psi_0$ is sufficient as to guarantee that the beams are entangled. Of course, for the ideal EPR state, the level Ψ_{\min} would become arbitrarily small as compared to Ψ_0 (tending to $-\infty$ when expressed on a logarithmic scale as in Figure 9.3). The maximum value Ψ_{\max} of the periodical curve indicates the level of anticorrelation implicit in the EPR state. The shape of the curve rising and falling between Ψ_{\min} and Ψ_{\max} shows the appearance of correlation and an anticorrelation between the quadrature amplitudes at Alice and Bob's station as the relative phase between Alice and

Bob is scanned. The existence of quantum correlation and hence entanglement in both quadrature-phase amplitudes (\hat{x} and \hat{p}) is thereby confirmed.

2.2 TELEPORTATION EXPERIMENT

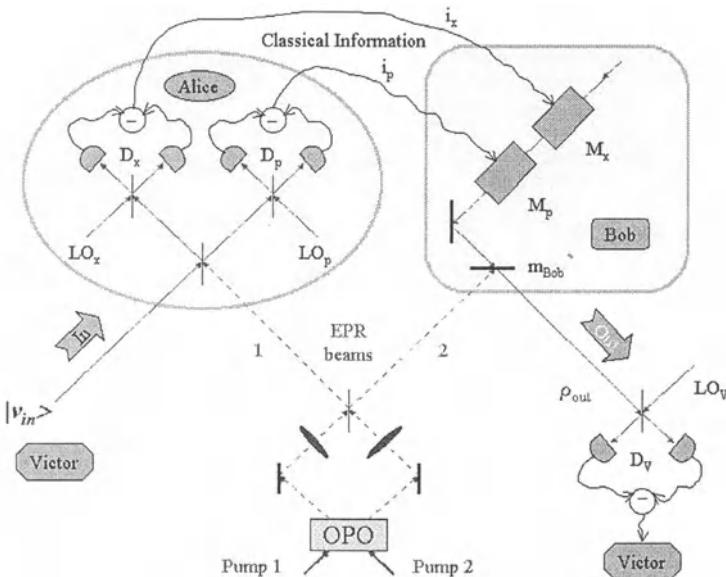


Figure 9.4 Experimental setup for the continuous variable teleportation [12].

Having discussed briefly the operational verification of entanglement for the EPR beams, we next turn to the experimental setup for the continuous-variable teleportation as shown in Figure 9.4. First Alice and Bob share the EPR beams that are created with the technique described in the previous subsection. The state of the electromagnetic field to be teleported ($\hat{x}_{in}, \hat{p}_{in}$) is created by Victor, which for our experiment is more precisely a particular set of modulation sidebands (coherent state). The beam to be teleported is combined with Alice's EPR beam (\hat{x}_1, \hat{p}_1) by using a half beam splitter. This process creates states

described by the quadrature amplitudes (\hat{x}_u, \hat{p}_u) and (\hat{x}_v, \hat{p}_v) , where

$$\begin{aligned}\hat{x}_u &= \frac{1}{\sqrt{2}}\hat{x}_{in} - \frac{1}{\sqrt{2}}\hat{x}_1, \\ \hat{p}_u &= \frac{1}{\sqrt{2}}\hat{p}_{in} - \frac{1}{\sqrt{2}}\hat{p}_1, \\ \hat{x}_v &= \frac{1}{\sqrt{2}}\hat{x}_{in} + \frac{1}{\sqrt{2}}\hat{x}_1, \\ \hat{p}_v &= \frac{1}{\sqrt{2}}\hat{p}_{in} + \frac{1}{\sqrt{2}}\hat{p}_1.\end{aligned}\quad (9.4)$$

Alice makes a measurement of both quadrature-phase amplitudes \hat{x}_u and \hat{p}_v by using two homodyne detectors and gets the classical values x_u and p_v . This measurement corresponds to the Bell-state measurement of continuous variables. In the ideal case ($r \rightarrow \infty$), Alice cannot get any information on the state itself because the amount of quantum “noise” (e^{2r}) in (\hat{x}_1, \hat{p}_1) is big enough to hide the information on the state to be teleported, which is a key feature of the measurement protocol. If, by contrast, she were to attempt to measure directly both quadrature-phase amplitudes of the state to be teleported simultaneously without the entangled input, she would get only partial information [2], and in the process destroy the state.

Figure 9.5 shows the outputs of one of Alice’s homodyne detectors. The horizontal axis corresponds to the phase of Alice’s local oscillator θ_{Ax} , which is being swept in time. The vertical axis $\Psi(\Omega)_x^{Alice}$ corresponds to spectral density of photocurrent fluctuations associated with the quadrature amplitude $\hat{x}_u(\Omega, \theta_{Ax})$, where the maxima in $\Psi(\Omega)_x^{Alice}$ give the power (relative to the vacuum state) for the amplitude $\hat{x}_u(\Omega, \theta_{Ax} = 0) \equiv \hat{x}_u(\Omega)$. In this experiment, Victor generates a coherent state which consists of a classical phase-space displacement and one unit of vacuum noise. The peak value in the periodic modulation of $\Psi(\Omega)_x^{Alice}$ in the figure corresponds to the power associated with $\frac{1}{\sqrt{2}}$ of the coherent displacement (-3dB), which is 22dB higher than the vacuum noise level in this particular case. The reduction by 3dB arises because the intensity of the unknown state is reduced by half by the beam splitter for mixing the unknown state and Alice’s EPR beam. The minima in the periodic variation of $\Psi(\Omega)_x^{Alice}$ are equivalent to the level of the corresponding flat trace Λ_x^{Alice} , which is the quantum noise level with Alice’s EPR beam present. The associated level without Alice’s EPR beam is $\Phi_{0,x}^{Alice}$ (with a vacuum-state input). The figure shows the quantum noise level with her EPR beam is higher than the level without her EPR beam, namely $\Lambda_x^{Alice} > \Phi_{0,x}^{Alice}$, in correspondence to a loss of information by Alice for quantum teleportation. Note that the quantum noise level with her EPR beam would diverge in the ideal case ($r \rightarrow \infty$).

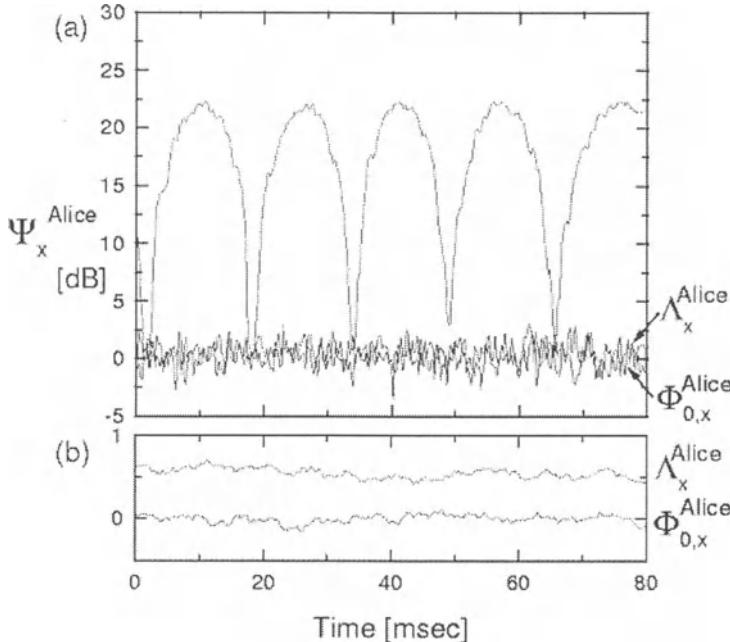


Figure 9.5 Output of one of Alice's homodyne detectors (D_x). $\Omega/2\pi = 2.9MHz$ and $\Delta\Omega/2\pi = 30kHz$. The part (b) is the expanded view with a ten-trace average for the input state which has no displacements, namely vacuum state. [12]

By way of Equation (9.4), Bob's EPR beam (\hat{x}_2, \hat{p}_2) is represented as follows [15],

$$\begin{aligned}\hat{x}_2 &= \hat{x}_{in} - \sqrt{2}e^{-r}\hat{\tilde{x}}_2^{(0)} - \sqrt{2}\hat{x}_u, \\ \hat{p}_2 &= \hat{p}_{in} + \sqrt{2}e^{-r}\hat{\tilde{p}}_1^{(0)} - \sqrt{2}\hat{p}_v.\end{aligned}\quad (9.5)$$

Alice's generalized Bell-state measurement results effectively in the quantum variables \hat{x}_u and \hat{p}_v being transformed into the classical variables x_u and p_v in the Equation (9.5). When the quantum efficiency of the homodyne detectors (η) is less than unity, the x_u and p_v fluctuate under the influence of the invasion of vacuum noise. In this case, \hat{x}_u and \hat{p}_v in the Equation (9.5) are replaced by $\eta\hat{x}_u + \sqrt{1 - \eta^2}\hat{\tilde{x}}_u^{(0)}$ and $\eta\hat{p}_v + \sqrt{1 - \eta^2}\hat{\tilde{p}}_v^{(0)}$, respectively, where $\hat{\tilde{x}}_u^{(0)}$ and $\hat{\tilde{p}}_v^{(0)}$ are the quadrature amplitudes of the respective invading vacua.

Alice sends the measurement results x_u and p_v to Bob. He uses this information to modulate a (coherent) light beam in both amplitude and phase, with some overall gain g [12]. This modulated beam is then combined coherently at the highly reflecting mirror m_{Bob} shown in Figure 9.4 to interfere with his component of the entangled EPR beam (\hat{x}_2, \hat{p}_2) , thereby creating the teleported output state $(\hat{x}_{tel}, \hat{p}_{tel})$. This procedure corresponds to a simple phase-space displacement of Bob's EPR beam as follows:

$$\begin{aligned}\hat{x}_{tel} &= \hat{x}_2 + g\sqrt{2}x_u, \\ \hat{p}_{tel} &= \hat{p}_2 + g\sqrt{2}p_v.\end{aligned}\quad (9.6)$$

In the absence of losses ($\eta = 1$) and for unity gain ($g = 1$), the quadrature operators associated with the teleported state become

$$\begin{aligned}\hat{x}_{tel} &= \hat{x}_{in} - \sqrt{2}e^{-r}\hat{\tilde{x}}_2^{(0)}, \\ \hat{p}_{tel} &= \hat{p}_{in} + \sqrt{2}e^{-r}\hat{\tilde{p}}_1^{(0)}.\end{aligned}\quad (9.7)$$

For $r \rightarrow \infty$, $\hat{x}_{tel} \rightarrow \hat{x}_{in}$, $\hat{p}_{tel} \rightarrow \hat{p}_{in}$, in correspondence to perfect teleportation.

Of course in an actual experiment, the gain g must be determined operationally. For the particular case of Figure 9.5, the displacement of the input coherent state determined by Alice's homodyne detectors (22dB above the vacuum-state limit) corresponds to half of the input signal power. If Bob's output (as verified by Victor) carries twice the power specified by Alice's output (namely, 25dB in the case at hand), the gain g is then determined to be unity, namely 0dB. Precisely speaking, the g should be corrected by the detection efficiency ζ associated with Alice's homodyne detection (propagation, homodyne efficiency, and detector quantum efficiency). But since $\zeta \approx 0.97$ is almost unity in our experiment, the aforementioned procedure for fixing $g = 1$ (0dB) can be used with small error.

In somewhat more global terms, the actual procedure for determining $g = 1$ (0dB) is illustrated by Figure 9.6. This figure gives the variation of the coherent amplitude and of the variance with gain g^2 without EPR beams. Since these two dependences are different and both agree with theory without adjustable parameters, we can conclude that our setup functions in agreement with our simple model. When A_{out} equals to A_{in} (here, $A_{in} = A_{out} = 21dB$),

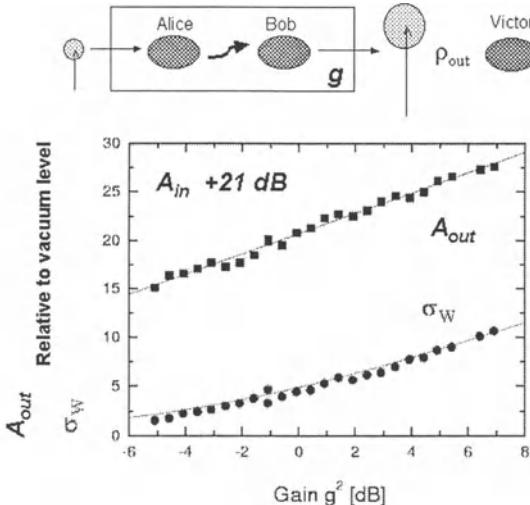


Figure 9.6 The variation of the coherent amplitude A_{out} and of the variance σ_W with gain g^2 without EPR beams. The input amplitude A_{in} is $+21\text{dB}$ above the vacuum-state limit in this particular case. The solid lines are the theoretical curves for $\zeta = 1$.

we can determine $g = 1$. From the Figure 9.6, we can see $\sigma_W = 4.8\text{dB}$ for $g = 1$, whose meaning will be presented later.

Moving then to the case of teleportation in the presence of entangled EPR beams, Bob combines his modulated beam with his EPR beam and reconstructs the state to be teleported. In this process, the “noise” arising from the EPR beam is effectively “subtracted” from Bob’s modulated beam by destructive interference at m_{Bob} .

Experimental results from this protocol are shown in Figure 9.7. The horizontal axis corresponds to the phase of Victor’s local oscillator, which is being swept in time. The vertical axis Ψ^{Victor} corresponds to the spectral density of photocurrent fluctuations associated with the quadrature amplitudes $\hat{x}_{tel}(\Omega)$ and $\hat{p}_{tel}(\Omega)$ measured by Victor for a fixed (but arbitrary) phase for the input state. The maximum value of the periodic curve corresponds to a coherent amplitude for the output state approximately 25dB above the vacuum-state level Φ_0^{Victor} ; here, the gain has been set to be $g \approx 1$ as in the previous discussion. This result shows the classical phase-space displacement is successfully reconstructed.

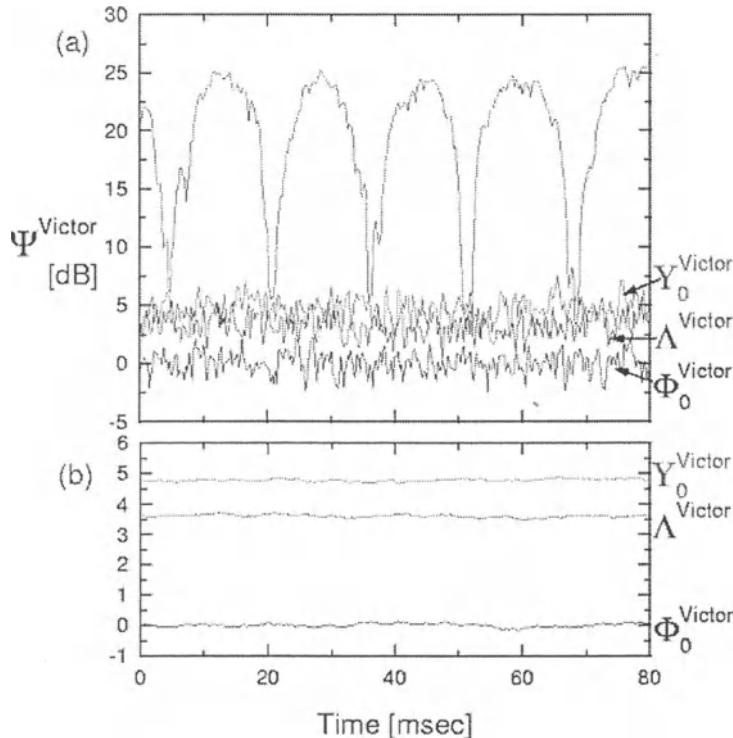


Figure 9.7 Bob's output verified by Victor. The part (b) is the expanded view with a ten-trace average for the vacuum input for Alice. [12]

The minima of the trace for Ψ^{Victor} correspond to the variance of the output state for the quadrature orthogonal to that of the coherent amplitude, and are equivalent to the level Λ^{Victor} shown by the labeled flat trace. The various phase-independent traces in the figure correspond to the quantum noise levels with the EPR beams present for Alice and Bob (Λ^{Victor}), without these EPR beams at both locations ($\Upsilon_0^{\text{Victor}}$), and with a vacuum-state input to Victor's

homodyne detector (Φ_0^{Victor}). Of course, “without the EPR beams” means that vacuum noise ($r = 0$) invades Alice and Bob’s stations, leading to a degradation of the “quality” of teleportation.

Indeed, for teleportation of coherent states in the absence of shared entanglement between Alice and Bob (no EPR beams), Equation (9.7) shows that the quantum noise for Bob’s output becomes three units of vacuum noise (in either quadrature, $\langle \Delta \hat{x}_{tel}^2 \rangle, \langle \Delta \hat{p}_{tel}^2 \rangle$). One unit comes from the original quantum noise of the input coherent state, and the other two units correspond to successive “quantum duties”, the first being to cross the boundary from the quantum to classical world (Alice’s attempt to detect both quadrature amplitudes) and the second from the classical to quantum (Bob’s generation of a coherent displacement) [11]. The experimental result $\Upsilon_0^{Victor} \approx 4.8dB$ in correspondence to a factor of 3 above the vacuum-state limit in Figures 9.6 and 9.7 indicates almost perfect performance of the “classical” teleportation with near unity detection efficiency (recall $\zeta = 0.97$). As discussed in more detail in Ref. [8, 9], Υ_0^{Victor} is the limit of “classical” teleportation, where explicitly we mean teleportation without shared entanglement.

From Figure 9.7 and similar measurements, we determine that Λ^{Victor} lies $1.1dB$ -lower than Υ_0^{Victor} . This means that quantum teleportation is successfully performed beyond the classical limit, as clarified by the following discussion. To quantify the “quality” of the teleportation for a pure state $|\psi_{in}\rangle$, we calculate the teleportation fidelity $F \equiv \langle \psi_{in} | \hat{\rho}_{out} | \psi_{in} \rangle$ [8, 9]. For the case of teleportation of coherent states, the boundary between classical and quantum teleportation has been shown to be fidelity $F = 0.50$ [8, 9]. We stress that this limit applies to the specific case of coherent states and only to the distinction between what Alice and Bob can accomplish with and without shared entanglement. Teleportation to accomplish other tasks in quantum information science requires yet higher values for the fidelity.

Nonetheless, when the input state is a coherent state, the fidelity F of the teleported output can be represented as follows [15]:

$$F = \frac{1}{2\sqrt{\sigma_Q^x \sigma_Q^p}} \exp \left[-(1-g)^2 \left(\frac{x_{in}^2}{2\sigma_Q^x} + \frac{p_{in}^2}{2\sigma_Q^p} \right) \right], \quad (9.8)$$

where σ_Q^x and σ_Q^p are the variances of the Q function of the teleported field for the corresponding quadratures. The relevant variances σ_Q^x and σ_Q^p can be determined from the measured efficiency factors in the experiment and are

given by the following equation [12]:

$$\begin{aligned}\sigma_Q^{x,p} = & \frac{1}{4}(1+g^2) + \frac{e^{2r_{x,p}}}{8}(g\xi_1 - \xi_2)^2 + \frac{e^{-2r_{x,p}}}{8}(g\xi_1 + \xi_2)^2 \\ & + \frac{1}{4}(1-\xi_1^2)g^2 + \frac{1}{4}(1-\xi_2^2) + \frac{g^2}{2}(\frac{1}{\eta^2} - 1),\end{aligned}\quad (9.9)$$

where $r_{x,p}$ are the squeezing parameters for the respective quadrature components, $\xi_{1,2}$ characterize the (amplitude) efficiency with which the EPR beams are propagated and detected along paths(1,2), and η gives the (amplitude) efficiency for detection of the unknown input state by Alice. We stress that all of these quantities can be directly measured, so that the comparison of theory as in the above equation and the experimentally recorded variances can be made with no adjustable parameters.

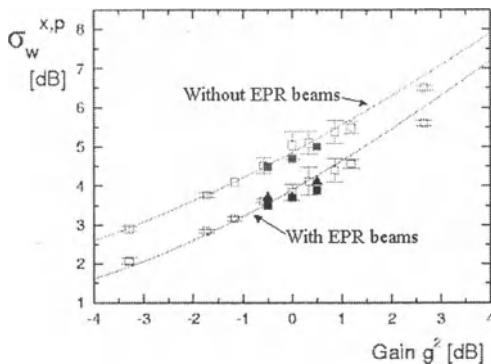


Figure 9.8 Variances $\sigma_W^{x,p}$ of the teleported field measured by Victor [12]. Open and filled symbols in the figure are experimental results. The open squares represent the results for the case with the slight imbalance of amount of squeezing in the two-mode squeezed vacuum. The filled squares and triangles represent the results for the case of the balanced amount of squeezing. The solid lines represent the theoretical predictions of Equation (9.9).

Following such a procedure, we show in Figure 9.8 the experimental results for the variances $\sigma_W^{x,p}$, as well as the theoretical prediction of Equation (9.9), again with no adjustable parameters. By using these measured values of σ_Q^x

and σ_Q^p together with the independently measured values for the gain g , we can use Equation (9.8) to arrive at an experimental estimate of the fidelity F_{exp} , with the results shown by the points in Figure 9.8 for the cases with and without the EPR beams present. We can also calculate F_{theory} by way of Equations (9.8, 9.9), with this theoretical prediction shown by the curves in Figure 9.9. The agreement between theory and experiment is evidently quite good.

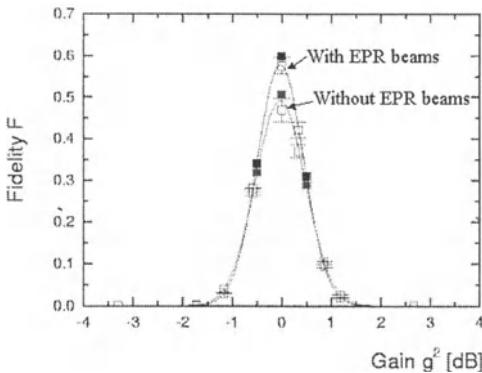


Figure 9.9 Fidelity F inferred from the measurement of Victor [12]. Open and filled squares in the figure are experimental estimates of the fidelity F_{exp} . The open squares represent the F_{exp} for the case with the slight imbalance of amount of squeezing in the two-mode squeezed vacuum. The filled squares represent the F_{exp} for the case of the balanced amount of squeezing. The solid lines represent the theoretical predictions F_{theory} .

From the Figure 9.9, we see that the fidelity F_{exp} for the case with EPR beams exceeds the classical limit $F_0 = 0.50$ for $g = 1$ (0dB), with the maximum value $F_{\text{exp}} = 0.58 \pm 0.02$ obtained. $F_{\text{exp}} > F_0$ is an unambiguous demonstration of the quantum character of the teleportation protocol.

3. SUMMARY

The fidelity $F_{\text{exp}} = 0.58 \pm 0.02$ has been obtained in an experiment with continuous variable quantum teleportation. This value exceeds the classical limit for the fidelity for the teleportation of coherent states of the electromagnetic field. As discussed in more detail in Ref. [8, 9], this is the first demonstration

of “bona fide” quantum teleportation for which every state entering Alice’s sending station is actually teleported to emerge from Bob’s receiving station with a fidelity exceeding that which would be possible if Alice and Bob shared only a classical communication channel.

Acknowledgments

The authors express their gratitude to S. L. Braunstein, J. L. Sorensen, C. A. Fuchs, E. S. Polzik, and S. J. van Enk. This work was supported by the NSF, by the ONR, and by DARPA via the QUIC Institute administered by the ARO. AF acknowledges T. Ide for preparing the figures.

References

- [1] Bennett, C. H., et al.,(1993) Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen Channels, *Phys. Rev. Lett.* **70**, 1895.
- [2] Arthurs, E. and Kelly Jr., J. L., (1965) On the simultaneous measurement of a pair of conjugate variables, *Bell. Syst. Tech. J.* **44**, 725.
- [3] Einstein, A., Podolsky, B., and Rosen, N.,(1935) Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.* **47**, 777.
- [4] Boschi, D., et al.,(1998) Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* **80**, 1121.
- [5] Bouwmeester, D., et al.,(1997) Experimental quantum teleportation, *Nature* **390**, 575.
- [6] Braunstein, S. L., and Kimble, H. J., (1998) A posteriori teleportation, *Nature* **394**, 840.
- [7] Kok, P., and Braunstein, S. L., (2000) Postselected versus nonpostselected quantum teleportation using parametric down-conversion, *Phys. Rev. A* **61**, 042304.
- [8] Braunstein, S. L., Fuchs, C. A., and Kimble, H. J., (2000) Criteria for continuous-variable quantum teleportation, *J. Mod. Opt.* **47**, 267.
- [9] Braunstein, S. L., Fuchs, C. A., Kimble, H. J., and van Loock, P., (2001) Quantum versus classical domains for teleportation with continuous variables, *Phys. Rev. A* **64**, 022321.
- [10] Vaidman, L., (1994) Teleportation of quantum states, *Phys. Rev. A* **49**, 1473.
- [11] Braunstein, S. L., and Kimble, H. J., (1998) Teleportation of continuous quantum variables, *Phys. Rev. Lett.* **80**, 869.

- [12] Furusawa, A., Sorensen, J. L., Braunstein, S. L., Fuchs, C. A., Kimble, H. J., and Polzik, E. S., (1998) Unconditional quantum teleportation, *Science* **282**, 706.
- [13] Reid, M. D. and Drummond P. D., (1988) Quantum correlations of phase in nondegenerate parametric oscillator, *Phys. Rev. Lett.* **60**, 2731; Reid M. D., (1989) Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification, *Phys. Rev. A* **40**, 913.
- [14] Ou, Z. Y., Pereira, S. F., Kimble, H. J., and Peng, K. C., (1992) Realization of the Einstein-Podolsky-Rosen paradox for continuous variables, *Phys. Rev. Lett.* **68**, 3663.
- [15] van Loock, P., Braunstein, S. L., and Kimble, H. J., (2000) Broadband teleportation, *Phys. Rev. A* **62**, 022309.
- [16] Furusawa, A., (1999) Quantum teleportation, *bit* **31**, no.10, 2, in Japanese.
- [17] Duan, L.-M., Giedke, G., Cirac, J. I., and Zoller, P., (2000) Inseparability criterion for continuous variable systems, *Phys. Rev. Lett.* **84**, 2722.
- [18] Simon, R., (2000) Peres-Horodecki separability criterion for continuous variable systems, *Phys. Rev. Lett.* **84**, 2726.

Chapter 10

DENSE CODING FOR CONTINUOUS VARIABLES*

Samuel L. Braunstein

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

H. J. Kimble

Norman Bridge Laboratory of Physics 12-33

California Institute of Technology, Pasadena, CA 91125

Abstract A scheme to achieve dense quantum coding for the quadrature amplitudes of the electromagnetic field is presented. The protocol utilizes shared entanglement provided by nondegenerate parametric down-conversion in the limit of large gain to attain high efficiency. For a constraint in the mean number of photons \bar{n} associated with modulation in the signal channel, the channel capacity for dense coding is found to be $\ln(1 + \bar{n} + \bar{n}^2)$, which always beats coherent-state communication and surpasses squeezed-state communication for $\bar{n} > 1$. For $\bar{n} \gg 1$, the dense coding capacity approaches twice that of either scheme.

An important component of contemporary quantum information theory is the investigation of the classical information capacities of noisy quantum communication channels. Here, classical information is encoded by the choice of one particular quantum state from among a predefined ensemble of quantum states by the sender Alice for transmission over a quantum channel to the receiver Bob. If Alice and Bob are allowed to communicate only via a one-way exchange along such a noisy quantum channel, then the optimal amount of classical information that can be reliably transmitted over the channel has recently been established [1, 2].

*S. L. Braunstein and H. J. Kimble, Physical Review A **61**, 042302/1-4 (2002).
Copyright (2000) by the American Physical Society.

Stated more explicitly, if a classical signal α taken from the ensemble P_α is to be transmitted as a quantum state $\hat{\rho}_\alpha$, then Holevo's bound for a bosonic quantum channel says that the mutual information $H(A:B)$ between the sender A (Alice) and receiver B (Bob) is bounded by [1]

$$H(A:B) \leq S(\hat{\rho}) - \int d^2\alpha P_\alpha S(\hat{\rho}_\alpha) \leq S(\hat{\rho}), \quad (10.1)$$

where $S(\hat{\rho})$ is the von Neumann entropy associated with the density operator $\hat{\rho} = \int d^2\alpha P_\alpha \hat{\rho}_\alpha$ for the mean channel state.

By contrast, if Alice and Bob share a quantum resource in the form of an ensemble of entangled states, then quantum mechanics enables protocols for communication that can circumvent the aforementioned bound on channel capacity. For example, as shown originally by Bennett and Wiesner [3], Alice and Bob can beat the Holevo limit by exploiting their shared entanglement to achieve dense quantum coding. Here, the signal is encoded at Alice's sending station and transmitted via one component of a pair of entangled quantum states, with then the second component of the entangled pair exploited for decoding the signal at Bob's receiving station. In this scheme, the cost of distributing the entangled states to Alice and Bob is not figured into the accounting of constraints on the quantum channel (e.g., the mean energy). Such neglect of the distribution cost of entanglement is sensible in some situations, as for example, if the entanglement were to be sent during off-peak times when the communication channel is otherwise under utilized, or if it had been conveyed by other means to Alice and Bob in advance (e.g., via a pair of *quantum CDs* with stored, entangled quantum states). Note that in general, no signal modulation is applied to the second (i.e., Bob's) component of the entangled state, so that it carries no information by itself.

Although quantum dense coding has most often been discussed within the setting of *discrete* quantum variables (e.g., *qubits*) [3, 4], in this paper we show that highly efficient dense coding is possible for *continuous* quantum variables. As in our prior work on quantum teleportation [5, 6, 7], our scheme for achieving quantum dense coding exploits squeezed-state entanglement, and therefore should allow *unconditional* signal transmission with high efficiency, in contrast to the *conditional* transmission with extremely low efficiency achieved in Ref. [4]. More specifically, for signal states α associated with the complex amplitude of the electromagnetic field, the channel capacity for dense coding is found to be $\ln(1 + \bar{n} + \bar{n}^2)$, where \bar{n} is the mean photon number for modulation in the signal channel. The channel capacity for dense coding in our scheme thus always beats coherent-state communication and surpasses squeezed-state communication for $\bar{n} > 1$. For $\bar{n} \gg 1$, the dense coding capacity approaches twice that of either scheme.

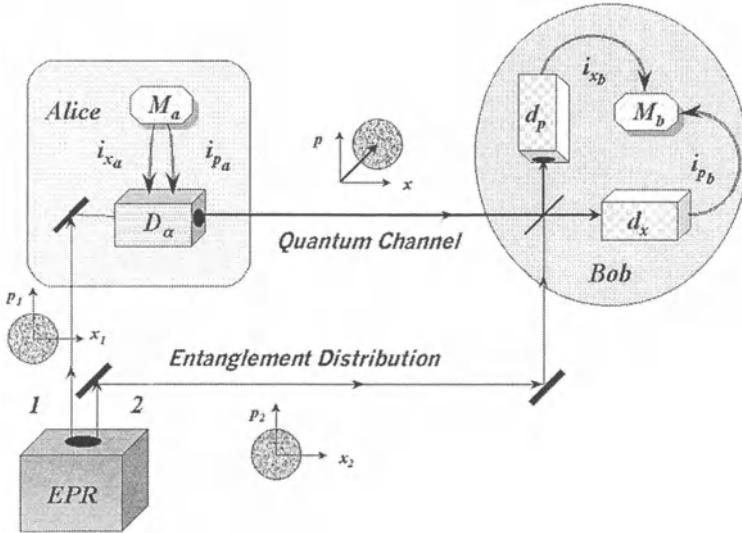


Figure 10.1 Illustration of the scheme for achieving super-dense quantum coding for signal states over the complex amplitude $\alpha = x + ip$ of the electromagnetic field. The quantum resource that enables dense coding is the EPR source that generates entangled beams (1, 2) shared by Alice and Bob.

As illustrated in Fig. 10.1, the relevant continuous variables for our protocol are the quadrature amplitudes (\hat{x}, \hat{p}) of the electromagnetic field, with the classical signal $\alpha = \langle \hat{x} \rangle + i\langle \hat{p} \rangle$ then associated with the quantum state $\hat{\rho}_\alpha$ drawn from the phase space for a single mode of the field. The entangled resource shared by Alice and Bob is a pair of EPR beams with quantum correlations between canonically conjugate variables $(\hat{x}, \hat{p})_{(1,2)}$ as were first described by Einstein, Podolsky, and Rosen (EPR [8]), and which can be efficiently generated via the nonlinear optical process of parametric down conversion, resulting in a highly squeezed two-mode state of the electromagnetic field [9, 10]. In the ideal case, the correlations between quadrature-phase amplitudes for the two beams (1, 2) are such that

$$\langle (\hat{x}_1 - \hat{x}_2)^2 \rangle \rightarrow 0, \quad \langle (\hat{p}_1 + \hat{p}_2)^2 \rangle \rightarrow 0, \quad (10.2)$$

albeit it with an concomitant divergence in the mean photon number \bar{n} in each channel.

Component 1 of this entangled pair of beams is input to Alice's sending station, where the message M_a^α corresponding to the classical signal α_{in} is encoded as the quantum state $\hat{\rho}_{\alpha_{in}}$ by a simple phase-space offset by way of the displacement operator $\hat{D}(\alpha_{in})$ applied to 1 [11]. The displacement $\hat{D}(\alpha_{in})$ can

be implemented in a straightforward fashion by amplitude and phase offsets generated by the (suitably normalized) classical currents (i_{x_a}, i_{p_a}) as in Ref. [7]. The state corresponding to Alice's displacement of the EPR beam constitutes the quantum signal and is transmitted along the quantum channel shown in Fig. 10.1 to Bob's receiving station, (Fig. 10.2) where it is decoded with the aid of the second component 2 of the original EPR pair of beams and the homodyne detectors (d_x, d_p). The resulting photocurrents (i_{x_b}, i_{p_b}) suitably normalized to produce $\alpha_{\text{out}} = i_{x_b} + i i_{p_b}$ constitute the message M_b^α received by Bob. In the limit $\bar{n} \rightarrow \infty$, Eq. (10.2) ensures $\alpha_{\text{out}} = \alpha_{\text{in}}$, so that the classical message would be perfectly recovered. However, even for finite \bar{n} as is relevant to a channel constrained in mean energy, the finite correlations implicit in the EPR beams enable quantum dense coding with enhanced channel capacity relative to either coherent state or squeezed state communication, as we now show.

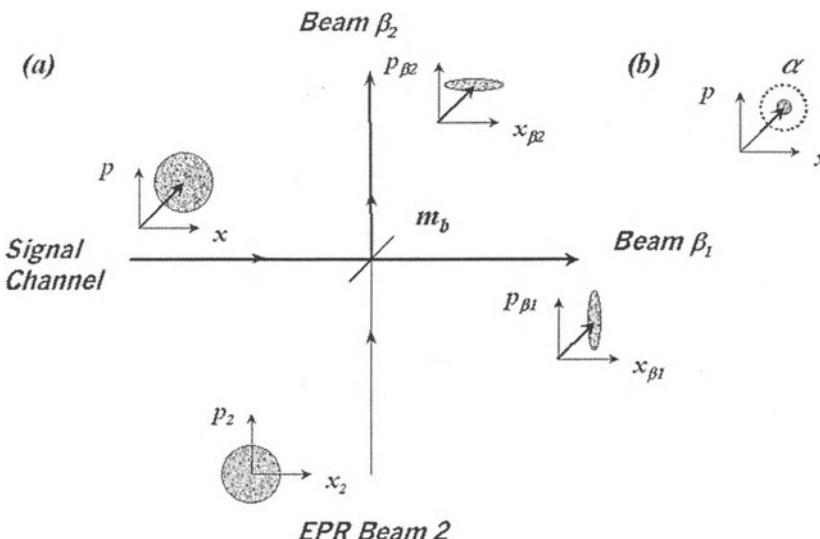


Figure 10.2 Depiction of signal decoding at Bob's receiving station. (a) At Bob's 50 – 50 beam splitter m_b , the displaced EPR beam 1 is combined with the component 2 to yield two independent squeezed beams, with the $\beta_{1,2}$ beams having fluctuations reduced below the vacuum-state limit along $(x_{\beta_1}, p_{\beta_2})$. Homodyne detection at (d_x, d_p) (Fig. 10.1) with LO phases set to measure $(x_{\beta_1}, p_{\beta_2})$, respectively, then yields the complex signal amplitude α_{out} with variance set by the associated squeezed states. (b) The net effect of the dense coding protocol is the transmission and detection of states of complex amplitude α with an effective uncertainty below the vacuum-state limit (indicated by the dashed circle).

Consider the specific case of EPR beams (1, 2) approximated by the two-mode squeezed state with Wigner function

$$\begin{aligned} W_{\text{EPR}}(\alpha_1, \alpha_2) = & \frac{4}{\pi^2} \exp[-e^{-2r}(\alpha_1 - \alpha_2)_R^2 - e^{2r}(\alpha_1 - \alpha_2)_I^2] \\ & - e^{2r}(\alpha_1 + \alpha_2)_R^2 - e^{-2r}(\alpha_1 + \alpha_2)_I^2], \end{aligned} \quad (10.3)$$

where the subscripts R and I refer to real and imaginary parts of the field amplitude α , respectively (i.e., $\alpha_{R,I} = x, p$). Note that for $r \rightarrow \infty$, the field state becomes the ideal EPR state as described in Eq. (10.2), namely,

$$W_{\text{EPR}}(\alpha_1, \alpha_2) \rightarrow C \delta(\alpha_{1R} + \alpha_{2R}) \delta(\alpha_{1I} - \alpha_{2I}). \quad (10.4)$$

As shown in Fig. 10.1, signal modulation is performed only on mode 1, with mode 2 treated as an overall shared resource by Alice and Bob (and which could have been generated by Alice herself). The modulation scheme that we choose is simply to displace mode 1 by an amount α_{in} . This leads to a displaced Wigner function given by $W_{\text{EPR}}(\alpha_1 - \alpha_{\text{in}}, \alpha_2)$, corresponding to the field state that is sent via the quantum channel from Alice to Bob.

Upon receiving this transmitted state (consisting of the modulated mode 1), the final step in the dense-coding protocol is for Bob to combine it with the shared resource (mode 2) and retrieve the original classical signal α_{in} with as high a fidelity as possible. As indicated in Fig. 10.1, this demodulation can be performed with a simple 50 – 50 beam splitter that superposes the modes (1, 2) to yield output fields that are the sum and difference of the input fields and which we label as β_1 and β_2 , respectively. The resulting state emerging from Bob's beam splitter has Wigner function

$$W_{\text{sum/diff}}(\beta_1, \beta_2) = W_{\text{EPR}}((\beta_1 + \beta_2)/\sqrt{2} - \alpha, (\beta_1 - \beta_2)/\sqrt{2}). \quad (10.5)$$

The classical signal that we seek is retrieved by homodyne detection at detectors (d_x, d_p) , which measure the analogs of position and momentum for the sum and difference fields (β_1, β_2) . For ideal homodyne detection the resulting outcomes are distributed according to

$$P(\beta|\alpha) = \frac{2e^{2r}}{\pi} \exp(-2e^{2r}|\beta - \alpha/\sqrt{2}|^2),$$

where $\beta = \beta_{1R} + i\beta_{2I}$ and represents a highly peaked distribution about the complex displacement $\alpha/\sqrt{2}$. For large squeezing parameter r this allows us to extract the original signal α which we choose to be distributed as

$$P_\alpha = \frac{1}{\pi\sigma^2} \exp(-|\alpha|^2/\sigma^2). \quad (10.6)$$

Note that mode 1 of this displaced state has a mean number of photons given by

$$\bar{n} = \sigma^2 + \sinh^2 r . \quad (10.7)$$

In order to compute the quantity of information that may be sent through this dense coding channel we note the unconditioned probability for the homodyne statistics is given by

$$P(\beta) = \frac{2}{\pi(\sigma^2 + e^{-2r})} \exp\left(\frac{-2|\beta|^2}{\sigma^2 + e^{-2r}}\right) . \quad (10.8)$$

The mutual information describing the achievable information throughput of this dense coding channel is then given by

$$\begin{aligned} H^{\text{dense}}(A : B) &= \int d^2\beta d^2\alpha P(\beta|\alpha)P_\alpha \ln\left(\frac{P(\beta|\alpha)}{P(\beta)}\right) \\ &= \ln(1 + \sigma^2 e^{2r}) . \end{aligned} \quad (10.9)$$

For a fixed \bar{n} in Eq. (10.7) this information is optimized when $\bar{n} = e^r \sinh r$, i.e., when $\sigma^2 = \sinh r \cosh r$ so yielding a dense coding capacity of

$$C^{\text{dense}} = \ln(1 + \bar{n} + \bar{n}^2) , \quad (10.10)$$

which for large squeezing r becomes

$$C^{\text{dense}} \sim 4r . \quad (10.11)$$

How efficient is this dense coding in comparison to single channel coding? Let us place a “common” constraint of having a fixed mean number of photons \bar{n} which can be modulated. For a single bosonic channel Drummond and Caves [12] and Yuen and Ozawa [13] have used Holevo’s result to show that the optimal channel capacity is just that given by photon counting from a maximum entropy ensemble of number states. In this case the channel capacity (the maximal mutual information) achieves the ensemble entropy, see Eq. (10.1), so

$$C = S(\rho) = (1 + \bar{n}) \ln(1 + \bar{n}) - \bar{n} \ln \bar{n} . \quad (10.12)$$

Substituting $\bar{n} = e^r \sinh r$ into this we find

$$C \sim 2r , \quad (10.13)$$

for large squeezing r . This is just one-half of the asymptotic dense coding mutual information, see Eq. (10.11). Thus asymptotically, at least, the dense coding scheme allows twice as much information to be encoded within a given

state, although it has an extra expense (not included within the simple constraint \bar{n}) of requiring shared entanglement.

It is worth noting that this dense coding scheme does *not* always beat the optimal single channel capacity. Indeed, for small squeezing it is worse. The break-even squeezing required for dense coding to equal the capacity of the optimal single channel communication is

$$r_{\text{break-even}} \simeq 0.7809 , \quad (10.14)$$

which corresponds to roughly 6.78 dB of two-mode squeezing or to $\bar{n} \simeq 1.884$. This break-even point takes into account the difficulty of making highly squeezed two-mode inxsqueezed states. No similar difficulty has been factored into making ideal number states used in the benchmark scheme with which our dense coding scheme is compared.

A fairer comparison is against single-mode coherent state communication with heterodyne detection. Here the channel capacity is well known [14, 15, 16] for the mean photon number constraint to be

$$C^{\text{coh}} = \ln(1 + \bar{n}) , \quad (10.15)$$

which is *always* beaten by the optimal dense coding scheme described by Eq. (10.10).

An improvement on coherent state communication is squeezed state communication with a single mode. The channel capacity of this channel has been calculated [16] to be

$$C^{\text{sq}} = \ln(1 + 2\bar{n}) , \quad (10.16)$$

which is beaten by the dense coding scheme of Eq. (10.10) for $\bar{n} > 1$, i.e., the break-even squeezing required is

$$r_{\text{break-even}}^{\text{sq}} \simeq 0.5493 , \quad (10.17)$$

which corresponds to 4.77 dB .

In summary, we have shown how to perform dense quantum coding for continuous quantum variables by utilizing squeezed state entanglement. For a constraint in the mean number of photons that may be modulated \bar{n} , the dense coding capacity is found to be $\ln(1 + \bar{n} + \bar{n}^2)$. This scheme always beats single-mode coherent-state communication and surpasses single-mode squeezed-state communication for $\bar{n} > 1$. Note that in terms of actual implementation, our protocol should allow for high efficiency, *unconditional* transmission with encoded information sent every inverse bandwidth time. This situation is in contrast to implementations that employ weak parametric down conversion, where transmission is achieved *conditionally* and relatively rarely. In fact Mattole *et al.* [4] obtained rates of only $1 \text{ in } 10^7$ per inverse bandwidth time [17].

By going to strong down conversion and using a characteristically different type of entanglement, our scheme should allow information to be sent with much higher efficiency and should simultaneously improve the ability to detect orthogonal Bell states. Indeed, these advantages enabled the first experimental realization of unconditional quantum teleportation within the past year [7]. Beyond the particular setting of quantum communication discussed here, this research is part of a larger program to explore the potential for quantum information processing with continuous quantum variables. Such investigations are quite timely in light of important recent progress concerning the prospects for diverse quantum algorithms with continuous variables, including universal quantum computation [18] and quantum error correction [19, 20, 21], with quantum teleportation being a prime example [5, 22, 23]. Although still in its earliest stages, theoretical protocols have been developed for realistic physical systems that should allow a variety of elementary processing operations for continuous quantum variables, including significantly quantum storage for EPR states [24, 25].

S.L.B. was supported in part by the UK Engineering and Physical Sciences Research Council and the Royal Academy of Engineering. The work of H.J.K. is supported by DARPA via the QUIC Institute which is administered by ARO, by the Office of Naval Research, and by the National Science Foundation.

References

- [1] A. S. Holevo, IEEE Trans. Info. Theory **44**, 269 (1998).
- [2] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
- [3] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
- [4] K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
- [5] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
- [6] P. van Loock, S. L. Braunstein, and H. J. Kimble, “Broadband teleportation,” LANL preprint, quant-ph/9902030.
- [7] A. Furusawa, J. Sørensen, S. L. Braunstein, C. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).
- [8] A. Einstein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777 (1935).
- [9] M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988); M. D. Reid, Phys. Rev. A **40**, 913 (1989).
- [10] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992); Appl. Phys. B: Photophys. Laser Chem. **55**, 265 (1992).
- [11] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, (Cambridge University Press, Cambridge, England, 1995).

- [12] C. M. Caves and P. D. Drummond, Rev. Mod. Phys. **66**, 481 (1994).
- [13] H. P. Yuen and M. Ozawa, Phys. Rev. Lett. **70**, 363 (1993).
- [14] J. P. Gordon, Proc. IRE **50**, 1898 (1962).
- [15] C. Y. She, IEEE Trans. Inf. Theory **IT-14**, 32 (1968).
- [16] Y. Yamamoto and H. A. Haus, Rev. Mod. Phys. **58**, 1001 (1986).
- [17] H. Weinfurter (private communication).
- [18] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
- [19] S. Lloyd and J. J.-E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).
- [20] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
- [21] S. L. Braunstein, Nature (London) **394**, 47 (1998).
- [22] C. H. Bennett et al., Phys. Rev. Lett. **70**, 1895 (1993).
- [23] L. Vaidman, Phys. Rev. A**49**, 1473 (1994).
- [24] A. S. Parkins and H. J. Kimble, e-print quant-ph/9904062.
- [25] A. S. Parkins and H. J. Kimble, e-print quant-ph/9907049.

Chapter 11

MULTIPARTITE GREENBERGER-HORNE-ZEILINGER PARADOXES FOR CONTINUOUS VARIABLES

Serge Massar and Stefano Pironio

Service de Physique Théorique, CP 225,

Université Libre de Bruxelles

1050 Brussels, Belgium

Abstract We show how to construct Greenberger-Horne-Zeilinger type paradoxes for continuous variable systems. We give two examples corresponding to 3-party and 5-party paradoxes. The paradoxes are revealed by carrying out position and momentum measurements. The structure of the quantum states which lead to these paradoxes is discussed.

When studying continuous variables systems, described by conjugate variables with commutation relation $[x, p] = i$, it is natural to inquire how non-locality can be revealed in those systems. Experimentally the operations that are easy to carry out on such systems involve linear optics, squeezing and homodyne detection. Using these operations, the states that can be prepared are Gaussian states and the measurements that can be performed are measurements of quadratures. But Gaussian states possess a Wigner function which is positive everywhere and so provide a trivial local-hidden variable model for measurement of x or p .

To exhibit non-locality in these systems, it is thus necessary to drop some of the requirements imposed by current day experimental techniques. For instance one can invoke more challenging measurements such as photon counting measurements or consider more general states that will necessitate higher order non-linear couplings to be produced. Using these two approaches it has recently been possible to extend from discrete variables to continuous variables systems the usual non-locality tests: Bell inequalities [1, 2, 3], Hardy's non-locality proof [4] and the Greenberger-Horne-Zeilinger paradox [5, 6, 7].

Greenberger-Horne-Zeilinger (GHZ) paradoxes [8] as formulated by Mermin [9] are particularly elegant and simple ways of demonstrating the non-locality of quantum systems since the argument can be carried out at the level of operators only. The existence of a generalization of the original GHZ paradox for qubits to continuous variables was first pointed out by Clifton [5] and was studied in more details in [6] and [7]. The paradox presented in [7] involve measurements of the parity of the number of photons, while in [5] and [6], it is associated with position and momentum variables. It is this last case that we will consider here. We shall summarize the results of [6] and show that the multipartite multidimensional GHZ paradoxes introduced in [10] can easily be generalized to the case of continuous variables by exploiting the non-commutative geometry of the phase space. This idea is closely related to the technique used to embed finite-dimensional quantum error correcting code in the infinite-dimensional Hilbert space of continuous variables systems [11].

Let us introduce the dimensionless variables

$$\tilde{x} = \frac{x}{\sqrt{\pi}L} \quad \text{and} \quad \tilde{p} = \frac{p}{\sqrt{\pi}} L, \quad (11.1)$$

where L is an arbitrary length scale. Consider the translation operators in phase space

$$X^\alpha = \exp(i\alpha\tilde{x}) \quad \text{and} \quad Y^\beta = \exp(i\beta\tilde{p}). \quad (11.2)$$

These unitary operators obey the commutation relation

$$X^\alpha Y^\beta = e^{i\alpha\beta/\pi} Y^\beta X^\alpha, \quad (11.3)$$

which follows from $[\tilde{x}, \tilde{p}] = i/\pi$ and the identity $e^A e^B = e^{[A,B]} e^B e^A$ (valid if A and B commute with their commutator). The continuous variable GHZ paradoxes will be built out of these operators.

Let us first consider the case of three spatially separated parties, A, B, C, each of which possess one part of an entangled system described by the canonical variables x_A, p_A, x_B, p_B, x_C and p_C . Consider the operators $X_j^{\pm\pi}$ and $Y_j^{\pm\pi}$ acting on the space of party j ($j = A, B, C$). Since $\alpha\beta = \pm\pi^2$, it follows from (11.3), that these operators obey the commutations relations $X_j^{\pm\pi} Y_j^{\pm\pi} = -Y_j^{\pm\pi} X_j^{\pm\pi}$. Using these operators let us construct the following four GHZ operators:

$$\begin{aligned} V_1 &= X_A^\pi & X_B^\pi & X_C^\pi \\ V_2 &= X_A^{-\pi} & Y_B^{-\pi} & Y_C^\pi \\ V_3 &= Y_A^\pi & X_B^{-\pi} & Y_C^{-\pi} \\ V_4 &= Y_A^{-\pi} & Y_B^\pi & X_C^{-\pi} \end{aligned} \quad (11.4)$$

These four operators give rise to a GHZ paradox as we now show. First note that the following two properties hold:

1. V_1, V_2, V_3, V_4 all commute. Thus they can be simultaneously diagonalized (in fact there exists a complete set of common eigenvectors).
2. The product $V_1 V_2 V_3 V_4 = -I_{ABC}$ equals minus the identity operator.

These properties are easily proven using the commutations relations $X_j^{\pm\pi} Y_j^{\pm\pi} = -Y_j^{\pm\pi} X_j^{\pm\pi}$. Any common eigenstate of V_1, V_2, V_3, V_4 will give rise to a GHZ paradox. Indeed suppose that the parties measure the hermitian operators x_j or p_j , $j = A, B, C$ on this common eigenstate. The result of the measurement associates a complex number of unit norm to either the X_j or Y_j unitary operators. If one of the combinations of operators that occurs in eq. (11.4) is measured, a value can be assigned to one of the operators V_1, V_2, V_3, V_4 . Quantum mechanics imposes that this value is equal to the corresponding eigenvalue. Moreover - due to property 2 - the product of the eigenvalues is -1.

But this is in contradiction with local hidden variables theories. Indeed in a local hidden theory one must assign, prior to the measurement, a complex number of unit norm to all the operators X_j and Y_j . Then taking the product of the four c-numbers assigned simultaneously to V_1, V_2, V_3, V_4 yields +1 instead of -1.

Remark that all other tests of non-locality for continuous variable systems [1, 2, 3, 4, 7] use measurements with a discrete spectrum (such as the parity photon number) or involving only a discrete set of outcome (such as the probability that $x > 0$ or $x < 0$). In our version of the GHZ paradox for continuous variables this discrete character doesn't seem to appear at first sight. However it turns out that it is also the case thought in a subtle way because eq. (11.4) can be viewed as an infinite set of 2 dimensional paradoxes (see [6] for more details).

In [10], GHZ paradoxes for many parties and multidimensional systems were constructed. These paradoxes were built using d -dimensional unitary operators with commutation relations:

$$XY = e^{2\pi i/d} YX \quad (11.5)$$

which is a generalization of the anticommutation relation of spin operators for two-dimensional systems. Using X^α and Y^β and choosing the coefficients α and β such that $\alpha\beta = 2\pi^2/d$ with d and integer, this commutation relation can be realized in a continuous variable systems and so all the paradoxes presented in [10] can be rephrased with minor modifications in the context of infinite-dimensional Hilbert space.

Let us for instance generalise to continuous variables the paradox for 5 parties each having a 4 dimensional systems described in [10]. We now consider

the operators $X^{\pm q}$, Y^q and Y^{-3q} where $q = \pi/\sqrt{2}$. They obey the commutation relation $X^{\pm q}Y^q = e^{\pm i\pi/2}Y^qX^{\pm q}$ and $X^{\pm q}Y^{-3q} = e^{\pm i\pi/2}Y^{-3q}X^{\pm q}$. Consider now the six unitary operators

$$\begin{aligned} W_1 &= X_A^q & X_B^q & X_C^q & X_D^q & X_E^q \\ W_2 &= X_A^{-q} & Y_B^{-3q} & Y_C^q & Y_D^q & Y_E^q \\ W_3 &= Y_A^q & X_B^{-q} & Y_C^{-3q} & Y_D^q & Y_E^q \\ W_4 &= Y_A^q & Y_B^q & X_C^{-q} & Y_D^{-3q} & Y_E^q \\ W_5 &= Y_A^q & Y_B^q & Y_C^q & X_D^{-q} & Y_E^{-3q} \\ W_6 &= Y_A^{-3q} & Y_B^q & Y_C^q & Y_D^q & X_E^{-q} \end{aligned} \quad (11.6)$$

One easily shows that these six unitary operators commute and that their product is minus the identity operator. Furthermore if one assigns a classical value to x_j and to p_j for $j = A, B, C, D, E$, then the product of the operators takes the value +1. Hence, using the same argument as in the three party case, we have a contradiction.

There is a slight difference between the paradox (11.6) and the 4-dimensional paradox described in [10]. The origin of this difference is that in a d -dimensional Hilbert space, if unitary operators X, Y obey $XY = e^{i\pi/d}YX$, then $X^d = Y^d = I$ (up to a phase which can be set to 1), or equivalently, $X^{d-1} = X^\dagger$ and $Y^{d-1} = Y^\dagger$. In the continuous case these relations no longer hold and the GHZ operators W_i 's must be slightly modified, i.e. the operator $X^{-q} = X^{q\dagger}$ and $Y^{-3q} = Y^{3q\dagger}$ have to be explicitly introduced in order for the product of the W_i 's to give minus the identity. Note that the same remark applies for the previous paradox (11.4) where in the discrete 2-dimensional version $X^\dagger = X$ and $Y^\dagger = Y$.

As we mentioned earlier the GHZ states are not Gaussian states. A detailed analysis of the common eigenstates of V_1, V_2, V_3, V_4 is given in [6]. Let us give an example of such an eigenstate. Define the following coherent superpositions of infinitely squeezed states:

$$\begin{aligned} |\uparrow\rangle &= \frac{1}{\sqrt{2}} \sum_{k=-\infty}^{\infty} (|\tilde{x} = 2k\rangle + i|\tilde{x} = 2k+1\rangle) \\ |\downarrow\rangle &= \frac{1}{\sqrt{2}} \sum_{k=-\infty}^{\infty} (|\tilde{x} = 2k\rangle - i|\tilde{x} = 2k+1\rangle) , \end{aligned} \quad (11.7)$$

where $|\tilde{x}\rangle = |x = \sqrt{\pi}L\tilde{x}\rangle$. Then a common eigenstate of the four GHZ operators V_1, V_2, V_3, V_4 is

$$(|\uparrow\rangle_A|\uparrow\rangle_B|\uparrow\rangle_C - |\downarrow\rangle_A|\downarrow\rangle_B|\downarrow\rangle_C)/\sqrt{2}.$$

However as shown in [6], for any choice of the eigenvalues of the operators V_k , there is an infinite family of eigenvectors, ie. the eigenspace is infinitely degenerate.

In summary we have shown the existence of multipartite GHZ paradoxes for continuous variable systems. These paradoxes involve measurements of position and momentum variables only, but the states which are measured are complex and difficult to construct experimentally.

Acknowledgments

We would like to thank N. Cerf for helpful discussions. We acknowledges funding by the European Union under project EQUIP (IST-FET program). S.M. is a research associate of the Belgian National Research Foundation.

References

- [1] K. Banaszek and K. Wódkiewicz, Phys. Rev. A **58**, 4345 (1998).
- [2] A. Kuzmich, I. A. Walmsley and L. Mandel, Phys. Rev. Lett. **85**, 1349 (2000).
- [3] Z. Chen, J. Pan, G. Hou and Y. Zhang, Phys. Rev. Lett. **88** 040406 (2002).
- [4] B. Yurke, M. Hillery and D. Stoler, Phys. Rev. A **60**, 3444 (1999).
- [5] R. Clifton, Phys. Lett. A **271**, 1 (2000).
- [6] S. Massar and S. Pironio, Phys. Rev. A **64** 062108 (2001).
- [7] Z. Chen and Y. Zhang, Phys. Rev. A **65** 044102 (2001).
- [8] D. M. Greenberger, M. Horne, A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos, ed., Kluwer, Dordrecht, The Netherlands (1989), p. 69.
- [9] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990) and Phys. Today, 43(6), 9 (1990).
- [10] N. Cerf, S. Massar, S. Pironio, *Greenberger-Horne-Zeilinger paradoxes for many qudits*, quant-ph/0107031, to be published in Phys. Rev. Lett.
- [11] D. Gottesman, A. Kitaev and J. Preskill, Phys. Rev. A **64** 012310 (2001).

Chapter 12

MULTIPARTITE ENTANGLEMENT FOR CONTINUOUS VARIABLES

Peter van Loock

Zentrum für Moderne Optik, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany

vanloock@kerr.physik.uni-erlangen.de

Samuel L. Braunstein

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

Abstract First, we show how the quantum circuits for generating and measuring multi-party entanglement of qubits can be translated to continuous quantum variables. We derive sufficient inseparability criteria for N -party continuous-variable states and discuss their applicability. Then, we consider a family of multipartite entangled states (multi-party multi-mode states with one mode per party) described by continuous quantum variables and analyze their properties. These states can be efficiently generated using squeezed light and linear optics.

Keywords: Multipartite entanglement, squeezed light

1. INTRODUCTION

What is the main motivation to deal with continuous variables for quantum communication purposes? Quantum communication schemes rely on state preparation, local unitary transformations, measurements, and classical communication. In addition, sometimes shared entanglement is part of the protocol. Within the framework of quantum optics, these ingredients can be efficiently implemented when they are applied to the continuous quadrature amplitudes of electromagnetic modes. For example, the tools for measuring a quadrature with near-unit efficiency or for displacing an optical mode in phase space are provided by homodyne detection and feed-forward techniques, respectively. Continuous-variable entanglement can be efficiently produced using squeezed

light and linear optics. In this chapter, we consider a rather general manifestation of continuous-variable entanglement, namely that between an arbitrary number of parties (modes). We will see that even those N -party entangled states where none of the N parties can be separated from the others in the total state vector are comparatively “cheap” in terms of the resources needed: their generation only requires one single-mode squeezed state and $N - 1$ beam splitters.

2. MULTIPARTITE ENTANGLEMENT

The main subject of this section is multi-party entanglement of infinite-dimensional states described by continuous variables. After a few general remarks on entanglement between two and more parties in arbitrary dimensions, we will show how the quantum circuits for creating and measuring qubit entanglement may be translated to continuous variables. Then we derive inequalities that may serve as sufficient multi-party inseparability criteria for continuous-variable states. These are applicable both for a theoretical test and for an indirect experimental verification of multi-party entanglement. Finally, we focus on a family of genuinely multi-party entangled continuous-variable states whose members are fully inseparable with respect to all their parties.

2.1 TWO PARTIES VERSUS MANY PARTIES

Bipartite entanglement, the entanglement of a pair of systems shared by two parties, is easy to handle for **pure states**. For any pure two-party state, orthonormal bases of each subsystem exist, $\{|u_n\rangle\}$ and $\{|v_n\rangle\}$, so that the total state vector can be written in the “Schmidt decomposition” [1] as

$$|\psi\rangle = \sum_n c_n |u_n\rangle |v_n\rangle , \quad (12.1)$$

where the summation goes over the smaller of the dimensionalities of the two subsystems. The Schmidt coefficients c_n are real and non-negative, and satisfy $\sum_n c_n^2 = 1$. The Schmidt decomposition may be obtained by transforming the expansion of an arbitrary pure bipartite state as

$$|\psi\rangle = \sum_{mk} a_{mk} |m\rangle |k\rangle = \sum_{nmk} u_{mn} c_{nn} v_{kn} |m\rangle |k\rangle = \sum_n c_n |u_n\rangle |v_n\rangle , \quad (12.2)$$

with $c_{nn} \equiv c_n$. In the first step, the matrix a with complex elements a_{mk} is diagonalised, $a = ucv^T$, where u and v are unitary matrices and c is a diagonal matrix with non-negative elements. In the second step, we defined $|u_n\rangle \equiv \sum_m u_{mn} |m\rangle$ and $|v_n\rangle \equiv \sum_k v_{kn} |k\rangle$ which form orthonormal sets due to the unitarity of u and v and the orthonormality of $|m\rangle$ and $|k\rangle$. A pure state of two d -level systems (“qudits”) is now maximally entangled when the Schmidt

coefficients of its total state vector are all equal. Since the eigenvalues of the reduced density operator upon tracing out one half of a bipartite state are the Schmidt coefficients squared,

$$\hat{\rho}_1 = \text{Tr}_2 \hat{\rho}_{12} = \text{Tr}_2 |\psi\rangle_{12}\langle\psi| = \sum_n c_n^2 |u_n\rangle_1\langle u_n|, \quad (12.3)$$

tracing out either qudit of a maximally entangled state leaves the other half in the maximally mixed state \mathbb{I}/d . A pure two-party state is factorizable (not entangled) if and only if the number of nonzero Schmidt coefficients is one. Any Schmidt number greater than one indicates entanglement. Thus, the “majority” of pure state vectors in the Hilbert space of two parties are nonmaximally entangled. Furthermore, any pure two-party state is entangled if and only if for suitably chosen observables, it yields a violation of inequalities imposed by local realistic theories [2]. A unique measure of bipartite entanglement for pure states is given by the partial von Neumann entropy, the von Neumann entropy ($-\text{Tr}\hat{\rho} \log \hat{\rho}$) of the remaining system after tracing out either subsystem [3]: $E_{\text{v.N.}} = -\text{Tr}\hat{\rho}_1 \log_d \hat{\rho}_1 = -\sum_n c_n^2 \log_d c_n^2$, ranging between zero and one (in units of “edits”).

Mixed states are more subtle, even for only two parties. As for the quantification of bipartite mixed-state entanglement, there are various measures available such as the entanglement of formation and distillation [4]. Only for pure states, these measures coincide and equal the partial von Neumann entropy. The definition of pure-state entanglement via the non-factorizability of the total state vector is generalized to mixed states through non-separability (or inseparability) of the total density operator. 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 [5],

$$\hat{\rho}_{12} = \sum_i P_i \hat{\rho}_{i1} \otimes \hat{\rho}_{i2}. \quad (12.4)$$

Otherwise, it is inseparable¹. In general, it is a non-trivial question whether a given density operator is separable or inseparable. Nonetheless, a very convenient method to test for inseparability is Peres’ partial transpose criterion [6]. For a separable state as in Eq. (12.4), transposition of either density matrix yields again a legitimate non-negative density operator with unit trace,

$$\hat{\rho}'_{12} = \sum_i P_i (\hat{\rho}_{i1})^T \otimes \hat{\rho}_{i2}, \quad (12.5)$$

since $(\hat{\rho}_{i1})^T = (\hat{\rho}_{i1})^*$ 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. In the (2×2) - and (2×3) -dimensional cases (and, for example, for

two-mode Gaussian states, see below), this condition is both necessary and sufficient. For any other dimension, negative partial transpose is only sufficient for inseparability [7]². Other sufficient inseparability criteria include violations of inequalities imposed by local realistic theories (though mixed inseparable states do not necessarily lead to such violations), an entropic inequality [namely $E_{\text{v.N.}}(\hat{\rho}_1) > E_{\text{v.N.}}(\hat{\rho}_{12})$, again with $\hat{\rho}_1 = \text{Tr}_2 \hat{\rho}_{12}$] [11], and a condition based on the theory of majorization [12]. Concluding the discussion of two-party entanglement, we emphasize that both the pure-state Schmidt decomposition and the partial transpose criterion for mixed states are also applicable to infinite dimensions. An example for the infinite-dimensional Schmidt decomposition is the two-mode squeezed vacuum state in the Fock (photon number) basis [13]. The unphysical operation (a positive, but not completely positive map) that corresponds to the transposition is time reversal [14]: in terms of continuous variables, any separable two-party state remains a legitimate state after the transformation $(x_1, p_1, x_2, p_2) \rightarrow (x_1, -p_1, x_2, p_2)$, where (x_i, p_i) are the phase-space variables (positions and momenta) for example in the Wigner representation. However, arbitrary inseparable states may be turned into unphysical states, and furthermore, inseparable two-party two-mode Gaussian states always become unphysical via this transformation [14].

Multipartite entanglement, the entanglement shared by more than two parties, is a more complex issue. For **pure** multi-party states, a Schmidt decomposition does not exist in general. The total state vector then cannot be written as a single sum over orthonormal basis states. There is, however, one very important representative of multipartite entanglement which does have the form of a multi-party Schmidt decomposition, namely the Greenberger-Horne-Zeilinger (GHZ) state [15]

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) , \quad (12.6)$$

here given as a three-qubit state. Although there is no rigorous definition of maximally entangled multi-party states due to the lack of a general Schmidt decomposition, the form of the GHZ state with all “Schmidt coefficients” equal suggests that it exhibits maximum multipartite entanglement. In fact, there are various reasons for assigning the attribute “maximally entangled” to the N -party GHZ states $[(|000\dots000\rangle + |111\dots111\rangle)/\sqrt{2}]$. For example, they yield the maximum violations of multi-party inequalities imposed by local realistic theories [16]. Further, their entanglement heavily relies on all parties, and if examined pairwise they do not contain simple bipartite entanglement (see below).

For the case of three qubits, any pure and fully entangled state can be transformed to either the GHZ state or the so-called W state [17],

$$|W\rangle = \frac{1}{\sqrt{3}} (|100\rangle + |010\rangle + |001\rangle) , \quad (12.7)$$

via stochastic local operations and classical communication (“SLOCC”, where stochastic means that the state is transformed with non-zero probability). Thus, with respect to SLOCC, there are two inequivalent classes of genuine tripartite entanglement, represented by the GHZ and the W state. Genuinely or fully tripartite entangled here means that the entanglement of the three-qubit state is not just present between two parties while the remaining party can be separated by a tensor product. Though genuinely tripartite, the entanglement of the W state is also “readily bipartite”. This means that the remaining two-party state after tracing out one party,

$$\text{Tr}_1 |W\rangle\langle W| = \frac{1}{3} (|00\rangle\langle 00| + |10\rangle\langle 10| + |01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01|) , \quad (12.8)$$

is inseparable which can be verified by taking the partial transpose [the eigenvalues are $1/3$, $1/3$, $(1 \pm \sqrt{5})/6$]. This is in contrast to the GHZ state where tracing out one party yields the separable two-qubit state

$$\begin{aligned} \text{Tr}_1 |GHZ\rangle\langle GHZ| &= \frac{1}{2} (|00\rangle\langle 00| + |11\rangle\langle 11|) \\ &= \frac{1}{2} (|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|) . \end{aligned} \quad (12.9)$$

Note that this is not the maximally mixed state of two qubits, $\mathbb{1}^{\otimes 2}/4$. The maximally mixed state of one qubit, however, is obtained after tracing out two parties of the GHZ state. Maximum bipartite entanglement is available from the GHZ state through a local measurement of one party in the conjugate basis $\{|0\rangle \pm |1\rangle\}/\sqrt{2}$ (plus classical communication about the result),

$$\frac{\frac{1}{2} (|0\rangle_1 \pm |1\rangle_1) ({}_1\langle 0| \pm {}_1\langle 1|) |GHZ\rangle}{\|\frac{1}{2} (|0\rangle_1 \pm |1\rangle_1) ({}_1\langle 0| \pm {}_1\langle 1|) |GHZ\rangle\|} = \frac{1}{\sqrt{2}} (|0\rangle_1 \pm |1\rangle_1) \otimes |\Phi^\pm\rangle . \quad (12.10)$$

Here, $|\Phi^\pm\rangle$ are two of the four Bell states, $|\Phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\Psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$.

What can be said about arbitrary **mixed** entangled states of more than two parties? There is of course an immense variety of inequivalent classes of multi-party mixed states [e.g., five classes of three-qubit states of which the extreme cases are the fully separable ($\hat{\rho} = \sum_i P_i \hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \otimes \hat{\rho}_{i3}$) and the fully (genuinely)

inseparable states [18]]. In general, multi-party inseparability criteria cannot be formulated in such a compact form as the two-party partial transpose criterion. Similarly, the quantification of multipartite entanglement, even for pure states, is still subject of current research. Existing multi-party entanglement measures do not appear to be unique as is the partial von Neumann entropy for pure two-party states. Furthermore, violations of multi-party inequalities imposed by local realism do not necessarily imply genuine multi-party inseparability. In the case of continuous variables, we may now focus on the following questions: How can we generate, measure, and (theoretically and experimentally) verify genuine multipartite entangled states? How do the continuous-variable states compare to their qubit counterparts with respect to various properties?

2.2 CREATING MULTIPARTITE ENTANGLEMENT

A compact way to describe how entanglement may be created is in terms of a quantum circuit. Quantum circuits consist of a sequence of unitary transformations (quantum gates), sometimes supplemented by measurements. A quantum circuit is independent of a particular physical realization.

Let us consider the generation of entanglement between arbitrarily many qubits. The quantum circuit shall turn N independent qubits into an N -partite entangled state. Initially, the N qubits shall be in the eigenstate $|0\rangle$. All we need is a circuit with the following two elementary gates: the Hadamard gate, acting on a single qubit as

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad (12.11)$$

and the controlled-NOT (C-NOT) gate, a two-qubit operation acting as

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow |11\rangle, \quad |11\rangle \rightarrow |10\rangle. \quad (12.12)$$

The first qubit (control qubit) remains unchanged under the C-NOT. The second qubit (target qubit) is flipped if the control qubit is set to 1, and is left unchanged otherwise. Equivalently, we can describe the action of the C-NOT gate by $|y_1, y_2\rangle \rightarrow |y_1, y_1 \oplus y_2\rangle$ with $y_1, y_2 = 0, 1$ and the addition modulo two \oplus . The N -partite entangled output state of the circuit (see Fig. 12.1) is the N -qubit GHZ state.

Let us translate the qubit quantum circuit to continuous variables [19]. The position and momentum variables x and p (units-free with $\hbar = \frac{1}{2}$, $[\hat{x}_l, \hat{p}_k] = i\delta_{lk}/2$) may correspond to the quadrature amplitudes of a single electromagnetic mode, i.e., the real and imaginary part of the single mode's annihilation operator: $\hat{a} = \hat{x} + i\hat{p}$. At this stage, it is convenient to consider position and momentum eigenstates. We may now replace the Hadamard by a

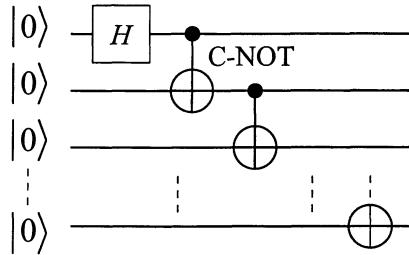


Figure 12.1 Quantum circuit for generating the N -qubit GHZ state. The gates (unitary transformations) are a Hadamard gate (“ H ”) and pairwise acting C-NOT gates.

Fourier transform,

$$\mathcal{F}|x\rangle_{\text{position}} = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} dy e^{2ixy} |y\rangle_{\text{position}} = |p = x\rangle_{\text{momentum}}, \quad (12.13)$$

and the C-NOT gates by appropriate beam splitter operations ³. The input states are taken to be zero-position eigenstates $|x = 0\rangle$. The sequence of beam splitter operations $\hat{B}_{jk}(\theta)$ is provided by a network of ideal phase-free beam splitters (with typically asymmetric transmittance and reflectivity) acting on the position eigenstates as

$$\hat{B}_{12}(\theta)|x_1, x_2\rangle = |x_1 \sin \theta + x_2 \cos \theta, x_1 \cos \theta - x_2 \sin \theta\rangle = |x'_1, x'_2\rangle. \quad (12.14)$$

Now we apply this sequence of beam splitters (making an “ N -splitter”),

$$\hat{B}_{N-1 N}(\pi/4) \hat{B}_{N-2 N-1} \left(\sin^{-1} 1/\sqrt{3} \right) \times \cdots \times \hat{B}_{12} \left(\sin^{-1} 1/\sqrt{N} \right), \quad (12.15)$$

to a zero-momentum eigenstate $|p = 0\rangle \propto \int dx |x\rangle$ of mode 1 (the Fourier transformed zero-position eigenstate) and $N - 1$ zero-position eigenstates $|x = 0\rangle$ in modes 2 through N . We obtain the entangled N -mode state $\int dx |x, x, \dots, x\rangle$. This state is an eigenstate with total momentum zero and all relative positions $x_i - x_j = 0$ ($i, j = 1, 2, \dots, N$). It is clearly an analogue to the qubit GHZ state with perfect correlations among the quadratures. However, it is an unphysical and unnormalizable state (e.g., for two modes, it corresponds to the maximally entangled, infinitely squeezed two-mode squeezed vacuum state with infinite energy). Rather than sending infinitely squeezed position eigenstates through the entanglement-generating circuit, we will now use finitely squeezed states.

In the Heisenberg representation, an ideal phase-free beam splitter operation acting on two modes with annihilation operators \hat{c}_k and \hat{c}_l is described by

$$\begin{pmatrix} \hat{c}'_k \\ \hat{c}'_l \end{pmatrix} = \begin{pmatrix} \sin \theta & \cos \theta \\ \cos \theta & -\sin \theta \end{pmatrix} \begin{pmatrix} \hat{c}_k \\ \hat{c}_l \end{pmatrix}. \quad (12.16)$$

Let us now define a matrix $B_{kl}(\theta)$ which is an N -dimensional identity matrix with the entries I_{kk} , I_{kl} , I_{lk} , and I_{ll} replaced by the corresponding entries of the above beam splitter matrix. Thus, the matrix for the N -splitter becomes

$$\begin{aligned} \mathcal{U}(N) &\equiv B_{N-1 N} \left(\sin^{-1} \frac{1}{\sqrt{2}} \right) B_{N-2 N-1} \left(\sin^{-1} \frac{1}{\sqrt{3}} \right) \\ &\quad \times \cdots \times B_{12} \left(\sin^{-1} \frac{1}{\sqrt{N}} \right). \end{aligned} \quad (12.17)$$

The entanglement-generating circuit is now applied to N position-squeezed vacuum modes. In other words, one momentum-squeezed and $N - 1$ position-squeezed vacuum modes are coupled by an N -splitter,

$$(\hat{a}'_1 \quad \hat{a}'_2 \quad \cdots \quad \hat{a}'_N)^T = \mathcal{U}(N) (\hat{a}_1 \quad \hat{a}_2 \quad \cdots \quad \hat{a}_N)^T, \quad (12.18)$$

where the input modes are squeezed [13] according to

$$\begin{aligned} \hat{a}_1 &= \cosh r_1 \hat{a}_1^{(0)} + \sinh r_1 \hat{a}_1^{(0)\dagger}, \\ \hat{a}_i &= \cosh r_2 \hat{a}_i^{(0)} - \sinh r_2 \hat{a}_i^{(0)\dagger}, \end{aligned} \quad (12.19)$$

with $i = 2, 3, \dots, N$ and vacuum modes labeled by the superscript '(0)'. In terms of the input quadratures, we have

$$\begin{aligned} \hat{x}_1 &= e^{+r_1} \hat{x}_1^{(0)}, & \hat{p}_1 &= e^{-r_1} \hat{p}_1^{(0)}, \\ \hat{x}_i &= e^{-r_2} \hat{x}_i^{(0)}, & \hat{p}_i &= e^{+r_2} \hat{p}_i^{(0)}, \end{aligned} \quad (12.20)$$

for $\hat{a}_j = \hat{x}_j + i\hat{p}_j$ ($j = 1, 2, \dots, N$). The squeezing parameters r_1 and r_2 determine the degree of squeezing of the momentum-squeezed and the $N - 1$ position-squeezed modes, respectively. The correlations between the output quadratures are revealed by the arbitrarily small noise in the relative positions and the total momentum for sufficiently large squeezing r_1 and r_2 ,

$$\begin{aligned} \langle (\hat{x}'_k - \hat{x}'_l)^2 \rangle &= e^{-2r_2}/2, \\ \langle (\hat{p}'_1 + \hat{p}'_2 + \cdots + \hat{p}'_N)^2 \rangle &= Ne^{-2r_1}/4, \end{aligned} \quad (12.21)$$

for $k \neq l$ ($k, l = 1, 2, \dots, N$) and $\hat{a}'_k = \hat{x}'_k + i\hat{p}'_k$. Note that all modes involved have zero mean values, thus the variances and the second moments are identical.

2.3 MEASURING MULTIPARTITE ENTANGLEMENT

Rather than constructing a circuit for generating entangled states, now our task shall be the measurement of multi-party entanglement, i.e., the projection onto the basis of maximally entangled multi-party states. For qubits, it is well-known that this can be achieved simply by inverting the above entanglement-generating circuit (a similar strategy also works for d -level systems [20]). The GHZ basis states for N qubits read

$$\begin{aligned} |\Psi_{n,m_1,m_2,\dots,m_{N-1}}\rangle &= \frac{1}{\sqrt{2}} (|0\rangle \otimes |m_1\rangle \otimes |m_2\rangle \otimes \cdots \otimes |m_{N-1}\rangle \\ &\quad + (-1)^n |1\rangle \otimes |1 \oplus m_1\rangle \otimes |1 \oplus m_2\rangle \otimes \cdots \otimes |1 \oplus m_{N-1}\rangle), \end{aligned} \quad (12.22)$$

where $n, m_1, m_2, \dots, m_{N-1} = 0, 1$. The projection onto the basis states $\{|\Psi_{n,m_1,m_2,\dots,m_{N-1}}\rangle\}$ is accomplished when the output states of the inverted circuit (see Fig. 12.1),

$$\begin{aligned} &(\text{CNOT}_{N-1 N} \text{CNOT}_{N-2 N-1} \cdots \text{CNOT}_{12} H_1)^{-1} \\ &= H_1 \text{CNOT}_{12} \text{CNOT}_{23} \cdots \text{CNOT}_{N-1 N}, \end{aligned} \quad (12.23)$$

are measured in the computational basis. Eventually, $\{|\Psi_{n,m_1,m_2,\dots,m_{N-1}}\rangle\}$ are distinguished via the measured output states

$$|n\rangle \otimes |m_1\rangle \otimes |m_1 \oplus m_2\rangle \otimes |m_2 \oplus m_3\rangle \otimes \cdots \otimes |m_{N-2} \oplus m_{N-1}\rangle. \quad (12.24)$$

Reentering the domain of continuous variables, let us now introduce the maximally entangled states

$$\begin{aligned} |\Psi(v, u_1, u_2, \dots, u_{N-1})\rangle &= \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} dx e^{2ivx} |x\rangle \otimes |x - u_1\rangle \\ &\quad \otimes |x - u_1 - u_2\rangle \otimes \cdots \otimes |x - u_1 - u_2 - \cdots - u_{N-1}\rangle. \end{aligned} \quad (12.25)$$

Since $\int_{-\infty}^{\infty} |x\rangle\langle x| = \mathbb{1}$ and $\langle x|x'\rangle = \delta(x - x')$, they form a complete,

$$\begin{aligned} &\int_{-\infty}^{\infty} dv du_1 du_2 \cdots du_{N-1} |\Psi(v, u_1, u_2, \dots, u_{N-1})\rangle\langle\Psi(v, u_1, u_2, \dots, u_{N-1})| \\ &= \mathbb{1}^{\otimes N}, \end{aligned} \quad (12.26)$$

and orthogonal,

$$\begin{aligned} &\langle\Psi(v, u_1, u_2, \dots, u_{N-1})|\Psi(v', u'_1, u'_2, \dots, u'_{N-1})\rangle \\ &= \delta(v - v')\delta(u_1 - u'_1)\delta(u_2 - u'_2)\cdots\delta(u_{N-1} - u'_{N-1}), \end{aligned} \quad (12.27)$$

set of basis states for N modes. For creating continuous-variable entanglement, we simply replaced the C-NOT gates by appropriate beam splitter operations. Let us employ the same strategy here in order to measure

continuous-variable entanglement. In other words, a projection onto the continuous-variable GHZ basis $\{|\Psi(v, u_1, u_2, \dots, u_{N-1})\rangle\}$ shall be performed by applying an inverse N -splitter followed by a Fourier transform of mode 1 and by subsequently measuring the positions of all modes. For an N -mode state with modes $\hat{b}_1, \hat{b}_2, \dots, \hat{b}_N$, this means that we effectively measure $\text{Im } \hat{b}'_1 \equiv \hat{p}'_1, \text{Re } \hat{b}'_2 \equiv \hat{x}'_2, \text{Re } \hat{b}'_3 \equiv \hat{x}'_3, \dots, \text{Re } \hat{b}'_N \equiv \hat{x}'_N$, with

$$(\hat{b}'_1 \quad \hat{b}'_2 \quad \dots \quad \hat{b}'_N)^T = \mathcal{U}^\dagger(N) (\hat{b}_1 \quad \hat{b}_2 \quad \dots \quad \hat{b}_N)^T. \quad (12.28)$$

For instance, in the three-mode case, the measured observables are

$$\begin{aligned} \hat{p}'_1 &= \frac{1}{\sqrt{3}}(\hat{p}_1 + \hat{p}_2 + \hat{p}_3), \\ \hat{x}'_2 &= \sqrt{\frac{2}{3}}\hat{x}_1 - \frac{1}{\sqrt{6}}(\hat{x}_2 + \hat{x}_3), \\ \hat{x}'_3 &= \frac{1}{\sqrt{2}}(\hat{x}_2 - \hat{x}_3), \end{aligned} \quad (12.29)$$

where here $\hat{b}_j = \hat{x}_j + i\hat{p}_j$. In fact, in a single shot, the quantities $v/\sqrt{3}, \sqrt{2/3}(u_1 + u_2/2)$, and $u_2/\sqrt{2}$ are determined through these measurements, and so are all the parameters $v \equiv p_1 + p_2 + p_3, u_1 \equiv x_1 - x_2$, and $u_2 \equiv x_2 - x_3$ required to detect the basis state $|\Psi(v, u_1, u_2)\rangle$ from Eq. (12.25) with $N = 3$. In general, for arbitrary N , the measurements yield $p'_1 = v/\sqrt{N}$ and

$$\begin{aligned} x'_2 &= \sqrt{\frac{N-1}{N}} \left(u_1 + \frac{N-2}{N-1} \left(u_2 + \frac{N-3}{N-2} (u_3 + \dots) \right) \right), \\ &\vdots && \vdots && \vdots \\ x'_{N-3} &= \sqrt{\frac{4}{5}} \left(u_{N-4} + \frac{3}{4} \left(u_{N-3} + \frac{2}{3} \left(u_{N-2} + \frac{1}{2} u_{N-1} \right) \right) \right), \\ x'_{N-2} &= \sqrt{\frac{3}{4}} \left(u_{N-3} + \frac{2}{3} \left(u_{N-2} + \frac{1}{2} u_{N-1} \right) \right), \\ x'_{N-1} &= \sqrt{\frac{2}{3}} \left(u_{N-2} + \frac{1}{2} u_{N-1} \right), \\ x'_N &= \frac{1}{\sqrt{2}} u_{N-1}, \end{aligned} \quad (12.30)$$

where $v \equiv p_1 + p_2 + \dots + p_N, u_1 \equiv x_1 - x_2, u_2 \equiv x_2 - x_3, \dots$, and $u_{N-1} \equiv x_{N-1} - x_N$. This confirms that the inverse N -splitter combined with the appropriate homodyne detections (that is tools solely from linear optics) enables in principle a complete distinction of the basis states $\{|\Psi(v, u_1, u_2, \dots, u_{N-1})\rangle\}$ in

Eq. (12.25). More precisely, the fidelity of the state discrimination can be arbitrarily high for sufficiently good accuracy of the homodyne detectors. We may conclude that the requirements of such a “GHZ state analyzer” for continuous variables are easily met by current experimental capabilities. This is in contrast to the GHZ state analyzer for photonic qubits [capable of discriminating or measuring states like those in Eq. (12.22)]. Although arbitrarily high fidelity can be approached in principle using linear optics and photon number detectors, one would need sufficiently many, highly entangled auxiliary photons and detectors resolving correspondingly large photon numbers [21, 20]. Neither of these requirements is met by current technology. Of course, the C-NOT gates of a qubit GHZ state measurement device can in principle be implemented via the so-called cross Kerr effect using nonlinear optics. However, on the single-photon level, this would require optical nonlinearities of exotic strength.

In this section, we have shown how measurements onto the maximally entangled continuous-variable GHZ basis can be realized using linear optics and quadrature detections. These schemes are an extension of the well-known two-party case, where the continuous-variable Bell basis [Eq. (12.25) with $N = 2$] is the analogue to the qubit Bell states [Eq. (12.22) with $N = 2$]. The continuous-variable and the qubit Bell states form those measurement bases that were used in the quantum teleportation experiments [22] and [23, 24], respectively. The extension of measurements onto the maximally entangled basis to more than two parties and their potential optical realization in the continuous-variable realm might be relevant to multi-party quantum communication protocols such as the multi-party generalization of entanglement swapping [25]. However, the entanglement resources in a continuous-variable protocol, namely the entangled continuous-variable states that are producible with squeezed light and beam splitters, exhibit only imperfect entanglement due to the finite degree of the squeezing. When can we actually be sure that they are multi-party entangled at all? In the next section, we will address this question and discuss criteria for the theoretical and the experimental verification of multipartite continuous-variable entanglement.

2.4 SUFFICIENT INSEPARABILITY CRITERIA

For continuous-variable two-party states, an inseparability criterion can be derived that does not rely on the partial transpose. It is based on the variances of quadrature combinations such as $\hat{x}_1 - \hat{x}_2$ and $\hat{p}_1 + \hat{p}_2$, motivated by the fact that the maximally entangled bipartite state $\int dx |x, x\rangle$ is a (zero-)eigenstate of these two combinations [26]. Similarly, in a continuous-variable Bell measurement, the quadrature combinations $\hat{x}_1 - \hat{x}_2$ and $\hat{p}_1 + \hat{p}_2$ are the relevant observables to be detected. Hence, for two modes, applying the variance-based inseparability criterion and measuring in the maximally entangled basis

can both be accomplished by equal means, namely a single beam splitter and two homodyne detectors. In other words, the effectively inverse circuit for the generation of bipartite entanglement provides the recipe for both measuring maximum entanglement and verifying nonmaximum entanglement. When looking for multi-party inseparability criteria for arbitrarily many modes, it seems to be natural to pursue a similar strategy. We are therefore aiming at a criterion which is based on the variances of those quadrature combinations that are the measured observables in a continuous-variable GHZ measurement.

Let us consider three modes. According to Eq. (12.29), we define the operators

$$\begin{aligned}\hat{u} &\equiv \frac{1}{\sqrt{2}}(\hat{x}_2 - \hat{x}_3) , \\ \hat{v} &\equiv \sqrt{\frac{2}{3}}\hat{x}_1 - \frac{1}{\sqrt{6}}(\hat{x}_2 + \hat{x}_3) , \\ \hat{w} &\equiv \frac{1}{\sqrt{3}}(\hat{p}_1 + \hat{p}_2 + \hat{p}_3) \times \sqrt{2} ,\end{aligned}\quad (12.31)$$

where we added a factor of $\sqrt{2}$ in \hat{w} compared to the first line of Eq. (12.29). Let us further assume that the three-party state $\hat{\rho}$ is fully separable and can be written as a mixture of tripartite product states,

$$\hat{\rho} = \sum_i P_i \hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \otimes \hat{\rho}_{i3} . \quad (12.32)$$

Using this state, we can calculate the total variance of the operators in Eq. (12.31),

$$\begin{aligned}& \langle (\Delta\hat{u})^2 \rangle_\rho + \langle (\Delta\hat{v})^2 \rangle_\rho + \langle (\Delta\hat{w})^2 \rangle_\rho \\&= \sum_i P_i \left(\langle \hat{u}^2 \rangle_i + \langle \hat{v}^2 \rangle_i + \langle \hat{w}^2 \rangle_i \right) - \langle \hat{u} \rangle_\rho^2 - \langle \hat{v} \rangle_\rho^2 - \langle \hat{w} \rangle_\rho^2 \\&= \sum_i P_i \frac{2}{3} \left(\langle \hat{x}_1^2 \rangle_i + \langle \hat{x}_2^2 \rangle_i + \langle \hat{x}_3^2 \rangle_i + \langle \hat{p}_1^2 \rangle_i + \langle \hat{p}_2^2 \rangle_i + \langle \hat{p}_3^2 \rangle_i \right) \\&\quad - \sum_i P_i \frac{2}{3} \left(\langle \hat{x}_1 \rangle_i \langle \hat{x}_2 \rangle_i + \langle \hat{x}_1 \rangle_i \langle \hat{x}_3 \rangle_i + \langle \hat{x}_2 \rangle_i \langle \hat{x}_3 \rangle_i \right. \\&\quad \left. - 2\langle \hat{p}_1 \rangle_i \langle \hat{p}_2 \rangle_i - 2\langle \hat{p}_1 \rangle_i \langle \hat{p}_3 \rangle_i - 2\langle \hat{p}_2 \rangle_i \langle \hat{p}_3 \rangle_i \right) - \langle \hat{u} \rangle_\rho^2 - \langle \hat{v} \rangle_\rho^2 - \langle \hat{w} \rangle_\rho^2\end{aligned}$$

$$\begin{aligned}
&= \sum_i P_i \frac{2}{3} \left(\langle (\Delta \hat{x}_1)^2 \rangle_i + \langle (\Delta \hat{x}_2)^2 \rangle_i + \langle (\Delta \hat{x}_3)^2 \rangle_i \right. \\
&\quad \left. + \langle (\Delta \hat{p}_1)^2 \rangle_i + \langle (\Delta \hat{p}_2)^2 \rangle_i + \langle (\Delta \hat{p}_3)^2 \rangle_i \right) \\
&\quad + \sum_i P_i \langle \hat{u} \rangle_i^2 - \left(\sum_i P_i \langle \hat{u} \rangle_i \right)^2 + \sum_i P_i \langle \hat{v} \rangle_i^2 - \left(\sum_i P_i \langle \hat{v} \rangle_i \right)^2 \\
&\quad + \sum_i P_i \langle \hat{w} \rangle_i^2 - \left(\sum_i P_i \langle \hat{w} \rangle_i \right)^2, \tag{12.33}
\end{aligned}$$

where $\langle \dots \rangle_i$ means the average in the product state $\hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \otimes \hat{\rho}_{i3}$. Similar to the derivation in Ref. [26], we can apply the Cauchy-Schwarz inequality $\sum_i P_i \langle \hat{u} \rangle_i^2 \geq (\sum_i P_i |\langle \hat{u} \rangle_i|)^2$, and see that the last two lines in Eq. (12.33) are bounded below by zero. Also taking into account the sum uncertainty relation $\langle (\Delta \hat{x}_j)^2 \rangle_i + \langle (\Delta \hat{p}_j)^2 \rangle_i \geq |[\hat{x}_j, \hat{p}_j]| = 1/2 (j = 1, 2, 3)$, we find that the total variance itself is bounded below by 1 (using $\sum_i P_i = 1$). Any total variance smaller than this boundary of 1 would imply that the quantum state concerned is not fully separable as in Eq. (12.32). But would this also imply that the quantum state is genuinely tripartite entangled in the sense that none of the parties can be separated from the others (as, for example, in the pure qubit states $|GHZ\rangle$ and $|W\rangle$)? This is obviously not the case and a total variance below 1 does not rule out the possibility of *partial separability*. The quantum state might still not be a genuine tripartite entangled state, since it might be written in one or more of the following forms⁴ [18]:

$$\hat{\rho} = \sum_i P_i \hat{\rho}_{i12} \otimes \hat{\rho}_{i3}, \quad \hat{\rho} = \sum_i P'_i \hat{\rho}_{i13} \otimes \hat{\rho}_{i2}, \quad \hat{\rho} = \sum_i P''_i \hat{\rho}_{i23} \otimes \hat{\rho}_{i1}. \tag{12.34}$$

Thus, in general, a violation of $\langle (\Delta \hat{u})^2 \rangle_\rho + \langle (\Delta \hat{v})^2 \rangle_\rho + \langle (\Delta \hat{w})^2 \rangle_\rho \geq 1$ does not necessarily witness genuine tripartite entanglement (a counterexample will be given below). However, it does witness genuine tripartite entanglement when the quantum state in question is pure and totally symmetric with respect to all three subsystems [28]. In that case, a possible separation of any individual subsystem,

$$\hat{\rho} = \hat{\rho}_{12} \otimes \hat{\rho}_3, \quad \hat{\rho} = \hat{\rho}_{13} \otimes \hat{\rho}_2, \quad \hat{\rho} = \hat{\rho}_{23} \otimes \hat{\rho}_1, \tag{12.35}$$

implies full separability, $\hat{\rho} = \hat{\rho}_1 \otimes \hat{\rho}_2 \otimes \hat{\rho}_3$. Hence a total variance below 1 negates the possibility of any form of separability in this case.

By extending the quadrature combinations in Eq. (12.31) from 3 to N parties (corresponding to the output modes of an inverse N -splitter) and performing a similar calculation as for $N = 3$ with an additional factor of $\sqrt{N-1}$ in the total momentum operator \hat{w} , we find that any N -mode state with modes

$\hat{b}_1, \hat{b}_2, \dots, \hat{b}_N$ which is *fully separable*, $\hat{\rho} = \sum_i P_i \hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \otimes \dots \otimes \hat{\rho}_{iN}$, obeys the inequality

$$\langle (\Delta \hat{p}'_1)^2 \rangle_\rho + \frac{\sum_{i=2}^N \langle (\Delta \hat{x}'_i)^2 \rangle_\rho}{N-1} \geq \frac{1}{2}. \quad (12.36)$$

Here, $\hat{p}'_1 \equiv \text{Im } \hat{b}'_1, \hat{x}'_2 \equiv \text{Re } \hat{b}'_2, \dots, \hat{x}'_N \equiv \text{Re } \hat{b}'_N$ are the corresponding output quadratures of the inverse N -splitter applied to the modes $\hat{b}_1, \hat{b}_2, \dots, \hat{b}_N$ [Eq. (12.28)]. Alternatively, one can also derive the following necessary condition for full separability [28],

$$\frac{\sum_{i,j}^N \langle (\Delta \hat{X}_{ij})^2 \rangle_\rho}{2(N-1)} + \langle (\Delta \hat{P})^2 \rangle_\rho \geq \frac{N}{2}. \quad (12.37)$$

In this inequality, $\hat{X}_{ij} = \hat{x}_i - \hat{x}_j$ and $\hat{P} = \sum_{i=1}^N \hat{p}_i$ are the relative positions and the total momentum of the relevant state with modes $\hat{b}_j = \hat{x}_j + i\hat{p}_j$.

The choice of the operators in the inequalities Eq. (12.36) and Eq. (12.37) relies upon the fact that the quantum fluctuations of these observables simultaneously vanish for maximum GHZ entanglement. This must be in agreement with their commutation relations, and indeed, we have

$$[\hat{X}_{ij}, \hat{P}] = [\hat{x}_i - \hat{x}_j, \hat{p}_i + \hat{p}_j] = 0, \quad (12.38)$$

for any N and i, j . Similarly, the output quadratures of the inverse N -splitter yield, for instance, for $N = 3$,

$$[\hat{p}_1 + \hat{p}_2 + \hat{p}_3, \hat{x}_2 - \hat{x}_3] = 0, \quad [\hat{p}_1 + \hat{p}_2 + \hat{p}_3, 2\hat{x}_1 - (\hat{x}_2 + \hat{x}_3)] = 0. \quad (12.39)$$

Both criteria in Eq. (12.36) and Eq. (12.37) represent necessary conditions for full separability, though they are not entirely equivalent [i.e., there are partially inseparable states that violate Eq. (12.37), but satisfy Eq. (12.36), see below]. Moreover, the criterion in Eq. (12.37) contains in some sense redundant observables. As we know from the previous section, N observables suffice to measure an N -party GHZ entangled state. These N observables are suitably chosen quadratures of the N output modes of an inverse N -splitter. Their detection simultaneously determines the total momentum and the $N-1$ relative positions $\hat{x}_1 - \hat{x}_2, \hat{x}_2 - \hat{x}_3, \dots$, and $\hat{x}_{N-1} - \hat{x}_N$ [Eq. (12.30)]⁵. However, in Eq. (12.37), there are $1 + [N(N-1)]/2$ different operators. Nevertheless, for two parties and modes, the conditions in Eq. (12.36) and Eq. (12.37) coincide and correspond to the necessary separability condition for arbitrary bipartite states given in Ref. [26].

In summary, we have shown in this section that the circuit for measuring GHZ entanglement also provides a sufficient inseparability criterion for

arbitrary multi-party continuous-variable states (pure or mixed, Gaussian or non-Gaussian) of arbitrarily many parties. This criterion is experimentally accessible via linear optics and homodyne detections. The disadvantage of not being a necessary inseparability condition (not even for Gaussian states, see below) might be unsatisfactory from a theoretical point of view, but would not be an obstacle to experimental inseparability proofs. A more serious drawback, in particular when considering an experimental verification of multi-party entanglement, is the fact that without additional assumptions, for arbitrary states, the criteria presented in this section are in general not sufficient for genuine multi-party inseparability. They verify only partial inseparability. In the next section, we will give a simple example for this.

2.5 MULTI-PARTY ENTANGLED STATES

2.5.1 Partial multipartite entanglement. Let us investigate how the following pure three-mode state described by the Heisenberg operators

$$\begin{aligned}\hat{x}'_1 &= (e^{+r} \hat{x}_1^{(0)} + e^{-r} \hat{x}_2^{(0)})/\sqrt{2}, & \hat{p}'_1 &= (e^{-r} \hat{p}_1^{(0)} + e^{+r} \hat{p}_2^{(0)})/\sqrt{2}, \\ \hat{x}'_2 &= (e^{+r} \hat{x}_1^{(0)} - e^{-r} \hat{x}_2^{(0)})/\sqrt{2}, & \hat{p}'_2 &= (e^{-r} \hat{p}_1^{(0)} - e^{+r} \hat{p}_2^{(0)})/\sqrt{2}, \\ \hat{x}'_3 &= \hat{x}_3^{(0)}, & \hat{p}'_3 &= \hat{p}_3^{(0)},\end{aligned}\quad (12.40)$$

behaves with respect to the multi-party inseparability criteria. Modes 1 and 2 are in a two-mode squeezed vacuum state [Eq. (12.18) and Eq. (12.20) for $N = 2$ and $r = r_1 = r_2$], and mode 3 is in the vacuum state. This three-party state is obviously only partially⁶ entangled (it is an example for the second class of the five classes of three-mode Gaussian states in Ref. [27]). Applying an inverse “tritter” (three-splitter) to these modes, calculating the relevant output variances, and inserting them into Eq. (12.36) yields

$$\frac{1}{4} \left(\frac{1}{3} e^{+2r} + e^{-2r} \right) + \frac{1}{6} \geq \frac{1}{2}, \quad (12.41)$$

as a necessary condition for full separability. We find that equality holds for $r = 0$ which doesn't tell us anything, though we know, of course, that the state is fully separable in this case and must obey Eq. (12.36). For some finite squeezing r , the inequality Eq. (12.41) is illustrated in Fig. 12.2. Similarly, application of the criterion in Eq. (12.37) to the above state leads to

$$\frac{1}{4} (3e^{-2r} + \cosh 2r + 2) \geq \frac{3}{2}. \quad (12.42)$$

Again, equality holds for $r = 0$. In Fig. 12.2, also this condition is depicted for some finite squeezing r .

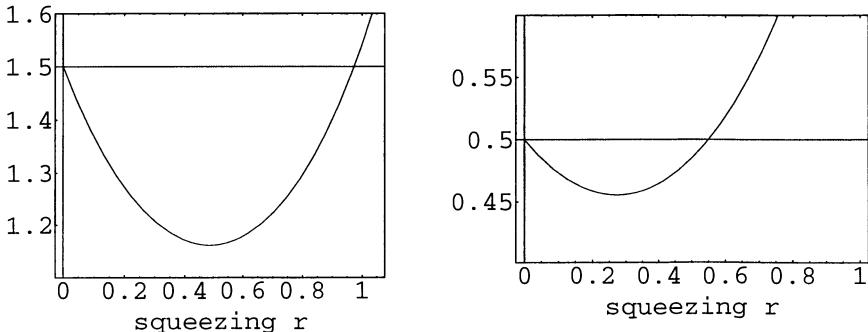


Figure 12.2 Application of the necessary conditions for full three-party separability. On the left: the inequality Eq. (12.42) with the boundary $3/2$ as a function of the squeezing r ; for $0 < r < 1$, the inequality is violated nearly everywhere. On the right: the inequality Eq. (12.41) with the boundary $1/2$ as a function of the squeezing r ; for $0 < r < 1$, the inequality is satisfied nearly as much as it is violated.

The comparison between the two conditions in this example demonstrates that they are not equivalent. For some squeezing, the partially entangled three-mode state violates Eq. (12.37) while satisfying Eq. (12.36). Moreover, both conditions can apparently be violated by an only partially entangled state. Hence, both their violation, though ruling out full separability, does not imply the presence of genuine multi-party entanglement. Another observation is that both conditions are satisfied for sufficiently large squeezing when the partial entanglement is sufficiently good. This confirms that the two conditions are necessary for full separability, but not sufficient, not even for a Gaussian state like that in our example. In fact, also the bipartite separability condition of Ref. [26] is both necessary and sufficient only for Gaussian states in a certain standard form (where any Gaussian state can be transformed into this standard form via local operations). The partially entangled three-mode state here lacks the symmetry that is required for a state to violate the separability conditions whenever it contains some entanglement. We will now turn to a family of multipartite entangled states which are totally symmetric with respect to all their parties, which do always violate both conditions for full multi-party separability, and which are indeed genuinely multi-party entangled.

2.5.2 Genuine multipartite entanglement. Let us consider the output states of the entanglement-generating circuit in section 2.2. There, we applied an N -splitter to one momentum-squeezed (r_1) and $N - 1$ position-squeezed (r_2) vacuum modes to obtain the modes $\hat{a}'_1, \hat{a}'_2, \dots, \hat{a}'_N$ [Eq. (12.18)]. Now one can easily see that the first multi-party separability condition is violated for any nonzero squeezing $r_1 > 0$ or $r_2 > 0$, because application of an inverse

N -splitter means

$$\begin{aligned} (\hat{a}_1'' \quad \hat{a}_2'' \quad \cdots \quad \hat{a}_N'')^T &= \mathcal{U}^\dagger(N) (\hat{a}_1' \quad \hat{a}_2' \quad \cdots \quad \hat{a}_N')^T \quad (12.43) \\ &= \mathcal{U}^\dagger(N) \mathcal{U}(N) (\hat{a}_1 \quad \hat{a}_2 \quad \cdots \quad \hat{a}_N)^T, \end{aligned}$$

with $\hat{a}_1, \hat{a}_2, \dots, \hat{a}_N$ from Eq. (12.19). Since $\mathcal{U}^\dagger(N)\mathcal{U}(N) = I$ (identity matrix), the squeezed quadratures of Eq. (12.20) can be directly inserted into Eq. (12.36) yielding a violation of $(e^{-2r_1} + e^{-2r_2})/4 \geq 1/2$ for any $r_1 > 0$ or $r_2 > 0$. Alternatively, using Eq. (12.21), the criterion in Eq. (12.37) becomes

$$\binom{N}{2} \frac{e^{-2r_2}}{2(N-1)} + \frac{Ne^{-2r_1}}{4} = \frac{N}{4} (e^{-2r_1} + e^{-2r_2}) \geq \frac{N}{2}. \quad (12.44)$$

This condition is also violated for any $r_1 > 0$ or $r_2 > 0$. Due to their purity and total symmetry we conclude that the members of the family of states which emerge from the N -splitter circuit are genuinely multi-party entangled for any $r_1 > 0$ or $r_2 > 0$. This applies in particular to the case where $r_1 > 0$ and $r_2 = 0$, i.e., when only *one* squeezed light mode is required for the creation of genuine multipartite entanglement.

Independent of the inequalities Eq. (12.36) and Eq. (12.37), there are also other ways to see that these particular states are genuinely multi-party entangled. One simply has to find some form of entanglement in these states. For example, by tracing out modes 2 through N of the pure N -mode state given in Eq. (12.18), one finds that the remaining one-mode state is mixed, provided $r_1 > 0$ or $r_2 > 0$ [28]. Thus, the pure N -mode state is somehow entangled and hence genuinely multi-party entangled due to its complete symmetry. Note that in order to infer even only partial entanglement via tracing out parties, the N -mode state here has to be pure. In contrast, the multi-party inseparability criteria of section 2.4 may verify partial inseparability for any N -mode state.

From a conceptual point of view, it is very illuminating to analyze which states of the above family of N -mode states can be transformed into each other via local squeezing operations [29]. For example, by applying local squeezers with squeezing s_1 and s_2 to the two modes of the bipartite state generated with only one squeezer [Eq. (12.20) for $N = 2$ with $r_2 = 0$], we obtain

$$\begin{aligned} \hat{x}_1'' &= e^{-s_1} \hat{x}_1' = (e^{+r_1-s_1} \hat{x}_1^{(0)} + e^{-s_1} \hat{x}_2^{(0)})/\sqrt{2}, \\ \hat{p}_1'' &= e^{+s_1} \hat{p}_1' = (e^{+s_1-r_1} \hat{p}_1^{(0)} + e^{+s_1} \hat{p}_2^{(0)})/\sqrt{2}, \\ \hat{x}_2'' &= e^{-s_2} \hat{x}_2' = (e^{+r_1-s_2} \hat{x}_1^{(0)} - e^{-s_2} \hat{x}_2^{(0)})/\sqrt{2}, \\ \hat{p}_2'' &= e^{+s_2} \hat{p}_2' = (e^{+s_2-r_1} \hat{p}_1^{(0)} - e^{+s_2} \hat{p}_2^{(0)})/\sqrt{2}. \end{aligned} \quad (12.45)$$

With the choice of $s_1 = s_2 = r_1/2 \equiv r$, the state in Eq. (12.45) is identical to a two-mode squeezed state built from two equally squeezed states [Eq. (12.20)]

for $N = 2$ with $r_1 \equiv r$, $r_2 \equiv r$. The latter and the state produced with only one squeezer [Eq. (12.20) with $r_1 = 2r$ and $r_2 = 0$] are equivalent under local squeezing operations. This means that Alice and Bob sharing the state produced with one squeezer $r_1 = 2r$ have access to the same amount of entanglement as in the “canonical” two-mode squeezed state with squeezing $r = r_1/2$, $E_{\text{v.N.}} = [\cosh(r_1/2)]^2 \log[\cosh(r_1/2)]^2 - [\sinh(r_1/2)]^2 \log[\sinh(r_1/2)]^2$ [30]. For a given amount of entanglement, however, the canonical two-mode squeezed vacuum state has the least mean photon number. Conversely, for a given mean energy, the canonical two-mode squeezed vacuum state contains the maximum amount of entanglement possible.

Similar arguments apply to the states of more than two modes. From the family of N -mode states, the state with the least mean photon number is determined by the relation

$$e^{\pm 2r_1} = (N - 1) \sinh 2r_2 \left[\sqrt{1 + \frac{1}{(N - 1)^2 \sinh^2 2r_2}} \pm 1 \right]. \quad (12.46)$$

This relation is obtained by requiring each mode of the N -mode states to be symmetric or “unbiased” in the x and p variances [29]. Only for $N = 2$, we obtain $r_1 = r_2$. Otherwise, the first squeezer with r_1 and the $N - 1$ remaining squeezers with r_2 have different squeezing. In the limit of large squeezing, we may use $\sinh 2r_2 \approx e^{+2r_2}/2$ and approximate e^{+2r_1} of Eq. (12.46) by

$$e^{+2r_1} \approx (N - 1)e^{+2r_2}. \quad (12.47)$$

We see that in order to produce the minimum-energy N -mode state, the single r_1 -squeezer is, in terms of the squeezing factor, $N - 1$ times as much squeezed as each r_2 -squeezer. However, also in this general N -mode case, the other N -mode states of the family can be converted into the minimum-energy states via local squeezing operations. This applies in particular to the N -mode states produced with just a single squeezer and to those built from N equally squeezed states. As a result, due to the equivalence under local entanglement-preserving operations, with a single sufficiently squeezed state and beam splitters, arbitrarily many genuinely multi-party entangled modes can be created just as well as with N squeezers and beam splitters.

In contrast to the three-mode state given by Eq. (12.40), the output states of the N -splitter are totally symmetric under interchange of parties. This becomes more transparent when we look at the states in the Wigner representation. For simplicity, let us assume $r = r_1 = r_2$. The position-squeezed input states of the N -splitter circuit, for instance, have the Wigner function

$$W(x, p) = \frac{2}{\pi} \exp(-2e^{+2r} x^2 - 2e^{-2r} p^2). \quad (12.48)$$

Through the linear N -splitter operation, the total input Wigner function to the N -splitter (one momentum-squeezed and $N - 1$ position-squeezed vacuum modes),

$$\begin{aligned} W_{\text{in}}(\mathbf{x}, \mathbf{p}) = & \left(\frac{2}{\pi} \right)^N \exp(-2e^{-2r}x_1^2 - 2e^{+2r}p_1^2) \\ & \times \exp(-2e^{+2r}x_2^2 - 2e^{-2r}p_2^2) \\ & \times \exp(-2e^{+2r}x_3^2 - 2e^{-2r}p_3^2) \\ & \times \cdots \times \exp(-2e^{+2r}x_N^2 - 2e^{-2r}p_N^2), \end{aligned} \quad (12.49)$$

is transformed into the output Wigner function

$$\begin{aligned} W_{\text{out}}(\mathbf{x}, \mathbf{p}) = & \left(\frac{2}{\pi} \right)^N \\ & \times \exp \left\{ -e^{-2r} \left[\frac{2}{N} \left(\sum_{i=1}^N x_i \right)^2 + \frac{1}{N} \sum_{i,j}^N (p_i - p_j)^2 \right] \right. \\ & \left. - e^{+2r} \left[\frac{2}{N} \left(\sum_{i=1}^N p_i \right)^2 + \frac{1}{N} \sum_{i,j}^N (x_i - x_j)^2 \right] \right\}. \end{aligned} \quad (12.50)$$

Here we have used $\mathbf{x} = (x_1, x_2, \dots, x_N)$ and $\mathbf{p} = (p_1, p_2, \dots, p_N)$. The pure-state Wigner function $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ is always positive, *symmetric* among the N modes, and becomes peaked at $x_i - x_j = 0$ ($i, j = 1, 2, \dots, N$) and $p_1 + p_2 + \dots + p_N = 0$ for large squeezing r . For $N = 2$, it exactly equals the well-known two-mode squeezed vacuum state Wigner function [13], which is proportional to $\delta(x_1 - x_2)\delta(p_1 + p_2)$ in the limit of infinite squeezing. As discussed previously, the state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ is genuinely N -partite entangled for any squeezing $r > 0$. The quantum nature of the cross correlations $x_i x_j$ and $p_i p_j$ appearing in $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ for any $r > 0$ is also confirmed by the purity of this state. This purity is guaranteed, since beam splitters turn pure states into pure states (it can also be checked via the correlation matrix of the Gaussian state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ [28]).

A nice example for a multi-party entangled state which is not a member of the above family of states and not totally symmetric with respect to all its modes is the $(M + 1)$ -mode state described by the Wigner function

$$\begin{aligned}
W_{\text{MQC}}(\mathbf{x}, \mathbf{p}) = & \left(\frac{2}{\pi} \right)^{M+1} \exp \left\{ -2e^{-2r_1} \left(\sin \theta_0 x_1 + \frac{\cos \theta_0}{\sqrt{M}} \sum_{i=2}^{M+1} x_i \right)^2 \right. \\
& -2e^{+2r_1} \left(\sin \theta_0 p_1 + \frac{\cos \theta_0}{\sqrt{M}} \sum_{i=2}^{M+1} p_i \right)^2 \\
& -2e^{+2r_2} \left(\cos \theta_0 x_1 - \frac{\sin \theta_0}{\sqrt{M}} \sum_{i=2}^{M+1} x_i \right)^2 \\
& -2e^{-2r_2} \left(\cos \theta_0 p_1 - \frac{\sin \theta_0}{\sqrt{M}} \sum_{i=2}^{M+1} p_i \right)^2 \\
& \left. -\frac{1}{M} \sum_{i,j=2}^{M+1} [(x_i - x_j)^2 + (p_i - p_j)^2] \right\},
\end{aligned} \tag{12.51}$$

where $\mathbf{x} = (x_1, x_2, \dots, x_{M+1})$, $\mathbf{p} = (p_1, p_2, \dots, p_{M+1})$, and

$$\begin{aligned}
\frac{1}{\sqrt{M+1}} \leq \sin \theta_0 \leq \sqrt{\frac{M}{M+1}}, \\
e^{-2r_1} \equiv \frac{\sqrt{M} \sin \theta_0 - \cos \theta_0}{\sqrt{M} \sin \theta_0 + \cos \theta_0}, \quad e^{-2r_2} \equiv \frac{\sqrt{M} \cos \theta_0 - \sin \theta_0}{\sqrt{M} \cos \theta_0 + \sin \theta_0}.
\end{aligned} \tag{12.52}$$

The significance of this $(M+1)$ -mode state is that it represents a kind of multiuser quantum channel (“MQC”) enabling optimal $1 \rightarrow M$ “telecloning” of arbitrary coherent states from one sender to M receivers [31]. Though not completely symmetric with respect to all $M+1$ modes (but to modes 2 through $M+1$), it is a pure Gaussian state which is indeed genuinely multi-party entangled. This can be seen, because none of the modes can be factored out of the total Wigner function. Despite its “asymmetry”, this state is not only partially multi-party entangled as is the asymmetric pure three-mode state given by Eq. (12.40). Of course, the bipartite entanglement between mode 1 on one side and modes 2 through $M+1$ on the other side is the most important property of $W_{\text{MQC}}(\mathbf{x}, \mathbf{p})$ in order to be useful for $1 \rightarrow M$ telecloning [31].

The generation of the state $W_{\text{MQC}}(\mathbf{x}, \mathbf{p})$ is very similar to that of the above family of multi-party entangled states produced with an N -splitter: first make a bipartite entangled state by combining two squeezed vacua, one squeezed in p with r_1 and the other one squeezed in x with r_2 , at a phase-free beam splitter with reflectivity/transmittance parameter $\theta = \theta_0$. Then keep one half (the mode 1) and send the other half together with $M-1$ vacuum modes through an

M -splitter. The annihilation operators of the initial modes \hat{a}_j before the beam splitters, $j = 1, 2, \dots, M + 1$, are then given by

$$\begin{aligned}\hat{a}_1 &= \cosh r_1 \hat{a}_1^{(0)} + \sinh r_1 \hat{a}_1^{(0)\dagger}, \\ \hat{a}_2 &= \cosh r_2 \hat{a}_2^{(0)} - \sinh r_2 \hat{a}_2^{(0)\dagger}, \\ \hat{a}_i &= \hat{a}_i^{(0)},\end{aligned}\quad (12.53)$$

where $i = 3, 4, \dots, M + 1$.

By using the ideal phase-free beam splitter operation from Eq. (12.16), with $B_{kl}(\theta)$ this time representing an $(M + 1)$ -dimensional identity matrix with the entries I_{kk} , I_{kl} , I_{lk} , and I_{ll} replaced by the corresponding entries of the beam splitter matrix in Eq. (12.16), the MQC-generating circuit can be written as

$$(\hat{b}_1 \quad \hat{b}_2 \quad \cdots \quad \hat{b}_{M+1})^T = \mathcal{U}_{MQC}(M + 1) (\hat{a}_1 \quad \hat{a}_2 \quad \cdots \quad \hat{a}_{M+1})^T, \quad (12.54)$$

with

$$\begin{aligned}\mathcal{U}_{MQC}(M + 1) &\equiv B_{M M+1} \left(\sin^{-1} \frac{1}{\sqrt{2}} \right) B_{M-1 M} \left(\sin^{-1} \frac{1}{\sqrt{3}} \right) \\ &\times \cdots \times B_{34} \left(\sin^{-1} \frac{1}{\sqrt{M-1}} \right) B_{23} \left(\sin^{-1} \frac{1}{\sqrt{M}} \right) \\ &\times B_{12}(\theta_0).\end{aligned}\quad (12.55)$$

The first beam splitter, acting on modes \hat{a}_1 and \hat{a}_2 , has reflectivity/transmittance parameter $\theta \equiv \theta_0$. The remaining beam splitters represent an M -splitter. In Eq. (12.54), the output modes \hat{b}_j correspond to the $M + 1$ modes of the MQC state described by W_{MQC} in Eq. (12.51). Let us now return to the totally symmetric multipartite entangled states given by Eq. (12.18) and explore some of their properties. For simplicity, we will thereby focus on those states emerging from the N -splitter circuit which are created with input states equally squeezed in momentum and position, $r = r_1 = r_2$.

2.5.3 Nonlocality and other properties. In this paragraph, we will discuss some of the properties of the state $W_{out}(\mathbf{x}, \mathbf{p})$ in Eq. (12.50). This will further illustrate the character of $W_{out}(\mathbf{x}, \mathbf{p})$ as a nonmaximally entangled multi-party state. One such property is that this state, despite having an always positive Wigner function, violates N -party Bell-type [2] (or Mermin-type [32]) inequalities imposed by local realism for any squeezing $r > 0$ [33]. The observables producing these violations are displaced photon-number parities rather than continuous variables such as x and p [34]. Like for the qubit states [32], the violations increase as the number of parties N grows. However, this

increase becomes steadily smaller for larger N , as opposed to the exponential increase for the maximally entangled qubit GHZ states [32]. This discrepancy may be explained by the fact that the violations are exposed only for finite squeezing where the state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ is a *nonmaximally* entangled multi-party state [33]. Note that, in general, the violations of N -party inequalities imposed by local realism do not necessarily imply the presence of genuine multipartite entanglement. However, for the pure and symmetric states $W_{\text{out}}(\mathbf{x}, \mathbf{p})$, once again, proving some kind of entanglement means proving genuine multipartite entanglement.

In order to prove the nonlocality exhibited by the state $W(\mathbf{x}, \mathbf{p}) \equiv W_{\text{out}}(\mathbf{x}, \mathbf{p})$, let us now use the fact that the Wigner function is proportional to the quantum expectation value of a displaced parity operator [35, 34]:

$$W(\boldsymbol{\alpha}) = \left(\frac{2}{\pi}\right)^N \langle \hat{\Pi}(\boldsymbol{\alpha}) \rangle = \left(\frac{2}{\pi}\right)^N \Pi(\boldsymbol{\alpha}), \quad (12.56)$$

where $\boldsymbol{\alpha} = \mathbf{x} + i\mathbf{p} = (\alpha_1, \alpha_2, \dots, \alpha_N)$ and $\Pi(\boldsymbol{\alpha})$ is the quantum expectation value of the operator

$$\hat{\Pi}(\boldsymbol{\alpha}) = \bigotimes_{i=1}^N \hat{\Pi}_i(\alpha_i) = \bigotimes_{i=1}^N \hat{D}_i(\alpha_i) (-1)^{\hat{n}_i} \hat{D}_i^\dagger(\alpha_i). \quad (12.57)$$

The operator $\hat{D}_i(\alpha_i)$ is the displacement operator,

$$\hat{D}(\alpha) = \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a}), \quad (12.58)$$

acting on mode i . Thus, $\hat{\Pi}(\boldsymbol{\alpha})$ is a product of displaced parity operators given by

$$\hat{\Pi}_i(\alpha_i) = \hat{\Pi}_i^{(+)}(\alpha_i) - \hat{\Pi}_i^{(-)}(\alpha_i), \quad (12.59)$$

with the projection operators

$$\hat{\Pi}_i^{(+)}(\alpha_i) = \hat{D}_i(\alpha_i) \sum_{k=0}^{\infty} |2k\rangle\langle 2k| \hat{D}_i^\dagger(\alpha_i), \quad (12.60)$$

$$\hat{\Pi}_i^{(-)}(\alpha_i) = \hat{D}_i(\alpha_i) \sum_{k=0}^{\infty} |2k+1\rangle\langle 2k+1| \hat{D}_i^\dagger(\alpha_i), \quad (12.61)$$

corresponding to the measurement of an even (parity +1) or an odd (parity -1) number of photons in mode i . This means that each mode is now characterized by a dichotomic variable similar to the spin of a spin-1/2 particle or the single-photon polarization. Different spin or polarizer orientations from the original

qubit based Bell inequality are replaced by different displacements in phase space. This set of two-valued measurements for each setting is just what we need for the nonlocality test.

In the case of N -particle systems, such a nonlocality test is possible using the N -particle generalization of the two-particle Bell-CHSH inequality [16]. This inequality is based on the following recursively defined linear combination of joint measurement results (in this paragraph, the symbol B does not refer to a beam splitter operation),

$$\begin{aligned} B_N &\equiv \frac{1}{2}[\sigma(a_N) + \sigma(a'_N)]B_{N-1} \\ &+ \frac{1}{2}[\sigma(a_N) - \sigma(a'_N)]B'_{N-1} = \pm 2, \end{aligned} \quad (12.62)$$

where $\sigma(a_N) = \pm 1$ and $\sigma(a'_N) = \pm 1$ describe two possible outcomes for two possible measurement settings (denoted by a_N and a'_N) of measurements on the N th particle. Note, the expressions B'_N are equivalent to B_N but with all the a_i and a'_i swapped. Provided that $B_{N-1} = \pm 2$ and $B'_{N-1} = \pm 2$, Equation (12.62) is trivially true for a single run of measurements where $\sigma(a_N)$ is either $+1$ or -1 and similarly for $\sigma(a'_N)$. Induction proves Eq. (12.62) for any N when we take

$$\begin{aligned} B_2 &\equiv [\sigma(a_1) + \sigma(a'_1)]\sigma(a_2) \\ &+ [\sigma(a_1) - \sigma(a'_1)]\sigma(a'_2) = \pm 2. \end{aligned} \quad (12.63)$$

Within the framework of local realistic theories with hidden variables $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_N)$ and the normalized probability distribution $P(\lambda)$, we obtain an inequality for the average value of $B_N \equiv B_N(\lambda)$,

$$\left| \int d\lambda_1 d\lambda_2 \dots d\lambda_N P(\lambda) B_N(\lambda) \right| \leq 2. \quad (12.64)$$

By the linearity of averaging, this is a sum of means of products of the $\sigma(a_i)$ and $\sigma(a'_i)$. For example, if $N = 2$, we obtain the CHSH inequality

$$|C(a_1, a_2) + C(a_1, a'_2) + C(a'_1, a_2) - C(a'_1, a'_2)| \leq 2, \quad (12.65)$$

with the correlation functions

$$C(a_1, a_2) = \int d\lambda_1 d\lambda_2 P(\lambda_1, \lambda_2) \sigma(a_1, \lambda_1) \sigma(a_2, \lambda_2). \quad (12.66)$$

Following Bell [2], an always positive Wigner function can serve as the hidden-variable probability distribution with respect to measurements corresponding to any linear combination of \hat{x} and \hat{p} . In this sense, the finitely squeezed two-mode squeezed state Wigner function could prevent the CHSH inequality from

being violated when restricted to such measurements: $W(x_1, p_1, x_2, p_2) \equiv P(\lambda_1, \lambda_2)$. The same applies to the Wigner function in Eq. (12.50): $W(\mathbf{x}, \mathbf{p}) \equiv P(\boldsymbol{\lambda})$ could be used to construct correlation functions

$$\begin{aligned} C(\mathbf{a}) &= \int d\lambda_1 d\lambda_2 \dots d\lambda_N P(\boldsymbol{\lambda}) \\ &\times \sigma(a_1, \lambda_1) \sigma(a_2, \lambda_2) \dots \sigma(a_N, \lambda_N), \end{aligned} \quad (12.67)$$

where $\mathbf{a} = (a_1, a_2, \dots, a_N)$. However, for parity measurements on each mode with possible results ± 1 for each differing displacement, this would require unbounded δ -functions for the local objective quantities $\sigma(a_i, \lambda_i)$ [34], as in this case we have

$$C(\mathbf{a}) \equiv \Pi(\boldsymbol{\alpha}) = (\pi/2)^N W(\boldsymbol{\alpha}). \quad (12.68)$$

This relation directly relates the correlation function to the Wigner function and is indeed crucial for the nonlocality proof of the continuous-variable states in Eq. (12.50).

Let us begin by analyzing the nonlocal correlations exhibited by the entangled two-party state. For this state, the two-mode squeezed state in Eq. (12.50) with $N = 2$, we may investigate the combination [34]

$$\mathcal{B}_2 = \Pi(0, 0) + \Pi(0, \beta) + \Pi(\alpha, 0) - \Pi(\alpha, \beta), \quad (12.69)$$

which according to Eq. (12.65) satisfies $|\mathcal{B}_2| \leq 2$ for local realistic theories. Here, we have chosen the displacement settings $\alpha_1 = \alpha_2 = 0$ and $\alpha'_1 = \alpha$, $\alpha'_2 = \beta$.

Writing the states in Eq. (12.50) as

$$\begin{aligned} \Pi(\boldsymbol{\alpha}) &= \exp \left\{ -2 \cosh 2r \sum_{i=1}^N |\alpha_i|^2 \right. \\ &\quad \left. + \sinh 2r \left[\frac{2}{N} \sum_{i,j}^N (\alpha_i \alpha_j + \alpha_i^* \alpha_j^*) - \sum_{i=1}^N (\alpha_i^2 + \alpha_i^{*2}) \right] \right\}, \end{aligned} \quad (12.70)$$

for $N = 2$ and $\alpha = \beta = i\sqrt{\mathcal{J}}$ with the real displacement parameter $\mathcal{J} \geq 0$ ⁷, we obtain $\mathcal{B}_2 = 1 + 2 \exp(-2\mathcal{J} \cosh 2r) - \exp(-4\mathcal{J} e^{+2r})$. In the limit of large r (so $\cosh 2r \approx e^{+2r}/2$) and small \mathcal{J} , \mathcal{B}_2 is maximized for $\mathcal{J} e^{+2r} = (\ln 2)/3$, yielding $\mathcal{B}_2^{\max} \approx 2.19$ [34], which is a clear violation of the inequality $|\mathcal{B}_2| \leq 2$. Smaller violations also occur for smaller squeezing and larger \mathcal{J} . Indeed, for any nonzero squeezing, some violation takes place [33].

We will now consider more than two parties. Let us first examine the three-mode state by setting $N = 3$ in Eq. (12.50). According to the inequality of the

correlation functions derived from Eq. (12.62)-(12.64), we have

$$|C(a_1, a_2, a'_3) + C(a_1, a'_2, a_3) + C(a'_1, a_2, a_3) - C(a'_1, a'_2, a'_3)| \leq 2 . \quad (12.71)$$

Thus, for the combination

$$\mathcal{B}_3 = \Pi(0, 0, \gamma) + \Pi(0, \beta, 0) + \Pi(\alpha, 0, 0) - \Pi(\alpha, \beta, \gamma), \quad (12.72)$$

a contradiction to local realism is demonstrated by $|\mathcal{B}_3| > 2$. The corresponding settings here are $\alpha_1 = \alpha_2 = \alpha_3 = 0$ and $\alpha'_1 = \alpha, \alpha'_2 = \beta, \alpha'_3 = \gamma$. With the choice $\alpha = \sqrt{\mathcal{J}}e^{i\phi_1}, \beta = \sqrt{\mathcal{J}}e^{i\phi_2}$, and $\gamma = \sqrt{\mathcal{J}}e^{i\phi_3}$, we obtain

$$\begin{aligned} \mathcal{B}_3 &= \sum_{i=1}^3 \exp(-2\mathcal{J} \cosh 2r - \frac{2}{3}\mathcal{J} \sinh 2r \cos 2\phi_i) \\ &- \exp \left\{ -6\mathcal{J} \cosh 2r - \frac{1}{3}\mathcal{J} \sinh 2r \sum_{i \neq j}^3 [\cos 2\phi_i - 4 \cos(\phi_i + \phi_j)] \right\}. \end{aligned} \quad (12.73)$$

Apparently, because of the symmetry of the entangled three-mode state, equal phases ϕ_i should also be chosen in order to maximize \mathcal{B}_3 . The best choice is $\phi_1 = \phi_2 = \phi_3 = \pi/2$, which ensures that the positive terms in Eq. (12.73) become maximal and the contribution of the negative term minimal. Therefore, we again use equal settings $\alpha = \beta = \gamma = i\sqrt{\mathcal{J}}$ and obtain

$$\mathcal{B}_3 = 3 \exp(-2\mathcal{J} \cosh 2r + 2\mathcal{J} \sinh 2r/3) - \exp(-6\mathcal{J} e^{+2r}) . \quad (12.74)$$

The violations of $|\mathcal{B}_3| \leq 2$ that occur with this result are similar to the violations of $|\mathcal{B}_2| \leq 2$ obtained for the two-mode state, but the $N = 3$ violations are even more significant than the $N = 2$ violations [33]. In the limit of large r (and small \mathcal{J}), we may use $\cosh 2r \approx \sinh 2r \approx e^{+2r}/2$ in Eq. (12.74). Then \mathcal{B}_3 is maximized for $\mathcal{J} e^{+2r} = 3(\ln 3)/16$: $\mathcal{B}_3^{\max} \approx 2.32$. This optimal choice requires smaller displacements \mathcal{J} than those of the $N = 2$ case for the same squeezing.

Let us now investigate the cases $N = 4$ and $N = 5$. From Eq. (12.62)-(12.64) with $N = 4$, the following inequality for the correlation functions can be derived:

$$\begin{aligned} &\frac{1}{2} |C(a_1, a_2, a_3, a'_4) + C(a_1, a_2, a'_3, a_4) + C(a_1, a'_2, a_3, a_4) \\ &+ C(a'_1, a_2, a_3, a_4) + C(a_1, a_2, a'_3, a'_4) + C(a_1, a'_2, a_3, a'_4) \\ &+ C(a'_1, a_2, a_3, a'_4) + C(a_1, a'_2, a'_3, a_4) + C(a'_1, a_2, a'_3, a_4) \\ &+ C(a'_1, a'_2, a_3, a_4) - C(a'_1, a'_2, a'_3, a_4) - C(a'_1, a'_2, a_3, a'_4) \\ &- C(a'_1, a_2, a'_3, a'_4) - C(a_1, a'_2, a'_3, a'_4) - C(a_1, a_2, a_3, a_4) \\ &- C(a'_1, a'_2, a'_3, a'_4)| \leq 2 . \end{aligned} \quad (12.75)$$

It is symmetric among all four parties as any inequality derived from Eq. (12.62)-(12.64) is symmetric among all parties. For the settings $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0$ and $\alpha'_1 = \alpha, \alpha'_2 = \beta, \alpha'_3 = \gamma, \alpha'_4 = \delta$, complying with local realism means $|\mathcal{B}_4| \leq 2$ where

$$\begin{aligned} \mathcal{B}_4 = & \frac{1}{2} [\Pi(0, 0, 0, \delta) + \Pi(0, 0, \gamma, 0) + \Pi(0, \beta, 0, 0) \\ & + \Pi(\alpha, 0, 0, 0) + \Pi(0, 0, \gamma, \delta) + \Pi(0, \beta, 0, \delta) \\ & + \Pi(\alpha, 0, 0, \delta) + \Pi(0, \beta, \gamma, 0) + \Pi(\alpha, 0, \gamma, 0) \\ & + \Pi(\alpha, \beta, 0, 0) - \Pi(\alpha, \beta, \gamma, 0) - \Pi(\alpha, \beta, 0, \delta) \\ & - \Pi(\alpha, 0, \gamma, \delta) - \Pi(0, \beta, \gamma, \delta) - \Pi(0, 0, 0, 0) \\ & - \Pi(\alpha, \beta, \gamma, \delta)] . \end{aligned} \quad (12.76)$$

Similarly, for $N = 5$ one finds

$$\begin{aligned} \mathcal{B}_5 = & \frac{1}{2} [\Pi(0, 0, 0, \delta, \epsilon) + \Pi(0, 0, \gamma, 0, \epsilon) + \Pi(0, \beta, 0, 0, \epsilon) \\ & + \Pi(\alpha, 0, 0, 0, \epsilon) + \Pi(0, 0, \gamma, \delta, 0) + \Pi(0, \beta, 0, \delta, 0) \\ & + \Pi(\alpha, 0, 0, \delta, 0) + \Pi(0, \beta, \gamma, 0, 0) + \Pi(\alpha, 0, \gamma, 0, 0) \\ & + \Pi(\alpha, \beta, 0, 0, 0) - \Pi(\alpha, \beta, \gamma, \delta, 0) - \Pi(\alpha, \beta, \gamma, 0, \epsilon) \\ & - \Pi(\alpha, \beta, 0, \delta, \epsilon) - \Pi(\alpha, 0, \gamma, \delta, \epsilon) - \Pi(0, \beta, \gamma, \delta, \epsilon) \\ & - \Pi(0, 0, 0, 0, 0)] , \end{aligned} \quad (12.77)$$

which has to satisfy $|\mathcal{B}_5| \leq 2$ and contains the same settings as for $N = 4$, but in addition we have chosen $\alpha_5 = 0$ and $\alpha'_5 = \epsilon$.

We can now use the entangled states of Eq. (12.70) with $N = 4$ and $N = 5$ and apply the inequalities to them. For the same reason as for $N = 3$ (symmetry among all modes in the states and in the inequalities), the choice $\alpha = \beta = \gamma = \delta = \epsilon = i\sqrt{\mathcal{J}}$ appears to be optimal (maximizes positive terms and minimizes negative contributions).

With this choice, we obtain

$$\begin{aligned} \mathcal{B}_4 = & 2 \exp(-2\mathcal{J} \cosh 2r + \mathcal{J} \sinh 2r) \\ & - 2 \exp(-6\mathcal{J} \cosh 2r - 3\mathcal{J} \sinh 2r) \\ & + 3 \exp(-4\mathcal{J} \cosh 2r) - \frac{1}{2} \exp(-8\mathcal{J} e^{+2r}) - \frac{1}{2} , \\ \mathcal{B}_5 = & 5 \exp(-4\mathcal{J} \cosh 2r + 4\mathcal{J} \sinh 2r/5) \\ & - \frac{5}{2} \exp(-8\mathcal{J} \cosh 2r - 24\mathcal{J} \sinh 2r/5) - \frac{1}{2} . \end{aligned} \quad (12.78)$$

Apparently, the maximum violation of $|\mathcal{B}_N| \leq 2$ (for our particular choice of settings) grows with increasing number of parties N [33]. The asymptotic

analysis (large r and small \mathcal{J}) yields, for instance, for $N = 5$: $\mathcal{B}_5^{\max} \approx 2.48$ with $\mathcal{J}e^{+2r} = 5(\ln 2)/24$. For a given amount of squeezing, smaller displacements \mathcal{J} than those for $N \leq 4$ (at the same squeezing) are needed to approach this maximum violation. Another interesting observation is that in all four cases ($N = 2, 3, 4, 5$), violations occur for any nonzero squeezing [33]. This implies the presence of N -partite entanglement for any nonzero squeezing. Moreover, also for modest finite squeezing, the size of the violations (at optimal displacement \mathcal{J}) grows with increasing N [33].

Larger numbers of parties $N > 5$ were also considered in Ref. [33]. The degree of nonlocality of the continuous-variable states, if represented by the maximum violation of the corresponding Bell-type inequalities, seems to grow with an increasing number of parties. This growth, however, decelerates for larger numbers of parties. Thus, the ‘evolution’ of the continuous-variable states’ nonlocality with an increasing number of parties and the corresponding ‘evolution’ of nonlocality for the qubit GHZ states are qualitatively similar but quantitatively different with an exponential increase for the qubits. The reason for this may be that the qubit GHZ states are maximally entangled, whereas the continuous-variable states are nonmaximally entangled for any finite squeezing. Similarly, the N -party version of the nonmaximally entangled qubit state $|W\rangle$ yields a non-exponential increase of the maximum violations (by employing, for example, an analysis analogous to that here [36]). Note that the observation of the nonlocality of the continuous-variable states here requires small but nonzero displacements $\mathcal{J} \propto e^{-2r}$, which is not achievable when the singular maximally entangled states for infinite squeezing are considered.

Finally, the “unbiased” minimum-energy states of the family of entangled N -mode states might yield larger violations. These states are not produced with N equal squeezers (as those states whose nonlocality we have analyzed here), but with one r_1 -squeezer and $N - 1$ r_2 - squeezers related as in Eq. (12.46). With growing N , the unbiased states increasingly differ from the states that we have used for the nonlocality test [see Eq. (12.47) for large squeezing]. On the other hand, the biased and the unbiased states are equivalent under local squeezing operations and thus cannot differ in their potential nonlocality. In addition, this equivalence shows that also the unbiased states are only nonmaximally entangled for finite squeezing, which suggests that they also do not lead to an exponential increase of the violations as for the qubit GHZ states.

In section 2.1, we discussed some properties of pure, fully entangled states of three qubits. An important feature of these states is that a distinction can be made between two inequivalent classes: states from the first class can be converted into the state $|\text{GHZ}\rangle$ via SLOCC, but not into the state $|W\rangle$ (not even with arbitrarily small probability). For the second class, exactly the opposite holds. In several senses, the representative $|\text{GHZ}\rangle$ of the former class would be best described as a maximally entangled state, whereas the representative $|W\rangle$

of the latter class is nonmaximally entangled. A distinct feature of the maximum entanglement of $|GHZ\rangle$ is that after tracing out one qubit, the remaining qubit pair is in a separable mixed state⁸. Apparently, the entanglement of $|GHZ\rangle$ heavily relies on all three parties. By contrast, the entanglement of the state $|W\rangle$ is robust to some extent against disposal of one qubit. When tracing out one qubit of $|W\rangle$, the remaining pair shares a mixed entangled state. In the continuous-variable setting, we can make analogous observations. By interpreting the state $\int dx |x, x, x\rangle$ as the analogue of $|GHZ\rangle$, we see that

$$\text{Tr}_1 \int dx dx' |x, x, x\rangle \langle x', x', x'| = \int dx |x\rangle_{22} \langle x| \otimes |x\rangle_{33} \langle x| , \quad (12.79)$$

which is clearly a separable mixed state (and indeed not the maximally mixed state $\propto \int dx dx' |x, x'\rangle \langle x, x'|$). More interesting is the behaviour of a regularized version of $\int dx |x, x, x\rangle$. In order to apply bipartite inseparability criteria, let us trace out (integrate out) one mode of the Wigner function $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ in Eq. (12.50) for $N = 3$,

$$\begin{aligned} \text{Tr}_1 W_{\text{out}}(\mathbf{x}, \mathbf{p}) &= \int dx_1 dp_1 W_{\text{out}}(\mathbf{x}, \mathbf{p}) \\ &\propto \exp \left[-2e^{+2r} \frac{e^{+2r} + 2e^{-2r}}{e^{-2r} + 2e^{+2r}} (x_2^2 + x_3^2) - 2e^{-2r} \frac{e^{-2r} + 2e^{+2r}}{e^{+2r} + 2e^{-2r}} (p_2^2 + p_3^2) \right. \\ &\quad \left. + 4e^{+2r} \frac{e^{+2r} - e^{-2r}}{e^{-2r} + 2e^{+2r}} x_2 x_3 + 4e^{-2r} \frac{e^{-2r} - e^{+2r}}{e^{+2r} + 2e^{-2r}} p_2 p_3 \right]. \end{aligned} \quad (12.80)$$

From the resulting Gaussian two-mode Wigner function, we can extract the inverse correlation matrix. For Gaussian N -mode states with zero mean values, the Wigner function is given by

$$W(\boldsymbol{\xi}) = \frac{1}{(2\pi)^N \sqrt{\det \mathbf{V}}} \exp \left\{ -\frac{1}{2} \boldsymbol{\xi} \mathbf{V}^{-1} \boldsymbol{\xi}^T \right\} , \quad (12.81)$$

with the $2N$ -dimensional vector $\boldsymbol{\xi}$ having the quadrature pairs of all N modes as its components,

$$\begin{aligned} \boldsymbol{\xi} &= (x_1, p_1, x_2, p_2, \dots, x_N, p_N) , \\ \hat{\boldsymbol{\xi}} &= (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \dots, \hat{x}_N, \hat{p}_N) , \end{aligned} \quad (12.82)$$

and with the $2N \times 2N$ correlation matrix \mathbf{V} having as its elements the second moments (symmetrized according to the Weyl correspondence),

$$\begin{aligned} \text{Tr}[\hat{\rho} (\Delta \hat{\xi}_i \Delta \hat{\xi}_j + \Delta \hat{\xi}_j \Delta \hat{\xi}_i)/2] &= \langle (\hat{\xi}_i \hat{\xi}_j + \hat{\xi}_j \hat{\xi}_i)/2 \rangle \\ &= \int W(\boldsymbol{\xi}) \xi_i \xi_j d^{2N} \xi = V_{ij}, \end{aligned} \quad (12.83)$$

where $\Delta\hat{\xi}_i = \hat{\xi}_i - \langle\hat{\xi}_i\rangle = \hat{\xi}_i$ for zero mean values. The last equality defines the correlation matrix for any quantum state, but for Gaussian states of the form Eq. (12.81), the Wigner function is completely determined by the second-moment correlation matrix. Now we can calculate the bipartite correlation matrix of the state in Eq. (12.80),

$$\mathbf{V} = \frac{1}{12} \begin{pmatrix} e^{+2r} + 2e^{-2r} & 0 & 2 \sinh 2r & 0 \\ 0 & e^{-2r} + 2e^{+2r} & 0 & -2 \sinh 2r \\ 2 \sinh 2r & 0 & e^{+2r} + 2e^{-2r} & 0 \\ 0 & -2 \sinh 2r & 0 & e^{-2r} + 2e^{+2r} \end{pmatrix}. \quad (12.84)$$

We could have also obtained this two-mode correlation matrix by extracting the three-mode correlation matrix \mathbf{V} of the state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ in Eq. (12.50) with $N = 3$ and ignoring all entries involving mode 1 [or equivalently by explicitly calculating the correlations between modes 2 and 3 with the Heisenberg operators in Eq. (12.18) for $r = r_1 = r_2$ and $N = 3$]. The resulting two-mode state is a (mixed) inseparable state for any nonzero squeezing $r > 0$. Note that, for instance, the total variance in Eq. (12.37) with $N = 2$ becomes for this state $(5e^{-2r} + e^{+2r})/6$, which drops below the boundary of 1 only for sufficiently small nonzero squeezing, but approaches infinity as the squeezing increases. However, we can easily verify the state's inseparability for any $r > 0$ by looking at the necessary two-party separability condition in product form given in Ref. [37]. We find that

$$\langle [\Delta(\hat{x}_2 - \hat{x}_3)]^2 \rangle \langle [\Delta(\hat{p}_2 + \hat{p}_3)]^2 \rangle = (2e^{-4r} + 1)/12, \quad (12.85)$$

which drops below the separability boundary of 1/4 for any $r > 0$. Of course, also the necessary and sufficient partial transpose criterion from Ref. [14] indicates entanglement for any $r > 0$ [28]. Recall that by first taking the “infinite-squeezing limit” and then tracing out one mode, we had obtained a separable state [Eq. (12.79)]. That was what we expected according to the result for the maximally entangled qubit state $|GHZ\rangle$.

So after all, we confirm what we had intuitively expected: the tripartite state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ for finite squeezing is a nonmaximally entangled state like the qubit state $|W\rangle$. Only for infinite squeezing does it approach the maximally entangled state $\int dx |x, x, x\rangle$, the analogue of $|GHZ\rangle$. This result reflects what is known for two parties. The two-mode squeezed state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ with $N = 2$ becomes a maximally entangled state $\int dx |x, x\rangle$, such as the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$, only for infinite squeezing. For finite squeezing, it is known to be nonmaximally entangled.

3. CONCLUSIONS

Let us conclude by asking whether we were able to find answers to the questions posed at the beginning of this chapter: how can we generate, measure, and (theoretically and experimentally) verify genuine multipartite entangled states for continuous variables? How do the continuous-variable states compare to their qubit counterparts with respect to various properties?

As for the generation, we demonstrated that genuinely N -party entangled states are producible with squeezed light resources and beam splitters. In particular, one sufficiently squeezed light mode is in principle the only resource needed to create any degree of genuine multi-party entanglement by means of linear optics. The resulting states, though genuinely multi-party entangled, are always nonmaximally entangled multi-party states due to the finite amount of the squeezing. They behave like the N -party versions of the qubit state $|W\rangle$. First, they also contain bipartite entanglement readily available between any pair of modes (just as $|W\rangle$ and as opposed to the qubit state $|GHZ\rangle$). Secondly, they yield a non-exponential increase of violations of multi-party Bell-type inequalities for growing number of parties (as for $|W\rangle$ and different from the qubit state $|GHZ\rangle$ for which the increase is exponential).

Furthermore, we have seen that by inverting the circuits for generating genuine but nonmaximum multi-party entanglement, one can perform projection measurements onto the maximally entangled multi-party (GHZ) basis for continuous variables. In contrast to the difficulties in performing such measurements for photonic qubits within the framework of linear optics, continuous-variable GHZ measurements only require beam splitters and homodyne detectors. In addition, we showed that the circuits for measuring maximum GHZ entanglement are also applicable to the theoretical and experimental verification of the nonmaximum entanglement of the multi-party states (which are those producible in the laboratory). The circuits provide a necessary condition for full separability of any N -partite N -mode state (pure or mixed, Gaussian or non-Gaussian) with any number of modes N . However, this condition is not sufficient for full separability and, more importantly, its violation does not verify genuine but only partial multipartite entanglement. For the theoretical verification of genuine multipartite entanglement, additional assumptions have to be taken into account such as the total symmetry of the relevant states. Therefore, an unambiguous experimental proof of genuine multipartite entanglement of continuous-variable states was not proposed in this chapter. A possible approach to this would be to consider the violation of stricter N -party Bell-type inequalities which cannot be violated by only partially entangled states. However, the experimental nonlocality test would then rely on observables such as the photon number parity, and hence become unfeasible with current technol-

ogy. More desirable would be a test for genuine multipartite entanglement that is solely based on linear optics and efficient homodyne detections.

Notes

1. Separable states also exhibit correlations, but those are purely classical. For instance, compare the separable state $\hat{\rho} = \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|)$ to the pure maximally entangled “Bell state” $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle)$ with the conjugate basis states $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The separable state $\hat{\rho}$ is classically correlated only with respect to the predetermined basis $\{|0\rangle, |1\rangle\}$. However, the Bell state $|\Phi^+\rangle$ is a priori quantum correlated in both bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, and may become a posteriori classically correlated depending on the particular basis choice in a local measurement. Similarly, we will see later that the inseparability criteria for continuous variables need to be expressed in terms of the positions and their conjugate momenta.

2. Inseparable states with positive partial transpose cannot be distilled to a maximally entangled state via local operations and classical communication. They are so-called “bound entangled” [8]. The converse, however, does not hold. An explicit example of a bound entangled state with negative partial transpose was given in Ref. [9]. In other words, not all entangled states that reveal their inseparability through negative partial transpose are distillable or “free entangled”. On the other hand, any state $\hat{\rho}_{12}$ that violates the so-called reduction criterion, $\hat{\rho}_1 \otimes \hat{1} - \hat{\rho}_{12} \geq 0$ or $\hat{1} \otimes \hat{\rho}_2 - \hat{\rho}_{12} \geq 0$, is both inseparable and distillable [10]. This reduction criterion is in general weaker than the partial transpose criterion and the two criteria are equivalent in the (2×2) - and (2×3) -dimensional cases.

3. A possible continuous-variable generalization of the C-NOT gate is $|x_1, x_2\rangle \rightarrow |x_1, x_1 + x_2\rangle$, where the addition modulo two of the qubit C-NOT, $|y_1, y_2\rangle \rightarrow |y_1, y_1 \oplus y_2\rangle$ with $y_1, y_2 = 0, 1$, has been replaced by the normal addition. However, for the quantum circuit here, a beam splitter operation as described by Eq. (12.14) is a suitable substitute for the generalized C-NOT gate.

4. A full classification of tripartite Gaussian states is given in Ref. [27] in analogy to that for qubits from Ref. [18]. In addition, necessary and sufficient three-mode inseparability criteria for Gaussian states are proposed in Ref. [27].

5. The variances of the $N - 1$ relative positions $\hat{x}_1 - \hat{x}_2$, $\hat{x}_2 - \hat{x}_3$, ..., and $\hat{x}_{N-1} - \hat{x}_N$ are also available via the variances of the output quadratures of the inverse N -splitter. First, the variance of $\hat{x}'_N = \frac{1}{\sqrt{2}}(\hat{x}_{N-1} - \hat{x}_N)$ corresponding to the last line in Eq. (12.30) is directly measurable. In addition, by converting the measured photocurrent into a light amplitude and “displacing” (feed-forward) \hat{x}'_{N-1} according to $\hat{x}'_{N-1} \rightarrow \hat{x}''_{N-1} = \hat{x}'_{N-1} - \frac{1}{\sqrt{3}}\hat{x}'_N = \sqrt{\frac{2}{3}}(\hat{x}_{N-2} - \hat{x}_{N-1})$, one can directly measure the variance of $\hat{x}_{N-2} - \hat{x}_{N-1}$ etc. Similarly, one would also employ this feed-forward technique in a multi-party quantum communication protocol that relies on the N classical results of an N -mode GHZ state measurement.

6. note that we use the term “partially entangled” here for states which are not genuinely multi-party inseparable. In the literature, sometimes “partial entanglement” is also referred to as nonmaximum entanglement of two or more parties (in the sense that for two parties the Schmidt coefficients are not all equal). As discussed later, also the genuinely multi-party entangled continuous-variable states are only nonmaximally entangled due to the finite degree of the squeezing.

7. This choice of two equal settings leads to the same result as that of Banaszek and Wodkiewicz [34] who used opposite signs: $\alpha = \sqrt{\mathcal{J}}$ and $\beta = -\sqrt{\mathcal{J}}$.

8. However, remember that this is not the maximally mixed state for two qubits. Only when tracing out two parties do we end up having the maximally mixed one-qubit state.

References

- [1] E. Schmidt, Math. Annalen **63**, 433 (1906).
- [2] J. S. Bell, Physics (N.Y.) **1**, 195 (1964).
- [3] C. H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996).

- [4] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).
- [5] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [6] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
- [8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
- [9] D. P. DiVincenzo *et al.*, Phys. Rev. A **61**, 062312 (2000).
- [10] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
- [11] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **210**, 377 (1996).
- [12] M. A. Nielsen and J. Kempe, Phys. Rev. Lett. **86**, 5184 (2001).
- [13] D. F. Walls and G. J. Milburn, *Quantum Optics*, Springer Verlag Berlin Heidelberg New York (1994).
- [14] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
- [15] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
- [16] D. N. Klyshko, Phys. Lett. A **172**, 399 (1993); N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).
- [17] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
- [18] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
- [19] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000).
- [20] M. Dušek, Los Alamos arXive quant-ph/0107119 (2001).
- [21] E. Knill, R. Laflamme, and G. J. Milburn, Nature **409**, 46 (2001).
- [22] A. Furusawa *et al.*, Science **282**, 706 (1998).
- [23] D. Bouwmeester *et al.*, Phys. Rev. Lett. **82**, 1345 (1999).
- [24] D. Boschi *et al.*, Phys. Rev. Lett. **80**, 1121 (1998).
- [25] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).
- [26] L.-M. Duan *et al.*, Phys. Rev. Lett. **84**, 2722 (2000).
- [27] G. Giedke *et al.*, Phys. Rev. A **64**, 052303 (2001).
- [28] P. van Loock, Fortschr. d. Phys., to appear.
- [29] W. P. Bowen, P. K. Lam, and T. C. Ralph, Los Alamos arXive quant-ph/0104108 (2001).
- [30] S. J. van Enk, Phys. Rev. A **60**, 5059 (1999).
- [31] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **87**, 247901 (2001).
- [32] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
- [33] P. van Loock and S. L. Braunstein, Phys. Rev. A **63**, 022106 (2001).

- [34] K. Banaszek and K. Wodkiewicz, Phys. Rev. A **58**, 4345 (1998).
- [35] A. Royer, Phys. Rev. A **15**, 449 (1977); H. Moya-Cessa and P. L. Knight, Phys. Rev. A **48**, 2479 (1993).
- [36] G. Li *et al.*, J. of Mod. Opt. **49**, 237 (2002).
- [37] S. M. Tan, Phys. Rev. A **60**, 2752 (1999).

Chapter 13

INSEPARABILITY CRITERION FOR CONTINUOUS VARIABLE SYSTEMS

Lu-Ming Duan^{1,2}, G. Giedke¹, J. I. Cirac¹, and P. Zoller¹

¹*Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*

²*Laboratory of Quantum Communication and Quantum Computation, University of Science and Technology of China, Hefei 230026, China*

Email: Luming.Duan@uibk.ac.at

As with discrete systems, quantum entanglement also plays the basic role in quantum information protocols with continuous variables. A problem of great importance is then to check whether a continuous variable state, generally mixed, is entangled (inseparable). For discrete systems, there is the Peres-Horodecki inseparability criterion [1, 2], based on the negativity of the partial transpose of the composite density operator. This negativity provides a necessary and sufficient condition for inseparability of 2×2 or 2×3 -dimensional systems. In this section, we will describe an entirely different inseparability criterion for continuous variable states, which was first proposed in Ref. [3]. The Peres-Horodecki criterion was also successfully extended to the continuous variable systems shortly afterwards, which will be described in the next section by Simon.

The inseparability criterion described here is based on the total variance of a pair of Einstein-Podolsky-Rosen (EPR) type operators. For any separable continuous variable states, this total variance is bounded from below by a certain value resulting from the uncertainty relation, whereas for entangled states this bound can be exceeded. So violation of this bound provides a sufficient condition for inseparability of any continuous variable state. Furthermore, for the set of Gaussian states, which are of great practical importance, this criterion turns out to be a necessary and sufficient condition for inseparability. In fact, for any Gaussian state the compliance with the low bound by a certain pair of EPR type operators guarantees that the state has a P-representation with positive distribution, so the state must be separable.

We say a quantum state ρ of two modes 1 and 2 is separable if and only if it can be expressed in the following form

$$\rho = \sum_i p_i \rho_{i1} \otimes \rho_{i2}, \quad (13.1)$$

where we assume ρ_{i1} and ρ_{i2} to be normalized states of the modes 1 and 2, respectively, and $p_i \geq 0$ to satisfy $\sum_i p_i = 1$.

A maximally entangled continuous variable state can be expressed as a co-eigenstate of a pair of EPR-type operators [4], such as $\hat{x}_1 + \hat{x}_2$ and $\hat{p}_1 - \hat{p}_2$. So the total variance of these two operators reduces to zero for maximally entangled continuous variable states. Of course, the maximally entangled continuous variable states are not physical, but for the physical entangled continuous variable states—the two-mode squeezed states [5], this variance will rapidly tend to zero by increasing the degree of squeezing. Interestingly, we find that for any separable state, there exists a lower bound to the total variance. To be more general, we consider the following type of EPR-like operators:

$$\hat{u} = |a| \hat{x}_1 + \frac{1}{a} \hat{x}_2, \quad (13.2)$$

$$\hat{v} = |a| \hat{p}_1 - \frac{1}{a} \hat{p}_2, \quad (13.3)$$

where we assume a is an arbitrary (nonzero) real number. For any separable state, the total variance of any pair of EPR-like operators in the form of Eq. (13.2,13.3) should satisfy a lower bound indicated by the following theorem:

Theorem 1 (sufficient criterion for inseparability): For any separable quantum state ρ , the total variance of a pair of EPR-like operators defined by Eq. (13.2,13.3) with the commutators $[\hat{x}_j, \hat{p}_{j'}] = \frac{i}{2} \delta_{jj'} (j, j' = 1, 2)$ satisfies the inequality

$$\langle (\Delta \hat{u})^2 \rangle_\rho + \langle (\Delta \hat{v})^2 \rangle_\rho \geq \frac{1}{2} \left(a^2 + \frac{1}{a^2} \right). \quad (13.4)$$

Proof. We can directly calculate the total variance of the \hat{u} and \hat{v} operators using the decomposition (13.1) of the density operator ρ , and finally get the following expression:

$$\begin{aligned}
 & \left\langle (\Delta \hat{u})^2 \right\rangle_\rho + \left\langle (\Delta \hat{v})^2 \right\rangle_\rho = \sum_i p_i \left(\langle \hat{u}^2 \rangle_i + \langle \hat{v}^2 \rangle_i \right) - \langle \hat{u} \rangle_\rho^2 - \langle \hat{v} \rangle_\rho^2 \\
 &= \sum_i p_i \left(a^2 \langle \hat{x}_1^2 \rangle_i + \frac{1}{a^2} \langle \hat{x}_2^2 \rangle_i + a^2 \langle \hat{p}_1^2 \rangle_i + \frac{1}{a^2} \langle \hat{p}_2^2 \rangle_i \right) \\
 &\quad + 2 \frac{a}{|a|} \left(\sum_i p_i \langle \hat{x}_1 \rangle_i \langle \hat{x}_2 \rangle_i - \sum_i p_i \langle \hat{p}_1 \rangle_i \langle \hat{p}_2 \rangle_i \right) - \langle \hat{u} \rangle_\rho^2 - \langle \hat{v} \rangle_\rho^2 \quad (13.5) \\
 &= \sum_i p_i \left[a^2 \left(\left\langle (\Delta \hat{x}_1)^2 \right\rangle_i + \left\langle (\Delta \hat{p}_1)^2 \right\rangle_i \right) \right. \\
 &\quad \left. + \frac{1}{a^2} \left(\left\langle (\Delta \hat{x}_2)^2 \right\rangle_i + \left\langle (\Delta \hat{p}_2)^2 \right\rangle_i \right) \right] \\
 &\quad + \sum_i p_i \langle \hat{u} \rangle_i^2 - \left(\sum_i p_i \langle \hat{u} \rangle_i \right)^2 + \sum_i p_i \langle \hat{v} \rangle_i^2 - \left(\sum_i p_i \langle \hat{v} \rangle_i \right)^2.
 \end{aligned}$$

In Eq. (13.5), the symbol $\langle \cdots \rangle_i$ denotes average over the product density operator $\rho_{i1} \otimes \rho_{i2}$. It follows from the uncertainty relation that $\left\langle (\Delta \hat{x}_j)^2 \right\rangle_i + \left\langle (\Delta \hat{p}_j)^2 \right\rangle_i \geq |[\hat{x}_j, \hat{p}_j]| = 1/2$ for $j = 1, 2$, and by applying the Cauchy-Schwarz inequality $\left(\sum_i p_i \right) \left(\sum_i p_i \langle \hat{u} \rangle_i^2 \right) \geq \left(\sum_i p_i |\langle \hat{u} \rangle_i| \right)^2$, we know that the last line of Eq. (13.5) is bounded from below by zero. Hence, the total variance of the two EPR-like operators \hat{u} and \hat{v} is bounded from below by $a^2 + \frac{1}{a^2}$ for any separable state. This completes the proof of the theorem.

Note that this theorem in fact gives a set of inequalities for separable states. The operators \hat{x}_j, \hat{p}_j ($j = 1, 2$) in the definition (13.1) can be any local operators satisfying the commutators $[\hat{x}_j, \hat{p}_{j'}] = \frac{i}{2} \delta_{jj'}$. In particular, if we apply an arbitrary local unitary operation $U_1 \otimes U_2$ to the operators \hat{u} and \hat{v} , the inequality (13.4) remains unchanged. Note also that without loss of generality we have taken the operators x_j and p_j dimensionless.

For inseparable states, the total variance of the \hat{u} and \hat{v} operators is required by the uncertainty relation to be larger than or equal to $\frac{1}{2} |a^2 - \frac{1}{a^2}|$, which reduces to zero for $a = 1$. For separable states the much stronger bound given by Eq. (13.4) must be satisfied. A natural question is then how strong the bound is. Is it strong enough to ensure that if some inequality in the form of Eq. (13.4) is satisfied, the state necessarily becomes separable? Of course, it will be very difficult to consider this problem for arbitrary continuous variable states. However, in recent experiments and protocols for quantum communication [6, 7, 8, 9, 10, 11, 12, 13], continuous variable entanglement is generated by two-mode squeezing or by beam splitters, and the communication noise results

from photon absorption and thermal photon emission. All these processes lead to Gaussian states. So, we will limit ourselves to consider Gaussian states, which are of great practical importance. We find that the inequality (13.4) indeed gives a necessary and sufficient inseparability criterion for all the Gaussian states. To present and prove our main theorem, we need first mention some notations and results for Gaussian states.

It is convenient to represent a Gaussian state by its Wigner characteristic function. A two-mode state with the density operator ρ has the following Wigner characteristic function [5]

$$\begin{aligned}\chi^{(w)}(\lambda_1, \lambda_2) &= \text{tr} \left[\rho \exp \left(\lambda_1 \hat{a}_1 - \lambda_1^* \hat{a}_1^\dagger + \lambda_2 \hat{a}_2 - \lambda_2^* \hat{a}_2^\dagger \right) \right] \\ &= \text{tr} \left\{ \rho \exp \left[2i \left(\lambda_1^I \hat{x}_1 + \lambda_1^R \hat{p}_1 + \lambda_2^I \hat{x}_2 + \lambda_2^R \hat{p}_2 \right) \right] \right\} \end{aligned} \quad (13.6)$$

where the parameters $\lambda_j = \lambda_j^R + i\lambda_j^I$, and the annihilation operators $\hat{a}_j = \hat{x}_j + i\hat{p}_j$, with the quadrature amplitudes \hat{x}_j, \hat{p}_j satisfying the commutators $[\hat{x}_j, \hat{p}_{j'}] = \frac{i}{2} \delta_{jj'} \quad (j, j' = 1, 2)$. For a Gaussian state, the Wigner characteristic function $\chi^{(w)}(\lambda_1, \lambda_2)$ is a Gaussian function of λ_j^R and λ_j^I [5]. Without loss of generality, we can write $\chi^{(w)}(\lambda_1, \lambda_2)$ in the form

$$\chi^{(w)}(\lambda_1, \lambda_2) = \exp \left[-\frac{1}{2} (\lambda_1^I, \lambda_1^R, \lambda_2^I, \lambda_2^R) M (\lambda_1^I, \lambda_1^R, \lambda_2^I, \lambda_2^R)^T \right] \quad (13.7)$$

In Eq. (13.7), linear terms in the exponent are not included since they can be easily removed by some local displacements of \hat{x}_j, \hat{p}_j and thus have no influence on separability or inseparability of the state. The correlation property of the Gaussian state is completely determined by the 4×4 real symmetric correlation matrix M , which can be expressed as

$$M = \begin{pmatrix} G_1 & C \\ C^T & G_2 \end{pmatrix}, \quad (13.8)$$

where G_1, G_2 , and C are 2×2 real matrices. To study the separability property, it is convenient to first transform the Gaussian state to some standard forms through local linear unitary Bogoliubov operations (LLUBOs) $U_l = U_1 \otimes U_2$. In the Heisenberg picture, the general form of the LLUBO U_l is expressed as $U_l (\hat{x}_j, \hat{p}_j)^T U_l^\dagger = H_j (\hat{x}_j, \hat{p}_j)^T$ for $j = 1, 2$, where H_j is some 2×2 real matrix with $\det H_j = 1$. Any LLUBO is obtainable by combining the squeezing transformation together with some rotations [14]. We have the following two lemmas concerning the standard forms of the Gaussian state:

Lemma 1 (standard form I): Any Gaussian state ρ_G can be transformed through LLUBOs to the standard form I with the correlation matrix given by

$$M_s^I = \begin{pmatrix} n & c & & \\ & n & c' & \\ c & & m & \\ & c' & & m \end{pmatrix}, (n, m \geq 1) \quad (13.9)$$

Proof. A LLUBO on the state ρ_G transforms the correlation matrix M in the Wigner characteristic function in the following way

$$\begin{pmatrix} V_1 & \\ & V_2 \end{pmatrix} M \begin{pmatrix} V_1^T & \\ & V_2^T \end{pmatrix}, \quad (13.10)$$

where V_1 and V_2 are real matrices with $\det V_1 = \det V_2 = 1$. Since the matrices G_1 and G_2 in Eq. (13.8) are real symmetric, we can choose first a LLUBO with orthogonal V_1 and V_2 which diagonalize G_1 and G_2 , and then a local squeezing operation which transforms the diagonalized G_1 and G_2 into the matrices $G'_1 = nI_2$ and $G'_2 = mI_2$, respectively, where I_2 is the 2×2 unit matrix. After these two steps of operations, we assume the matrix C in Eq. (13.8) is changed into C' , which always has a singular value decomposition, thus it can be diagonalized by another LLUBO with suitable orthogonal V_1 and V_2 . The last orthogonal LLUBO does not influence G'_1 and G'_2 any more since they are proportional to the unit matrix. Hence, any Gaussian state can be transformed by three-step LLUBOs to the standard form I. The four parameters n, m, c , and c' in the standard form I are related to the four invariants $\det G_1$, $\det G_2$, $\det C$, and $\det M$ of the correlation matrix under LLUBOs by the equations $\det G_1 = n^2$, $\det G_2 = m^2$, $\det C = cc'$, and $\det M = (nm - c^2)(nm - c'^2)$.

Lemma 2 (standard form II): Any Gaussian state ρ_G can be transformed through LLUBOs into the standard form II with the correlation matrix given by

$$M_s^{II} = \begin{pmatrix} n_1 & c_1 & & \\ & n_2 & c_2 & \\ c_1 & & m_1 & \\ & c_2 & & m_2 \end{pmatrix}, \quad (13.11)$$

where the n_i , m_i and c_i satisfy

$$\frac{n_1 - 1}{m_1 - 1} = \frac{n_2 - 1}{m_2 - 1}, \quad (13.12)$$

$$|c_1| - |c_2| = \sqrt{(n_1 - 1)(m_1 - 1)} - \sqrt{(n_2 - 1)(m_2 - 1)}. \quad (13.13)$$

Proof. First, any Gaussian state can be tranformed through LLUBOs to the standard form I. We then apply two additional local squeezing operations on the standard form I, and get the state with the following correlation matrix

$$M' = \begin{pmatrix} nr_1 & \sqrt{r_1 r_2} c & \frac{c'}{\sqrt{r_1 r_2}} \\ \sqrt{r_1 r_2} c & \frac{n}{r_1} & mr_2 \\ \frac{c'}{\sqrt{r_1 r_2}} & mr_2 & \frac{m}{r_2} \end{pmatrix}, \quad (13.14)$$

where r_1 and r_2 are arbitrary squeezing parameters. M' in Eq. (13.14) has the standard form M_s^{II} (13.11) if r_1 and r_2 satisfy the following two equations

$$\frac{\frac{n}{r_1} - 1}{nr_1 - 1} = \frac{\frac{m}{r_2} - 1}{mr_2 - 1}, \quad (13.15)$$

$$\sqrt{r_1 r_2} |c| - \frac{|c'|}{\sqrt{r_1 r_2}} = \sqrt{(nr_1 - 1)(mr_2 - 1)} - \sqrt{\left(\frac{n}{r_1} - 1\right)\left(\frac{m}{r_2} - 1\right)}. \quad (13.16)$$

Our task remains to prove that Eqs. (13.15) and (13.16) are indeed satisfied by some positive r_1 and r_2 for arbitrary Gaussian states. Without loss of generality, we assume $|c| \geq |c'|$ and $n \geq m$. From Eq. (13.15), r_2 can be expressed as a continuous function of r_1 with $r_2(r_1 = 1) = 1$ and $r_2(r_1) \xrightarrow{r_1 \rightarrow \infty} m$. Substituting this expression $r_2(r_1)$ into Eq. (13.16), we construct a function $f(r_1)$ by subtracting the right hand side of Eq. (13.16) from the left hand side. Obviously, $f(r_1 = 1) = |c| - |c'| \geq 0$, and $f(r_1) \xrightarrow{r_1 \rightarrow \infty} \sqrt{r_1 m} \left(|c| - \sqrt{n(m - \frac{1}{m})}\right) \leq 0$, where the inequality $|c| \leq \sqrt{n(m - \frac{1}{m})}$ results from the physical condition $\langle (\Delta \hat{u}_0)^2 \rangle + \langle (\Delta \hat{v}_0)^2 \rangle \geq |[\hat{u}_0, \hat{v}_0]|$ with $\hat{u}_0 = \sqrt{m - \frac{1}{m}} \hat{x}_1 - \frac{c}{|c|} \sqrt{n} \hat{x}_2$ and $\hat{v}_0 = \frac{\sqrt{n}}{m} \hat{p}_2$. It follows from continuity that there must exist a $r_1^* \in [1, \infty)$ which makes $f(r_1 = r_1^*) = 0$. So Eqs. (13.15) and (13.16) have at least one solution. This proves lemma 2.

We remark that corresponding to a given standard form I or II, there are a class of Gaussian states, which are equivalent under LLUBOs. Note that separability or inseparability is a property not influenced by LLUBOs, so all the Gaussian states with the same standard forms have the same separability or inseparability property. With the above preparations, now we present the following main theorem:

Theorem 2 (necessary and sufficient inseparability criterion for Gaussian states): A Gaussian state ρ_G is separable if and only if when expressed in its standard form II, the inequality (13.4) is satisfied by the following two EPR-type operators

$$\hat{u} = a_0 \hat{x}_1 - \frac{c_1}{|c_1|} \frac{1}{a_0} \hat{x}_2, \quad (13.17)$$

$$\hat{v} = a_0 \hat{p}_1 - \frac{c_2}{|c_2|} \frac{1}{a_0} \hat{p}_2, \quad (13.18)$$

where $a_0^2 = \sqrt{\frac{m_1-1}{n_1-1}} = \sqrt{\frac{m_2-1}{n_2-1}}$.

Proof. The ‘only if’ part follows directly from theorem 1. We only need to prove the ‘if’ part. From lemma 2, we can first transform the Gaussian state through LLUBOs to the standard form II. The state after transformation is denoted by ρ_G^{II} . Then, substituting the expression (13.17,13.18) of \hat{u} and \hat{v} into the inequality (13.4), and calculating $\langle (\Delta \hat{u})^2 \rangle + \langle (\Delta \hat{v})^2 \rangle$ using the correlation matrix M_s^{II} , we get the following inequality

$$a_0^2 \frac{n_1 + n_2}{4} + \frac{m_1 + m_2}{4a_0^2} - \frac{1}{2} (|c_1| + |c_2|) \geq \frac{1}{2} \left(a_0^2 + \frac{1}{a_0^2} \right), \quad (13.19)$$

which, combined with Eq. (13.12,13.13), yields

$$|c_1| \leq \sqrt{(n_1 - 1)(m_1 - 1)}. \quad (13.20)$$

$$|c_2| \leq \sqrt{(n_2 - 1)(m_2 - 1)} \quad (13.21)$$

The inequality (13.20,13.21) ensures that the matrix $M_s^{II} - I$ is positive semi-definite. So there exists a Fourier transformation to the following normal characteristic function of the state ρ_G^{II}

$$\begin{aligned} \chi_{II}^{(n)}(\lambda_1, \lambda_2) &= \chi_{II}^{(w)}(\lambda_1, \lambda_2) \exp \left[\frac{1}{2} \left(|\lambda_1|^2 + |\lambda_2|^2 \right) \right] \\ &= \exp \left[-\frac{1}{2} \left(\lambda_1^I, \lambda_1^R, \lambda_2^I, \lambda_2^R \right) \left(M_s^{II} - I \right) \left(\lambda_1^I, \lambda_1^R, \lambda_2^I, \lambda_2^R \right)^T \right] \end{aligned} \quad (13.22)$$

This means that ρ_G^{II} can be expressed as

$$\rho_G^{II} = \int d^2\alpha d^2\beta P(\alpha, \beta) |\alpha, \beta\rangle \langle \alpha, \beta|, \quad (13.23)$$

where $P(\alpha, \beta)$ is the Fourier transformation of $\chi_{II}^{(n)}(\lambda_1, \lambda_2)$ and thus is a positive Gaussian function. Eq. (13.23) shows ρ_G^{II} is separable. Since the original Gaussian state ρ_G differs from ρ_G^{II} by only some LLUBOs, it must also be separable. This completes the proof of theorem 2.

Now we have a necessary and sufficient inseparability criterion for all the Gaussian states. We conclude the paper by applying this criterion to a simple example. Consider a two-mode squeezed vacuum state $e^{r(\hat{a}_1^\dagger \hat{a}_2^\dagger - \hat{a}_1 \hat{a}_2)} |vac\rangle$ with the squeezing parameter r . This state has been used in recent experiment for continuous variable quantum teleportation [13]. Suppose that the two optical modes are subject to independent thermal noise during transmission with the same damping coefficient denoted by η and the same mean thermal photon number denoted by \bar{n} . It is easy to show that after time t , the standard correlation matrix for this Gaussian state has the form of Eq. (13.9) with $n = m = \cosh(2r)e^{-2\eta t} + (2\bar{n} + 1)(1 - e^{-2\eta t})$ and $c = -c' = \sinh(2r)e^{-2\eta t}$ [15]. So the inseparability criterion means that if the transmission time t satisfies

$$t < \frac{1}{2\eta} \ln \left(1 + \frac{1 - e^{-2r}}{2\bar{n}} \right), \quad (13.24)$$

the state is entangled; otherwise it becomes separable. Interestingly, Eq. (13.24) shows that if there is only vacuum fluctuation noise, i.e., $\bar{n} = 0$ (this seems to be a good approximation for optical frequency), the initial squeezed state is always entangled. This result does not remain true if thermal noise is present. In the limit $\bar{n} \gg 1$, the state is not entangled any more when the transmission time $t \geq \frac{1 - e^{-2r}}{4\eta\bar{n}}$.

References

- [1] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [2] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
- [3] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
- [4] A. Einstein, B. Podolsky, and R. Rosen, Phys. Rev. **47**, 777 (1935).
- [5] C. W. Gardiner and P. Zoller, Quantum Noise (2nd. Ed.), Springer-Verlag (1999).
- [6] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
- [7] S. L. Braunstein, H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
- [8] S. L. Braunstein, Nature **394**, 47 (1998).
- [9] S. L. Braunstein and S. Lloyd, Phys. Rev. Lett. **82**, 1789 (1999).
- [10] G. J. Milburn and S. L. Braunstein, quant-ph/9812018.
- [11] P. Loock, A. L. Braunstein, and H. J. Kimble, quant-ph/9902030.
- [12] A. S. Parkins, and H. J. Kimble, quant-ph/9904062.

- [13] A. Furusawa et al., Science **282**, 706 (1998).
- [14] S. L. Braunstein, quant-ph/9904002.
- [15] L. M. Duan and G. C. Guo, Quantum Semiclass. Opt. **9**, 953 (1997).

Chapter 14

SEPARABILITY CRITERION FOR GAUSSIAN STATES

R. Simon

The Institute of Mathematical Sciences, Tharamani, Chennai 600 113, India

Abstract The PPT (positivity under partial transpose) criterion is studied in the context of separability of continuous variable bipartite states. The partial transpose operation admits, in the Wigner representation of quantum mechanics, a geometric interpretation as momentum reversal or mirror reflection in phase space. This recognition leads to uncertainty principles, stronger than the traditional ones, to be obeyed by all PPT (separable as well as bound entangled) states. In the special case of bipartite two-mode systems, the PPT criterion turns out to be necessary and sufficient condition for separability, for all Gaussian states: a $1 + 1$ system has no bound entangled Gaussian state. The symplectic group of linear canonical transformations and the representation of these transformations through (metaplectic) unitary Hilbert space operators play an important role in our analysis.

A major part of the effort in quantum information science has traditionally been in respect of systems with finite number of Hilbert space dimensions, more specifically in respect of qubits corresponding to Hilbert space dimension two. But recently there has been much interest in the canonical case of continuous variable systems [1, 2, 3, 4, 5, 6]. We may mention, in particular, the experimental realization of quantum teleportation of coherent states [7]. This achievement has acted as a significant impetus for this interest.

Entanglement or inseparability plays a central role as the primary resource in almost all branches of the emerging field of quantum information and quantum computation [8]. Issues related to entanglement are considerably richer in the context of mixed states compared to the situation with pure states. For instance, while it is nearly trivial to test if a given bipartite state is separable, we do not yet have an effective algorithm to test if a given mixed state of a bipartite system is separable or entangled.

A particularly elegant criterion for checking if a (bipartite mixed) state is separable or not was formulated by Peres [9]. This criterion based on partial

transposition turns out to be necessary and sufficient for separability for all states of 2×2 and 2×3 dimensional bipartite systems, but ceases to be so in higher dimensions as shown by Horodecki [10]. Entanglements which are not witnessed by the partial transpose operation cannot be distilled, and for this reason such entanglements have come to be known as bound entanglements.

With increasing Hilbert space dimension, tests for separability will be expected to become more and more difficult to implement in practice, and less and less definitive in their outcome. On the other hand, in the infinite dimensional case corresponding to continuous variable systems Gaussian states are of particular interest from the point of view of experiments, and for this reason a test for separability which is decisive for all Gaussian states could be of considerable value in the continuous case, even if it fails to be decisive for non-Gaussian states. Hence is the importance of the result established in Ref. [11] that the partial transpose condition proves both necessary and sufficient (NS) condition for separability, for all Gaussian states of a bipartite system of two harmonic oscillators. We should hasten to add that the partial transpose criterion of separability ceases to be NS, even for Gaussian states, when both sides of the system (Alice and Bob) have two or more oscillators each, as shown by Werner and Wolf [12].

An interesting approach to separability of Gaussian states, based on the total variance of a pair of Einstein-Podolsky-Rosen type operators, was independently formulated by Duan et al. [13]. This approach too leads to a criterion which proves NS in the $1 + 1$ case. The same authors have proposed also an entanglement purification protocol to generate maximally entangled states from two-mode squeezed states or from mixed Gaussian entangled states [14].

The origin of the fact that the issue of separability is easily tractable in the case of Gaussian states can be traced as follows. First, a Gaussian state is fully determined by its first and second moments. The Weyl group of unitary operators which effect translations in phase space are manifestly *separable*, and hence their action does not affect the separability or otherwise of a state. We may thus assume, without loss of generality, that the first moments of the state of our interest all vanish. In other words, separability of a Gaussian state is determined entirely by the variance (or covariance) matrix of the state. The problem thus gets reduced from study of the *infinite* dimensional density matrix to analysis of the *finite* dimensional variance matrix.

Secondly, under the unitary action of the symplectic group of real linear canonical transformation the moments of a quantum state in general, and the variance matrix in particular, undergo simple geometric changes. One may thus use *local* symplectic transformations (local transformations have no effect on separability) to convert the variance matrix into a canonical form in which the separability issue becomes particularly easy to settle.

Characterization of a Gaussian state in term of its variance matrix (and first moments) and the action of symplectic transformations on the state take a particularly revealing and convenient form in the Wigner representation of quantum mechanics. Further, the partial transpose operation acquires a suggestive geometric interpretation in this representation. For these reasons the Wigner representation proves convenient for analysis of the issue of separability for Gaussian states.

1. LINEAR CANONICAL TRANSFORMATIONS

Consider a system of n oscillators described by phase space variables $q_1, p_1; q_2, p_2; \dots; q_n, p_n$ or by the corresponding canonical operators $\hat{q}_1, \hat{p}_1; \hat{q}_2, \hat{p}_2; \dots; \hat{q}_n, \hat{p}_n$. It is convenient to arrange these phase space variables and hermitian operators into column vectors

$$\xi = \begin{pmatrix} q_1 \\ p_1 \\ q_2 \\ p_2 \\ \vdots \\ q_n \\ p_n \end{pmatrix}, \quad \hat{\xi} = \begin{pmatrix} \hat{q}_1 \\ \hat{p}_1 \\ \hat{q}_2 \\ \hat{p}_2 \\ \vdots \\ \hat{q}_n \\ \hat{p}_n \end{pmatrix}. \quad (14.1)$$

The complete set of canonical commutation relations

$$\begin{aligned} [\hat{q}_j, \hat{q}_k] &= 0, \quad [\hat{p}_j, \hat{p}_k] = 0; \\ [\hat{q}_j, \hat{p}_k] &= \delta_{jk}, \quad j, k = 1, 2, \dots, n \end{aligned} \quad (14.2)$$

can be written in the useful compact form [15]

$$[\hat{\xi}_\alpha, \hat{\xi}_\beta] = i \Omega_{\alpha\beta}, \quad \alpha, \beta = 1, 2, \dots, 2n; \quad (14.3)$$

where

$$\Omega = \begin{pmatrix} J & 0 & 0 & \cdots & 0 \\ 0 & J & 0 & \cdots & 0 \\ 0 & 0 & J & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & J \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (14.4)$$

Linear homogeneous canonical transformations in the $2n$ -dimensional phase space of our n -oscillator system act as Hilbert space unitary operators in the quantum description. With a set of canonical coordinates chosen for the phase space, such a transformation is identified by its matrix S :

$$S : \xi \rightarrow \xi' = S\xi. \quad (14.5)$$

Clearly, this transformation is canonical if and only if S respects

$$S\Omega S^T = \Omega, \quad (14.6)$$

which is recognized as the defining condition for $Sp(2n, R)$, the group of symplectic matrices. Thus, linear canonical transformations are in one-to-one correspondence with elements of the *symplectic group* $Sp(2n, R)$. It is useful to note that $\det S = 1$, $\forall S \in Sp(2n, R)$, and that $S \in Sp(2n, R)$ implies $S^T \in Sp(2n, R)$.

Let $\mathcal{U}(S)$ be a Hilbert space unitary operator corresponding to the canonical transformation S . This means we have the following evolution for the operators $\hat{\xi}$:

$$\mathcal{U}(S) : \hat{\xi}_\alpha \rightarrow \hat{\xi}'_\alpha = \mathcal{U}(S)^\dagger \hat{\xi}_\alpha \mathcal{U}(S) = \sum_{\beta=1}^{2n} S_{\alpha\beta} \hat{\xi}_\beta. \quad (14.7)$$

We could have written this in the abbreviated form $\hat{\xi}' = \mathcal{U}(S)^\dagger \hat{\xi} \mathcal{U}(S) = S \hat{\xi}$.

In order that the unitary operators $\mathcal{U}(S)$ give a representation of $Sp(2n, R)$, we should be able to choose the former in such a way that $\mathcal{U}(S)\mathcal{U}(S') = \mathcal{U}(SS')$, $\forall S, S' \in Sp(2n, R)$. Clearly, $\mathcal{U}(S)^\dagger \hat{\xi} \mathcal{U}(S) = S \hat{\xi}$ allows, in the correspondence $S \rightarrow \mathcal{U}(S)$, freedom of a S -dependent phase factor $\exp(i\phi(S))$ multiplying $\mathcal{U}(S)$. Can we make a one-to-one choice $S \rightarrow \phi(S)$ such that $\mathcal{U}(S)\mathcal{U}(S') = \mathcal{U}(SS')$, $\forall S, S' \in Sp(2n, R)$? The answer turns out to be in the negative. The maximum simplification one can obtain in this regard is a one-to-two correspondence $S \rightarrow \pm \mathcal{U}(S)$. In other words this correspondence yields a two-valued unitary ‘representation’ of the symplectic group. Conversely, these unitary operators close to form the defining representation of a new group called the *metaplectic group* $Mp(2n, R)$. This group is a double cover of the symplectic group. A detailed discussion of the symplectic-metaplectic connection, with further references, can be found in Ref. [16]. The situation is somewhat analogous to the well known connection between $SO(3)$ and $SU(2)$. The major difference is that $SO(3)$ is doubly connected and so its double cover $SU(2)$ is simply connected (and hence is the universal cover of $SO(3)$); but $Sp(2n, R)$ is infinitely connected, and so also is its double cover.

The point being made is that what is natural for the quantum description of a system of oscillators at the state vector level is the metaplectic group rather than the symplectic group. The symplectic group is recovered in the description at the density operator level (or, equivalently, in the Wigner description), though. This subtle aspect can be appreciated by considering just one oscillator. After evolution through one period, which corresponds to the identity element of $Sp(2, R)$, the position and momentum — and indeed the entire phase space — return to their original configuration. But the unitary evolution of a statevector $|\psi\rangle$ of the same oscillator through one period returns $-|\psi\rangle$ rather than $|\psi\rangle$

itself. The state vector is recovered in full only after two periods. Originating in this subtlety is not only the zero-point energy, but also the Gouy phase picked up by a light beam as it crosses a focus [17], the $\pi/4$ phase picked up by the WKB wavefunction at the turning points, and the Maslov index.

2. THE WIGNER DESCRIPTION

The Wigner description of quantum mechanics is at the density operator level, rather than at the state vector level, and it treats pure states and mixed states on the same footing. In this description density operators of a quantum system are put into one-to-one correspondence with real-valued functions over the (classical) phase space through the rule [18, 15]

$$W(q, p) = \pi^{-n} \int d^n q' \langle q - q' | \hat{\rho} | q + q' \rangle \exp(2i q' \cdot p). \quad (14.8)$$

where $q = (q_1, q_2, \dots, q_n)$ and $p = (p_1, p_2, \dots, p_n)$. We will often write $W(\xi)$ in place of $W(q, p)$. It is clear that this map is invertible, and thus the function $W(q, p)$ captures the density matrix in its entirety. In most aspects of structure and dynamics, the Wigner distribution function $W(q, p)$ behaves exactly like the phase space density in classical statistical mechanics, but $W(q, p)$ is not pointwise nonnegative for most quantum states. Indeed, the Wigner function of a pure state is pointwise nonnegative if and only if the state is Gaussian [19]!

The defining properties of Wigner distributions are transcriptions, through the map (14.8), of those of density operators. Thus, hermiticity of density operator $\hat{\rho}$ is equivalent to the corresponding phase space distribution being real, while the condition $\text{tr} \hat{\rho} = 1$ transcribes into $\int d^{2n} \xi W(\xi) = 1$. The nonnegativity of $\hat{\rho}$, which can be stated as the requirement that $\text{tr}(\hat{\rho} \hat{\rho}') \geq 0$ for every density operator $\hat{\rho}'$, gets translated into the condition

$$\text{tr}(\hat{\rho} \hat{\rho}') = (2\pi)^n \int d^{2n} \xi W(\xi) W'(\xi) \geq 0, \quad (14.9)$$

for every Wigner distribution $W'(\xi)$. In particular, a phase space distribution $W(\xi)$ which is known to be a Wigner distribution corresponds to a pure state if and only if

$$(2\pi)^n \int d^{2n} \xi [W(\xi) W'(\xi)]^2 = 1. \quad (14.10)$$

In the nonnegativity condition $\text{tr}(\hat{\rho} \hat{\rho}') \geq 0$, it is sufficient to restrict $\hat{\rho}'$ to pure states; so also in the condition (14.9) it proves sufficient to restrict $W'(\xi)$ to pure state Wigner functions.

The Wigner description offers several advantages in respect of our primary concern, namely the issue of separability of Gaussian states. Foremost among

these is the action of canonical transformations. We have noted that the symplectic group $Sp(2n, R)$ acts unitarily and irreducibly on the n -mode Hilbert space [20]. The (infinite dimensional) unitary operator $\mathcal{U}(S)$ corresponding to $S \in Sp(2n, R)$ transforms the state vector $|\psi\rangle$ to $|\psi'\rangle = \mathcal{U}(S)|\psi\rangle$, and hence the density operator $\hat{\rho}$ to $\hat{\rho}' = \mathcal{U}(S)\hat{\rho}\mathcal{U}(S)^\dagger$. This transformation takes a strikingly simple form in the Wigner description, and this is one reason for the effectiveness of the Wigner picture in handling canonical transformations [20]:

$$S: \hat{\rho} \longrightarrow \mathcal{U}(S)\hat{\rho}\mathcal{U}(S)^\dagger \iff W(\xi) \longrightarrow W'(\xi) = W(S^{-1}\xi). \quad (14.11)$$

That is, $W'(S\xi) = W(\xi)$ for every canonical transformation $S \in Sp(2n, R)$, and the Wigner function transforms as a *Sp*($2n, R$) *scalar field*.

Secondly, the transpose map T and the partial transpose map PT take transparent geometric form in the Wigner description. Indeed, it follows from the definition of Wigner distribution that transpose operation on the density operator, which is equivalent to complex conjugation of the elements of the density matrix in the position representation, transcribes faithfully into momentum reversal operation in the Wigner description:

$$\begin{aligned} T: W(q, p) &\rightarrow W'(q, p) = W(q, -p) = W(\Lambda\xi), \\ \Lambda &= \text{diag}(1, -1; 1, -1; \dots; 1, -1) \\ &= \sigma_3 \oplus \sigma_3 \oplus \dots \oplus \sigma_3. \end{aligned} \quad (14.12)$$

This mirror reflection, which inverts the p coordinates leaving q coordinates unchanged, is consistent with our expectation that transpose operation on the density operator is the same thing as *time reversal*.

The transposition map takes density operators to density operators and, equivalently, Wigner distributions to Wigner distributions. This statement is, in a sense, worded stronger than what it really is: transposition cannot be implemented as a physical process. Transposition with respect to one subsystem of a composite system (partial transpose) can take Wigner distributions (density operators) into phase space distributions (operators) which are not Wigner distributions (density operators). Thus, partial transpose acts as a potential entanglement witness, for it does not necessarily preserve the ‘Wigner quality’ of the phase space distribution of an entangled state.

Finally, moments of the canonical operators are related to the Wigner distribution in exactly the same manner they are related to the phase space density in classical statistical mechanics. The first moments $\langle \hat{\xi}_\alpha \rangle \equiv \text{tr}(\hat{\xi}_\alpha \hat{\rho})$ are given by

$$\langle \hat{\xi}_\alpha \rangle = \text{tr}(\hat{\rho} \hat{\xi}) = \int d^{2n}\xi W(\xi) \xi_\alpha. \quad (14.13)$$

Let us define difference or fluctuation operators $\Delta\hat{\xi}$ through $\Delta\hat{\xi} = \hat{\xi} - \langle \hat{\xi} \rangle$. Clearly, the $2n$ components of $\Delta\hat{\xi}$ obey the same commutation relations as

those of $\hat{\xi}$. Similarly, we may define $\Delta\xi_\alpha = \xi_\alpha - \langle \xi_\alpha \rangle$. The uncertainties are defined as the expectations of the hermitian operators $\{\Delta\hat{\xi}_\alpha, \Delta\hat{\xi}_\beta\} = (\Delta\hat{\xi}_\alpha\Delta\hat{\xi}_\beta + \Delta\hat{\xi}_\beta\Delta\hat{\xi}_\alpha)/2$:

$$\langle \{\Delta\hat{\xi}_\alpha, \Delta\hat{\xi}_\beta\} \rangle = \text{tr} \left(\{\Delta\hat{\xi}_\alpha, \Delta\hat{\xi}_\beta\} \hat{\rho} \right) = \int d^{2n}\xi \Delta\xi_\alpha \Delta\xi_\beta W(\xi). \quad (14.14)$$

It proves useful to arrange the uncertainties $\langle \{\Delta\hat{\xi}_\alpha, \Delta\hat{\xi}_\beta\} \rangle$ into a real $2n \times 2n$ matrix V defined through $V_{\alpha\beta} \equiv \langle \{\Delta\hat{\xi}_\alpha, \Delta\hat{\xi}_\beta\} \rangle$. This matrix is variously known as the variance, covariance, or noise matrix.

3. GAUSSIAN STATES AND THEIR NOISE MATRIX

Given an infinite-dimensional hermitian operator of unit trace, it is not always easy to test its nonnegativity and establish that it is a valid density operator. Testing the Wigner quality of a real phase space distribution is equally difficult. This issue can, however, be elegantly resolved for Gaussian states of a system of n oscillators, for an arbitrary value of n .

The distinguishing feature of Gaussian states is that they are fully characterised by their first and second moments. Indeed, the Wigner distribution of a Gaussian state has the form

$$W(\xi) = \left((2\pi)^n \sqrt{\det V} \right)^{-1} \exp \left(-\frac{1}{2} (\xi - \langle \xi \rangle)^T V^{-1} (\xi - \langle \xi \rangle) \right). \quad (14.15)$$

The first moments given by the $2n$ components of $\langle \xi \rangle$ can assume arbitrary real values. They can be changed at will by the unitary action of the Weyl displacement operators. Further, the value of the first moments affect in no way the Wigner quality of the phase space distribution. We can therefore assume, without loss of generality, that our Gaussian state has vanishing first moments; it is then completely specified by the positive definite variance matrix V !

What are the additional conditions that the noise matrix $V > 0$ should satisfy in order that the Gaussian distribution in (14.15) is a Wigner distribution? To obtain these conditions, which arise basically from the uncertainty principle, note first of all that the symplectic transformation law (14.11) implies that the first moments change as

$$S : \langle \xi \rangle \rightarrow \langle \xi' \rangle = S \langle \xi \rangle, \quad (14.16)$$

and that the variance matrix undergoes the congruence

$$S : V \rightarrow V' = S V S^T. \quad (14.17)$$

In view of (14.6), this *congruence* is equivalent to the *conjugation*

$$S : V\Omega \rightarrow V'\Omega = S V \Omega S^{-1}. \quad (14.18)$$

Thus, $\beta_\ell \equiv \text{tr}(V\Omega)^{2\ell}$, $\ell = 1, 2, \dots, n$ are *symplectic invariants*. And these are the only independent invariants of V , $(V\Omega)^k$ being traceless for odd values of k .

It is clear that not every rotation in the $2n$ -dimensional phase space is a canonical transformation. Indeed, the set of all phase space rotations forming a subgroup of $Sp(2n, R)$ is isomorphic to the n^2 -dimensional unitary group $U(n)$. And n^2 is smaller than $2n^2 - n$, the dimension of the full rotation group $SO(2n)$, for $n > 1$. We do not, therefore, expect in general to be able to diagonalize a real symmetric matrix V using symplectic congruence $V \rightarrow V' = S V S^T$, $S \in Sp(2n, R)$. *Williamson theorem* [21, 15, 22] guarantees that if V possesses the additional quality of being *positive definite*, it can be diagonalized through symplectic congruence. That is, $V > 0$ implies that there exists an $S_V \in Sp(2n, R)$ such that

$$S_V : V \rightarrow V_{WC} = S_V V S_V^T = \text{diag}(\kappa_1, \kappa_1; \kappa_2, \kappa_2; \dots; \kappa_n, \kappa_n) \quad (14.19)$$

Comparing with the Gaussian Wigner distribution in (14.15), it is clear that the Williamson canonical form V_{WC} corresponds to product of single-mode thermal state Wigner distributions, the temperature parameter of the j -th mode being determined by κ_j . The invariant traces are easily computed to be

$$\beta_\ell = -2 \sum_{j=1}^n (\kappa_j)^{2\ell}, \quad \ell = 1, 2, \dots, n. \quad (14.20)$$

We may as well take these κ_j 's as a complete set of algebraically independent symplectic invariants associated with the variance matrix V . These preparatory remarks enable us to give a complete characterization of variance matrices, and hence of Gaussian states.

Proposition 1: The following three conditions are equivalent to one another, and form necessary and sufficient condition for a real symmetric positive definite $2n \times 2n$ matrix V to be a physical variance matrix:

1. $V + \frac{i}{2}\Omega \geq 0$.
2. $V \geq \frac{1}{4}\Omega^T V^{-1} \Omega = \frac{1}{4}\Omega V^{-1} \Omega^T > 0$.
3. $V \geq \frac{1}{2}S S^T$, for some $S \in Sp(2n, R)$.

Proof: Note that the above conditions, each of which subsumes $V > 0$, are $Sp(2n, R)$ -invariant, as they should be, and this is the key to their proof: the uncertainty principle must be satisfied not only by the components of $\hat{\xi}$, but also by those of $\hat{\xi}' = S \hat{\xi}$, for every $S \in Sp(2n, R)$.

For a single mode state with *diagonal* variance matrix $V = \text{diag}(\kappa, \kappa)$, the acceptability condition or uncertainty principle reads $\kappa \geq 1/2$. Since the

Williamson normal form corresponds to product of single mode states, the acceptability condition for the normal form follows from that for the single mode case. That is $V_{WC} = \text{diag}(\kappa_1, \kappa_1; \kappa_2, \kappa_2; \dots; \kappa_n, \kappa_n)$ is acceptable as a variance matrix if and only if $\kappa_j \geq 1/2$, for $j = 1, 2, \dots, n$. We can now employ the symplectic metric Ω to rewrite this condition as $V_{WC} + \frac{i}{2}\Omega \geq 0$. Covariance of this condition under symplectic congruence leads to $V + \frac{i}{2}\Omega \geq 0$ in the general case.

The variable canonically conjugate to ξ'_α is given by $(\Omega \xi')_\alpha$. Product of the variances of this pair of conjugate variables should be bounded below by $1/4$, and this may be written as $\text{var}(\xi'_\alpha) \geq \frac{1}{4}[\text{var}((\Omega \xi')_\alpha)]^{-1}$. Stating this in a manifestly covariant form we have $V \geq \frac{1}{4}\Omega^T V^{-1} \Omega = \frac{1}{4}\Omega V^{-1} \Omega^T$.

Finally, the acceptability condition on V_{WC} can be written as the requirement $V_{WC} \geq \frac{1}{2}$. The statement that V is acceptable if and only if $V \geq \frac{1}{2}S S^T$, for some $S \in Sp(2n, R)$ is simply a covariant rendering of this requirement.

This completes proof of the proposition, and gives a complete characterization of Gaussian states: *the Gaussian phase space distribution (14.15) is a Wigner distribution if and only if V satisfies the above acceptability condition.*

We may note in passing that the formulation of the necessary and sufficient condition above is invariant under the transpose or momentum reversal map which takes V into $\Lambda V \Lambda^T = \Lambda V \Lambda$ or, equivalently, Ω into $\Lambda^{-1} V (\Lambda^T)^{-1} = -\Omega$. While the first two versions are manifestly invariant, invariance of the third one follows from the fact that $\Lambda S \Lambda \in Sp(2n, R)$, $\forall S \in Sp(2n, R)$, even though Λ itself is not an element of $Sp(2n, R)$. We conclude this Section with the following observation.

Proposition 2: The variance matrix of a state has the special form $V = \frac{1}{2}S S^T$, with $S \in Sp(2n, R)$, if and only if the state under consideration is a Gaussian pure state.

4. SEPARABILITY CRITERION FOR THE VARIANCE MATRIX

We are now equipped to consider a bipartite system consisting of n modes, with m modes in the possession of Alice and the remaining $n - m$ modes in Bob's possession. Let us introduce the following notations:

$$\begin{aligned} q_A &= (q_1, q_2, \dots, q_m), \quad p_A = (p_1, p_2, \dots, p_m), \\ \xi_A &= (q_1, p_1; q_2, p_2; \dots; q_m, p_m); \\ q_B &= (q_{m+1}, q_{m+2}, \dots, q_n), \quad p_B = (p_{m+1}, p_{m+2}, \dots, p_n), \\ \xi_A &= (q_{m+1}, p_{m+1}; q_{m+2}, p_{m+2}; \dots; q_n, p_n); \\ \xi &= (\xi_A, \xi_B). \end{aligned} \tag{14.21}$$

Consistent with this notation we may write the symplectic metric Ω as a direct sum of the symplectic metrics of the two subsystems:

$$\Omega = \begin{pmatrix} \Omega_A & 0 \\ 0 & \Omega_B \end{pmatrix} = \Omega_A \oplus \Omega_B. \quad (14.22)$$

Let $\hat{\rho}$ be a bipartite density matrix, and $W(\xi) = W(\xi_A, \xi_B)$ the corresponding Wigner distribution. The partial transpose map with respect to the Bob subsystem corresponds to

$$\begin{aligned} W(\xi) &\rightarrow W'(\xi) = W(\Lambda'\xi) = W(\xi_A, \Lambda_B \xi_B), \\ \Lambda' &= \begin{pmatrix} \text{Id}_A & 0 \\ 0 & \Lambda_B \end{pmatrix} = \text{Id}_A \oplus \Lambda_B. \end{aligned} \quad (14.23)$$

Though $W(\Lambda\xi)$ is a Wigner distribution for every Wigner distribution $W(\xi)$, the distribution $W(\Lambda'\xi)$ need not be Wigner. Stated differently, the momentum reversal map is *positive* but *not completely positive*. Since it is not completely positive, it does not correspond to any physically realizable process or channel. It does, however, prove to be of value in exposing or witnessing entanglement.

By definition, a quantum state $\hat{\rho}$ of the bipartite system is separable if and only if $\hat{\rho}$ can be expressed in the form

$$\hat{\rho} = \sum_k p_k \hat{\rho}_{A,k} \otimes \hat{\rho}_{B,k}, \quad (14.24)$$

with *nonnegative* p_k 's, where $\hat{\rho}_{A,k}$'s and $\hat{\rho}_{B,k}$'s are density operators of the subsystems of Alice and Bob respectively. Clearly, product states correspond to product Wigner distributions and separable states separable Wigner distributions:

$$W(\xi) = \sum_k p_k W_{A,k}(\xi_A) W_{B,k}(\xi_B). \quad (14.25)$$

where $W_{A,k}(\xi_A)$'s and $W_{B,k}(\xi_B)$'s are Wigner functions of the subsystems of Alice and Bob respectively. Product of Wigner distributions of the subsystems goes to product of Wigner distributions, and it follows that a separable wigner distribution goes to a (separable) Wigner distribution under the partial transpose map which corresponds to reversal of Bob's momenta, leaving Alice's variables unaffected.

It is clear that the variance matrix of a product state $W_{\text{product}}(\xi) = W_A(\xi_A) W_B(\xi_B)$ has the separable form

$$V = \begin{pmatrix} V_A & 0 \\ 0 & V_B \end{pmatrix} = V_A \oplus V_B, \quad (14.26)$$

where V_A and V_B are the variance matrices of the subsystems. Let $V_{A,k} \oplus V_{B,k}$ be the variance matrix of the product state $W_k(\xi) = W_{A,k}(\xi_A)W_{B,k}(\xi_B)$, and let $\xi^{(k)}$ be its first moments. Then the variance matrix of the separable state (14.25) is given by [recall that $\langle \xi \rangle$ has been assumed to vanish for $W(\xi)$]

$$V = \sum_k p_k V_{A,k} \oplus V_{B,k} + \sum_k p_k \xi^{(k)} \xi^{(k)T}. \quad (14.27)$$

Since convex sum of variance matrices is a variance matrix, and since

$$\sum_k p_k V_{A,k} \oplus V_{B,k} = \left(\sum_k p_k V_{A,k} \right) \oplus \left(\sum_k p_k V_{B,k} \right), \quad (14.28)$$

the first sum on the right hand side of (14.27) is a variance matrix. Since it has the block-diagonal form $V_A \oplus V_B$ where V_A and V_B are acceptable variance matrices, it follows from the third form of the condition in Proposition 1 that there exist symplectic matrices $S_A \in sp(2m, R)$ and $S_B \in Sp(2n - 2m, R)$ such that

$$\begin{aligned} \sum_k p_k V_{A,k} \oplus V_{B,k} &= \left(\sum_k p_k V_{A,k} \right) \oplus \left(\sum_k p_k V_{B,k} \right) \\ &\geq \frac{1}{2} S_A S_A^T \oplus S_B S_B^T. \end{aligned} \quad (14.29)$$

Since the second sum on the right hand side of (14.27) is a manifestly nonnegative matrix, we have established a necessary condition on the variance matrix of a separable state.

Proposition 3: If V is the variance matrix of a separable state, then there are matrices $S_A \in Sp(2m, R)$ and $S_B \in Sp(2n - 2m, R)$ such that

$$V \geq \frac{1}{2} S_A S_A^T \oplus S_B S_B^T. \quad (14.30)$$

The validity of this condition is quite general: the number of modes in the possession of Alice and Bob can be arbitrary, and the state under reference need not be Gaussian.

If the state under consideration is Gaussian, the above result can be considerably strengthened. To this end, we begin by noting the following.

Proposition 4: The variance matrix of a state has the special form $V = \frac{1}{2} S_A S_A^T \oplus S_B S_B^T$, with $S_A \in Sp(2m, R)$ and $S_B \in Sp(2n - 2m, R)$, if and only if the state under consideration is a Gaussian state which is both a pure state and a product state.

Let us denote the block-diagonal matrix $\frac{1}{2}S_A S_A^T \oplus S_B S_B^T$ by V_{GPP} to indicate the fact that it represents a Gaussian, pure, and product state. If the condition in Proposition 3 is met, we have $V = V_{\text{GPP}} + V_{\text{class}}$, for some $V_{\text{class}} \geq 0$, and the subscript of V_{class} anticipates a *classical* probability distribution we are going to associate with V_{class} . Let r be the rank (dimension of the range) of V_{class} , and let the $r \times r$ matrix $V_{\text{class}}^{(\text{res})}$ be the restriction of V_{class} to its range. Then $V = V_{\text{GPP}} + V_{\text{class}}$ implies

$$\begin{aligned} W_V(\xi) &= \left[(2\pi)^{r/2} \sqrt{\det V_{\text{class}}^{(\text{res})}} \right] \int d^r \xi' \\ &\quad \times \exp \left[-\frac{1}{2} \xi'^T (V_{\text{class}}^{(\text{res})})^{-1} \xi' \right] W_{V_{\text{GPP}}}(\xi - \xi'), \end{aligned} \quad (14.31)$$

where $d^r \xi'$ indicates integratlon over the range of V_{class} , and $W_{V_{\text{GPP}}}(\xi - \xi')$ is the Wigner distribution of the GPP state. Thus we have

Proposition 5: A Gaussian state with variance matrix V is separable if and only if

$$V \geq \frac{1}{2} S_A S_A^T \oplus S_B S_B^T \quad (14.32)$$

for some $S_A \in Sp(2m, R)$, $S_B \in Sp(2n - 2m, R)$.

5. SEPARABILITY AND UNCERTAINTY PRINCIPLE

Positivity under partial transpose (PPT) has important implications on the uncertainty principle, and it is useful to explore this aspect in some detail. The uncertainty principle $V + \frac{i}{2}\Omega \geq 0$ is a direct consequence of the canonical commutation relations (14.3) and the nonnegativity of the density matrix $\hat{\rho}$. It is *equivalent* to the statement that for every pair of $2n$ -dimensional phase space vectors $d = (d_A, d_B)$, $d' = (d'_A, d'_B)$, the hermitian operators $\hat{X}(d) = d^T \hat{\xi} = \sum_\alpha d_\alpha \hat{\xi}_\alpha$ and $\hat{X}(d') = d'^T \hat{\xi} = \sum_\alpha d'_\alpha \hat{\xi}_\alpha$ obey

$$\begin{aligned} \langle (\Delta \hat{X}(d))^2 \rangle + \langle (\Delta \hat{X}(d'))^2 \rangle &\geq |[\hat{X}(d), \hat{X}(d')]| \\ &= |d'^T \Omega d| \\ &= |d_A^T \Omega_A d'_A + d_B^T \Omega_B d'_B|. \end{aligned} \quad (14.33)$$

Partial transpose acts on the Wigner distribution as momentum reversal on Bob's side and, as a result, the variance matrix undergoes the change $V \rightarrow \tilde{V} = \Lambda' V \Lambda'$. Since $W(\Lambda' \xi)$ has to be a Wigner distribution if the state under consideration is separable, we have

$$\tilde{V} + \frac{i}{2}\Omega \geq 0, \quad \tilde{V} = \Lambda' V \Lambda', \quad \Omega = \begin{pmatrix} \Omega_A & 0 \\ 0 & \Omega_B \end{pmatrix}, \quad (14.34)$$

as a *necessary* condition for separability. Equivalently,

$$V + \frac{i}{2} \tilde{\Omega} \geq 0, \quad \tilde{\Omega} = \Lambda' \Omega \Lambda' = \begin{pmatrix} \Omega_A & 0 \\ 0 & -\Omega_B \end{pmatrix}, \quad (14.35)$$

so that separability of $\hat{\rho}$ implies the additional restriction

$$\begin{aligned} \langle (\Delta \hat{X}(d))^2 \rangle + \langle (\Delta \hat{X}(d'))^2 \rangle &\geq |d'^T \tilde{\Omega} d| \\ &= |d_A^T \Omega_A d'_A - d_B^T \Omega_B d'_B|. \end{aligned} \quad (14.36)$$

Combining this partial transposed uncertainty principle with the original (14.33) we have

$$\langle (\Delta \hat{X}(d))^2 \rangle + \langle (\Delta \hat{X}(d'))^2 \rangle \geq |d_A^T \Omega_A d'_A| + |d_B^T \Omega_B d'_B|, \quad (14.37)$$

$$\forall d, d' \in \mathcal{R}^{2n}.$$

This restriction, to be obeyed by all PPT states, is generically stronger than the usual uncertainty principle (14.33). For instance, let $\hat{X}(d)$ commute with $\hat{X}(d')$, i.e., let $d^T \Omega d' = 0$. What our result shows is that if the state is PPT, then $\hat{X}(d)$ and $\hat{X}(d')$ cannot both have arbitrarily small uncertainties unless $d^T \tilde{\Omega} d' = 0$ as well, i.e., unless $d_A^T \Omega_A d_A$ and $d_B^T \Omega_B d_B$ vanish individually.

An example in the $1+1$ case may help. The two operators $\hat{X} = \hat{x}_1 + \hat{p}_1 + \hat{x}_2 + \hat{p}_2$, $\hat{Y} = \hat{x}_1 - \hat{p}_1 - \hat{x}_2 + \hat{p}_2$ commute, but the sum of their uncertainties in any PPT state has to be ≥ 4 .

6. TWO-MODE SYSTEMS

In this case wherein Alice and Bob hold a single mode each, the set of all homogeneous real linear canonical transformations constitute the ten-parameter real symplectic group $Sp(4, R)$, and Ω and $\tilde{\Omega}$ become

$$\Omega = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}, \quad \tilde{\Omega} = \begin{pmatrix} J & 0 \\ 0 & -J \end{pmatrix}. \quad (14.38)$$

The variance matrix can be written in the block form

$$V = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}. \quad (14.39)$$

Separability of a state is not affected by *local transformations* which act independently on the Hilbert spaces of Alice's and Bob's subsystems. Of particular interest in the present case is the unitary metaplectic action of the six-parameter $Sp(2, R) \otimes Sp(2, R)$ subgroup of $Sp(4, R)$ corresponding to independent *local linear canonical transformations* on the subsystems of Alice and Bob:

$$\begin{aligned} S_{\text{local}} &\in Sp(2, R) \otimes Sp(2, R) \subset Sp(4, R) : \\ S_{\text{local}} &= \begin{pmatrix} S_1 & 0 \\ 0 & S_2 \end{pmatrix}, \quad S_1 JS_1^T = J = S_2 JS_2^T. \end{aligned} \quad (14.40)$$

It is possible and desirable to cast the stronger uncertainty principle (14.37) for separable states in an $Sp(2, R) \otimes Sp(2, R)$ invariant form.

The congruence $V \rightarrow S_{\text{local}} V S_{\text{local}}^T$ by the local group changes the blocks of V in the following manner:

$$A \rightarrow S_1 A S_1^T, \quad B \rightarrow S_2 B S_2^T, \quad C \rightarrow S_1 C S_2^T.$$

Thus, the $Sp(2, R) \otimes Sp(2, R)$ invariants associated with V are $I_1 = \det A$, $I_2 = \det B$, $I_3 = \det C$, and $I_4 = \text{tr}(AJCJBJC^TJ)$ [$\det V$ is an obvious invariant, but it is a function of the I_k 's, namely $\det V = I_1 I_2 + I_3^2 - I_4$].

It turns out that the (matrix) uncertainty inequality $V + \frac{i}{2}\Omega \geq 0$ is equivalent, in the two-mode case, to the $Sp(2, R) \otimes Sp(2, R)$ invariant (scalar) inequality

$$\begin{aligned} \det A \det B + \left(\frac{1}{4} - \det C \right)^2 &- \text{tr}(AJCJBJC^TJ) \\ &\geq \frac{1}{4}(\det A + \det B). \end{aligned} \quad (14.41)$$

To prove this result, first note that the two inequalities are equivalent for variance matrices of the special form

$$V_0 = \begin{pmatrix} a & 0 & c_1 & 0 \\ 0 & a & 0 & c_2 \\ c_1 & 0 & b & 0 \\ 0 & c_2 & 0 & b \end{pmatrix}. \quad (14.42)$$

But any variance matrix can be brought to this special form by effecting a suitable local canonical transformation corresponding to some element of $Sp(2, R) \times Sp(2, R)$. In view of the manifest $Sp(2, R) \otimes Sp(2, R)$ invariant structure of (14.41), it follows that the two inequalities are indeed equivalent for all two-mode variance matrices.

Under partial transpose or momentum reversal on Bob's side represented by the phase space mirror reflectin $\Lambda' = \text{Id} \oplus \sigma_3$, we have $V \rightarrow \tilde{V} = \Lambda' V \Lambda'$. That is, $C \rightarrow C\sigma_3$ and $B \rightarrow \sigma_3 B \sigma_3$, while A remains unchanged [σ_3 is the diagonal Pauli matrix: $\sigma_3 = \text{diag}(1, -1)$]. As a consequence, $I_3 = \det C$ flips signature while I_1, I_2 and I_4 remain unchanged. Thus, condition (14.34) for \tilde{V} takes a form identical to (14.41) with only the signature in front of $\det C$ in the second term on the left hand side reversed. Thus the PPT requirement that the variance matrix of a separable state has to obey $\Lambda' V \Lambda' + \frac{i}{2}\Omega \geq 0$ inaddition to the fundamental uncertainty principle $V + \frac{i}{2}\Omega \geq 0$, takes the form

$$\begin{aligned} \det A \det B + \left(\frac{1}{4} - |\det C| \right)^2 &- \text{tr}(AJCJBJC^TJ) \\ &\geq \frac{1}{4}(\det A + \det B). \end{aligned} \quad (14.43)$$

This is the final form of the implication of PPT on the variance matrix of a two-mode bipartite state. This condition is invariant not only under phase space mirror reflection (partial transpose) Λ' , but also under $Sp(2, R) \otimes Sp(2, R)$, as it should be! It constitutes a *complete description* of the implication PPT has for the second moments of *any* state.

For the standard form V_0 , our condition (14.43) reads

$$4(ab - c_1^2)(ab - c_2^2) \geq (a^2 + b^2) + 2|c_1 c_2| - 1/4. \quad (14.44)$$

But the point is that the separability (PPT) check (14.43) can be applied directly on V , with no need to transform it to the special form V_0 .

To summarise, conditions (14.33), (14.41), and $V + \frac{i}{2}\Omega \geq 0$ are equivalent statements of the fundamental uncertainty principle, and hence will be satisfied by every physical state. The mutually equivalent statements (14.37), (14.43), and (14.34) constitute the PPT criterion at the level of the second moments, and should necessarily be satisfied by every separable state, Gaussian or otherwise.

As the reader may anticipate, we can make stronger statements for Gaussian states: separability and PPT become *equivalent* in the two-mode Gaussian case. To this end, note that states with $\det C \geq 0$ definitely satisfy the PPT condition (14.43), which in this case is subsumed by the physical condition (14.41). We will begin by establishing that such Gaussian states are indeed separable.

Lemma: Gaussian states with $\det C \geq 0$ are separable.

Proof: First consider the case $\det C > 0$. We can arrange $a \geq b$, $c_1 \geq c_2 > 0$ in the special form V_0 in (14.42). Let us do a local canonical transformation $S_{\text{local}} = \text{diag}(x, x^{-1}, x^{-1}, x)$, corresponding to reciprocal local scalings (squeezings) at the Alice and Bob ends, and follow it by $S'_{\text{local}} = \text{diag}(y, y^{-1}, y, y^{-1})$, corresponding to common local scalings at these ends. We have, as a result,

$$V_0 \rightarrow V'_0 = \begin{pmatrix} y^2 x^2 a & 0 & y^2 c_1 & 0 \\ 0 & y^{-2} x^{-2} a & 0 & y^{-2} c_2 \\ y^2 c_1 & 0 & y^2 x^{-2} b & 0 \\ 0 & y^{-2} c_2 & 0 & y^{-2} x^2 b \end{pmatrix}. \quad (14.45)$$

Choose x such that $c_1/(x^2 a - x^{-2} b) = c_2/(x^{-2} a - x^2 b)$. That is, $x = [(c_1 a + c_2 b)/(c_2 a + c_1 b)]^{1/4}$. With this choice, V'_0 acquires such a structure that it can be diagonalized by rotation through *equal* amounts in the q_1, q_2 and

p_1, p_2 planes:

$$V'_0 \rightarrow V''_0 = \text{diag}(\kappa_+, \kappa'_+, \kappa_-, \kappa'_-); \quad (14.46)$$

$$\kappa_{\pm} = \frac{1}{2}y^2 \left\{ x^2a + x^{-2}b \pm [(x^2a - x^{-2}b)^2 + 4c_1^2]^{1/2} \right\}, \quad (14.47)$$

$$\kappa'_{\pm} = \frac{1}{2}y^{-2} \left\{ x^{-2}a + x^2b \pm [(x^{-2}a - x^2b)^2 + 4c_2^2]^{1/2} \right\}. \quad (14.48)$$

Such an equal rotation is a canonical transformation; and therefore V''_0 is a valid variance matrix. For our diagonal V''_0 , the uncertainty principle $V''_0 + \frac{i}{2}\Omega \geq 0$ simply reads that the product $\kappa_- \kappa'_- \geq 1/4$ (and subsumes $\kappa_+ \kappa'_+ \geq 1/4$). It follows that we can choose y such that $\kappa_-, \kappa'_- \geq 1/2$ (for instance, choose y so as to render $\kappa_- = \kappa'_-$). Then $V''_0 \geq 1/2 \text{Id}_4$, where Id_4 is the four-dimensional unit matrix. Since V'_0 and V''_0 are rotationally related, this implies $V'_0 \geq 1/2 \text{Id}_4$. Hence we conclude, by Proposition 4, that the Gaussian state corresponding to V'_0 is separable. This in turn implies that the original V corresponds to a separable state, since V and V'_0 are related by local transformation. This completes proof for the case $\det C > 0$.

Now suppose $\det C = 0$, so that in V_0 we have $c_1 \geq 0 = c_2$. Carry out a local scaling corresponding to $S_{\text{local}} = \text{diag}(\sqrt{2a}, 1/\sqrt{2a}, \sqrt{2b}, 1/\sqrt{2b})$, taking $V_0 \rightarrow V'_0$; the diagonal entries of V'_0 are $(2a^2, 1/2, 2b^2, 1/2)$, and the two nonzero off diagonal entries equal $2abc_1$. With this form for V'_0 , the uncertainty principle $V'_0 + \frac{i}{2}\Omega \geq 0$ implies $V'_0 \geq 1/2 \text{Id}_4$, establishing separability of the Gaussian state. This completes proof of our Lemma.

The main separability theorem for Gaussian states is an immediate consequence of the Lemma, as we shall demonstrate.

Theorem: Positivity under partial transpose is necessary and sufficient condition for separability, for all $1 + 1$ bipartite Gaussian states.

Proof: We consider in turn the two distinct cases $\det C < 0$ and $\det C \geq 0$. Suppose $\det C < 0$. Then there are two possibilities. If (14.33) [or (14.34)] is violated, then the Gaussian state is definitely entangled since (14.33) is a necessary condition for separability. If (14.33) is respected, then the mirror reflected state is a physical Gaussian state with $\det C > 0$ (recall that mirror reflection flips the signature of $\det C$), and is separable by the above lemma. This implies separability of the original state, since a mirror reflected separable state is separable. Finally, suppose $\det C \geq 0$. Condition (14.33) is definitely satisfied since it is subsumed by the uncertainty principle $V + \frac{i}{2}\Omega \geq 0$ in the $\det C \geq 0$ case. By our lemma, the state is separable. This completes proof of the theorem.

7. BOUND ENTANGLED GAUSSIAN STATES

The considerations of Ref. [11] detailed above were restricted to the bipartite situation wherein the subsystems of Alice and Bob consist of a single mode each, the principal result being that there is no bound entangled Gaussian state in the $1 + 1$ case. A rather remarkable work of Werner and Wolf [12] goes beyond the $1 + 1$ case to establish two important results. Introducing the notion of *minimal PPT*, they show that the principal result of Ref. [11] presented as the above theorem implies that there exists no bound entangled Gaussian state in the $1 + N$ case either.

More importantly, they present example of a bound entangled Gaussian state in the $2 + 2$ case. The noise matrix of their example has a simple structure:

$$V = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 4 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 2 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix} \quad (14.49)$$

Their proof that this Gaussian state is PPT, and that it is not separable, is distinguished by effective use of symmetry arguments.

To conclude, we note that a recent work of Giedke et. al. [23] formulates a necessary and sufficient condition for separability of Gaussian states of bipartite systems of arbitrary number of modes. These authors show that all bipartite Gaussian states with nonpositive partial transpose are distillable.

References

- [1] L. Vaidman, Phys. Rev. A **49**, 1473 (1994); L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999).
- [2] A. S. Parkins and H. J. Kimble, quant-ph/9904062; quant-ph/9907049; quant-ph/9909021.
- [3] S. L. Braunstein, Nature **394**, 47 (1998); quant-ph/9904002; S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999)..
- [4] G. J. Milburn and S. L. Braunstein, quant-ph/9812018.
- [5] P. van Loock, S. L. Braunstein, and H. J. Kimble, quant-ph/9902030; P. van Loock and S. L. Braunstein, quant-ph/9906021; quant-ph/9906075.
- [6] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **88**, 869 91998).

- [7] A. Furusawa et al., *Science* **282**, 706 (1998).
- [8] C. H. Bennett, *Phys. Today* **48**, 24 (1995);
D. P. DiVincenzo, *Science* **270**, 255 (1995).
- [9] A. Peres, *Phys. Rev. Lett.* **77**, 1413 (1996).
- [10] P. Horodecki, *Phys. Lett. A* **232**, 333 (1997).
- [11] R. Simon, *Phys. Rev. Lett.* **84**, 2726 (2000).
- [12] R.F. Werner and M.M. Wolf, *Phys. Rev. Lett.* **86**, 3658 (2001).
- [13] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **84**, 2722 (2000).
- [14] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **84**, 4002 (2000).
- [15] R. Simon, E. C. G. Sudarshan, and N. Mukunda, *Phys. Rev. A* **36**, 3868 (1987).
- [16] R. Simon and N. Mukunda, in *Symmetries in Science V*, Ed. B. Gruber (Plenum, NY, 1993), p. 659–689.
- [17] R. Simon and N. Mukunda, *Phys. Rev. Lett.* **70**, 880 (1993).
- [18] E. P. Wigner, *Phys. Rev.* **40**, 749 (1932); R. G. Littlejohn, *Phys. Rep.* **138**, 193 (1986).
- [19] R. Hudson, *Rep. Math. Phys.* **6**, 249 (1975).
- [20] R. Simon, E. C. G. Sudarshan, and N. Mukunda, *Phys. Rev. A* **37**, 3028 (1988).
- [21] J. Williamson, *Am. J. Math.* **58**, 141 (1936). See also V.I. Arnold, *Mathematical Methods of Classical Mechanics* (Springer-Verlag, NY, 1978), Appendix 6.
- [22] R. Simon, N. Mukunda, and B. Dutta, *Phys. Rev. A* **49**, 1567 (1994).
- [23] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, *Phys. Rev. Lett.* **84**, 176904 (2001).

Chapter 15

DISTILLABILITY AND ENTANGLEMENT PURIFICATION FOR GAUSSIAN STATES

Géza Giedke,^{1,2} Lu-Ming Duan,^{1,3} J. Ignacio Cirac^{1,2} and Peter Zoller¹

¹*Institute for Theoretical Physics*

University of Innsbruck, Innsbruck, Austria

²*Max-Planck Institute for Quantum Optics*

Garching, Germany

³*Institute for Quantum Information*

Caltech, CA 91125, USA

geza.giedke@mpq.mpg.de

Abstract We review the concepts of distillability and entanglement purification. We prove that all inseparable Gaussian two-mode continuous variable states are distillable. We present a entanglement purification protocol for Gaussian states and discuss a quantum optical implementation of this protocol.

1. ENTANGLEMENT PURIFICATION

Entanglement (cf. Ch. II.7) is one of the most striking and characteristic features of quantum mechanics. In quantum communication it is also a valuable *resource*: it is necessary for many applications such as quantum teleportation [1] or quantum cryptography[2], and is typically used up in those processes. Ideally, the communicating parties A(lice) and B(ob) share maximally entangled states, which enable them to perfectly implement the desired protocols. In reality, however, due to loss and decoherence in the channel connecting A and B, it is only possible to generate mixed, partially entangled states between distant locations, which are often not directly useful for the task at hand. A way to overcome this problem is offered by *entanglement purification* or *distillation* [3, 4, 5], which describes the process of obtaining at least one maximally entangled state out of many partially entangled ones. In general, any sequence of *local quantum operations* (possibly correlated by *classical communication*) that allows A and B to transform a (sufficiently large) number of entangled states

ρ into at least one pure maximally entangled state comprises an entanglement purification protocol (EPP). EPPs establish the feasibility of quantum communication in a realistic setting; in particular, combining quantum teleportation and entanglement purification in the *quantum repeater protocol* [6] allows for efficient quantum communication through noisy channels over arbitrary distances. Thus EPPs play as important a role for quantum communication as do quantum error correcting codes (QECC) for quantum computing. Indeed, there is a close connection between QECCs and EPPs [4].

Unfortunately, it is currently not known, in general, which mixed states ρ can be distilled in this manner. At the moment we only have conditions that are either necessary or sufficient for *distillability*, but not both. First, obviously the state ρ must be inseparable (entangled) for it to be distillable. Moreover, there exists a stronger *necessary* condition, namely that ρ must have non-positive partial transpose [7]. Surprisingly enough, there are entangled states which cannot be transformed into maximally entangled states at all (i.e. which are *undistillable*) since their density matrices remain positive under partial transposition [8]; these states are also called *bound entangled*. Bound entanglement has been found in bipartite systems of dimension $N > 6$ [9] and also in continuous variable (CV) systems [10, 19]. There is evidence that this condition is in general not sufficient, since there seem to exist states that have non-positive partial transpose but that nevertheless are not distillable [11]. On the other hand, a useful *sufficient* condition for $N \times N$ systems, the so-called *reduction criterion*, has been established [12]. It states that if there exists some vector $|\psi\rangle$ such that

$$\langle\psi|(\text{tr}_B\rho\otimes\mathbb{1}-\rho)|\psi\rangle < 0. \quad (15.1)$$

then the state ρ is distillable. Here, tr_B stands for the partial trace with respect to the second subsystem. An important aspect of this criterion is that if one can find a state $|\psi\rangle$ satisfying (15.1), then one can explicitly construct a protocol to distill ρ [12].

The question of distillability of general CV states is a formidable task that we do not attempt to tackle here. Rather we consider in the remainder of this chapter a simple but important class of CV states, namely *Gaussian states* of two modes. There are several reasons to focus on these states. First, most of the CV states that can currently be prepared in the lab are Gaussian states [13]. Second, important CV quantum communication protocols are based on Gaussian states (teleportation [14, 15], cryptography [16]), and finally, Gaussian states are mathematically well understood, e.g., there exists an inseparability criterion. Thus the largest set of potentially distillable states is easily characterized. In the next section we will show that indeed *all* inseparable two-mode Gaussian states can be distilled.

2. GAUSSIAN STATES

We consider states that are defined on the Hilbert space $L^2(\mathbb{R})$ (or N copies thereof: $L^2(\mathbb{R})^{\otimes N} \equiv L^2(\mathbb{R}^N)$), that is, e.g., states of one or more modes of the electromagnetic field. (We will in the following often use quantum optical terms, like ‘‘modes’’ or ‘‘beam splitters’’, because quantum optics currently offers the most promising setting for the realization of CV systems; this does not limit the presented results to quantum optical systems.)

General definitions For such systems, it is convenient to describe the state ρ by its characteristic function [17, 18]

$$\chi(\xi) = \text{tr}[\rho W(\xi)]. \quad (15.2)$$

Here $\xi = (q_1, \dots, q_N, p_1, \dots, p_N) \in \mathbb{R}^{2N}$ is a real vector and

$$W(\xi) = e^{-i \sum_{k=1}^N (q_k R_k + p_k R_{k+N})}, \quad (15.3)$$

where R_k are the canonical operators of the k th system, respectively, $X_k = R_k$, $P_k = R_{k+N}$, satisfying commutation relations $[R_k, R_l] = -iJ_{kl}\mathbb{1}$ ($\hbar = 1$), where J_{kl} are the entries of the $2N \times 2N$ matrix J defined by $J(q_1, \dots, q_N, p_1, \dots, p_N)^T = (-p_1, \dots, -p_N, q_1, \dots, q_N)^T$. $W(\xi)$ is called the Weyl operator [and is identical to the quantum optical displacement operator $D(\alpha)$ for $\alpha = (p_1 - iq_1, \dots, p_N - iq_N)$].

For a general density operator ρ we define (following [19]) the *mean* or displacement as the vector d

$$d_k = \text{tr}(\rho R_k)$$

and the *covariance* (or *correlation*) *matrix* M by

$$M_{kl} = 2\text{tr}[\rho(R_k - d_k\mathbb{1})(R_l - d_l\mathbb{1})] + iJ_{kl}. \quad (15.4)$$

The characteristic function contains all the information about the state (see e.g., [17, 18]), that is, one can find ρ starting from χ .

The *Gaussian states* are exactly those for which χ is a Gaussian function of ξ [20]

$$\chi(\xi) = e^{-\frac{1}{4}\xi^T M \xi + id^T \xi}, \quad (15.5)$$

i.e., a Gaussian state is fully characterized by the correlation matrix M and the displacement vector d .

Not all $2N \times 2N$ matrices are allowed, since the characteristic function must correspond to the density operator of a physical state, i.e., to a positive operator. It has been shown [20, 19] that a given correlation matrix M corresponds to a physical state if and only if (iff) $M > 0$ and

$$M - iJ \geq 0 \quad (15.6)$$

Quasifree transformations There is an important set of unitary transformations intimately related to Gaussian states: the so called *quasifree* or linear Bogoliubov transformations. They map a state with characteristic function χ to one with $\tilde{\chi}$ defined by $\tilde{\chi}(\xi) = \chi(S\xi + d)$ where S is a symplectic¹ $2N \times 2N$ matrix and d a real vector in \mathbb{R}^{2N} . Clearly, Gaussian states are mapped to Gaussian states by quasifree transformations.

Quasifree transformations can be implemented with Hamiltonians that are at most quadratic in the quadrature operators X_k, P_k . For optical fields this means that they can be performed with beam splitters, phase shifters and squeezers, i.e., currently available technology.

Gaussian states of two modes Any Gaussian state of two modes can be transformed into what we called the *standard form*, using local quasifree transformations (LQT) only [21, 22]. For a state in standard form the corresponding characteristic function has displacement $d = 0$ and the correlation matrix M has the simple form

$$M = \begin{pmatrix} M_A & M_{AB} \\ M_{AB}^T & M_B \end{pmatrix}, \quad (15.7)$$

where the block matrices are diagonal; and M_a, M_b proportional to the identity:

$$M_A = \begin{pmatrix} n_a & 0 \\ 0 & n_a \end{pmatrix}, M_B = \begin{pmatrix} n_b & 0 \\ 0 & n_b \end{pmatrix}, M_{AB} = \begin{pmatrix} k_x & 0 \\ 0 & k_p \end{pmatrix}. \quad (15.8)$$

The four real parameters (n_a, n_b, k_x, k_p) fully characterize a Gaussian state up to LQTs. They can be easily calculated from the LQT-invariants $|M_A|$, $|M_B|$, $|M_{AB}|$ and $|M|$ via:

$$n_a^2 = |M_A|, n_b^2 = |M_B|, k_x k_p = |M_{AB}|, \quad (15.9a)$$

$$(n_a n_b - k_x^2)(n_a n_b - k_p^2) = |M|, \quad (15.9b)$$

where $|M|$ denotes the determinant of M ; without loss of generality we can choose $k_x \geq |k_p|$.

Recall that not all values of these parameters are allowed, since the correlation matrix must be positive and satisfy the condition (15.6). In terms of the parameters (15.9) we can reexpress these conditions as

$$(n_a n_b - k_x^2)(n_a n_b - k_p^2) + 1 \geq n_a^2 + n_b^2 + 2k_x k_p, \quad (15.10a)$$

$$n_a n_b - k_x^2 \geq 1. \quad (15.10b)$$

Inseparability On the other hand, in [22] it was shown that a Gaussian state is entangled iff it does not transform into a proper state under partial transposition. Starting from this result it is easy to show that a Gaussian state is entangled iff the corresponding parameters satisfy [28]

$$(n_a n_b - k_x^2)(n_a n_b - k_p^2) + 1 < n_a^2 + n_b^2 - 2k_x k_p. \quad (15.11)$$

3. DISTILLABILITY OF GAUSSIAN STATES

In the following we present the proof given in [23] that a Gaussian state ρ of two modes is distillable if and only if its parameters fulfill (15.11), that is, iff it is entangled. We will proceed as follows: first, we recall the proof of the reduction criterion in [12] and extend the result to infinite dimensions, providing a sufficient condition for distillability of CV states. Secondly, we show for *symmetric* Gaussian states, i.e. states for which $n_a = n_b = n$, that the inseparability criterion (15.11) is equivalent to the reduction criterion. Thus all symmetric inseparable states are distillable. Finally, we show that all the states which are not symmetric ($n_a \neq n_b$) can be brought into a symmetric form by using local operations maintaining inseparability and thus distillability.

We start by reviewing the proof of the reduction criterion for distillability and generalizing it to infinite dimensions.

3.1 THE REDUCTION CRITERION

For N -level systems Let a density matrix ρ and the pure state $|\psi\rangle = \sum_{n,m} a_{nm} |n\rangle \otimes |m\rangle$ fulfill the condition (15.1), where the vectors $|n\rangle$ form an orthonormal basis. The coefficients a_{nm} define a matrix $A = (a_{nm})$ satisfying $AA^\dagger = \text{tr}_B(|\psi\rangle\langle\psi|)$. Distillation of ρ is divided into three steps.

(i) The first is a filtering operation: The operator $AA^\dagger \otimes \mathbb{1}$ can be viewed as an element of a positive-operator-valued measure (POVM), which defines a generalized measurement [24]. Conditional on the measurement outcome corresponding to $AA^\dagger \otimes \mathbb{1}$ we obtain the state

$$\tilde{\rho} = A^\dagger \otimes \mathbb{1} \rho A \otimes \mathbb{1} / \text{tr}(\rho A A^\dagger \otimes \mathbb{1}), \quad (15.12)$$

which still satisfies (15.1) but now with $|\psi\rangle = |\Phi_+^N\rangle := \frac{1}{\sqrt{N}} \sum_{k=1}^N |k, k\rangle$, the symmetric maximally entangled state of two N -level systems. In this case, (15.1) implies $\text{tr}(\tilde{\rho} |\Phi_+^N\rangle\langle\Phi_+^N|) > 1/N$.

A state satisfying this inequality can be distilled by a generalization of the protocol of Ref. [3], which consists of two steps: depolarization and joint measurements.

(ii) Applying an operation of the form $U \otimes U^*$ (U a randomly chosen unitary) depolarizes $\tilde{\rho}$, i.e. transforms it into a mixture of the maximally entangled state $|\Phi_+^N\rangle$ (which is invariant under transformations of the form $U \otimes U^*$) and the

completely mixed state $\frac{1}{N^2} \mathbb{1}$; the overlap of ρ with $|\Phi_+^N\rangle$ remains unchanged. (iii) Taking two entangled pairs in this depolarized form, both A and B perform the generalized XOR gate $\text{XOR}_N : |k\rangle|l\rangle \mapsto |k\rangle|(l+k)\text{mod}N\rangle$ on their respective systems. Then both measure the state of their second system in the basis $|k\rangle$. The first pair is kept, if they get the same result otherwise it is discarded (as the second pair always is). The resulting state has a density matrix ρ' , which has a larger overlap with the maximally entangled state $|\Phi_+^N\rangle$ than the original ρ . Iterating the last two steps sufficiently often, the overlap between the resulting state and $|\Phi_+^N\rangle$ approaches 1, that is, the distilled state converges to the maximally entangled state $|\Phi_+\rangle$.

For infinite dimensional systems That distillability is implied by Ineq. (15.1) was proved in [12] for finite dimensional systems; to apply this condition to CV states we have to extend the proof to $\dim\mathcal{H} = \infty$.

Let $\{|k\rangle : k = 0, 1, \dots\}$ be an orthonormal basis of \mathcal{H} , let $\mathcal{H}_n = \text{span}\{|0\rangle, |1\rangle, \dots, |n\rangle\}$, and let ρ be a density matrix on $\mathcal{H} \otimes \mathcal{H}$. Assume that $\exists |\psi\rangle \in \mathcal{H}, \epsilon > 0$ such that $\langle\psi|(\text{tr}_B \rho \otimes \mathbb{1} - \rho)|\psi\rangle \leq -\epsilon < 0$. Since $\rho_n = P_{\mathcal{H}_n} \rho P_{\mathcal{H}_n}$ converges to ρ (e.g. in the weak operator topology), there is $N \geq 0$ such that $\langle\psi|(\text{tr}_B \rho_n \otimes \mathbb{1} - \rho_n)|\psi\rangle \leq -\epsilon/2$ for all $n \geq N$. Thus ρ can be projected by local operations to a distillable state ρ_N and is therefore itself distillable. ■

3.2 DISTILLABILITY OF GAUSSIAN STATES

If both the states ρ and ψ occurring in (15.1) are Gaussian with displacements $d_\rho = d_\psi = 0$ and correlation matrices M_ρ, M_ψ respectively, then (15.1) takes the form [25] ($|M|$ denotes the determinant of M):

$$2[|M_{\text{tr}_B \rho} + M_{\text{tr}_B \psi}|]^{-1/2} - 4[|M_\rho + M_\psi|]^{-1/2} < 0. \quad (15.13)$$

Let ρ be a symmetric Gaussian state in standard form and ψ the pure two-mode squeezed state $|\psi\rangle = \frac{1}{\cosh r} \sum_n \tanh^n r |nn\rangle$. This is itself a Gaussian state and the four parameters (15.9) are $n_a = n_b = \cosh r, k_x = -k_p = \sinh r$. In the limit of large r (keeping only the leading terms in e^r) Ineq. (15.13) becomes after some simple algebra

$$(n + k_x)(n - k_p) > 1. \quad (15.14)$$

But Ineq. (15.14) is – for symmetric states – implied by the inseparability criterion: in that case, (15.11) simplifies to $|n^2 - k_x k_p - 1| < n(k_x - k_p)$, which implies Ineq. (15.14), proving that all symmetric inseparable Gaussian states are distillable.

If the state is not symmetric, it means that the reduced state at one of the two sides has larger entropy than the other. This suggests to let a pure state interact with the “hotter” side to cool it down. To do this without destroying the

entanglement of ρ , we proceed as follows: ρ is transformed such that the correlation matrix of its *Wigner function* takes on its standard form with parameters (N_a, N_b, K_x, K_p) . The Wigner function is the symplectic Fourier transform of the characteristic function (15.5) and therefore also Gaussian for Gaussian states. The *Wigner correlation matrix* M_W is related to the (characteristic) correlation matrix by $M_W = -JM^{-1}J$ [26]. One can formulate the conditions (15.10,15.11) similarly in terms of the parameters (N_a, N_b, K_x, K_p) , which are related to the parameters of χ by

$$(N_a, N_b, K_x, K_p) = (n_b, n_a, -k_p, -k_x)/\sqrt{|M|}.$$

A state in the standard form (15.8) can be brought into the Wigner standard form by local squeezing operations.

Now assume that $N_b < N_a$, i.e., B is the hotter side. B takes an ancilla mode in the vacuum state and couples it to its mode using a beam splitter with transmittivity $\cos^2 \theta$. After a homodyne measurement of the ancilla results a state $\tilde{\rho}$ with Wigner correlation matrix \tilde{M} with²

$$\tilde{M}_A = \frac{1}{\nu} \begin{pmatrix} c^2 N_a + s^2 D_x & 0 \\ 0 & c^2 N_a + s^2 N_a N_b \end{pmatrix},$$

$$\tilde{M}_B = \frac{1}{\nu} \begin{pmatrix} N_b & 0 \\ 0 & (c^2 N_b + s^2) \nu \end{pmatrix},$$

$$\tilde{M}_{AB} = \frac{1}{\nu} \begin{pmatrix} c K_x & 0 \\ 0 & c K_p \nu \end{pmatrix},$$

where the abbreviations $c = \cos \theta$, $s = \sin \theta$, $\nu = s^2 N_b + c^2$, and $D_{x,p} = N_a N_b - K_{x,p}^2$ were used. Symmetry, i.e. $|\tilde{M}_A| = |\tilde{M}_B|$, requires

$$\tan^2 \theta = \frac{N_a^2 - N_b^2}{N_b - D_x N_a}. \quad (15.15)$$

Checking (15.11) for \tilde{M} one easily sees that the sign of the left-hand side does not change; therefore the transformed state is inseparable iff the original one was inseparable. It remains to be shown that there always exists a θ to satisfy (15.15), i.e., that the right hand side of Eq. (15.15) is positive. The numerator is positive since $N_b < N_a$, the denominator is positive for all states since the second part of condition (15.10) implies that $(N_a - D_x N_b) > 0$ and the first part assures that $(N_a - D_x N_b)(N_b - D_p N_a) \geq (N_a K_x + N_b K_p)^2 \geq 0$, hence all Gaussian states can be symmetrized this way. But since every Gaussian state can be brought into Wigner standard form by local unitaries, this completes the proof. ■

This implies that the protocol of Ref. [12] can in principle be used to obtain maximally entangled states in a finite dimensional Hilbert space from any given inseparable Gaussian two-mode state.

Before discussing EPPs in more detail in the following, we end this section on distillability by mentioning an interesting recent result. The equivalence of inseparability and distillability of Gaussian states holds only for the case of two modes. Werner and Wolf showed in [19] that if both A and B possess more than one mode, there exist Gaussian states that are *bound entangled*, namely states that are entangled but whose density matrices remain positive under partial transposition. In later work [23] it was shown that for any number of modes bipartite Gaussian states are distillable iff their partial transpose is not positive.

4. ENTANGLEMENT PURIFICATION FOR GAUSSIAN STATES

In this section we discuss some processes that may be used to accomplish entanglement purification.

For qubit systems, efficient entanglement purification protocols have been found [3], but none has so far been realized experimentally due to the great difficulty to perform repeated collective operations in realistic quantum communication systems. Direct extensions of these schemes have been considered for entanglement purification of Gaussian states, but until now none of these extensions has provided an EPP for Gaussian states [27, 28]. Moreover, extensive numerical investigations of local quasifree transformations acting on several pairs of entangled Gaussian states and ancillas have failed to turn up any improvement in entanglement or related properties [28]. In fact, it was shown very recently [35] that it is impossible to distill Gaussian states with LQT and homodyne measurements.

Thus, the discussion should be extended to a larger class of operations to distill entanglement of CV states. In [29] a protocol to increase the entanglement for the special case of pure two-mode squeezed states has been proposed, which is based on conditional photon number subtraction; the efficiency, however, seems to be an obstacle for its practical realization. In the following two subsections we will discuss briefly the EPP for all Gaussian states based on the proof in Sec. 3. and then in detail a more practical protocol [30, 31] that circumvents the major difficulties of the general scheme, and allows to distill entanglement of a subset of (pure and mixed) Gaussian states.

4.1 AN EPP FOR ALL GAUSSIAN STATES

Let us briefly consider how the steps for distillation of an inseparable Gaussian state ρ using (the generalization of) the protocol of Ref. [12] might be accomplished quantum optically.

As usual for EPPs A and B share a large number of identically prepared entangled systems in the known state ρ .

0.) Symmetrization: Remove displacements $d \neq 0$; symmetrize ρ if necessary; bring the symmetric state into standard form. All these steps can be performed by the local use of beam splitters, one-mode squeezers, ancilla systems in coherent states, and a homodyne measurement.

For a state in symmetric standard form the filtering operation (15.12) required in the EPP is unnecessary, since then ρ already satisfies Ineq. (15.1) with the state $|\psi\rangle \propto \lim_{\lambda \rightarrow 1} \sum_k \lambda^k |k\rangle |k\rangle$ (in the photon number basis). This gives $a_{nm} = \lim_{\lambda \rightarrow 1} \lambda^{n+m} \delta_{nm}$, hence $A = (a_{nm}) = \mathbb{1}$.

1.) Depolarization: Transform the state into a mixture of $|\Phi_+^{N+1}\rangle$ and the maximally mixed state $\propto \mathbb{1}$ by applying $U \otimes U^*$ with U randomly chosen. However, the class of currently realizable unitaries is in fact very limited and we do not know how to depolarize an arbitrary state quantum optically.

2.) Joint measurement: This is the central step of the distillation protocol. A bilocal XOR is used to mutually entangle two entangled pairs. A subsequent measurement selects a distilled subensemble.

This operation may be implemented by a measurement of the total photon number $N_\alpha = N_{\alpha 1} + N_{\alpha 2}, \alpha = A, B$ on both sides: The state conditional on both A and B obtaining the same result N differs only by a local unitary transformation (namely $|n, N-n\rangle_\alpha \mapsto |n, N\rangle_\alpha$) from the one obtained by directly following the steps described in Sec. 3., i.e., first projecting bi-locally to the $N+1$ dimensional subspace \mathcal{H}_{N+1} ($\rho \mapsto \rho_{N+1}$), then performing the bi-local XOR _{$N+1$} , and finally measuring the target system with result N^3 . As shown before, for a sufficiently large value of N , the truncated state ρ_{N+1} is distillable and then step 2.) produces a state with larger overlap with the $N+1$ -level maximally entangled state $|\Phi_+^{N+1}\rangle$.

Each iteration of these two steps brings the state closer to a maximally entangled state in the Hilbert space of dimension N , where $(N+1)^2$ is the last result of the total photon number measurement. Hence with finite probability one can get arbitrarily close to a maximally entangled state in any finite dimensional space provided the initial supply of states ρ is sufficiently large.

4.2 A PRACTICAL EPP

In this subsection, we describe the entanglement purification scheme presented in [30, 31], having the following properties: (i) It produces maximally entangled states in a finite dimensional subspace. For a relevant class of states this is accomplished in a single step. (ii) For pure states it reaches the maximal allowed efficiency in the asymptotic limit (when the number of pairs of modes goes to infinity). (iii) It can be readily extended to distill maximally entangled

states from a relevant class of mixed Gaussian states which result from losses in the light transmission. Furthermore, we propose and analyze how to implement this protocol experimentally using high finesse cavities and cross-Kerr nonlinearities. We begin by describing the entanglement purification protocol for pure two-mode squeezed states, and then extend the protocol to include mixed Gaussian CV states, and describe a physical implementation in the next subsection.

For pure states First assume that we have generated m entangled pairs A_i, B_i ($i = 1, 2, \dots, m$) between two distant sides A and B. Each pair of modes A_i, B_i are prepared in the pure two-mode squeezed state $|\Psi\rangle_{A_i B_i}$, which in the number basis has the form

$$|\Psi\rangle_{A_i B_i} = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} \lambda^n |n\rangle_{A_i} |n\rangle_{B_i}, \quad (15.16)$$

where $\lambda = \tanh(r)$, and r is the squeezing parameter [18]. The entanglement $E(|\Psi\rangle_{A_i B_i})$ of the two-component state (15.16) is uniquely quantified by the von Neumann entropy of the reduced density operator of one subsystem. The joint state $|\Psi\rangle_{(A_i B_i)}$ of the m entangled pairs is simply the product of all the $|\Psi\rangle_{A_i B_i}$, which can be rewritten as

$$|\Psi\rangle_{(A_i B_i)} = (1 - \lambda^2)^{\frac{m}{2}} \sum_{j=0}^{\infty} \lambda^j \sqrt{f_j^{(m)}} |j\rangle_{(A_i B_i)}, \quad (15.17)$$

where $(A_i B_i)$ is abbreviation of the symbol $A_1, B_1, A_2, B_2, \dots$ and A_m, B_m , and the normalized state $|j\rangle_{(A_i B_i)}$ is defined as

$$|j\rangle_{(A_i B_i)} = \frac{1}{\sqrt{f_j^{(m)}}} \sum_{i_1, i_2, \dots, i_m}^{i_1 + i_2 + \dots + i_m = j} |i_1, i_2, \dots, i_m\rangle_{(A_i)} \otimes |i_1, i_2, \dots, i_m\rangle_{(B_i)}. \quad (15.18)$$

The function $f_j^{(m)}$ in Eq. (15.17) and (15.18) is given by $f_j^{(m)} = \frac{(j+m-1)!}{j!(m-1)!}$.

Note that the state $|j\rangle_{(A_i B_i)}$ represents a maximally entangled state in the subspace corresponding to a local photon number of j at both sides. To concentrate the entanglement of these m entangled pairs, we perform a QND measurement of the total photon number $N_{A_1} + N_{A_2} + \dots + N_{A_m}$ on the A side (we will describe later how to implement this measurement experimentally). The QND measurement projects the state $|\Psi\rangle_{(A_i B_i)}$ onto the two-party maximally entangled state $|j\rangle_{(A_i B_i)}$ with probability

$$p_j = (1 - \lambda^2)^m \lambda^{2j} f_j^{(m)}.$$

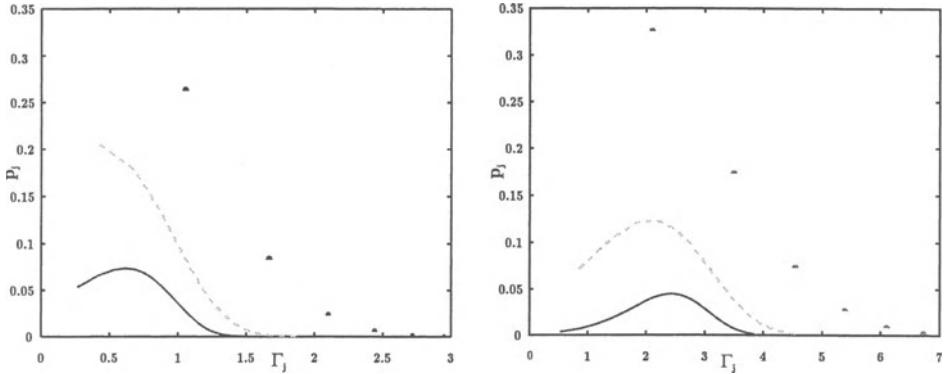


Figure 15.1 The purification success probability versus entanglement increase ratio for two (left) and four (right) pairs. Dotted line for the squeezing parameter $r = 0.5$, dashed line for $r = 1.0$, and solid line for $r = 1.5$.

The entanglement of the resulting state $|j\rangle_{(A_iB_i)}$ is given by $E(|j\rangle_{(A_iB_i)}) = \log f_j^{(m)}$. The quantity

$$\Gamma_j = E(|j\rangle_{(A_iB_i)}) / E(|\Psi\rangle_{A_iB_i})$$

defines the entanglement increase ratio, and if $\Gamma_j > 1$, we get a more entangled state. Even with a small number m , the probability of obtaining a more entangled state is quite high. Figs. 15.1a,b show the probability of achieving an entanglement increase ratio Γ_j for various values of initial entanglement and initial number of pairs.

To measure how efficient the scheme is, we define the entanglement transfer efficiency Υ with the expression

$$\Upsilon = \frac{\sum_{j=0}^{\infty} p_j^{(m)} E(|j\rangle_{(A_iB_i)})}{m E(|\Psi\rangle_{A_iB_i})}. \quad (15.19)$$

It is the ratio of the average entanglement after concentration measurement to the total initial entanglement contained in the m pairs. Obviously, $\Upsilon \leq 1$ should always hold. With the squeezing parameter $r = 0.5, 1.0$ or 1.5 , the entanglement transfer efficiency versus the number of pairs m is shown in Fig. 15.2.

From this figure, we see that the entanglement transfer efficiency is near to 1 for a large number of pairs. In fact, it can be proven that as $m \rightarrow \infty$, we would get with unit probability a maximally entangled state with entanglement $mE(|\Psi\rangle_{A_iB_i})$. To show this, we calculate the mean value and the variance of

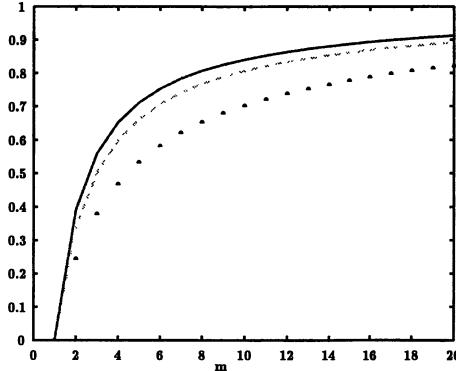


Figure 15.2 The entanglement transfer efficiency versus the number of pairs m in simultaneous concentration. Dotted line for $r = 0.5$, dashed line for $r = 1.0$, and solid line for $r = 1.5$.

the distribution $p_j^{(m)}$, and find

$$\begin{aligned}\bar{j} &= \frac{m\lambda^2}{(1-\lambda^2)}, \\ \overline{(\Delta j)^2} &= \frac{m\lambda^2}{(1-\lambda^2)^2}.\end{aligned}\quad (15.20)$$

The results show that if m tends to infinity, $\sqrt{\overline{(\Delta j)^2}/\bar{j}} \rightarrow 0$ and the distribution $p_j^{(m)}$ tends to a δ -like function. Furthermore, around the mean value \bar{j} , the entanglement of the resulting state $|\bar{j}\rangle_{(A_i B_i)}$ is

$$E(|\bar{j}\rangle_{(A_i B_i)}) \xrightarrow{m \rightarrow \infty} m E(|\Psi\rangle_{A_i B_i}), \quad (15.21)$$

so the entanglement transfer efficiency tends to unity. This proves that the purification method described above is optimal in the asymptotic limit ($m \rightarrow \infty$), analogous to the purification protocol presented in [5] for the qubit case. For any finite number of entangled pairs, this purification protocol is more efficient than that in [5], since it takes advantage of the special relations between the coefficients in the two-mode squeezed state.

An interesting feature of this entanglement purification protocol is that for any measurement outcome $j \neq 0$, we always get a useful maximally entangled state in some finite Hilbert space, though the entanglement of the outcome state $|j\rangle_{(A_i B_i)}$ does not necessarily exceed that of the original state $|\Psi\rangle_{A_i B_i}$ if j is small.

For mixed entangled states In reality, due to unavoidable losses during light transmission, we will not start from an ideal two-mode squeezed state, but

rather from a mixed state described by the following master equation

$$\dot{\rho} = -i \left(H_{\text{eff}} \rho - \rho H_{\text{eff}}^\dagger \right) + \sum_{i=1}^m \left(\eta_A a_{A_i} \rho a_{A_i}^\dagger + \eta_B a_{B_i} \rho a_{B_i}^\dagger \right) \quad (15.22)$$

where ρ is the density operator of the m entangled pairs with $\rho(0) = |\Psi\rangle_{(A_i B_i)} \langle \Psi|$, the pure two-mode squeezed state (15.16), and the effective Hamiltonian

$$H_{\text{eff}} = -i \sum_{i=1}^m \left(\frac{\eta_A}{2} a_{A_i}^\dagger a_{A_i} + \frac{\eta_B}{2} a_{B_i}^\dagger a_{B_i} \right). \quad (15.23)$$

In Eqs. (15.22) and (15.23), a_{α_i} denotes the annihilation operator of the mode α_i , ($\alpha = A$ or B), and we have assumed that the damping rates η_A and η_B are the same for all the m entangled pairs, but η_A and η_B may be different from each other. Eq. (15.22) describes a situation in which single photon absorption is the only relevant source of noise as is typically the case at optical frequencies.

Small Noise In many practical cases, it is reasonable to assume that the light transmission noise is small. Let τ denote the transmission time, then $\eta_A \tau$ and $\eta_B \tau$ are small factors. To the first order in $\eta_A \tau$ and $\eta_B \tau$ the final state of the m entangled pairs is in the language of quantum trajectories [18] either $|\Psi^{(0)}\rangle_{(A_i B_i)} \propto e^{-iH_{\text{eff}}\tau} |\Psi\rangle_{(A_i B_i)}$ (no quantum jumps occurred) or $|\Psi^{(\alpha_i)}\rangle_{(A_i B_i)} \propto \sqrt{\eta_\alpha \tau} a_{\alpha_i} |\Psi\rangle_{(A_i B_i)}$ (a jump occurred in the α_i channel ($\alpha = A, B$ and $i = 1, 2, \dots, m$)). The final density operator is a mixture of all these possible states. To distill entanglement from this mixed state, we perform QND measurements of the total photon number on both sides A and B, with results j_A and j_B , respectively. We then compare j_A and j_B through classical communication (CC), and keep the outcome state if and only if $j_A = j_B$. Let $P_A^{(j)}$ and $P_B^{(j)}$ denote the projections onto the eigenspaces of the corresponding total number operators $\sum_{i=1}^m a_{A_i}^\dagger a_{A_i}$ and $\sum_{i=1}^m a_{B_i}^\dagger a_{B_i}$ with eigenvalue j , respectively. It is easy to show that

$$\begin{aligned} P_A^{(j)} P_B^{(j)} |\Psi^{(0)}\rangle_{(A_i B_i)} &= |j\rangle_{(A_i B_i)}, \\ P_A^{(j)} P_B^{(j)} |\Psi^{(\alpha_i)}\rangle_{(A_i B_i)} &= 0. \end{aligned} \quad (15.24)$$

So if $j_A = j_B = j$, the outcome state is the maximally entangled state $|j\rangle_{(A_i B_i)}$ with entanglement $\log(f_j^{(m)})$. The probability to get the state $|j\rangle_{(A_i B_i)}$ is now given by $p'_j = (1 - \lambda^2)^m \lambda^{2j} f_j^{(m)} e^{-(\eta_A + \eta_B)\tau j}$. It should be noted that the projection operators $P_A^{(j)} P_B^{(j)}$ cannot eliminate the states obtained from the

initial state $|\Psi\rangle_{(A_iB_i)}$ by a quantum jump on each side A and B. The total probability of this kind of quantum jumps is proportional to $m^2\bar{n}^2\eta_A\eta_B\tau^2$. So the condition for small transmission noise requires $m^2\bar{n}^2\eta_A\eta_B\tau^2 \ll 1$, where $\bar{n} = \sinh^2(r)$ is the mean photon number for a single mode.

Asymmetric Noise In the purification of mixed entanglement, we need CC to confirm that the measurement results on both sides are the same, and during this CC, we implicitly assume that the storage noise for the modes is negligible. In fact, that the storage noise is much smaller than the transmission noise is a common assumption made in all the entanglement purification schemes which need the help of repeated CC [3]. If we make this assumption for continuous variable systems, there exists another simple configuration in which the purification protocol works. Let the two-mode squeezed states be generated at side A. After state generation, we keep the modes A_i on side A with a very small storage loss rate η_A , and at the same time the modes B_i are transmitted to the distant side B with a loss rate $\eta_B \gg \eta_A$. We call this a configuration with an asymmetric transmission noise. In this configuration, the purification protocol is exactly the same as that described in the above paragraph. We note that the component in the final mixed density operator which is kept by the projection $P_A^{(j)}P_B^{(j)}$ should be subject to the same times of quantum jumps on each side A and B. We want this component to be a maximally entangled state. This requires that the total probability of the same nonzero number of quantum jumps on both sides to be very small. Clearly, this total probability is always smaller than $\bar{n}\eta_A\tau$, no matter how large the damping rate η_B is. So the working condition of the purification protocol in the asymmetric transmission noise configuration is given by $\bar{n}\eta_A\tau \ll 1$. The loss rate η_B can be large. The probability to obtain the maximally entangled state $|j\rangle_{(A_iB_i)}$ is still given by $p'_j = (1 - \lambda^2)^m \lambda^{2j} f_j^{(m)} e^{-(\eta_A + \eta_B)\tau j}$.

A-posteriori Purification For continuous variable systems the assumption of storage with a very small loss rate is typically unrealistic. In that case, we can use the following simple method to circumvent the storage problem. Note that the purpose of distilling maximally entangled states often is to directly use them in some quantum communication protocol, such as quantum cryptography or quantum teleportation. So we can modify the above purification protocol by the following procedure: immediately after the state generation, we make a QND measurement of the total photon number on side A (measurement result j_A). Then we do *not* store the resulting state on side A, but immediately use it (e.g., perform the corresponding measurement as required by a quantum cryptography protocol [16]). During this process, the modes B_i are being sent to the distant side B, and when they arrive, we make another QND measurement of the modes B_i and get a outcome j_B . The resulting state on side B can be directly used (for quantum cryptography, for instance) if $j_A = j_B$, and

discarded otherwise. By this method, we formally get maximally entangled states through posterior confirmation, and at the same time we need not store the modes on both sides.

4.3 IMPLEMENTATION OF THE EPP

To experimentally implement the above purification scheme, we first have to generate Gaussian entangled states between two distant sides, and then perform a local QND measurement of the total excitation number of several entangled pairs. Here we describe the experimental scheme proposed in [30, 31], which uses high finesse optical cavities to store CV entangled states and cavity enhanced cross-Kerr interactions to realize the local QND measurement.

Gaussian entangled states between two distant cavities can be generated as follows (cf. Fig. 15.3): we transmit and then couple the two outputs of a nondegenerate optical parametric amplifier to distant high finesse cavities. The steady state of the cavities is nothing but a Gaussian continuous entangled state described by the solution of Eq. (15.22) after taking into account the propagation loss [32, 31].

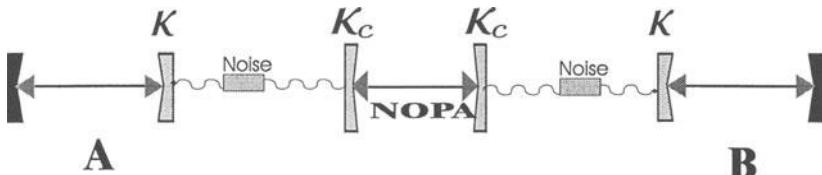


Figure 15.3 Schematic setup for generating Gaussian entangled states between two distant cavities.

The difficult part is to perform a QND measurement of the total photon number contained in several local cavities. We use the setup depicted in Fig. 15.4 to achieve this goal. (For convenience, we use the two-cavity measurement as an example to illustrate the method. Extension of the measurement method to multi-cavity cases is straightforward.)

The measurement model depicted in Fig. 15.4 is an example of a cascaded quantum system [18]. The incident light b_{i1} can be expressed as $b_{i1} = b'_{i1} + g\sqrt{\gamma}$, where $g\sqrt{\gamma}$ (g is a large dimensionless factor) is a constant driving field, and b'_{i1} is the standard vacuum white noise, satisfying $\langle b'^{\dagger}_{i1}(t)b'_{i1}(t') \rangle = 0$ and $\langle b'_{i1}(t)b'^{\dagger}_{i1}(t') \rangle = \delta(t - t')$. The Hamiltonian for the Kerr medium is assumed to be $H_i = \hbar\chi N_i b_i^{\dagger} b_i$, ($i = 1$ or 2), where b_i is the annihilation operator for the ring cavity mode, and χ is the cross-phase modulation coefficient. The self-phase modulation can be made much smaller than the cross-phase modulation with some resonance conditions for the Kerr

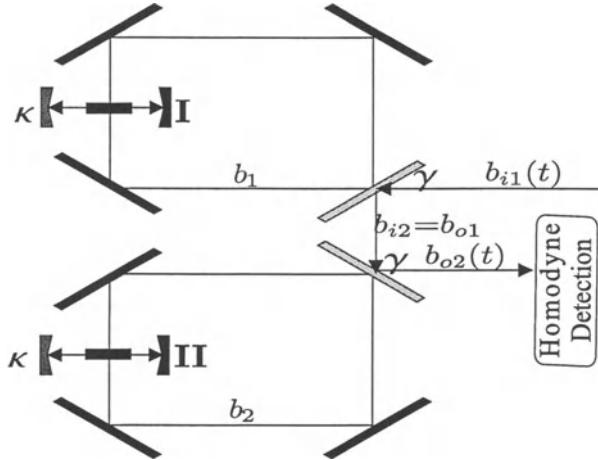


Figure 15.4 Schematic experimental setup to measure the total photon number $N_1 + N_2$ contained in the cavities I and II. The cavities I and II, each with a small damping rate κ and with a cross Kerr medium inside, are put respectively in a bigger ring cavity. The ring cavities with the damping rate γ are used to enhance the cross Kerr interactions. A strong continuous coherent driving light $b_{i1}(t)$ is incident on the first ring cavity, whose output b_{o1} is directed to the second ring cavity. The output $b_{o2}(t)$ of the second ring cavity is continuously observed through a homodyne detection.

medium, and thus is negligible [33, 34]. In the frame rotating at the optical frequency, the Langevin equations describing the dynamics in the two ring cavities have the form

$$\begin{aligned}\dot{b}_1 &= -i\chi N_1 b_1 - \frac{\gamma}{2} b_1 - \sqrt{\gamma} b'_{i1} - g\gamma, \\ \dot{b}_2 &= -i\chi N_2 b_2 - \frac{\gamma}{2} b_2 - \sqrt{\gamma} b_{i2},\end{aligned}\tag{15.25}$$

with the boundary conditions (see Fig. 1) $b_{i2} = b_{o1} = b'_{i1} + g\sqrt{\gamma} + \sqrt{\gamma}b_1$ and $b_{o2} = b_{i2} + \sqrt{\gamma}b_2$. In the realistic case $\gamma \gg \chi \langle N_i \rangle$, ($i = 1, 2$), we can adiabatically eliminate the cavity modes b_i , and express the final output b_{o2} of the second ring cavity as an operator function of the observable $N_1 + N_2$. The experimentally measured quantity is the integration of the homodyne photocurrent over the measurement time T . Choosing the phase of the driving

field so that $g = i|g|$, the measured observable corresponds to the operator

$$\begin{aligned} X_T &= \frac{1}{T} \int_0^T \frac{1}{\sqrt{2}} [b_{o2}(t) + b_{o2}^\dagger(t)] dt \\ &\approx \frac{4\sqrt{2}|g|\chi}{\sqrt{\gamma}} (N_1 + N_2) + \frac{1}{\sqrt{T}} X_T^{(b)}, \end{aligned} \quad (15.26)$$

where $X_T^{(b)} = \frac{1}{\sqrt{2}} (b_T + b_T^\dagger)$, and b_T , satisfying $[b_T, b_T^\dagger] = 1$, is defined by $b_T = \frac{1}{\sqrt{T}} \int_0^T b'_{i1}(t) dt$. Eq. (15.26) assumes $\gamma \gg \chi \langle N_i \rangle$ and $e^{-\gamma T} \ll 1$. There are two different contributions in Eq. (15.26). The first term represents the signal, which is proportional to $N_1 + N_2$, and the second term is the vacuum noise. The distinguishability of this measurement is given by $\delta n = \frac{\sqrt{\gamma}}{8|g|\chi\sqrt{T}}$. If $\delta n < 1$, i.e., if the measuring time $T > \frac{\gamma}{64|g|^2\chi^2}$, we effectively perform a measurement of $N_1 + N_2$; and if T is also smaller than $\frac{1}{\kappa\langle N_i \rangle}$, the photon loss in the cavities I and II during the measurement is negligible. So the setup gives an effective QND measurement of the total photon number operator $N_1 + N_2$ under the condition

$$\frac{\gamma}{64|g|^2\chi^2} < T < \frac{1}{\kappa\langle N_i \rangle}. \quad (15.27)$$

This condition seems to be feasible with the present technology. For example, if we assume the cross-Kerr interaction is provided by the resonantly enhanced Kerr nonlinearity as considered and demonstrated in [33, 34], the Kerr coefficient $\chi/2\pi \sim 0.1\text{MHz}$ would be obtainable⁴. We can choose the decay rates $\kappa/2\pi \sim 4\text{MHz}$ and $\gamma/2\pi \sim 100\text{MHz}$, and let the dimensionless factor $g \sim 100$ (for a cavity with cross area $S \sim 0.5 \times 10^{-4}\text{cm}^2$, $g \sim 100$ corresponds a coherent driving light with intensity about 40mWcm^{-2}). The mean photon number $\langle N_1 \rangle = \langle N_2 \rangle = \sinh^2(r) \sim 1.4$ for a practical squeezing parameter $r \sim 1.0$. With the above parameters, Eq. (15.27) can be easily satisfied if we choose the measuring time $T \sim 8\text{ns}$. More favorable values for the parameters are certainly possible.

To bring the above proposal into a real experiment, there are several imperfections which should be considered. These include phase instability of the driving field, imbalance between the two ring cavities, light absorption in the Kerr medium and the mirrors, self phase modulation effects, light transmission loss between the ring cavities, and inefficiency of the detectors. To realize a QND measurement, the imperfections should be small enough. We have deduced quantitative requirements for all the imperfections listed above [31].

With the parameters given in the above paragraph, all these requirements can be met experimentally.

Acknowledgments

G.G. acknowledges financial support by the German Friedrich-Naumann-Stiftung. This work was supported by the Austrian Science Foundation under the SFB “Control and Measurement of Coherent Quantum Systems” (Project 11), the European Union under the TMR network ERB–FMRX–CT96–0087 and the project EQUIP (contract IST-1999-11053), the European Science Foundation, and the Institute for Quantum Information GmbH, Innsbruck.

Notes

1. S is called symplectic if $S^T JS = J$.
2. See [35] for the general formalism to describe measurements on Gaussian states.
3. To be more precise: this equivalence holds on the infinite dimensional space, when XOR: $|n, m\rangle \mapsto |n, m+n\rangle$. For states in a N dimensional subspace (as obtained after the first step) this equivalence is only true for measurement outcomes $N_\alpha \leq N$
4. In fact, Ref. [33] considered a configuration, yielding a Kerr coefficient $\chi \sim 100\text{MHz}$, to realize a single-photon turnstile device. But the estimation there puts a stringent limit on the required cavity parameters [K. M. Gheri *et al.*, Phys. Rev. A **60**, R2673, 1999]. We take a much more moderate estimation of the relevant parameters and find $\chi/2\pi \sim 0.1\text{MHz}$ is obtainable. This value of the Kerr coefficient is large enough for performing the QND measurement, though it is certainly not enough for realizing a single-photon turnstile device.

References

- [1] Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, Nature **390**, 575, (1997); D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).
- [2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C.H. Bennett, G. Brassard, N. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
- [3] N. Gisin, Phys. Lett. A **210**, 151 (1996); C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
- [4] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Phys. Rev. A **54** 3824 (1996).
- [5] C.H. Bennett, H.J. Bernstein, S. Popescu, B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
- [6] H.-J. Briegel, W. Dür, J.I. Cirac, P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

- [7] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
- [8] P. Horodecki, Phys. Lett. A **232**, 233 (1997).
- [9] M. Lewenstein, D. Bruss, J.I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, R. Tarrach, J. Mod. Opt. **47**, 2481 (2000), quant-ph/0006064.
- [10] P. Horodecki, M. Lewenstein Phys. Rev. Lett. **85**, 2657 (2000).
- [11] W. Dür, J.I. Cirac, M. Lewenstein D. Bruß, Phys. Rev. A **61**, 062313 (2000), quant-ph/9910022; D. DiVincenzo, P. Shor, J. Smolin, B. Terhal, A. Thapliyal, Phys. Rev. A **61**, 062312 (2000), quant-ph/9910026.
- [12] M. Horodecki, P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
- [13] H.-A. Bachor, *A guide to experiments in quantum optics*, Wiley-VCH, Weinheim (1998).
- [14] L. Vaidman, Phys. Rev. A **49**, 1473 (1994); S.L. Braunstein, H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
- [15] A. Furusawa, J. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, E.S. Polzik, Science **282**, 706 (1998).
- [16] T.C. Ralph, Phys. Rev. A **61**, 010303R (2000); M. Hillery, Phys. Rev. A **61**, 022309 (2000); M. Reid, Phys. Rev. A **62**, 062308 (2000), quant-ph/9909030; T.C. Ralph, Phys. Rev. A **62**, 062307 (2000), quant-ph/0007024.
- [17] D. Petz, *An Invitation to the Algebra of Canonical Commutation Relations*, Leuven University Press, Leuven (1990).
- [18] C. Gardiner, P. Zoller, *Quantum Noise* 2nd ed., Springer-Verlag, Berlin (1999).
- [19] R.F. Werner, M.M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001), quant-ph/0009118 (2000).
- [20] J. Manuceau, A. Verbeure, Comm. Math. Phys. **9**, 293 (1968).
- [21] L. Duan, G. Giedke, J.I. Cirac, P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
- [22] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
- [23] G. Giedke, L.-M. Duan, J.I. Cirac, P. Zoller, Quant. Inf. Comp. **1**(3), 79 (2001); quant-ph/0104072 and quant-ph/0007061.
- [24] C. Helstrom, *Quantum detection and estimation theory*, Associate Press, London (1976).
- [25] H. Scutaru, J. Math. Phys. **39**, 6403 (1998).
- [26] H. Scutaru, Phys. Lett. A **141**, 223 (1989).
- [27] S. Parker, S. Bose, M.B. Plenio, Phys. Rev A, **61**, 032305 (1999).
- [28] G. Giedke, PhD Thesis, Universität Innsbruck (2001).

- [29] T. Opatrný, G. Kurizki, D.-G. Welsch, Phys. Rev. A **61**, 032302 (1999).
- [30] L.-M. Duan, G. Giedke, J.I. Cirac, P. Zoller, Phys. Rev. Lett. **84**, 4002 (2000).
- [31] L.-M. Duan, G. Giedke, J.I. Cirac, P. Zoller, Phys. Rev. A **62**, 032304 (2000).
- [32] A. S. Parkins, H. J. Kimble, Phys. Rev. A **61**, 052104 (2000).
- [33] A. Imamoğlu, H. Schmid, G. Woods, M. Deutsch, Phys. Rev. Lett. **79**, 1467 (1997); **81**, 2836 (1998).
- [34] L.V. Hau, S.E. Harris, Z. Dutton, C.H. Behroozi, Nature **397**, 594 (1999).
- [35] G. Giedke and J. I. Cirac, quant-ph/0204085.

Chapter 16

ENTANGLEMENT PURIFICATION VIA ENTANGLEMENT SWAPPING

S. Parker

*Optics Section, The Blackett Laboratory, Imperial College
London, England, SW7 2BW
s.parker@ic.ac.uk*

S. Bose

*Centre for Quantum Computing, Clarendon Laboratory,
University of Oxford, England, OX1 3DU
sougato.bose@qubit.org*

M. B. Plenio

*Optics Section, The Blackett Laboratory, Imperial College
London, England, SW7 2BW
m.plenio@ic.ac.uk*

Abstract In this section we aim to generalize the entanglement swapping procedure to continuous variable systems and show that for certain types of pure continuous variable states this process can increase the amount of entanglement between separated parties i.e. achieve entanglement *purification*. To show this we will need a generalization of the von Neumann entropy - the finite state entanglement measure - to continuous variables together with a numerical procedure for its calculation.

1. INTRODUCTION

The experimental [1, 2, 3, 4] and theoretical [5] realization of teleportation in continuous variable systems has demonstrated that entanglement between separated systems is essential in order to be able to perform teleportation and

that the efficiency of the procedure is strongly dependent on the amount of entanglement therein.

It is therefore important that we are able to quantify the amount of entanglement in these processes and provide procedures to concentrate this entanglement. This problem of concentrating entanglement is more precisely phrased as follows: given an entangled bipartite state shared between two spatially separated parties (Alice and Bob) the aim is to increase the amount of entanglement using only local operations and classical communication [6, 7, 8]. This process is known as *entanglement purification*, and for continuous variable systems was first considered in [9] and investigated further in a number of directions. Many nice results on the distillability of Gaussian states have been obtained [10], including distillability criteria and actual physical implementations of distillation schemes. Also the structure of the entanglement of continuous variable states has been investigated with nice results such as bound entangled states [11].

A significant amount of progress has been made in the purification of discrete systems [6, 7, 12]. An example to be used in this chapter for pure finite level states is entanglement swapping [13], a process very similar to teleportation, which can achieve purification of entanglement from two bipartite systems into just one. In the swapping process one particle from each of two pairs of entangled particles can become entangled without ever having interacted when a joint measurement is performed on the other two particles. This is a probabilistic process dependent on the measurement result, and the entanglement of the first two particles is also probabilistic. On average it cannot increase but for some of the measurement results the entanglement can be more than that of either initial pair. This is one method, therefore, of achieving entanglement purification.

We will present two classes of continuous entangled states and show that a continuous generalization of the entanglement swapping procedure using the continuous controlled-NOT and Hadamard gates introduced by Braunstein [14] is able to produce purification in one of our two classes.

For the quantification of entanglement and of the efficiency of the concentration procedures a measure of entanglement is required. For pure finite states it is generally accepted that in the asymptotic limit of many copies the only measure of entanglement that is sensible is the *entropy of entanglement* [6]. Here we use a direct generalization of this to verify whether or not the attempted purification procedure has been successful.

2. ENTANGLING GATES AND CLASSES OF ENTANGLED STATES

For finite level states two basic operations used in quantum information procedures are the Hadamard transform and the controlled-NOT gate. The

continuous analogue of the former single "particle" gate is the Fourier transform:

$$\mathcal{F}|x\rangle = \frac{1}{\sqrt{\pi}\sigma} \int e^{2ixy/\sigma^2} |y\rangle dy. \quad (16.1)$$

The scale length, σ , included here is normally used to make the expression dimensionless but we will also use it later as a convenient scale with which to compare various lengths in the states we will be dealing with. If we set $\sigma = 1$ and work in units $\hbar = 1/2$ this is also, of course, the transform used to go from the position to the momentum basis. The inverse, \mathcal{F}^\dagger is obtained by replacing i by $-i$ in Eq. (16.1) giving the result that $\mathcal{F}\mathcal{F}^\dagger|x\rangle = \mathcal{F}^\dagger\mathcal{F}|x\rangle = |x\rangle$.

There are a number of generalizations we could use for the continuous controlled-NOT gate: the phase-free beam splitter transformation $\mathcal{B}(\frac{\pi}{4})|x, y\rangle = \left| \frac{x-y}{\sqrt{2}}, \frac{x+y}{\sqrt{2}} \right\rangle$ is one good candidate but we will use a slightly simpler version:

$$\mathcal{C}_{12}|x\rangle_1|y\rangle_2 = |x\rangle_1|y+x\rangle_2, \quad (16.2)$$

whose inverse is obtained by replacing the + with a - sign on the right hand side.

We can now define the 'entangling' operation and its inverse:

$$\mathcal{E}_{12} = \mathcal{C}_{12}\mathcal{F}_1 \quad \mathcal{E}_{12}^\dagger = \mathcal{F}_1^\dagger\mathcal{C}_{12}^\dagger. \quad (16.3)$$

which is just the individual inverse operations performed in reverse order. Note however that it is only the CNOT gate that is able to entangle states but in the case of our gate \mathcal{C}_{12} it can only do so if particle 1 is in a superposition state in the basis we are dealing with. We therefore also require an operation that creates a superposition state for the first particle. Thus we will use the Fourier transform.

The operation \mathcal{E}_{12} can be used to form entangled states from different initial unentangled states of two particles. Applying it to two Gaussian wavepackets

$$|G_\alpha(x_1)\rangle_1 = \int_{-\infty}^{\infty} \exp\left[-\frac{(x-x_1)^2}{\alpha^2\sigma^2}\right] |x\rangle_1 dx \quad (16.4)$$

and $|G_\beta(x_2)\rangle_2$ produces the state

$$\begin{aligned} & \mathcal{C}_{12}\mathcal{F}_1|G_\alpha(x_1)\rangle_1|G_\beta(x_2)\rangle_2 \\ &= \int_{-\infty}^{\infty} \exp\left[\frac{1}{\sigma^2}\left(-x^2\alpha^2 - \frac{y^2}{\beta^2} + 2ix_1x\right)\right] \\ & \quad |x\rangle_1|x+y+x_2\rangle dxdy \\ & \equiv |B_{\alpha\beta}(x_1, x_2)\rangle_{12}. \end{aligned} \quad (16.5)$$

Such states can be used to demonstrate teleportation of an unknown state, the fidelity of the teleportation approaching unity as α and $\beta \rightarrow 0$, where the state becomes like an infinitely squeezed two mode squeezed state or an EPR state [15]. We will call the states $|B_{\alpha\beta}(x_1, x_2)\rangle_{12}$ *partially correlated entangled states*.

Our second class of states cannot easily be formed using this operation as they are a different kind of entangled state. They are a direct generalization of the so called Schrödinger cat states, which are a superposition of two coherent states $|\alpha\rangle$. The Wigner function for one of these states is shown in figure 16.1.

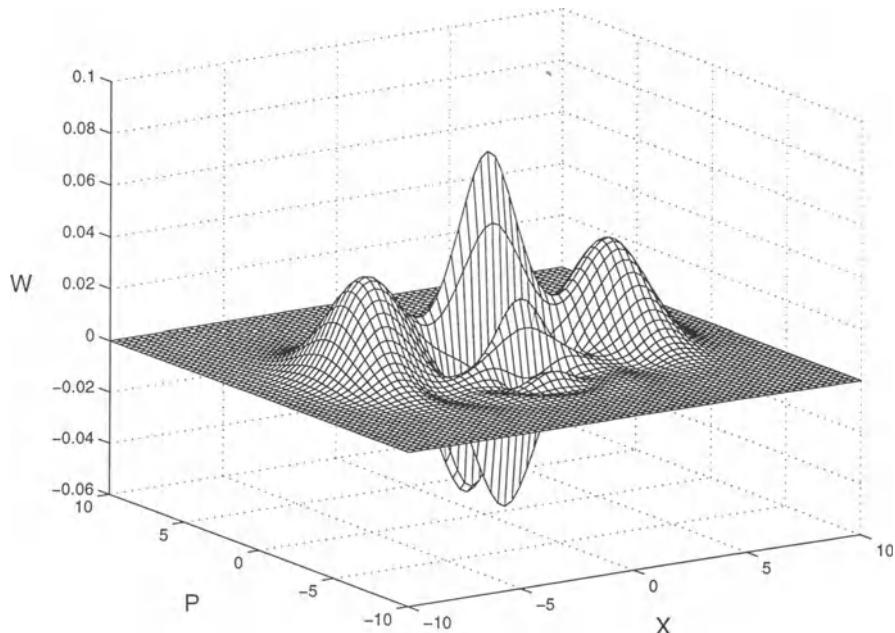


Figure 16.1 Wigner function for a Schrödinger cat state, $1/\sqrt{2}(|+\alpha\rangle + |-\alpha\rangle)$ with coherent states $|\alpha\rangle = |3\rangle$.

Our generalizations we will call *two-mode cat states* [16, 17], as they are Schrödinger cat states of two modes whose locations are correlated with each

other quantum mechanically:

$$\begin{aligned}
 |C(d)\rangle_{12} &= \int_{-\infty}^{\infty} \left[A_0 e^{-(x-d)^2 - (y+d)^2} + A_1 e^{-(x+d)^2 - (y-d)^2} \right] \\
 &\quad |x\rangle_1 |y\rangle_2 dx dy \\
 &= \int_{-\infty}^{\infty} \sum_{j=0}^1 \left[A_j e^{-(x-(-1)^j d)^2 - (y+(-1)^j d)^2} \right] \\
 &\quad |x\rangle_1 |y\rangle_2 dx dy. \tag{16.6}
 \end{aligned}$$

The complex coefficients, A_j , are such that $|A_0|^2 + |A_1|^2 = 1$ (so the state is not normalized correctly). This state is a superposition of the first particle being located around d and the second around $-d$ and *vice versa*. The scale length does not appear here (it is set to unity) as an increase in scale length is equivalent to a decrease in the value of d .

3. QUANTIFICATION OF ENTANGLEMENT

The measure of entanglement for pure bipartite states, the entropy of entanglement, $E(\rho_{12})$, is just the Von Neumann entropy, S , of either partial density operator, ρ_1 or ρ_2 , of the system [6]

$$E(\rho_{12}) \equiv S(\rho_1) = S(\rho_2) = - \sum_i \lambda_i \log_2 \lambda_i, \tag{16.7}$$

where the λ_i 's are the eigenvalues of ρ_1 or ρ_2 . We can very simply generalize this to continuous variable systems but we need to know a little about the eigenvalues of such systems. Let us express a continuous variable state as follows

$$|\psi\rangle_{12} = \int \psi(x, y) |x\rangle_1 |y\rangle_2 dx dy, \tag{16.8}$$

and find the partial density operator of one of the particles (the first, say) by tracing out the other

$$\begin{aligned}
 \rho_1 &= \int_2 \langle x| (\langle \psi | \langle \psi |)_{12} |x\rangle_2 dx \\
 &= \int \rho_1(x, y) |x\rangle_1 \langle y| dx dy. \tag{16.9}
 \end{aligned}$$

We now wish to find the eigenvalues of ρ_1 and so we form a *continuous* eigenvalue equation

$$\int \rho_1(x, y) \phi_i(y) dy = \lambda_i \phi_i(x), \tag{16.10}$$

where λ_i is the eigenvalue corresponding to $\phi_i(x)$ and ρ_1 is known as the *kernel* of the equation. The mathematics we require is covered in the area of integral eigenvalue equations [18]. In particular we will be interested in Hermitian kernels (for which $\rho_1^*(y, x) = \rho_1(x, y)$) which are integrable over the two continuous degrees of freedom, i.e. they are *quadratically integrable*.

Such kernels have many interesting properties [9, 18] of which we will list the important ones for the work that follows. Firstly, the eigenvalues of *all* Hermitian kernels are real and the set of eigenfunctions linearly independent, complete and orthogonal. Secondly, those Hermitian kernels which are *quadratically integrable* in general have infinitely many eigenvalues (although certain kernels may have a finite number), and these eigenvalues have no accumulation points (except at zero), i.e. the eigenvalues do not form a continuous set.

It is now obvious that the generalization of the entropy of entanglement to continuous systems is trivial and is again the Von Neumann entropy of either partial density operator, except that the summation over eigenvalues in Eq. (16.7) may have infinitely many terms. It should be noted however, that such an entanglement measure is not continuous anymore. In fact, in any neighbourhood of a product state lies an arbitrarily strongly entangled state. Such surprising behaviour is removed if one introduces the physical constraint of states of bounded energy as was shown in Ref. [19].

One important property of the entropy of entanglement for discrete systems is its invariance under local unitary transformation. This has been shown to be true for its continuous generalization [9] and other important properties such as concavity, subadditivity, strong subadditivity and the triangle inequality also follow for this measure of entanglement as they do its finite partner [20] provided the relevant quantities converge when we deal with infinite systems.

The measure could in principle be generalized to a mixed state measure analogous to the entanglement of formation [7, 21] or the relative entropy of entanglement [22], however, in this section we focus on the pure state case.

4. THE CALCULATION OF ENTANGLEMENT

We will now move on to calculating the entanglement in the two types of entangled states we have formed. We will find that in general we cannot calculate the entanglement easily and will need to employ a number of different methods, both analytic and numeric.

4.1 SOME MATHEMATICAL PRELIMINARIES

Let us first look at our first class of states, the partially correlated entangled states, $|B_{\alpha\beta}(x_1, x_2)\rangle_{12}$. We have two partial traces we could take but for pure states both partial traces will have the same set of eigenvalues. We will consider

only one of these, tracing out the second particle. The integral eigenvalue equation corresponding to this partial trace (aside from normalization) is

$$\int \exp \left[\frac{1}{\sigma^2} \left(- \left(\alpha^2 + \frac{1}{2\beta^2} \right) (x^2 + x'^2) + 2ix_1(x - x') + \frac{xx'}{\beta^2} \right) \right] \phi_i(x') dx' = \lambda_i \phi_i(x). \quad (16.11)$$

It can then be shown [9] that this eigenvalue equation is equivalent to (in that it has the same set of eigenvalues, aside from normalization) the following one

$$\underbrace{\int \exp \left[-(1+P)(x^2 + x'^2) + 2xx' \right]}_{K(x,x')} \phi(x') dx' = \lambda \phi(x) \quad (16.12)$$

where $K(x, x')$ is the kernel of our integral eigenvalue equation representing the elements of the density operator and

$$P = 2\alpha^2\beta^2. \quad (16.13)$$

Notice that the eigenvalues are independent of the scale length, σ , and the value of x_1 or x_2 . It is only dependent on the product of widths of the original Gaussian distributions with respect to σ .

Similarly we calculate the partial trace of the two-mode cat state and find that its corresponding integral eigenvalue equation is

$$\underbrace{\int \sum_{j=0}^1 \sum_{k=0}^1 \left[A_j A_k^* e^{-(x - (-1)^j d)^2 - (x' - (-1)^k d)^2 + 2d^2 \delta_{jk}} \right]}_{K(x,x')} \phi(x') dx' = \lambda \phi(x). \quad (16.14)$$

This, however, is not easily transformed into a simpler form.

4.2 NUMERICAL PROCEDURE FOR THE PARTIALLY CORRELATED STATES

We cannot solve many of the integral eigenvalue equations we encounter so we must use some numerical approximation [23]. The most direct approach is to solve a discrete eigenvalue equation by approximating the integral by the rectangle rule. Our eigenvalue equation has infinite limits so there must also be a cut-off point in the limits beyond which we do not approximate the integral.

First, therefore, we discretize the eigenvalue equation (16.11) into $2n + 1$ parts ($i = -n, \dots, 0, \dots, n$) each of width δ covering the range $-w \leq x \leq w$ where $w = n\delta$. Our eigenvalue equation then becomes

$$\delta \sum_{p=-n}^n \rho_{pq} \phi_p = \lambda \phi_q, \quad (16.15)$$

where for the partially correlated states

$$\rho_{pq} = \exp [(-(1 + 2\alpha^2\beta^2)(p^2 + q^2) + 2pq) \delta^2]. \quad (16.16)$$

The entropy of entanglement is then approximated by

$$E(\alpha, \beta) = \sum_r \left(\frac{\lambda_r}{\sum_s \lambda_s} \log_2 \left(\frac{\lambda_r}{\sum_t \lambda_t} \right) \right), \quad (16.17)$$

where the outer sum is over the set of eigenvalues and the sums over s and t are to normalize the set of eigenvalues as the ρ_{pq} is not normalized.

What we are doing here is sampling the spectra of eigenvalues over discrete ranges. If we were to take $\delta \rightarrow 0$ and $n \rightarrow \infty$ we should converge to the exact value of the entropy of entanglement as in Eq. (16.7). In fact, for these states there is an analytical result for the entropy of entanglement [3] which we will discuss in the next section. In practice for most values of α and β , $2n+1 = 201$ and w around 10 standard deviations from the mean were sufficient to produce results in agreement with the analytic result accurate to 6 significant figures.

The numerical results for the entanglement are shown in figure 16.2 for varying values of α and β . They were generated using numerical procedures for eigenvalue problems from the NAG library.

We expect the entanglement to increase when the parameters α and β are reduced as this corresponds to a reduction in the spread or uncertainty in the wavefunction of the two particles before the entangling operations were performed. As these parameters approach zero the states become like the entangled states of Vaidman [15]. These are simultaneous eigenstates of the operators $\hat{x}_1 + \hat{x}_2$ and $\hat{p}_1 - \hat{p}_2$ and are therefore maximally correlated. The entanglement is then infinite and convergence in the numerical procedure is difficult to achieve for these small values of α and β .

4.3 ANALYTICAL RESULTS FOR THE PARTIALLY CORRELATED STATES

Here we use a result for a two mode squeezed state [3] with squeezing parameter r [24]:

$$\psi(x, y) = \exp \left(-\frac{1}{4} (e^{2r}(x+y)^2 + e^{-2r}(x-y)^2) \right). \quad (16.18)$$

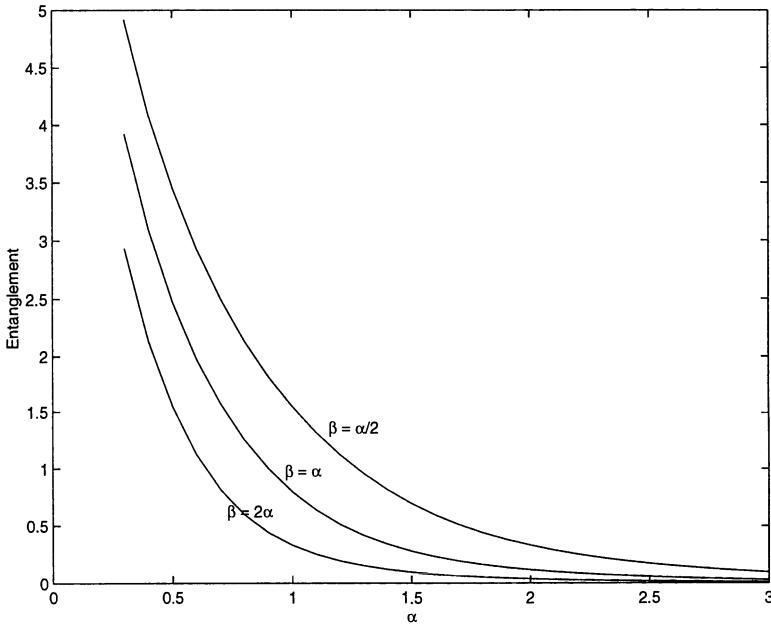


Figure 16.2 Entanglement of a partially correlated state in terms of α and β , the widths of the Gaussians from which they are formed.

After taking the partial trace of this state the integral eigenvalue equation can also be transformed into the form of Eq. (16.11) with a parameter [9]

$$P = 2 \operatorname{cosech}^2(2r). \quad (16.19)$$

This tells us a number of things, firstly that our partially correlated states are just a generalization of two-mode squeezed states and secondly, as the state can be written analytically in the number basis [3]

$$|\psi\rangle_{12} = \frac{1}{\cosh(r)} \sum_{n=0}^{\infty} (\tanh(r))^n |n\rangle_1 |n\rangle_2 \quad (16.20)$$

we can calculate the entanglement exactly:

$$E = \cosh^2(r) \log_2(\cosh^2(r)) - \sinh^2(r) \log_2(\sinh^2(r)). \quad (16.21)$$

This in turn gives us an analytical result for our partially correlated states via the substitution $2r = \operatorname{arcsinh}(1/\alpha\beta)$ into Eq. (16.21). This follows directly from Eqs. (16.19) and (16.13).

4.4 NUMERICAL PROCEDURE FOR THE TWO-MODE CAT STATE

Now we move on to the entanglement of the cat states. We must proceed directly by discretizing the density operator of equation (16.13) and making it the kernel of equation (16.15). Results for the entanglement of the cat states are shown in figure 16.3 with varying parameters d and $|A_0|^2$.

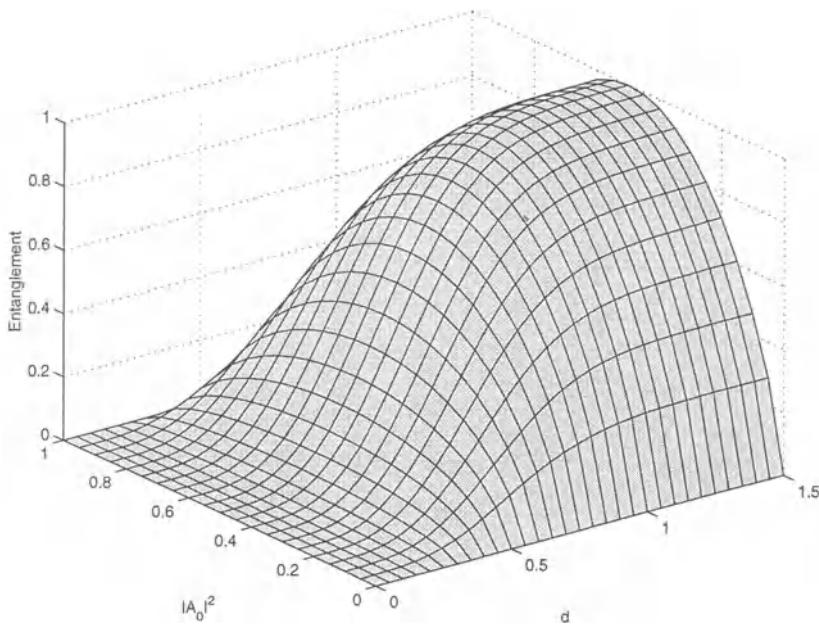


Figure 16.3 Entanglement of the cat states against (half) the distance between Gaussians, d , and the coefficient A_0 . The entanglement is greatest for high values of d where the Gaussians become orthogonal, and for $|A_0|^2 = 0.5$ as with discrete entanglement.

Note that the entanglement for any given value of d is maximum when $|A_0|^2 = 1/2$ and that the entanglement increases with d for given values of A_0 , approaching the limit $E = -|A_0|^2 \log_2 |A_0|^2 - |A_1|^2 \log_2 |A_1|^2$ as $d \rightarrow \infty$, where the separated Gaussians become orthogonal. Note also that only two eigenvalues dominated the contribution to the entropy. These observations, therefore, tell us that these states behave very much like discrete 2-level entangled systems.

5. ENTANGLEMENT PURIFICATION VIA ENTANGLEMENT SWAPPING

Let us first briefly describe the process of entanglement swapping for pure states of two levels [25]. Given two pairs of entangled states a Bell state measurement on one of the particles from each of the pairs can leave the remaining two particles entangled with each other. How entangled they are depends on the measurement result. Let us assume that the initial two pairs are in the same pure state:

$$|\psi\rangle_{12} = \alpha|00\rangle_{12} + \beta|11\rangle_{12} \quad (16.22)$$

and $|\psi\rangle_{34}$. Then a Bell state measurement on particles 2 and 3 will, for certain measurement results, leave particles 1 and 4 in states

$$(\alpha^2|00\rangle_{14} \pm \beta^2|11\rangle_{14})/\sqrt{2} \quad (16.23)$$

with probability $(\alpha^4 + \beta^4)/2$, which is less entangled (provided the two pairs are not already maximally entangled ($\alpha = \beta = 1/\sqrt{2}$)), and states

$$\alpha\beta(|01\rangle_{14} \pm |10\rangle_{14})/\sqrt{2} \quad (16.24)$$

with probability $\alpha^2\beta^2$, which is maximally entangled. Therefore the probability of obtaining a maximally entangled state increases with the amount of entanglement in the initial states. Note also that the *average* entanglement obtained at the end cannot be more than the initial amount of entanglement in one of the pairs.

We can then see that this procedure can be used (by Alice and Bob) for purification. Alice and Bob share an entangled state and Bob holds another copy of the same entangled state as in the upper part of figure 16.4. Bob performs entanglement swapping by making a Bell state projection on one particle from each pair of entangled particles. With a certain probability, this will produce a maximally entangled state.

Generalization of this procedure to continuous variable states is also straight forward (see also [26]). However, we will replace the Bell state measurement with the reverse entangling operation \mathcal{E}^\dagger followed by *separate* measurements on each of the two particles. This is entirely equivalent to a Bell state measurement.

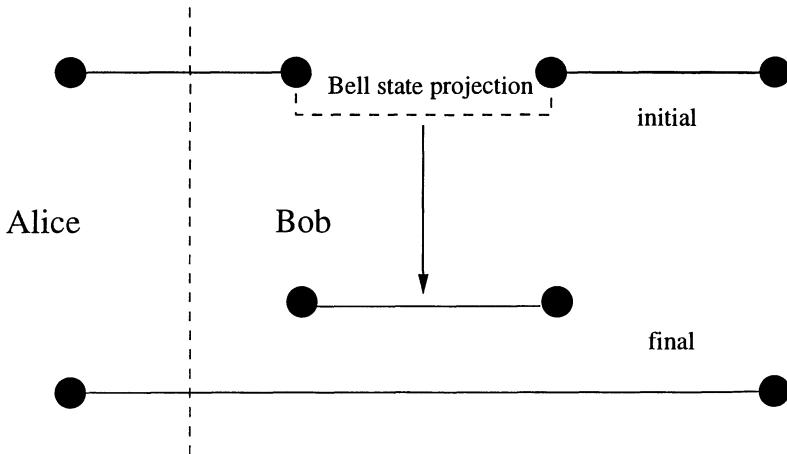


Figure 16.4 The entanglement swapping procedure. Bob, holding a copy of the entangled state shared by himself and Alice, performs a Bell state measurement on a particle from each pair and, for certain measurement outcomes, the entanglement of the final shared pair is higher than that of the initial shared pair.

5.1 PARTIALLY CORRELATED STATES

So we attempt the entanglement swapping procedure with the partially correlated states, starting with infinite resolution projective measurements:

$$\begin{aligned}
 & {}_2 \langle a | {}_4 \langle b | \left(\mathcal{E}_{24}^\dagger (|B_{\alpha\alpha}(0, c)\rangle_{12} |B_{\beta\beta}(0, c)\rangle_{34}) \right) \\
 & = \int \exp \left[\frac{1}{\sigma^2(\alpha^2 + \beta^2)} \left(-x^2 g(\alpha, \beta) - y^2 g(\beta, \alpha) + 2xy \right. \right. \\
 & \quad \left. \left. + 2b(y - x) - 2ia(y\alpha^2 + x\beta^2) \right) \right] |x\rangle_1 |y\rangle_3 \quad (16.25)
 \end{aligned}$$

where

$$g(\alpha, \beta) = \alpha^4 + \alpha^2\beta^2 + 1. \quad (16.26)$$

Has the entanglement increased? Again we can take the partial trace of this state and transform the kernel into the form of Eq. (16.11). This gives us a parameter $P_{swap} = 2[(\alpha^4 + \alpha^2\beta^2 + 1)(\beta^4 + \beta^2\alpha^2 + 1) - 1]$ where before the swapping process the parameter was $P_0 = 2\alpha^4$ or $2\beta^4$. Note firstly that P_{swap} does not depend on the measurement results a and b and is therefore not probabilistic so any increase in entanglement would be *deterministic* thereby breaking laws of the conservation of entanglement. However $P_{swap} \geq P_0$ and the entanglement is strictly decreasing with increase in P so the swapped pair has less entanglement and we have not achieved purification.

Of course, our final projections in this method were onto the unphysical states $|a\rangle$ and $|b\rangle$ but further calculations indicate that with finite width projections (performed by projecting onto the Gaussian states of Eq. (16.4)) the parameter P still increases. Such calculations involve 6th degree polynomials in the width parameters (α and β etc.) so proving that P increases for all values of these parameters is difficult and we have not been able to do so analytically. However, numerical results indicate that this is true.

5.2 TWO-MODE CAT STATES

We now attempt a similar method with the two-mode cat states, but setting the scale length $\sigma = 1$ and making *finite* resolution measurements of width μ :

$$\begin{aligned} |\psi\rangle_{14} &= {}_2\langle G_\mu(a)| {}_3\langle G_\mu(b)| \left(\mathcal{E}_{23}^\dagger (|C(d)\rangle_{12}|C(d)\rangle_{34}) \right) \\ &= \int \sum_{j,k=0}^1 A_j A_k e^{-(x-(-1)^j d)^2 - (y+(-1)^k d)^2} \\ &\times e^{(dbh(\mu)((-1)^j + (1+\mu^2)(-1)^k) + 2d^2 \delta_{jk})} \\ &\times e^{(iad h(\mu)((1+\mu^2)(-1)^j - (-1)^k))} |x\rangle_1 |y\rangle_4 dx dy \quad (16.27) \end{aligned}$$

where

$$h(\mu) = \frac{2}{2 + 2\mu^2 + \mu^4}. \quad (16.28)$$

Writing this state out in full in the high precision measurement limit, $\mu = 0$

$$\begin{aligned} |\psi\rangle_{14} &= \int \left(\begin{array}{ccc} A_0 A_0 & e^{-2d^2+2db} & e^{-(x-d)^2-(y+d)^2} \\ +A_0 A_1 & e^{2iad} & e^{-(x-d)^2-(y-d)^2} \\ +A_1 A_0 & e^{-2iad} & e^{-(x+d)^2-(y+d)^2} \\ +A_1 A_1 & e^{-2d^2-2db} & e^{-(x+d)^2-(y-d)^2} \end{array} \right) \\ &\quad |x\rangle_1 |y\rangle_4 dx dy \quad (16.29) \end{aligned}$$

and looking at the particular case where the probabilistic measured values are $a = b = 0$ we can see purification for high values of d as the middle two terms now dominate and have coefficients of equal magnitude. As $d \rightarrow \infty$ they become maximally entangled. This is again very much like the action of discrete entanglement under purification procedures: the coefficients of the states have changed, not the states themselves.

For the results of figure 16.5 and 16.6 we have chosen the values $A_0 = \sqrt{0.3}$ and $d = 1.0$. They show the entanglement of the resulting state (16.26) for a range of values of a and b with $\mu = 0$ and 0.5 respectively.

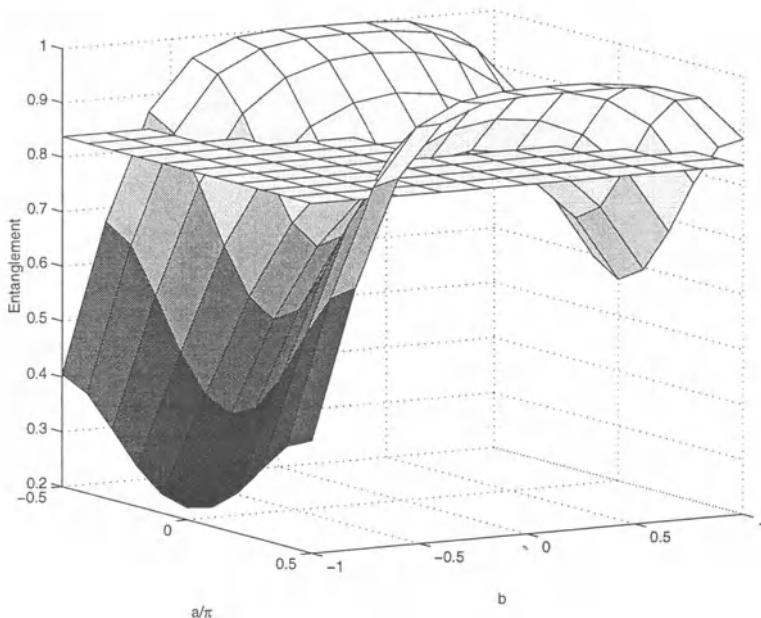


Figure 16.5 Entanglement of swapped cat states with $\mu = 0$. Above the level of the plane purification has been achieved.

The horizontal planes are at the level of entanglement of either cat state before the purification procedure is performed, that is, above this plane purification has been achieved.

6. SUMMARY

We should now address why it is that we have observed purification via entanglement swapping in only one of the sets of states that we have considered. As mentioned above the two-mode cat states have many characteristics like those of discrete two-level entanglement and so it is not surprising that the method of entanglement swapping generalized from these systems is successful.

The failure of the procedure for the partially correlated states is more difficult to explain. These states are the kind of states used in continuous variable teleportation experiments [1, 2, 3, 4, 5] and a simple method of purification would be ideal. However, we were unable to find any simple continuous procedure that would produce purification, indeed no procedure was found where the final entanglement was in anyway probabilistic in the measurement outcomes, an essential ingredient if a successful procedure is not to violate conservation laws of entanglement. In fact it has been brought to our attention

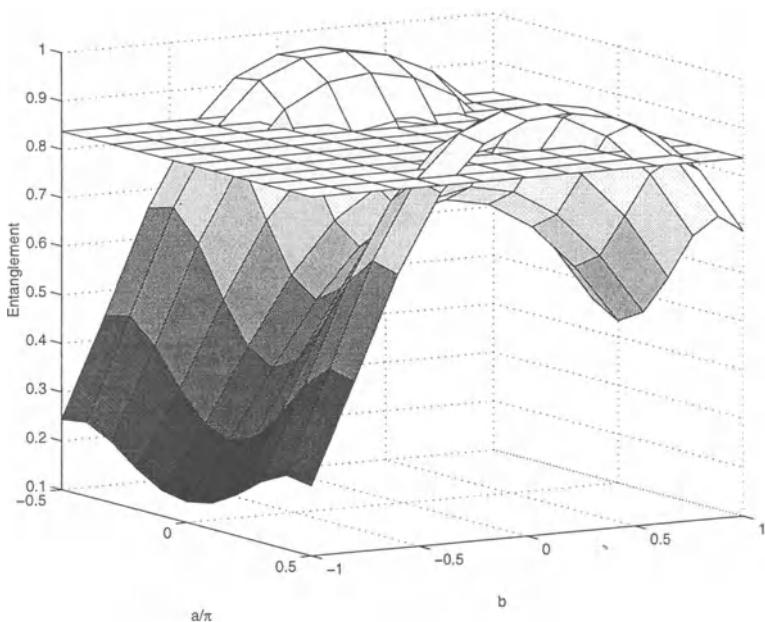


Figure 16.6 Entanglement of swapped cat states with $\mu = 0.5$. Again purification has been achieved above the level of the plane, but with the inaccuracy in the measurement part of the entanglement swapping process the amount of purification is reduced.

[27] that such methods could never increase the amount of entanglement for Gaussian states. When completing this chapter it was found rigorously, that Gaussian operations never allow entanglement distillation of Gaussian states, see Ref. [28].

Fortunately, more recent work has now achieved entanglement purification in Gaussian states [10] using non-demolition measurements with a number of entangled pairs. However, what exactly the key difference is between the two types of states presented here which allows purification by our methods in one class but not the other is still unclear. There are obvious correspondences between the form of entanglement in the two mode cat states and discrete systems and it would be interesting to find a condition for continuous variable purification, as it has been attempted here, which a state undergoing purification must obey. The fact that purification has been demonstrated here and elsewhere in continuous systems, however, are interesting results.

Acknowledgments

This work is supported by the United Kingdom Engineering and Physical Sciences Research Council (EPSRC), the Inlaks Foundation, The Leverhulme Trust, the EU TMR-networks ERB 4061PL95-1412 and ERB FMRXCT96-0066, the EU project EQUIP and the European Science Foundation programme on quantum information theory.

References

- [1] S. L. Braunstein, H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
- [2] G. J. Milburn, S. L. Braunstein, Phys. Rev. A **60**, 937 (1999).
- [3] S.J. van Enk, Phys. Rev. A **60**, 5095 (1999).
- [4] T. C. Ralph, P. K. Lam, Phys. Rev. Lett. **81**, 5668 (1998).
- [5] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik, Science, **282**, 706 (1998).
- [6] C. H. Bennett, H. J. Herbert, S. Popescu, B. Schumacher, Phys. Rev. A **53**, 2046 (1996); S. Popescu, D. Rohrlich, Phys. Rev. A **56**, R3319 (1997).
- [7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [8] M. B. Plenio and V. Vedral, Contemp.Phys. **39**, 431 (1998)
- [9] S. Parker, S. Bose, M. B. Plenio, Phys. Rev. A **61**, 032305 (2000).
- [10] Lu-Ming Duan, G. Giedke, J. I. Cirac, P. Zoller, Phys. Rev. A **62**, 032304 (2000); Lu-Ming Duan, G. Giedke, J. I. Cirac, P. Zoller, *Physical implementation for entanglement purification of Gaussian continuous variable quantum states*, LANL eprint: quant-ph 0003116.; Geza Giedke, Lu-Ming Duan, J. Ignacio Cirac, Peter Zoller, *All inseparable two-mode Gaussian continuous variable states are distillable* Lanl e-print quant-ph/0007061
- [11] M. Lewenstein and P. Horodecki, lanl e-print quant-ph/0001035
- [12] H. -K. Lo, S. Popescu, *Concentrating entanglement by local actions - beyond mean values*, LANL eprint: quant-ph 9707038; M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999); G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999); D. Jonathan, M. B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999); L. Hardy, Phys. Rev. A **60**, 1912 (1999).
- [13] M. Zukowski, A. Zeilinger, M. A. Horne, A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993); J.-W. Pan, D. Bouwmeester, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998); S. Bose, V. Vedral, P. L. Knight, Phys. Rev. A **57**, 822 (1998).
- [14] S. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
- [15] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).

- [16] B. C. Sanders, Phys. Rev. A **45**, 6811 (1992).
- [17] C. C. Gerry, Phys. Rev. A **55**, 2478 (1997).
- [18] F. G. Tricomi, *Integral Equations*, Wiley, New York (1967).
- [19] J. Eisert, C. Simon and M. B. Plenio, J. Phys. A **35**, 3911 (2002).
- [20] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).
- [21] S. Hill, W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997); W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
- [22] V. Vedral, M. B. Plenio, Phys. Rev. A **57**, 1619 (1998); V. Vedral, M. B. Plenio, K. Jacobs, P. L. Knight, Phys. Rev. A **56**, 4452 (1997); V. Vedral, M. B. Plenio, M. A. Rippin, P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997); M. Murao, M. B. Plenio, S. Popescu, V. Vedral, P. L. Knight, Phys. Rev. A **57**, 4075 (1998); V. Vedral, M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
- [23] D.A. Kofke, A. J. Post, J. Chem. Phys. **98**, 4853 (1993).
- [24] U. Leonhardt, *Measuring the Quantum State of Light*, Cambridge University Press
- [25] S. Bose, V. Vedral, P. L. Knight, Phys. Rev. A **60**, 194 (1999).
- [26] R. E. S. Polkinghorne, T. C. Ralph, Phys. Rev. Lett. **83**, 2095 (1999); P. van Loock, S. Braunstein, Phys. Rev. A **61**, 010302(R) (2000)
- [27] T. Opatrný, G. Kurizki, D.-G. Welsch, Phys. Rev. A **61**, 032302 (2000).
- [28] J. Eisert, S. Scheel and M. B. Plenio, quant-ph/0204052; and G. Giedke and J. I. Cirac, quant-ph/0204085.

III

CONTINUOUS VARIABLE OPTICAL-ATOMIC INTERFACING

Chapter 17

BOUND ENTANGLEMENT FOR CONTINUOUS VARIABLES IS A RARE PHENOMENON

Paweł Horodecki¹, J. Ignacio Cirac² and Maciej Lewenstein³

¹ Faculty of Applied Physics and Mathematics

Technical University of Gdańsk, 80–952 Gdańsk, Poland

² Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria

³ Institut für Theoretische Physik, Universität Hannover

30167 Hannover, Germany

Abstract We discuss the notion of bound entanglement (BE) for continuous variables (CV). We show that the set of non-distillable states (NDS) for CV is nowhere dense in the set of all states, i.e., the states of infinite-dimensional bipartite systems are generically distillable. This automatically implies that the sets of separable states, entangled states with positive partial transpose, and bound entangled states are also nowhere dense in the set of all states. All these properties significantly distinguish quantum CV systems from the spin like ones. The aspects of the definition of BE for CV is also analysed, especially in context of Schmidt numbers theory. In particular the main result is generalised by means of arbitrary Schmidt number and single copy regime.

1. INTRODUCTION

Bound entanglement [1] is the entanglement which cannot be distilled (purified), i.e. no pure state entanglement can be obtained from it by means of local operations and classical communication (LOCC)[2]. So far, it has been studied mainly for spin like systems. These studies have allowed to discover many interesting properties of bound entanglement, for both bipartite[3], and multiparticle systems[4]. Recently, much attention has been devoted continuous variable (CV) systems (c.f. [5]). Bound entanglement has also been considered for continuous variables (CV), and the first nontrivial examples of BES for CV have been constructed[6] (see also [7]). Once we have some examples of BES for CV, it is interesting to ask how frequent is the phenomenon

of bound entanglement, i. e. how many states of that kind are in set of all CV states?

The question of "how many quantum states having some interesting property are there?" is very natural. In the context of entanglement it was first considered in Ref. [8], where the problem of the volume of the subset of separable (non-entangled) states in the set of all bipartite states of spin systems was considered. Numerical evidence has shown that the volume of the set of separable states approaches zero when the size of the spin goes to infinity. It was also shown that for any finite spin system the volume of separable states is nonzero due to the existence of a separable neighborhood, i.e. an open ball of separable states in the vicinity of the maximally mixed state in arbitrary dimension. Further first analytical bounds on the size of neighbourhood have been provided [9]. All this raised a series of questions concerning the interpretation of experiments of quantum computing based on high temperature NMR; many interesting analyses have been performed in this context [10, 11].

The question of the "size" of the set representing separable states has been recently answered [12] for CV; it has been shown that for bipartite states this subset is nowhere dense (relative to the trace–norm topology). This implies that this set does not contain any open ball and also that CV states are generically non–separable. On the other hand there exists another subset that is of interest in the context of entanglement. This is the subset of of non–distillable states (NDS), i.e. states that cannot be distilled. This subset contains the separable states, and therefore it might well be that an appreciable fraction of all states are in such a subset. In this paper we show that this is not the case; that is, the subset of NDS is nowhere dense in the set of bipartite states of CV. We present two different proofs of this fact. One uses the uniform topology, and the other one the trace–norm topology.

We also perform analysis how one can relax conditions of NDS in context of CV in comparison with the standard definition, and prove stronger version of the main result with help of Schmidt numbers theory [13] and single copy regime (see [15, 14]).

There are several results which follow from our proofs. In particular, since the subset of NDS contains the subset of BES, we have that that subset is also nowhere dense. The same thing occurs with the subset of states with positive partial transpose (PPT) [1] and therefore with those PPT states that are entangled. Moreover, since the subset of separable states is also contained in the one of NDS, our results include the ones given in Ref. [12].

2. NON-DISTILLABLE STATES FOR CONTINUOUS VARIABLES

The main subject of this paper is the question about whether generic CV states are non-distillable. We present below the answer to this question: the subset of NDS is nowhere dense. In this section we first discuss the definition of NDS. Then, we present two proofs of our result. First, it will be proven using the uniform topology and exploiting the fact that any density operator can be considered as the limit of a sequence of density operators defined on a finite support. Then, following the approach of Ref. [12] we shall prove the general statement that any proper closed subset of bipartite states which is invariant under local transformations is nowhere dense (in the trace norm topology). This generalizes the results of Ref. [12] and, as we shall see, together with the fact that the set of NDS is closed, proves our claims.

2.1 FREE AND BOUND ENTANGLED STATES

Let us denote by M set of all density operators acting on $H_A \otimes H_B$, where $H_A \cong H_B \cong L^2(R)$. Let us consider a density operator $\rho \in M$. The notion of distillability of entanglement introduced in Ref. [2] has been operationally characterised. Namely, according to Ref. [1], ρ is distillable (free entangled) iff there exists some finite $n \in N$, two rank two projectors P_A, P_B acting on H_A, H_B , respectively, such that

$$((P_A \otimes P_B)\rho^{\otimes n}(P_A \otimes P_B))^{T_B} \not\geq 0; \quad (17.1)$$

otherwise, ρ is non-distillable. Entangled but non-distillable states are called bound entangled states [1]. Here we call D and N the set of all distillable and non-distillable density operators, respectively. Physically, this definition tells us that a state is distillable iff out of a sufficiently large number of copies we can obtain by local operations two qubits which are entangled. The reason for that is clear. First, given the fact that one can distill maximally entangled states out of all entangled states of qubits, this means that if the above condition is true, we can always distill maximally entangled qubit states out of the original state ρ . Second, if the above condition is not fulfilled for any n , then we will not be able to produce (asymptotically) any qubit maximally entangled state by using local operations alone.

In the following we will reexpress Eq. (17.1) as follows:

$$\epsilon \equiv \langle \Psi | ((P_A \otimes P_B)\rho^{\otimes n}(P_A \otimes P_B))^{T_B} | \Psi \rangle < 0 \quad (17.2)$$

for some $|\Psi\rangle \in H_A \otimes H_B$. Without loosing generality we can take $|\Psi\rangle = P_A \otimes P_B^{T_B} |\Psi\rangle$, i.e. $|\Psi\rangle$ belongs to the $2 \otimes 2$ subspace determined by $P_A, P_B^{T_B}$.

It is easy to see then that

$$(|\Psi\rangle\langle\Psi|)^{T_B} = \sum_{k=1}^4 \lambda_k |\phi_k\rangle\langle\phi_k|, \quad (17.3)$$

where $-1/2 \leq \lambda_k \leq 1$, i.e. $|\lambda_k| \leq 1$ and the $|\phi_k\rangle$ are also in the same 2×2 subspace.

2.2 NON-DISTILLABLE STATES FOR CV ARE NOWHERE DENSE: PROOF I

In this subsection we show that the set N of NDS states is *nowhere dense* in the set of all states M . We will first recall some definitions. A subset A of a topological space X is nowhere dense if its closure contains no open set. Note that if A is already closed then it is nowhere dense iff it contains no open set. For example, the subset of integer numbers Z in R (with the topology induced by the absolute value metric) is nowhere dense since it is already close and no neighborhood of any integer contains only integers.

In this subsection we will use the uniform topology for operators, which is the one derived from the operator norm. First we will show that N is closed with that topology by proving that its complement, D , is open. Then, we will show that D is dense in the set of all density operators. From this last point it follows that N (equivalently, its closure) contains no open set and therefore it is nowhere dense.

In order to show that D is open, let us consider some $\rho \in D$. According to the definition of D , there exists some finite integer n , and a Schmidt rank two state $|\Psi\rangle \in H_A \otimes H_B$ such that Eq. (17.2) is fulfilled with (17.3). Let us consider an open ball $B_\eta(\rho) = \{\rho', ||\rho' - \rho|| < \eta\}$. We will show that for $\eta < |\epsilon|/4n$, $B_\eta(\rho) \subset D$.

To this aim we argue that

$$\begin{aligned} & |\langle\Psi|((P_A \otimes P_B)(\rho^{\otimes n} - (\rho')^{\otimes n})(P_A \otimes P_B))^{T_B}|\Psi\rangle| \\ &= \left| \sum_{k=1}^4 \lambda_k \langle\phi_k|\rho^{\otimes n} - (\rho')^{\otimes n}|\phi_k\rangle \right| \\ &\leq 4||\rho^{\otimes n} - (\rho')^{\otimes n}|| \leq 4\eta n. \end{aligned} \quad (17.4)$$

The latter inequality can be proven by induction, using the identity

$$\begin{aligned} \rho^{\otimes n} - (\rho')^{\otimes n} &= \frac{1}{2}(\rho^{\otimes n-1} + (\rho')^{\otimes n-1}) \otimes (\rho - \rho') \\ &+ \frac{1}{2}(\rho^{\otimes n-1} - (\rho')^{\otimes n-1}) \otimes (\rho + \rho'), \end{aligned} \quad (17.5)$$

and the fact that both $\|\rho\|$ and $\|\rho'\|$ are smaller than one. Thus, if $\eta < |\epsilon|/4n$, we see that for any $\rho' \in B_\eta(\rho)$,

$$\langle \Psi | ((P_A \otimes P_B)(\rho')^{\otimes n} (P_A \otimes P_B))^T \Psi \rangle < 0, \quad (17.6)$$

ergo ρ' is distillable.

Now we show that D is dense in M . To this aim we observe that for any $\rho \in M$ we can always find a sequence $\{\rho_n\}_{n=0}^\infty$, with $\rho_n \in D$ such that $\rho_n \xrightarrow{u} \rho$. We consider the spectral decomposition of ρ as

$$\rho = \sum_{n=1}^{\infty} p_n |\Psi_n\rangle \langle \Psi_n|, \quad (17.7)$$

where we have chosen $p_1 \geq p_2, \dots$. Note that since ρ is a trace class operator, the sequence p_n converges monotonically to zero. On the other hand, we can write the Schmidt decomposition of each $|\Psi_n\rangle$ as

$$|\Psi_n\rangle = \sum_{k=1}^{\infty} \sqrt{\lambda_{n,k}} |u_{n,k}, v_{n,k}\rangle, \quad (17.8)$$

where again we have chosen $\lambda_{n,k} \geq \lambda_{n,k+1} \geq 0$ and $\lambda_{n,k}$ converges monotonically to zero as $k \rightarrow \infty$. Now, we define

$$\tilde{\rho}_N \equiv \sum_{n=1}^N p_n |\Psi_{N,n}\rangle \langle \Psi_{N,n}|, \quad (17.9)$$

where

$$|\Psi_{N,n}\rangle = \sum_{k=1}^N \sqrt{\lambda_{n,k}} |u_{n,k}, v_{n,k}\rangle. \quad (17.10)$$

It is clear that $\tilde{\rho}_N$ is supported on $H_A^N \otimes H_B^N$, where both H_A^N have finite dimension. Thus, we can always find two pairs of orthogonal vectors $|a_{1,2}^N\rangle \in H_A \ominus H_A^N$ and $|b_{1,2}^N\rangle \in H_B \ominus H_B^N$. Let us define $|\Phi^N\rangle = (|a_1, b_1\rangle + |a_2, b_2\rangle)/\sqrt{2}$ and

$$\rho_N = K_N (\tilde{\rho}_N + \frac{1}{N} |\Phi^N\rangle \langle \Phi^N|), \quad (17.11)$$

where K_N is a normalization constant. It is clear that $\rho_N \xrightarrow{N \rightarrow \infty} \rho$. On the other hand, defining

$$P_A^N = |a_1\rangle \langle a_1| + |a_2\rangle \langle a_2|, \quad (17.12a)$$

$$P_B^N = |b_1\rangle \langle b_1| + |b_2\rangle \langle b_2| \quad (17.12b)$$

and taking $n = 1$ it is clear that $\rho_N \in D$. This completes the proof. \square

Obviously the fact that the set of NDS states for CV is nowhere dense, implies that the contained in it sets of BES and PPT states are also nowhere dense. One can, however, prove the latter directly using the method used above. The only difference would be that the state $|\Psi\rangle$ which in above proof belongs to a $2 \otimes 2$ subspace has to be substituted by a general vector $|\Psi\rangle$ of arbitrary Schmidt rank, but at the same time there is no need to consider n -fold tensor products, since the PPT property of ρ is maintained for arbitrary number of its copies. One has to use, however, the property of the partially transposed projector $\|(|\Psi\rangle\langle\Psi|)^{T_B}\| \leq 1$.

2.3 NON-DISTILLABLE STATES FOR CV ARE NOWHERE DENSE: PROOF II

In order to demonstrate the statement of the previous section in another way, we first need to recall notions of several necessary tools, which have been used in Ref. [12]. Let $\mathcal{B}(\mathcal{H}_1) \otimes \mathcal{B}(\mathcal{H}_2)$ stand for bounded operators on Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ describing our bipartite system. We assume that at least one of the subsystems is described by CV, and hence it has the infinite dimension.

Now, consider a third auxiliary system described by \mathcal{H}_3 . It is convenient to describe all states in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ as reduced states of some *pure* states in the extended space $\mathcal{H} \otimes \mathcal{H}_3$. If we have a pure state $|v_{123}\rangle\langle v_{123}|$ in the extended space, then the reduced state $\text{Tr}_3(|v_{123}\rangle\langle v_{123}|)$ is denoted by ϱ_{12} . Let us denote by \mathcal{T} the set of all states on $\mathcal{B}(\mathcal{H}_1) \otimes \mathcal{B}(\mathcal{H}_2)$. This is a set of unit trace operators with nonnegative spectrum. We shall also endow this set with the norm topology $\|\cdot\|_T$, $\|A\|_T \equiv \text{Tr}(\sqrt{A^\dagger A})$. Now, one defines [12] the map Φ from the unit sphere \mathcal{S} representing all wavefunctions from $\mathcal{H} \otimes \mathcal{H}_3$ to the set of states \mathcal{T} in the following way :

$$\Phi(v_{123}) = \text{Tr}_3(|v_{123}\rangle\langle v_{123}|) = \varrho_{12}. \quad (17.13)$$

The map $\Phi : \mathcal{S} \rightarrow \mathcal{T}$ is *continuous* (in the norm $\|\cdot\|_T$) and *onto*. In particular it maps dense subsets onto dense subsets (see [12] for explanation).

Consider the set \mathcal{X} of all vectors $v_{123} = A \otimes I \otimes I(v_{123})$ for all $A \in \mathcal{B}(\mathcal{H}_1)$. The vector v_{123} is called *1-cyclic* (see [12]) if the closure of \mathcal{X} in the norm $\|\cdot\|_T$ turns out to be *the whole* space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$. The physical interpretation of 1-cyclic vectors in both finite dimensional, as well as in the CV case, is that those are the vectors which have maximal possible Schmidt rank. Note, that according to Lemma 2 of Ref. [25] they form a dense set in $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$.

Now we consider the following simple

Observation 1. - Let the set \mathcal{ND} be (i) a proper closed (in $\|\cdot\|_T$ norm) subset of the set of states \mathcal{T} which is (ii) invariant under the operations $A \otimes I$.

Then any vector v_{123} satisfying $\Phi(v_{123}) \in \mathcal{ND}$ cannot be 1-cyclic and \mathcal{ND} is nowhere dense in \mathcal{T} .

The above observation is a natural generalization of the Lemma 1 of Ref. [12]. To show this, consider such vector v that its “reduction” $\Phi(v)$ belongs to \mathcal{ND} , and take any vector

$$v' = A \otimes I \otimes I(v), \quad (17.14)$$

defined for arbitrary A , such that $\|v'\| = 1$. We shall show first that $\Phi(v')$ also belongs to \mathcal{ND} . Indeed (see [12]) we have $\Phi(v') = A \otimes I \Phi(v) A^\dagger \otimes I$ and (because the norm of v' is one) the trace $\Phi(v')$ is one. But, because the set \mathcal{ND} is closed under the operation $A \otimes I(\cdot)A^\dagger \otimes I$, we see that $\Phi(v')$ still belongs to the set.

Now suppose that v were 1-cyclic. Then, that the set \mathcal{M} of all vectors v' would be dense in the unit sphere \mathcal{S} of all normalized vectors belonging to $\mathcal{H} \otimes \mathcal{H}_3$. As the map Φ is continuous and onto, it certainly would map \mathcal{M} onto some new set denoted by $\Phi(\mathcal{M})$, which would be dense in set of all bipartite states \mathcal{T} . Thus closure of $\Phi(\mathcal{M})$ must have give all \mathcal{T} . But, on the other hand any element of $\Phi(\mathcal{M})$ (which is defined as $\Phi(v')$ for some vector v' of the form (17.14)) belongs to \mathcal{ND} . As the latter is closed, the closure of $\Phi(\mathcal{M})$ would have to be a subset of \mathcal{ND} . But \mathcal{ND} was supposed to be closed and strictly smaller than the set \mathcal{T} , so the closure of $\Phi(\mathcal{M})$ cannot be equal to \mathcal{T} . This gives the required contradiction. The above reasoning follows the lines of the proof of Ref. [12]. The only difference is that instead of the specific set of separable states considered there, here we have considered an abstract set \mathcal{ND} , which has some special properties. Note, that the assumptions of Observation 1 and the fact that the 1-cyclic vectors form a dense set in \mathcal{S} imply that the closed set \mathcal{ND} is nowhere dense. If it had contained a open set, then, following continuity of Φ this open set would have had to be an image of open subset of $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$, which would have had to contain a ball, an thus a 1-cyclic vector. Now, to show that the set of NDS states is nowhere dense we have to show that it is (i) invariant under local operations of the type $A \otimes I$, (ii) closed in the trace norm $\|\cdot\|_T$. The first property (i) is immediate, since a NDS cannot be converted into a free entangled state by means of local operations. The second one is not so obvious for continuous variables, but it follows from the results of the previous subsection. We thus have:

Observation 2.- The property of non-distillability is invariant under the one side local action $A \otimes I(\cdot)A^\dagger \otimes I$.

The proof is simple - the arguments of Ref. [1] can be applied (see also [6]) to show that any local separable superoperator cannot cause that the state loses the non-distillability property.

Observation 3.- The set of all NDS is closed in the norm $\|\cdot\|_T$.

To prove the closeness of the set of NDS, we prove that its complement, i.e. the set of distillable states D is open in the trace norm. To this aim we repeat the arguments of subsection A and consider some $\rho \in D$, for which there exists some finite integer number n , P_A, P_B , rank two projectors acting on H_A, H_B , and a rank two vector $|\Psi\rangle \in H_A \otimes H_B$ such that Eq. (17.2) is fulfilled. We consider now an open ball in the trace norm, i.e. $\tilde{B}_\eta(\rho) = \{\rho' | ||\rho' - \rho||_T < \eta\}$. Note that if $\rho' \in \tilde{B}_\eta(\rho)$ then the operator norm fulfills $||\rho' - \rho|| \leq ||\rho' - \rho||_T < \eta$ [16]. Using the same argument as before we show that for $\eta < |\epsilon|/4n$, $\tilde{B}_\eta(\rho) \subset D$, which completes the proof. \square

Combining the Observations 1.-3. we see that the set of NDS states is nowhere dense in the trace norm, which implies the same property for the BES, PPT states, and separable states.

3. BOUND ENTANGLEMENT: AN ANALYSIS

As mentioned in the introduction, non-trivial BES for continuous variables (CV) have been discovered. In this subsection we discuss some of the details regarding these states, as well as whether entangled states in CV with infinite Schmidt number represent are generic in the set of entangled states.

3.1 CONTINUOUS VARIABLE BOUND ENTANGLED STATES

The construction of non-trivial BES for CV systems [6] was based on an idea similar to the one used for spin systems, for which it has been proven that any entangled state with positive partial transpose[17] cannot be distilled[1]. The crucial element of the construction was to create the state in such a way that it cannot be obtained simply by embedding a bound entangled state in a finite dimensional Hilbert space into the Hilbert space of CV.

The particular example ϱ of CV BES proposed by us was first of all assumed to satisfy the condition that its partial transpose ϱ^{T_B} , defined as

$$\varrho_{m\mu,n\nu}^{T_B} \equiv \langle m, \mu | \varrho^{T_B} | n, \nu \rangle = \varrho_{m\nu,n\mu}, \quad (17.15)$$

has a nonnegative spectrum. Such requirement was, however, not sufficient, as one could invent the following "trivial" example of a PPT entangled states for CV[6]

$$\tilde{\sigma} = \bigoplus_{n=1}^{\infty} p_n \sigma_n. \quad (17.16)$$

The above state is build from infinitely many "copies" of the same $3 \otimes 3^1$ BES σ labeled by σ_n . Each of σ_n has the matrix elements of the original σ , but in the basis $S_n = \{|i, j\rangle\}_{i,j=3n}^{3n+3}$. Here $\{p_i\}_{i=1}^{\infty}$ is an infinite sequence of nonzero probabilities, $\sum_{i=1}^{\infty} p_i = 1$. The bound entanglement of the CV state $\tilde{\sigma}$ is in a

certain sense spurious, as it can in principle be reversibly converted by means of local operations and classical communication into the $3 \otimes 3$ entanglement.

One could easily construct another example, similar to the one above, with σ_n acting in $k_n \otimes k_n$ Hilbert space with $k_n \rightarrow \infty$, and $\tilde{\sigma}$ being block diagonal as in (17.16). This example is much more interesting as far as CV are concerned, because it can not be reversibly converted into any state of fixed spin. Thus to some extend it might be regarded as generic BE. However, such a state would still be a mixture of “locally orthogonal” spin states, which does not exploit fully the CV Hilbert space structure, i.e. infinite dimension fully. In fact, if such CV BES were produced by a random mixture, they could be easily “decoupled” by local projective measurements and classical communication.

Thus we propose to define generic BES for CV in a stronger way, namely as the states from which no pure entanglement can be distilled, and they cannot be represented by the states of the above sort.

This is a somewhat phenomenological definition, but it implies to single out some required properties of the generic CV BES. The first nontrivial examples of the generic CV BES, presented in Ref. [6], fulfill those requirements. These states have the form:

$$\varrho \propto |\Psi\rangle\langle\Psi| + \sum_{n=1}^{\infty} \sum_{m>n}^{\infty} |\Psi_{mn}\rangle\langle\Psi_{mn}|, \quad (17.17)$$

with the following definitions of the symbols: $|\Psi\rangle = \sum_{n=1}^{\infty} a_n |n, n\rangle$, $|\Psi\rangle \in \mathcal{H} = l^2(\mathcal{C}) \otimes l^2(\mathcal{C})$ with the finite norm $\|\Psi\|^2 = \sum_{n=1}^{\infty} |a_n|^2 = q < \infty$, and vectors

$$|\Psi_{mn}\rangle = c_m a_n |n, m\rangle + (c_m)^{-1} a_m |m, n\rangle, \quad (17.18)$$

for $n < m$ with (in general) complex a_n and c_n , such that (i) $0 < |c_{n+1}| < |c_n| < 1$, (ii) $\sum_{n=1}^{\infty} \sum_{m>n}^{\infty} \|\Psi_{mn}\|^2$ is finite. The latter condition can be achieved for example by setting $a_n = a^n$, $c_n = c^n$, for some $0 < a < c < 1$, see [6]. Physically, the vector $|\Psi\rangle$, when normalized, may describe a state of two modes of the quantized electromagnetic field, or more generally two harmonic oscillators. The state (17.17) has the following properties: (i) it is bound entangled, as it has the PPT property (i. e. it has the positive partial transpose); (ii) it is not a simple “direct sum” of finite spin BES in a sense of the “spurious” examples discussed above (Eq. (17.16)).

Recently considerable attention has been devoted to the so called Gaussian states. In systems of two harmonic oscillator modes (one of Alice, one of Bob), i.e. in the, so called, Gaussian 1×1 case, it has been shown that no bound entanglement exists – such Gaussian states are either separable [18, 19], or distillable [20]. In another words, in this case PPT property is a necessary and sufficient condition for separability, and non-distillability. This result can be

extended to the case $1 \times N$. Soon after realizing this facts Werner and Wolf have found an example of a Gaussian BES with PPT property [7]. This result has been achieved by considering first covariance matrices of Gaussian states and their null subspaces. It was noted that the Gaussian state is separable, iff its covariance matrix can be minorized by some block diagonal covariance matrix. Second, the characterization of PPT states in terms of covariance matrix has been found. The BES has been constructed using an elegant explicit construction, performed using the analysis of the range and the “subtraction method” first developed for spin systems in Refs. [21, 22, 23, 24]. In the terminology of Refs. [21, 22, 23, 24] the states found in Ref. [7] are examples of the so called “edge states”. The approach of Ref. [7] can be used further to analyze multiparticle entanglement. In particular, one can try to “split” the covariance matrix of $n \times n$ state in a way to get $m \times m \times m$ state with some bound entanglement properties. Indeed, we have recently managed to solve the separability problem for the case of tripartite system with one mode per each party [25]. The result of Werner and Wolf appeared first a little surprising in the view of Refs. [18, 19, 20]. Recently, some of us have been able to clarify this and solve ultimately the separability [26] and distillability [27] problems for Gaussian states of two parties sharing arbitrary number of modes. While the PPT property remains a valid necessary and sufficient condition for non-distillability, the separability criterion has a complex form of a nonlinear map for covariance matrices.

Finally, it is worth mentioning that it is not known yet whether there exist BES which do not have PPT, even though there is a strong indication of this fact [28]. If this were finally true, this would have important implications in the context of distillation [29], since it may well happen that by mixing two NDS one obtains a distillable one.

3.2 QUESTION OF GENERICITY: THE STRUCTURAL POINT OF VIEW

There is one open question whether the given CV entanglement represents a *generic* entanglement in the sense that it has infinite Schmidt number (see [13]), i. e. whether it is the limit of matrices whose Schmidt number goes to infinity. This means that, in principle, in order to generate the state, one would have to be able to generate the states of arbitrary Schmidt rank. However, some of the CV BES states similar to “spurious” ones could have also this property - if a finite dimensional $n \otimes n$ PPT states with Schmidt rank of order $O(n^\alpha)$ with some $0 < \alpha \leq 1$ existed, then we could put in the expression (17.16) the $k_n \otimes k_n$ states σ_n with the rank $O(k_n^\alpha)$ where say $k_{n+1} = 2(\sum_{i=1}^n k_n)$. Thus, we see that in order to describe the generic CV entangled states it seems reasonable to require the stronger version the notion of infinite Schmidt number. Intuitively,

it should mean that the pure states with infinite Schmidt rank are necessarily involved in the mixed state representation. One possible definition would be that a generic CV state with infinite Schmidt rank should be necessarily of the form $\varrho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$, with $|\Psi_i\rangle$ not necessarily orthogonal, but with *at least one* $|\Psi_i\rangle$ of infinite rank. Such states obviously exist – take for instance one pure state of infinite Schmidt rank, or a convex combination of two such states. However, in the above definition the precise notion of the decomposition in the CV case in the sense of Ref. [30] has to be specified. Another possible definition (which seems to be significantly weaker) would be to require the generic CV state to be the limit of $n \otimes n$ states of Schmidt rank n^α for some $0 < \alpha \leq 1$.

Concerning BES – we do not know whether there exists any BES for CV with PPT property, having at the same time the feature of being a generic CV state, whatever it would mean. It is worth stressing at this point that according to the results of Ref. [31], PPT entangled state in $n \otimes n$ space are expected to have Schmidt number smaller than n . In fact, in the Appendix A, we present the arguments analogous to those used in Ref. [31] that the typical PPT bound entangled states in $n \otimes n$ space either have the Schmidt number of order $O(1)$, or their partial transpose have this property. It is possible, however, that the recently introduced Gaussian bound entangled states [7, 26] satisfy all requirements as far as the CV genericity is concerned. It would thus be interesting to analyze the Schmidt number of those states.

3.3 QUESTION OF GENERICITY: DISTILLATION POINT OF VIEW

In former section we have dealt with question of genericity of CV state as far as *the structure of the state is concerned*. Bound (nondistillable) entanglement is directly related to distillation procedures. It is important to address the question from different point of view i. e. analysing the output of distillation procedure from the point of view of genericity.

The present result of section II clearly shows that NDS in the sense of standard definition (that no entanglement can be distilled from given state) is nowhere dense in set of CV states. This is an important theorem generalising previous results. However in the classical definition of NDS treats both finite and infinite dimensional entanglement nondistillable. For sake of many applications the next step of study which would operationally distinguish those two quantities would be desirable.

In such approach “fully CV NDS” would be all the states that do not allow for distillation of *infinite* pure entanglement (whatever it means). This significantly increases the set of states that are interpreted as bound entangled.

As we shall see below this leads to more complicated issue. We will not give definite answers here. However further methods of investigation will be suggested.

Again, as in previous section, one of proposed definitions could be the following:

A. The state ϱ represents “fully CV free (nondistillable)” entanglement if and only if it is possible (impossible) to distill nonzero amount of pure states with infinite Schmidt rank from state ϱ .

Nonzero amount is here understood in sense of usual distillation yield (i.e. as a nonzero amount of pairs). Note that to qualify distilled entanglement in finite dimensions the condition of asymptotic approaching the maximally entangled state $|\Psi_+\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^m |e_i, e_i\rangle$ was required. It is known however that there is no maximally entangled states of infinite Schmidt rank. Thus in place of Ψ_+ one would have probably use some fixed pure state Ψ_∞ having the reduced density matrix nonsingular or at least of infinite rank (this is equivalent to the infinite Schmidt rank of Ψ_∞).

Another interesting (weaker) definition would be more in spirit of Ref. [6] where increasing sequences of finite Schmidt rank were used. Namely one can propose:

B. The state ϱ represents CV free (nondistillable) entangled if and only if it is possible (impossible) to distill nonzero amount $\eta_p > 0$ of p -Schmidt rank states with $\limsup_p \eta_p > 0$.

The main difficulty dealing with Schmidt rank in those definitions is that the operational methods of its detection in context of CV are not enough developed.

For example it is not known whether the proposal B above is equivalent to the following generalisation of the “two-qubit subspace”(see sec. II A):

the state is fully free (bound) entangled iff there is (no) n and the family of bilocal filters $A_p \otimes B_p$ such that the new n -copy states

$$\varrho'_p = A_p \otimes B_p \varrho^{\otimes n} A_p^\dagger \otimes B_p / (A_p \otimes B_p \varrho^{\otimes n} A_p^\dagger \otimes B_p) \quad (17.19)$$

violate the p -Schmidt rank test via positive map i. e. $[\mathbb{I} \otimes \Lambda_p](\varrho'_p)$ is not positive matrix. The map $\Lambda_p(X) \equiv \text{Tr}(X)I - (p-1)^{-1}X$ is $p-1$ -positive but not p -positive and was used to detect p -Schmidt rank of isotropic entangled states [13].

Dealing with the state (17.19) is not easy because even in the case of finite dimensions the possibility of asymptotically singular denominator in formulas like (17.19) leads to surprising effects (see [15]). Nevertheless, after simplification we shall utilise the above point of view. In particular, putting $A_p \otimes B_p$ equal identity we shall generalise the results of section II.

3.4 NDS FOR CV ARE NOWHERE DENSE: GENERALISATION INVOLVING SCHMIDT NUMBERS

Here, using the trace norm topology from sec. II. B we shall prove the stronger version of the main result of sect. II. Suppose for moment that as a “fully CV free entanglement” we shall treat *only* very special CV states. Namely only those form which it is possible to produce p -Schmidt number state (with p fixed but *arbitrary* high) from *a single copy* by means of special LOCC protocol given in Appendix B. The protocol is a natural generalisation of the protocol utilising reduciton criterion [14].

Those special states form the set, say D_p^1 (1 stands for “single copy” and p for Schmidt rank). This set is significantly smaller than the one formed by the classical definition of free entangled states (see sec. II. A.). If as “fully CV free states” one treats the set D_p^1 (which still seems to contain too much states, c. f. discussion of sec. III.B, but this is for dydactic purposes) than one enlarges the set of what is understood as “fully CV bound” or “fully CV nondistillable”.

Below we shall see that though the latter is larger it is still nowhere dense. To have it we need to prove that D_p^1 is (i) open and (ii) dense in set of all density operators. Any state $\varrho \in D_p^1$ satisfies by the very definition (see Appendix B) the inequality:

$$\langle \Psi | [\mathbb{I} \otimes \Lambda_p](\varrho) | \Psi \rangle = \epsilon < 0. \quad (17.20)$$

Now suppose that $\varrho' \in \tilde{B}_\eta(\varrho) = \{\varrho', ||\varrho - \varrho'||_T < \eta\}$. Then

$$\begin{aligned} |\langle \Psi | [\mathbb{I} \otimes \Lambda_p](\varrho - \varrho') | \Psi \rangle| &= |\langle \Psi | (\varrho_A \otimes I - \varrho'_A \otimes I \\ &+ (p-1)^{-1}(\varrho - \varrho') | \Psi \rangle| \leq |Tr[\varrho_\Psi(\varrho_A - \varrho'_A) \otimes I]| + \\ &|\langle \Psi | (p-1)^{-1}(\varrho - \varrho') | \Psi \rangle| \leq Tr[\varrho_A^\Psi | \varrho_A - \varrho'_A]| + \\ &(p-1)^{-1} |\langle \Psi | \varrho - \varrho' | \Psi \rangle| \leq \eta(1 + (p-1)^{-1}) \end{aligned} \quad (17.21)$$

where ϱ_A^Ψ is reduced density matrix of pure state $|\Psi\rangle\langle\Psi|$.

Where we have used two properties (i) $||\varrho_A - \varrho'_A||_T \leq \eta$ because partial trace is tracepreserving completely positive map which does not increase the trace norm $||A||_T$; (ii) $\langle \phi | A | \phi \rangle \leq ||A|| \leq ||A||_T$ for positive A where $||A||$ stands for operator norm as in sect. II.B. Thus, for $\eta < \frac{|\epsilon|}{(1+(p-1)^{-1})}$, any $\varrho' \in \tilde{B}_\eta(\varrho)$ satisfies $\langle \Psi | [\mathbb{I} \otimes \Lambda_p](\varrho') | \Psi \rangle < 0$ i. e. *ergo* belongs to D_p^1 . This implies that the latter is open. Now to prove that D_p^1 is dense one can repeat the argument of sec. II.A with $|\Psi_N\rangle \in (H_A \ominus H_A^N) \otimes (H_B \ominus H_B^N)$ being maximally entangled pure state of Schmidt rank p : $|\Psi_N\rangle = \frac{1}{\sqrt{p}} \sum_{i=1}^p |e_i, f_i\rangle$ (the only difference is that the resulting state should be shown to satisfy (17.20) which is easy to see). Thus D_p^1 is dense and open so its complement is nowhere dense in set of all

states which completes the proof. Remarkable that the line of the proof remains completely correct for “uniform” assumption [i.e., (17.20) satisfied with one ϵ for *all* natural p some $|\Psi\rangle = |\Psi(p)\rangle$] but than the assumption itself can be easily shown to be *false* in the sense that no state can satisfy it.

4. CONCLUSIONS

In this paper we have considered non-distillable states for continuous variables. In the main part of the paper we have proven that the subset of non-distillable states is nowhere dense in the set of all CV states. This is a much stronger result than the recent one by Clifton and Halvorson [12], which prove the same result for the set of separable states, since that one is contained in the set of NDS. Moreover, our results imply that the subsets of BES and PPT states are also nowhere dense. Thus, generic CV states are distillable. We have also presented some examples of BES and discussed their genericity from the point of view of CV and their Schmidt number. In the Appendix A we have presented an evidence that all PPT BES in $n \otimes n$ systems either have Schmidt number smaller than $O(1)$, or their partial transposes have this property. Finally we have analysed the genericity of CV entanglement in context of Schmidt number. In particular, we have studied the assumptions of the main theorem and proved more general result that nowhere dense is the set of all states from which it is impossible to produce p -Schmidt rank state from a single copy in some (well defined) way. The latter involves single copy protocol (provided in Appendix B) being a generalisation of that obtained with help of reduction criterion. By providing some proposals of definitions of what can be treated as “fully CV” we have shown that further investigation of genericity in context of CV is desirable.

We thank Anna Sanpera, Dagmar Bruß, Geza Giedke and Otfried Gühne for useful discussions. This work has been supported by the DFG (SFB 407 and Schwerpunkt “Quanteninformationsverarbeitung”), the Austrian Science Foundation (SFB “control and measurement of coherent quantum systems”), the European Union Programme “EQUIP” (IST-1999-11053) and the Institute for Quantum Information GmbH. Part of the work was completed at The Erwin Schrödinger International Institute for Mathematical Physics, during the Program “Quantum Measurement and Information”, Vienna 2000.

Appendix: Schmidt number of PPT BES for $n \otimes n$ systems

In this Appendix we essentially repeat the arguments used in the Ref. [31] to support the conjecture that in $3 \otimes 3$ systems all PPT BES have Schmidt number 2. We consider now the $n \otimes n$ case, with n large. Let $r(\rho)$ denotes the rank of ρ ; our aim is to present a strong evidence for the following conjecture:

Conjecture .- All PPT entangled states in $n \otimes n$ systems either have Schmidt number of the order of $O(1)$ or their partial transposes have this property.

Note, that this conjecture concerns for instance projections of the PPT BES (17.17) onto $n \otimes n$ spaces. We observe that

- It is enough to show the conjecture for the, so called, edge states [22, 23, 24], i.e. the PPT states δ such that there exist no product vector $|e, f\rangle$ in their range, such that $|e^*, f\rangle$ is in the range of the partially transposed operator δ^{TA} .
- Let $r(\rho)$ denotes the rank of ρ . It is likely that it is enough to prove the conjecture for the edge states of maximal ranks [22], i.e. those whose ranks fulfill $r(\delta) + r(\delta^{TA}) = 2n^2 - 2n + 1$. We expect that such states are dense in the set of all edge states. To show the latter statement, we consider an edge state $\tilde{\delta}$ which does not have maximal ranks. We can always add to it infinitesimal amount of projectors on product vectors destroying the edge property. The resulting state ρ would have more product states in its range, than the product states used to destroy the edge property. Subtracting projector on product states different from the latter ones, would typically allow to construct an edge state δ with maximal ranks, which would be infinitesimally close to $\tilde{\delta}$ in any norm.
- Let $R(A)$, $K(A)$ denotes the range and kernel of A , respectively. The canonical form of an non-decomposable entanglement witness that detects the edge state δ is ([23, 24], see also [32])

$$W = P + Q^{TA} - \epsilon \mathbf{I}, \quad (17.A.1)$$

where the positive operators P, Q have their ranges $R(P) = K(\delta)$, $R(Q) = K(\delta^{TA})$, and $\epsilon > 0$ is sufficiently small so that for any product vector $\langle e, f | W | e, f \rangle \geq 0$.

- If we can show that for any edge state with maximal ranks and any corresponding witness W detecting its entanglement, there exist a vector $|\psi^s\rangle$ of Schmidt number s such that $\langle \psi^s | W | \psi^s \rangle < 0$, then we would conclude that all edge states with maximal ranks, and thus all edge states, and thus all PPT entangled state have the Schmidt number $< s$. Equivalently, it is sufficient to show that $\langle \psi^s | W + \epsilon \mathbf{I} | \psi^s \rangle \leq 0$.

Let us therefore try to construct the desired vector $|\psi^s\rangle$ of Schmidt number s . In general such (unnormalized) vector will have a form

$$|\psi^s\rangle \propto \sum_{i=1}^s l_i |e_i, f_i\rangle, \quad (17.A.2)$$

where l_i are arbitrary complex coefficients for $i = 1, \dots, s$, and $|e_i, f_i\rangle$ are linearly independent product vectors for $i = 1, \dots, s$. Note, that the vector (17.A.2) depends on s complex parameters l_i for $i = 1, \dots, s$, whereas each of the s vectors $|e_i\rangle, |f_i\rangle$ depends themselves of $n-1$ relevant complex parameters.

Let $r(P) = k_1$, and $r(Q) = 2n - 1 - k_1$. Since we want to prove the conjecture either for the edge state δ , or for its partial transpose, without loosing the generality, we may assume that $k_1 \geq 1$. We may then single out one projector out of P , and write $P = P_1 + |\Psi\rangle\langle\Psi|$, where $P_1 \geq 0$, $r(P_1) = r(P) - 1$, and $|\Psi\rangle$ is in the range of P . We can choose then $|e_i, f_i\rangle$ in such a way that $Q|e_i^*, f_i\rangle = 0$, and $P_1|e_i, f_i\rangle = 0$. These are effectively $2n - 2$ equations for vectors $|e_i, f_i\rangle$ which depend on $2n - 2$ parameters, so that we expect a finite, but quite large number of solutions (c.f. [22]). At the same time, $\langle\psi^s|Q|\psi^s\rangle$ will become a quadratic hermitian form of l_i 's with vanishing diagonal elements. Such a hermitian form has typically more than one dimensional subspace \mathcal{N} of negative eigenvalues for large s . But, one has to fulfill also the last equation implied by $\langle\psi^s|\Psi\rangle = 0$; this limits the values of l_i to a hyperplane, which should have at least one dimensional common subspace with the subspace of negative eigenvalues \mathcal{N} . This would prove that either the Schmidt number of δ or of δ^{TA} is of the order of 1.

Note that for a given δ , if the presented construction can be shown to be successful for every witness of δ , then it provides a sufficient condition for the state δ to have the Schmidt number smaller than s .

Appendix: Producing state of p -Schmidt rank form single CV copy

In this Appendix we briefly show how to produce (by means of local operations and classical communication - LOCC) the p -Schmidt rank state from any CV state violating the separability condition

$$[\mathbb{I} \otimes \Lambda_p](\varrho) \geq 0. \quad (17.B.1)$$

Following Ref. [20] this is further generalisation of the distillation protocol of Ref. [14] where the above criterion with $p = 2$ (called reduction criterion c. f. [34]) has been used. The separability tests of the form (17.B.1) (which can be called $p - 1$ -reduction criteria) for $p > 2$ considered first in [13] are examples of general positive maps separability tests (see [33]).

Consider some CV state ϱ and suppose that there exists $|\Psi\rangle$ such that $\langle\Psi|[\mathbb{I} \otimes \Lambda_p](\varrho)|\Psi\rangle = \epsilon < 0$. Then following arguments of Ref. [20] we get that there must exist N such that for any $m > N$ the new $m \otimes m$ state ϱ_m produced from ϱ by projection onto the finitedimensional support of $\mathcal{H}_m \otimes \mathcal{H}_m$ satisfies

$$\langle\Psi|[\mathbb{I} \otimes \Lambda_p](\varrho_m)|\Psi\rangle \leq \frac{\epsilon}{2} < 0. \quad (17.B.2)$$

Now instead of $|\Psi\rangle$ we put $|\Psi'\rangle$ being a normalised projection of $|\Psi\rangle$ on support of ϱ_m . In this way we get the inequality identical to the one of [14] with the only difference that p was equal 2 there. This allows to repeat the reasoning of Ref. [14]: after the application of suitable local filtering and $U \otimes U^*$ twirling to ϱ_m one produces the $m \otimes m$ isotropic state $\varrho_{is} = (1-q)\frac{I}{m^2} + q|\Psi_+\rangle\langle\Psi_+|$ with the fidelity $F \equiv \langle\Psi_+|\varrho_{is}|\Psi_+\rangle > \frac{p-1}{m}$. But the latter implies (see [13]) that the final state (produced from initial ϱ by means of local operations and classical communication - LOCC) has the Schmidt number at least p . This concludes the analysis. Note that further steps of recurrence protocol with generalised XOR ([14]) can be applied.

Notes

1. Subsequently we shall denote by $n \otimes n$ states the states of quantum systems defined on the Hilbert space $\mathcal{H} = \mathcal{C}^n \otimes \mathcal{C}^n$. The space will be sometimes called “ $n \otimes n$ space”.

References

- [1] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
- [2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
- [3] P. Horodecki, M. Horodecki and R. Horodecki, Phys. Rev. Lett. **82**, 1046 (1999).
- [4] M. Murao, V. Vedral, Phys. Rev. Lett. **86**, 352 (2001); P. W. Shor, J. A. Smolin, and A. V. Thapliyal, quant-ph/0005117. W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999); W. Dür and J. I. Cirac, Phys. Rev. A **62**, 22302 (2000).
- [5] See S. Braunstein and J. Kimble, quant-ph/9910010, and references therein; for experiments see A. Furusawa *et al.* Science **282**, 706 (1998).
- [6] P. Horodecki and M. Lewenstein, Phys. Rev. Lett. **85**, 2657 (2000).
- [7] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).
- [8] K. Życzkowski, P. Horodecki, A. Sanpera and M. Lewenstein, Phys. Rev. A **58** 833 (1998); K. Życzkowski, Phys. Rev. A **60** 3496 (1999).
- [9] G. Vidal, R. Tarrach, Phys. Rev. A **59** 141 (1999).
- [10] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu and R. Schack: Phys. Rev. Lett. **83**, 1054 (1999); R. Schack and C. M. Caves, Phys. Rev. A **60**, 4354 (1999).
- [11] N. Linden and S. Popescu, Phys. Rev. Lett. **87**, 047901 (2001).
- [12] R. Clifton and H. Halvorson, Phys. Rev. A **61**, 012108 (2000).

- [13] B. M. Terhal and P. Horodecki, Phys. Rev. A **61**, 040301(R) (2000).
- [14] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4026 (1999).
- [15] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
- [16] R. V. Kadison and J. R. Ringrose, “*Fundamentals of the Theory of Operator Algebras*”, Academic Press, (1983).
- [17] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
- [18] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
- [19] R. Simon, Phys. Rev. Lett. **84** 2726 (2000).
- [20] G. Giedke, , L. M. Duan, J. I. Cirac, and P. Zoller, quant-ph/0007061.
- [21] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998); A. Sanpera, R. Tarrach and G. Vidal, Phys. Rev. A **58**, 826 (1998).
- [22] B. Kraus, J. I. Cirac, S. Karnaś, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000); P. Horodecki, M. Lewenstein, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 032310 (2000).
- [23] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. **62**, 052310 (2000).
- [24] M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac, Phys. Rev. **63**, 044304 (2001).
- [25] G. Giedke, B. Kraus, M. Lewenstein and J. I. Cirac, Phys. Rev. A **64**, 052303 (2001).
- [26] G. Giedke, B. Kraus, M. Lewenstein and J. I. Cirac, Phys. Rev. Lett. **87**, 167904 (2001).
- [27] G. Giedke, L.-M. Duan, J. I. Cirac and P. Zoller, Quant. Inf. Comp. **1**(3), 79 (2001).
- [28] D.P. DiVincenzo, P. W. Shor, J. A. Smolin, B. Terhal and A. Thapliyal, Phys. Rev. A, **61** 062312 (2000); W. Dür, J. I. Cirac, M. Lewenstein and D. Bruss, Phys. Rev. A **61** 062313 (2000).
- [29] P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **86**, 2681 (2001).
- [30] L. P. Hughston, R. Jozsa and W. W. Wootters, Phys. Lett. A **183**, 14 (1993).
- [31] A. Sanpera, D. Bruss, M. Lewenstein, Phys. Rev. A **63**, 050301 (R) (2001).
- [32] B. Terhal, Lin. Algebr. Appl. **323**, 61 (2000).
- [33] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. A **223**, 1 (1996);
- [34] N. Cerf, C. Adami, and R. M. Gingrich, Phys. Rev. **60**, 898 (1999).

Chapter 18

ATOMIC CONTINUOUS VARIABLE PROCESSING AND LIGHT-ATOMS QUANTUM INTERFACE

Alex Kuzmich

Norman Bridge Laboratory of Physics 12-33

California Institute of Technology, California 91125, USA

kuzmich@caltech.edu

Eugene S. Polzik

QUANTOP - Quantum Optics Center

Danish National Research Foundation

Institute of Physics and Astronomy, University of Aarhus, Denmark

polzik@ifa.au.dk

Abstract In this Chapter methods for generation of squeezed and entangled states of atomic ensembles are described along with the protocols for quantum state exchange between light and atomic samples. Realization of these protocols provides the means to store/retrieve quantum information transmitted by light in/from atomic samples, which can be used for processing of this information. Polarization variables (Stokes parameters) of a multi-photon light pulse and spin components of a multi-atom atomic ensemble are the continuous variables employed in these protocols. Two different methods for a quantum state exchange are analyzed: (a) mapping of non-classical states of light onto atomic spins via complete absorption of resonant light, (b) teleportation-like transfer of a quantum state via a QND-type interaction between off-resonant light and atoms.

1. INTRODUCTION

The ability to implement quantum interfacing between light and matter is crucial for many aspects of quantum information processing including distributed computing, quantum networks, computational complexity, eavesdropping in quantum cryptography, to name a few. Continuous field and atomic variables have a dramatic practical advantage for this type of operations compared to

single-particle qubits, namely efficient quantum state exchange for the former can be achieved without high-Q cavities necessary for operations with the latter. Whereas efficient quantum state exchange between single photons and single atoms requires cavity QED with strong coupling [1], efficient state exchange between collective quantum variables of light and atoms can be achieved in free space with very weak interaction on a single photon/single atom level. “Strong” interaction in case of continuous variables for multiphoton pulses and multi-atom samples reduces to high on-resonance optical density of the atomic sample, which is easy to achieve experimentally.

An efficient quantum state interaction between light and atoms at the level of continuous variables allows to carry out a number of quantum state/quantum information processing protocols. In this chapter we will describe some of them with the emphasis on experimental implementation. First we will define continuous variables for atomic spin polarized ensembles and polarized light and introduce coherent, squeezed and entangled spin states. We will then consider mapping of a quantum state of light onto atomic state via complete absorption of resonant squeezed light. This method of mapping a quantum state of resonant light onto atoms (Section 2) has been proposed in [2], further investigated in [3, 4], and experimentally implemented for generation of spin squeezing in [5]. Next we will discuss an off-resonant dispersive interaction of light and atomic ensembles. This approach proved to be especially successful in several aspects. We will show how it allows for a quantum non-demolition (QND) measurement of spin projection leading to generation of a spin squeezed state [6]. An important problem of atomic teleportation for continuous variables will be considered. Teleportation requires a resource of entanglement, more specifically distant entangled atomic samples are needed. Whereas both discrete and continuous variable entangled (EPR) states of light have been successfully generated by several groups [7, 8, 9], entanglement of distant atomic systems has been experimentally achieved only recently [10] with continuous variables following the proposals [11, 12]. Its applications to atomic teleportation and interspecies light-atoms teleportation will be considered.

2. CONTINUOUS QUANTUM VARIABLES FOR POLARIZED LIGHT AND SPIN-POLARIZED ATOMS

In this section we introduce continuous variables for light and atoms, which will be used for all quantum protocols throughout the Chapter. Quantum state of a polarized pulse of light will be described by the Stokes operators such as $\hat{S}_x = \frac{c}{2} \int_0^T (\hat{a}_+^\dagger(\tau) \hat{a}_-(\tau) + \hat{a}_-^\dagger(\tau) \hat{a}_+(\tau)) d\tau$, $\hat{S}_y = \frac{c}{2i} \int_0^L (\hat{a}_+^\dagger(\tau) \hat{a}_-(\tau) - \hat{a}_-^\dagger(\tau) \hat{a}_+(\tau)) d\tau$, $\hat{S}_z = \frac{c}{2} \int_0^L (\hat{a}_+^\dagger(\tau) \hat{a}_+(\tau) - \hat{a}_-^\dagger(\tau) \hat{a}_-(\tau)) d\tau$. $\hat{a}_+(t)$ and $\hat{a}_-(t)$ are annihilation operators for two circular polarizations propagating along the

z axis, with commutation relations $[\hat{a}_i(t), \hat{a}_j(t')] = \delta_{ij}\delta(t - t')$, $i, j = +, -$. The Stokes parameters obey the standard spin commutation relations,

$$[\hat{S}_y, \hat{S}_z] = i\epsilon_{xyz}\hat{S}_x. \quad (18.1)$$

In the following we will assume that light is polarized in the classical sense along the x axis, i.e. that only \hat{S}_x has a non-zero mean value. All the interactions considered below introduce only minute changes in the mean polarization, and therefore we substitute \hat{S}_x with its classical mean value $\langle \hat{S}_x \rangle$.

Analogous to polarized light, a quantum state of a collection of N spin 1/2 atoms can be described by its collective spin $\hat{\mathbf{F}} \equiv \sum_{k=1}^N \hat{\mathbf{F}}^{(k)}$ with commutation relations

$$[\hat{F}_y, \hat{F}_z] = i\epsilon_{xyz}\hat{F}_x. \quad (18.2)$$

As with light, we will assume that atoms are spin polarized in the classical sense along the x axis, and that this mean polarization does not change much. Therefore the quantum states of polarization, both for light and atoms, considered here are generated by small rotations of the collective spin (Stokes vector for light) around its mean value. A formal analogy between the multi-particle spin ensembles considered here and standard position/momentum-like continuous variables in the phase plane comes from the commutation relations (18.1,18.2). Under the assumption of small spin rotations, the right hand sides of these equations are constants. Dividing the equations by the absolute values of their right hand sides, one obtains standard commutation relations of position/momentum for normalized spin variables. The procedure of substituting small rotations on the Bloch sphere with displacements on the plane is known [13] as *contraction* of the group $SU(2)$ to group $U(1)$. For example, for small rotations around the $|F, -F\rangle$ state (that is, the state with mean polarization along the z -axis), this is achieved with the following correspondence between the generators of the groups:

$$\begin{aligned} \hat{F}_+ &\rightarrow \hat{a}^\dagger, \\ \hat{F}_- &\rightarrow \hat{a}, \\ (\hat{F}_z + F) &\rightarrow \hat{a}^\dagger \hat{a}, \end{aligned} \quad (18.3)$$

(analogous relations hold for the Stokes vector of light, of course). This contraction of the group $SU(2)$ onto the group $U(1)$ is at the heart of the approaches to continuous quantum information processing that we describe below. The spin formalism allows us to treat light and atoms on an equal footing. In the following, when it is not specified otherwise, “spin” refers to both light and atoms.

2.1 COHERENT SPIN STATES

For concreteness, let us choose the z-axis as the quantization axis and let us write the state $|\frac{\pi}{2}, 0\rangle$ (i.e. with all spins oriented along the x-axis) in the basis of eigenstates of \hat{F}_z :

$$|\frac{\pi}{2}, 0\rangle = 2^{-F} \sum_{m=-F}^F \binom{2F}{F-m}^{\frac{1}{2}} |F, m\rangle. \quad (18.4)$$

Here $F \equiv N/2$. When N is a large number, it is possible to write this CSS in the approximate form

$$|\frac{\pi}{2}, 0\rangle = (\pi F)^{-1/4} \sum_{m=-F}^F \exp\left(-\frac{m^2}{2F}\right) |F, m\rangle. \quad (18.5)$$

Commutation relations (18.2) for the spin $\hat{\mathbf{F}}$ have Heisenberg uncertainty relationship associated with them

$$\langle(\Delta\hat{F}_x)^2\rangle\langle(\Delta\hat{F}_y)^2\rangle \geq \frac{1}{4}|\langle\hat{F}_z\rangle|^2, \quad (18.6)$$

plus cyclic permutations. Here we define the variance of the operator \hat{A} by $(\Delta A)^2 \equiv \langle\hat{A}^2\rangle - \langle\hat{A}\rangle^2$. The CSS (18.5) satisfies the minimum uncertainty product allowed by (18.6), and so, is a *minimum uncertainty state*. For example, it is straightforward to show that for the state in Eq.(18.4) $\langle(\Delta\hat{F}_z)^2\rangle = \langle(\Delta\hat{F}_y)^2\rangle = F/2$, while $\langle\hat{F}_x\rangle = F$, so that the equality in (18.6) holds. CSS can not exceed the *standard quantum limit* (SQL) of phase measurement accuracy $\delta\phi_{SQL}$ given by $1/\sqrt{N}$, where N is the number of elementary $1/2$ spins.

2.2 SQUEEZED SPIN STATES

A spin state $\hat{\mathbf{F}}$ is called a *Squeezed Spin State* (SSS) if the *squeezing parameter* η defined by

$$\eta = 2F \frac{\langle(\Delta\hat{F}_{\perp})^2\rangle}{|\langle\hat{F}_{\theta,\phi}\rangle|^2} \quad (18.7)$$

is less than 1 for some (θ, ϕ) . Here \hat{F}_{\perp} is spin component in a direction orthogonal to (θ, ϕ) . The squeezing parameter η determines the accuracy of phase measurement $\delta\phi$:

$$\delta\phi = \sqrt{\frac{\eta}{N}}. \quad (18.8)$$

It is possible to show that for a CSS the minimum value of η is 1. Moreover, it has been shown [14] that there exist no *unentangled* spin states (in which the collective spin state is the direct product of single-spin states) for which the value of the squeezing parameter η is below unity. The only way to reduce η (and, as we see from Eq.(18.8), to enhance the accuracy of phase measurements) is to introduce quantum-mechanical correlations between individual spins.

Many different *entangled* classes of states have been proposed theoretically (see, for example, Refs. [15, 16, 17, 18] and references therein) that satisfy the definition of SSS. In most practical situations of interest the SSS's are entangled rather weakly. Then a SSS can be written as ($\chi \ll 1$):

$$\left| \frac{\pi}{2}, 0, \chi \right\rangle = \frac{(\pi F)^{-1/4}}{\sqrt{1 + 3\chi^2 F}} \sum_{m=-F}^F \exp \left(-\frac{m^2(1 + 3\chi^2 F)}{2F} \right) |F, m\rangle, \quad (18.9)$$

where the squeezing parameter η is related to χ by $\eta = 1/(1 + 3\chi^2 F)$. For this SSS \hat{F}_z has reduced variance $\langle (\Delta \hat{F}_z)^2 \rangle = \frac{F}{2}(1 + 3\chi^2 F)^{-1}$, while the variance of \hat{F}_y is increased, $\langle (\Delta \hat{F}_y)^2 \rangle = \frac{F}{2}(1 + 3\chi^2 F)$. For $\chi \ll 1$ $\langle \hat{F}_x \rangle \simeq F$, so that this state is a minimum uncertainty one.

2.3 EPR SPIN STATES

Another important class of entangled spin states are *EPR-correlated spin states*. An important feature of these states is that they describe two *distant* spins that are correlated in a non-classical way. It is rather cumbersome to describe this kind of entanglement in the Schrodinger picture that we used above for CSSs and SSSs. Instead, in the Heisenberg picture, the spin components satisfy the following relations

$$\begin{aligned} \hat{F}_{x1} + \hat{F}_{x2} &= \sqrt{2} \exp(-r) \hat{F}_{xv}, \\ \hat{F}_{y1} - \hat{F}_{y2} &= \sqrt{2} \exp(-r) \hat{F}_{yv}, \end{aligned} \quad (18.10)$$

where \hat{F}_{xv} , \hat{F}_{yv} are x- and y- spin components of an auxiliary spin in a CSS directed along the z-axis (we assume that all three spins have the same length F). r is the parameter that characterizes the strength of the quantum correlations between these two spatially separated spins.

For two spins with opposite classical orientation, $\langle \hat{F}_{z1} \rangle = -\langle \hat{F}_{z2} \rangle$, the necessary and sufficient condition for entanglement can be formulated in terms of the variances of measured quantities [19] as

$$\left\langle \left(\Delta(\hat{F}_{x1} + \hat{F}_{x2}) \right)^2 \right\rangle + \left\langle \left(\Delta(\hat{F}_{y1} - \hat{F}_{y2}) \right)^2 \right\rangle < 2\langle \hat{F}_z \rangle. \quad (18.11)$$

The interpretation of this condition follows from the fact that for both spins in CSSs the following equality holds: $\langle (\Delta(\hat{F}_{x,y}))^2 \rangle = \frac{1}{2}\langle \hat{F}_z \rangle$. Entanglement between the elementary spins of the two samples is, therefore, according to the above condition equivalent to the spin variances smaller than that for samples in a CSSs, which is characterized by uncorrelated individual atoms. The entangled state of this type is a two-mode squeezed state for the continuous spin variables.

3. LIGHT-ATOMS STATE TRANSFER VIA RESONANT INTERACTION

One of the fundamental operations of the continuous quantum information processing is the quantum mapping of a (short-lived) field mode state into a corresponding quantum state of a collection of (long-lived) atomic spins and backwards (such procedures are often called quantum memory writing and reading). One of the ways to achieve such a mapping is by complete absorption of e.-m. field by the atoms. In particular, absorption of squeezed states of light gives rise to SSSs of atoms.

We consider free space illumination of a collection of atoms by a beam of squeezed light. The discussion is limited to excited states of atoms, which are not directly suitable for memory purposes. However, it is instructive to consider this case anyway, for which 50% of the amount of squeezing of the exciting optical field can be transferred onto spin squeezing of the excited atomic states. The limitation on the degree of atomic spin squeezing is due to spontaneous emission. Further development of this approach for ground state atoms and Raman transitions has been proposed [3].

3.1 THEORY

Let us consider the propagation of quantum correlated e.-m. fields through an atomic medium which fully absorbs (and spontaneously re-emits) the incoming light field. In the process of propagation some quantum statistical properties of the field are altered by the interaction with atoms. The atoms acquire certain quantum features of the field via the absorption mechanism, and at the same time, spontaneously emit photons. In the steady state the scattered and the incoming light intensities are identical and they are proportional to the total excited state population of the atomic medium. In the limit of weak fields, the emission is also coherent; both the scattered field amplitude, and the atomic dipole amplitude are proportional to the incoming field amplitude. This suggests that certain collective atomic operators exhibit new and non-classical noise properties due to the interaction with the fields. We consider a V-transition with each arm $0 \leftrightarrow 1(2)$ interacting with a separate quantum field, $\hat{a}_{1(2)}$ (see Fig. 18.1). The two excited states can be two magnetic sublevels (say, with $m = 1$ and $m = -1$) in which case the spin will correspond to the orientation

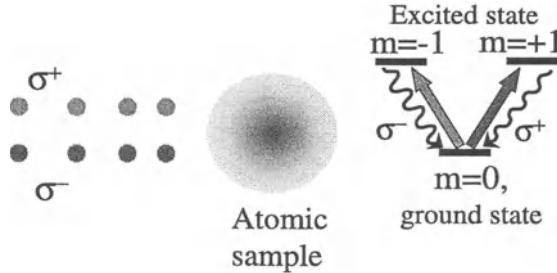


Figure 18.1 Spin squeezing of an excited state via complete absorption of squeezed light. Linearly polarized squeezed light can be viewed as a superposition of quantum correlated modes in right- and left-circular polarizations. When these modes excite the atomic state as shown in the Figure, quantum correlations (squeezing) are partially transferred to the atomic state. Spontaneous emission which prevents perfect transfer is also shown.

and/or alignment of the excited ensemble. Alternatively, the two states can be two hyperfine sublevels. We treat the case when the $0 - 2$ transition interacts with a squeezed vacuum mode, and the $0-1$ transition interacts with a coherent field mode. To analyze the noise properties of the collective upper-states atomic coherence \hat{F}_{12} we assume that the coherent amplitude α is much stronger than the squeezed vacuum fluctuations, and subsequently that the coherent part of \hat{F}_{01} is much greater than the fluctuating quantity \hat{F}_{02} . The mean spin is along the z -direction and has a value equal to half of the total atomic population in the excited state $|1\rangle$:

$$\langle \hat{F}_z \rangle = \frac{\langle \hat{a}_1^{in\dagger} \hat{a}_1^{in} \rangle}{2\gamma}, \quad (18.12)$$

$\langle \hat{F}_x \rangle = \langle \hat{F}_y \rangle = 0$. The components where we shall look for squeezing are $\hat{F}_{x,y}$. Detailed calculations [2] result in the collective atomic operator \hat{F}_{12} at frequency Δ being expressed simply in terms of the incident and the transmitted field operators:

$$\tilde{\hat{F}}_{12}(\Delta) \simeq \frac{\alpha^*}{\gamma - i\Delta} \hat{a}_2^{(in)}(\omega_1 + \Delta) + \frac{\alpha^*}{\gamma - i\Delta} \hat{d}_2^{(in)}(\omega_1 + \Delta) \quad (18.13)$$

Here γ is the rate of spontaneous decay, ω_1 is the frequency of the atomic transition, $\hat{a}_2^{(in)}(\omega_1 + \Delta)$ is the annihilation operator describing the incident

squeezed vacuum field, $\hat{d}_2^{(in)}(\omega_1 + \Delta)$ is the annihilation operator describing the bath of the spontaneous decay modes.

Let us examine if the $\hat{F}_{x,y}$ are squeezed. We find from Eq.(18.13) that the variances of the atomic spin components are linked to the quadrature phase variances $\hat{X}_{x,y}^2$ of the input field \hat{a}_2 :

$$\langle \hat{F}_{x,y}^2 \rangle = \frac{1}{4} \langle \hat{F}_z \rangle \left(4 \langle \hat{X}_{x,y}^2 \rangle + 1 \right). \quad (18.14)$$

For the vacuum input field \hat{a}_2 the variances $4 \langle \hat{X}_{+, -}^2 \rangle = 1$ and the x, y spin variances are equal to $\frac{1}{2} \langle \hat{F}_z \rangle$ as would be expected for the coherent spin state. With broadband squeezed vacuum as input field \hat{a}_2 , one of the variances vanishes, e.g. $\langle \hat{X}_x^2 \rangle = 0$, and we obtain the spin squeezed state with 50% degree of squeezing: $\langle \hat{F}_x^2 \rangle = \frac{1}{4} \langle \hat{F}_z \rangle$.

In the example above spin squeezing is achieved in an off-diagonal element of the excited state orientation. By slightly changing the geometry of the experiment one can also achieve squeezing in the diagonal elements, i.e. in the population difference between the two excited states. In order to achieve this goal the coherent and squeezed vacuum fields with orthogonal polarizations should be mixed at a polarizer to produce quantum correlated left- and right-circularly polarized fields \hat{a}_1 and \hat{a}_2 . With the average atomic spin oriented along the direction of the coherent polarization x , either \hat{F}_y or \hat{F}_z components can be squeezed by 50%, depending on the phase difference between the squeezed vacuum and the coherent beam. The latter case ("longitudinal spin squeezing") corresponds to sub-Poissonian fluctuations in the population difference between the two excited states.

3.2 EXPERIMENT

The experimental realization of this proposal has been carried out with a collection of cold Cesium atoms confined in a magneto-optical trap [5, 20]. Atoms are excited with a weak quantum pump (Fig.18.2) from the ground state to the excited state $6P_{3/2}, F = 5$ (hereby abbreviated as $6P$). The pump is a mixture of the x -polarized coherent beam and y -polarized squeezed vacuum produced by a frequency tunable optical parametric oscillator below threshold. A weak linearly polarized probe in the configuration shown in Fig.18.2 is sensitive to the following three operators: \hat{F}_z , $\hat{F}_x^2 - \hat{F}_y^2$, and $\hat{F}_x \hat{F}_y + \hat{F}_y \hat{F}_x$ [21]. These are spin operators describing the entire $6P$ ensemble. They obey the commutation relation $\frac{i}{2} [\hat{F}_z, \hat{F}_x \hat{F}_y + \hat{F}_y \hat{F}_x] = \hat{F}_x^2 - \hat{F}_y^2$. We consider these three components as components of a quasi-spin operator. With the coherent component of the excitation polarized along the x axis the only component of the spin polarization with a non-zero mean is $\langle \hat{F}_x^2 - \hat{F}_y^2 \rangle$. The uncertainty relation following from the commutation relation is: $\delta(\hat{F}_z) \delta(\hat{F}_x \hat{F}_y + \hat{F}_y \hat{F}_x) \geq$

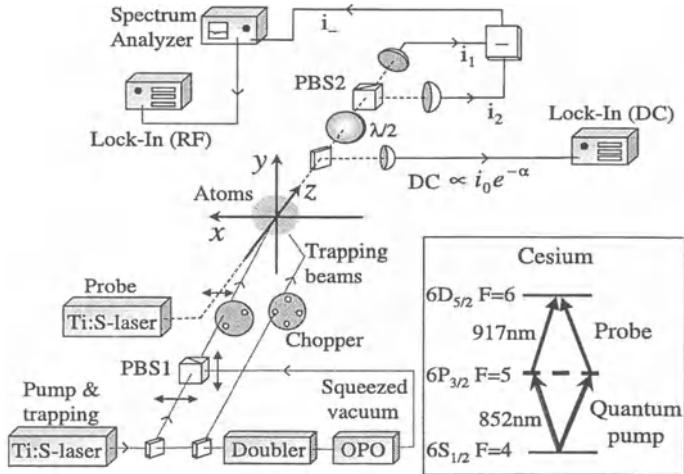


Figure 18.2 Outline of the experimental set-up.

$|\langle \hat{F}_x^2 - \hat{F}_y^2 \rangle|$. Since the operators describe the whole ensemble, the right hand side of this inequality is proportional to the number of atoms N in the $6P$ state. Excitation of the atoms with coherent light will lead to the quantum noise of the z component $\delta(\hat{F}_z)_{coh} = \sqrt{5|\langle \hat{F}_x^2 - \hat{F}_y^2 \rangle|/(2F + 3)} \sim \sqrt{N}$ due to the uncorrelated noise of individual atomic spins. Following the theory described in the previous section, one should expect that injection of the squeezed e.-m. vacuum into the other port of the polarizer PBS1 (Fig.18.2) should lead to squeezed $\delta(\hat{F}_z)_{sq} < \delta(\hat{F}_z)_{coh}$ or antisqueezed $\delta(\hat{F}_z)_{antisq} > \delta(\hat{F}_z)_{coh}$ spin states depending on the phase of the squeezed vacuum field.

Turning now to the experiment, about 10^9 Cs atoms have been collected in a magneto-optical trap. The spin noise of the $6P$ state has been detected using the probe polarization noise technique described in detail in Ref.[22](Fig. 18.2). The change in the probe differential photocurrent noise caused by atoms is

$$\delta i^2(\Delta) = -[1 - \exp(-\alpha_\Delta)] + s\alpha_0 \exp(-2\alpha_\Delta)(\delta\hat{F})^2$$

$(\delta\hat{F})^2$ is the atomic noise contribution depending on the geometry of the experiment, α_Δ is the probe optical depth at detuning Δ , s is the saturation parameter of the probe light. The expression for δi^2 is normalized to the probe shot noise in the absence of atoms. The term in square brackets is the probe shot noise reduction δi_{shot}^2 due to the absorption and the rest is the atomic noise contribution of interest. Note that in the limit of small optical depth α_Δ this

expression is similar to the Eq.(18.17) for the polarization component of the off-resonant probe described in detail below.

When atoms are excited in $6P$ state with linearly polarized coherent light, a certain level of atomic noise $(\delta \hat{F})^2$ corresponding to the coherent spin state is measured. When squeezed light is used for excitation instead, a different level of $(\delta \hat{F})^2$ is generated. If this level is lower the spin state is squeezed. The squeezed light after PBS1 will have fluctuations in either the polarization axis direction or in the ellipticity (depending on the phase) reduced below the noise level of the coherent field (Standard Quantum Limit - SQL). For the ellipticity-squeezed light, the fluctuations in the intensity difference between the σ^+ - and σ^- -polarized components of the pump field are reduced below the SQL. This gives reduced fluctuations in the difference between the number of atoms in the $+m$ and $-m$ Zeeman levels. This difference in populations is described quantitatively by the collective spin component \hat{F}_z . Thus, the ellipticity-squeezed light gives reduced fluctuations in \hat{F}_z , whereas the polarization-squeezed light is antisqueezed in ellipticity resulting in increased \hat{F}_z noise and reduced $\hat{F}_x \hat{F}_y + \hat{F}_y \hat{F}_x$ noise. Squeezed vacuum with the central frequency resonant with the pump transition is generated in the sub-threshold optical parametric oscillator (OPO). The amount of squeezing is quantified by the variance of the quadrature phase operator $X_{\pi/2}^2$ of the e.-m. field polarized along y and out-of-phase with the coherent component of the pump. For perfectly squeezed ellipticity $X_{\pi/2}^2 = 0$ and for coherent fields/ordinary vacuum $4X_{\pi/2}^2 = 1$. In order to achieve the best mapping of quantum properties of light onto atoms, the optical depth for the quantum pump is sustained at the highest possible level, $\alpha_{pump} \approx 4$. We concentrate on the measurement of δF_z because the sensitivity of our polarization measurements to squeezing of the conjugated variable $\delta(\hat{F}_x \hat{F}_y + \hat{F}_y \hat{F}_x)$ is found to be much smaller.

The experimental results presented in Fig.18.3 are normalized to the atomic spin noise corresponding to the SQL achieved with coherent excitation (horizontal line). When the squeezed vacuum is out-of-phase with the coherent component of the pump, $4X_{\pi/2}^2 > 1$. This phase corresponds to the quantum noise of the spin component \hat{F}_z above the coherent spin noise level. The observed excess noise is plotted in Fig.18.3 as dots. The spectrum of the observed antisqueezed excess spin noise can be written as $\delta i_{antisq}^2(\Delta) - \delta i_{coh}^2(\Delta) \propto \tilde{D}^2(\Delta) \left((\delta \hat{F}_z)^2 - (\delta \hat{F}_z)_{coh}^2 \right)$. The excess spin noise is expected to have the spectral shape given by the square of the Doppler broadened dispersion profile $\tilde{D}^2(\Delta)$. We introduce η , the mapping-readout efficiency for quantum correlations, by relating the observed spin noise to $4X_{\pi/2}^2$. With Δ_{max} being the detuning giving the maximum excess noise we get: $\delta i_{antisq}^2(\Delta_{max}) = \frac{1}{\eta+1} (1 + \eta 4X_{\pi/2}^2) \delta i_{coh}^2(\Delta_{max})$. $\eta = 1$ gives 50% of noise reduction for per-

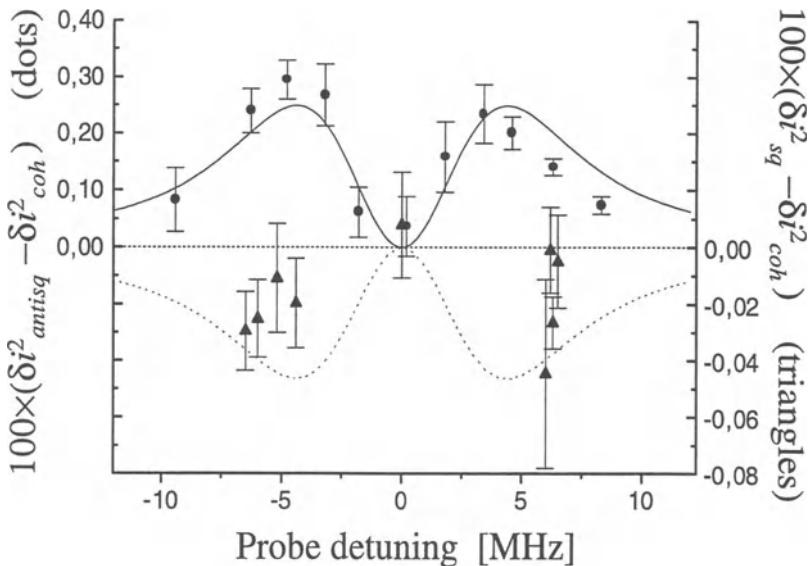


Figure 18.3 Experimental data.

fect squeezing and is the theoretical maximum efficiency in a 3-level system when spontaneous decay is taken into account, as discussed above. For a multi-level system, such as Cesium ground state, the upper limit on η is lower [20]. The data in Fig. 18.3 corresponds to (4.5 ± 0.6) dB of the excess noise in the antisqueezed quadrature of the pump giving $4X_{\pi/2}^2 \simeq 2.8$. This corresponds to the value of the mapping-readout efficiency $\eta = 0.09 \pm 0.02$. The imperfect efficiency is caused by many factors, including the admixture of the noise of other spin polarization components than F_z , the multilevel effects, imperfect polarizations, the residual magnetic field, imperfect overlap of the pump and the probe, reabsorption of uncorrelated spontaneously emitted photons at 852 nm, and the finite bandwidth of the squeezed light.

With the squeezed vacuum in-phase we measure $\delta i_{sq}^2(\Delta_{max})$. The average squeezing of the pump light available at the trap site is (-1.8 ± 0.2) dB corresponding to $4X_{\pi/2}^2 \simeq 0.65$. The expected quantum spin noise spectrum for such pump and the efficiency $\eta = 0.09$ is plotted as a dotted line in Fig. (18.3). The experimental data are plotted as triangles. All available experimental data obtained in 9 runs each lasting between 4 and 11 hours is shown. The long integration time is needed even with all the implemented lock-in detection stages because the quantum spin noise reduction corresponds to only $\simeq 2 \cdot 10^{-4}$ of the probe shot noise. Each point in the figure is the average of one run with 13 to 45 individual measurements. Each of these

individual measurements consists of 6 min. of averaging with the squeezed vacuum interacting with the atoms, and 6 min. of averaging with the squeezed vacuum blocked.

We define the degree of the observed spin squeezing (quantum spin noise reduction) by $\xi = (\delta i_{sq}^2 - \delta i_{coh}^2) / \delta i_{coh}^2$. The best experimental points in Fig.18.3 are in reasonable agreement with the expected degree of the quantum spin noise reduction which is -2.7% . A drift in the value of ξ on the time scale of hours within the range from 1% to -5% has been observed. We attribute the drift to slow uncontrolled changes in the trap geometry, leading to changes in local magnetic fields, density and polarizations. The best observed value around ± 6 MHz is $\xi = -(5 \pm 1)\%$ (4 hours average, 17 individual measurements). The average value for all the 183 individual measurements at ± 6 MHz is $\xi = -(1.4 \pm 0.4)\%$.

Summarizing, the free space complete absorption approach does provide mapping of a quantum state of light onto atomic state, albeit with relatively low efficiency.

4. OFF-RESONANT ATOM-LIGHT INTERACTION AS QUANTUM INTERFACE

Interaction of polarized light with spin-polarized atoms has been a subject of intensive investigations in atomic physics for several decades (for a review, see Ref. [23]). Polarization analysis of light transmitted through an atomic medium has been widely used for measurements of atomic orientation and alignment. Off-resonant atom-photon interaction as a probe of the spin orientation for atoms with total ground state electronic angular momentum equal $\hbar/2$ has been proposed in Ref. [24]. Recently it has been realized that the same interaction can reveal not just the mean value of the atomic spin, but its quantum state as well. As opposed to the classical case, in quantum world the back action of light on atoms cannot be ignored. This back action leads to entanglement of light and atoms, which in turn can be used to generate entanglement between separate atomic samples and other quantum information operations on atoms, as described below in this section.

The unitary time-evolution operator corresponding to the interaction with light propagating along the z -axis has the following form (the derivation is outlined in Appendix A):

$$\hat{U} = \exp(-ia\hat{S}_z\hat{F}_z), \quad (18.15)$$

where a is given by $a = \frac{\sigma}{A(I+\frac{1}{2})}\Delta\alpha_v$, σ is the resonant absorption cross-section for an unpolarized photon on an unpolarized atom of total spin F , A is the area of the transverse cross section of the light beam, γ is the spontaneous emission rate of the upper atomic level, Δ is the detuning. The dynamic vector

polarizability $\alpha_v = \pm 1$ for the D_1 transition of alkali atoms, while $\alpha_v = \mp \frac{1}{2}$ for the D_2 transition. Here the upper sign is for hyperfine sublevel with $F = I + \frac{1}{2}$, while the lower sign is for the $F = I - \frac{1}{2}$ hyperfine sublevel, I is the value of the nuclear spin. It is clear that the above Hamiltonian conserves the z-projection of the atomic spin and therefore can be used for a QND measurement of the spin as described below. This Hamiltonian can also serve as a resource for

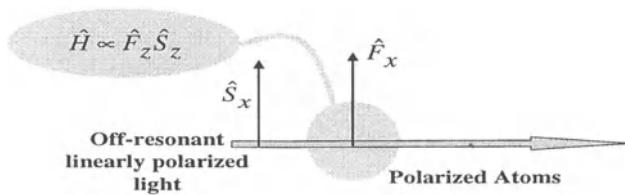


Figure 18.4 Outline of the atom-light QND interaction scheme.

a continuous XOR gate, one of the cornerstones for the quantum information processing with continuous variables. To show this, let us derive equations of motion for the field and atomic variables. Let the light pulse with the mean polarization along the x-axis propagate along the z-axis through the atomic sample also with the mean spin along the x-axis (Fig.18.4). In the Heisenberg picture transformations of the spin operators can be written as

$$\begin{pmatrix} \hat{F}_x \\ \hat{F}_y \\ \hat{F}_z \end{pmatrix}^{(out)} = \begin{pmatrix} \cos(a\hat{S}_z) & -\sin(a\hat{S}_z) & 0 \\ \sin(a\hat{S}_z) & \cos(a\hat{S}_z) & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \hat{F}_x \\ \hat{F}_y \\ \hat{F}_z \end{pmatrix}^{(in)}, \quad (18.16)$$

and a similar expression with $\hat{\mathbf{F}}$ and $\hat{\mathbf{S}}$ interchanged. In the limit of small rotations on the Bloch and Stokes spheres the relevant spin components can be written as follows:

$$\begin{aligned} \hat{S}_y^{(out)} &\approx \hat{S}_y^{(in)} + a\hat{F}_z^{(in)}\langle\hat{S}_x^{(in)}\rangle \approx \hat{S}_y^{(in)} + \frac{an}{2}\hat{F}_z^{(in)} \\ \hat{F}_y^{(out)} &\approx \hat{F}_y^{(in)} + (aN\hat{F})\hat{S}_z^{(in)}, \end{aligned} \quad (18.17)$$

whereas the z-components of the spin are constants of motion. Here the Stokes vector $\hat{\mathbf{S}}$ of the light pulse has the length $\langle\hat{\mathbf{S}}_{in}\rangle = \frac{n}{2}\mathbf{x}$, where n is the

number of photons in the pulse. As can be seen from the above equations, the interaction Hamiltonian (18.15) provides a continuous analog of XOR gate if $a\sqrt{FnN/2} = 1$ (F is the value of the spin of one atom). The rotations of individual qunats are achieved for light with the help of $\lambda/2$ and $\lambda/4$ plates and for atomic spins by applying dc magnetic fields.

Many algorithms of the field of discrete quantum information have their continuous analogs if every qubit is replaced with a qunat, every XOR-gate is replaced with a continuous XOR-gate, and every single qubit rotation is replaced with a corresponding rotation of the qunat in the quadrature plane [25]. Using collections of atomic spins and the field modes as qunats is a suitable architecture for implementation of continuous quantum information algorithms. Below we will show how using such philosophy one can, for example, achieve exact mapping of quantum states between light and atomic spins, in both directions. But first we will describe the experiment demonstrating the feasibility of the above Hamiltonian for continuous quantum information applications, namely for generation of spin squeezed states of atoms.

4.1 SPIN SQUEEZING VIA QND MEASUREMENTS

The interaction described by Eq.(18.15) is of the exact form required to perform QND measurements of a spin projection [26, 27]. Indeed, the essential feature of a QND measurement [28] is that an operator of a signal particle \hat{A} is coupled to an operator \hat{B} of a probe particle via an interaction Hamiltonian \hat{H}_i that commutes with \hat{A} . By making a (destructive) measurement on the operator \hat{C} conjugate to \hat{B} , one obtains information about \hat{A} without disturbing \hat{A} . Another important requirement is that the free evolution Hamiltonian of the signal particle commutes with \hat{A} , so that the QND observable \hat{A} is a constant of motion.

The idea of the atom-light spin-QND interaction is outlined in Fig.18.4. Interaction (18.15) leads to rotation of the polarization of the field that is proportional to \hat{F}_z , entangling atoms and photons in the process. Subsequent optical polarization measurements project atomic spins into a SSS, as first proposed in Ref. [26].

4.1.1 Theory. The Heisenberg picture operators transform according to the relations (18.16). Now let us suppose that $\hat{S}_y^{(out)}$ is measured. We assume that initially both $\hat{\mathbf{F}}$ and $\hat{\mathbf{S}}$ are in coherent spin states along the x-axis, with $\langle \hat{\mathbf{F}}^{(in)} \rangle = \frac{N}{2}\mathbf{x}$, $\langle \hat{\mathbf{S}}^{(in)} \rangle = \frac{n}{2}\mathbf{x}$, where N and n are the numbers of elementary 1/2-spins comprising angular momenta $\hat{\mathbf{F}}$ and $\hat{\mathbf{S}}$, respectively. We find that $\langle \hat{S}_y^{(out)} \rangle = \frac{1}{2}\langle \sin(a\hat{F}_z^{(in)}) \rangle n$, or, for $a\sqrt{\langle (\Delta\hat{F}_z^{(in)})^2 \rangle} = (a\sqrt{N})/2 \ll 1$, $\langle \hat{S}_y^{(out)} \rangle \simeq \frac{1}{2}a\langle \hat{F}_z^{(in)} \rangle n$. The last approximate equality suggests assigning to

\hat{F}_z the "QND shift" of $\hat{F}_z \approx \frac{2}{an} \hat{S}_y^{(out)}$. Subtracting this operator from $\hat{F}_z^{(out)}$ we obtain the modified expression:

$$\hat{F}'_z \equiv \hat{F}_z^{(out)} - \frac{2}{an} \hat{S}_y^{(out)}. \quad (18.18)$$

We find

$$\langle \hat{F}_x \rangle = \frac{N}{2} \cos^n \frac{a}{2},$$

$$\begin{aligned} \langle (\Delta \hat{F}'_z)^2 \rangle &= \frac{N}{4} + \frac{1}{2na^2} (n(1 - \cos^N a) + (1 + \cos^N a)) \\ &- \frac{N}{a} \sin \frac{a}{2} \cos^{N-1} \frac{a}{2}. \end{aligned} \quad (18.19)$$

For a and n such that $Na^2 \ll n^{-1/3}$ (we assume $N, n \gg 1$), we find $\langle \hat{F}_x \rangle = (N/2) \exp[-\xi/2]$, $\langle (\Delta \hat{F}'_z)^2 \rangle = 1/(4\xi)$. The squeezing parameter as defined by Eq.(18.7) is then found to be

$$\eta \simeq \frac{\exp[\xi/2]}{\sqrt{N\xi}}, \quad (18.20)$$

where $\xi = na^2/4$. The last expression for η is minimized when $\xi = 1$, and we obtain $\eta_{min} \simeq \sqrt{e}/\sqrt{N} \simeq 1.7/\sqrt{N}$, which shows that the scheme could prepare nearly maximally-entangled (Heisenberg-limited) spin states. In the spirit of the concept of QND measurement, the particular SSS is conditioned on the outcome of the $\hat{S}_y^{(out)}$ measurement. Subtraction of $\frac{2}{an} \hat{S}_y^{(out)}$ in (18.18) takes care of the random variation from trial to trial of the direction of $\langle \hat{\mathbf{F}} \rangle$.

4.1.2 Experiment. The experimental implementation of spin squeezing via QND measurement is reported in [6]. Let us consider a beam of atoms of density ρ , spin-polarized along the x-axis, moving with speed v through a light beam propagating along the z-axis. For simplicity we assume that the atomic beam and the light beam have square profiles of the same size d along the y-axis, while the atomic beam has width L along the z-axis. Further, let us assume that the atomic spins are subjected to a time-dependent sinusoidal magnetic field $\mathbf{e}_y B \cos(\Omega t)$. The z-component of $\hat{\mathbf{F}}(t)$ is given by $\hat{F}_z(t) = \cos(\phi(t)) \hat{F}_z^{(in)}(t) + \sin(\phi(t)) \hat{F}_x^{(in)}(t)$. Here $\hat{F}^{(in)}$ is the incident collective spin, $\phi(t) = \phi \sin(\Omega t)$ and we assume $\phi = (\mu B)/(\hbar\Omega) \ll 1$ so that $\hat{F}_z(t) \simeq \hat{F}_z^{(in)}(t) + \phi \sin(\Omega t) \hat{F}_x^{(in)}(t)$ (μ is the atomic magnetic moment). The QND-type atom-light interaction leads to polarization rotation of the probe light by an amount which is proportional to $\hat{F}_z(t)$. Let us introduce the following

observable,

$$\hat{S}_y(\Omega) \equiv \int_0^T dt \hat{s}_y(t) \sin(\Omega t), \quad (18.21)$$

which corresponds to the output of a spectrum analyzer that is being fed with the difference of photocurrents from the detectors D_1 and D_2 , $\hat{s}_y(t) \equiv \frac{1}{2}(\hat{a}_v^\dagger(t)\hat{a}_v(t) - \hat{a}_h^\dagger(t)\hat{a}_h(t))$. Here $T = 1/B$, where B is the resolution bandwidth of the spectrum analyzer. The accuracy of measurement of the amplitude of spin rotation ϕ can be determined from equation

$$\delta\phi = \frac{\sqrt{\langle(\Delta\hat{S}_y(\Omega))^2\rangle}}{|\frac{d}{d\phi}\langle\hat{S}_y(\Omega)\rangle|}. \quad (18.22)$$

We obtain

$$\langle\hat{S}_y(\Omega)\rangle = \frac{F^{(i)}}{4}\phi\chi N \frac{P}{\hbar\omega}\tau, \quad (18.23)$$

where $F^{(i)}$ is the total spin of one atom ($F^{(i)} = 4$ in our experiment), $\tau \equiv d/v$, $N = \rho dv TL$ is the total number of atoms passing through the interaction region during time T and P is the optical power of the probe beam. We obtain for the second moment

$$\langle(\Delta\hat{S}_y(\Omega))^2\rangle = \chi^2 F^{(i)} N \left(\frac{P}{2\hbar\omega}\right)^2 \left(\frac{\sin(\frac{1}{2}\Omega\tau)}{\Omega}\right)^2 + \frac{P}{8\hbar\omega B}, \quad (18.24)$$

where the first and second terms are due to (atomic) spin noise and photon shot noise, respectively. Now we can calculate the measurement accuracy of the spin rotation angle from Eq.(18.22) and we find

$$\delta\phi = \frac{\sqrt{2}}{\sqrt{2F^{(i)}N}} \sqrt{\left(\frac{\sin(\frac{1}{2}\Omega\tau)}{\Omega\tau}\right)^2 + \frac{4\hbar\omega}{(\chi\tau)^2NPB}}. \quad (18.25)$$

When $\frac{4\hbar\omega}{(\chi\tau)^2NPB} \ll 1$, the photon shot noise corresponding to the last term under the square root sign is much smaller than the atomic noise and can be neglected. In this case, for low frequencies $\Omega \ll 1/\tau$ we find that the measurement accuracy is given by the SQL, $\delta\phi_{SQL} = 1/\sqrt{F^{(i)}N}$. From Eq.(18.25) it follows that, as the frequency Ω of the applied spin rotation increases, the phase uncertainty $\delta\phi$ falls below the SQL. The limit on the achievable uncertainty is due to the photon shot noise. If the collective atom-photon coupling is high enough (through the use of either dense atomic samples

or optical cavities for the probing beam), the limit is determined by the back-action of the probe photons onto the collective atomic spin. The measurement accuracy of the spin rotation angle is then the Heisenberg limit $1/N$ [26].

An outline of the experimental setup is shown in Fig. 18.5. A paraffin-coated glass cell contains Cs atoms. Under the conditions of our experiment, the measured lifetime of spin polarization in the cell is on the order of 1 s, which means that the atoms undergo thousands of collisions with the walls without being depolarized.

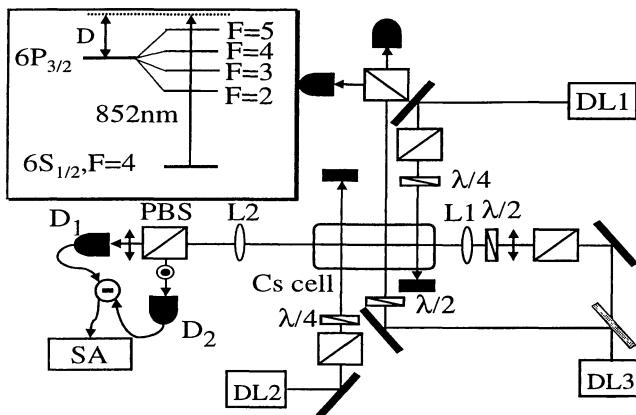


Figure 18.5 Outline of the experimental setup. Not shown are 3 pairs of coils to produce dc magnetic fields and a coil producing rf magnetic field. See text for details.

Initially it is important to prepare the atomic sample in a CSS. There are two important features of a CSS: (a) it is fully spin-polarized along some direction (and therefore has maximum coherence) and (b) spin fluctuations of the sample are at the shot-noise level given by $\sqrt{F/2}$, where F is the value of the collective spin.

In our experiment two 852 nm diode lasers DL1 and DL2 are used to spin-polarize the atomic medium. Both light beams are circularly polarized with the same helicity and propagate along the direction of the magnetic field of several Gauss. The laser DL1 of about 3 mW average power (adjusted with a neutral density filter) is tuned to the $6S_{1/2}, F = 3 \rightarrow 6P_{3/2}$ transition(s), while the laser DL2 of less than 100 μ W average power is tuned to the $6S_{1/2}, F = 4 \rightarrow 6P_{3/2}$ transition(s). A small portion of the linearly polarized light from DL3 is split off and used to monitor the degree of spin polarization. This probe beam propagates through the cell along the direction of spin polarization. By scanning the frequency across the Doppler profile, we measure the dispersive profile of the polarization rotation angle and the Lorentzian profile for absorption. The major

part of the light from laser DL3 is used as our QND-probe (see below). We align the magnetic field (and therefore also the spin polarization) orthogonally to the probe beam with the help of the Faraday rotation signal in the dc channels of our homodyne detectors on the QND-probe beam. The degree of spin-polarization of the atoms is found to be greater than 95%.

The QND probe beam is detuned about three Doppler widths from the center of the $6S_{1/2}, F = 4 \rightarrow 6P_{3/2}$ transition(s). A 1 mW light beam with Gaussian waist of 100 μm is focused into the gas cell. The optical pumping beams and the probe beam do not spatially overlap. The probe beam is then refocused by lens L2 onto a Glan-Thompson polarizing beam splitter (PBS) whose outputs are measured by two (85% quantum efficiency) photodiodes D_1 and D_2 . The outputs of the photodiodes are amplified, and the difference signal is fed into a spectrum analyzer SA , where noise spectra between 3 and 20 MHz are recorded.

An important aspect of the spin squeezing experiment is the need to identify the spin shot-noise level. By analogy with the use of thermal light for the photon shot noise normalization, we make use of the unpolarized atoms as benchmark for the spin shot noise. We have shown earlier in this Chapter, that the spin noise of unpolarized atoms in a cell scales linearly with the number of atoms, as expected for an uncorrelated sample of atoms. Because our Cs atoms have total spin $F = 4$ instead of elementary 1/2-spins, the spin noise of an unpolarized collection of atoms is $\frac{2}{3}(F + 1)$ times larger than the spin noise of the CSS with an equal number of atoms. As we argued above, the spin shot-noise can be measured at $\Omega = 0$. From the experimental point of view, however, the difficulty of measuring it in this way is connected with the fact that our probe laser has a large amount of excess amplitude and phase noise at frequencies below 1 MHz. Because of this, we prefer to normalize with respect to the shot noise, with the magnetic field applied in a direction perpendicular to the QND-probe propagation. In this case the spin noise manifests itself at the Larmor precession frequency ω_L , while the amount of the observed noise is reduced to half. We find the peak shot atomic noise to be about four times the photon shot noise.

To obtain the shot noise level for the CSS, we make use of the results of the spin noise measurement with unpolarized atoms. We take into account the factor of $2(F + 1)/3$ for the difference between the shot noises of an unpolarized sample of atoms and the CSS, and also of the fact that after optical pumping we have 16/9 times more atoms in the $F=4$ state than in the unpumped cell. That was also confirmed experimentally from absorption measurements. The spin noise level for the CSS obtained in this way is shown in Fig. 18.6 (broken line).

Next, we reduce the magnetic field back to 2 Gs and apply a rf magnetic field along the y -axis in order to produce a small rotation. Fig. 18.6 (solid

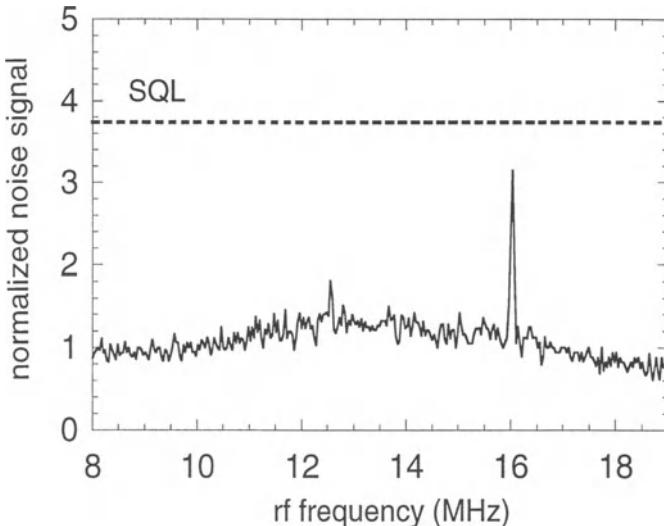


Figure 18.6 Measured spin noise spectrum. The dashed line indicates the SQL accuracy of spin rotation measurement. The peak at 16 MHz is due to spin rotation by the applied rf coils and is a demonstration of sub-shot noise atomic interferometry.

line) shows the spin noise spectrum observed under these conditions. The solid line is the SQL of the spin projection measurement for a CSS when the shot noise of the probe is taken into account. The peak at 16 MHz is the measured spin rotation due to the applied rf field. This demonstrates the sub-shot noise performance of the atomic spin interferometer.

4.2 QUANTUM MAPPING OF COLLECTIVE SPIN ON POLARIZED LIGHT

Mapping of light onto atoms and visa versa using complete absorption of light and interspecies teleportation is considered elsewhere in this Chapter. Let us show that both of these goals can be achieved by using the atom-light QND interaction of Eq.(18.15). The method is similar to the interspecies teleportation protocol, since it also requires an entangled (squeezed) input state of the system that is being mapped on. For concreteness, let us consider mapping the atomic spin $\hat{\mathbf{F}}$ onto the Stokes vector $\hat{\mathbf{S}}$ (although all of the derivation below equally describes the reverse situation of mapping light onto atoms simply by exchanging $\hat{\mathbf{S}}$ and $\hat{\mathbf{F}}$). Let the Stokes vector $\hat{\mathbf{S}}$ of the light pulse be initially in a SSS, $\langle \hat{\mathbf{S}}_{in} \rangle \approx \frac{n}{2}\mathbf{x}$, where n is the number of photons in the pulse, and the y-component of the spin is squeezed, $\langle (\Delta \hat{S}_y^{(in)})^2 \rangle \ll n/4$. We further assume $n = FN$ and $\frac{an}{2} = 1$. First, we direct the light pulse through the cell

along the z-axis. The Heisenberg picture transformations of the y-components of the spins are given by Eqs. (18.17), whereas the z-components of the spins are constants of motion. Next we exchange the z-and y-components:

$$\begin{aligned}\hat{S}_y^{(out-1)} &= \hat{S}_z^{(out)}, \\ \hat{S}_z^{(out-1)} &= \hat{S}_y^{(out)}.\end{aligned}\quad (18.26)$$

As the next step, we pass the pulse through the cell along the y-axis. As a result, we obtain

$$\hat{S}_z^{(out-2)} = \hat{S}_y^{(out)} = \hat{S}_y^{(in)} + \hat{F}_z^{(in)}, \quad (18.27)$$

$$\begin{aligned}\hat{S}_y^{(out-2)} &= \hat{S}_z^{(out)} - \hat{F}_y^{(out)} \\ &= \hat{S}_z^{(in)} - (\hat{F}_y^{(in)} + \hat{S}_z^{(in)}) = -\hat{F}_y^{(in)},\end{aligned}\quad (18.28)$$

Since the light is initially in a squeezed state, with $\langle(\Delta\hat{S}_y^{(in)})^2\rangle \ll n/4$, we can neglect the first term in the Eq.(18.27). Thus, we have achieved exact mapping of atomic spin state onto polarized light.

4.3 ENTANGLEMENT OF TWO DISTANT ATOMIC SAMPLES

Teleportation principle described elsewhere in this book requires an entanglement resource. More specifically, teleportation of atomic states or teleportation of a state of light onto a state of an atomic sample requires two entangled atomic samples as an initial resource.

4.3.1 Theory. Generation of the EPR-entangled atomic samples may be utilized by a QND-type interaction with off-resonant light. It appears that the off-resonant interaction described above is enough to produce an entangled state of two separate atomic objects with just a coherent pulse of light as initial resource. As shown in Ref. [12], when an off-resonant pulse classically polarized along x is transmitted along z axis through two atomic samples with opposite mean spins, $F_{x1} = -F_{x2}$, the light and atomic variables evolve as

$$\begin{aligned}\hat{S}_y^{(out)} &= \hat{S}_y^{(in)} + \frac{an}{2}(\hat{F}_{z1}^{(in)} + \hat{F}_{z2}^{(in)}), \hat{S}_z^{(out)} = \hat{S}_z^{(in)} \\ \hat{F}_{y1}^{(out)} &= \hat{F}_{y1}^{(in)} + \frac{aN}{2}\hat{S}_z^{(in)}, \hat{F}_{y2}^{(out)} = \hat{F}_{y2}^{(in)} - \frac{aN}{2}\hat{S}_z^{(in)} \\ \hat{F}_{z1,2}^{(out)} &= \hat{F}_{z1,2}^{(in)}\end{aligned}\quad (18.29)$$

The first line describes the Faraday effect (polarization rotation of the probe), whereas the second line shows the back action of light on atoms, i. e., spin

rotation due to the angular momentum of light. Therefore, the measurement of $\hat{S}_y^{(out)}$ reveals the value of $\hat{F}_{z1}^{(in)} + \hat{F}_{z2}^{(in)}$ (provided the constant $\frac{an}{2}$ is large enough, so that $\hat{S}_y^{(in)}$ is relatively small) without changing this value. It follows from the second and third lines that the total y projection for two samples stays unchanged due to the back action cancellation. This is where the choice of the opposite in direction and equal in size classical spin orientations for the two samples is crucial. It is also assumed that the $\hat{S}_z^{(in)}$ component of light is not changed in propagation between the two samples, i.e., losses of light are rather small. We refer to Ref. [12] for a detailed analysis of the role of losses. The procedure can be repeated with another pulse of light measuring now the sum of y components, $\hat{F}_{y1}^{(in)} + \hat{F}_{y2}^{(in)}$, again in a non-demolition way, while at the same time leaving the previously measured value of $\hat{F}_{z1}^{(in)} + \hat{F}_{z2}^{(in)}$ intact. As a result, the sum of the y components and the sum of the z components of spins of the two samples are known exactly in the ideal case, and therefore the two samples are entangled according to Eq.(18.11), since the uncertainties on the left-hand side become negligible. An important modification of the above protocol is the addition of a magnetic field oriented along the x direction, which allows to use a single entangling pulse to measure both y and z components at the same time. The Larmor precession of the y, z components with a common frequency Ω does not change their mutual orientation and size and therefore does not affect the entanglement. Moreover, in the lab frame the spin state is now encoded at the frequency Ω , and, as usual, it is easier to reduce to the quantum noise level an *ac* measurement than a *dc* one. Measurements on the light can be now conducted only around its spectral component $\hat{S}_y^{(out)}(\Omega)$. By choosing a suitable value of radio-frequency Ω we can reduce the probe noise to the minimal level of the vacuum (shot) noise. In the presence of the magnetic field along x the spin behavior is described by the following equations:

$$\frac{d}{dt}\hat{F}_z(t) = \Omega\hat{F}_y(t), \quad \frac{d}{dt}\hat{F}_y(t) = -\Omega\hat{F}_z(t) + \frac{aN}{2}\hat{S}_z(t)$$

The Stokes parameters of light evolve according to Eq.(18.29). Solving Eq.(18.29) we obtain:

$$\begin{aligned} \hat{S}_y^{(out)}(t) &= \hat{S}_y^{(in)}(t) + \frac{an}{2}\{(\hat{F}_{z1}^{(in)} + \hat{F}_{z2}^{(in)})\cos(\Omega t) \\ &\quad + (\hat{F}_{y1}^{(in)} + \hat{F}_{y2}^{(in)})\sin(\Omega t)\}. \end{aligned} \quad (18.30)$$

The spin components $\hat{F}_{z,y}^{(in)}$ are now defined in the frame rotating at the frequency Ω around the magnetic field axis, x . Measuring the $\cos(\Omega t)/\sin(\Omega t)$ component of the photocurrent we perform a projection measurement of the z/y component of the total spin for the two samples. This measurement entangles two atomic ensembles. The degree of entanglement depends on the ratio

of the second "atomic" term in Eq.(18.30) to the Fourier component of the first term, $\hat{S}_y^{(in)}(t) \cos(\Omega t)$ or $\hat{S}_y^{(in)}(t) \sin(\Omega t)$. The latter is just the component of the shot noise of the probe at the frequency Ω .

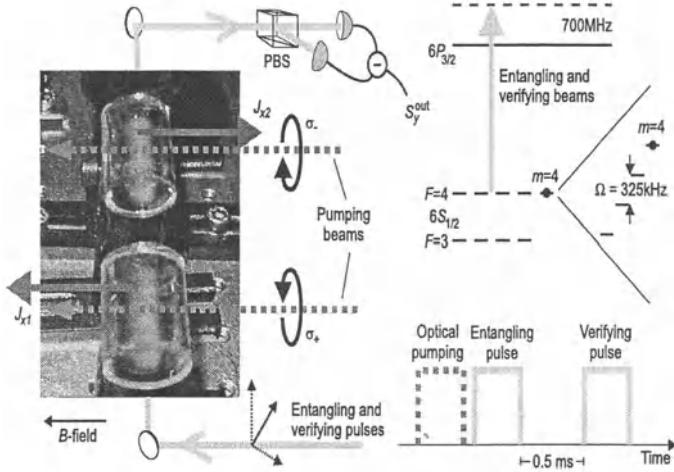


Figure 18.7 Outline of the experimental set-up.

4.3.2 Experiment. Experimental implementation of the entanglement of two atomic objects has been carried out with two gas samples each containing approximately 10^{12} Cesium atoms [10]. The schematic of the experimental set-up is shown in Fig.18.7. The two cells are coated from inside with paraffin coating which enhances the ground state coherence time up to $5 - 30m$ sec depending on the density of atoms. The first and the second sample are initially prepared in CSSs oriented along the magnetic field and against it, respectively. This is achieved by optical pumping into the $F = 4, m_F = 4$ and $F = 4, m_F = -4$, respectively for the two samples. The degree of orientation of around $97 - 98\%$ brings us very close to a perfect CSS. Then the optical pumping is switched off and a probe pulse with the duration of $0.5m$ sec is sent through both samples. Its Stokes operator is measured using a polarizing beam splitter and two balanced detectors. The differential photocurrent from the detectors is split in two and its $\cos(\Omega t)$ and $\sin(\Omega t)$ power spectral components $(S_y^{\text{out}}(\Omega))^2$ and $(S_y^{\text{out}}(\Omega))^2$ are measured with lock-in amplifiers. As follows from 18.30, the total spectral variance at frequency Ω contains two contributions: one from the shot noise of the probe light, another proportional to the atomic state variance:

$$\begin{aligned} \Delta^2 &= S^2 = (S_y^{\text{out}}(\Omega))^2 + (S_y^{\text{out}}(\Omega))^2 \\ &= \delta \hat{S}_y^2 + \kappa \left\{ (\hat{F}_{z1}^{(in)} + \hat{F}_{z2}^{(in)})^2 + (\hat{F}_{y1}^{(in)} + \hat{F}_{y2}^{(in)})^2 \right\}. \quad (18.31) \end{aligned}$$

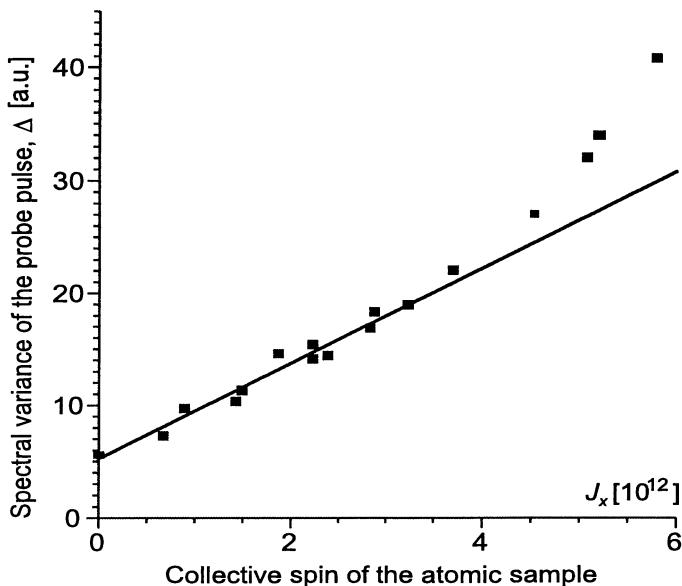


Figure 18.8 Measured spectral variance for coherent spin state.

To establish the level of the measured quantity S_{CSS}^2 corresponding to the CSS we have performed repeated measurements of Δ with freshly prepared atomic samples in CSS. The results as a function of the mean collective atomic spin F_x are shown in Fig.18.8. The value of Δ at $F_x = 0$ corresponds to the shot noise of the probe. The linear growth of Δ with F_x is the characteristic signature of the quantum (projection) spin noise. Classical fluctuations due to technical noise of lasers, etc, result in a quadratic dependence, which can be seen at higher values of F_x . The linear dependence together with nearly 100% orientation of the sample allows us to take the linear fit to the data in Fig.18.8 as the CSS level corresponding to the right-hand side of the entanglement condition (18.11). The coefficient $\kappa = \frac{1}{2}(\sigma\gamma n/4FA\Delta)^2 \approx 3$ is estimated [12] using $\sigma \approx \lambda^2/2\pi$ as the resonant dipole cross section, $\gamma = 5MHz$ - the full width of the optical transition, $A = 2cm^2$ - the probe beam cross section and $n \approx 10^{13}$ - the number of photons in the probe pulse with the power of $5mW$. With this estimate we obtain a resonable agreement with experimental results in Fig.18.8. The measurement sequence aimed at the generation and verification of the entanglement consists of the optical pumping pulses preparing samples in a CSS, the entangling pulse preparing the samples in the entangled state (pulse I) and the verifying pulse coming after the delay time and verifying the entanglement (pulse II), Fig.18.7. These pulses have the same duration and optical frequency as the probe pulse used for the CSS measurements. The pho-

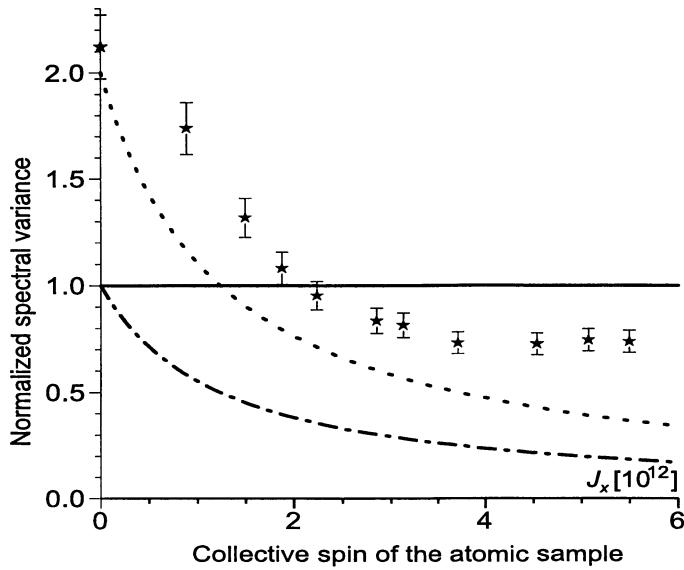


Figure 18.9 Normalized spectral variance showing entangled state of the two cells.

tocurrents from the two pulses are subtracted electronically and the variance of the difference, S_{EPR}^2 , is measured. The vanishing S_{EPR}^2 corresponds to two repeated measurements on the total spin state of the two samples producing the same results, i.e. to a perfect knowledge of both z and y total components for the two samples, and therefore to a perfectly entangled state. In the experiment the correlation between the entangling and verifying pulse measurements is imperfect for several reasons. First, the two optical pulses possess quantum(shot) noise which does not cancel out. Second, decoherence processes change the spin state between the two measurements. The first imperfection can be reduced by increasing the size of the atomic portion of S^2 compared to the shot noise of the probe. The results of measurements with the delay of $0.5m$ sec between preparation of the entangled state and its verification are shown in Fig.18.9. The results are normalized to the CSS limit (the linear fit in Fig.18.8). This limit thus corresponds to the unity level in Fig.18.9. The raw experimental data for the entangled state are shown as stars. The values below the unity level verify that the entangled state of the two atomic samples has been generated and maintained for $0.5m$ sec. For detailed derivation of the degree of entanglement from the data in Fig.18.9 we refer to Ref. [10]. The degree of entanglement calculated operationally from the data without additional assumptions is $(35 \pm 7)\%$. The degree of entanglement useful for teleportation calculated using an additional, experimentally proven assumption of the initially CSS for both samples is higher, $(52 \pm 7)\%$. The predicted fidelity

of teleportation with such entangled samples is $F = 55\%$, which is higher than the classical limit of 50%. Higher degrees of atomic entanglement should be possible with improved experimental conditions.

4.4 TELEPORTATION OF ATOMS ON LIGHT

Now we turn our attention to protocols of continuous quantum communication involving *both atoms and light*. Implementation of these protocols results in transfer of the quantum state of one macroscopic spin onto the other one. Shared entanglement of two *auxiliary* spins is necessary to achieve this goal. It turns out that the EPR-entangled spins described by Eqs.(18.10) are the right kind of states for this task.

The e.m. field continuous quantum teleportation of Refs.[25, 30] relies on the continuous entanglement of the EPR-type output of an optical parametric oscillator (OPO) below threshold. The EPR-type correlations of the output modes of the OPO and the EPR spin states are very closely related. In fact, the most practical way to generate EPR spin state of light in the lab is to mix each of the EPR modes (polarized, e.g., along the y-axis) with strong coherent fields polarized along the x-axis, on polarizing beamsplitters. Then, for the Stokes vectors of the output fields $\hat{\mathbf{S}}^{(1)}$ and $\hat{\mathbf{S}}^{(2)}$ we obtain:

$$\begin{aligned}\hat{S}_z^{(1)} &\approx \sqrt{n}\hat{X}_1, \hat{S}_y^{(1)} \approx \sqrt{n}\hat{Y}_1, \\ \hat{S}_z^{(2)} &\approx \sqrt{n}\hat{X}_2, \hat{S}_y^{(2)} \approx \sqrt{n}\hat{Y}_2,\end{aligned}\quad (18.32)$$

where n is the number of photons in each of the coherent fields (for simplicity assumed to be equal for both fields). That is, the spin components of the Stokes vectors of the output states of light are given by the corresponding quadrature operators of the OPO output. Since the latter obey relations of the form of Eqs.(18.10), we obtain relations Eqs.(18.10) for the z- and y -spin components of the output states of light.

As was pointed out in the original teleportation proposal [29], it is imperative to be able to perform *joint* measurements on the quantum state to be teleported and one of the EPR states. Off-resonant atom-photon interaction described by Eq.(18.15) allows us to achieve this goal. The interaction leads to rotation of the polarization of the field that is proportional to \hat{F}_z . Subsequent optical polarization measurements provide the classical information in our protocols.

Let Alice pass her bright EPR beam 1 with the Stokes vector $\hat{\mathbf{S}}^{(1)}$ through the cell containing polarized atomic vapor along the z-axis. The unitary time evolution operator of Eq.(18.15) in the case of small spin fluctuations in $\hat{\mathbf{F}}$ and

$\hat{S}_y (\sqrt{\langle (\Delta \hat{F}_{z,y})^2 \rangle} \ll F, \sqrt{\langle (\Delta \hat{S}_{z,y})^2 \rangle} \ll S)$ leads to Eqs.(18.17).

$$\begin{aligned}\hat{S}_y^{(1)(out)} &\approx \hat{S}_y^{(1)(in)} + \frac{an_1}{2} \hat{F}_z^{(in)}, \\ \hat{F}_y^{(out)} &\approx \hat{F}_y^{(in)} + (aN F) \hat{S}_z^{(1)(in)}.\end{aligned}\quad (18.33)$$

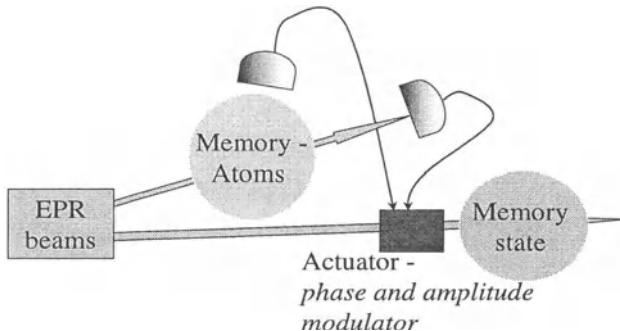


Figure 18.10 Outline of the scheme to teleport atomic quantum state on light.

These equations for interaction of the collective atomic spin with light resemble the beamsplitter relations used for teleportation of a mode of electromagnetic field in Refs.[25, 30]. An insightful analysis of why a linear device of a beamsplitter allows to perform joint measurements necessary for quantum teleportation has been given by Vaidman and Yoran [31].

The *nonlinear* atom-light interaction of Eq.(18.15) is analogous to the QND-type interaction for the optical quadratures $\sim \hat{X}_a \hat{X}_b$. Unlike the beamsplitter, which mixes both the \hat{X} and the \hat{Y} quadratures of the two input beams in the same fashion, interaction $\sim \hat{X}_a \hat{X}_b$ mixes only *one* pair of quadratures (\hat{Y}_a and \hat{Y}_b), leaving the other pair (\hat{X}_a and \hat{X}_b) unchanged. Relations (18.33) correspond to a 50:50 beamsplitter of the optical teleportation when

$$|a| \sqrt{FN n_1 / 2} = 1. \quad (18.34)$$

Subsequent (destructive) measurement of $\hat{S}_y^{(1)(out)}$ provides Alice with half of the classical information needed for implementation of "feed-forward" on Bob's bright EPR beam to complete the quantum teleportation. The other half must come from the measurement of $\hat{F}_y^{(out)}$. Although it is possible

in principle to use a completely destructive measurement (e.g., by means of photoionization), experimentally it may be more convenient to employ another QND measurement using an auxiliary coherent pulse. It will be convenient to rotate the spin by $\pi/2$ around the x-axis, so that propagating along the z-axis pulse will measure $\hat{F}_y^{(out)}$. The corresponding transformation is

$$\begin{aligned}\hat{S}_z^{(coh)(out)} &\approx \hat{S}_z^{(coh)(in)} + \frac{an_{coh}}{2} \hat{F}_y^{(out)} \\ &\approx \hat{S}_z^{(coh)(in)} + \frac{an_{coh}}{2} \hat{F}_y^{(in)} + \frac{n_{coh}}{n_1} \hat{S}_z^{(1)(in)}.\end{aligned}\quad (18.35)$$

The first term is negligible if $n_{coh}/n_1 \gg 1$. After Alice sends the results of measurements of $\hat{S}_y^{(1)(out)}$ and $\hat{S}_z^{(coh)(out)}$ to Bob, reconstruction of $\hat{F}^{(in)}$ in $\hat{\mathbf{S}}^{(2)}$ is achieved by Bob rotating the latter around the z-axis by the angle $\phi_1 = -\frac{2}{\sqrt{n_1 n_2}} S_y^{(1)(out)}$ and around the y-axis by the angle $\phi_2 = -\frac{2\sqrt{n_1}}{n_{coh}\sqrt{n_2}} S_z^{(coh)(out)}$. The rotations are equivalent to displacements because the angles are small. We obtain using Eqs.(18.10)

$$\begin{aligned}\hat{S}_y^{(2)(out)} &\approx \sqrt{\frac{n_2}{2FN}} \hat{F}_z^{(in)} + \sqrt{2} \exp(-r) \hat{S}_{yv}, \\ \hat{S}_z^{(2)(out)} &\approx \sqrt{\frac{n_2}{2FN}} \hat{F}_y^{(in)} + \sqrt{2} \exp(-r) \hat{S}_{zv}.\end{aligned}\quad (18.36)$$

The last terms in these expressions are due to the extra noise introduced by the imperfect EPR spin state. This noise goes to zero as r goes to infinity. The factor of square root of two in the last terms corresponds to the "quantum duty" of the quantum teleportation [25], as seen explicitly in the case of zero parametric gain, $r = 0$. Eqs.(18.36) show that the Stokes vector $\hat{\mathbf{S}}_2^{out}$ is identical to the initial collective spin vector of Alice's atoms when

$$\frac{n_2}{2FN} = 1. \quad (18.37)$$

The teleportation protocol described above may serve as a read-out for quantum memory with atoms as a memory cell. On the other hand, if the process of mapping of the Stokes vector $\hat{\mathbf{S}}_2^{out}$ onto another atomic spin [3] follows the described atom-to-light teleportation, atom-to-atom teleportation is achieved.

4.5 MAPPING OF AN UNKNOWN QUANTUM STATE OF LIGHT ON ATOMS (QUANTUM MEMORY)

Suppose Alice and Bob have in their disposal two atomic ensembles entangled as described in Section 3.3. Their mean polarizations are $\langle \hat{F}_{Ax} \rangle = \langle \hat{F}_{Bx} \rangle$ and the other two spin projections of the ensembles are entangled, so that

$\hat{F}_{Ay} - \hat{F}_{By} = 0$ and $\hat{F}_{Az} + \hat{F}_{Bz} = 0$. If Alice receives an unknown state of light with a polarization state described by the non-zero mean Stokes parameter \hat{S}_{Ux} and zero-mean $\hat{S}_{Uz}, \hat{S}_{Uy}$, she can via a sequence of classical measurements followed by a classical signal transmission map this state onto Bob's atomic "memory cell".

The protocol proceeds as follows. The unknown state of light is sent through Alice's ensemble along the z axis and the \hat{S}'_{Uy} of the transmitted light is measured by the detector D_{A1} producing the signal

$$\hat{d}_{A1} = \hat{S}_{Uy} + \hat{F}_{Az}$$

Alice's atomic state after this measurement becomes

$$\hat{F}'_{Az} = \hat{F}_{Az}, \hat{F}'_{Ay} = \hat{F}_{Ay} + \hat{S}_{Uz}$$

Next Alice's atomic state is rotated around the direction of the mean spin, x , so that $\hat{F}'_{Az} \rightarrow \hat{F}''_{Ay}$ and $\hat{F}'_{Ay} \rightarrow -\hat{F}''_{Az}$. A strong coherent beam with the mean polarization along x axis is then sent through Alice's ensemble along the z axis and its y Stokes parameter is measured by the detector D_{A2} with the result

$$\frac{n}{n_c} \hat{d}_{A2} = \frac{n}{n_c} \hat{S}_y^{coh} + \hat{F}''_{Az} \approx -\hat{F}'_{Ay} = \hat{F}_{Ay} + \hat{S}_{Uz}$$

In the above equations n, n_c are the mean photon numbers of the unknown state of light and the strong coherent beam respectively, and we assume $n/n_c \ll 1$.

The mapping of the unknown state of light onto Bob's ensemble is now completed by displacing the z, y component of his spin by $d_{A1}, -\frac{n}{n_c} d_{A2}$ to obtain

$$\begin{aligned}\hat{F}'_{Bz} &= \hat{F}_{Bz} + \hat{S}_{Uy} + \hat{F}_{Az} = \hat{S}_{Uy}, \\ \hat{F}'_{By} &= \hat{F}_{By} - \hat{S}_{Uz} - \hat{F}_{Ay} = -\hat{S}_{Uz},\end{aligned}$$

Thus, we have used entanglement between two macroscopic atomic spins to map a polarization quantum state of a light pulse onto atoms, with potential for long storing times.

4.6 COMMUNICATION VIA TELEPORTATION BETWEEN ATOMIC SAMPLES

We now describe a protocol which performs the direct teleportation of the quantum state of Alice's collective spin onto Bob's collection of atoms without using light as an intermediate carrier of the quantum state. Suppose we have

two macroscopic spin systems (Alice's and Bob's) in the initial states given by collective spin operators \hat{F}_A, \hat{F}_B with mean polarizations $\langle \hat{F}_{Ax} \rangle = \langle \hat{F}_{Bx} \rangle$ and with the other two projections $\hat{F}_{Ay}, \hat{F}_{By}, \hat{F}_{Az}, \hat{F}_{Bz}$. We also have at our disposal a source of the EPR spin states of light as described above. The Stokes' vector of the Alice's EPR beam is rotated by $\pi/2$ around the x -axis so that the Stokes operators are $\hat{S}_{Az} = -\hat{S}_{By}, \hat{S}_{Ay} = -\hat{S}_{Bz}$. The protocol begins with Alice sending her EPR beam along the z -axis and measuring its y -Stokes parameter with the detector D_{A1} , and Bob sending a coherent x -polarized pulse \hat{S}_B^{coh} containing n_c photons along the y -axis and measuring its z -Stokes parameter with the detector D_{B1} . The resulting atomic states of Alice and Bob are described by the following operators:

$$\begin{aligned}\hat{F}'_{Az} &= \hat{F}_{Az}, \hat{F}'_{Ay} = \hat{F}_{Ay} + \hat{S}_{Az}, \\ \hat{F}'_{By} &= \hat{F}_{By}, \hat{F}'_{Bz} = \hat{F}_{Bz} - \hat{S}_B^{coh}.\end{aligned}\quad (18.38)$$

In these equations we combined conditions $n_1 = n_2 = n$ and (18.34),(18.37) to obtain unity coupling coefficients between \hat{F} and \hat{S} projections. The Stokes parameters measured by detectors D_{A1} and D_{B1} are

$$\hat{D}_{A1} = \hat{S}_{Ay} + \hat{F}_{Az}, \quad (18.39)$$

$$\frac{n}{n_c} \hat{D}_{B1} = \frac{n}{n_c} \hat{S}_B^{coh} - \hat{F}_{By} \approx -\hat{F}_{By} \quad (18.40)$$

We assume $n/n_c \ll 1$. While the above measurements are performed, the second EPR beam sent by Alice to Bob begins its journey along the quantum channel. Next Alice sends a coherent x -polarized probe containing n_c photons along y axis onto the detector D_{A2} . The detector measures

$$\frac{n}{n_c} \hat{D}_{A2} = \frac{n}{n_c} \hat{S}_B^{coh} - \hat{F}'_{Ay} = \hat{F}'_{Ay} \quad (18.41)$$

Alice now sends $D_{A1}, \frac{n}{n_c} D_{A2}$ to Bob along a classical channel. When Bob receives the EPR beam from Alice he sends it along z axis onto the detector D_{B2} which reads

$$\hat{D}_{B2} = \hat{S}_{By} + \hat{F}'_{Bz} \quad (18.42)$$

After that the state of Bob's atoms is

$$\hat{F}''_{By} = \hat{F}'_{By} + \hat{S}_{Bz}, \hat{F}''_{Bz} = \hat{F}'_{Bz} \quad (18.43)$$

To complete the teleportation Bob now rotates his atomic state. We use displacements instead of rotations to simplify the expressions. Bob's state is

displaced along z by $-D_{A2} - D_{B2}$ and along y by $D_{A1} - D_{B1}$. The final state of his atoms, according to Eqs.(18.39,18.41,18.42,18.43), is described by

$$\begin{aligned}\hat{F}_{Bz}^{tele} &= \hat{F}_{Bz}'' - D_{A2} - D_{B2} = -\hat{F}_{Ay} \\ \hat{F}_{By}^{tele} &= \hat{F}_{By}'' + D_{A1} - D_{B1} = \hat{F}_{Az}\end{aligned}\quad (18.44)$$

and the teleportation of the unknown state of the Alice's collection of atomic spins onto Bob's atoms is proven (within a rotation of π around the x -axis). In the above equations we assumed perfect entanglement between the EPR beam components ($r \rightarrow \infty$ in Eqs.(18.10)). We have also used the fact that the measured values $F_{Bz,By}$ of operators $\hat{F}_{Bz,By}$ are obtained with the QND-type Hamiltonian, and therefore $\hat{F}_{Bz,By} - F_{Bz,By} = 0$ (same is true for \hat{S}_{By}^{coh}).

4.7 QUANTUM STATE SWAPPING BETWEEN TWO ATOMIC SYSTEMS

We now describe a protocol which exchanges initial quantum states of two collections of atomic spins. Suppose Alice's and Bob's spin samples are in the initial state given operators \hat{F}_A, \hat{F}_B with mean polarizations $\langle \hat{F}_{Ax} \rangle = \langle \hat{F}_{Bx} \rangle$. We again have at our disposal the EPR source of light as described above, with Stokes operators \hat{S}_z, \hat{S}_y for one of the beams, and $-\hat{S}_z, \hat{S}_y$ for the other. Both EPR beams are mixed with strong beams containing equal photon numbers, $n_1 = n_2 = n$, polarized along the x -axis in a way similar to the previous section. One of the EPR beams is used for a joint measurement on the z spin components of both samples by sending it through both of them along the z -axis. The resulting states of atomic samples are:

$$\begin{aligned}\hat{F}'_{Az} &= \hat{F}_{Az}; \hat{F}'_{Bz} = \hat{F}_{Bz}, \\ \hat{F}'_{Ay} &= \hat{F}_{Ay} + \hat{S}_z; \hat{F}'_{By} = \hat{F}_{By} + \hat{S}_z;\end{aligned}\quad (18.45)$$

and the state of the beam is

$$\hat{S}'_z = \hat{S}_z; \hat{S}'_y = \hat{S}_y + \hat{F}_{Az} + \hat{F}_{Bz} \quad (18.46)$$

In the above equations we assumed conditions (18.34),(18.37) to be fulfilled. Next, the second EPR beam shifted in phase by $\pi/2$ is sent along the y -axis of the two atomic samples to perform a joint measurement on the y spin components. The beam is transformed by the phase shift and the change of the direction in the following way $-\hat{S}_z, -\hat{S}_y \rightarrow \hat{S}'_z, \hat{S}'_y$. The evolution operator in this new coordinate system is $\hat{U} = \exp(-ia\hat{S}'_y \hat{F}_y)$. We obtain

$$\begin{aligned}\hat{F}_{Az}'' &= \hat{F}_{Az} - \hat{S}_y^y = \hat{F}_{Az} + \hat{S}_y; \hat{F}_{Bz}'' = \hat{F}_{Bz} + \hat{S}_y, \\ \hat{F}_{Ay}'' &= \hat{F}_{Ay}' = \hat{F}_{Ay} + \hat{S}_z; \hat{F}_{By}'' = \hat{F}_{By}' = \hat{F}_{By} + \hat{S}_z,\end{aligned}\quad (18.47)$$

and

$$\begin{aligned}\hat{S}_z^{r'} &= -\hat{S}_z' = -\hat{S}_z + \hat{F}_{Ay}' + \hat{F}_{By}' = \hat{F}_{Ay} + \hat{F}_{By} + \hat{S}_z \\ \hat{S}_y^{r'} &= -\hat{S}_y' = -\hat{S}_y\end{aligned}\quad (18.48)$$

Here we used Eqs. (18.45, 18.46). After interacting with the atoms the two EPR beams are detected by photodetectors D_1, D_2 . The Stokes parameter S_y' (18.46) is measured for the first beam and the Stokes parameter $S_z^{r'}$ (18.48) for the second. The results of the measurements are used to rotate the atomic spins in order to achieve the teleportation. The projections \hat{F}_{Az}'' and \hat{F}_{Bz}'' are displaced by the value S_y' obtained from D_1 , and the projections \hat{F}_{Ay}'' and \hat{F}_{By}'' are displaced by the value $S_z^{r'}$. The results are

$$\begin{aligned}\hat{F}_{Az}^{tele} &= \hat{F}_z'' - S_y' = -\hat{F}_{Bz}, \\ \hat{F}_{Ay}^{tele} &= \hat{F}_y'' - S_z^{r'} = -\hat{F}_{By}.\end{aligned}\quad (18.49)$$

Similarly for the other atomic system

$$\begin{aligned}\hat{F}_{Bz}^{swap} &= -\hat{F}_{Az} \\ \hat{F}_{By}^{swap} &= -\hat{F}_{Ay}\end{aligned}\quad (18.50)$$

Eqs.(18.49),(18.50) prove that the initial collective quantum states of the two samples have been exchanged.

A different method for atomic continuous variable teleportation, using coherent light and entangled atomic samples, was proposed in Ref. [12].

5. SUMMARY

One of the most striking features of quantum information processing with continuous variables is the relative simplicity of realization of the light-atoms quantum interface. As opposed to the case of discrete variables (single photons and atoms) such interface for continuous variables does not require strong coupling via cavity QED. Free space interaction of light with atomic ensembles provides enough coupling for quantum state exchange and entanglement of continuous variables. We have presented two approaches to continuous quantum information processing, one based on resonant interaction, the other

one relying on off-resonant atom-light interaction. Experiments within both approaches, performed in the last three years, resulted in several advances in the field of quantum information with continuous variables: mapping of non-classical (squeezed) states of light onto collective atomic spin [5], preparation of squeezed spin states of atoms via quantum non-demolition measurements [6], demonstration of Einstein-Podolsky-Rosen entanglement of two distant atomic samples [10], and, more recently, demonstration of long-lived quantum memory effect for non-classical states of light [32].

One can envision extending this work to more complex algorithms of continuous quantum information, such as, e.g. quantum search and quantum error correction for continuous variables [25, 33] and quantum communication between distant atomic samples [11, 12, 34]. Another promising direction of research is to implement real-time feedback on continuous atomic variables, aimed, e.g., at continuous error correction in the system. Such continuous (weak) quantum feedback can be often advantageous compared to instantaneous (strong) measurements [35].

Acknowledgments

We are indebted to many of our collaborators who contributed to the work reviewed in this chapter, particularly to L. Mandel, N. P. Bigelow, I. Cirac, L.-M. Duan, B. Julsgaard, J. Hald, A. Kozhekin, K. Mølmer, J.L. Sørensen, and P. Zoller.

Appendix: A

Let us assume that we have a running-wave cavity with a single spatial mode of the electromagnetic field interacting with a collection of N atoms. First, we consider an idealized case of alkali-like atoms with zero nuclear spin. The interaction Hamiltonian describing the atoms-field systems can be written as

$$\hat{H}_I = \hbar \sum_{i=1}^2 \sum_{\mu=1}^N g \exp(i \frac{\omega_{ii+1}}{c} z^\mu) \hat{a}_i \hat{\sigma}_{ii+1}^\mu + h.c., \quad (18.A.1)$$

where \hat{a}_+ , \hat{a}_- are annihilation operators for the right- and left-hand polarized components of the field. g is the coupling constant, z^μ is the position of the μ -th atom in the sample. For large detuning $\Delta \gg \gamma$ the dynamics of the system can be described by the *effective* interaction Hamiltonian (see, e.g. [36])

$$\hat{H}_{eff} = \hbar \sum_{i=1}^2 \frac{g^2}{\frac{1}{2}i\gamma + D} \hat{a}_i^+ \hat{a}_i \hat{J}_{ii} = \hbar\Omega(\hat{S}_z \hat{J}_z + \frac{1}{4}\hat{n}\hat{N}). \quad (18.A.2)$$

The second term is spin independent and can be omitted. \hat{H}_{eff} as it is written above is not Hermitian. In order to make the Hamiltonian to be Hermitian, one

must add terms that describe interaction with the external system responsible for relaxation (in our case, the bath of spontaneous emission modes of the atoms serves as such external system). However, for our purposes, we can neglect this issue and simply take the Hermitian part of the Hamiltonian (18.A.2). From the experimental point of view, a very interesting situation is of free-space atom light coupling. One can show [26, 12] that the effective Hamiltonian still has the form of Eq. (18.A.2). The anti-Hermitian part of the Hamiltonian (18.A.2), allows us to write down the expression for the coupling constant g through directly measurable quantities: photon-atom atomic cross-section σ and the transverse cross-sectional area of the light beam A . The on-resonance absorption length l_a is given by $(\sigma N/AL)^{-1}$. Using the equations of motion for the electric field that Hamiltonian (18.A.2) results in, we obtain the following expression for l_a :

$$l_a = \frac{c\gamma}{2g^2N}$$

Comparing the two expressions, we find $g^2 = (\sigma c\gamma)/(2LA)$. If instead of the D_1 transition we consider the D_2 one, we would find a similar result, with an extra factor of $\frac{1}{2}$ present in the expression for the Hamiltonian. The unitary evolution \hat{U} operator is obtained by exponentiating the Hermitian part of the Hamiltonian: $\hat{U} = \exp(-i\hat{H}_h L/c)$.

The isotopes of interest of the alkali atoms have non-zero nuclear spin. In this case we need to express the “average” value of the z-component of the electronic angular momentum through the total angular momentum of the atom. The following relation can be obtained [37]:

$$\hat{J}_z^{avg} = \hat{F}_z \frac{F(F+1) + 3/4 - I(I+1)}{2F(F+1)} = \pm \hat{F}_z \frac{1}{(I+1/2)}$$

Combining the formulas, we arrive at the Eq.(18.15) for the unitary evolution operator. It is interesting to note that a more rigorous derivation for atoms possessing nuclear spin [38] gives the same result as the intuitive procedure of averaging electronic spin.

References

- [1] A. S. Parkins and H. J. Kimble, *J. Opt. B* **1**, 496 (1999); S. Bose, P. L. Knight, M. B. Plenio, and V. Vedral, *Phys. Rev. Lett.* **83**, 5158 (1999).
- [2] A. Kuzmich, K. Mølmer, and E. S. Polzik, *Phys. Rev. Lett.* **79**, 4782 (1997).
- [3] A. E. Kozhekin, K. Mølmer, E. S. Polzik, *Phys. Rev. A* **62**, 033809 (2000).
- [4] E. S. Polzik, *Phys. Rev. A* **59**, 4202 (1999).
- [5] J. Hald, J. L. Sørensen, C. Schori, and E. S. Polzik, *Phys. Rev. Lett.* **83**, 1319 (1999).

- [6] A. Kuzmich, L. Mandel, and N. P. Bigelow, Phys. Rev. Lett. **85**, 1594 (2000).
- [7] Z. Y. Ou, S. F. Pereira, J. H. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992).
- [8] Ch. Silberhorn, P. K. Lam, O. Weiss, F. Konig, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **86**, 4267 (2001).
- [9] C. Schori, J. L. Sørensen, E. S. Polzik, quant-ph/0205015.
- [10] B. Julsgaard, A. Kozhekin, and E. S. Polzik, Nature **413**, 400 (2001).
- [11] A. Kuzmich and E. S. Polzik, Phys. Rev. Lett. **85**, 5639 (2000).
- [12] Lu-Ming Duan, J.I. Cirac, P. Zoller, and E. S. Polzik, Phys. Rev. Lett. **85**, 5643 (2000).
- [13] F. T. Arecchi, E. Courtens, R. Gilmore, and H. Thomas, Phys. Rev. A **6**, 2211 (1972).
- [14] I. Cirac, unpublished.
- [15] M. Kitagawa and M. Ueda, Phys. Rev. Lett. **67**, 1852 (1991); Phys. Rev. A **47**, 5138 (1993).
- [16] D. J. Wineland, J. J. Bollinger, W. M. Itano, and F. L. Moore, Phys. Rev. A **46**, R6797 (1992);
- [17] D. J. Wineland, J. J. Bollinger, W. M. Itano, and D. J. Heinzen, Phys. Rev. A **50**, 67 (1994).
- [18] G. S. Agarwal and R. R. Puri, Phys. Rev. A, **41**, 3782
- [19] L.-M. Duan, G. Giedke, J. I. Cirac, P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
- [20] J. Hald and E. S. Polzik. Special Issue: Quantum Coherence and Entanglement. Journal of Optics B: Quantum and Semiclassical Optics, **3**, S83 (2001).
- [21] F. Laloe, M. Leduc, and P. Miguzzi, J. Phys. **30**, 277 (1969).
- [22] J. L. Sørensen, J. Hald, and E. S. Polzik, Phys. Rev. Lett. **80**, 3487 (1998).
- [23] W. Happer, Rev. Mod. Phys. **44**, 169 (1972).
- [24] W. Happer and B. S. Mathur, Phys. Rev. Lett. **18**, 577 (1967).
- [25] S. L. Braunstein, Nature, **394**, 47 (1998); S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
- [26] A. Kuzmich, N. P. Bigelow, and L. Mandel, Europhys. Lett. A **42**, 481 (1998).
- [27] K. Mølmer, Eur. Phys. J. D **5**, 301 (1999); Y. Takahashi, K. Honda, N. Tanaka, K. Toyoda, K. Ishikawa, and T. Yabuzaki, Phys. Rev. A **60**, 4974 (1999).

- [28] J. -Ph. Poizat, J. -F. Roch, and P. Grangier, Ann. Phys. Fr. **19**, 265 (1994).
- [29] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [30] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).
- [31] L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999).
- [32] C. Schori, B. Julsgaard, J. L. Sørensen, and E. S. Polzik, quant-ph/0203023.
- [33] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
- [34] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000).
- [35] C. Ahn, A. C. Doherty, and A. J. Landahl, quant-ph/0110111.
- [36] M. Brune, S. Haroche, J. M. Raimond, L. Davidovich, and N. Zagury, Phys. Rev. A **45**, 5193 (1992).
- [37] L. D. Landau and E. M. Lifshitz, *Quantum mechanics: non-relativistic theory* (Pergamon Press, New York, 1991).
- [38] W. Happer and B. S. Mathur, Phys. Rev. **163**, 12 (1965).

IV

LIMITS ON QUANTUM INFORMATION AND CRYPTOGRAPHY

Chapter 19

LIMITATIONS ON DISCRETE QUANTUM INFORMATION AND CRYPTOGRAPHY

Samuel L. Braunstein

Informatics, Bangor University, Bangor LL57 1UT, United Kingdom

schmuel@sees.bangor.ac.uk

Arun K. Pati

Institute of Physics, Bhubaneswar-751005, Orissa, INDIA

Theoretical Physics Division, BARC, Mumbai, INDIA

akpati@iopb.res.in

Abstract In this chapter we briefly discuss some of the limitations to processing discrete quantum information, such as no-cloning, no-complementing and no-deleting. The no-cloning principle, in particular, has important practical implications; for example, quantum cryptography uses it to guarantee security against eavesdroppers.

1. INTRODUCTION

Quantum information differs from classical information in a variety of ways. Knowing these differences is crucial to understanding the ultimate limits to our ability to store, process and extract useful information from quantum states. These are some of the primary tasks for any protocol in information theory. Among the key differences between classical and quantum information are no-cloning [1, 2], no-complementing [3] and no-deleting [4]. These limitations may appear as hurdles, but with the right insight they can be turned into practical applications. For example, the no-cloning principle lies at the heart of quantum cryptography.

Firstly, one must appreciate the fact that (or the lack of) *knowledge* about a quantum state plays an important role. Suppose we are given an arbitrary qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (19.1)$$

where α and β are complex numbers. Because one can ignore the overall phase factor we may always choose α to be real. Thus, an arbitrary qubit may be represented by a point on a two-dimensional sphere with the two real parameters θ and ϕ , where $\alpha = \cos(\theta/2)$ and $\beta = \sin(\theta/2)\exp(i\phi)$ with $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$.

If a qubit is prepared by a third party, then it may be completely *unknown* to us. Our lack of knowledge about the preparation procedure translates into our inability to pinpoint the state on this sphere. In principle, to precisely determine such a completely unknown state might require a vast amount of information corresponding to the many bits needed to specify the two parameters θ and ϕ [5]. If we had prepared the qubit ourselves then we would have known its location and hence we would not have lacked any information. In studying the fundamental limitations to processing quantum information this preparation knowledge is important.

More generally, a state may be prepared from a limited alphabet of possible choices. In particular, the state ρ is assumed to be selected from one of a set of states $\{\rho_i\}$ each of which occur with respective (and known) probabilities p_i . If the alphabet (consisting of the set $\{\rho_i\}$) and the associated probabilities p_i is known, then only the specific choice from this set remains unknown. For example, for continuous variables, we often consider a restricted alphabet of the set of coherent states for representing information.

2. THE NO-CLONING PRINCIPLE

In principle classical information can be copied perfectly. But what about information stored in quantum states, such as in the polarization of a photon or the spin of an electron? This interesting question was raised by Wootters, Zuerk [1] and Dieks [2]. They discovered that the linearity of quantum theory forbids the perfect copying of an unknown quantum state.

Suppose, we are asked to copy an *unknown* qubit. A cloning machine would start with the original state, a second standard state which will be transformed into the copy and possibly an ancilla state. Thus, the cloning machine will be described by an operator \mathcal{U}_C which maps $\mathcal{U}_C : \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \rightarrow \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$, with the three Hilbert spaces referring to original, copy and ancilla respectively. For a given original state its action will be

$$|\psi\rangle_1 |\Sigma\rangle_2 |A\rangle_3 \rightarrow |\psi\rangle_1 |\psi\rangle_2 |A_\psi\rangle_3, \quad (19.2)$$

where $|\Sigma\rangle$ is the standard (target) state, and $|A\rangle$ is the initial and $|A_\psi\rangle$ is the final state of the ancilla.

How would this machine act on orthogonal inputs $|0\rangle$ and $|1\rangle$? We would expect them to transformation according to

$$\begin{aligned} |0\rangle_1|\Sigma\rangle_2|A\rangle_3 &\rightarrow |0\rangle_1|0\rangle_2|A_0\rangle_3 \\ |1\rangle_1|\Sigma\rangle_2|A\rangle_3 &\rightarrow |1\rangle_1|1\rangle_2|A_1\rangle_3 . \end{aligned} \quad (19.3)$$

However, these transformations are enough to specify the actions of our cloner machine on an arbitrary qubit $|\psi\rangle$ as input. In particular, by the linearity of quantum theory we have

$$\begin{aligned} |\psi\rangle_1|\Sigma\rangle_2|A\rangle_3 &\rightarrow \alpha|0\rangle_1|0\rangle_2|A_0\rangle_3 + \beta|1\rangle_1|1\rangle_2|A_1\rangle_3 \\ &\neq [\alpha^2|0\rangle_1|0\rangle_2 + \beta^2|1\rangle_1|1\rangle_2 \\ &\quad + \alpha\beta(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)]|A_\psi\rangle_3 \\ &= |\psi\rangle_1|\psi\rangle_2|A_\psi\rangle_3 . \end{aligned} \quad (19.4)$$

Thus, the cloning machine must fail for completely unknown states. If we knew the state we could rotate it back to $|0\rangle$ or $|1\rangle$ and perform the cloning operation.

For a restricted alphabet of quantum states such as two non-orthogonal states from a set $\mathcal{S} = \{\psi_k\}$, $k = 1, 2, \dots, K$, the proof of no-cloning theorem follows just from unitarity of the evolution. Thus the deterministic cloning of non-orthogonal states is impossible [8, 9, 10]. However, one can give up either exactness of the clone or determinism of the process in the cloning operation. It may be shown that approximate cloning is possible using a unitary operation or that exact cloning is possible with a unitary operation plus a suitable measurement outcome.

The possibility of producing approximate copies of a quantum state has been considered by Buzek and Hillery [11]. Here, one demands that all inputs should be copied equally well (so the performance should have a *universal* character) and that the fidelity of cloning should be maximal. For example, the simplest universal cloner of a qubit making $1 \rightarrow 2$ copies can attain an optimal [12] fidelity $F = 5/6$. An explicit circuit for achieving this universal cloning has been determined [13]. More generally, universal cloning has been considered for $1 \rightarrow M$ copies [14, 15]. The fidelity goes as $F_{1 \rightarrow M} = (2M+1)/(3M)$ and has been shown to be consistent with a no-superluminal-signaling condition [16, 17]. Further, the fidelity of universal cloner for qudits (d -dimensional generalizations of qubits) for $N \rightarrow M$ copies goes as $F_{N \rightarrow M}(d) = [N(d-1) + M(N+1)]/[M(N+d)]$. Notice that when $d \rightarrow \infty$ then $F_{N \rightarrow M}(\infty) = N/M$. This was also obtained in Ref. [18] while discussing quantum information distribution and continuous variable quantum cloning.

In addition, it is possible to design probabilistic cloning machines [19]. A state selected from a set of non-orthogonal, linearly-independent states $\mathcal{S} = \{\psi_k\}$, $k = 1, 2, \dots, K$, can be exactly cloned with a finite probability of

success. For any two non-orthogonal pairs (i, j) the success probability is $\frac{1}{2}(p_i + p_j) \leq 1/(1 + |\langle \psi_i | \psi_j \rangle|)$. Further, it was shown that linearly independent quantum states can evolve into a linear superposition of multiple copies with a branch for failure [20]. Probabilistic and deterministic cloning transformations were shown to be special cases of this operation. A cloning machine that interpolates between approximate and exact clones has also been proposed [21].

The impossibility of cloning has been used to argue the impossibility of completely determining the wavefunction of a single unknown quantum system [9]. However, we might ask to what extent can one determine the state given a finite number of copies. This is related to optimal state estimation. For the case of qubits the best fidelity for recreating a state based on measurement results from N copies [6] is $F = (N + 1)/(N + 2)$. For a d -dimensional qudits this optimal fidelity of state estimation [7] is $F = (N + 1)/(N + d)$. Thus, given a single qubit we can extract out only $\frac{2}{3}$'s worth of the fidelity. One can see that if we are given an infinite number of copies will the state estimation fidelity approaches unity.

Finally, one may ask whether it is possible to clone a quantum state by supplementing extra information (either quantum or classical)? Classically we can always determine the state, so no further information is necessary. Surprisingly, however, for cloning a quantum system the supplementary information must be sufficient to manufacture the clone! This provides us with a stronger version of the no-cloning theorem [22].

3. NO-COMPLEMENTING PRINCIPLE

We know that a classical bit 0 can be complemented to 1 or vice-versa. In the quantum world, if a qubit is in a computational state $|0\rangle$ or $|1\rangle$ it can also be complemented, for example, by applying the Pauli operator σ_x . However, is it possible to complement an arbitrary qubit? If we could complement a qubit by a physical operation, then we would take $|\psi\rangle$ to $|\bar{\psi}\rangle$, where $\langle \psi | \bar{\psi} \rangle = 0$. So the complementing operation should be defined by

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha^*|1\rangle - \beta^*|0\rangle . \quad (19.5)$$

Note that this is an *antiunitary operation*. An anti-unitary operation though a positive map is not a completely positive (CP) map. This means that it cannot be implemented by any physical operation. This shows that it is impossible to complement an unknown qubit [3]. Nevertheless, it is possible to design an approximate and universal NOT (or complementing) gate. The fidelity of producing the complemented qubit is exactly equal to the state estimation fidelity of a single qubit, i.e., $\frac{2}{3}$.

4. NO-DELETION PRINCIPLE

Classically we may delete one copy against others, uncopying it in a perfectly reversible manner. However, in the quantum world this is not the case. This limitation complements no-cloning principle which says that given two (or more) copies of an unknown quantum state one cannot delete a copy acting jointly on both the copies [4].

If we could have a quantum deleting machine it would act on two initially identical qubits in some unknown state $|\psi\rangle$ and an ancilla in some initial state $|A\rangle$. This machine is supposed to delete one of the copies and replace it with some standard qubit $|\Sigma\rangle$. The quantum deleting therefore would yield

$$|\psi\rangle|\psi\rangle|A\rangle \rightarrow |\psi\rangle|\Sigma\rangle|A_\psi\rangle, \quad (19.6)$$

where $|A_\psi\rangle$ is the final state of the ancilla. The only solution to this equation is to swap the second and third qubits. However, this obviously should be excluded for any sensible definition of a deleting machine, since the information has only been moved to another location.

Similar to the no-cloning theorem, deletion of a copy from two non-orthogonal states is impossible [22]. Recently, it has been shown that probabilistic deletion of copies of linearly independent quantum states is allowed [23, 24, 25]. However, it remains an open question how to design a universal and approximate quantum deleting machine.

Next we discuss how these limitations can be turned around into positive applications such as cryptography.

5. CRYPTOGRAPHY

Cryptography is the art of secretly sending messages from sender to receiver. Usually the sender and receiver establish a key and using it they can encrypt and decrypt a message. The security of a cryptic message thus depends on how well the secrecy of the decryption key is maintained.

The first provably secure encryption scheme was invented by Vernam in 1917 and is often called the one-time pad. Here a secret key of random numbers is added (using modulo arithmetic) to a simple numerical representation of the message. For each number from the message a new number from the key must be used. It can be shown that in the absence of knowledge of the key, the encoded message carries no information about the original. A subtle point in this result is that the key must not be reused, hence the name one-time pad. Because of this the main problem with this encoding scheme is the requirement for distributing a copy of the (long) key to the receiver without its falling into hostile hands.

It should be noted that one way around the key-distribution problem has been “solved” by public key cryptosystems. The most well-known is the RSA

scheme invented by Rivest, Shamir and Adelman [26]. Here the encoding key is placed in the public domain, whereas the decoding key is kept secret. Security relies on the computational difficulty of extracting the decoding key from knowledge of the encoding key alone. It is generally accepted that any procedure for determining the former relies on factoring the large numbers appearing in the latter. Because factoring is apparently computationally intractable, the RSA scheme is believed to provide suitable security. Of course, all this would change if scalable quantum computers capable of running Shor's algorithm became available.

Public key cryptography solves the key distribution problem at the expense of absolute security. To guarantee absolute security we must go back to the Vernam cipher and find a way of guaranteeing the security of distribution of the key. Here is where quantum mechanics comes in. Quantum cryptography is really a method of creating pairs of correlated keys between sender and receiver, without the need for transporting these keys through the intervening space. Quantum cryptography is sometimes more precisely called quantum key distribution.

In quantum key distribution, the key is created through a protocol based on the transfer of quantum states between sender and receiver (Alice and Bob, respectively). Suppose an eavesdropper (Eve), who wishes to circumvent the security of this protocol, couples an ancilla to the states transmitted between Alice and Bob and evolves as

$$\begin{aligned} |\psi_1\rangle_1|A\rangle_2 &\rightarrow |\psi_1\rangle_1|A_1\rangle_2 \\ |\psi_2\rangle_1|A\rangle_2 &\rightarrow |\psi_2\rangle_1|A_2\rangle_2 . \end{aligned} \quad (19.7)$$

Her intention is to extract information about the states sent by measuring the final state of the ancilla and distinguishing the outcomes. However, unitarity of this coupling implies $\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle\langle A_1|A_2\rangle$. Thus, if the protocol utilizes non-orthogonal states then the final states of the ancilla become identical. As a consequence if Eve is to extract information, she can only do so by disturbing the state transmitted. In essence, this is really nothing more than the no-cloning principle at work.

For qubit-based quantum cryptography there have been two basic schemes. Those involving the sending of states from non-orthogonal bases, such as the original protocol Bennett and Brassard invented in 1984 (called BB84) [27], and those relying on sharing entanglement between sender and receiver, such as Ekert's scheme [28]. We shall not discuss the potential advantages of either scheme here. Below we give a brief discussion to the BB84 protocol.

First Alice generates a random sequence of 0's and 1's. Then she randomly chooses between two different bases to encode the information. In one basis, she encodes 0 as $|0\rangle$ and 1 as $|1\rangle$. In the second basis, she encodes 0 as $\frac{1}{\sqrt{2}}(|0\rangle +$

$|1\rangle$) and 1 as $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. (Note that these two bases are incompatible.) At the receiving end, Bob randomly chooses between these bases to make his measurements. Only when Alice and Bob happen to be using compatible bases will their bits be correlated. Next, Alice and Bob communicate over a public channel. They reveal their choice of bases for each round, thus discovering during which rounds their results should agree. Of these they make a small selection to “sacrifice” in order to check the fidelity of this correlation. Any deviation from the ideal is a signal of potential information gained by Eve. When they are happy that Eve has been excluded, they may use the remaining (unrevealed) bits from their compatible choice of bases. Thus, this protocol has managed to create, in separated locations, pairs of random numbers — the key.

There has been tremendous developments in the area of quantum cryptography. For example, to exclude Eve, one may use privacy amplification or even quantum privacy amplification in order to improve the robustness of the protocol [29]. Finally, an absolute prove of the security of BB84 has been given by Shor and Preskill [30]. For a recent account on discrete quantum cryptography see Ref. [31].

References

- [1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
- [2] D. Dieks, Phys. Lett. A **92**, 271 (1982).
- [3] V. Buzek and M. Hillery, Phys. Rev. A **60**, R2626 (1999).
- [4] A. K. Pati and S. L. Braunstein, Nature **404**, 164 (2000).
- [5] R. Jozsa, in *Geometric Issues in the Foundations of Science*, Eds. S. Huggett et al, Oxford University Press, 1997.
- [6] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
- [7] R. Derka, V. Buzek and A. Ekert, Phys. Rev. Lett. **80**, 1571 (1997).
- [8] H. P. Yuen, Phys. Lett. A **113**, 405 (1986).
- [9] G. M. D’Ariano and H. P. Yuen, Phys. Rev. Lett. **76**, 2832 (1996).
- [10] H. Barnum et al, Phys. Rev. Lett. **76**, 2818 (1996).
- [11] V. Buzek and M. H. Hillery, Phys. Rev. A **54**, 1844 (1996).
- [12] D. Brub et al, Phys. Rev. A **57**, 2368 (1998).
- [13] V. Buzek et al, Phys. Rev. A **56**, 3446 (1997).
- [14] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
- [15] M. Keyl and R. F. Werner, J. Math. Phys. **40**, 3283 (1999).
- [16] N. Gisin, Phys. Lett. A **242**, 1 (1998).
- [17] S. Ghosh, G. Kar and A. Roy, Phys. Lett. A **261**, 17 (1999).

- [18] S. L. Braunstein, V. Bužek and M. Hillery, Phys. Rev. A **63**, 052313 (2001).
- [19] L. M. Duan and G. C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
- [20] A. K. Pati, Phys. Rev. Lett. **83**, 2849 (1999).
- [21] A.Chefles and S. M. Barnett, Phys. Rev. A **60**, 136 (1999).
- [22] R. Jozsa, quant-ph/0204153.
- [23] Y. Feng, S. Zhang and M. Yim, Phys. Rev. A **65**, 042324 (2002).
- [24] J. Feng, Y. F. Gao, J. S. Wang, and M. S. Zhan, Phys. Rev. A **65**, 052311 (2002).
- [25] D. Qiu, Phys. Rev. A **65**, 052303 (2002).
- [26] R. Rivest, A. Shamir and L. Adelman, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).
- [27] C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conference on Computers, Systems and Signal Processing (IEEE Press, Los Alamitos, Calif. 1984), p. 175.
- [28] A. Ekert, Phys. Rev. Lett. **67**, 661-663 (1991).
- [29] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, Phys. Rev. Lett. **77**, 288 (1996).
- [30] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
- [31] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

Chapter 20

QUANTUM CLONING WITH CONTINUOUS VARIABLES

Nicolas J. Cerf

Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium

ncerf@ulb.ac.be

1. INTRODUCTION

Quantum information theory has developed dramatically over the past decade, driven by the prospects of quantum-enhanced communication and computation systems. Among the most striking successes, one finds for example the discovery of quantum factoring, quantum key distribution, or quantum teleportation. Most of these concepts were initially developed for discrete quantum variables, in particular quantum bits, which have now become the symbol of quantum information. Recently, however, a lot of attention has been devoted to investigating the use of *continuous-variable* systems in quantum informational or computational processes. Continuous-spectrum quantum variables, for example the quadrature components of a light mode, may be easier to manipulate than quantum bits. It is actually sufficient to process squeezed states of light into linear optics circuits in order to perform various quantum information processes over continuous variables [1]. As reported in the present book, variables with a continuous spectrum have been shown to be useful to carry out quantum teleportation, quantum entanglement purification, quantum error correction, or even quantum computation.

In this Chapter, the issue of *cloning* a continuous-variable quantum system will be analyzed, and a Gaussian cloning transformation will be introduced. Cloning machines, that is, transformations that achieve the best approximate copying of a quantum state compatible with the no-cloning theorem, have been a fundamental research topic over the last five years (see e.g., [2] for an overview). This question is of particular significance given the close connection between quantum cloning and quantum cryptography: using an optimal cloner generally makes it possible to obtain a tight bound on the best individual eavesdropping strategy in a quantum cryptosystem. This provides a strong

incentive to investigating continuous-variable cloning in view of the recent proposals for quantum key distribution relying on continuous (Gaussian) key carriers [3, 4].

Here, we will focus on a Gaussian cloning transformation, which copies equally well any two canonically conjugate continuous variables such as the two quadrature components of a light mode [5]. More precisely, it achieves the *optimal* cloning of a continuous variable that satisfies the requirement of covariance with respect to displacements and rotations in phase space. Consequently, this cloner duplicates all coherent states with a same fidelity ($F = 2/3$). The optical implementation of this cloner and its extension to N -to- M cloners will also be discussed. Finally, the use of this cloner for the security assessment of continuous-variable quantum key distribution schemes will be sketched.

2. LIMITS ON OPTIMAL CLONING

Let us start by stating the problem of continuous-variable cloning in physical terms. Consider, as an example of canonically conjugate continuous variables, the quadrature components of a light mode, denoted as x and p . This notation reflects the fact that x and p behave just like the position and momentum of a particle in a one-dimensional space, namely their commutator is $[x, p] = i$ (we put $\hbar = 1$ in this paper). If the wave function is a Dirac delta function—the particle is fully localized in *position* space, then x can be measured exactly, and several perfect copies of the system can be prepared. However, such a cloning process fails to exactly copy non-localized states, *e.g.*, momentum states. Conversely, if the wave function is a plane wave with momentum p —the particle is localized in *momentum* space, then p can be measured exactly and one can again prepare several perfect copies of this plane wave. However, such a “plane-wave cloner” is then unable to copy position states exactly. In short, it is impossible to copy perfectly the eigenstates of two conjugate variables such as x and p : this is essentially the content of the so-called *no-cloning* theorem [6, 7].

In the next Section, we will show that a *cloning* transformation can nevertheless be found that provides two copies of a continuous system, but at the price of a non-unity cloning fidelity. In other words, the cloning machine yields two *imperfect* copies of the system. Before describing this cloning machine in detail, let us find a lower bound on the cloning-induced noise by exploiting a connection with measurement theory. More specifically, we make use of the fact that measuring x on one clone and p on the other clone cannot beat the optimal joint measurement of x and p on the original system [8]. It is known that such a joint measurement of a pair of conjugate observables on a single quantum system obeys an inequality akin to the Heisenberg uncertainty relation but with an extra contribution to the minimum variance [9]. Denoting by x and

p the two quadratures of the input mode, and by X and P the corresponding jointly measured output quadratures, we have

$$X = x + n_x \quad (20.1a)$$

$$P = p + n_p \quad (20.1b)$$

where n_x and n_p stand for the excess noise that we have on the measured quadratures. Since we consider a joint measurement, the variables X and P must commute: they can be viewed respectively as the x and p quadratures of two distinct modes. Thus, we have

$$[X, P] = [x, p] + [x, n_p] + [n_x, p] + [n_x, n_p] = 0 \quad (20.2)$$

Assuming that the excess noises n_x and n_p are independent of the input quadratures, *i.e.*, $[x, n_p] = [n_x, p] = 0$, we get $[n_x, n_p] = -i$, implying that n_x and n_p must obey an uncertainty relation. Specifically, any attempt to measure x and p simultaneously on a quantum system is constrained by the inequality

$$\Delta n_x \Delta n_p \geq 1/2 \quad (20.3)$$

where Δn_x^2 and Δn_p^2 denote the variances of the excess noises originating from the joint measurement device. If the variances of the x and p quadratures of the input state are denoted by δx^2 and δp^2 , respectively, we thus have for the variances of the measured values $\Delta X^2 = \delta x^2 + \Delta n_x^2$ and $\Delta P^2 = \delta p^2 + \Delta n_p^2$. As a consequence, the Heisenberg uncertainty relation $\delta x \delta p \geq 1/2$ together with inequality (20.3) implies the relation [9]

$$\Delta X \Delta P \geq 1 \quad (20.4)$$

where we have used the inequality $a^2 + b^2 \geq 2\sqrt{a^2 b^2}$. Thus, the best possible joint measurement of x and p with a same precision on both quadratures of a coherent state ($\delta x^2 = \delta p^2 = 1/2$) gives

$$\Delta X^2 = \Delta P^2 = 1 \quad (20.5)$$

Compared with the vacuum noise, we note that the joint measurement of x and p effects an additional noise of minimum variance $1/2$, so that the measured values suffer *twice* the vacuum noise.

Inequality (20.3) immediately translates into a lower bound on the cloning-induced noise variance [8]. If we assume that the device that is used in order to perform the joint measurement of x and p is actually a cloning machine followed by two measuring apparatuses (x being measured on one clone and p on the other clone), we conclude that the variance of the noise added by this cloning machine cannot be lower than $1/2$ in order to comply with Eq. (20.3), that is

$$\Delta n_x^2 = \Delta n_p^2 \geq 1/2 \quad (20.6)$$

(We require here the same noise level on x and p .) This can also be shown explicitly by writing the canonical transformation of the cloner [10]. Denoting by $X_{a(b)}$ and $P_{a(b)}$ the two quadratures of the output mode a (resp. b), we have

$$X_a = x + n_{x,a} \quad (20.7a)$$

$$P_a = p + n_{p,a} \quad (20.7b)$$

$$X_b = x + n_{x,b} \quad (20.7c)$$

$$P_b = p + n_{p,b} \quad (20.7d)$$

where x and p are the two quadratures of the input mode and $n_{x/p,a/b}$ stand for the excess noises. Since the clones are carried by different modes (a and b), we have $[X_a, P_b] = [X_b, P_a] = 0$. Assuming, as before, that the excess noises are independent of the input mode, we get $[n_{x,a}, n_{p,b}] = [n_{x,b}, n_{p,a}] = -i$. This gives rise to two no-cloning uncertainty relations

$$\Delta n_{x,a} \Delta n_{p,b} \geq 1/2 \quad (20.8a)$$

$$\Delta n_{x,b} \Delta n_{p,a} \geq 1/2 \quad (20.8b)$$

which constrain the excess noise variances $\Delta n_{x/p,a/b}^2$ of the two clones [5, 10]. Consequently, if the cloning process induces a small position (momentum) error on the first copy, then the second copy is necessarily affected by a large momentum (position) error. The Gaussian cloner we will discuss in the next Session saturates these inequalities and is symmetric in a and b (and in x and p):

$$\Delta n_{x,a}^2 = \Delta n_{p,a}^2 = \Delta n_{x,b}^2 = \Delta n_{p,b}^2 = 1/2 \quad (20.9)$$

To simplify the notation, we will denote this cloning-induced excess noise variance as σ^2 in the following.

3. GAUSSIAN CLONING TRANSFORMATION

We will define a class of cloning machines that yield two imperfect copies of a continuous-variable system, the underlying cloning transformation being *covariant* with respect to displacements in phase space (x, p) . By this, we mean that any two input states that are related by a displacement result in copies that are related in the same way; hence, the resulting cloning fidelity is invariant under displacements in phase space. Specifically, let us seek for a displacement-covariant transformation which duplicates with a same fidelity all coherent states $|\psi\rangle$. Thus, if two input states are identical up to a displacement $\hat{D}(x', p') = e^{-ix'\hat{p}}e^{ip'\hat{x}}$, then their respective copies should be identical up to the same displacement. Denoting by \mathcal{H} the Hilbert space corresponding to a single system, cloning can be defined as a completely-positive trace-preserving

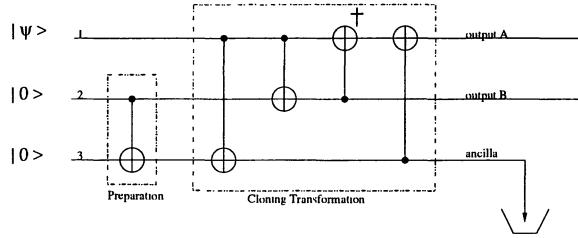


Figure 20.1 Quantum circuit for the continuous-variable cloning transformation. It consists of four C-NOT gates preceded by a preparation stage. Here, the ancillae are prepared in the state given by Eq. (20.19). See [5, 12].

linear map $\mathcal{C} : \mathcal{H} \rightarrow \mathcal{H}^{\otimes 2} : |\psi\rangle\langle\psi| \rightarrow \mathcal{C}(|\psi\rangle\langle\psi|)$ such that

$$\begin{aligned} & \mathcal{C} \left[\hat{D}(x', p') |\psi\rangle\langle\psi| \hat{D}^\dagger(x', p') \right] \\ &= \hat{D}(x', p')^{\otimes 2} \mathcal{C}(|\psi\rangle\langle\psi|) \hat{D}^\dagger(x', p')^{\otimes 2} \end{aligned} \quad (20.10)$$

for all displacements $\hat{D}(x', p')$.

As shown in [5], this cloning map can be achieved via a unitary transformation $\hat{\mathcal{U}}$ acting on three modes: the input mode (variable 1) supplemented with two auxiliary modes, the blank copy (variable 2) and an ancilla (variable 3). The two auxiliary variables must be initially prepared in the joint state

$$|\chi\rangle_{2,3} = \iint_{-\infty}^{\infty} dx dp f(x, p) |\Psi(x, -p)\rangle_{2,3} \quad (20.11)$$

where $f(x, p)$ is an (arbitrary) complex amplitude function, and

$$|\Psi(x, p)\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dx' e^{ipx'} |x'\rangle|x' + x\rangle \quad (20.12)$$

are the EPR states (the maximally-entangled states of two continuous variables). The cloning transformation is defined as

$$\hat{\mathcal{U}}_{1,2,3} = e^{-i(\hat{x}_3 - \hat{x}_2)\hat{p}_1} e^{-i\hat{x}_1(\hat{p}_2 + \hat{p}_3)} \quad (20.13)$$

where \hat{x}_k (\hat{p}_k) is the position (momentum) operator for variable k . As shown in Fig. 20.1, this can be interpreted as a sequence of four continuous-variable controlled-NOT (C-NOT) gates, each being defined as the unitary transformation $e^{-i\hat{x}_k\hat{p}_l}$ with k (l) referring to the control (target) variable [11].

Remarkably, Eq. (20.13) coincides with the discrete C-NOT gate sequence that achieves the qubit cloning transformation [13], up to a sign ambiguity

originating from the fact that a continuous C-NOT gate is not equal to its inverse. After applying \hat{U} to the state $|\psi\rangle_1|\chi\rangle_{2,3}$, we get the joint state

$$\int \int_{-\infty}^{\infty} dx dp f(x, p) \hat{D}(x, p) |\psi\rangle_1 |\Psi(x, -p)\rangle_{2,3} \quad (20.14)$$

where variables 1 and 2 are taken as the two outputs of the cloner (clones a and b), while variable 3 (the ancilla) must simply be traced over. This is a peculiar state in that it can be reexpressed in a similar form by exchanging the two clones, namely

$$\int \int_{-\infty}^{\infty} dx dp g(x, p) \hat{D}(x, p) |\psi\rangle_2 |\Psi(x, -p)\rangle_{1,3} \quad (20.15)$$

with

$$g(x, p) = \frac{1}{2\pi} \int \int_{-\infty}^{\infty} dx' dp' e^{i(px' - xp')} f(x', p') \quad (20.16)$$

being the two-dimensional Fourier transform of $f(x, p)$. The resulting state of the individual clones can then be written as

$$\rho_a = \int \int_{-\infty}^{\infty} dx dp |f(x, p)|^2 \hat{D}(x, p) |\psi\rangle \langle \psi| \hat{D}^\dagger(x, p) \quad (20.17a)$$

$$\rho_b = \int \int_{-\infty}^{\infty} dx dp |g(x, p)|^2 \hat{D}(x, p) |\psi\rangle \langle \psi| \hat{D}^\dagger(x, p) \quad (20.17b)$$

which is consistent with tracing Eq. (20.10) over any one of the clones. Thus, the clones are affected by position and momentum errors that are distributed according to $|f(x, p)|^2$ and $|g(x, p)|^2$. A central point here is that interchanging the two clones amounts to substitute the function f with its two-dimensional Fourier transform g . This property is crucial as it ensures that the two copies suffer from *complementary* position and momentum errors. Indeed, one can check [5] that the four excess noise variances defined as

$$\Delta n_{x,a}^2 = \int \int_{-\infty}^{\infty} dx dp x^2 |f(x, p)|^2, \quad (20.18a)$$

$$\Delta n_{p,a}^2 = \int \int_{-\infty}^{\infty} dx dp p^2 |f(x, p)|^2 \quad (20.18b)$$

$$\Delta n_{x,b}^2 = \int \int_{-\infty}^{\infty} dx dp x^2 |g(x, p)|^2, \quad (20.18c)$$

$$\Delta n_{p,b}^2 = \int \int_{-\infty}^{\infty} dx dp p^2 |g(x, p)|^2 \quad (20.18d)$$

obey the no-cloning inequalities (20.8a) and (20.8b). (Here, we assume that the first-order moments of $|f(x, p)|^2$ and $|g(x, p)|^2$ vanish, that is, the clones are not biased.)

Within this class of cloning machines parametrized by $f(x, p)$, a particularly simple *rotation-covariant* cloner can be found that provides two *identical* copies of a continuous system with the *same* error distribution in position and momentum. It corresponds to the choice $f(x, p) = g(x, p) = e^{-(x^2+p^2)/2}/\sqrt{\pi}$. This cloner is named “Gaussian” as it effects Gaussian-distributed position- and momentum-errors on the input mode: the excess noise on both clones is distributed as $e^{-(x^2+p^2)/\pi}$, that is, as a bi-variate rotational-invariant Gaussian of variance $\sigma^2 = 1/2$. This cloner is *optimal*, as it satisfies Eq. (20.9). Here, the two auxiliary variables must be prepared in the state

$$|\chi\rangle_{2,3} = \frac{1}{\sqrt{\pi}} \int \int_{-\infty}^{\infty} dy dz e^{-(y^2+z^2)/2} |y\rangle_2 |y+z\rangle_3 \quad (20.19)$$

which is simply the product vacuum state $|0\rangle_2 |0\rangle_3$ processed by a C-NOT gate $e^{-i\hat{x}_2\hat{p}_3}$. The resulting transformation effected by $\hat{\mathcal{U}}$ on an input position state $|x\rangle$ is thus given by

$$\begin{aligned} |x\rangle_1 |\chi\rangle_{2,3} &\rightarrow \frac{1}{\sqrt{\pi}} \int \int_{-\infty}^{\infty} dy dz e^{-(y^2+z^2)/2} \\ &|x+y\rangle_1 |x+z\rangle_2 |x+y+z\rangle_3 \end{aligned} \quad (20.20)$$

where the three variables denote the two clones and the ancilla, respectively. For an arbitrary input state $|\psi\rangle$, it is readily checked that this transformation outputs two clones whose individual states are Gaussian distributed with a variance $\sigma^2 = 1/2$, namely

$$\rho_a = \rho_b = \frac{1}{\pi} \int \int_{-\infty}^{\infty} dx dp e^{-(x^2+p^2)} \hat{D}(x, p) |\psi\rangle \langle \psi| \hat{D}^\dagger(x, p), \quad (20.21)$$

In particular, if the input is a coherent state $|\alpha\rangle$ with $\alpha = (x+ip)/\sqrt{2}$, it is easy to calculate the fidelity of this cloner by using $|\langle\alpha|\alpha'\rangle|^2 = \exp(-|\alpha - \alpha'|^2)$:

$$F = \langle\alpha|\rho_{a(b)}|\alpha\rangle = \frac{1}{1+\sigma^2} = \frac{2}{3} \quad (20.22)$$

This cloning fidelity does not depend on α , so this Gaussian cloner copies *all* coherent states with the same fidelity $2/3$. It can be viewed as the continuous counterpart of the universal qubit cloner [13], as its cloning fidelity is invariant under rotations in phase space. The physical origin of the cloning noise becomes, however, much more evident in the case of continuous variables: the Gaussian noise that affects the clones can simply be traced back to the Gaussian wave function of the two ancillary modes, see (20.19). This suggests that the noise that inevitably arises when cloning is intrinsically linked to the vacuum fluctuations of the auxiliary modes.

Note finally that this formalism can easily be extended to the cloning of squeezed state instead of coherent states [5]. One simply unsqueeze the state before cloning and then squeeze the clones again. For any value of the squeezing parameter r , one can then define a Gaussian cloner that copies with fidelity 2/3 all squeezed states of which the same quadrature is squeezed by the same amount r . In contrast, cloning these squeezed states using the rotation-covariant cloner defined above results in a fidelity that decreases as r increases.

4. OPTICAL IMPLEMENTATION

It is very instructive to write the cloning transformation in the Heisenberg picture, that is, following the evolution of the annihilation operators associated with the modes that are involved. Again, mode 1 denotes the input mode, and modes 2 and 3 the ancillary modes. Mode 1' and 2' stand for the two clones, while 3' is the ancilla that is traced over after cloning. Here, $a_j = (x_j + ip_j)/\sqrt{2}$ stands for the annihilation operator for mode j . We require that the cloning transformation conserves the mean values, *i.e.*, $\langle a'_1 \rangle = \langle a'_2 \rangle = \langle a_1 \rangle$, so that the clones are centered on the original coherent state. We also require that the cloning transformation is covariant under rotations in phase space. It is shown in [14] that the optimal transformation satisfying these requirements is

$$a'_1 = a_1 + \frac{a_2}{\sqrt{2}} + \frac{a_3^\dagger}{\sqrt{2}} \quad (20.23a)$$

$$a'_2 = a_1 - \frac{a_2}{\sqrt{2}} + \frac{a_3^\dagger}{\sqrt{2}} \quad (20.23b)$$

$$a'_3 = a_1^\dagger + \sqrt{2} a_3 \quad (20.23c)$$

where mode 1 is initially prepared in an arbitrary coherent state $|\alpha\rangle$, with $\alpha = (x + ip)/\sqrt{2}$, while modes 2 and 3 are prepared in the vacuum state. This transformation clearly satisfies the commutation rules $[a'_i, a'_j] = \delta_{i,j}$ and yields the correct mean values (x, p) for the two clones (modes 1' and 2'). Also, one can easily check that the quadrature variances of the clones are equal to twice the vacuum noise, in accordance with the cloning excess noise variance $\sigma^2 = 1/2$. This transformation actually coincides with the Gaussian cloner introduced in the previous Section. Interestingly, we note here that the state in which the ancilla 3 is left after cloning is centered on $(x, -p)$, that is the *phase-conjugated* state $|\alpha^*\rangle$. This means that, in analogy with the universal qubit cloner, the Gaussian cloner generates an “anticlone” (or time-reversed state) together with the two clones.

As suggested by the above transformation, a possible optical implementation of this Gaussian cloner consists in processing the input mode a_1 into a linear

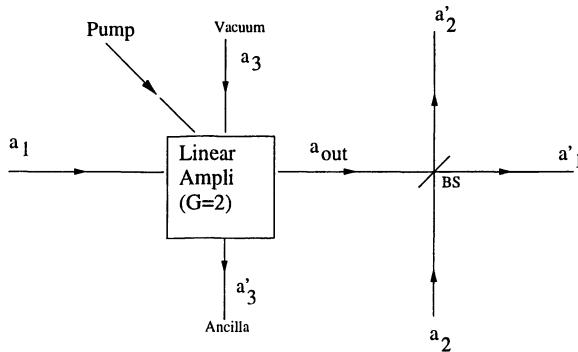


Figure 20.2 Implementation of a Gaussian cloner using a phase-insensitive linear amplifier and a 50:50 beam-splitter (BS). See [12].

phase-insensitive amplifier [15] of gain $G = 2$:

$$a_{out} = \sqrt{2} a_1 + a_3^\dagger, \quad a'_3 = a_1^\dagger + \sqrt{2} a_3, \quad (20.24)$$

with mode 3 denoting the idler mode. This amplifier is limited by the quantum noise so it naturally leads to an optimal cloner. A gain $G = 2$ is needed since the cloner doubles the energy by creating two clones with the same energy as the input state. One then produces these two clones simply by processing the output signal of the amplifier through a 50:50 phase-free beam splitter,

$$a'_1 = \frac{1}{\sqrt{2}}(a_{out} + a_2), \quad a'_2 = \frac{1}{\sqrt{2}}(a_{out} - a_2), \quad (20.25)$$

as shown in Fig. 20.2. The rotation covariance of the resulting cloner is ensured by the fact that the amplifier and the beam splitter are phase-insensitive. Actually, combining Eqs. (20.24) and (20.25) results in the same canonical transformation as above, so this optical setup indeed implements the optimal Gaussian cloner. It is readily checked that this setup leads to an equal x - and p -error variance of $1/2$ for both clones.

5. GAUSSIAN CLONERS WITH MULTIPLE INPUTS AND OUTPUTS

Let us now consider the general problem of optimal $N \rightarrow M$ cloning, extending what was done in [16] for the case of quantum bits. Consider a Gaussian transformation which, from N (≥ 1) identical replicas of an original input state, produces M (≥ 2) output copies whose individual states are again given by an expression similar to Eq. (20.21) but with an error variance $\sigma^2_{N,M}$. (For the $1 \rightarrow 2$ Gaussian cloner above, we had $\sigma^2_{1,2} = 1/2$.) Using an

argument based on the concatenation of cloners, it is possible to derive a lower bound on $\sigma_{N,M}^2$, that is [8]

$$\sigma_{N,M}^2 \geq \frac{1}{N} - \frac{1}{M}, \quad (20.26)$$

so that the corresponding cloning fidelity for coherent states satisfies

$$F_{N,M} \leq \frac{MN}{MN + M - N}. \quad (20.27)$$

The proof is connected to quantum state estimation theory, the key idea being that cloning should not be a way of circumventing the noise limitation encountered in any measuring process. More specifically, concatenating a $N \rightarrow M$ cloner with a $M \rightarrow L$ cloner results in a $N \rightarrow L$ cloner that cannot be better than the *optimal* $N \rightarrow L$ cloner. We then make use of the fact that the excess noise variance of this $N \rightarrow L$ cloner simply is the sum of the excess noise variances of the two component cloners [8]. Denoting by $\sigma_{N,M}^2$ the excess noise variance of the *optimal* $N \rightarrow M$ cloner, we get the inequality $\sigma_{N,L}^2 \leq \sigma_{N,M}^2 + \sigma_{M,L}^2$. In particular, if $L \rightarrow \infty$, we have

$$\sigma_{N,\infty}^2 - \sigma_{M,\infty}^2 \leq \sigma_{N,M}^2 \quad (20.28)$$

Since the limit of cloning with an infinite number of clones corresponds to a measurement, Eq. (20.28) simply implies that cloning the N replicas before measuring the M resulting clones does not provide a mean to enhance the accuracy of a direct measurement of the N replicas. This limit is useful because the joint measurement of x and p on N identical replicas of a coherent state is known to give a minimum noise variance $\sigma_{N,\infty}^2 = 1/N$. This, combined with Eq. (20.28), gives the minimum noise variance induced by cloning, Eq. (20.26), along with the corresponding cloning fidelity, Eq. (20.27). Note that these bounds can also be derived when $N = 1$ using techniques similar to the ones used for describing quantum nondemolition measurements. This was done in a paper establishing a link between cloning and teleportation for continuous variables [10]: for the $1 \rightarrow 2$ cloner, the teleportation fidelity must exceed $F_{1,2} = 2/3$ in order to guarantee that the teleported state is of better quality than the state kept by the emitter.

Just like for the $1 \rightarrow 2$ cloner, the bounds Eqs. (20.26) and (20.27) can be attained by a transformation whose implementation requires only a phase-insensitive linear amplifier and beam splitters [14, 17]. Loosely speaking, the procedure consists in concentrating the N input modes into a single mode by use of a network of beam splitters, then in amplifying the resulting mode and distributing the output mode of the amplifier into M modes through a second network of beam-splitters. A convenient way to achieve these concentration and distribution stages is provided by networks of beam splitters that realize

a Discrete Fourier Transform (DFT). Cloning is then achieved by the following three-step procedure (see Fig. 20.3). First step: the N input modes are concentrated into a single mode through a DFT (acting on N modes):

$$a'_k = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \exp(ikl2\pi/N) a_l, \quad (20.29)$$

with $k = 0 \dots N - 1$. This operation concentrates the energy of the N input modes a_l into one single mode a'_0 (hereafter renamed a_0) and leaves the remaining $N - 1$ modes ($a'_1 \dots a'_{N-1}$) in the vacuum state. Second step: the mode a_0 is amplified with a linear amplifier of gain $G = M/N$. This results in

$$a'_0 = \sqrt{\frac{M}{N}} a_0 + \sqrt{\frac{M}{N} - 1} a_z^\dagger, \quad (20.30a)$$

$$a'_z = \sqrt{\frac{M}{N} - 1} a_0^\dagger + \sqrt{\frac{M}{N}} a_z. \quad (20.30b)$$

Third step: amplitude distribution by performing a DFT (acting on M modes) between the mode a'_0 and $M - 1$ blank modes in the vacuum state:

$$a''_k = \frac{1}{\sqrt{M}} \sum_{l=0}^{M-1} \exp(ikl2\pi/M) a'_l, \quad (20.31)$$

with $k = 0 \dots M - 1$, and $a'_i = a_i$ for $i = N \dots M - 1$. The DFT now distributes the energy contained in the output of the amplifier among the M output clones.

It is readily checked that this procedure meets the requirements we put on the $N \rightarrow M$ cloner, and is optimal. Indeed the quadrature variance of the M output modes gives $1/2 + 1/N - 1/M$, implying that the cloning-induced excess noise variance is $1/N - 1/M$. Furthermore, the transformation is rotation covariant since the amplifier and the beam splitters are phase insensitive. In conclusion, we see that the optimal $N \rightarrow M$ cloning transformation can be implemented using only passive elements except for a single linear amplifier.

The above cloning transformation can be extended even further by considering a generalized cloner that produces M clones from N replicas of a coherent state and N' replicas of its complex conjugate [18]. It is again universal over the set of coherent states in the sense that the cloning fidelities are invariant for all input coherent states. Interestingly, it can be shown that supplementing the N input states $|\psi\rangle^{\otimes N}$ with N' phase-conjugated input states $|\psi^*\rangle^{\otimes N'}$ can, under certain circumstances, provide clones with a *higher* fidelity than the above $N + N' \rightarrow M$ cloner. Note that, together with the M clones, this phase-conjugate input cloner also yields M' antyclones (approximate copies

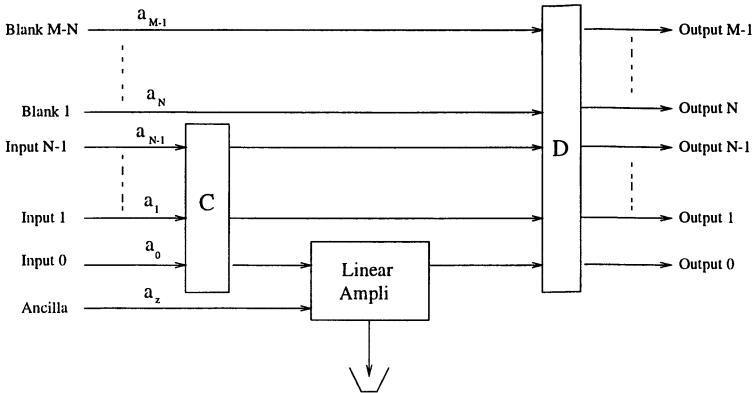


Figure 20.3 Implementation of an $N \rightarrow M$ continuous-variable cloning machine based on a phase-insensitive linear amplifier. Here, C stands for the amplitude concentration stage while D refers to amplitude distribution. Both can be realized using a network of beam-splitters that achieve a DFT. See [14].

of $|\psi^*\rangle$) at no cost, with $N - N' = M - M'$. The advantage of having phase-conjugated inputs for a continuous-variable cloner actually also has a counterpart in the context of qubit cloners. Indeed, motivated by this finding on continuous-variable cloners, an optimal universal cloning transformation was recently derived that produces M copies of an unknown pair of orthogonal qubits [19]. For $M > 6$, the cloning fidelity for a pair of orthogonal qubits can be shown to be higher than that of the optimal cloning of a pair of identical qubits. This is a first example of a quantum informational process that was initially described for continuous-variable systems and only later on extended back to quantum bits.

6. EAVESDROPPING IN CONTINUOUS-VARIABLE QUANTUM CRYPTOGRAPHY

As mentioned above, quantum cloning can be viewed as an individual eavesdropping strategy in continuous-variable quantum cryptography. Consider a quantum key distribution scheme in which the key is encoded into the displacement of a coherent or a squeezed state that is drawn from a Gaussian distribution [3, 4]. In the continuous-variable protocol defined in [3], which we will analyze here, squeezed states need to be used. The emitter (Alice) prepares a squeezed state for which the quadrature that is squeezed, x or p , is chosen at random, and then displaces it by $\hat{D}(r, 0)$ or $\hat{D}(0, r)$ depending on x or p is squeezed. Here, r is drawn from a Gaussian distribution, and constitutes a continuous key element. The receiver (Bob) then measures either the x - or p -quadrature of the state he received, this choice being again random. After Bob's measurement,

Alice reveals the quadrature she squeezed (and displaced) and Bob rejects the cases where he measured the wrong quadrature, this discussion being made over an authenticated public channel (this procedure is known as sifting). The subset of states that are accepted by Bob then constitutes a Gaussian raw key (correlated Gaussian data at Alice's and Bob's side). Indeed, denoting as v the variance of the quadrature that is squeezed by Alice, Bob gets for his measured quadrature an outcome r' that is Gaussian distributed around r with a variance v (assuming for the moment that the quantum channel is perfect and that there is no eavesdropping). If the variance of the random displacements r imposed by Alice is noted V , then this raw key shared by Alice and Bob can be viewed as resulting from a Gaussian additive-noise channel characterized by a signal-to-noise ratio of V/v .

The maximum amount of shared key bits that can be extracted from this Gaussian raw key can be analyzed by applying some standard notions of Shannon theory for continuous channels (see *e.g.* [20]). Consider a discrete-time continuous channel that adds a Gaussian noise of variance v to the signal. If the input r of the channel is a Gaussian signal of variance V , the uncertainty on r can be measured by its Shannon entropy $h(r) = 2^{-1} \log_2(2\pi e V)$ bits. Conditionally on r , the output r' is distributed as a Gaussian of variance v , so that the entropy of r' conditionally on r becomes $h(r'|r) = 2^{-1} \log_2(2\pi e v)$ bits. Now, the overall distribution of r' is of course the convolution of these two distributions, *i.e.*, a Gaussian of variance $V + v$, so that the output entropy is $h(r') = 2^{-1} \log_2(2\pi e (V + v))$ bits. According to Shannon theory, the information processed through this noisy channel $r \rightarrow r'$ can be expressed as the amount by which the uncertainty on r' is reduced by knowing r , that is

$$I \text{ (bits)} = h(r') - h(r'|r) = \frac{1}{2} \log_2 \left(1 + \frac{V}{v} \right) \quad (20.32)$$

where V/v is the signal-to-noise ratio. This is Shannon's famous formula for the capacity of a Gaussian additive-noise channel. It is worth noticing that this capacity is achieved in the case where the input is distributed as a Gaussian, which is precisely the case under consideration here.

In the protocol analyzed in [3], the variances v and V are related by the constraint that Alice's choice of encoding the key into either x or p should be invisible to a potential eavesdropper. In the first case, Alice applies a Gaussian-distributed displacement $\hat{D}(r, 0)$ on a squeezed state whose x quadrature has a variance v , so that the quadratures x and p of this Gaussian mixture have a variance $V + v$ and $1/(4v)$, respectively. In the second case, Alice applies a displacement $\hat{D}(0, r)$ on a squeezed state in p , resulting in a Gaussian mixture with variances $1/(4v)$ and $V + v$ for x and p . These two Gaussian mixtures are required to be indistinguishable, which simply translates into the requirement

that they have the same x variance and p variance:

$$V + v = \frac{1}{4v} \quad (20.33)$$

This gives for the information

$$I = \log_2 \left(\frac{1/2}{v} \right) \quad (20.34)$$

which measures the maximum number of key bits that can be extracted asymptotically (at the limit of long sequences) per use of the channel. (The factor $1/2$ here is just the vacuum noise, so we see that this protocol requires squeezing, that is, $v < 1/2$.) The actual methods that may be used to discretize the Gaussian raw key and correct the resulting errors so as to extract a common bit string are known as *reconciliation* protocols [21].

Let us now consider the information that is transmitted in the presence of an eavesdropper. We assume that the eavesdropper (Eve) processes each key element into a Gaussian cloning machine, keeps one clone, and sends the other one to Bob. Once the quadrature that contains the key (x or p) is revealed by Alice and Bob, Eve properly measures her clone. Clearly, Eve needs to use an asymmetric version of the Gaussian cloner described above as she must be able to tune the information she gains, and therefore the disturbance she effects in the transmission. (A possible implementation of this asymmetric Gaussian cloner is discussed in [17].) Thus, Eve adds some extra noise on the quadrature encoding the key, which results in a reduced signal-to-noise ratio on Alice-Bob channel. Remember here, that the quality of the two clones obey a no-cloning uncertainty relation akin to the Heisenberg relation, implying that the product of the x -error variance on the first clone times the p -error variance on the second one remains bounded by $(1/2)^2$; see Eqs. (20.8a) and (20.8b). In particular, if x and p are treated symmetrically, we have

$$\Delta n_B^2 \Delta n_E^2 \geq (1/2)^2 \quad (20.35)$$

This translates into a balance between the signal-to-noise ratio in Alice-Bob channel $V/(v + \Delta n_B^2)$ and that in Alice-Eve channel $V/(v + \Delta n_E^2)$. This latter channel is also a Gaussian channel so it can be treated similarly. Using Eq. (20.33), we can write the information processed respectively in Alice-Bob and Alice-Eve channels as

$$I_{AB} = \frac{1}{2} \log_2 \left(\frac{1 + 4v \Delta n_B^2}{4v(v + \Delta n_B^2)} \right) \quad (20.36a)$$

$$I_{AE} = \frac{1}{2} \log_2 \left(\frac{1 + 4v \Delta n_E^2}{4v(v + \Delta n_E^2)} \right) \quad (20.36b)$$

which gives

$$I_{AB} + I_{AE} - I = \frac{1}{2} \log_2 \left(\frac{(1 + 4v \Delta n_B^2)(1 + 4v \Delta n_E^2)}{4(v + \Delta n_B^2)(v + \Delta n_E^2)} \right) \quad (20.37)$$

One can then show that $I_{AB} + I_{AE} - I \leq 0$ by checking that the quantity inside the logarithm is less or equal to one. This simplifies to the condition

$$1 - 4v^2 \leq 4 \Delta n_B^2 \Delta n_E^2 (1 - 4v^2) \quad (20.38)$$

which is indeed true as a consequence of Eq. (20.35) and $v < 1/2$. Consequently, we have proven that, in this quantum cryptographic protocol, the no-cloning uncertainty relation translates into an information exclusion principle [3]

$$I_{AB} + I_{AE} \leq I \quad (20.39)$$

In other words, the information I_{AE} gained by Eve is upper bounded by the defect of information at Bob's side, $I - I_{AB}$, which implies that the security is guaranteed if $I_{AB} \geq I/2$ (since Bob then has an advantage over Eve, $I_{AB} \geq I_{AE}$). Note that the bound in Eq. (20.39) is saturated by the asymmetric Gaussian cloner discussed above, which strongly suggests that this is the optimal individual attack (this actually can be proven rigorously). In practice, Alice and Bob can estimate the potentially eavesdropped information in the following way. Alice discloses the values r she sent for a random subset of the raw key. Then, Bob compares them to the values r' he received, in order to estimate the variance of the distribution of the differences $r' - r$, *i.e.*, the excess noise variance Δn_B^2 . This is sufficient to estimate I_{AB} , and, via Eq. (20.39), an upper bound on I_{AE} .

An extended continuous-variable quantum key distribution protocol relying on Gaussian key carriers has recently been proposed in [4], where coherent states may be used instead of squeezed states. The encoding then consists in imposing a displacement $\hat{D}(x, p)$ onto the vacuum state with x and p being drawn from a bi-variate Gaussian distribution. Here, the choice of the quadrature is made by Bob, who decides to measure x or p at random and then discloses his choice on the public channel. The corresponding value of Alice's displacement (x or p) together with Bob's measured outcome again can be viewed as resulting from a Gaussian channel, so the above information-theoretic treatment can be extended. In particular, one can calculate I_{AB} and I_{AE} in the case of an individual attack based on asymmetric Gaussian cloners. The security analysis of this coherent-state protocol is beyond the scope of the present paper (see [4]).

Acknowledgments

I would like to thank S. L. Braunstein, S. Iblisdir, P. van Loock, S. Massar, and G. Van Assche for their contribution to the work reported on here.

References

- [1] S. L. Braunstein. Quantum error correction for communication with linear optics. *Nature* 394, 47 (1998).
- [2] S. L. Braunstein, V. Buzek, and M. Hillery. Quantum-information distributors: Quantum network for symmetric and asymmetric cloning in arbitrary dimension and continuous limit. *Phys. Rev. A* 63, 052313 (2001).
- [3] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* 63, 052311 (2001).
- [4] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* 88, 057902 (2002).
- [5] N. J. Cerf, A. Ipe, and X. Rottenberg. Cloning of continuous quantum variables. *Phys. Rev. Lett.* 85, 1754 (2000).
- [6] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature* 299, 802 (1982).
- [7] D. Dieks. Communication by EPR devices. *Phys. Lett. A* 92, 271 (1982).
- [8] N. J. Cerf and S. Iblisdir. Optimal N -to- M cloning of conjugate quantum variables. *Phys. Rev. A* 62, 040301 (2000).
- [9] E. Arthurs and J. L. Kelly, Jr. On the simultaneous measurement of a pair of conjugate observables. *Bell Syst. Tech. J.* 44, 725 (1965).
- [10] F. Grosshans and P. Grangier. Quantum cloning and teleportation criteria for continuous quantum variables. *Phys. Rev. A* 64, 010301 (2001).
- [11] S. L. Braunstein. Error correction for continuous variables. *Phys. Rev. Lett.* 80, 4084 (1998).
- [12] N. J. Cerf and S. Iblisdir. Universal copying of coherent states: a Gaussian cloning machine. In *Quantum Communication, Computing, and Measurement 3*, (Kluwer Academic, New York, 2001), pp. 11–14.
- [13] V. Buzek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A* 54, 1844 (1996).
- [14] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar. Optimal cloning of coherent states with a linear amplifier and beam splitters. *Phys. Rev. Lett.* 86, 4438 (2001).

- [15] C. M. Caves. Quantum limits on noise in linear amplifiers. *Phys. Rev. D* 26, 1817 (1982).
- [16] N. Gisin and S. Massar. Optimal quantum cloning machines. *Phys. Rev. Lett.* 79, 2153 (1997).
- [17] J. Fiurasek. Optical implementation of continuous-variable quantum cloning machines. *Phys. Rev. Lett.* 86, 4942 (2001).
- [18] N. J. Cerf and S. Iblisdir. Quantum cloning machines with phase-conjugate input modes. *Phys. Rev. Lett.* 87, 247903 (2001).
- [19] J. Fiurasek, S. Iblisdir, S. Massar, and N. J. Cerf. Quantum cloning of orthogonal qubits. *Phys. Rev. A* 65, 040302(R) (2002).
- [20] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley & Sons, New York, 1991.
- [21] N. J. Cerf, S. Iblisdir, and G. Van Assche. Cloning and cryptography with quantum continuous variables. *Eur. Phys. J. D* 18, 211 (2002).

Chapter 21

QUANTUM KEY DISTRIBUTION WITH CONTINUOUS VARIABLES IN OPTICS

T. C. Ralph

Department of Physics, Centre for Quantum Computer Technology,

University of Queensland, St Lucia 4072, QLD, Australia

ralph@physics.uq.edu.au

Abstract We discuss a quantum key distribution scheme in which small phase and amplitude modulations of quantum limited, CW light beams carry the key information. We identify universal constraints on the level of shared information between the intended receiver (Bob) and any eavesdropper (Eve) and use this to make a general evaluation of the security and efficiency of the scheme.

1. INTRODUCTION

The distribution of random number keys for cryptographic purposes can be made secure by using the fundamental properties of quantum mechanics to ensure that any interception of the key information can be detected. This was first discussed for discrete systems in Refs. [1, 2, 3]. Experimental demonstrations have been carried out using low photon number, optical sources [4, 5].

The basic mechanism used in quantum cryptographic schemes is the fact that the act of measurement in quantum mechanics inevitably disturbs the system. This measurement back-action exists for both discrete and continuous quantum mechanical variables. Thus it is natural to ask if quantum cryptographic schemes based on continuous variables are possible. There are a number of practical disadvantages with discrete quantum cryptographic schemes, mainly associated with the lack of true single photon sources. Also it is of fundamental interest to quantum information research to investigate links between discrete variable, single photon phenomena and continuous variable, multi-photon effects. This has motivated a consideration of quantum cryptographic schemes using multi-photon light modes [6, 7, 8, 9, 10, 11, 12, 13, 14].

Most of these schemes use squeezed light [15] in their protocols, either by producing entanglement from the squeezing [11, 9, 10] or using the squeezing directly [8, 12]. In contrast to these, schemes based on coherent states have also been discussed [7, 14]. The signals from which the key material is obtained are encoded in various ways in the different schemes.

The question of optimum protocols and eavesdropper strategies has been studied in detail for the single quanta case [16], leading to general proofs of security for discrete systems [17, 18]. A general proof of the optimum eavesdropper strategy for individual attacks in a simple continuous variable scheme was presented in Ref. [11]. Physical implementations saturating this optimum strategy were discussed in Refs [11, 13, 14]. A general proof of absolute security for a more sophisticated scheme was presented in Ref. [12].

In this chapter we will analyse in some detail quantum key distribution protocols based on the optical coherent state and squeezed state schemes introduced in Refs. [7, 11]. Our emphasis will be on specific implementations that Alice and Bob might use rather than general limits. The particular implementations have been chosen mostly for their simplicity rather than their optimality. Eve on the other hand is always assumed to be employing the optimum eavesdropping strategies allowed by quantum physics [19]. We estimate the efficiency of the two schemes and hence secure key transmission rates under conditions of negligible and non-negligible losses.

In Section I we review the encoding of information on light with small amplitude and phase modulations and introduce a particular encoding scheme. In Section II we find the minimum disturbance that an optimum eavesdropping scheme will introduce. The coherent state cryptographic scheme is introduced in Section III and the minimum error rates that an optimum Eve will introduce are calculated. In Section IV the concepts of mutual information, data reconciliation and privacy amplification are introduced and specific examples are applied to the coherent state scheme. The security and efficiency of the scheme are evaluated. The squeezed state cryptographic scheme is introduced, analysed and evaluated in Section V. In section VI we discuss a physical implementation of the optimal eavesdropper strategy and we conclude in Section VII.

2. ENCODING INFORMATION WITH SMALL AMPLITUDE AND PHASE MODULATIONS

One way of encoding information on a light beam is by imposing small modulations of the phase or amplitude of the beam at some radio frequency (rf) with respect to the main optical frequency. We suppose that these signals are imposed at an rf sufficiently large that technical noise can be ignored and so our measurement precision is limited only by quantum noise. Typically frequencies

in excess of about a MHz will suffice. That quantum mechanics must impose limits in this situation is because the amplitude and phase quadrature amplitudes of the beam are the analogues of position and momentum variables. Hence they are continuous, non-commuting variables that exhibit uncertainty relations.

We can represent our light field via

$$\hat{a}(t) = \alpha + \delta\hat{a}(t) + \delta s(t) \quad (21.1)$$

where \hat{a} is a bosonic annihilation operator which we have decomposed into a steady state part, the coherent amplitude, α , treated classically, and two time varying parts: the quantum fluctuations, modelled by the operator $\delta\hat{a}(t)$; and the classical modulation, modelled by $\delta s(t)$. If we take the phase of α real then the amplitude fluctuations, \tilde{X}^+ , and the phase fluctuations, \tilde{X}^- , are given by

$$\begin{aligned}\tilde{X}^+ &= \delta\hat{a}(t)^\dagger + \delta s(t)^* + \delta\hat{a}(t) + \delta s(t) \\ \tilde{X}^- &= i(\delta\hat{a}(t)^\dagger + \delta s(t)^* - \delta\hat{a}(t) - \delta s(t))\end{aligned} \quad (21.2)$$

Homodyne detection using a local oscillator with a coherent amplitude much larger than that of the signal beam can be used to measure the fluctuations. Spectral analysis then extracts the fluctuation power at a particular rf, ω , such that

$$V^+(\omega) = \langle |\tilde{X}^+|^2 \rangle = V_n^+ + V_s^+ \quad (21.3)$$

and

$$V^-(\omega) = \langle |\tilde{X}^-|^2 \rangle = V_n^- + V_s^- \quad (21.4)$$

where V_n^+ (V_n^-) is the amplitude (phase) quantum noise power whilst V_s^+ (V_s^-) is the amplitude (phase) signal power. The tilde indicates a Fourier transform.

The amount of information that can be carried on a Gaussian, additive noise, communication channel, such as we will consider here, depends on the signal to noise [20]. For a fixed bandwidth, any reduction in the signal to noise will inevitably lead to increased errors in the transmission. In our cryptographic scheme signals will be encoded on both quadratures but read out from only one, randomly chosen. This will force any eavesdroppers to monitor both the amplitude and phase quadratures simultaneously. For these non-commuting observables the information that can be obtained in this way is strictly limited by the generalized uncertainty principle for simultaneous measurements [21, 22]. We will discuss this principle in detail in the next section. Here let us consider a simple example. Suppose we try to observe both quadratures by dividing the beam in two at a 50:50 beamsplitter and detecting the amplitude quadrature of

one beam and the phase quadrature of the other. Originally the signal to noises are given by

$$(S/N)^\pm = \frac{V_s^\pm}{V_n^\pm} \quad (21.5)$$

However the signal to noises detected after the beamsplitter are

$$(S/N)_{sim}^\pm = \left(\frac{V_n^\pm}{V_n^\pm + V_m^\pm} \right) S/N^\pm = T^\pm S/N^\pm \quad (21.6)$$

where we define T^+ (T^-), the amplitude (phase) signal transfer coefficient, as the ratio of signal to noise out to signal to noise in. The quantum noise which is inevitably added through the empty beamsplitter port is V_m^\pm . The spectral powers are normalized to the quantum noise limit (QNL) such that a coherent beam has $V_n^\pm = 1$. Normally the partition noise will also be at this limit ($V_m^\pm = 1$). For a classical light field, i.e. where $V_n^\pm \gg 1$ the penalty will be negligible. However for a coherent beam a halving of the signal to noise for both quadratures is unavoidable.

One specific encoding scheme is that of binary pulse code modulation. The data is encoded as a train of Fourier transform limited pulses with average power V_s . A pulse on represents a “1”, a pulse off represents a “0”. For such bandwidth limited transmission the bit error rate or error probability (\mathcal{B}) and the signal to noise (S/N) are related by [23]

$$\mathcal{B} = \frac{1}{2} \operatorname{erfc} \frac{1}{2} \sqrt{\frac{1}{2} S/N} \quad (21.7)$$

Suppose our signal to noise is initially 13 dB. From Eq.21.7 direct detection of a single quadrature will retrieve its pulse train with a bit error rate of 1%. If the beam is in a coherent state and we simultaneously detect both quadratures then Eq.21.6 tells us that the signal to noise is halved. Eq.7 then predicts the error rate will rise to 5%.

Alternatively, and more efficiently, signals can be encoded as coherent signals. Given the ability to phase lock to the signal frequency a mathematical equivalence exists between the situation of signal side bands on a QNL background and that of a DC coherent state of the same amplitude. We can thus represent a coherent signal, of amplitude α by the state ket $|\alpha\rangle$. If the information is sent as a Gaussian distribution of such states, then in principle the Shannon channel capacity [20]

$$C = \frac{1}{2} \log_2 [1 + \frac{S}{N}] \quad (21.8)$$

can be achieved by a suitable encoding. By using Gaussian distributions of coherent states on both quadratures (ie of purely real and imaginary amplitudes)

a more efficient continuous variable quantum key distribution protocol can be constructed [14]. A similar encoding, but based on squeezed states was introduced earlier [13]. Never-the-less qualitatively similar results are obtained from an analysis of the binary pulse encoding, which we will pursue here for its simplicity.

3. OPTIMUM EAVESDROPPER STRATEGY

In this section we will use the generalized uncertainty principle to identify the minimum disturbance allowed by quantum mechanics to the information Bob receives given a particular level of interception by Eve. The idea is shown schematically in Fig. 21.1. A single quantum limited beam is sent from Alice to Bob. Eve makes some unspecified interception of the beam enroute. Bob and Eve obtain some measurement results. We will show that quantum mechanics sets unambiguous limits on the level of quantum noise that must appear in Bob and Eve's results. In the following sections we will apply these results to specific quantum cryptographic systems.

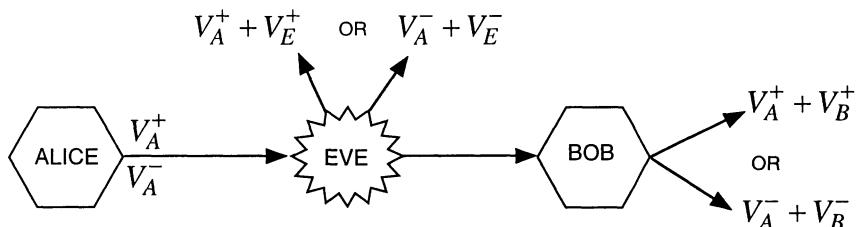


Figure 21.1 Schematic of general set-up. Alice sends information encoded in the amplitude (V_A^+) and phase (V_A^-) spectra. Bob makes measurements of either the amplitude or phase quadrature. Some additional noise is present on his measurements, V_B^\pm . Eve does not know which quadrature Bob will measure thus she needs to be able to extract information about both quadratures from her intercepted material. This leads to strict bound on the allowed values of the additional noise which must appear on her measurements (V_E^\pm)

A more general statement of the generalized uncertainty principle [22] requires that for *any* simultaneous measurements of conjugate quadrature amplitudes

$$V_M^+ V_M^- \geq 1 \quad (21.9)$$

where V_M^\pm are the measurement penalties for the amplitude (+) and phase (-) quadratures, normalized to the amplification gain between the system observables and the measuring apparatus. For example suppose an attempt to measure the amplitude quadrature variance of a system V_k^+ returned the result

$G_1 V_k^+ + G_2 V_m^+$ where V_m^+ represents noise. Then we would have $V_M^+ = (G_2/G_1)V_m^+$. Eq.21.6 follows directly from Eq.21.9 for ideal simultaneous measurements. Let us investigate what general restrictions this places on the information that Eve can intercept and the subsequent corruption of Bob's signal. Firstly Eve's measurements will inevitably carry measurement penalties V_E^\pm constrained by

$$V_E^+ V_E^- \geq 1 \quad (21.10)$$

Now suppose Bob makes an ideal (no noise added) amplitude measurement on the beam he receives. In order to satisfy Eq.21.9 it must be true that the noise penalty carried on the amplitude quadrature of this beam V_B^+ due to Eve's intervention, is sufficiently large such that

$$V_B^+ V_E^- \geq 1 \quad (21.11)$$

Similarly, Bob can also choose to make ideal measurements of the phase quadrature so we must also have

$$V_E^+ V_B^- \geq 1 \quad (21.12)$$

Eqs.21.10,21.11,21.12 set strict quantum mechanical limits on the minimum disturbance Eve can cause to Bob's information given a particular maximum quality of the information she receives. This applies regardless of the method she uses to eavesdrop. Note that quantum memory does not negate the above results provided we insist that Alice and Bob do not exchange any potentially revealing classical information until Alice is sure that Bob has received and measured her signals.

These relations could form the basis of a security analysis of any continuous variable quantum cryptographic scheme in which a single quantum beam is exchanged. However the ramifications of a particular level of disturbance will vary for different schemes. In the following section we will analyse the security of a very simple scheme based on the exchange of a beam in a coherent state.

4. COHERENT STATE QUANTUM CRYPTOGRAPHY

Consider the set up depicted in Fig. 21.2. A possible protocol is as follows. Alice generates two independent random strings of numbers and encodes one on the phase quadrature, and the other on the amplitude quadrature of a bright coherent beam. The amplitude and phase signals are imposed at the same frequency with equal power. Bob uses homodyne detection to detect either the amplitude or phase quadrature of the beam when he receives it. He swaps randomly which quadrature he detects. On a public line Bob then tells Alice at which quadrature he was looking, at any particular time. They pick some

subset of Bob's data to be the test and the rest to be the key. For example, they may pick the amplitude quadrature as the test signal. They would then compare results for the times that Bob was looking at the amplitude quadrature. If Bob's results agreed with what Alice sent, to within some acceptable error rate, they would consider the transmission secure. They would then use the undisclosed phase quadrature signals, sent whilst Bob was observing the phase quadrature, to create their key. By randomly swapping which quadrature is key and which is test throughout the data comparison an increased error rate on either quadrature will immediately be obvious.

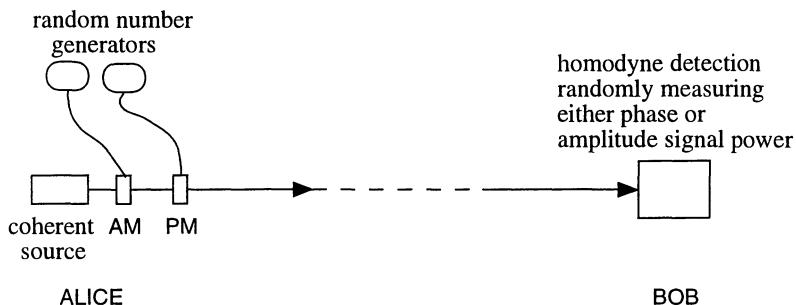


Figure 21.2 Schematic of coherent light cryptographic set-up. AM is an amplitude modulator whilst PM is a phase modulator.

Before making a general analysis of security let us first consider some specific strategies an eavesdropper could adopt. Eve could guess which quadrature Bob is going to measure and measure it herself. She could then reproduce the digital signal of that quadrature and impress it on another coherent beam which she would send on to Bob. She would learn nothing about the other quadrature through her measurement and would have to guess her own random string of numbers to place on it. When Eve guesses the right quadrature to measure Bob and Alice will be none the wiser, however, on average 50% of the time Eve will guess wrong. Then Bob will receive a random string from Eve unrelated to the one sent by Alice. These will agree only 50% of the time. Thus Bob and Alice would see a 25% bit error rate in the test transmission if Eve was using this strategy. This is analogous to the result for single quanta schemes in which this type of strategy is the most readily available. Another single measurement strategy Eve could use is to do homodyne detection at a quadrature angle half-way between phase and amplitude. This fails because the signals become mixed. Thus Eve can tell when both signals are 0 or both are 1 but she cannot tell the difference between 1,0 and 0,1. This again leads to a 25% bit error rate.

However, for bright beams it is possible to make simultaneous measurements of the quadratures, with the caveat that there will be some loss of information. So a second strategy that Eve could follow would be to split the beam in half,

measure both quadratures and impose the information obtained on the respective quadratures of another coherent beam which she sends to Bob. How well will this strategy work? We performed this calculation at the end of section I using Eq.21.7. The halving of signal to noise imposed by the 50:50 beamsplitter means the information Eve intercepts and subsequently passes on to Bob will have an error probability of 5% (for the particular case of bandwidth limited binary pulse code modulation). This is clearly a superior strategy and would be less easily detected. Further more Eve could adopt a third strategy of only intercepting a small amount of the beam and doing simultaneous detection on it. For example, by intercepting 16% of the beam, Eve could gain information about both quadratures with an error rate of 25% whilst Bob and Alice would observe only a small increase of their error rate to 1.7%. In other words Eve could obtain about the same amount of information about the key that she could obtain using the “guessing” strategy, whilst being more difficult to detect.

Now let us analyze this coherent state scheme using Eqs.21.10,21.11,21.12. We choose to couch our evaluation in terms of bit error rates because they represent an unambiguous, directly observable measure of the extent to which Eve can intercept information and the resulting corruption of Bob’s information. This connection will be developed in Section IV. Depending on the particular technique Eve uses Bob and Alice may be able to gain additional evidence for Eve’s presence by making a more detailed comparison of the sent and received signals. This can only increase the security of the system. By considering a general limit on error rates we can find a minimum guaranteed security against eavesdropping regardless of the technique Eve employs.

The signal transfer coefficients for Bob and Eve will be given by

$$\begin{aligned}
 T_E^+ &= \frac{(S/N)_{eve}^+}{(S/N)_{in}^+} = \frac{V_{in}^+}{V_{in}^+ + V_E^+} \\
 T_E^- &= \frac{(S/N)_{eve}^-}{(S/N)_{in}^-} = \frac{V_{in}^-}{V_{in}^- + V_E^-} \\
 T_B^+ &= \frac{(S/N)_{bob}^+}{(S/N)_{in}^+} = \frac{V_{in}^+}{V_{in}^+ + V_B^+} \\
 T_B^- &= \frac{(S/N)_{bob}^-}{(S/N)_{in}^-} = \frac{V_{in}^-}{V_{in}^- + V_B^-}
 \end{aligned} \tag{21.13}$$

Substituting Eqs.21.13 into Eqs.21.10,21.11,21.12 and using the fact that $V_{in}^\pm = 1$ we find

$$\begin{aligned}
 T_E^+ + T_E^- &\leq 1 \\
 T_E^+ + T_B^- &\leq 1 \\
 T_B^+ + T_E^- &\leq 1
 \end{aligned} \tag{21.14}$$

Eqs.21.14 clearly show that any attempt by Eve to get a good signal to noise on one quadrature (e.g. $T_E^+ \rightarrow 1$) results not only in a poor signal to noise in her information of the other quadrature (e.g. $T_E^- \rightarrow 0$) but also a poor signal to noise for Bob on that quadrature (e.g. $T_B^- \rightarrow 0$), making her presence obvious. This is the general limit of the guessing strategy presented in the last section and leads to the same error rates.

Because of the symmetry of Bob's readout technique Eve's best approach is a symmetric attack on both quadratures. Eqs.21.14 then reduces to two equations

$$\begin{aligned} 2T_E^\pm &\leq 1 \\ T_E^\pm + T_B^\pm &\leq 1 \end{aligned} \quad (21.15)$$

If Eve extracts her maximum allowable signal to noise transfer, $T_E^\pm = 0.5$, then ideally Bob suffers the same penalty $T_B^\pm = 0.5$. This is the general limit of the second strategy of the previous section. The same reduction in Bob's signal to noise occurs as in the specific implementation thus this implementation can be identified as an optimum eavesdropper strategy for obtaining maximum simultaneous information about both quadratures.

Eve's best strategy is to intercept only as much information as she can without being detected. The system will be secure if that level of information can be made negligible. Suppose, as in the last section, Eve only intercepts a signal transfer of $T_E^\pm = .08$. From Eq.21.15 this means Bob can receive at most a signal transfer of $T_B^\pm = .92$. This is greater than the result for the specific implementation discussed in the last section, thus that implementation is not an optimum eavesdropper strategy. Using the optimum eavesdropper strategy the error rates for the specific encoding scheme discussed in the last section will be: if Eve intercepts information with an error probability of 25%, then the minimum error rate in Bob's information will be 1.4%.

In Fig. 21.3 we represent the general situation by plotting the minimum error rate Bob and Alice can observe against the error rate in Eve's intercepted information using Eq.21.7 and 21.15. An error rate of 50% (i.e. completely random) represents no information about the data. Two traces are shown, representing different initial signal to noises in Alice's data. This graph shows that in principle any incursion by Eve will result in some increase in Bob and Alice's error rate. However one could also argue that any finite resolution in Bob and Alice's determination of their error rate will allow Eve to do better than the random result. In order to assess whether this system can be made secure we need to introduce the concepts of mutual information and privacy amplification.

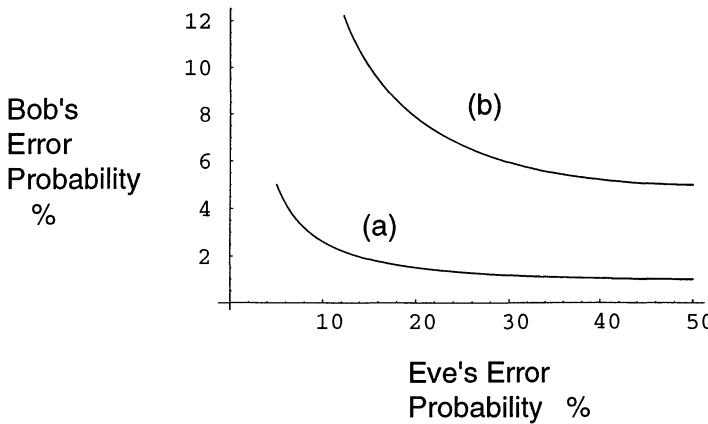


Figure 21.3 Minimum allowable error probabilities in the data of Bob and Eve are plotted for two signal to noise levels of Alice's beam. Trace (a) is for a signal to noise of 13dB whilst trace (b) is for a signal to noise of 10dB.

5. MUTUAL INFORMATION AND PRIVACY AMPLIFICATION

The mutual information of party 1 and party 2 is the information overlap between the data possessed by the two parties. The binary entropy of party 1's data, x , is given by

$$H(x) = -p_x \log_2 p_x - (1 - p_x) \log_2 (1 - p_x) \quad (21.16)$$

where p_x and $1 - p_x$ are the probabilities of the two outcomes. Similarly party 2's data, y , has binary entropy

$$H(y) = -p_y \log_2 p_y - (1 - p_y) \log_2 (1 - p_y) \quad (21.17)$$

The joint entropy of the two data strings is then given by

$$H(x, y) = -\sum_{x,y} p_{x,y} \log_2 p_{x,y} \quad (21.18)$$

with $p_{x,y}$ the joint probabilities. The mutual information is defined

$$H(x : y) = H(x) + H(y) - H(x, y) \quad (21.19)$$

If the two data strings x and y are random then $H(x) = H(y) = 1$. Suppose the error probability between the data strings is \mathcal{B} , then the joint probabilities are given by $p_{0,0} = p_{1,1} = 1 - \mathcal{B}$ and $p_{0,1} = p_{1,0} = \mathcal{B}$. Thus we find

$$H(x : y) = 1 + \mathcal{B} \log_2 \mathcal{B} + (1 - \mathcal{B}) \log_2 (1 - \mathcal{B}) \quad (21.20)$$

Suppose A is Alice's data string, B is Bob's data string and E is Eve's data string. Maurer has shown [24] that provided $H(A : B) > H(A : E)$ then it is in principle possible for Alice and Bob to extract a secret key from the data. Eve's mutual information with this secret key can be made arbitrarily small. From Eq.21.20 we see that this condition will be satisfied provided Bob's error rate is less than Eve's. From Fig. 21.3 we see that provided Alice and Bob's error rate does not exceed 5% for case (a) or 12% for case (b) then secret key generation is in principle possible. In the following we will look at a simple specific example of a secret key generation protocol and evaluate its efficiency.

Because of the transmission errors (and possibly the actions of Eve) Alice and Bob won't share the same data string. However techniques exist for data reconciliation which allow Alice and Bob to select with high probability a subset of their data which is error free, whilst giving Eve minimal extra knowledge. As a simple example Alice and Bob could perform a parity check on randomly chosen pairs of bits. If the error rate between Bob and Alice is low then the probability of both bits being wrong is very low. Thus discarding all pairs which fail the parity check will lead to a big reduction in errors in the shared data whilst not revealing the values of the individual bits to Eve. A series of parity checks will lead with high probability to zero errors. Eve can also remove the pairs that Bob removes and in a worse case scenario may remove up to the same number of errors as Bob. But if Eve initially had significantly more errors than Bob then she will still have significant errors after the reconciliation, whilst Bob and Alice will have virtually none. The data string length will be reduced by a factor of approximately $1 - 2\mathcal{B}_B$, where \mathcal{B}_B is Bob's error probability.

In order to reduce Eve's mutual information to a negligible amount the technique of privacy amplification is employed [25]. This involves the random hashing or block coding of the reconciled key into a shorter key. As a simple example Alice and Bob could randomly pick data strings of length n from the reconciled key and form a new key from the sum, modulo 2, of each n unit block. It is important that the privacy amplification is "orthogonal" to the reconciliation protocol. That is none of the pairs used in the parity checks should appear together in the privacy amplification blocks. The length of the new key will be reduced by a factor of $1/n$. The error probability in the new key will be given by

$$\mathcal{B}_{pa} = \sum_{k=0}^{n/2} \frac{n!}{(2k)!(n-2k)!} (1-\mathcal{B})^{n-2k} \mathcal{B}^{2k} \quad (21.21)$$

where \mathcal{B} is the error probability of the original string. If $\mathcal{B} \approx 0$, as for Bob and Alice, then this process introduces virtually no errors. But when Eve copies this process her errors will be "amplified", hopefully to the point where her mutual information is negligible. Some caution is required in evaluating Eve's mutual information now. Just as Bob and Alice were able to select a sub-set

of results they knew were correct in the reconciliation process, so Eve can also obtain a (smaller) subset of results for which she has greater confidence. We make the worst case assumption that after privacy amplification Eve is left with some small probability, p_r , of possessing certain bits that she knows are right, and a large probability, $1 - p_r$, of possessing bits which are completely random. In such a situation it is appropriate to set Eve's mutual information as

$$H(A : E) = p_r = 1 - 2\mathcal{B}_{pae} \quad (21.22)$$

where \mathcal{B}_{pae} is Eve's average error probability, as given by Eq.21.21.

Let us now apply these techniques to the continuous variable protocol of the previous section to evaluate its security. After Bob has received all the data from Alice he tells her at which quadrature he was looking at any particular time and Alice sorts out her sent data accordingly. They then compare a randomly chosen sub-section of their data (approximately half) and determine the error rate. For the example in the previous section they expect a base error rate of 1%. Let them reject the data and start again if they detect an error rate of $\geq 2\%$. To be cautious, let us assume that in fact the error rate could have been as high as 2.5%. For sufficiently long data strings there will be negligible probability of this error rate being exceeded in the undisclosed data [26]. From Fig. 21.3 (trace (a)) we can read off that Eve's error rate must be $\geq 10.5\%$. Applying our simple information reconciliation protocol Bob and Alice's error probability can be reduced to virtually zero whilst Eve's error rate is $\geq 8\%$. We now apply privacy amplification. Fig. 21.4 (trace (a)) shows Eve's mutual information as a function of the block length, n . Clearly Eve's mutual information is decreasing exponentially as a function of block length. This is the signature of a secure system. A linear expenditure of resources results in an exponentially small mutual information with Eve. In fact Bob and Alice can do better by using a smaller initial signal strength. If Alice reduces the size of the signal she sends to about half that of the previous example (now with a signal to noise of about 10dB) Bob's base error rate will rise to 5%. They set their error threshold at 6%. To be cautious we assume the error rate could be as high as 6.5%. From Fig. 21.3 (trace (b)) we find that Eve's error rate must be $\geq 26\%$. After reconciliation Eve's error rate must still be $\geq 19.5\%$. Fig. 21.4 (trace(b)) plots Eve's mutual information as a function of the block length for this situation showing a more rapid decay. This is approximately the optimum signal strength. However Alice and Bob may also seek to improve the efficiency of the system by employing more sophisticated reconciliation and privacy amplification protocols.

To this point we have assumed that the transmission line between Alice and Bob is lossless. In practice this will not be true. If we make no constraints on Eve's technical abilities then we must assume that all lost light has fallen into her hands [27]. Thus we must calculate Eve's potential mutual information

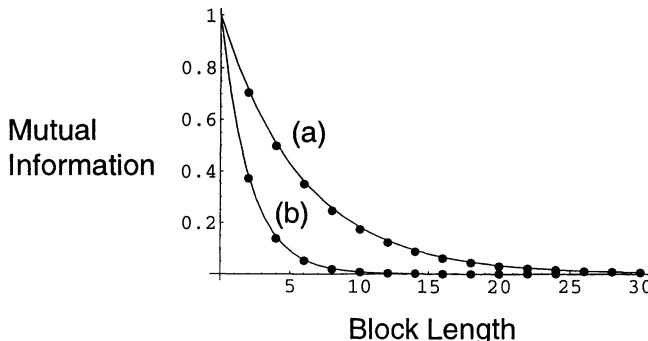


Figure 21.4 Decay of Eve mutual information as a function of the block length, n , in Alice and Bob's privacy amplification protocol is plotted for two signal to noise levels of Alice's beam. Trace (a) is for a signal to noise of 13dB whilst trace (b) is for a signal to noise of 10dB. The solid traces are exponential fits.

from Bob's error rate as if there was no loss, but we must set our error threshold quite high because the losses will drive up Bob's errors. In this simple approach it is clear that loss of 50% or more can not be tolerated because Eve's and Bob's error rates become equal at this point. Indeed as losses approach 50% the expenditure of resources by Bob and Alice needed to reconcile and privacy amplify will increase rapidly.

Let us estimate by what factor the length of the final secure key would be reduced over the length of the original string sent by Alice in a system with 25% loss. Consider an original signal to noise of about 10dB, leading to a base error rate with 25% loss of 7.7%. Setting as before our maximum error rate 1.5% above the base rate at 9.3% we can bound Eve's error rate at $\geq 16.3\%$. Bob and Alice sacrifice half their data in this step. Reconciliation will reduce Bob and Alice's data string by a factor of 0.81 and leave Eve with an error rate $\geq 7\%$. If we require that Eve's mutual information be ≤ 0.001 for the transmission to be considered secure then we find a block length of $n = 46$ is required in the privacy amplification step. Thus the secure key will be reduced by a factor of $0.5 \times 0.81 \times 0.02 = 0.01$. (A similar estimate for the optimum no loss case gives a reduction factor of 0.025) Data transmission via rf signals is a mature technology and bit transmission rates of 100 MHz would seem quite reasonable. Thus secure key transmission rates of a MHz would seem practical under these conditions. This is about three orders of magnitude better than what is presently achievable with single photon schemes. On the other hand single quanta schemes can tolerate much higher losses [4].

The loss problem can be circumvented by using postselection techniques [28] or reverse reconciliation [29]. Both these techniques exploit the asymmetry in the correlations between Eve and Alice's data and Eve and Bob's data, ie

the fact that $H(B : E) < H(A : E)$. Using these techniques there is no in principle loss bound, just as in the discrete case.

6. SQUEEZED STATE QUANTUM CRYPTOGRAPHY

The preceding discussion has shown that a cryptographic scheme based on coherent light can produce secure keys with an efficiency of at least $1/40 \rightarrow 1/100$. We now consider whether squeezed light can offer improved efficiency.

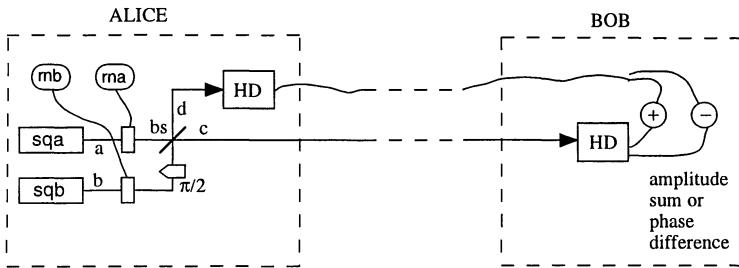


Figure 21.5 Schematic of squeezed light cryptographic set-up. Sqza and sqzb are phase locked squeezed light sources. Rna and Rnb are independent random number sources. Bs and pbs are non-polarizing and polarizing beamsplitters respectively. Half-wave plates to rotate the polarizations are indicated by $\lambda/2$ and optical amplification by A . The $\pi/2$ phase shift is also indicated. HD stands for homodyne detection system.

The set-up is shown in Fig. 21.5. Once again Alice encodes her number strings digitally, but now she impresses them on the amplitude quadratures of two, phase locked, amplitude squeezed beams, a and b , one on each. A $\pi/2$ phase shift is imposed on beam b and then they are mixed on a 50:50 beamsplitter. The resulting output modes, c and d , are given by

$$\begin{aligned} c &= \sqrt{\frac{1}{2}}(a + ib) \\ d &= \sqrt{\frac{1}{2}}(a - ib) \end{aligned} \quad (21.23)$$

These beams are now in an entangled state which will exhibit Einstein, Podolsky, Rosen (EPR) type correlations [30, 32]. Negligible information about the signals can be extracted from the beams individually because the large fluctuations of the anti-squeezed quadratures are now mixed with the signal carrying squeezed quadratures. One of the beams, say c , is transmitted to Bob. The other beam, d , Alice retains and uses homodyne detection to measure either its amplitude or phase fluctuations, with respect to a local oscillator in phase with the original beams a and b . She randomly swaps which quadrature she measures, and stores the results. Bob, upon receiving beam c , also randomly

chooses to measure either its amplitude or phase quadrature and stores his results. After the transmission is complete Alice sends the results of her measurements on beam d to Bob on an open channel. About half the time Alice will have measured a different quadrature to Bob in a particular time window. Bob discards these results. The rest of the data corresponds to times when they both measured the same quadratures. If they both measured the amplitude quadratures of each beam Bob adds them together, in which case he can obtain the power spectrum

$$\begin{aligned} V^+ &= \langle |(\tilde{c}^\dagger + \tilde{c}) + (\tilde{d}^\dagger + \tilde{d})|^2 \rangle \\ &= V_{s,a} + V_{n,a}^+ \end{aligned} \quad (21.24)$$

where the tilde indicate Fourier transforms. Thus he obtains the data string impressed on beam a , $V_{s,a}$, imposed on the sub-QNL noise floor of beam a , $V_{n,a}^+$. Alternatively if they both measured the phase quadratures of each beam, Bob subtracts them, in which case he can obtain the power spectrum

$$\begin{aligned} V^- &= \langle |(\tilde{c}^\dagger - \tilde{c}) - (\tilde{d}^\dagger - \tilde{d})|^2 \rangle \\ &= V_{s,b} + V_{n,b}^+ \end{aligned} \quad (21.25)$$

i.e. he obtains the data string impressed on beam b , $V_{s,b}$, imposed on the sub-QNL noise floor of beam b , $V_{n,b}^+$. Thus the signals lie on conjugate quadratures but *both* have sub-QNL noise floors. This is the hallmark of the EPR correlation [33]. As for the coherent state case Alice and Bob now compare some sub-set of their shared data and check for errors. If the error rate is sufficiently low they deem their transmission secure and use reconciliation and privacy amplification on the undisclosed sub-set of their data to produce a secure key.

Consider now eavesdropper strategies. Eve must intercept beam c if she is to extract any useful information about the signals from the classical channel (containing Alice's measurements of beam d) sent later. She can adopt the guessing strategy by detecting a particular quadrature of beam c and then using a similar apparatus to Alice's to re-send the beam and a corresponding classical channel later. As before she will only guess correctly what Bob will measure half the time thus introducing a BER of 25%. Instead she may try simultaneous detection of both quadratures of beam c . As in the coherent case the noise she introduces into her own measurement (V_E^\pm) and that she introduces into Bob's (V_B^\pm) are in general limited according to Eqs. 21.10, 21.11 and 21.12. However now the consequences of these noise limits on the signal to noise transfers that Eve and Bob can obtain behave quite differently because the signals they are trying to extract lie on sub-QNL backgrounds. The maximum signal transfer

coefficients that Eve can extract are given by

$$\begin{aligned} T_E^+ &= \frac{(V_E^+ + 2V_{n,b}^-)V_{n,a}^+}{2V_{n,a}^+V_{n,b}^- + V_E^+(V_{n,a}^+ + V_{n,b}^-)} \\ T_E^- &= \frac{(V_E^- + 2V_{n,a}^-)V_{n,b}^+}{2V_{n,b}^+V_{n,a}^- + V_E^-(V_{n,b}^+ + V_{n,a}^-)} \end{aligned} \quad (21.26)$$

Similarly Bob's are

$$\begin{aligned} T_B^+ &= \frac{(V_B^+ + 2V_{n,b}^-)V_{n,a}^+}{2V_{n,a}^+V_{n,b}^- + V_B^+(V_{n,a}^+ + V_{n,b}^-)} \\ T_B^- &= \frac{(V_B^- + 2V_{n,a}^-)V_{n,b}^+}{2V_{n,b}^+V_{n,a}^- + V_B^-(V_{n,b}^+ + V_{n,a}^-)} \end{aligned} \quad (21.27)$$

To achieve maximum security we require that the anti-squeezed quadratures of the beams have large excess noise. This could easily be arranged experimentally. The maximum signal transfer coefficients (Eq.21.26 and Eq.21.27) then reduce to

$$\begin{aligned} T_E^+ &= \frac{V_{n,a}^+}{V_{n,a}^+ + 0.5V_E^+} \\ T_E^- &= \frac{V_{n,b}^+}{V_{n,b}^+ + 0.5V_E^-} \end{aligned} \quad (21.28)$$

and similarly Bob's are

$$\begin{aligned} T_B^+ &= \frac{V_{n,a}^+}{V_{n,a}^+ + 0.5V_B^+} \\ T_B^- &= \frac{V_{n,b}^+}{V_{n,b}^+ + 0.5V_B^-} \end{aligned} \quad (21.29)$$

For the squeezed noise floors the same ($V_{n,a}^+ = V_{n,b}^+ = V_n$) we find the signal transfers are restricted via

$$4V_n^2\left(\frac{1}{T_E^+} - 1\right)\left(\frac{1}{T_E^-} - 1\right) \geq 1 \quad (21.30)$$

$$4V_n^2\left(\frac{1}{T_E^+} - 1\right)\left(\frac{1}{T_B^-} - 1\right) \geq 1 \quad (21.31)$$

$$4V_n^2 \left(\frac{1}{T_B^+} - 1 \right) \left(\frac{1}{T_E^-} - 1 \right) \geq 1 \quad (21.32)$$

It is straightforward to show that a symmetric attack on both quadratures is Eve's best strategy as it leads to a minimum disturbance in both her and Bob's measurements. Using this symmetry to simplify Eq.21.30 leads to the following general restriction on the signal transfer Eve can obtain:

$$T_E^\pm \leq \frac{2V_n}{2V_n + 1} \quad (21.33)$$

Once the squeezing exceeds 3 dB ($V_n = 0.5$) the signal to noise that Eve can obtain simultaneously is reduced below that for the coherent state scheme. In the limit of very strong squeezing ($V_n \rightarrow 0$) Eve can extract virtually no information simultaneously. Similarly Bob's signal transfer is restricted according to:

$$\frac{T_E^\pm T_B^\pm}{(1 - T_E^\pm)(1 - T_B^\pm)} \leq 4V_n \quad (21.34)$$

If squeezing is strong then almost any level of interception by Eve will result in very poor signal transfer to Bob. In Fig. 21.6 we show plots of error rates of Bob versus minimum error rates of Eve for various levels of squeezing. In comparison with the coherent scheme (Fig. 21.3) it can be seen that larger disturbances are caused in Bob's information for the same quality of Eve's interception. As a numerical example consider the specific encoding scheme of section I and suppose the squeezing is 10 dB ($V_n = 0.1$). Assuming no loss and using the same assumptions as those used to evaluate the coherent scheme in the last section we find that a secure key of length 0.07 times the original data string length can be generated. That is an efficiency of about 1/14, to be compared to the coherent case of 1/40, a clear improvement.

As for the coherent scheme losses of 50% or more cannot be tolerated in this simple approach however the more sophisticated protocols mentioned in the coherent state context can also be implemented with squeezing to achieve high loss operation.

7. TELEPORTATION AS AN OPTIMUM EAVESDROPPER STRATEGY

It is interesting to consider what physical techniques Eve could use to realize the optimal attack strategy we have assumed her capable of throughout this discussion. Firstly she would need to replace the lossy transmission line that Bob and Alice are using with her own transmission line of negligible loss. Given that Bob and Alice will presumably employ the most efficient transmission line

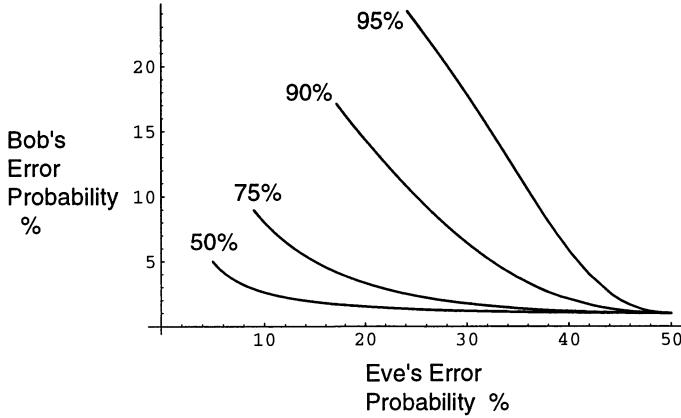


Figure 21.6 Minimum allowable error probabilities in the data of Bob and Eve are plotted for various levels of squeezing.

they can obtain, Eve's job is not trivial. A conceptually simple strategy for Eve is a completely passive intervention; also known as the beamsplitter attack [14]. That is she takes only the lost light. This she holds in "quantum memory" until Bob has revealed the bases in which his measurements were made. At this point she then measures her held portion of the beam in the relevant bases. In the presence of transmission efficiency η Bob's noise penalty will be

$$V_B^\pm = \frac{1 - \eta}{\eta} \quad (21.35)$$

whilst if Eve obtains all the lost light she will have a noise penalty

$$V_E^\pm = \frac{\eta}{1 - \eta} \quad (21.36)$$

thus saturating the inequalities of Eq.21.11 and 21.12.

In a low loss situation Eve needs to make an active interception of the beam. An optimum technique in this situation is for Eve to make an optimal clone of the beam which she again holds in quantum memory until Bob reveals his bases. This technique also saturates the inequalities of Eq.21.11 and 21.12 [13].

The above technique requires quantum memory. Eve can also use continuous variable teleportation [35, 36, 37] in the following way as an optimum eavesdropper strategy without requiring quantum memory.

Quantum teleportation uses shared entanglement to convert quantum information into classical information and then back again (see Fig. 21.6). In particular continuous variable teleportation uses 2-mode squeezed light as its

entanglement resource. In the limit of very strong squeezing no information about the teleported system can be extracted from the classical channel but a perfect reproduction of the quantum system can be retrieved. On the other hand with lower levels of squeezing some information about the system can be obtained from the the classical channel but at the expense of a less than perfect reproduction. We show in the following that under particular operating conditions the disturbance in the teleported state is precisely the minimum required by the generalized uncertainty principle, given the quality of information that can be extracted from the classical channel. Teleportation thus constitutes an optimum eavesdropper strategy.

Eve's strategy would be to send the field she intercepts from Alice through a teleporter, adjusted such that she can read some information out of the classical channel, but still reconstruct the field sufficiently well such that Bob and Alice don't see a large error rate. The classical channel of a lossless continuous variable teleporter can be written [11, 32]

$$\begin{aligned} F_c &= K(\hat{f}_{in} + \hat{j}_1^\dagger) \\ &= K(\hat{f}_{in} + \sqrt{G}\hat{v}_1^\dagger + \sqrt{G-1}\hat{v}_2) \end{aligned} \quad (21.37)$$

where \hat{f}_{in} is the annihilation operator of the input to the teleporter and $\hat{j}_1 = \sqrt{G}\hat{v}_1 + \sqrt{G-1}\hat{v}_2^\dagger$ is the annihilation operator for one of the entangled beams. The \hat{v}_i are the vacuum mode inputs to the squeezers, G is the parametric gain of the squeezers and $K \gg 1$ is the measurement amplification factor. Being a classical channel simultaneous measurements of both quadratures can be made without additional penalty thus immediately Eve's measurement penalty is

$$V_E^\pm = 2G - 1 \quad (21.38)$$

For no squeezing ($G = 1$) $V_E^\pm = 1$, the minimum possible for simultaneous detection of both quadratures (see Eq.21.10). For large squeezing ($G \gg 1$) V_E^\pm become very large and Eve can obtain little information from the classical channel.

The output of the teleporter is given by

$$\begin{aligned} \hat{f}_{out} &= \lambda\hat{f}_{in} + \hat{j}_1^\dagger - \hat{j}_2 \\ &= \lambda\hat{f}_{in} + (\lambda\sqrt{G} - \sqrt{G-1})\hat{v}_1^\dagger + (\sqrt{G} - \lambda\sqrt{G-1})\hat{v}_2 \end{aligned} \quad (21.39)$$

where λ is the gain of the teleporter and $\hat{j}_2 = \sqrt{G}\hat{v}_2 + \sqrt{G-1}\hat{v}_1^\dagger$ is the annihilation operator for the other entangled beam. Thus Bob's measurement penalty for ideal measurements of either of the quadratures is

$$V_B^\pm = \frac{(\lambda\sqrt{G} - \sqrt{G-1})^2 + (\sqrt{G} - \lambda\sqrt{G-1})^2}{\lambda^2} \quad (21.40)$$

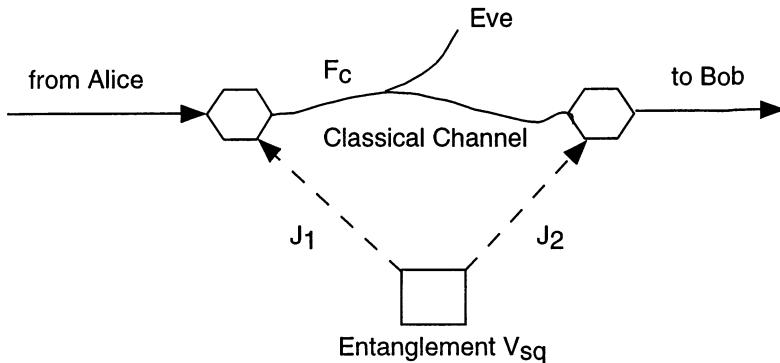


Figure 21.7 Schematic of teleportation being used as an optimum eavesdropper strategy.

If Eve operates the teleporter with gain [38]

$$\lambda_{opt} = \frac{1 + V_{sq}^2}{1 - V_{sq}^2} \quad (21.41)$$

where $V_{sq} = (\sqrt{G} - \sqrt{G - 1})^2$, then Bob's noise penalty is

$$V_B^\pm(\lambda_{opt}) = \frac{1}{2G - 1} \quad (21.42)$$

and so Eve causes the minimum allowable disturbance, i.e. $V_E^\pm V_B^\pm = 1$.

8. CONCLUSION

In this chapter we have investigated continuous variable quantum cryptography as it could be realized in optics by analysing the security and efficiency of specific implementations of two systems based on coherent and squeezed state light respectively. An Eve employing an optimal eavesdropper attack is assumed throughout. Possible optimal attack strategies that Eve could employ are outlined.

We find that the coherent scheme can be made secure, but is not very efficient. None-the-less, given the maturity of optical communication technology based on rf modulation, this system may prove competitive with discrete schemes.

The squeezed state scheme can also be made secure and in principle is more efficient than the coherent state system.

We have looked at simple protocols throughout this analysis which we hope clearly illustrate the basic principles. However we have noted that more sophisticated encoding, reconciliation and privacy amplification techniques would lead to significant improvements in performance.

Acknowledgements

We thank Michael Nielsen, Christine Silberhorn and Philippe Grangier for useful discussions. This work was supported by the Australian Research Council.

References

- [1] S. Wiesner, *Sigact News*, **15**, 78 (1983), C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore), 175 (1984).
- [2] C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).
- [3] A. K. Ekart, *Phys. Rev. Lett.* **67**, 661 (1991).
- [4] W. T. Buttler et al, *Phys. Rev. A* **57**, 2379 (1998).
- [5] H. Zbinden et al, *Appl.Phys.B* **67**, 743 (1998).
- [6] Y. Mu et al, *Opt.Comm.* **123**, 344 (1996).
- [7] T. C. Ralph, *Phys. Rev. A* **61** 010303(R) (1999).
- [8] M. Hillery, *Phys. Rev. A* **61** 022309 (2000).
- [9] M. D. Reid, *Phys. Rev. A* **62** 062308 (2000).
- [10] Ch .Silberhorn, N .Korolkova and G .Leuchs, *Phys. Rev. Lett.* **88**, 167902 (2002).
- [11] T. C. Ralph, *Phys. Rev. A* **62** 062306 (2000).
- [12] D. Gottesman and J. Preskill, *Phys. Rev. A* **63**, 022309 (2001).
- [13] N. J. Cerf, M. Levy, G. Van Assche, *Phys. Rev. A* **63**, 052311 (2001).
- [14] F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88** 057902 (2002).
- [15] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, Berlin, 1994).
- [16] C. A. Fuchs and A. Peres, *Phys. Rev. A* **53**, 2038 (1996), C. A. Fuchs, N. Gisin, R. B. Griffiths, C. -S. Niu and A. Peres, *Phys. Rev. A* **56**, 1163 (1997), I. Cirac and N. Gisin, *Phys.Lett.A* **229**, 1 (1997).
- [17] D. Mayers, *Advances in Cryptology*, Proceedings of Crypto '96, 343 (Springer-Verlag, 1996).
- [18] H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
- [19] We only explicitly consider individual eavesdropper attacks here.
- [20] C. E. Shannon, *Bell System Tech. J.* **27**, 623 (1948).
- [21] Y. Yamamoto and H. A. Haus, *Rev.Mod.Phys.*, **58**, 1001 (1986).
- [22] E. Arthurs and M. S. Goodman, *Phys. Rev. Lett.* **60**, 2447 (1988).

- [23] A. Yariv, *Optical Electronics in Modern Communications* (Oxford University Press, 5th Edition, New York 1997).
- [24] U. M. Maurer, IEEE Trans.Inf.Theo. **39**, 1733 (1993).
- [25] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer, IEEE Trans.Inf.Theo. **41**, 1915 (1995).
- [26] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge 2000).
- [27] This is a stronger assumption about Eve's capabilities than was used in assessing the effect of losses in Ref.[10].
- [28] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, G. Leuchs, quant-ph/0204064 (2002).
- [29] F. Grosshans, P. Grangier, quant-ph/0204127 (2002).
- [30] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
- [31] G. Yeoman and S. M. Barnett, Journal Mod. Opt. **40**, 1497 (1993).
- [32] T. C. Ralph and P. K. Lam, Phys. Rev. Lett.**81**, 5668 (1998).
- [33] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett.**68**, 3663 (1992).
- [34] S. M. Barnett and S. J. D. Phoenix, Phil.Trans.R.Soc.Lond.A **354**, 793 (1996).
- [35] L. Vaidman, Phys. Rev. A**49**, 1473 (1994).
- [36] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett.**80**, 869 (1998).
- [37] A Furusawa, J L Sorensen, S L Braunstein, C A Fuchs, H J Kimble and E S Polzik, Science, **282**, 706 (1998).
- [38] The gain condition λ_{opt} corresponds to the point of maximum signal transfer on the T-V graph of Reference [32]

Chapter 22

SECURE QUANTUM KEY DISTRIBUTION USING SQUEEZED STATES

Daniel Gottesman

EECS: Computer Science Div., University of California, Berkeley, CA 94720, USA
gottesma@eecs.berkeley.edu

John Preskill

California Institute of Technology, Pasadena, CA 91125, USA
preskill@theory.caltech.edu

Abstract We prove the security of a quantum key distribution scheme based on transmission of squeezed quantum states of a harmonic oscillator. Our proof employs quantum error-correcting codes that encode a finite-dimensional quantum system in the infinite-dimensional Hilbert space of an oscillator, and protect against errors that shift the canonical variables p and q . If the noise in the quantum channel is weak, squeezing signal states by 2.51 dB (a squeeze factor $e^r = 1.34$) is sufficient in principle to ensure the security of a protocol that is suitably enhanced by classical error correction and privacy amplification. Secure key distribution can be achieved over distances comparable to the attenuation length of the quantum channel.

1. INTRODUCTION

Two of the most important ideas to emerge from recent studies of quantum information are the concepts of quantum error correction and quantum key distribution. Quantum error correction allows us to protect unknown quantum states from the ravages of the environment. Quantum key distribution allows us to conceal our private discourse from potential eavesdroppers.

In fact these two concepts are more closely related than is commonly appreciated. A quantum error correction protocol must be able to reverse the effects of both bit flip errors, which reflect the polarization state of a qubit about the x -axis, and phase errors, which reflect the polarization about the z -axis. By

reversing both types of errors, the protocol removes any entanglement between the protected state and the environment, thus restoring the purity of the state.

In a quantum key distribution protocol, two communicating parties verify that qubits polarized along both the x -axis and the z -axis can be transmitted with an acceptably small probability of error. An eavesdropper who monitors the x -polarized qubits would necessarily disturb the z -polarized qubits, while an eavesdropper who monitors the z -polarized qubits would necessarily disturb the x -polarized qubits. Therefore, a successful verification test can show that the communication is reasonably private, and the privacy can then be amplified via classical protocols.

In quantum key distribution, the eavesdropper collects information by entangling her probe with the transmitted qubits. Thus both error correction and key distribution share the goal of protecting quantum states against entanglement with the outside world.

Recently, this analogy between quantum error correction and quantum key distribution has been sharpened into a precise connection, and used as the basis of a new proof of security against all possible eavesdropping strategies [18]. Earlier proofs of security (first by Mayers [13, 14], and later by Biham *et al.* [3]) made no explicit reference to quantum error correction; nevertheless, the connection between quantum error correction and quantum key distribution is a powerful tool, enabling us to invoke the sophisticated formalism of quantum error-correcting codes in an analysis of the security of quantum key distribution protocols.

Also recently, new quantum error-correcting codes have been proposed that encode a finite-dimensional quantum system in the infinite-dimensional Hilbert space of a quantum system described by continuous variables [8]. In this paper, we will apply these new codes to the analysis of the security of quantum key distribution protocols. By this method, we prove the security of a protocol that is based on the transmission of squeezed quantum states of an oscillator. The protocol is secure against all eavesdropping strategies allowed by the principles of quantum mechanics.

In our protocol, the sending party, Alice, chooses at random to send either a state with a well defined position q or momentum p . Then Alice chooses a value of q or p by sampling a probability distribution, prepares a narrow wave packet centered at that value, and sends the wave packet to the receiving party, Bob. Bob decides at random to measure either q or p . Through public discussion, Alice and Bob discard their data for the cases in which Bob measured in a different basis than Alice used for her preparation, and retain the rest. To correct for possible errors, which could be due to eavesdropping, to noise in the channel, or to intrinsic imperfections in Alice's preparation and Bob's measurement, Alice and Bob apply a classical error correction and privacy

amplification scheme, extracting from the raw data for n oscillators a number $k < n$ of key bits.

Alice and Bob also sacrifice some of their data to perform a verification test to detect potential eavesdroppers. When verification succeeds, the probability is exponentially small in n that any eavesdropper has more than an exponentially small amount of information about the key. Intuitively, this protocol is secure because an eavesdropper who monitors the observable q necessarily causes a detectable disturbance of the complementary observable p (and vice versa).

Since preparing squeezed states is technically challenging, it is important to know how much squeezing is needed to ensure the security of the protocol. The answer depends on how heavily the wave packets are damaged during transmission. When the noise in the channel is weak, we show that it suffices in principle for the squeezed state to have a width smaller by the factor $e^{-r} = .749$ than the natural width of a coherent state (corresponding to an improvement by 2.51 dB in the noise power for the squeezed observable, relative to vacuum noise). It is also important to know that security can be maintained under realistic assumptions about the noise and loss in the channel. Our proof of security applies if the protocol is imperfectly implemented, and shows that secure key distribution can be achieved over distances comparable to the attenuation length of the channel. Squeezed-state key distribution protocols may have some practical advantages over single-qubit protocols, in that neither single-photon sources nor very efficient photodetectors are needed.

Key distribution protocols using continuous variable quantum systems have been described previously by others [16, 9, 17], but ours is the first complete discussion of error correction and privacy amplification, and the first proof of security against arbitrary attacks.

In §2. we review continuous variable quantum error-correcting codes [8] and in §3. we review the argument [18] exploiting quantum error-correcting codes to demonstrate the security of the BB84 quantum key distribution scheme [1]. This argument is extended to apply to continuous variable key distribution schemes in §4. and §5. Estimates of how much squeezing is required to ensure security of the protocol are presented in §6. The effects on security of losses due to photon absorption are analyzed in §7., and §8. contains conclusions.

2. CODES FOR CONTINUOUS QUANTUM VARIABLES

We begin by describing codes for continuous quantum variables [8]. The two-dimensional Hilbert space of an encoded qubit embedded in the infinite-dimensional Hilbert space of a system described by canonical variables q and p (satisfying $[q, p] = i$) can be characterized as the simultaneous eigenspace of

the two commuting operators

$$S_q = e^{i(2\sqrt{\pi})q} , \quad S_p = e^{-i(2\sqrt{\pi})p} , \quad (22.1)$$

the code's "stabilizer generators." If the eigenvalues are $S_q = S_p = 1$, then the allowed values of q and p in the code space are integer multiples of $\sqrt{\pi}$, and the codewords are invariant under shifts in q or p by integer multiples of $2\sqrt{\pi}$. Thus an orthogonal basis for the encoded qubit can be chosen as

$$\begin{aligned} |\bar{0}\rangle &\propto \sum_{s=-\infty}^{\infty} |q = (2s) \cdot \sqrt{\pi}\rangle \\ &\propto \sum_{s=-\infty}^{\infty} |p = s \cdot \sqrt{\pi}\rangle , \\ |\bar{1}\rangle &\propto \sum_{s=-\infty}^{\infty} |q = (2s + 1) \cdot \sqrt{\pi}\rangle \\ &\propto \sum_{s=-\infty}^{\infty} (-1)^s |p = s \cdot \sqrt{\pi}\rangle . \end{aligned} \quad (22.2)$$

The operators

$$\bar{Z} \equiv e^{i(\sqrt{\pi})q} , \quad \bar{X} \equiv e^{-i(\sqrt{\pi})p} , \quad (22.3)$$

commute with the stabilizer generators and so preserve the code subspace; they act on the basis eq. (22.1) according to

$$\begin{aligned} \bar{Z} : \quad |\bar{0}\rangle &\rightarrow |\bar{0}\rangle , \quad |\bar{1}\rangle \rightarrow -|\bar{1}\rangle , \\ \bar{X} : \quad |\bar{0}\rangle &\rightarrow |\bar{1}\rangle , \quad |\bar{1}\rangle \rightarrow |\bar{0}\rangle . \end{aligned} \quad (22.4)$$

This code is designed to protect against errors that induce shifts in the values of q and p . To correct such errors, we measure the values of the stabilizer generators to determine the values of q and p modulo $\sqrt{\pi}$, and then apply a shift transformation to adjust q and p to the nearest integer multiples of $\sqrt{\pi}$. If the errors induce shifts Δq , Δp that satisfy

$$|\Delta q| < \sqrt{\pi}/2 , \quad |\Delta p| < \sqrt{\pi}/2 , \quad (22.5)$$

then the encoded state can be perfectly restored.

A code that protects against shifts is obtained for any choice of the eigenvalues of the stabilizer generators. The code with

$$S_q = e^{2\pi i \phi_q} , \quad S_p = e^{-2\pi i \phi_p} , \quad (22.6)$$

can be obtained from the $\phi_q = \phi_p = 0$ code by applying the phase space translation operator

$$e^{i\sqrt{\pi}(q\phi_p)} e^{-i\sqrt{\pi}(p\phi_q)} ; \quad (22.7)$$

the angular variables ϕ_q and $\phi_p \in (-1/2, 1/2]$ denote the allowed values of $q/\sqrt{\pi}$ and $p/\sqrt{\pi}$ modulo an integer. In this code space, the encoded operations \bar{Z} and \bar{X} (which square to the identity) can be chosen to be

$$\bar{Z}(\phi_q) = e^{i\sqrt{\pi}(q-\phi_q\sqrt{\pi})} , \quad \bar{X}(\phi_p) = e^{-i\sqrt{\pi}(p-\phi_p\sqrt{\pi})} . \quad (22.8)$$

The code with stabilizer eq. (22.1) can be generalized in a variety of ways [8]. For example, we can increase the dimension of the protected code space, and we can modify the code to protect against shifts that are asymmetric in q and in p . If we choose the stabilizer to be

$$\begin{aligned} S_q(n, \alpha) &= \exp \left[i(\sqrt{2\pi d}) \cdot (q/\alpha) \right] , \\ S_p(n, \alpha) &= \exp \left[-i(\sqrt{2\pi d}) \cdot (p\alpha) \right] , \end{aligned} \quad (22.9)$$

where d is a positive integer and α is a positive real number, then the code has dimension d and protects against shifts that satisfy

$$|\Delta q| < \frac{\alpha}{2} \cdot \sqrt{\frac{2\pi}{d}} , \quad |\Delta p| < \frac{1}{2\alpha} \cdot \sqrt{\frac{2\pi}{d}} . \quad (22.10)$$

The codewords eq. (22.1) are nonnormalizable states, infinitely “squeezed” in q and p . In practice, we must always work with normalizable finitely squeezed states. For example, a Gaussian approximation $|\tilde{0}\rangle$ to the ideal codeword $|\bar{0}\rangle$ of the $d = 2, \alpha = 1$ code, characterized by squeezing parameters $\Delta_q, \Delta_p \ll 1$, is

$$\begin{aligned} |\tilde{0}\rangle &\approx \left(\frac{4}{\pi} \right)^{1/4} \int_{-\infty}^{\infty} dq |q\rangle e^{-\frac{1}{2}(\Delta_p^2)q^2} \\ &\times \sum_{s=-\infty}^{\infty} e^{-\frac{1}{2}(q-2s\sqrt{\pi})^2/\Delta_q^2} \\ &\approx \frac{1}{\pi^{1/4}} \int_{-\infty}^{\infty} dp |p\rangle e^{-\frac{1}{2}(\Delta_q^2)p^2} \\ &\times \sum_{s=-\infty}^{\infty} e^{-\frac{1}{2}(p-s\sqrt{\pi})^2/\Delta_p^2} ; \end{aligned} \quad (22.11)$$

the approximate codeword $|\tilde{0}\rangle$ can be obtained by subjecting $|\bar{0}\rangle$ to shifts in q and p governed by Gaussian distributions with widths Δ_q and Δ_p respectively.

If Δ_q and Δ_p are small, then in principle these shifts can be corrected with high probability: e.g., for $\Delta_q = \Delta_p \equiv \Delta$, the probability that a shift in q or p causes an uncorrectable error is no worse than the probability that the size of the shift exceeds $\sqrt{\pi}/2$, or

$$\begin{aligned} \text{Error Prob} &\leq \frac{2}{\sqrt{\pi\Delta^2}} \int_{\sqrt{\pi}/2}^{\infty} dq e^{-q^2/\Delta^2} \\ &\leq \frac{2\Delta}{\pi} \exp(-\pi/4\Delta^2). \end{aligned} \quad (22.12)$$

For the $d = 2$ code with $\alpha \neq 1$, this same estimate of the error probability applies if we rescale the widths appropriately,

$$\Delta_q = \Delta \cdot \alpha, \quad \Delta_p = \Delta/\alpha. \quad (22.13)$$

We can concatenate a shift-resistant code with an $[[n, k, d]]$ stabilizer quantum code. That is, first we encode (say) a qubit in each of n oscillators; then k better protected qubits are embedded in the block of n . If the typical shifts are small, then the qubit error rate will be small in each of the n oscillators, and the error rate in the k protected qubits will be much smaller. The quantum key distribution protocols that we propose are based on such concatenated codes.

We note quantum codes for continuous quantum variables with an *infinite-dimensional* code space were described earlier by Braunstein [5], and by Lloyd and Slotine [11]. Entanglement distillation protocols for continuous variable systems have also been proposed [15, 7].

3. QUANTUM KEY DISTRIBUTION AND QUANTUM ERROR-CORRECTING CODES

Now let's recall the connection between stabilizer quantum codes and quantum key distribution schemes [18].

We say that a protocol for quantum key distribution is secure if (1) the eavesdropper Eve is unable to collect a significant amount of information about the key without being detected, (2) the communicating parties Alice and Bob receive the same key bits with high probability, and (3) the key generated is essentially random. Then if the key is intercepted, Alice and Bob will know it is unsafe to use the key and can make further attempts to establish a secure key. If eavesdropping is not detected, the key can be safely used as a one-time pad for encoding and decoding.¹

Establishing that a protocol is secure is tricky, because there inevitably will be some noise in the quantum channel used to distribute the key, and the effects of eavesdropping could be confused with the effects of the noise. Hence the protocol must incorporate error correction to establish a shared key despite the noise, and privacy amplification to control the amount of information about the key that can be collected by the eavesdropper.

In the case of the BB84 key distribution invented by Bennett and Brassard [1], the necessary error correction and privacy amplification are entirely classical. Nevertheless, the formalism of quantum error correction can be usefully invoked to show that the error correction and privacy amplification work effectively [18]. The key point is that if Alice and Bob carry out the BB84 protocol, we can show that the eavesdropper is no better off than if they had executed a protocol that applies quantum error correction to the transmitted quantum states. Appealing to the observation that Alice and Bob *could have* applied quantum error correction (even though they didn't really apply it), we place limits on what Eve can know about the key.

3.1 ENTANGLEMENT DISTILLATION

First we will describe a key distribution protocol that uses a quantum error-correcting code to purify entanglement, and will explain why the protocol is secure. The connection between quantum error correction and entanglement purification was first emphasized by Bennett *et al.* [2]; our proof of security follows a proof by Lo and Chau [12] for a similar key distribution protocol. Later, following Shor and Preskill [18], we will see how the entanglement-purification protocol is related to the BB84 protocol.

A stabilizer code can be used as the basis of an entanglement-purification protocol with one-way classical communication [2, 12]. Two parties, both equipped with quantum computers, can use this protocol to extract from their initial shared supply of noisy Bell pairs a smaller number of Bell pairs with very high fidelity. These purified Bell pairs can then be employed for EPR quantum key distribution. Because the distilled pairs are very nearly pure, the quantum state of the pairs has negligible entanglement with the quantum state of the probe of any potential eavesdropper; therefore no measurement of the probe can reveal any useful information about the secret key.

Let's examine the distillation protocol in greater detail. Suppose that Alice and Bob start out with n shared EPR pairs. Ideally, these pairs should be in the state

$$|\Phi^{(n)}\rangle \equiv |\phi^+\rangle^{\otimes n}, \quad (22.14)$$

where $|\phi^+\rangle$ is the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$; however, the pairs are noisy, approximating $|\Phi^{(n)}\rangle$ with imperfect fidelity. They wish to extract $k < n$ pairs that are less noisy.

For this purpose, they have agreed in advance to use a particular $[[n, k, d]]$ stabilizer code. The code space can be characterized as a simultaneous eigenspace of a set of mutually commuting stabilizer generators $\{M_i, i = 1, 2, \dots, n-k\}$. Each M_i is a “Pauli operator,” a tensor product of n single-qubit operators where

each single-qubit operator is one of $\{I, X, Y, Z\}$ defined by

$$\begin{aligned} I &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ Y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, & Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \quad (22.15)$$

The operations $\{\bar{X}_a, \bar{Z}_a, a = 1, 2, \dots, k\}$ acting on the encoded qubits are Pauli operators that commute with all of the M_i .

The Bell state $|\phi^+\rangle$ is the simultaneous eigenstate with eigenvalue one of the two commuting operators $X_A \otimes X_B$ and $Z_A \otimes Z_B$ (where subscripts A and B indicate whether the operator acts on Alice's or Bob's qubit). Thus the state $|\Phi^{(n)}\rangle$ is the simultaneous eigenstate with eigenvalue one of the commuting operators

$$\begin{aligned} M_{i,A} \otimes M_{i,B}, &\quad i = 1, 2, \dots, n-k, \\ \bar{X}_{a,A} \otimes \bar{X}_{a,B}, &\quad a = 1, 2, \dots, k, \\ \bar{Z}_{a,A} \otimes \bar{Z}_{a,B}, &\quad a = 1, 2, \dots, k. \end{aligned} \quad (22.16)$$

Now suppose that Alice and Bob both measure the $n - k$ commuting M_i 's. If the state they measure is precisely $|\Phi^{(n)}\rangle$, then Alice and Bob obtain identical measurement outcomes. Furthermore, since their measurements do not disturb the encoded operations \bar{X}_a and \bar{Z}_a , their measurement would prepare the encoded state $|\bar{\Phi}^{(k)}\rangle \equiv |\bar{\phi}^+\rangle^{\otimes k}$, the encoded state with

$$\begin{aligned} \bar{X}_{a,A} \otimes \bar{X}_{a,B} &= \bar{Z}_{a,A} \otimes \bar{Z}_{a,B} = 1, \\ a &= 1, 2, \dots, k, \end{aligned} \quad (22.17)$$

in the code subspace with the specified values of $M_i = \pm 1$.

However, since the initial pairs are noisy, Alice's and Bob's measurement of the M_i 's need not match perfectly; they should apply error correction to improve the fidelity of their encoded pairs. Thus Alice broadcasts the values of the $M_{i,A}$'s that she obtained in her measurements. Comparing to his own measurements, Bob computes the relative syndrome $M_{i,A} \cdot M_{i,B}$. From this relative syndrome, he infers what recovery operation he should apply to his qubits to ensure that the $M_{i,B}$'s match the $M_{i,A}$'s, and he performs this operation. Now Alice and Bob are in possession of k encoded pairs with improved fidelity.

These encoded pairs can be used for EPR key distribution. For each $a = 1, 2, \dots, k$, Alice and Bob measure \bar{Z}_a , obtaining outcomes that are essentially random and agree with high probability. These outcomes are their shared private key.

3.2 VERIFICATION

If the initial pairs are *too* noisy, either because of the intervention of an eavesdropper or for other reasons, then the purification protocol might not succeed. Alice and Bob need to sacrifice some of their EPR pairs to verify that purification is likely to work. If verification fails, they can abort the protocol.

Under what conditions will purification succeed? If their pairs were perfect, each would be in the state $|\phi^+\rangle$, the simultaneous eigenstate with eigenvalue one of the two commuting observables $X \otimes X$ and $Z \otimes Z$. Suppose for a moment, that each of the pairs *is* a simultaneous eigenstate of these observables (a Bell state), but not necessarily with the right eigenvalues: in fact no more than t_X of the n pairs have $X \otimes X = -1$, and no more than t_Z of the n pairs have $Z \otimes Z = -1$. Then, if Alice and Bob use a stabilizer code that can correct up to t_Z bit flip errors and up to t_X phase errors, the purification protocol will work perfectly — it will yield the encoded state $|\bar{\Phi}^{(k)}\rangle = |\bar{\phi}^+\rangle^{\otimes k}$ with fidelity $F = 1$.

Now, the initial n pairs might not all be in Bell states. But suppose that Alice and Bob were able to perform a Bell measurement on each pair, projecting it onto a simultaneous eigenstate of $X \otimes X$ and $Z \otimes Z$. Of course, since Alice and Bob are far apart from one another, they cannot really do this Bell measurement. But let's nevertheless imagine that they first perform a Bell measurement on each pair, and then proceed with the purification protocol. Purification works if the Bell measurement yields no more than t_X pairs with $X \otimes X = -1$ and no more than t_Z pairs with $Z \otimes Z = -1$. Therefore, if the initial state of the n pairs has the property that Bell measurement applied to all the pairs will, with very high probability, produce pairs with no more than t_Z bit flip errors and no more than t_X phase errors, then we are assured that Bell measurement followed by purification will produce a very high fidelity approximation to the encoded state $|\bar{\Phi}^{(k)}\rangle$.

But what if Alice and Bob execute the purification protocol without first performing the Bell measurement? We know that the purification works perfectly applied to the space $\mathcal{H}_{\text{good}}$ spanned by Bell pairs that differ from $|\phi^+\rangle^{\otimes n}$ by no more than t_Z bit flip errors and no more than t_X phase errors. Let Π denote the projection onto $\mathcal{H}_{\text{good}}$. Then if the protocol is applied to an initial density operator ρ of the n pairs, the final density operator ρ' approximates $|\bar{\Phi}^{(k)}\rangle$ with fidelity

$$F \equiv \langle \bar{\Phi}^{(k)} | \rho' | \bar{\Phi}^{(k)} \rangle \geq \text{tr}(\Pi \rho) . \quad (22.18)$$

Therefore, the fidelity is at least as large as the probability that t_Z or fewer bit flip errors and t_X or fewer phase errors would have been found if Bell measurement had been performed on all n pairs.

To derive the inequality eq. (22.18), we represent ρ as a pure state $|\Psi\rangle_{SE}$ of the n pairs (the “system” S) and an ancilla (the “environment” E , which might be under Eve’s control). The recovery superoperator can be represented as a unitary operator U_{SR} that is applied to S and an auxiliary system (the “reservoir” R) that serves as a repository for the entropy drawn from the pairs by error correction. Denote the initial pure state of the reservoir by $|0\rangle_R$. Then the state of system, environment, and reservoir to which the recovery operation is applied can be resolved into a “good” component

$$|\Psi_{\text{good}}\rangle_{SER} = (\Pi_S \otimes I_{ER}) |\Psi\rangle_{SE} \otimes |0\rangle_R , \quad (22.19)$$

and an orthogonal component

$$|\Psi_{\text{bad}}\rangle_{SER} = ((I_S - \Pi_S) \otimes I_{ER}) |\Psi\rangle_{SE} \otimes |0\rangle_R . \quad (22.20)$$

Since the states $|\Psi_{\text{good}}\rangle_{SER}$ and $|\Psi_{\text{bad}}\rangle_{SER}$ are orthogonal, the unitary recovery operation $U_{SR} \otimes I_E$ maps them to states $|\Psi'_{\text{good}}\rangle_{SER}$ and $|\Psi'_{\text{bad}}\rangle_{SER}$ that are also orthogonal to one another. Furthermore, since recovery works perfectly on the space $\mathcal{H}_{\text{good}}$, we have

$$|\Psi'_{\text{good}}\rangle_{SER} = |\bar{\Phi}^{(k)}\rangle_S \otimes |\text{junk}\rangle_{ER} , \quad (22.21)$$

where the state $|\text{junk}\rangle_{ER}$ of environment and reservoir has norm

$$\begin{aligned} {}_{ER}\langle \text{junk} | \text{junk} \rangle_{ER} &= {}_{SER}\langle \Psi'_{\text{good}} | \Psi'_{\text{good}} \rangle_{SER} \\ &= {}_{SER}\langle \Psi_{\text{good}} | \Psi_{\text{good}} \rangle_{SER} = \text{tr}(\Pi\rho) . \end{aligned} \quad (22.22)$$

Thus the fidelity of the recovered state can be expressed as

$$\begin{aligned} F &= {}_{SER}\langle \Psi' | \left(|\bar{\Phi}^{(k)}\rangle_S S \langle \bar{\Phi}^{(k)}| \right) \otimes I_{ER} | \Psi' \rangle_{SER} \\ &= {}_{SER}\langle \Psi'_{\text{good}} | \left(|\bar{\Phi}^{(k)}\rangle_S S \langle \bar{\Phi}^{(k)}| \right) \otimes I_{ER} | \Psi'_{\text{good}} \rangle_{SER} \\ &\quad + {}_{SER}\langle \Psi'_{\text{bad}} | \left(|\bar{\Phi}^{(k)}\rangle_S S \langle \bar{\Phi}^{(k)}| \right) \otimes I_{ER} | \Psi'_{\text{bad}} \rangle_{SER} \\ &= \text{tr}(\Pi\rho) + \langle \bar{\Phi}^{(k)} | \rho'_{\text{bad}} | \bar{\Phi}^{(k)} \rangle \geq \text{tr}(\Pi\rho) , \end{aligned} \quad (22.23)$$

where

$$\rho'_{\text{bad}} = \text{tr}_{ER} (|\Psi'_{\text{bad}}\rangle_{SER} {}_{SER}\langle \Psi'_{\text{bad}}|) ; \quad (22.24)$$

eq. (22.18) then follows. The key point is that, because of eq. (22.21), and because $|\Psi'_{\text{good}}\rangle_{SER}$ and $|\Psi'_{\text{bad}}\rangle_{SER}$ are orthogonal, there is no “good-bad” cross term in eq. (22.22).

Our arguments so far show that Alice and Bob can be assured that entanglement purification will work very well if they know that it is highly unlikely that

more than t_Z bit flip errors or more than t_X phase errors would have been found if they had projected their pairs onto the Bell basis. While they have no way of directly checking whether this condition is satisfied, they can conduct a test that, if successful, will provide them with high statistical confidence. We must now suppose that Alice and Bob start out with more than n pairs; to be definite, suppose they have about $2n$ to start, and that they are willing to sacrifice about half of them to conduct their verification test. Alice randomly decides which pairs are for verification (the “check pairs”) and which are for key distribution (the “key pairs”), and for each of her check qubits, she randomly decides to measure either X or Z . Then Alice publicly announces which are the check pairs, whether she measured X or Z on her half of each check pair, and the results of those measurements (in addition to the results of her measurements of the stabilizer generators).

Upon hearing of Alice’s choices, Bob measures X or Z on his half of each of the check pairs; thus Alice and Bob are able to measure $X \otimes X$ on about half of their check pairs, and they measure $Z \otimes Z$ on the remaining check pairs. Now since the check pairs were randomly chosen, the eavesdropper Eve has no way of knowing which are the check pairs, and she can’t treat them any differently than the key pairs; hence the measured error rate found for the check pairs will be representative of the error rate that would have been found on the key pairs if Alice and Bob had projected the key pairs onto the Bell basis. Therefore, Alice and Bob can use their check data and classical sampling theory to estimate how many bit flip and phase errors would have been expected if they had measured the key pairs.

For example, in a sample of N pairs, suppose that if Alice and Bob both measured Z for all the pairs, a fraction p of their measurements would disagree, indicating bit flip errors. Then if they randomly sample $M < N$ of the pairs, the probability distribution for the number $M(p - \varepsilon)$ of errors found would be²

$$P(\varepsilon) < \exp(-M\varepsilon^2/2p(1-p)). \quad (22.25)$$

If Alice and Bob have no *a priori* knowledge of the value of p , then by Bayes’ theorem, the conditional probability that the total number of errors in the population is pN , given that there are $p_Z M$ errors in the sample, is the same as the probability that there are $p_Z M$ errors in the sample given that there are pN errors in the total population. Writing $p = p_Z + \varepsilon$, the number of errors on the $N - M$ untested pairs is $Np - Mp_Z = (N - M)p_Z + N\varepsilon = (N - M) \cdot (p_Z + \varepsilon')$, where $\varepsilon' = N\varepsilon/(N - M)$. Expressing $P(\varepsilon)$ in terms of ε' we find

$$P(\varepsilon') < \exp\left(-\frac{M(N - M)^2\varepsilon'^2}{2N^2p_Z(1 - p_Z)}\right), \quad (22.26)$$

a bound on the probability that the fraction of the untested pairs with errors is larger than $p_Z + \varepsilon'$. In particular, if they test about $M = n/2$ pairs for bit flip

errors out of a total of about $N = n + n/2$ pairs, the probability that a fraction $p_Z + \varepsilon'$ of the remaining $N - M = n$ pairs have bit flip errors is

$$P(\varepsilon') < \exp\left(-n\varepsilon'^2/9p_Z(1-p_Z)\right). \quad (22.27)$$

A similar argument applies to the probability of phase errors. We conclude that by conducting the verification test, Alice and Bob can be very confident that, if they had measured $Z \otimes Z$ (or $X \otimes X$) on the n key pairs, no more than $(p_Z + \varepsilon')n$ (or $(p_X + \varepsilon')n$) errors would have been found. By choosing a quantum error-correcting code that can correct this many errors with high probability, they can be confident that the encoded state they prepare approximates $|\bar{\Phi}^{(k)}\rangle$ with fidelity exponentially close to one.

It is important to emphasize that this argument requires no assumption about how the errors on different pairs may be correlated with one another. Rather the argument is applied to a hypothetical situation in which the value of $Z \otimes Z$ (or $X \otimes X$) already has been measured and recorded for all of the check pairs and all of the key pairs. Sampling theory is then used to address the question: how reliably does a “poll” of M bits randomly chosen from among N allow us to predict the behavior of the rest of the population. Classical sampling theory can be applied to the values of both $Z \otimes Z$ and $X \otimes X$ for the key pairs, because the operators commute and so are simultaneously measurable in principle [12].

Furthermore, if the state of the encoded pairs that Alice and Bob use for key distribution is exponentially close to being a pure state, it follows from Holevo’s theorem that Eve’s mutual information with the distributed key is exponentially small [12, 18]. In the worst case, the imperfect fidelity of Alice’s and Bob’s pairs is entirely due to Eve’s intervention; then the complete state consisting of the pairs and Eve’s probe is pure, and the Von Neumann entropy $S(\rho_E) \equiv -\text{tr } \rho_E \log \rho_E$ of the state ρ_E of the probe equals the entropy of the state ρ_{AB} of the pairs. By extracting a key from their pairs, Alice and Bob in effect prepare a state for Eve governed by an ensemble with density matrix ρ_E . According to Holevo’s theorem, the mutual information $I(AB; E)$ of this state preparation with any measurement that Eve can carry out on her probe satisfies

$$I(AB; E) \leq S(\rho_E) = S(\rho_{AB}), \quad (22.28)$$

and since ρ_{AB} is very nearly pure, $S(\rho_{AB})$ and $I(AB; E)$ are very close to zero. Specifically, if the fidelity of ρ_{AB} is $F = 1 - \delta$, then the largest eigenvalue of ρ_{AB} is at least $1 - \delta$. For a system with dimension D , the density matrix with largest eigenvalue $1 - \delta$ that has the maximal Von Neumann entropy is

$$\rho_{\max} = \text{diag}\left(1 - \delta, \frac{\delta}{D-1}, \frac{\delta}{D-1}, \dots, \frac{\delta}{D-1}\right). \quad (22.29)$$

for which

$$\begin{aligned} S(\rho_{\max}) &= -(1 - \delta) \log_2(1 - \delta) - \delta \log_2(\delta/(D - 1)) \\ &= \delta \cdot \left(\frac{1}{\log_e 2} + \log_2(D - 1) - \log_2 \delta \right) + O(\delta^2). \end{aligned} \quad (22.30)$$

Taking $D = 2^{2k}$ (the total dimension of Alice's and Bob's code spaces), we conclude that

$$S(\rho_{AB}) \leq \delta \cdot \left(\frac{1}{\log_e 2} + 2k + \log_2(1/\delta) \right) + O(\delta^2). \quad (22.31)$$

Finally, we have shown that if the verification test succeeds, then with probability exponentially close to one (the probability that the error rate inferred from the check sample is not seriously misleading), Eve's mutual information with the key is exponentially small (because the state of the key bits approximates $|\bar{\Phi}^{(k)}\rangle$ with fidelity exponentially close to one). This proof of security applies to any conceivable eavesdropping strategy adopted by Eve.

The proof relies on the ability of quantum error-correcting codes to reverse the errors caused by interactions between the key pairs and Eve's probe. Hence it may seem odd that the proof works for arbitrary attacks by Eve, since quantum error correction works effectively only for a restricted class of error superoperators. Specifically, the error superoperator acting on a block of n qubits can be expanded in terms of a basis of "Pauli error operators," where in each term of the expansion bit flip errors and/or phase errors are inflicted on specified qubits within the block. The encoded quantum information is well protected only if the error superoperator has nearly all of its support on Pauli operators that can be corrected by the code, *e.g.*, those with no more than t_Z bit flip errors and t_X phase errors.

If Eve's probe interacts collectively with many qubits, it may cause more bit flip or phase errors than the code can correct. But the crucial point is that, with high probability, an attack that causes many errors on the key bits will also cause many errors on the check bits, and Alice and Bob will detect Eve's presence.

3.3 REDUCTION TO THE BB84 PROTOCOL

Since the entanglement distillation protocol requires only one-way classical communication, this protocol is actually equivalent to one in which Alice, rather than preparing Bell pairs and sending half of each pair to Bob, instead prepares an encoded quantum state that she sends to Bob. Using a set of stabilizer generators on which she and Bob have agreed in advance, Alice chooses a random eigenvalue for each stabilizer generator M_i ; then employing the corresponding $[[n, k, d]]$ quantum code, she prepares one of 2^k mutually orthogonal codewords.

Alice also decides at random which of her qubits will be used for key distribution and which will be used for verification. For each of the check bits, she decides at random whether to send an X eigenstate (with random eigenvalue) or a Z eigenstate (with random eigenvalue).

Bob receives the qubits sent by Alice, carefully deposits them in his quantum memory, and publicly announces that the qubits have been received. Alice then publicly reveals which qubits were used for the key, and which qubits are the check qubits. She announces the stabilizer eigenvalues that she chose to encode her state, and for each check qubit, she announces whether it was prepared as an X or Z eigenstate, and with what eigenvalue.

Once Bob learns which qubits carry the encoded key information, he measures the stabilizer operators and compares his results with Alice's to obtain a relative error syndrome. He then performs error recovery and measures the encoded state to decipher the key.

Bob also measures the check qubits and compares the outcomes to the values announced by Alice, to obtain an estimate of the error rate. If the error rate is low enough, error recovery applied to the encoded key bits will succeed with high probability, and Alice and Bob can be confident in the security of the key. If the error rate is too high, Bob informs Alice and they abort the protocol.

As described so far, the protocol requires that Alice and Bob have quantum memories and quantum computers that are used to store the qubits, measure stabilizer generators, and correct errors. But if they use a stabilizer code of the CSS (Calderbank-Shor-Steane) type [6, 19], then the protocol can be simplified further. The crucial property of the CSS codes is that there is a clean separation between the syndrome information needed to correct bit flip errors and the syndrome information needed to correct phase errors.

A CSS quantum stabilizer code is associated with a classical binary linear code C_1 on n bits, and a subcode $C_2 \subset C_1$. Let H_1 denote the parity check matrix of C_1 and H_2 the generator matrix for the code C_2 (and hence the parity check matrix of the dual code C_2^\perp). The stabilizer generators of the code are of two types. Associated with the i th row of the matrix H_1 is a “ Z -generator,” the tensor product of I 's and Z 's

$$M_{Z,i} = \otimes_{j=1}^n (Z_j)^{(H_1)_{ij}} , \quad (22.32)$$

and associated with the i th row of H_2 is an “ X -generator,” the tensor product of I 's and X 's

$$M_{X,i} = \otimes_{j=1}^n (X_j)^{(H_2)_{ij}} . \quad (22.33)$$

Since H_1 has $n - k_1$ rows, where $k_1 = \dim(C_1)$, and H_2 has k_2 rows, where $k_2 = \dim(C_2)$ there are all together $n - k_1 + k_2$ stabilizer generators, and the dimension of the code space (the number of encoded qubits) is $k = k_1 - k_2$.

From measurements of the Z generators, bit flip errors can be diagnosed, and from measurement of the X generators, phase errors can be diagnosed.

The elements of a basis for the code space with eigenvalues of stabilizer generators

$$M_{Z,i} = (-1)^{s_i}, \quad M_{X,i} = (-1)^{t_i} \quad (22.34)$$

are in one-to-one correspondence with the k cosets of C_2 in C_1 ; they can be chosen as

$$|\psi(v)\rangle_{x,z} = \frac{1}{|C_2|^{1/2}} \sum_{w \in C_2} (-1)^{z \cdot w} |v + w + x\rangle; \quad (22.35)$$

here $v \in C_1$ is a representative of a C_2 coset, and x, z are n -bit strings satisfying

$$H_1 x = s, \quad H_2 z = t. \quad (22.36)$$

Thus, to distribute the key, Alice chooses x and z at random, encodes one of the $|\psi(v)\rangle_{x,z}$'s, and sends the state to Bob. After Bob confirms receipt, Alice broadcasts the values of x and z . Bob compares Alice's values to his own measurements of the stabilizer generators to infer a relative syndrome, and he performs error correction. Then Bob measures Z of each of his n qubits, obtaining a bit string $v + w + x$. Finally, he subtracts x and applies H_2 to compute $H_2 v$, from which he can infer the coset represented by v and hence the key.

Now notice that Bob extracts the encoded key information by measuring Z of each of the qubits that Alice sends. Thus Bob can correctly decipher the key information by correcting any bit flip errors that occur during transmission. Bob does not need to correct phase errors, and therefore he has no use for the phase syndrome information; hence there is no need for Alice to send it.

Without in any way weakening the effectiveness of the protocol, Alice can prepare the encoded state $|\psi(v)\rangle_{x,z}$, but discard her value of z , rather than transmitting it; thus we can consider the state sent by Alice to be averaged over the value of z . Averaging over the phase $(-1)^{z \cdot w}$ destroys the coherence of the sum over $w \in C_2$ in $|\psi(v)\rangle_{x,z}$; in effect, then, Alice is preparing n qubits as Z eigenstates, in the state $|v + w + x\rangle$, sending the state to Bob, and later broadcasting the value of x . We can just as well say that Alice sends a random string u , and later broadcasts the value of $u + v$. Bob receives $u + e$ (where e has support on the bits that flip due to errors) extracts $v + e$, corrects it to the nearest C_1 codeword, and infers the key, the coset $v + C_2$.

Alice and Bob can carry out this protocol even if Bob has no quantum memory. Alice decides at random to prepare her qubits as X or Z eigenstates, with random eigenvalues, and Bob decides at random to measure in the X or Z basis. After public discussion, Alice and Bob discard the results in the

cases where they used different bases and retain the results where they used the same basis. Thus the protocol we have described is just the BB84 protocol invented by Bennett and Brassard [1], accompanied by classical error correction (adjusting $v + e$ to a C_1 codeword) and privacy amplification (extracting the coset $v + C_2$).

What error rate is acceptable? In a random CSS code, about half of the $n - k$ generators correct bit flips, and about half correct phase flips. Suppose that the verification test finds that bit flip errors ($Z_A \otimes Z_B = -1$) occur with probability p_Z and phase errors ($X_A \otimes X_B = -1$) occur with probability p_X . Classical coding theory shows that a random CSS code can correct the bit flips with high probability if the number of typical errors on n bits is much smaller than the number of possible bit flip error syndromes, which holds provided that

$$\binom{n}{np_Z} 2^{-(n-k)/2} \sim 2^{nH_2(p_Z)-(n-k)/2} \ll 1, \quad (22.37)$$

where $H_2(x) = -x \log_2 x - (1-x) \log_2(1-x)$ is the binary entropy function. Similarly, the phase errors can be corrected with high probability provided the same relation holds with p_Z replaced by p_X . Therefore, asymptotically as $n \rightarrow \infty$, secure key bits can be extracted from transmitted key bits at any rate R satisfying

$$\begin{aligned} R &= \frac{k}{n} < 1 - 2H_2(p_Z), \\ R &= \frac{k}{n} < 1 - 2H_2(p_X). \end{aligned} \quad (22.38)$$

This upper bound on R crosses zero at p_Z (or p_X) = .1100. We conclude that secure key distribution is possible if $p_{X,Z} < 11\%$.

The random coding argument applies if the errors in the key qubits are randomly distributed. To assure that this is so, we can direct Alice to perform a random permutation of the qubits before sending them to Bob. After Bob confirms receipt, Alice can broadcast the permutation she performed, and Bob can invert it.

Again, the essence of this argument is that the amount of information that an eavesdropper could acquire is limited by how successfully we could have carried out quantum error correction if we had chosen to – and that this relation holds irrespective of whether we really implemented the quantum error correction or not.

Other proofs of the security of the BB84 protocol have been presented [13, 3], which don't make direct use of this connection with quantum error-correcting codes. However, these proofs do use classical error correction and privacy amplification, and they implicitly exploit the structure of the CSS codes.

3.4 IMPERFECT SOURCES

Our objective in this paper is to analyze the security of key distribution schemes that use systems described by continuous quantum variables. The analysis will follow the strategy we have just outlined, in which an entanglement-purification protocol is reduced to a protocol that does not require the distribution of entanglement. But first we need to discuss a more general version of the argument.

In the entanglement-purification protocol, whose reduction to the BB84 protocol we have just described, there is an implicit limitation on the eavesdropper's activity. We have assumed that Alice prepares perfect entangled pairs in the state $|\phi^+\rangle$, and then sends half of each pair to Bob. Eve has been permitted to tamper with the qubits that are sent to Bob in any way she chooses, but she has not been allowed any contact with Alice's qubits. Therefore, if we imagine that Alice measures her qubits before sending to Bob, we obtain a BB84 protocol in which Alice is equipped with a perfect source of polarized qubits. When she sends a Z eigenstate, the decision to emit a $|0\rangle$ or a $|1\rangle$ is perfectly random, and the state emerges from her source with perfect fidelity. Similarly, when she sends an X eigenstate, the decision to send $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$ is perfectly random, and the state is prepared with perfect fidelity. Furthermore, Eve has no knowledge of what Alice's source does, other than what she is able to infer by probing the qubits as they travel to Bob.

Security can be maintained in a more general scenario. In the entanglement-purification protocol, we can allow Eve access to Alice's qubits. As long as Eve has no way of knowing which pairs Alice and Bob will select for their verification test, and no way of knowing whether the check pairs will be measured in the Z or X basis, then the protocol still works: eavesdropping can be detected irrespective of whether Eve probes Alice's qubits, Bob's qubits, or both.

Now if we imagine that Alice measures her qubits before sending to Bob, we obtain a BB84-like protocol in which Alice's source is imperfect and/or Eve is able to collect some information about how Alice's source behaves. Our proof that the BB84-like protocol is secure still works as before. However the proof applies only to a restricted type of source — it must be possible to simulate Alice's source exactly by measuring half of a two-qubit state.

To be concrete, consider the following special case, which will suffice for our purposes: Alice has many identical copies of the two-qubit state ρ_{AB} . To prepare a "Z-state" she measures qubit A in the basis $\{|0\rangle_A, |1\rangle_A\}$. Thus she

sends to Bob one of the two states

$$\begin{aligned}\rho_0 &= \frac{{}_A\langle 0|\rho_{AB}|0\rangle_A}{\text{tr}({}_A\langle 0|\rho_{AB}|0\rangle_A)}, \\ \rho_1 &= \frac{{}_A\langle 1|\rho_{AB}|1\rangle_A}{\text{tr}({}_A\langle 1|\rho_{AB}|1\rangle_A)},\end{aligned}\quad (22.39)$$

chosen with respective probabilities

$$\begin{aligned}\text{Prob}(0) &= \text{tr}({}_A\langle 0|\rho_{AB}|0\rangle_A), \\ \text{Prob}(1) &= \text{tr}({}_A\langle 1|\rho_{AB}|1\rangle_A).\end{aligned}\quad (22.40)$$

Similarly, to prepare an X -state she measures in the basis $\{|+\rangle, |-\rangle\}$, sending one of

$$\begin{aligned}\rho_+ &= \frac{{}_A\langle +|\rho_{AB}|+\rangle_A}{\text{tr}({}_A\langle +|\rho_{AB}|+\rangle_A)}, \\ \rho_- &= \frac{{}_A\langle -|\rho_{AB}|-\rangle_A}{\text{tr}({}_A\langle -|\rho_{AB}|-\rangle_A)},\end{aligned}\quad (22.41)$$

chosen with respective probabilities

$$\begin{aligned}\text{Prob}(+) &= \text{tr}({}_A\langle +|\rho_{AB}|+\rangle_A), \\ \text{Prob}(-) &= \text{tr}({}_A\langle -|\rho_{AB}|-\rangle_A).\end{aligned}\quad (22.42)$$

Unless the state ρ_{AB} is precisely the pure state $|\phi^+\rangle$, Alice's source isn't doing exactly what it is supposed to do. Depending on how ρ_{AB} is chosen, the source might be biased; for example it might send ρ_0 with higher probability than ρ_1 . And the states ρ_0 and ρ_1 need not be the perfectly prepared $|0\rangle$ and $|1\rangle$ that the protocol calls for.

Now suppose that Alice's source always emits one of the states $\rho_0, \rho_1, \rho_+, \rho_-$, and that after the qubits emerge from the source, Eve is free to probe them any way she pleases. Even though Alice's source is flawed, Alice and Bob can perform verification, error correction, and privacy amplification just as in the BB84 protocol. To verify, Bob measures Z or X , as before; if he measures Z , say, they check to see whether Bob's outcome $|0\rangle$ or $|1\rangle$ agrees with whether Alice sent ρ_0 or ρ_1 (even though the state that Alice sent may not have been a Z eigenstate). Thereby, Alice and Bob estimate error rates p_Z and p_X . If both error rates are below 11%, then the protocol is secure.

We emphasize again that the security criterion $p_X, p_Z < 11\%$ applies not to all sources, but only to the restricted class of imperfect sources that can be simulated by measuring half of a (possibly noisy) entangled state. To give an extreme example of a type of source to which the security proof does not apply, suppose that Alice *always* sends the Z -state $|0\rangle$ or the X -state $|+\rangle$.

Clearly the key distribution protocol will fail, even if Bob's bits always agree with Alice's! Indeed, a source with these properties cannot be obtained by measuring half of any two-qubit state ρ_{AB} . Rather, if the source is obtained by such a measurement, then a heavy bias when we send a Z -state would require that the error probability be large when we send an X -state.

4. DISTRIBUTING A KEY BIT WITH CONTINUOUS VARIABLES

Now let's consider how the above ideas can be applied to continuous variable systems. We will first describe how in principle Alice and Bob can extract good encoded pairs of qubits from noisy EPR pairs. However, the distillation protocol requires them to make measurements that are difficult in practice. Then we will see how key distribution that invokes (difficult) entanglement distillation can be reduced to key distribution based on (easier) preparation, transmission, and detection of squeezed states.

Suppose that Alice and Bob share pairs of oscillators. Ideally each pair has been prepared in an EPR state, a simultaneous eigenstate (let's say with eigenvalue 0) of $q_A - q_B$ and $p_A + p_B$. Now suppose that Alice measures the two commuting stabilizer generators defined in eq. (22.1), obtaining the outcomes

$$S_{q,A} = e^{2\pi i \phi_{q,A}} , \quad S_{p,A} = e^{-2\pi i \phi_{p,A}} , \quad (22.43)$$

or

$$\begin{aligned} q_A &= \phi_{q,A} \cdot \sqrt{\pi} \pmod{\sqrt{\pi}} , \\ p_A &= \phi_{p,A} \cdot \sqrt{\pi} \pmod{\sqrt{\pi}} . \end{aligned} \quad (22.44)$$

Now, the initial state was an eigenstate with eigenvalue one of the operators $S_{q,A} \otimes S_{q,B}^{-1}$ and $S_{p,A} \otimes S_{p,B}$. The observables measured by Alice commute with these, and so preserve their eigenvalues. Thus if the initial EPR state of the oscillators were perfect, Alice's measurement would also prepare for Bob a simultaneous eigenstate of the stabilizer generators with

$$\begin{aligned} S_{q,B} &\equiv e^{2\pi i \phi_{q,B}} = e^{2\pi i \phi_{q,A}} , \\ S_{p,B} &\equiv e^{-2\pi i \phi_{p,B}} = e^{2\pi i \phi_{p,A}} , \end{aligned} \quad (22.45)$$

or

$$\begin{aligned} q_B &= q_A \pmod{\sqrt{\pi}} , \\ p_B &= -p_A \pmod{\sqrt{\pi}} . \end{aligned} \quad (22.46)$$

Similarly, the initial state was an eigenstate with eigenvalue one of the observables

$$\bar{X}_A(\phi_p) \otimes \bar{X}_B(\phi_p) , \quad \bar{Z}_A(\phi_q) \otimes \bar{Z}_B(\phi_q)^{-1} , \quad (22.47)$$

which also commute with the stabilizer generators that Alice measured. Thus Alice's measurement has prepared an encoded Bell pair in the code space labeled by (ϕ_q, ϕ_p) , the state

$$|\bar{\phi}^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|\bar{0}\rangle_A |\bar{0}\rangle_B + |\bar{1}\rangle_A |\bar{1}\rangle_B) . \quad (22.48)$$

Of course the initial EPR pair shared by Alice and Bob might be imperfect, and then the encoded state produced by Alice's measurement will also have errors. But if the EPR pair is not too noisy, they can correct the errors with high probability. Alice broadcasts her measured values of the stabilizer generators to Bob; Bob also measures the stabilizer generators and compares his values to those reported by Alice, obtaining a relative syndrome

$$e^{i(\phi_{q,A} - \phi_{q,B})}, \quad e^{-i(\phi_{p,A} + \phi_{p,B})} . \quad (22.49)$$

That is, the relative syndrome determines the value of $q_A - q_B \pmod{\sqrt{\pi}}$, and $p_A + p_B \pmod{\sqrt{\pi}}$. Using this information, Bob can shift his oscillator's q and p (by an amount between $-\sqrt{\pi}/2$ and $\sqrt{\pi}/2$) to adjust $q_A - q_B \pmod{\sqrt{\pi}}$, and $p_A + p_B \pmod{\sqrt{\pi}}$ both to zero. The result is that Alice and Bob now share a bipartite state in the code subspace labeled by (ϕ_q, ϕ_p) .

If the initial noisy EPR state differs from the ideal EPR state only by relative shifts of Bob's oscillator relative to Alice's that satisfy $|\Delta q|, |\Delta p| < \sqrt{\pi}/2$, then the shifts will be corrected perfectly. And if larger shifts are highly unlikely, then Alice and Bob will obtain a state that approximates the desired encoded Bell pair $|\bar{\phi}^+\rangle$ with good fidelity. This procedure is a “distillation” protocol in that Alice and Bob start out with a noisy entangled state in a tensor product of infinite dimensional Hilbert spaces, and “distill” from it a far cleaner entangled state in a tensor product of two-dimensional subspaces.

Once Alice and Bob have distilled an encoded Bell pair, they can use it to generate a key bit, via the usual EPR key distribution protocol: Alice decides at random to measure either \bar{X} or \bar{Z} , and then publicly reveals what she chose to measure but not the measurement outcome. Bob then measures the same observable and obtains the same outcome – that outcome is the shared key bit.

How do they measure \bar{X} or \bar{Z} ? If Alice (say) wishes to measure \bar{Z} , she can measure q , and then subtract ϕ_q from the outcome. The value of \bar{Z} is determined by whether the result is an even ($\bar{Z} = 1$) or an odd ($\bar{Z} = -1$) multiple of $\sqrt{\pi}$. Similarly, if Alice wants to measure \bar{X} , she measures p and subtracts ϕ_p – The value of \bar{X} is determined by whether the result is an even ($\bar{X} = 1$) or an odd ($\bar{X} = -1$) multiple of $\sqrt{\pi}$.

Imperfections in the initial EPR pairs are inescapable not just because of experimental realities, but also because the ideal EPR pairs are unphysical nonnormalizable states. Likewise, the stabilizer operators cannot even in principle be measured with arbitrary precision (the result would be an infinite bit

string), but only to some finite m -bit accuracy. Still, if the EPR pairs have reasonably good fidelity, and the measurements have reasonably good resolution, entanglement purification will be successful.

To summarize, Alice and Bob can generate a shared bit by using the continuous variable code for entanglement purification, carrying out this protocol:

Key distribution with entanglement purification

- 1:** Alice prepares (a good approximation to) an EPR state of two oscillators, a simultaneous eigenstate of $q_A - q_B = 0 = p_A + p_B$, and sends one of the oscillators to Bob.
- 2:** After Bob confirms receipt, Alice and Bob each measure (to m bits of accuracy) the two commuting stabilizer generators of the code, $e^{i(2\sqrt{\pi})q}$ and $e^{-i(2\sqrt{\pi})p}$. (Equivalently, they each measure the value of q and p modulo $\sqrt{\pi}$.) Alice broadcasts her result to Bob, and Bob applies shifts in q and p to his oscillator, so that his values of q and p modulo $\sqrt{\pi}$ now agree with Alice's (to m -bit accuracy). Thus, Alice and Bob have prepared (a very good approximation to) a Bell state $|\bar{\phi}^+\rangle$ of two qubits encoded in one of the simultaneous eigenspaces of the two stabilizer operators.
- 3:** Alice decides at random to measure one of the encoded operators \bar{X} or \bar{Z} ; then she announces what she chose to measure, but not the outcome. Bob measures the same observable; the result is the shared bit that they have generated.

Now notice that, except for Bob's confirmation that he received the states, this protocol requires only one-way classical communication from Alice to Bob. Alice does not need to receive any information from Bob before she measures her stabilizer operators or before she measures the encoded operation \bar{X} or \bar{Z} . Therefore, the protocol works just as well if Alice measures her oscillator before sending the other one to Bob. Equivalently, she prepares an encoded state, adopting randomly selected values of the stabilizer generators. She also decides at random whether the encoded state will be an \bar{X} eigenstate or a \bar{Z} eigenstate, and whether the eigenvalue will be $+1$ or -1 .

Again, since the codewords are unphysical nonnormalizable states, Alice can't really prepare a perfectly encoded state; she must settle for a "good enough" approximate codeword.

In summary, we can replace the entanglement-purification protocol with this equivalent protocol:

Key distribution with encoded qubits

- 1:** Alice chooses random values (to m bits of accuracy) for the stabilizer generators $e^{i(2\sqrt{\pi})q}$ and $e^{-i(2\sqrt{\pi})p}$, chooses a random bit to decide whether

to encode a \bar{Z} eigenstate or an \bar{X} eigenstate, and chooses another random bit to decide whether the eigenvalue will be ± 1 . She then prepares (a good approximation to) the encoded eigenstate of the chosen operator with the chosen eigenvalue in the chosen code, and sends it to Bob.

- 2: After Bob confirms receipt, Alice broadcasts the stabilizer eigenvalues and whether she encoded a \bar{Z} or an \bar{X} .
- 3: Bob measures q or p . He subtracts from his outcome the value modulo $\sqrt{\pi}$ determined by Alice's announced value of the stabilizer generator, and corrects the result to the nearest integer multiple of $\sqrt{\pi}$. He extracts a bit determined by whether the multiple of $\sqrt{\pi}$ is even or odd; this is the shared bit that they have generated.

To carry out this protocol, Alice requires sophisticated tools that enable her to prepare the approximate codewords, and Bob needs a quantum memory to store the state that he receives until he hears Alice's classical broadcast. However, we can reduce the protocol to one that is much less technically demanding.

When Bob extracts the key bit by measuring (say) q , he needs Alice's value of q modulo $\sqrt{\pi}$, but he does not need her value of the other stabilizer generator. Therefore, there is no need for Alice to send it; surely, the eavesdropper will be no better off if Alice sends less classical information. If she doesn't send the value of S_p , then we can consider the protocol averaged over the unknown value of this generator. Formally, for perfect (nonnormalizable) codewords the density matrix describing the state that is accessible to a potential eavesdropper then has a definite value of S_q but is averaged over all possible values of S_p – it is a (nonnormalizable) equally weighted superposition of all position eigenstates with a specified value of $q \bmod \sqrt{\pi}$; *e.g.* in the case where Alice prepares a \bar{Z} eigenstate, we have

$$\begin{aligned} & \rho(\phi_q, \bar{Z} = 1) \\ & \propto \sum_s |q = (2s + \phi_q)\sqrt{\pi}\rangle\langle q = (2s + \phi_q)\sqrt{\pi}|, \\ & \rho(\phi_q, \bar{Z} = -1) \\ & \propto \sum_s |q = (2s + 1 + \phi_q)\sqrt{\pi}\rangle\langle q = (2s + 1 + \phi_q)\sqrt{\pi}|. \end{aligned} \tag{22.50}$$

Averaged over ϕ_q as well, Alice is sending a random position eigenstate. Likewise, in the case where Alice prepares an \bar{X} eigenstate, she sends a random momentum eigenstate.

Therefore, the protocol in which Alice prepares encoded qubits can be replaced by a protocol that is simpler to execute but is no less effective and no less secure. Instead of bothering to prepare the encoded qubit, she just decides

at random to send either a q or p eigenstate, with a random eigenvalue. If Bob had a quantum memory, he could store the state, and wait to hear from Alice whether the state she sent was a q or p eigenstate; then he could measure that observable. Subtracting $\phi_q\sqrt{\pi}$ (or $\phi_p\sqrt{\pi}$) from his measurement outcome, he would obtain an even or odd multiple of $\sqrt{\pi}$.

But Bob does not really need the quantum memory. As in the BB84 protocol, it suffices for Bob to decide at random to measure either q or p , and then publicly compare his basis with Alice's. They discard the results where they used different bases and retain the others.

A problem with this procedure is that the position and momentum eigenstates are unphysical nonnormalizable states, and the probability distribution that Alice samples to decide on what value of q or p to send is also nonnormalizable. For it to implementable, we need to modify the procedure so that Alice sends narrow q or p wave packets, and chooses the position of the center of the wave packet by sampling a broad but normalizable distribution.

Therefore, Alice and Bob can adopt the following protocol:

Key distribution with squeezed states

- 1: Alice chooses a random bit to decide whether to send a state squeezed in q or in p . She samples a (discrete approximation to) a probability distribution $P_{\text{pos}}(q)$ or $P_{\text{mom}}(p)$ to choose a value of q or p , and then sends to Bob a narrow wave packet centered at that value.
- 2: Bob receives the state and decides at random to measure either q or p .
- 3: After Bob confirms receipt, Alice and Bob broadcast whether they sent or measured in the q or p basis. If they used different bases, they discard their results. If they used the same basis, they retain the result and proceed to Step 4.
- 4: Alice broadcasts the value that she sent, modulo $\sqrt{\pi}$ (to m -bit accuracy). Bob subtracts Alice's value from what he measured, and corrects to the nearest integer multiple of $\sqrt{\pi}$. He and Alice extract their shared bit according to whether this integer is even or odd.

5. A SECURE PROTOCOL USING CONTINUOUS VARIABLES

Now we are ready to combine the protocol of §3. with the protocol of §4.. The result is a protocol based on concatenating the continuous variable code with an $[[n, k, d]]$ binary CSS code. The concatenated code embeds a k -dimensional Hilbert space in the infinite-dimensional Hilbert space of n oscillators.

Again, we first imagine that Alice and Bob carry out an entanglement distillation protocol. They start out sharing n pairs of oscillators, each in a (noisy) EPR state. By measuring the stabilizer generators of the concatenated code,

they distill k encoded Bell pairs of much better fidelity, and then generate a key by measuring the encoded Bell pairs.

By once again following the chain of reductions recounted in §3. and §4., we arrive at an equivalent protocol involving transmission of squeezed states. The complete protocol, including verification, error correction, and privacy amplification, becomes:

Continuous-variable QKD

- 1:** Alice has $(4 + \delta)n$ oscillators. For each oscillator, Alice decides at random to prepare either a state squeezed in q or a state squeezed in p . The position of the squeezed state is determined by sampling (a discrete approximation to) a probability distribution $P_{\text{pos}}(q)$ or $P_{\text{mom}}(p)$. Alice then sends the oscillators to Bob.
- 2:** Bob receives the $(4 + \delta)n$ oscillators, measuring each in the q or p basis at random.
- 3:** Bob confirms that the oscillators have been received, and then Alice announces whether each oscillator was squeezed in q or in p .
- 4:** Alice and Bob discard the results in the cases where Bob measured in a different basis than Alice used in her preparation. With high probability, there are at least $2n$ measured values left (if not, abort the protocol). Alice decides randomly on a set of $2n$ values to use for the protocol, and chooses at random n of these to be check values.
- 5:** For all $2n$ measured values, Alice announces the value of q or p modulo $\sqrt{\pi}$ (to m bits of accuracy).
- 6:** Bob subtracts the corresponding number announced by Alice from each of his measured values, and then corrects the result to the nearest integer multiple of $\sqrt{\pi}$. Bob and Alice now extract bit values determined by whether the multiple of $\sqrt{\pi}$ is even or odd.
- 7:** Alice and Bob announce the values of their check bits. If too few of the check bits agree, they abort the protocol.
- 8:** Alice announces $u + v$, where u is the string consisting of the remaining non-check bits, and v is a random codeword in C_1 .
- 9:** Bob subtracts $u + v$ from his code qubits, $u + e$, and corrects the result, $v + e$, to a codeword in C_1 . With high probability, Bob recovers v .
- 10:** Alice and Bob use the C_2 coset $v + C_2$ as the key.

Here, to be specific, we have instructed Alice and Bob to sacrifice n check bits for each n bits that are used for key distribution. They might instead use fewer or more, depending on how stringent a bound on the eavesdropper's mutual information they require.

The check bits provide Alice and Bob with estimates of the bit error rates p_Z (respectively p_X) when states squeezed in q (respectively p) are transmitted.

Our analysis of the BB84 protocol indicates that the squeezed state protocol is secure provided that p_Z and p_X are both below 11%, and assuming that Alice and Bob scramble and unscramble the oscillators (by applying a random permutation and its inverse).

However, as noted in §3.4, the proof and the security criterion $p_Z, p_X < 11\%$ apply only if Alice's source can be simulated by measuring half of an entangled state of two oscillators. In particular, we may imagine that Alice has many pairs of oscillators identically prepared in the state ρ_{AB} , and that she prepares the state that she sends to Bob by measuring oscillator A . When she measures in the q basis, she sends the state

$$\rho_B(q) = \frac{{}_A\langle q|\rho_{AB}|q\rangle_A}{\text{tr}({}_A\langle q|\rho_{AB}|q\rangle_A)} \quad (22.51)$$

with probability

$$P_{\text{pos}}(q) = \text{tr}({}_A\langle q|\rho_{AB}|q\rangle_A), \quad (22.52)$$

and when she measures in the p basis, she sends the state

$$\rho_B(p) = \frac{{}_A\langle p|\rho_{AB}|p\rangle_A}{\text{tr}({}_A\langle p|\rho_{AB}|p\rangle_A)} \quad (22.53)$$

with probability

$$P_{\text{mom}}(p) = \text{tr}({}_A\langle p|\rho_{AB}|p\rangle_A). \quad (22.54)$$

Thus, the states that Alice sends need not be perfect position or momentum eigenstates for the proof of security to work, and Alice's source might even have a bias so that the raw key bit carried by an oscillator is more likely to be a 0 than a 1. Still, for a source of this type, if Alice and Bob verify that the error rate for the raw key bits is below 11% in both bases, then the protocol is provably secure. We will discuss examples in §6. and §7.

Intuitively, the squeezed state protocol is secure because the eavesdropper cannot monitor the value of q (or p) transmitted without introducing a detectable disturbance in the complementary observable p (or q). As shown in Fig. 22.1, the Wigner functions of the signal states squeezed in p and in q overlap, so that the states cannot be reliably distinguished.

6. GAUSSIAN STATES

Perfectly squeezed states (position or momentum eigenstates) are unphysical nonnormalizable states, so the protocol will actually be carried out with imperfectly squeezed states. Furthermore, engineering a source that produces highly squeezed states would be quite technically demanding. How much squeezing

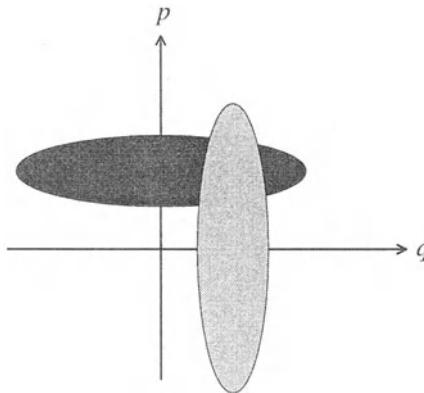


Figure 22.1 One-sigma contours of the Wigner functions for typical squeezed states used in the quantum key distribution protocol, with squeeze factor $\tilde{\Delta} = e^{-r} = 1/2$. The signal states squeezed in p and in q overlap with one another, preventing Eve from learning about one without disturbing the other.

is really needed for the protocol to be secure? A related question is, how must we choose the probability distributions $P_{\text{pos}}(q)$ and $P_{\text{mom}}(p)$ that govern the center of the squeezed state?

We will analyze the most favorable case, in which the squeezed states are Gaussian wave packets and the probability distributions are also Gaussian. We will begin again with a description of how the code is used for entanglement purification, but where Alice and Bob start with many copies of a Gaussian entangled pair of oscillators that is an approximate eigenstate of $q_A - q_B$ and $p_A + p_B$. If we imagine that Alice measures half of each pair before she sends the other half to Bob, then we obtain a protocol in which Alice sends imperfectly squeezed states governed by a particular probability distribution.

The initial Gaussian entangled state of the two oscillators is

$$\begin{aligned}
 |\psi(\Delta)\rangle_{AB} &= \frac{1}{\sqrt{\pi}} \int dq_A dq_B \exp \left[-\frac{1}{2} \Delta^2 \left(\frac{q_A + q_B}{2} \right)^2 \right] \\
 &\quad \times \exp \left[-\frac{1}{2} (q_A - q_B)^2 / \Delta^2 \right] |q_A, q_B\rangle \\
 &= \frac{1}{\sqrt{\pi}} \int dp_A dp_B \exp \left[-\frac{1}{2} \Delta^2 \left(\frac{p_A - p_B}{2} \right)^2 \right] \\
 &\quad \times \exp \left[-\frac{1}{2} (p_A + p_B)^2 / \Delta^2 \right] |p_A, p_B\rangle , \tag{22.55}
 \end{aligned}$$

where Δ^2 is real and positive. Since $|\psi(\Delta)\rangle_{AB}$ is actually invariant under

$$\Delta^2 \rightarrow 4/\Delta^2, \quad q_B \rightarrow -q_B, \quad p_B \rightarrow -p_B \quad (22.56)$$

we may assume without loss of generality (changing the sign of the position and momentum of Bob's oscillator if necessary), that $0 < \Delta^2 \leq 2$. In the limiting case $\Delta^2 = 2$, $|\psi(\Delta)\rangle_{AB}$ becomes the product of two oscillator vacuum states. For $\Delta^2 < 2$, it is an entangled state. The amount of entanglement shared between the oscillators, in "ebits," is defined as

$$E(\Delta) \equiv S(\rho_A) = -\text{tr } \rho_A \log_2 \rho_A, \quad (22.57)$$

(the Von Neumann entropy of Alice's density matrix $\rho_A = \text{tr}_B |\psi(\Delta)\rangle\langle\psi(\Delta)|$, and can be expressed as [20]

$$\begin{aligned} E(\Delta) = & (\cosh^2 r) \log_2(\cosh^2 r) \\ & - (\sinh^2 r) \log_2(\sinh^2 r), \end{aligned} \quad (22.58)$$

where

$$\Delta^2 \equiv 2e^{-2r}. \quad (22.59)$$

In this entangled state, if Alice measures the position of her oscillator and obtains the outcome q_A , she prepares for Bob the Gaussian state

$$\begin{aligned} |\psi(q_A)\rangle_B &= \frac{1}{(\pi\tilde{\Delta}^2)^{1/4}} \int dq_B \\ &\times \exp\left(-\frac{1}{2}(q_B - q_{B0})^2/\tilde{\Delta}^2\right) |q_B\rangle, \end{aligned} \quad (22.60)$$

where

$$q_{B0} = \left(\frac{1 - \frac{1}{4}\Delta^4}{1 + \frac{1}{4}\Delta^4} \right) q_A = \left(1 - \tilde{\Delta}^4 \right)^{1/2} q_A, \quad (22.61)$$

and

$$\tilde{\Delta}^2 = \frac{\Delta^2}{1 + \frac{1}{4}\Delta^4}. \quad (22.62)$$

The probability distribution for the outcome of Alice's measurement can be expressed as

$$P(q_A) = \frac{\tilde{\Delta}}{\sqrt{\pi}} \exp\left(-\tilde{\Delta}^2 q_A^2\right), \quad (22.63)$$

and we can easily see from eq. (22.54) that if Alice and Bob both measure q , then the difference of their outcomes is governed by the probability distribution

$$\text{Prob}(q_A - q_B) = \frac{1}{\sqrt{\pi\Delta^2}} \exp[-(q_A - q_B)^2/\Delta^2]. \quad (22.64)$$

Similar formulas apply if Alice and Bob measure p .

Suppose that Alice and Bob try to distill one good qubit from the imperfect entangled state $|\psi(\Delta)\rangle_{AB}$. They both measure the stabilizer generators, that is, the values of q and p modulo $\sqrt{\pi}$. Alice broadcasts her values, and Bob adjusts his values so that they agree with Alice's; thereby they obtain a pair of encoded qubits, which would have been in the state $|\bar{\phi}^+\rangle$ if the initial pair of oscillators had been a perfect EPR pair ($\Delta^2 = 0$). Then if Alice and Bob were to proceed to perform a complete Bell measurement on their encoded qubit pair, the probability p_Z that they would find $\bar{Z} \otimes \bar{Z} = -1$ is no worse than the probability that, if q_A and q_B were measured, the results would differ by more than $\sqrt{\pi}/2$, or

$$\begin{aligned} p_Z &\leq \frac{2}{\sqrt{\pi\Delta^2}} \int_{\sqrt{\pi}/2}^{\infty} dq e^{-q^2/\Delta^2} \\ &\leq \frac{2\Delta}{\pi} \exp(-\pi/4\Delta^2), \end{aligned} \quad (22.65)$$

and similarly for p_X (the probability that $\bar{X} \otimes \bar{X} = -1$). For the values of Δ that are typically of interest (*e.g.* $\Delta < 1$), the error probability is dominated by values of $q_A - q_B$ (or $p_A + p_B$) lying in the range $[\sqrt{\pi}/2, 3\sqrt{\pi}/2]$, so that the estimate of the error probability can be sharpened to

$$p_Z, p_X \sim \frac{2}{\sqrt{\pi\Delta^2}} \int_{\sqrt{\pi}/2}^{3\sqrt{\pi}/2} dq e^{-q^2/\Delta^2}. \quad (22.66)$$

After error correction and measurement in the encoded Bell basis, the initial bipartite pure state of two oscillators, with entanglement E given by eq. (22.57) and (22.59), is reduced to a bipartite mixed state, diagonal in the encoded Bell basis, with fidelity $F = (1 - p_Z)(1 - p_X)$; this encoded state has entanglement of formation [2]

$$E = H_2 \left(\frac{1}{2} + \sqrt{F(1 - F)} \right) \quad (22.67)$$

(where H_2 is the binary entropy function).

If Alice and Bob have a large number n of oscillators in the state $|\psi(\Delta)\rangle_{AB}$, they can carry out an entanglement distillation protocol based on the concatenation of the single-oscillator code with a binary CSS code, and they will be able to

distill qubits of arbitrarily good fidelity at a finite asymptotic rate provided that p_Z and p_X are both below 11%; from eq. (22.66) we find that this condition is satisfied for $\Delta < .784$ (which should be compared with the value $\Delta = \sqrt{2}$ corresponding to a product of two oscillators each in its vacuum state). Thus secure EPR key distribution is possible in principle with two-mode squeezed states provided that the squeeze parameter r satisfies $r > -\log_e(.784/\sqrt{2}) = .590$; from eq. (22.57) and (22.67), $\Delta = .784$ corresponds to $E = 1.19$ ebits carried by each oscillator pair, which is reduced by error correction and encoded Bell measurement to $E = .450$ ebits carried by each of the encoded Bell pairs.

Now consider the reduction of this entanglement distillation protocol to a protocol in which Alice prepares a squeezed state and sends it to Bob. In the squeezed-state scheme, Alice sends the state $|\psi(q_A)\rangle$ with probability $P(q_A)$. The width $\tilde{\Delta}$ of the state that Alice sends is related to the parameter Δ appearing in the estimated error probability according to

$$\Delta^{-2} = \tilde{\Delta}^{-2} \cdot \frac{1}{2}(1 + \sqrt{1 - \tilde{\Delta}^4}) . \quad (22.68)$$

The state Alice sends is centered not at q_A but at $q_{B0} = q_A \cdot (1 - \tilde{\Delta}^4)^{1/2}$. Nevertheless, in the squeezed state protocol that we obtain as a reduction of the entanglement distillation protocol, it is q_A rather than q_{B0} that Alice uses to extract a key bit, and whose value modulo $\sqrt{\pi}$ she reports to Bob. The error probability that is required to be below 11% to ensure security is the probability that error correction adjusts Bob's measurement outcome to a value that differs from q_A (not q_{B0}) by an odd multiple of $\sqrt{\pi}$. As we have noted, this error probability is below 11% for $\Delta < .784$, which (from eq. (22.62)) corresponds to $\tilde{\Delta} < .749$; this value should be compared to the value $\tilde{\Delta} = 1$ for an oscillator in its vacuum state. Thus, secure squeezed-state key distribution is possible in principle using single-mode squeezed states, provided that the squeeze parameter r defined by $\tilde{\Delta} = e^{-r}$ satisfies $r > -\log_e(.749) = .289$. When interpreted as suppression, relative to vacuum noise, of the quantum noise afflicting the squeezed observable, this amount of squeezing can be expressed as $10 \cdot \log_{10}(\tilde{\Delta}^{-2}) = 2.51$ dB.

The error rate is below 1% for $\tilde{\Delta} < .483$ ($\Delta < .486$), and drops precipitously for more highly squeezed states, *e.g.*, to below 10^{-6} for $\tilde{\Delta} \sim \Delta < .256$. For example, if the noise in the channel is weak, Alice and Bob can use the Gaussian squeezed state protocol with $\tilde{\Delta} \sim 1/2$ (see Fig. 22.2) to generate a shared bit via the q or p channel with an error rate ($\sim 1.2\%$) comfortably below 11%; thus the protocol is secure if augmented with classical binary error correction and privacy amplification.

Of course, if the channel noise is significant, there will be a more stringent limit on the required squeezing. Many kinds of noise (for instance, absorption of photons in an optical fiber) will cause a degradation of the squeezing factor.

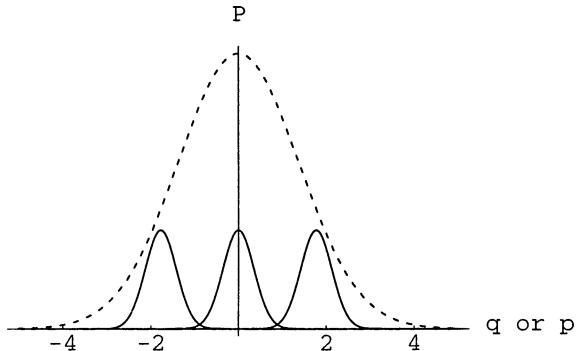


Figure 22.2 Probability distributions for the squeezed quantum key distribution protocol, with squeeze factor $\tilde{\Delta} = 1/2$. The dotted line is the probability distribution P (a Gaussian with variance $(1/2\tilde{\Delta}^2) \cdot (1 - \tilde{\Delta}^4)$) that Alice samples to determine the center of the squeezed signal that she sends. The solid lines are the probability distributions in position or momentum of the squeezed states (Gaussians with variance $\tilde{\Delta}^2/2$, shown with a different vertical scale than P) centered at $-\sqrt{\pi}$, 0, and $\sqrt{\pi}$. The intrinsic error probability due to imperfect squeezing (prior to binary error correction and privacy amplification) is 1.2%.

If this is the only consequence of the noise, the squeezing exiting the channel should still satisfy $\Delta < .784$ for the protocol to be secure, as we discuss in more detail in §7. Otherwise, the errors due to imperfect squeezing must be added to errors from other causes to determine the overall error rate.

So far we have described the case where the p states and the q states are squeezed by equal amounts. The protocol works just as well in the case of unequal squeezing, if we adjust the error correction procedure accordingly. Consider carrying out the entanglement distillation using the code with general parameter α rather than $\alpha = 1$. The error rates are unaffected if the squeezing in q and p is suitably rescaled, so that the width of the q and p states becomes

$$\Delta_q = \Delta \cdot \alpha, \quad \Delta_p = \Delta/\alpha. \quad (22.69)$$

In this modified protocol, Alice broadcasts the value of q modulo $\sqrt{\pi} \cdot \alpha$ or the value of p modulo $\sqrt{\pi}/\alpha$. Bob subtracts the value broadcast by Alice from his own measurement outcome, and then adjusts the difference he obtains to the nearest multiple of $\sqrt{\pi} \cdot \alpha$ or $\sqrt{\pi}/\alpha$. The key bit is determined by whether the multiple of $\sqrt{\pi} \cdot \alpha$, or $\sqrt{\pi}/\alpha$, is even or odd.

Thus, for example, the error rate sustained due to imperfect squeezing will have the same (acceptably small) value irrespective of whether Alice sends states with $\Delta_q = \Delta_p = 1/2$, or $\Delta_q = 1$ and $\Delta_p = 1/4$; Alice can afford to send coherent states about half the time if she increases the squeezing of her other transmissions by a compensating amount.

Can we devise a secure quantum key distribution scheme in which Alice always sends coherent states? To obtain, as a reduction of an entanglement distillation protocol, a protocol in which coherent states ($\tilde{\Delta} = 1$) are always transmitted, we must consider the case $\Delta^2 = 2$. But in that case, the initial state of Alice's and Bob's oscillators is a product state. Bob's value of q or p is completely uncorrelated with Alice's, and the protocol obviously won't work. This observation does not exclude secure quantum key distribution schemes using coherent states, but if they exist another method would be needed to prove the security of such schemes.

In general, the source that we obtain by measuring half of the entangled pair is biased. If Δ is not small compared to $\sqrt{\pi}$, then Alice is significantly more likely to generate a 0 than a 1 as her raw key bit. But as we have already discussed in §3.4, after error correction and privacy amplification, the protocol is secure if p_X and p_Z are both less than 11%. This result follows because the squeezed state protocol is obtained as a reduction of an entanglement distillation protocol.

7. LOSSES AND OTHER IMPERFECTIONS

The ideal BB84 quantum key distribution protocol is provably secure. But in practical settings, the protocol cannot be implemented perfectly, and the imperfections can compromise its security. (See [4] for a recent discussion.) For example, if the transmitted qubit is a photon polarization state carried by an optical fiber, losses in the fiber, detector inefficiencies, and dark counts in the detector all can impose serious limitations. In particular, if the photons travel a distance large compared to the attenuation length of the fiber, then detection events will be dominated by dark counts, leading to an unacceptably large error rate.

Furthermore, most present-day implementations of quantum cryptography use, not single photon pulses, but weak coherent pulses; usually the source “emits” the vacuum state, occasionally it emits a single photon, and with non-negligible probability it emits two or more photons. Quantum key distribution with weak coherent pulses is vulnerable to a “photon number splitting” attack, in which the eavesdropper diverts extra photons, and acquires complete information about their polarization without producing any detectable disturbance. A weaker pulse is less susceptible to photon number splitting, but increases the risk that the detector will be swamped by dark counts.

From a practical standpoint, quantum key distribution with squeezed states may not necessarily be better than BB84, but it is certainly different. Alice requires a source that produces a specified squeezed state on demand; fortunately, the amount of squeezing needed to ensure the security of the protocol is relatively modest. Bob uses homodyne detection to measure a specified quadrature

amplitude; this measurement may be less sensitive to detector defects than the single-photon measurement required in BB84.

But, as in the BB84 protocol, losses due to the absorption of photons in the channel will enhance the error rate in squeezed-state quantum key distribution, and so will limit the distance over which secure key exchange is possible. We study this effect by modeling the loss as a damping channel described by the master equation

$$\dot{\rho} = \Gamma \left(a\rho a^\dagger - \frac{1}{2}a^\dagger a\rho - \frac{1}{2}\rho a^\dagger a \right); \quad (22.70)$$

here ρ is the density operator of the oscillator, a is the annihilation operator, and Γ is the decay rate. Eq. (22.70) implies that

$$\frac{d}{dt} \langle a^\dagger k a^l \rangle_t = -\frac{1}{2}(k+l)\Gamma \langle a^\dagger k a^l \rangle_t, \quad (22.71)$$

where

$$\langle \mathcal{O} \rangle_t = \text{tr } (\mathcal{O}\rho(t)) \quad (22.72)$$

denotes the expectation value of the operator \mathcal{O} at time t . Integrating, we find

$$\langle a^\dagger k a^l \rangle_T = e^{-\frac{1}{2}(k+l)\Gamma T} \langle a^\dagger k a^l \rangle_0, \quad (22.73)$$

and so, by expanding in power series,

$$\langle : f(a^\dagger, a) : \rangle_T = \langle : f(\xi a^\dagger, \xi a) : \rangle_0, \quad \xi = e^{-\Gamma T/2} \quad (22.74)$$

where f is an analytic function, and $:f:$ denotes normal ordering (that is, in $:f(a^\dagger, a):$, all a^\dagger 's are placed to the left of all a 's).

In particular, by normal ordering and applying eq. (22.74), we find

$$\langle e^{i\beta q} \rangle_T = e^{-\frac{1}{4}(1-\xi^2)\beta^2} \langle e^{i\beta \xi q} \rangle_0, \quad (22.75)$$

where $q = (a + a^\dagger)/\sqrt{2}$ is the position operator. A similar formula applies to the momentum operator or any other quadrature amplitude. Eq. (22.75) shows that if the initial state at $t = 0$ is Gaussian (q is governed by a Gaussian probability distribution), then so is the final state at $t = T$ [10]. The mean $\langle q \rangle$ and variance Δq^2 of the initial and final distributions are related by

$$\begin{aligned} \langle q \rangle_T &= \xi \langle q \rangle_0, \\ \left(\Delta q_T^2 - \frac{1}{2} \right) &= \xi^2 \left(\Delta q_0^2 - \frac{1}{2} \right). \end{aligned} \quad (22.76)$$

Now let's revisit the analysis of §6., taking into account the effects of losses. We imagine that Alice prepares entangled pairs of oscillators in the state (22.54),

and sends one oscillator to Bob through the lossy channel; then they perform entanglement purification. This protocol reduces to one in which Alice prepares a squeezed state that is transmitted to Bob. In the squeezed-state protocol, Alice decides what squeezed state to send by sampling the probability distribution $P(q_A)$ given in eq. (22.63); if she chooses the value q_A , then she prepares and sends the state $|\psi(q_A)\rangle$ in eq. (22.59). When it enters the channel, this state is governed by the probability distribution

$$P(q_B|q_A) = \frac{1}{\tilde{\Delta}\sqrt{\pi}} \exp\left(-(q_B - q_{B0})^2/\tilde{\Delta}^2\right), \quad (22.77)$$

and when Bob receives the state this distribution has, according to eq. (22.76), evolved to

$$P'(q_B|q_A) = \frac{1}{\Delta'\sqrt{\pi}} \exp\left(-(q_B - q'_{B0})^2/\Delta'^2\right), \quad (22.78)$$

where

$$\begin{aligned} q'_{B0} &= \xi q_{B0} \equiv \xi(1 - \tilde{\Delta}^4)^{1/2} q_A, \\ \Delta'^2 &= \xi^2 \tilde{\Delta}^2 + (1 - \xi^2). \end{aligned} \quad (22.79)$$

By integrating over q_A in $P'(q_A, q_B) = P'(q_B|q_A) \cdot P(q_A)$, we can obtain the final marginal distribution for the difference $q_A - q_B$:

$$\begin{aligned} P'(q_A - q_B; \xi) &= \frac{1}{\Delta_\xi \sqrt{\pi}} \exp\left(-(q_A - q_B)^2/\Delta_\xi^2\right), \\ \Delta_\xi^{-2} &= \frac{\tilde{\Delta}^2}{1 + \xi^2 - 2\xi(1 - \tilde{\Delta}^4)^{1/2} + (1 - \xi^2)\tilde{\Delta}^2}, \end{aligned} \quad (22.80)$$

which generalizes eq. (22.68). We can express the damping factor ξ as

$$\xi = e^{-\kappa d/2}, \quad (22.81)$$

where d is the length of the channel and κ^{-1} is its attenuation length (typically of the order of 10 km in an optical fiber).

The protocol is secure if the error rate in both bases is below 11%; as in §6., this condition is satisfied for $\Delta_\xi < .784$. Thus we can calculate, as a function of the initial squeezing parameter $\tilde{\Delta}$, the maximum distance d_{\max} that the signal states can be transmitted without compromising the security of the protocol.

For $\tilde{\Delta} \ll 1$, we find

$$\kappa d_{\max} = (1.57) \cdot \tilde{\Delta} + O(\tilde{\Delta}^2). \quad (22.82)$$

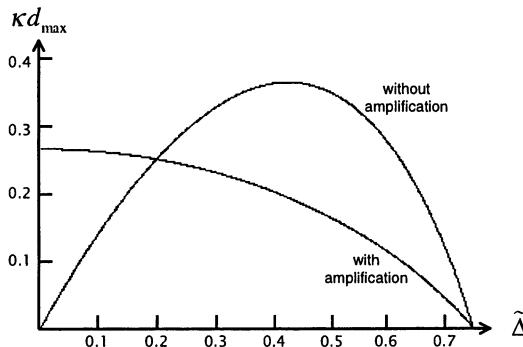


Figure 22.3 The effect of channel losses on the security of quantum key distribution using squeezed states. The maximum length κd_{max} of the channel (in units of the attenuation length) is plotted as a function of the width $\tilde{\Delta}$ of the squeezed state that enters the channel. For a longer channel, the error rate due to losses is too large and the proof of security breaks down. The curve labeled “with amplification” applies to the protocol in which the signal is amplified prior to detection in order to compensate for the losses; the curve labeled “without amplification” applies to the protocol in which the signal is not amplified.

Thus, the more highly squeezed the input signal, the *less* we can tolerate the losses in the channel. This feature, which sounds surprising on first hearing, arises because the amount of squeezing is linked with the size of the range in q_A that Alice samples. Errors are not unlikely if losses cause the value of q_B to decay by an amount comparable to $\sqrt{\pi}/2$. In our protocol, if the squeezed states have a small width $\tilde{\Delta}$, then the typical states prepared by Alice are centered at a large value $q_A \sim \tilde{\Delta}^{-1}$; therefore, a small *fractional* decay can cause an error.

On the other hand, even without losses, Alice needs to send states with $\tilde{\Delta} < .749$ to attain a low enough error rate, and as $\tilde{\Delta}$ approaches .749 from below, again only a small loss is required to push the error probability over 11%. Thus there is an intermediate value of $\tilde{\Delta}$ that optimizes the value of d_{max} , as shown in Fig. 22.3. This optimal distance,

$$\kappa d_{\text{max, opt}} \approx .367 , \quad (22.83)$$

is attained for $\tilde{\Delta} \sim .426$.

Our analysis so far applies if Alice and Bob have no prior knowledge about the properties of the channel. But if the loss $\xi^2 = e^{-\kappa d}$ is known accurately, they might achieve a lower error rate if Bob compensates for the loss by multiplying his measurement outcome by ξ^{-1} before proceeding with error

correction and privacy amplification. This amplification of the signal by Bob is entirely classical, but to analyze the security in this case, we may consider an entanglement purification scenario in which Bob applies a quantum amplifier to the signal before measuring. Since the quantum amplifier (which amplifies all quadrature amplitudes, not just the one that Bob measures) is noisier, the protocol will be no less secure if Bob uses a classical amplifier rather than a quantum one.

So now we consider whether entanglement purification will succeed, where the channel acting on Bob's oscillator in each EPR pair consists of transmission through the lossy fiber followed by processing in Bob's amplifier. If the error rate is low enough, the key will be secure even if the amplifier, as well as the optical fiber, are under Eve's control.

Bob's linear amplifier can be modeled by a master equation like eq. (22.70), but with a and a^\dagger interchanged, and where Γ is now interpreted as a rate of gain. The solution is similar to eq. (22.74), except the normal ordering is replaced by *anti*-normal ordering (all a 's are placed to the *left* of all a^\dagger 's), and with ξ^2 replaced by the gain $\xi^{-2} = e^{\Gamma T} \geq 1$. We conclude that the amplifier transforms a Gaussian input state to a Gaussian output state, and that the mean $\langle q \rangle$ and variance Δq^2 of the Gaussian position distribution are modified according to

$$\begin{aligned}\langle q \rangle &\rightarrow \xi^{-1} \langle q \rangle , \\ \Delta q^2 &\rightarrow \xi^{-2} \Delta q^2 + \frac{1}{2} (\xi^{-2} - 1) .\end{aligned}\quad (22.84)$$

Other quadrature amplitudes are transformed similarly.

Now suppose that a damping channel with loss ξ^2 is followed by an amplifier with gain ξ^{-2} . Then the mean of the position distribution is left unchanged, but the variance evolves as

$$\begin{aligned}\Delta q^2 &\rightarrow \xi^{-2} \left(\xi^2 \Delta q^2 + \frac{1}{2} (1 - \xi^2) \right) + \frac{1}{2} (\xi^{-2} - 1) \\ &= \Delta q^2 + (\xi^{-2} - 1) .\end{aligned}\quad (22.85)$$

For this channel, the probability distribution governing $q_A - q_B$ is again a Gaussian as in eq. (22.79), but now its width is determined by

$$(\Delta_\xi)_{\text{amp}}^{-2} = \frac{\frac{1}{2} \tilde{\Delta}^2}{1 - (1 - \tilde{\Delta}^4)^{1/2} + (\xi^{-2} - 1) \tilde{\Delta}^2} .\quad (22.86)$$

Error rates in the q and p bases are below 11%, and the protocol is provably secure, for $(\Delta_\xi)_{\text{amp}} < .784$.

By solving $(\Delta_\xi)_{\text{amp}} = .784$, we can find the maximum distance d (where $\xi^{-2} = e^{\kappa d}$) for which our proof of security holds; the result is plotted in

Fig. 22.3. When the squeezed input is narrow, $\tilde{\Delta} \ll 1$, the solution becomes

$$\xi^{-2} \equiv \exp(\kappa d_{\max}) = 1.307 + O(\tilde{\Delta}^2), \quad (22.87)$$

or

$$\kappa d_{\max} \approx .268. \quad (22.88)$$

Comparing the two curves in Fig. 22.3, we see that the protocol with amplification remains secure out to longer distances than the protocol without amplification, *if* the input is highly squeezed. In that case, the error rate in the protocol without amplification is dominated by the decay of the signal, which can be corrected by the amplifier. But if the input is less highly squeezed, then the protocol without amplification remains secure to longer distances. In that case, the nonzero width of the signal state contributes significantly to the error rate; the amplifier noise broadens the state further.

With more sophisticated protocols that incorporate some form of quantum error correction, continuous-variable quantum key distribution can be extended to longer distances. For example, if Alice and Bob share some noisy pairs of oscillators, they can purify the entanglement using protocols that require two-way classical communication [15, 7]. After pairs with improved fidelity are distilled, Alice, by measuring a quadrature amplitude in her laboratory, prepares a squeezed state in Bob's; the key bits can be extracted using the same error correction and privacy amplification schemes that we have already described.

Our proof of security applies to the case where squeezed states are carried by a lossy channel (assuming a low enough error rate), because this scenario can be obtained as a reduction of a protocol in which Alice and Bob apply entanglement distillation to noisy entangled pairs of oscillators that they share. More generally, the proof applies to any imperfections that can be accurately modeled as a quantum operation that acts on the shared pairs before Alice and Bob measure them. As one example, suppose that when Alice prepares the squeezed state, it is not really the q or p squeezed state that the protocol calls for, but is instead slightly rotated in the quadrature plane. And suppose that when Bob performs his homodyne measurement, he does not really measure q or p , but actually measures a slightly rotated quadrature amplitude. In the entanglement-distillation scenario, the imperfection of Alice's preparation can be modeled as a superoperator that acts on her oscillator before she makes a perfect quadrature measurement, and the misalignment of Bob's measurement can likewise be modeled by a superoperator acting on his oscillator before he makes a perfect quadrature measurement. Therefore, the squeezed state protocol with this type of imperfect preparation and measurement is secure, as long as the error rate is below 11% in both bases. Of course, this error rate

includes both errors caused by the channel and errors due to the imperfection of the preparation and measurement.

We also recall that in the protocols of §5., Alice's preparation and Bob's measurement were performed to m bits of accuracy. In the entanglement distillation scenario, this finite resolution can likewise be well modeled by a quantum operation that shifts the oscillators by an amount of order 2^{-m} before Alice and Bob perform their measurements. Thus the proof applies, with the finite resolution included among the effects contributing to the permissible 11% error rate. The finite accuracy causes trouble only when Alice's and Bob's results lie a distance apart that is within about 2^{-m} of $\sqrt{\pi}/2$; thus, just a few bits of accuracy should be enough to make this additional source of error quite small.

8. CONCLUSIONS

We have described a secure protocol for quantum key distribution based on the transmission of squeezed states of a harmonic oscillator. Conceptually, our protocol resembles the BB84 protocol, in which single qubit states are transmitted. The BB84 protocol is secure because monitoring the observable Z causes a detectable disturbance in the observable X , and vice versa. The squeezed state protocol is secure because monitoring the observable q causes a detectable disturbance in the observable p , and vice versa. Security is ensured even if the adversary uses the most general eavesdropping strategies allowed by the principles of quantum mechanics.

In secure versions of the BB84 scheme, Alice's source should emit single-photons that Bob detects. Since the preparation of single-photon states is difficult, and photon detectors are inefficient, at least in some settings the squeezed-state protocol may have practical advantages, perhaps including a higher rate of key production. Squeezing is also technically challenging, but the amount of squeezing required to ensure security is relatively modest.

The protocol we have described in detail uses each transmitted oscillator to carry one raw key bit. An obvious generalization is a protocol based on the code with stabilizer generators given in eq. (22.8), which encodes a d -dimensional protected Hilbert space in each oscillator. Then a secure key can be generated more efficiently, but more squeezing is required to achieve an acceptable error rate.

Our protocols, including their classical error correction and privacy amplification, are based on CSS codes: each of the stabilizer generators is either of the “ q ”-type (the exponential of a linear combination of n q 's) or of the “ p ”-type (the exponential of a linear combination of n p 's). The particular CSS codes that we have described in detail belong to a restricted class: they are *concatenated* codes such that each oscillator encodes a single qubit, and then a block of

those single-oscillator qubits are assembled to encode k better protected qubits using a binary $[[n, k, d]]$ stabilizer code. There are more general CSS codes that embed k protected qubits in the Hilbert space of n oscillators but do not have this concatenated structure [8]; secure key distribution protocols can be based on these too. The quantum part of the protocol is still the same, but the error correction and privacy amplification make use of more sophisticated close packings of spheres in n dimensions.

We analyzed a version of the protocol in which Alice prepares Gaussian squeezed states governed by a Gaussian probability distribution. The states, and the probability distribution that Alice samples, need not be Gaussian for the protocol to be secure. However, for other types of states and probability distributions, the error rates might have to be smaller to ensure the security of the protocol.

Our proof of security applies to a protocol in which the squeezed states propagate through a lossy channel, over a distance comparable to the attenuation length of the channel. To extend continuous-variable quantum key distribution to much larger distances, quantum error correction or entanglement distillation should be invoked.

Strictly speaking, the security proof we have presented applies if Alice's state preparation (including the probability distribution that she samples) can be exactly realized by measuring half of an imperfectly entangled state of two oscillators. The protocol remains secure if Alice's source can be well approximated in this way. Our proof does not work if Alice occasionally sends two identically prepared oscillators when she means to send just one; the eavesdropper can steal the extra copy, and then the privacy amplification is not guaranteed to reduce the eavesdropper's information to an exponentially small amount.

Acknowledgments

We thank Andrew Doherty, Steven van Enk, Jim Harrington, Jeff Kimble, and especially Hoi-Kwong Lo for useful discussions and comments. This work has been supported in part by the Department of Energy under Grant No. DE-FG03-92-ER40701, and by DARPA through the Quantum Information and Computation (QUIC) project administered by the Army Research Office under Grant No. DAAH04-96-1-0386. Some of this work was done at the Aspen Center for Physics. This paper first appeared in Physical Review A

Notes

1. We implicitly assume that Eve uses a strategy that passes the verification test with nonnegligible probability, so that the rate of key generation is not exponentially small. If, for example, Eve were to intercept all qubits sent by Alice and resend them to Bob, then she would almost certainly be detected, and key bits would not be likely to be generated. But in the rare event that she is not detected and some key bits are generated, Eve would know a lot about them.

2. This bound is not tight. It applies if the sample of M pairs is chosen from the population of N *with replacement*. In fact the sample is chosen without replacement, which suppresses the fluctuations. A better bound was quoted by Shor and Preskill [18].

References

- [1] Bennett, C. H., and G. Brassard (1984), “Quantum cryptography: Public-key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India), pp. 175–179; C. H. Bennett and G. Brassard (1985), “Quantum public key distribution,” IBM Technical Disclosure Bulletin **28**, 3153–3163.
- [2] Bennett, C. H., D. P. DiVincenzo, J. A. Smolin and W. K. Wootters (1996), “Mixed state entanglement and quantum error correction,” Phys. Rev. A **54**, 3824–3851, quant-ph/9604024.
- [3] Biham, E., M. Boyer, P. O. Boykin, T. Mor and V. Roychowdhury (2000), “A proof of the security of quantum key distribution,” in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pp 715–724. New York: ACM Press, quant-ph/9912053.
- [4] Brassard, G., N. Lütkenhaus, T. Mor, and B. C. Sanders (2000), “Limitations on practical quantum cryptography,” Phys. Rev. Lett. **85**, 1330, quant-ph/9911054.
- [5] Braunstein, S. (1998), “Error correction for continuous quantum variables,” Phys. Rev. Lett. **80**, 4084, quant-ph/9711049.
- [6] Calderbank, A. R., and P. W. Shor (1996), “Good quantum error correcting codes exist,” Phys. Rev. A **54**, 1098–1105, quant-ph/9512032.
- [7] Duan, L. M., G. Giedke, J. I. Cirac, and P. Zoller (1999), “Entanglement purification of Gaussian continuous variable quantum states,” quant-ph/9912017; L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller (2000), “Physical implementation for entanglement purification of Gaussian continuous variable quantum systems,” quant-ph/0003116.
- [8] Gottesman, D., A. Kitaev, and J. Preskill (2000), “Encoding a qudit in an oscillator,” quant-ph/0008040.
- [9] Hillery, M. (1999), “Quantum cryptography with squeezed states,” quant-ph/9909006.

- [10] Holevo, A. S. (1998), “Sending quantum information with Gaussian states,” quant-ph/9809022.
- [11] Lloyd, S., and J. E. Slotine (1998), “Analog quantum error correction,” Phys. Rev. Lett. **80**, 4088, quant-ph/9711021.
- [12] Lo, H.-K., and H. F. Chau (1999), “Unconditional security of quantum key distribution over arbitrarily long distances,” Science **283**, 2050–2056, quant-ph/9803006.
- [13] Mayers, D. (1996), “Quantum key distribution and string oblivious transfer in noisy channels,” *Advances in Cryptology—Proceedings of Crypto ’96*, pp. 343–357. New York: Springer-Verlag
- [14] Mayers, D. (1998), “Unconditional security in quantum cryptography,” J. Assoc. Comput. Mach. (to be published), quant-ph/9802025.
- [15] Parker, S., S. Bose, and M. B. Plenio (2000), “Entanglement quantification and purification in continuous variable systems,” Phys. Rev. A **61**, 32305, quant-ph/9906098.
- [16] Ralph, T. C. (1999), “Continuous variable quantum cryptography,” quant-ph/9907073; “Security of continuous variable quantum cryptography,” quant-ph/0007024.
- [17] Reid, M. D. (1999), “Quantum cryptography using continuous variable Einstein-Podolsky-Rosen correlations and quadrature phase amplitude measurements,” quant-ph/9909030.
- [18] Shor, P. W., and J. Preskill (2000), “Simple proof of security of the BB84 quantum key distribution protocol,” Phys. Rev. Lett. **85**, 441–444, quant-ph/0003004.
- [19] Steane, A. M. (1996), “Multiple particle interference and error correction,” Proc. Roy. Soc. Lond. A **452**, 2551–2577, quant-ph/9601029.
- [20] van Enk, S. J. (1999), “A discrete formulation of teleportation of continuous variables,” Phys. Rev. A **60**, 5095, quant-ph/9905081.

Chapter 23

EXPERIMENTAL DEMONSTRATION OF QUANTUM DENSE CODING AND QUANTUM CRYPTOGRAPHY WITH CONTINUOUS VARIABLES

Kunchi Peng, Qing Pan, Jing Zhang and Changde Xie

The State Key Laboratory of Quantum Optics and Quantum Optics Devices

Institute of Opto-Electronics

Shanxi University

Taiyuan 030006

P.R.China

Abstract In this paper we will present the experimental demonstrations of quantum dense coding and quantum cryptography using continuous electromagnetic field with Einstein-Podolsky-Rosen(EPR) correlations. The bright EPR optical beams with the quantum correlations between the amplitude and phase quadratures are produced from a nondegenerate optical parametric amplifier. The direct detection technology of the Bell-state is utilized in the measurements of the quantum correlations and the signals modulated on the quadratures instead of usual homodyne detection. Usability of experimentally accessible squeezed-state entanglements, high efficiencies of bit transmission and information detection, relatively straightforward systems and operating procedures, and security directly provided by quantum correlations make the presented schemes valuable to be applied to the developing quantum information science.

1. INTRODUCTION

Recently, more and more investigation interests in quantum information science have focus on exploiting the quantum system which possesses continuous spectra [1-19]. The successful experiments on the quantum teleportation [20] and quantum dense coding [21] using EPR correlations of continuous electromagnetic fields provided possible technologies for quantum information processing based on continuous variables. High bit transmission rates and

high detection efficiency are the key advantages of continuous variable systems better than discrete systems.

In this paper we will present the experimental schemes and results on continuous variable quantum dense coding and quantum cryptography. The experimental technologies for the generation of EPR correlated beams and the detection of the Bell-state will be described firstly.

2. GENERATION OF BRIGHT EPR BEAMS

It has been theoretically and experimentally demonstrated that EPR beams with correlated amplitude quadratures and anticorrelated phase quadratures or correlated phase quadratures and anticorrelated amplitude quadratures may be produced by a continuous nondegenerate optical parametric amplifier(NOPA) operating at amplification or deamplification [21-26]. For the former, the variances of the difference of amplitude quadratures $\langle \delta(X_1 - X_2)^2 \rangle$ and the sum of phase quadratures $\langle \delta(Y_1 + Y_2)^2 \rangle$ are both smaller than the shot noise limit (SNL) defined by the vacuum fluctuation. For the later, there are inverse correlations between the quadratures, that is

$$\langle \delta(X_1 + X_2)^2 \rangle < SNL \quad \text{and} \quad \langle \delta(Y_1 - Y_2)^2 \rangle < SNL \quad (23.1)$$

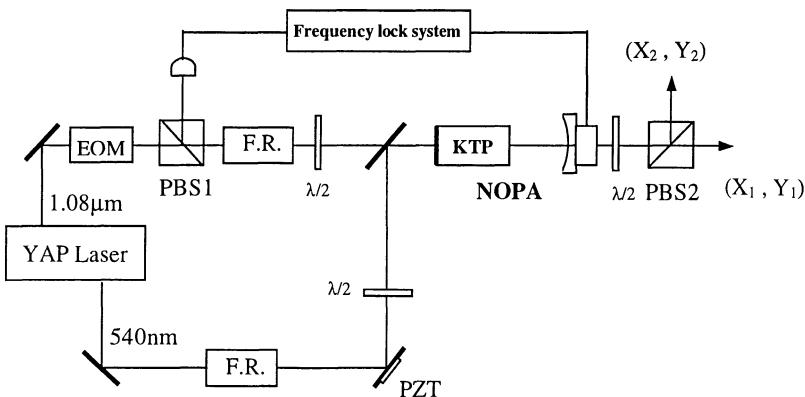


Figure 23.1 Experimental setup for the generation of EPR beams: YAP-Nd:YAlO₃, F.R.-Faraday Rotator, EOM-Electric Optical modulator, PBS-polarizing beam splitter.

The schematic of experimental setup for the generation of EPR beams is shown in Fig. 23.1. The entangled EPR beam is generated from a NOPA consisting of an a-cut type II KTP (KTiOPO₄, Potassium Titanyl Phosphate)

crystal (10mm long), the front face of which is coated to be used as the input coupler(the transmission>95% at 540nm wavelength and 0.5% at 1080nm) and the other face is coated with the dual-band antireflection at both 540nm and 1080nm, as well as a concave mirror of 50mm-curvature radius, which is used as the output coupler of EPR beam at 1080nm (the transmission of 5% at 1080 and high reflectivity at 540nm). The output coupler is mounted on a piezoelectric transducer to lock actively the cavity length on resonance with the injected seed wave at 1080nm using the FM sideband technique. By fine tuning the crystal temperature the birefringence between signal and idler waves in KTP is compensated and the simultaneous resonance in the cavity is reached. The process of adjusting temperature to meet double resonance can be monitored with an oscilloscope during scanning the length of cavity. Once the double resonance is completed the NOPA is locked on the frequency of the injected seed wave [25]. The measured finesse, the free spectral range, and the line-width of the parametric oscillator are 110, 2.8G, and 26 MHz, respectively. The pump source of NOPA is a home-made all-solid-state intracavity frequency-doubled and frequency-stabilized CW ring Nd:YAP (Nd:YAlO₃, Yttrium-Aluminum-Perovskite) laser [27]. The output second-harmonic wave at 540nm and the leaking fundamental wave at 1080nm from the laser serve as the pump light and the seed wave respectively. The laser-diode pumped all-solid-state laser and the semi-monolithic F-P configuration of the parametric cavity ensure the stability of system, so the frequency and phase of light waves can be well-locked during the experiments.

The NOPA is pumped by the harmonic wave at 540nm, that is controlled just below the oscillation threshold of the NOPA, and the polarization of that is along the b axis of the KTP crystal. Due to the large transmission (>95%) of input coupler at 540nm, the pump field only passes the cavity twice without resonating. After the seed beam at 1080nm polarized at 45° relative to the b axis of the KTP crystal is injected into the cavity, it is decomposed to signal and idler seed waves with identical intensity and the orthogonal polarization along the b and c axes, respectively, which correspond to the vertical and horizontal polarization. The temperature of KTP crystal placed in a special designed oven is actively controlled around the temperature for achieving type II noncritical phase matching (63°C) with a broad full width of about 30°C [25]. An electronics feedback circuit is employed to stabilize actively the temperature of crystal to a few mK.

Locking the relative phase between the pump laser and the injected seed wave of NOPA to $2n\pi$ or $(2n+1)\pi$, where n is integer, to enforce the NOPA operating at amplification or deamplification, the entangled EPR beam with the quantum correlation of amplitude(or phase) quadratures and the quantum anticorrelation of phase(or amplitude) quadratures was generated [21,25]. The two halves of the EPR beams are just the signal and idler modes of the subharmonic wave field

produced from type II parametric down conversion, thus they have orthogonal polarizations originally. The output signal and idler beams are separated by a polarizing-beam-splitter (PBS2) to be a pair of EPR beams, (X_1, Y_1) and (X_2, Y_2) , which possess the feature of nonlocal quantum entanglement of the amplitude and phase quadratures.

3. DIRECT MEASUREMENT OF BELL-STATES

The homodyne detection is extensively applied in phase-sensitive measurements of electromagnetic field quadratures and has been successfully used in the quantum teleportation experiment of continuous variables [20]. However, for performing the homodyne detection the local oscillator(LO) is needed and the well spatial and temporal mode matching between the LO and the detected beam is required, which make some troubles to experimental implementation. For passing by the troubles we proposed a direct detection scheme of Bell-state [28] and applied it to accomplish the quantum dense coding [21] and the quantum cryptography [29] with continuous variables.

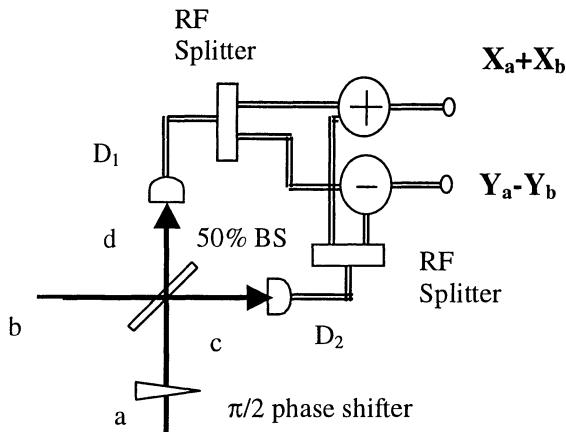


Figure 23.2 Direct measurement of the Bell state. BS: 50% beam splitter. D1 and D2: detectors.

Fig. 23.2 is the diagram of the direct detection system. Two bright coherent beams with identical intensities are expressed by the annihilation operators a and b . A phase shift of $\pi/2$ is imposed on beam a , and then the beams are mixed on a 50% beamsplitter. The resulting output beams c and d are given by:

$$c = \frac{\sqrt{2}}{2}(a + ib); \quad d = \frac{\sqrt{2}}{2}(a - ib). \quad (23.2)$$

We define upper-case operators in the rotating frame about the center frequency ω_0 ,

$$O(t) = o(t)e^{i\omega_0 t}, \quad (23.3)$$

with $O = [a, b, c, d]$ and $o = [\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}]$. By the Fourier transformation we have

$$O(\Omega) = \frac{1}{\sqrt{2\pi}} \int dt O(t) e^{-i\Omega t}. \quad (23.4)$$

The fields are now described as functions of the modulation frequency Ω . Thus we can consider any field as a carrier $O(0)$ oscillating at frequency ω_0 with an average value equal to the steady state field, surrounded by “noise side-bands” $O(\Omega)$ oscillating at frequency $\omega_0 \pm \Omega$ with zero average values. The amplitude and phase quadrature can be written as

$$X_O(\Omega) = O(\Omega) + O^+(-\Omega); \quad Y_O(\Omega) = \frac{1}{i}[O(\Omega) - O^+(-\Omega)], \quad (23.5)$$

The two bright output beams can be directly detected by D_1 and D_2 . The discussed photocurrents are normalized with the average value of the field. The normalized output photocurrents spectra are given by

$$\begin{aligned} \hat{i}_c(\Omega) &= \frac{1}{2}(X_a(\Omega) + Y_a(\Omega) - Y_b(\Omega) + X_b(\Omega)) \\ \hat{i}_d(\Omega) &= \frac{1}{2}(X_a(\Omega) - Y_a(\Omega) + Y_b(\Omega) + X_b(\Omega)) \end{aligned} \quad (23.6)$$

The Eq. (23.6) shows that the photocurrent of each arm of the 50% beam-splitter consists of two parts, part one (term 1 and term 4) is self terms of two input fields $X_a(\Omega)$ and $X_b(\Omega)$ at the beam splitter, the part 2 comprises the interference terms (2 and 3) including phase quadratures $Y_a(\Omega)$ and $Y_b(\Omega)$ deriving from the $\pi/2$ phase shift. Comparing \hat{i}_c and \hat{i}_d in Eq. (23.6), it is obvious that the self terms of two arms are correlated (or in phase), and the interference terms are anticorrelated (or out of phase). Each of photocurrents is divided into two parts through the RF power splitter. The sum and difference of the divided photocurrents are

$$\begin{aligned} \hat{i}_+(\Omega) &= \frac{1}{\sqrt{2}}(\hat{i}_c(\Omega) + \hat{i}_d(\Omega)) = \frac{1}{\sqrt{2}}(X_a(\Omega) + X_b(\Omega)) \\ \hat{i}_-(\Omega) &= \frac{1}{\sqrt{2}}(\hat{i}_c(\Omega) - \hat{i}_d(\Omega)) = \frac{1}{\sqrt{2}}(Y_a(\Omega) - Y_b(\Omega)) \end{aligned} \quad (23.7)$$

We can see that the sum \hat{i}_+ of photocurrents of two arms c, d only leaves the self terms which include the amplitude quadrature of the signal field \hat{a} and \hat{b} ; the difference photocurrent \hat{i}_- leaves the interference terms, which gives the information of their phase quadratures. Thus a combined Bell-state measurement of beams and is achieved with this simple self-homodyne detector. In our dense coding and cryptography experiments, the detected fields \hat{a} and \hat{b} are the signal and idler modes, (X_1, Y_1) and (X_2, Y_2) , of the output field from the NOPA operating at deamplification, so there are quantum anticorrelation and correlation between their amplitude and phase quadratures (see the inequalities (23.1)).

The correlations measured by self-homodyne detector between the quadrature-phase amplitudes of the two halves of EPR beam are show in Fig. 23.3. Both variances of $\langle \delta(X_1 + X_2)^2 \rangle$ (Fig. 23.3(a)) and $\langle \delta(Y_1 - Y_2)^2 \rangle$ (Fig. 23.3 (b)) measured directly are ~ 4 dB below that of the SNL (considering the electronics noise that is 8dB below the SNL, the actual fluctuation should be ~ 5.4 dB below that of the SNL). The product of the correspondent conditional variances of the EPR beam is $\langle \delta(X_1 + X_2)^2 \rangle \langle \delta(Y_1 - Y_2)^2 \rangle = 0.63$. The bright EPR beam of $\sim 70\mu\text{mW}$ (the correspondent photon-number flow is about $3.8 \times 10^{14}\text{s}^{-1}$) was obtained at the following operation parameters of NOPA: the pump power 150mW just below the power of the oscillation threshold of 175mW and the polarization of that was along the b axis of the KTP crystal. The power of the injected seed wave was 10mW before entering the input coupler of the cavity and that was polarized at 45° relative to the b axis.

4. QUANTUM DENSE CODING

The experimental diagram of the quantum dense coding is shown in Fig. 23.4. The two halves (1 and 2) of the EPR entangled beam were distributed to the sender Alice and the receiver Bob, respectively. At Alice the classical amplitude and phase signals were modulated on the one half of EPR beam (beam 1), which led to a displacement signal sent via the quantum channel. Since each half of EPR beam had huge noise individually, for perfect EPR entanglement $\langle \delta(X_{1(2)})^2 \rangle \rightarrow \infty$ and $\langle \delta(Y_{1(2)})^2 \rangle \rightarrow \infty$, the signal to noise ratios in the beam 1 for both amplitude and phase signals tended to zero, so no one other than Bob can gain any signal information from the modulated beam under ideal condition. At Bob, the signals were decoded with the aid of the other half of the EPR beam (beam 2), which was combined with the modulated first half of EPR beam (beam 1) on a 50% beam-splitter, in our experiment which consisted of two polarized-beamsplitters and a half-wave-plate [30], and, before combination, a $\pi/2$ phase shift was imposed between them according to the requirement of direct measurement of Bell-State [28]. The bright outcomes from two ports of the beamsplitter were directly detected by a pair of photodiodes D1 and D2

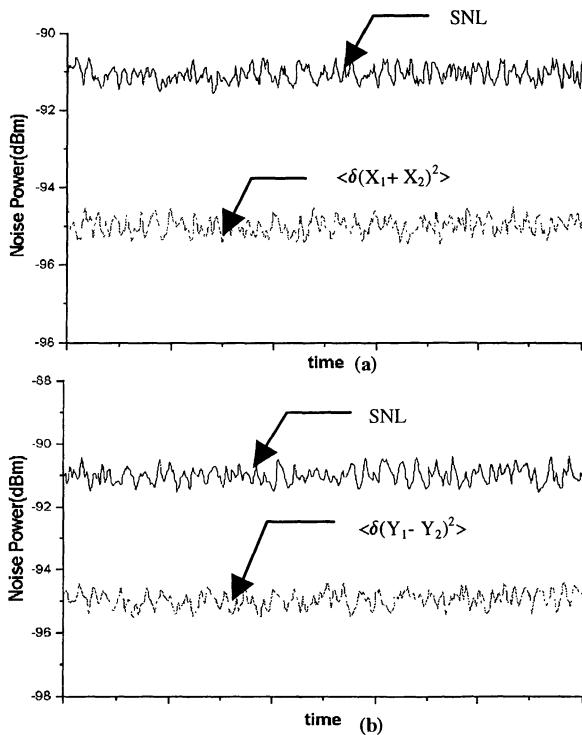


Figure 23.3 Spectral densities of photocurrent fluctuations $\langle \delta(X_1 + X_2)^2 \rangle$ (a) and $\langle \delta(Y_1 + Y_2)^2 \rangle$ (b), SNL-the Shot Noise Limit. Acquisition parameters: radio frequency (rf) $\Omega/2\pi=2\text{MHz}$, resolution bandwidth $\Delta\Omega/2\pi=30\text{KHz}$, Video bandwidth 0.1KHz, the electronics noise is 8dB below the SNL.

(ETX500 InGaAs), and then each photocurrent of D1 and D2 was divide into two parts through the power splitters. The sum and difference of the divided photocurrent were nothing else but the transmitted amplitude and phase signals from Alice to Bob, which are expressed by [28]

$$\begin{aligned}\hat{i}_+(\Omega) &= \frac{1}{\sqrt{2}}(X_1(\Omega) + X_2(\Omega) + X_s(\Omega)) \\ \hat{i}_-(\Omega) &= \frac{1}{\sqrt{2}}(Y_1(\Omega) - Y_2(\Omega) + Y_s(\Omega)).\end{aligned}\quad (23.8)$$

where $X_s(\Omega)$ and $Y_s(\Omega)$ are the modulated amplitude and phase signals on the first half of EPR beam at the sender Alice. With perfect EPR entangled beam $\langle X_1(\Omega) + X_2(\Omega) \rangle \rightarrow 0$ and $\langle Y_1(\Omega) - Y_2(\Omega) \rangle \rightarrow 0$, Eqs. (23.7) and (23.8) are simplified:

$$\hat{i}_+(\Omega) = \frac{1}{\sqrt{2}}\{X_s(\Omega)\} \quad (23.9)$$

$$\hat{i}_-(\Omega) = \frac{1}{\sqrt{2}}\{Y_s(\Omega)\}. \quad (23.10)$$

It means that under ideal conditions, the signals $X_s(\Omega)$ and $Y_s(\Omega)$ encoded on the amplitude quadrature and phase quadrature of beam 1 are simultaneously retrieved at the receiver Bob without any error. In general, the both encoded signals will be recovered with a sensitivity beyond that of the SNL when the beam 1 and beam 2 are quantum entangled. In fact, the sum of the amplitude quadratures between the two halves of EPR beam commutes with the difference of its phase quadrature, therefore the detected variances in them can be below that of the SNL simultaneously, and not violate the uncertainty principle [24]. Fig. 23.5 shows the directly measured amplitude [Fig. 23.5(a)] and phase [Fig. 23.5(b)] signals at Bob, which are the signals of 2MHz modulated on the first half of EPR beam (beam 1) by the amplitude and phase modulators at Alice. It can be seen that the original signals are retrieved with the high signal to noise ratio of ~ 4 dB and ~ 3.6 dB beyond that of the SNL under the help of the other half of EPR beam (beam 2)(accounting for the electronics noise of ~ 8 dB below the SNL, the actual value should be ~ 5.4 dB and ~ 4.8 dB respectively). Compared with the previously completed sub shot noise limit optical measurements and quantum non-demolition measurements for a signal, in which the squeezed state light have been applied, our experiments have achieved the simultaneous measurements of two signals modulated on the amplitude and phase quadratures respectively with the precision beyond that of the SNL by means of exploiting the EPR entanglement. Although when sending and modulating two quadratures of a coherent beam a factor of two in channel capacity may also be gained, the signal-to-noise ratios of measurements are not able to breakthrough the SNL.

As well-discussed in Ref. [15], in which a signal is transmitted via two quantum channels of EPR pair, in our scheme the individual signal channel

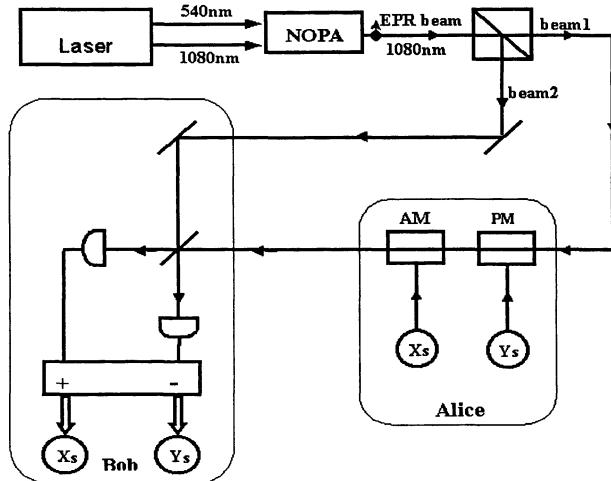


Figure 23.4 Schematic of the experimental apparatus for dense coding for continuous variables. Two bits of classical information X_s and Y_s are encoded on the amplitude and phase quadratures of a half of EPR beam (beam 1) at Alice, then are decoded by the other half of EPR beam (beam 2) at Bob.

has a high degree of immunity to unauthorized interception since very low signal-to-noise ratios. Fig. 23.6 demonstrates the security of the signal channel against eavesdropping, where the trace 23.6(a) is the fluctuation spectrum of the first half of EPR beam 1 with the modulated signals measured individually at Bob while the other half of EPR beam is not applied, which is ~ 4.4 dB (after the correction to the electronics noise floor, it should actually be ~ 5.4 dB) above the SNL. It is obvious that no signal can be extracted since the signals are totally submerged in the large noise background.

5. QUANTUM CRYPTOGRAPHY

In recent years the cryptographic schemes employing continuous coherent and nonclassical light fields have been suggested [6-19]. A lot of interest has arisen in continuous variable quantum cryptography (CVQC) with EPR beams due to that the experimental demonstrations of quantum teleportation [20] and quantum dense coding [21] for continuous variables (CV). J.Kimble and his colleagues completed the quantum communication of dual channels with correlated nonclassical states of light [15]. However in this case, an eavesdropper (Eve) could simultaneously access the signal and idler beams without the

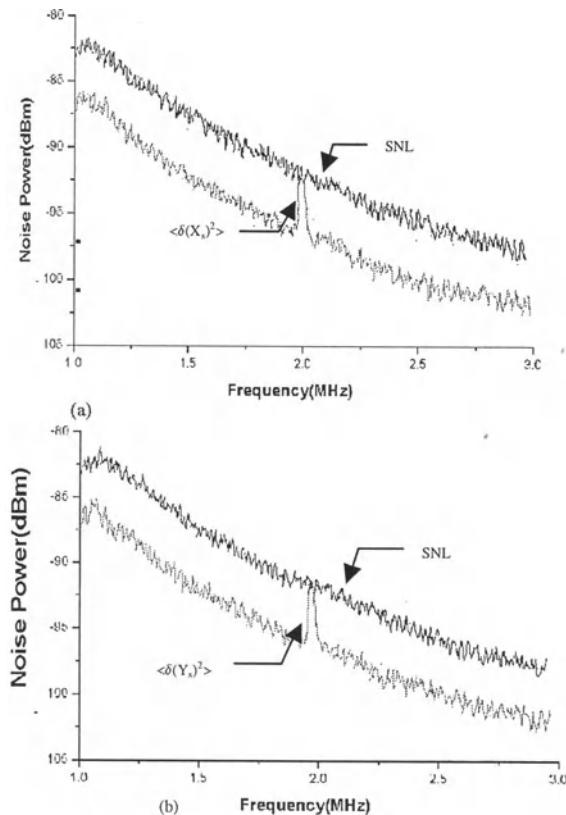


Figure 23.5 Measured amplitude (a) and phase signal (b) at Bob, when EPR beam 1 is phase and amplitude modulated at 2MHz at Alice. SNL—the Shot Noise Limit (black line). Acquisition parameter: measured frequency range 1.0MHz-3.0MHz, resolution bandwidth 30KHz, video bandwidth 0.1KHz, the electronics noise is 8dB below the SNL.

knowledge of the legitimate receiver. The first experimental demonstration on CVQC has been achieved by Peng's group at very recent date [29].

In Ref. [29], a scheme using the nonlocal correlation of bright EPR beams to implement QC is presented, in which the source generating EPR beams is placed inside the receiver, only one of the EPR correlated beams (signal beam) is sent to Alice and other one (idler beam) is retained by Bob. The security of the presented system is directly provided by EPR correlations between amplitude and phase quadratures of continuous bright optical beams and no-cloning of quantum fluctuations. Any random choice on measurements of quadratures are not needed and the sender encodes the key string with predetermined binary

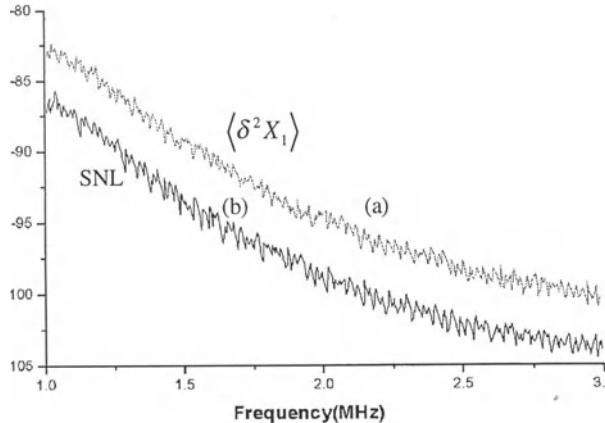


Figure 23.6 Spectral density of photocurrent fluctuations of beam 1 with the modulation signals (trace(a)), the modulated signals are submerged in the noise background. SNL—the Shot Noise Limit (trace(b)) Acquisition parameter: measured frequency range 1.0MHz-3.0MHz, resolution bandwidth 30KHz, vides bandwidth 0.1KHz; the electronics noise is 5.6dB below the SNL.

bits [13]. All transmitted bits are used for constituting the key string without bit rejection, thus the transmission efficiency of 100% may be achieved in principle.

The quadrature amplitudes of the two output field modes from a NOPA operating at deamplification are [22,23,26]:

$$\begin{aligned} X_1 &= [X_{01} \cosh(r) - X_{02} \sinh(r)] \\ Y_1 &= [Y_{01} \cosh(r) + Y_{02} \sinh(r)] \\ X_2 &= [X_{02} \cosh(r) - X_{01} \sinh(r)] \\ Y_2 &= [Y_{02} \cosh(r) + Y_{01} \sinh(r)] \end{aligned} \quad (23.11)$$

where X_{01} , X_{02} and Y_{01} , Y_{02} are the amplitude and phase quadratures of input signal and idler modes of the NOPA respectively, r ($0 \leq r \leq +\infty$) is the correlation parameter between modes 1 and 2 which depends on the strength and the time of parametric interaction, $r = 0$ without correlation, $r > 0$ with partial correlation, $r \rightarrow \infty$ with perfect correlation. From Eqs. (23.1) the normalized fluctuation variances of the amplitude quadratures for the output modes 1 and 2 are calculated:

$$\langle \delta^2(X_1) \rangle = \langle \delta^2(Y_1) \rangle = \langle \delta^2(X_2) \rangle = \langle \delta^2(Y_2) \rangle = \frac{e^{2r} + e^{-2r}}{2} \quad (23.12)$$

The quantum correlation variances between the quadratures are

$$\langle \delta^2(X_1 + X_2) \rangle = \langle \delta^2(Y_1 - Y_2) \rangle = 2e^{-2r} \quad (23.13)$$

Here we have assumed that the two modes are totally balanced during the process of measurements and this requirement is easily achieved in the experiments. Generally, r is a function of the noise frequencies. The modulated signals at given radio frequencies (rf) can be considered as a noise $\delta X_s(\Omega)$ and $\delta Y_s(\Omega)$. When the powers of $\delta X_s(\Omega)$ and $\delta Y_s(\Omega)$ are smaller than the original quantum noise power of the signal beam (Eqs. (23.12)) and larger than the correlation noise power (Eqs. (23.13)), the signals are submerged in the noise background of the signal beam (X_1, Y_1) and may be decoded by the correspondent idler beam (X_2, Y_2) of the EPR beams. Thus, the strength $\langle \delta^2 X_s \rangle$ of the modulated signals should satisfy the following inequalities:

$$\begin{aligned} 2e^{-2r(\Omega)} &< \langle \delta^2 X_s(\Omega) \rangle < \frac{e^{2r(\Omega)} + e^{-2r(\Omega)}}{2} \\ 2e^{-2r(\Omega)} &< \langle \delta^2 X_s(\Omega) \rangle < \frac{e^{2r(\Omega)} + e^{-2r(\Omega)}}{2} \end{aligned} \quad (23.14)$$

Fig. 23.7 shows the functions of the variances $\langle \delta^2(X_1) \rangle = \langle \delta^2(Y_1) \rangle$ (curve I) and $\langle \delta^2(X_1 + X_2) \rangle = \langle \delta^2(Y_1 - Y_2) \rangle$ (curve II) versus the correlation parameters. At the cross point A of the curves I and II, $r = r_1 = 0.275$, the variance is 2.4dB below the normalized SNL of EPR beams (line ii) and when $r > r_1$ the variances of signal beam (curve I) are higher than the correlation fluctuations (curve II). The line of variance=1 (line i) stands for the SNL of the noise power of signal beam which is 3dB below that of both EPR correlated beams (line ii). The larger the correlation parameter is, the higher the noise power of the signal beam is and the lower the correlation variance is. For a perfect transmission line of noiseless the correlation parameter of the NOPA should be larger than $r_1 = 0.275$ at least for accomplishing the quantum cryptography. The quantum correlation of ~2.4dB is a kind of boundary where the security becomes more favorable due to that the interception of Eve becomes harder. The height of the modulated signals should be between curve (I) and curve (II) for a given value $r > r_1$.

At Bob station, the signals $\delta X_s(\Omega)$ and $\delta Y_s(\Omega)$ modulated on the amplitude and phase quadratures of signal beam (X_1, Y_1) are decoded by the retained idler beam by means of the direct detection of photocurrents and two rf beam splitters. The normalized photocurrents measured with the positive (+) and negative (-) power combiners are :

Variance

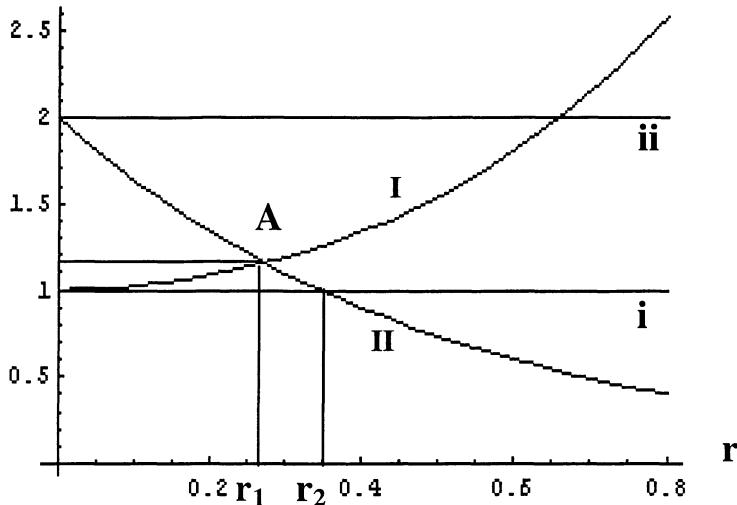


Figure 23.7 The variances of $\langle \delta^2(X_1) \rangle = \langle \delta^2(Y_1) \rangle$ (curve I) and $\langle \delta^2(X_1 + X_2) \rangle = \langle \delta^2(Y_1 - Y_2) \rangle$ versus the correlation parameter r . The line (i) and (ii) are the SNL of signal beam and EPR beams, respectively. At the point A ($r = r' \approx 0.275$) the variance is ~ 2.4 dBm below the SNL of EPR beams (ii).

$$\begin{aligned}\hat{i}_+(\Omega) &= \frac{1}{\sqrt{2}} \{ [X_1(\Omega) + X_2(\Omega)] + X_s(\Omega) * BV \} \quad (23.15) \\ \hat{i}_-(\Omega) &= \frac{1}{\sqrt{2}} \{ [Y_1(\Omega) - Y_2(\Omega)] + Y_s(\Omega) * \overline{BV} \}\end{aligned}$$

Where BV and \overline{BV} stand for the bit values 1 and 0. \overline{BV} is the NOT of BV , that means when BV equals “1” the \overline{BV} must be “0”, vice versa.

Fig. 23.8 is the schematic of the quantum cryptography system. The EPR source, NOPA, is set inside the Bob receiving station. The one of the bright EPR correlated beams, the signal beam (X_1, Y_1), is sent to the Alice sending station where Alice encodes the transmitted information on the amplitude and phase quadratures by the choice of the modulation types with the binary bit values, for example the modulated amplitude signals stands for “1” and the phase signals for “0”. Then the encoded signal beam is transmitted back to Bob where the information is decoded by the retained other one of the EPR correlated beams.

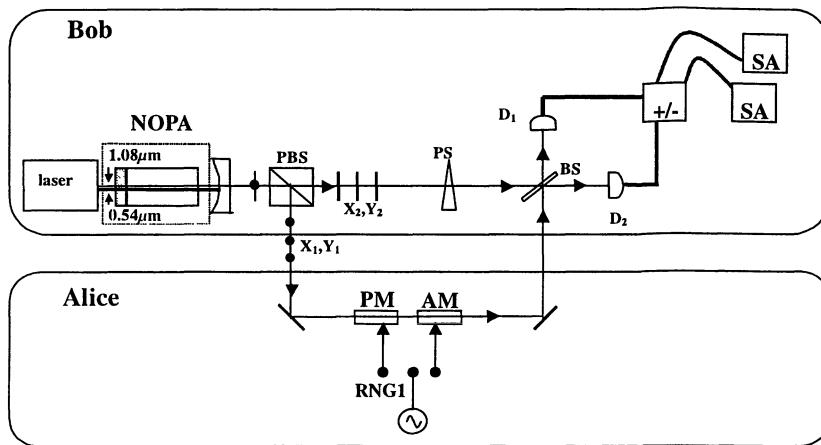


Figure 23.8 The schematic of the quantum cryptography using the EPR beams, AM-amplitude modulator, PM-phase modulator, RNG-random number generator, SA-spectrum analyzer, PS-phase shifter, BS-beamsplitter of 50%, PBS-polarization beamsplitter, NOPA-nondegenerate optical parametric amplifier.

A secretly encoded and transmitted binary bit string is summarized in Table 23.1. At the time points $t_1, t_2 \dots t_6$, Alice encodes the signal beam and sends it back to Bob, then Bob simultaneously measures the amplitude and phase modulation signals. The measured amplitude signals at t_1, t_4, t_5 stand for “1”, the phase singles at t_2, t_3, t_6 for “0”. The upper traces are the spectral densities of noise power of the SNL for the EPR beams which is used to evaluate the quantum correlations. The middle traces are the noise spectra of signal beam in which the modulated signals are submerged in the noise background totally and the lower traces are the variances $\langle \delta^2(X_1 + X_2) \rangle$ and $\langle \delta^2(Y_1 - Y_2) \rangle$, which are 3.8dBm below the noise level of the SNL of the EPR beams, and the secret signals modulated at 2MHz emerge from the squeezed noise backgrounds. A secret key string characterized by the binary bit values 100110 is obtained. The acquisition parameters of the noise spectral densities in Table 23.1 are: the measured frequency range 1.0-3.0MHz, resolution bandwidth 30KHz, video bandwidth 0.1KHz. The electronic noise, which has not been given in the noise spectra of Table 23.1, is about 8dBm below that of the SNL of the EPR beams.

In experiments, we should pay attention on matching the optical distances between the signal and idler beams to reach optimum correlation and detection efficiency. Especially for long distance transmission one must add optical retarder and attenuator in the idler beam retained by Bob to make its travel distance from EPR source to the beam splitter of the detection system and the

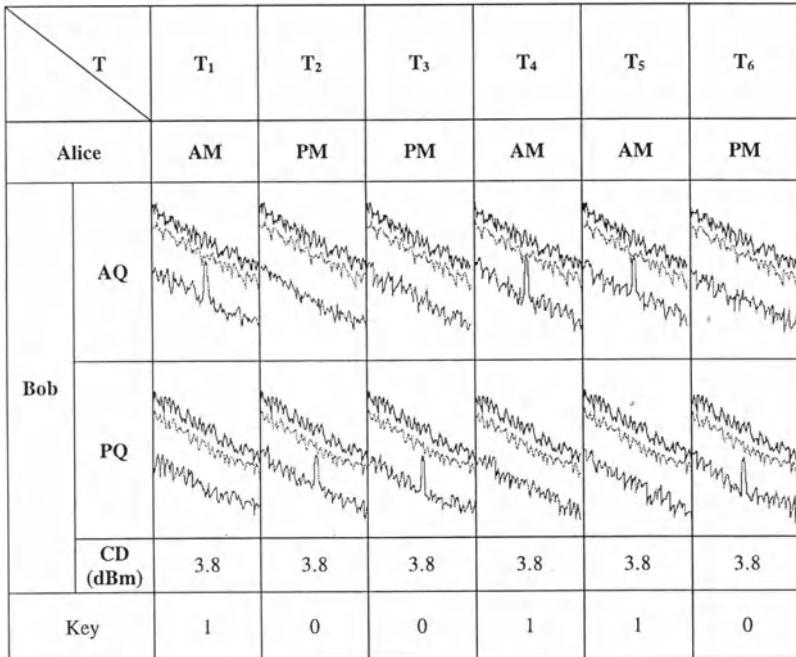


Table 23.1 The generation of the predetermined secret key string, AQ-Amplitude modulation signals, PQ-Phase modulation signals, CD-The correlation degrees between signal and idler beams measured by Bob. Key-The secret keys, upper traces-The SNL of EPR beams, middle traces-the noise spectra of signal beam, lower traces-the noise spectra of $\langle \delta^2(X_1 + X_2) \rangle$ and $\langle \delta^2(Y_1 - Y_2) \rangle$.

detected intensity approximately equal to that of the signal beam. Recently, the schemes on storing quantum entanglement in atomic spins system or in cavity QED have been presented [31,32], that probably can provide a practical technique for retaining an EPR component in Bob.

The intensity fluctuations of signal and idler fields of the bright EPR beams generated by the NOPA are quantum-correlated at any instant and nobody can make or copy a light field which has the identical quantum fluctuations. The basis of the security of the presented protocol is the quantum correlation. In experiment, the SNR(signal to noise ratio) of the decoded signals depends on the original correlation of EPR beams and the losses of a given transmission line, which is independent of Alice's bit value. Any decrease of the measured SNR and the correlation degree relative to the predicted results alerts Bob to

the additional loss caused by a partial tapping of the signal channel, perhaps by Eve. If Eve wants to perform the quantum-nondemolition-measurement (QND) on one of the amplitude-phase quadratures of the signal beam, the other quadrature must be disturbed and the disturbance must be reflected on the measured results of Bob. The deviation would indicate the possibility that Eve have performed a QND. More quantitative analyses on protecting against the optical tap attack of Eve have been presented in the previous publications [11-15] and can be used in the discussion to the presented protocol.

For the ideal case of the EPR beams with perfect quantum correlation, the SNR on the signal channel goes to zero due to the fact that the quantum noise of the signal beam goes to infinite [15,28]. Thus, the attacking from optical tap or the optical QND on the signal beam has no possibility to extract information hidden in the infinite quantum noise without the help of the other one of the EPR correlated beams. However, for the imperfect correlations the signal channel has large but finite quantum noise background. In this case, the eavesdroppers can enhance the measurement SNR by narrowing the resolution bandwidth (RBW) of the spectral analyzer (SA) according to [33]:

$$SNR = \frac{\langle i_s^2 \rangle}{\langle i_N^2 \rangle} = \eta I_s / BF_0 \quad (23.16)$$

where $\langle i_s^2 \rangle$ and $\langle i_N^2 \rangle$ are the mean square signal and noise photocurrents respectively, I_s is the photon number flux of the signal beam, η is the quantum efficiency of the detection system and F_0 is the Fano factor of the signal beam, $F_0 \rightarrow \infty$ for perfect correlated EPR beams and $F_0 = 1$ without quantum correlation(coherent state light). For the given η , I_s and F_0 , the usable RBW of the measurement is limited by the requirement of $SNR \geq 1$, i.e.

$$B_0 \leq \frac{\eta I_s}{F_0} \quad (23.17)$$

It means that the duration of measurement should be larger than B_0^{-1} . For secure communication Alice should encode the message with a bit rate larger than B_0 decided by Eq. (23.17), so that Eve can not intercept information due to having no enough interval to accomplish the measurement. In our experiment when $B = 30kHz$, the signals have been totally submerged in the noise background (the middle traces in Table 23.1), thus the condition is easily satisfied in the practical optical communication.

A possible eavesdropping scheme using fake EPR beams is shown in Fig. 23.9. Eve intercepts totally the signal beam (X_1, Y_1) and transmits a fake signal beam (X'_1, Y'_1) produced by a fake EPR source (EPR2) in her station to Alice. Alice has no ability to recognize the fake beam. She modulates the information on it and then sends out as usual. Eve intercepts the beam with messages again and

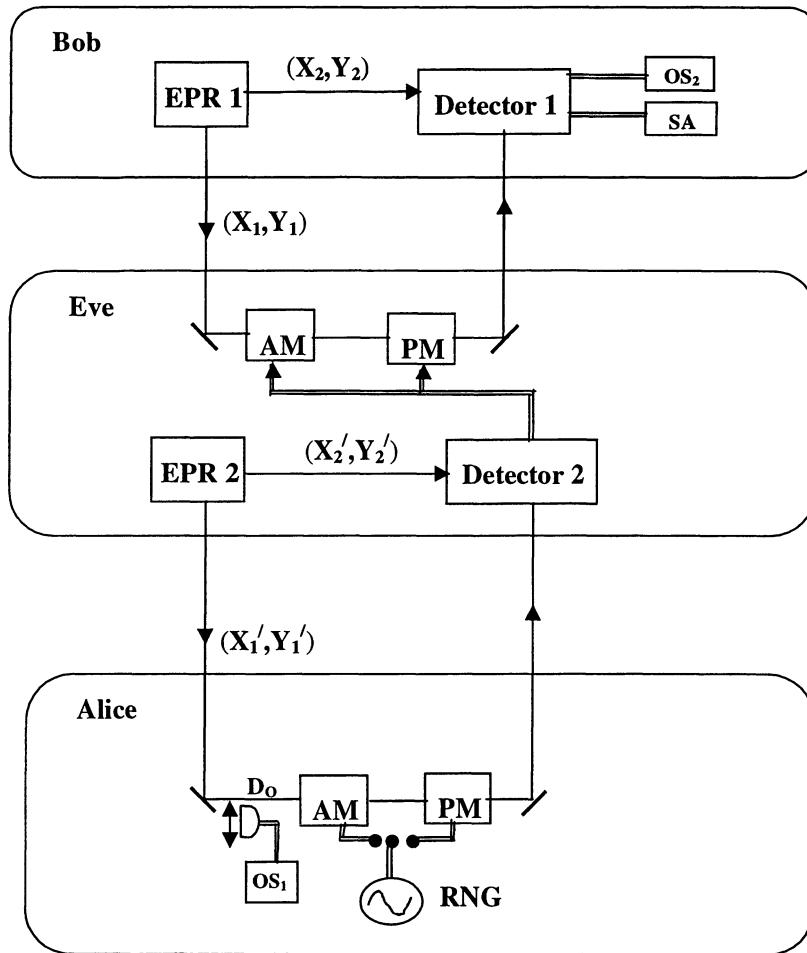


Figure 23.9 Diagram of eavesdropping Scheme using fake EPR beams, EPR_1 , EPR_2 -Sources of EPR beams, AM, PM-Amplitude and phase modulators, SA-spectral analyzer, OS_1 , OS_2 -Oscilloscopes, Detector 1, 2-Detection systems of Bell-state, D_O -photoelectric detector, RNG-random number generator.

decodes the information with the other one of the fake EPR correlated beams (X'_1, Y'_1) retained by her. At the same time she modulates the real signal beam (X_1, Y_1) according to the intercepted bit values and sends it back to Bob who also does not know that the information has been intercepted. To reveal this type of quantum interception Alice may randomly block the signal beam with

a photoelectric detector (D_0) connected to an oscilloscope at some appointed time points t_k for a short time interval Δt_k during the duration of transmission. The shape of intensity fluctuation of the signal beam at the blocked moment can be recorded as a function of time by an oscilloscope (OS_1). In Bob station, the photocurrent of the sum of the amplitude quadratures $\langle \delta^2(X_1 + X_2) \rangle$ is split to two parts by a power splitter, one is sent to a spectrum analyzer (SA) for the noise spectrum measurement and other one to an oscilloscope (OS_2) for recording the fluctuation of photocurrents. If there is no Eve between Alice and Bob, while the signal beam is blocked by D_0 the oscilloscope OS_2 in Bob station records the function of intensity fluctuation of the idler beam $\langle \delta^2 X_2(t) \rangle$ which is anticorrelated with $\langle \delta^2 X_1(t) \rangle$ recorded by OS_1 at same time and the correlation extent only depends on the quality of the EPR source (EPR1) and the losses of transmission line. Fig. 23.10 shows the intensity fluctuation shapes of $\langle \delta^2 X_1(t) \rangle$ (trace1) and $\langle \delta^2 X_2(t) \rangle$ (trace2) simultaneously recorded by OS_1 and OS_2 respectively. The partial anticorrelation between the shapes of the fluctuations is very obvious and the measured root-mean-square (rms) voltages for the sum and difference of traces 1 and 2 are $568.64\mu V$ and $655.29\mu V$ respectively. For two uncorrelated beams with same intensity, the rms voltages for sum and difference photocurrents should be equal, thus the difference between rms voltages also shows the presence of quantum correlation. If Eve interrupts the real signal beam, the intensity fluctuations of $\langle \delta^2 X'_1(t) \rangle$ recorded by Alice at the blocked moment are totally not correlated with that recorded by OS_2 at same time. After a set of communication is finished, Alice publicly sends the wave shapes of intensity fluctuation and the rms voltages recorded by OS_1 to Bob, where Bob compares with that recorded by himself with OS_2 at same time points. The absence of anticorrelation between the two sets of fluctuation shapes and the same rms voltages for the sum and difference indicate the presence of Eve. In this case the transmitted secret key string should be abandoned. If the fluctuation shapes recorded by Bob and Alice are quantum anticorrelated in some extent determined by the EPR source (EPR1) of Bob and losses of transmission line, we may deem that the communication is secure. During the duration of the signal transmission the more the times of blocking the signal beam are, the higher the degree of security is, but the longer the time on the transmission line occupied by the measurement for security is. Therefore we have to do a trade-off between the signal transmission and the security measurement in practical communication.

The intervention strategies would be various and the discussion on the complete security lies beyond the scope of the present paper. We consider that the presented protocol is a worthy candidate for investigating the quantum cryptography because of its good security directly provided by quantum correlation and no-cloning of quantum fluctuation.

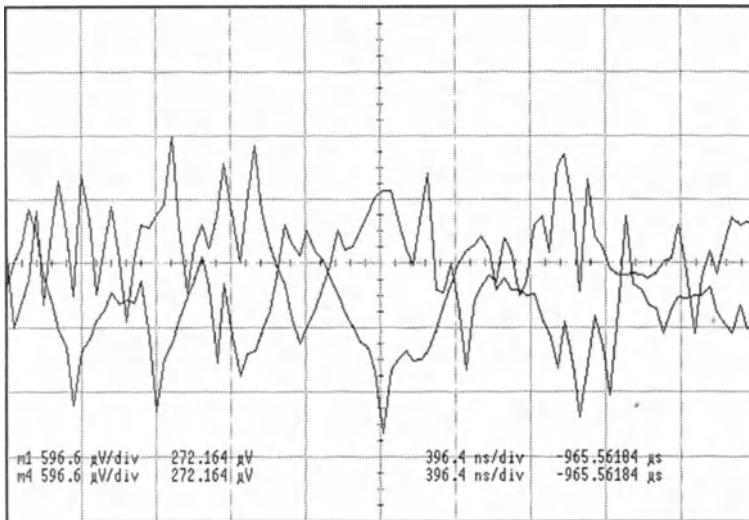


Figure 23.10 The fluctuation shapes of signal (1) and idler (2) beams recorded by the oscilloscopes OS₁ and OS₂ at Alice and Bob.

6. CONCLUSION

We have experimentally demonstrated the quantum dense coding and quantum cryptography with continuous variables. Due to using the bright EPR correlated beams, the transmitted signals are directly modulated on the amplitude and phase quadratures of signal beam with the amplitude and phase modulators compatible with that used in the present optical communication system operating at very high rates. The application of the direct detection technology of the Bell-state simplifies the measurement system and the aligning procedures, and further improves the detection efficiency. Available high bits transmission rates and high detection efficiency are favorable features of the presented schemes. Besides, we have proved that the experimentally achievable quantum correlation and squeezing level may be used for performing the quantum communication. Unlike most of proposed protocols for quantum cryptography based on BB84 [34], our scheme does not require any randomly chooses of measuring components, so there is no the usual 50% bit rejection. The predetermined secret key string is directly modulated on the optical beam(the carrier of signals) just like that used in traditional optical communication systems. The partial compatibility with classical optical communication

technology and the simplicity of encoding and decoding procedures would be welcome by technicians working for communications.

These works were funded by the National Fundamental Research Program (No.2001CB309304) and the National Nature Science Foundation (No.698370 10,60178012)

References

- [1] Braunstein, S. L. (1998) Error correction for continuous quantum variables. *Phys. Rev. lett.* 80, 4084-4087.
- [2] Braunstein, S. L. (1998) Quantum error correction for communication with linear optics. *Nature (London)* 394, 47-49
- [3] Braunstein, S. L. & Kimble, H. J. (2000) Dense coding for continuous variables. *Phys. Rev. A* 61, 042302
- [4] Ban, M. (1999) Quantum dense coding via a two-mode squeezed-vacuum state. *J. opt. B: Quantum Semiclass. Opt.* 1 L9-L11
- [5] Loock, P. Van & Braunstein, S. L. (2000) Unconditional entanglement swapping for continuous variables. *Phys. Rev. A* 61, 10302(R)
- [6] Gottesman, D., & Preskill, J. (2001) Secure quantum key distribution using squeezed states. *Phys. Rev. A* 63, 022309
- [7] Hillery, M., (2000) Quantum cryptography with squeezed states. *Phys. Rev. A* 61, 022309
- [8] Cerf, N. J., Levy, M., & Assche, G. V., (2000) Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* 63, 052311
- [9] Cerf, N. J., Iblisdir, S., & Assche, G. V., (2001) Cloning AND Cryptography with Quantum Continuous Variables. *quant-ph/0107077* [Eur.Phys.J.D(to be published)]
- [10] Assche G. V. et al., (2001) Reconciliation of a Quantum-Distributed Gaussian Key. *cs.CR/0107030* (to be published)
- [11] Ralph, T. C. (2000) Continuous variable quantum cryptography. *Phys. Rev. A* 61, 010303(R)
- [12] Ralph, T. C., (2000) Security of continuous-variable quantum cryptography. *Phys. Rev. A* 62, 062306
- [13] Reid, M. D., (2000) Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A* 62, 062308
- [14] Silberhorn, C., Korolkova, N., & Leuchs, G., (2001) Quantum key distribution with bright entangled beams. *quant-ph/0109009*

- [15] Pereira, S. F., Ou, Z. Y., & Kimble, H. J., (2000) Quantum communication with correlated nonclassical states. Phys. Rev. A 62, 042311; Kimble, H. J., Ou, Z. Y., & Pereira, S. F., Method and Apparatus for Quantum Communication Employing Nonclassical Correlations of Quadrature-Phase Amplitudes. U.S. Patent No. 5,339,182, Issued 8/16/94.
- [16] Bencheikh, K. et al., (2001) Quantum key distribution with continuous variables. J. Mod. Opt. 48, 1903
- [17] Lorenz, S. et al., (2001) Squeezed light from microstructured fibres: towards free space quantum cryptography. quant-ph/0109018
- [18] Navez, P. et al., (2001) A “quantum public key” based cryptographic scheme for continuous variables. quant-ph/0101113
- [19] Grosshans, F., & Grangier, P., (2002) Continuous Variable Quantum Cryptography Using Coherent States. Phys. Rev. Lett. 88, 057902
- [20] Furusawa, A. et al. (1998) Unconditional quantum teleportation. Science 282, 706-709
- [21] Li, X. Y. et al. Quantum Dense Coding Exploiting a Bright Einstein-Podolsky-Rosen Beam. Phys. Rev. Lett. 88, 047904 (2002)
- [22] Reid, M. D., & Drummond, P. D. (1988) Quantum Correlations of Phase in Nondegenerate Parametric Oscillation. Phys. Rev. Lett. 60, 2731-2733
- [23] Reid, M. D. (1989) Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification. Phys. Rev. A 40, 913
- [24] Ou, Z. Y., Pereira, S. F., & Kimble, H. J. (1992) Realization of the Einstein-Podolsky-Rosen paradox for continuous variables in nondegenerate optical parametric amplifier. Appl. Phys. B 55, 265
- [25] Zhang, Y. et al. (2000) Experimental generation of bright two-mode quadrature squeezed light from a narrow-band nondegenerate optical parametric amplifier. Phys. Rev. A 62, 023813
- [26] Zhang, Y., Su, H., Xie, C. D. & Peng, K. C. (1999) Quantum variances and squeezing of output field from NOPA. Phys. Lett. A 259, 171
- [27] Li, X. Y., Pan, Q., Jing, J. T., Xie, C. D., & Peng, K. C., (2001) LD pumped intracavity frequency-doubled and frequency-stabilized Nd:YAP/KTP laser with 1.1w output at 540nm, Optics Communications, (01) 01685-6
- [28] Zhang, J. & Peng, K. C. (2000) Quantum teleportation and dense coding by means of bright amplitude-squeezed light and direct measurement of a Bell state. Phys. Rev. A 62, 064302
- [29] Jing, J., Pan, Q., Xie, C. D. & Peng, K. C. (2002) Quantum Cryptography Using Einstein-Podolsky-Rosen Correlations of Continuous Variables. quant-ph/0204111

- [30] Pan, Q., Zhang, Y., Zhang, T. C., Xie, C. D. & Peng, K. C., Experimental investigation of intensity difference squeezing using Nd:YAP laser as pump source, *J. Phys. D: Appl. Phys.* 30(1997) 1588-1590
- [31] Julsgaard, B., Kozhekin, A., & Polzik, E. S. (2001) Experimental long-lived entanglement of two macroscopic objects. *Nature* 413, 400-403
- [32] Parkins, A. S. & Kimble, H. J. (2000) Position-momentum Einstein-Podolsky-Rosen state of distantly separated trapped atoms. *Phys. Rev. A* 61, 052104
- [33] Li, Y. Q., Lynam, P., Xiao, M., & Edwards, P. J. Sub-Shot-Noise laser Doppler Anemometry with Amplitude-Squeezed Light. *Phys. Rev. Lett.* 78, 3105 (1997)
- [34] Bennett, C. H., & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proc.IEEE Int. Conf. On Computers, Systems and Signal Processing(Bangalore), 175-179 (IEEE, New York,1984)

Chapter 24

QUANTUM SOLITONS IN OPTICAL FIBRES: BASIC REQUISITES FOR EXPERIMENTAL QUANTUM COMMUNICATION

G. Leuchs, Ch. Silberhorn, F. König, P. K. Lam, A. Sizmann, N. Korolkova

Zentrum für Moderne Optik,

Universität Erlangen - Nürnberg, Germany

leuchs@physik.uni-erlangen.de

www.zemo.org

Abstract Continuous variable quantum entanglement emerges from nonlinear interactions of fibre optical solitons in combination with some linear operation. We describe the detection and characterization of bright EPR-entanglement and QND-entanglement produced in this way and discuss the prospects of bright-beam-based quantum communication.

1. INTRODUCTION

Non-local properties of continuous variables have been the focus of the historic discussion which today is considered the starting point of quantum information [1]. At the time, however, the disputants did not have any application in mind. They were rather struggling for the proper interpretation of quantum theory. Einstein, Podolsky, and Rosen called the scenario they described [2] a Gedanken-experiment for a good reason. Nobody knew how to create continuous variable quantum systems in an entangled state which could be used in the laboratory to test for the non-locality of quantum theory. Then in 1951, Bohm reformulated the EPR-Gedanken-experiment in terms of discrete spin variables [3] laying the foundation for the laboratory studies to come. The incentive for more refined experiments rose when Bell derived a general criterion based on which the non-locality of quantum theory could be put to a stringent test [4]. The experiments by Clauser et al. [5] and Aspect et al. [6] which followed all aimed at a better understanding of the foundations of quantum

theory. One reason for their success was that dichotomic quantum systems can be prepared experimentally in a state of close-to-perfect entanglement. And even without any entanglement a discrete quantum system has the additional advantage that the detector sends 'on-off' messages conveniently providing a built-in discriminator function. It is therefore not surprising (in retrospect) that when proposing quantum teleportation and quantum key distribution Bennett et al. [7] used the example of the discrete quantum variables which had proven to be so successful. The numerous experiments which followed were pioneered by Zeilinger et al. [9]. Soon cryptography will be the first real world application of quantum information [8]. However, the production process for the entangled photon pairs used in these experiments is spontaneous parametric down conversion and is therefore probabilistic. You never know ahead of time at which point the experiment will be successful. For cryptographic key distribution the probabilistic production of single photons may be less of a concern but for other cases such as teleportation the concern seems more serious. Along with the probabilistic production, the signal rate is fairly low.

Ou et al. [10] were the first to demonstrate that entanglement can be produced experimentally also with the continuous variable field quadratures of two different modes of light. Ou et al. used an optical parametric amplifier to produce entangled light beams at a very low light level. Such continuous variable entanglement can be seen to be quite complementary to entangled pairs of photons. Continuous variable entanglement is less perfect and more fragile with respect to attenuation but it is not probabilistic. It is there at your disposal. This and the much higher transmission rates may well be favourable in some applications. Recently bright light entanglement was achieved using the interference scheme [11] and using a nondegenerate optical parametric amplifier [12], an additional advantage being the availability of efficient direct detection. Furthermore, nonlinear coupling between bright light fields has been demonstrated to lead to quantum correlation and entanglement [13, 14, 15] which has not yet been achieved for single interacting photons. It should be noted here that future developments of cavity quantum electrodynamics may lead to deterministic sources of single photons [16, 17] and maybe also of entangled photon pairs. Commercial tools for fibre-optic test and measurement are beginning to exploit the ultrasensitivity of photon counting techniques at telecommunication wavelength [18, 19], paving the way towards photon-counting communication technology.

In the following sections of this chapter we discuss the steps towards experimental quantum information processing with an example of experiments using fibre optical soliton pulses. The nonlinear interaction of solitons in a fibre combined with linear optical elements such as beam splitters is enough to assemble non-trivial basic building blocks for continuous variable quantum communication.

2. CONTINUOUS VARIABLE ENTANGLEMENT: AN EXPERIMENTAL CLASSIFICATION

Implementation of inter-channel coupling. One of the most attractive features of continuous variable quantum information is the possibility of information processing exclusively with linear inter-channel operations [20]. The basic example is the simple and elegant way to generate continuous variable entanglement by overlapping two squeezed beams on a beam splitter [11, 21, 22, 23]. Closely related is the entanglement produced at the output of the non-degenerate type II optical parametric oscillator (OPO) [10, 12, 24], which, however, uses a nonlinear interaction between two channels.

Single squeezed beams for entanglement generation can be produced in different nonlinear interactions within a single channel, e.g. type I OPO [22], or Kerr medium [11]. These beams are then used as a resource to create entanglement by their linear interference at a beam splitter. The entanglement, therefore, emerges from a linear interaction between two non-linear channels. Soliton pulses in silica fibres allow for very efficient implementation of this scheme exploiting the Kerr nonlinearity of an optical fibre to generate long-term stable and easy to handle amplitude squeezing. The entanglement, which emerges in this case, is connected to the non-local correlations between quantum uncertainties of the conjugate variables in two spatially separated intense beams.

It is also possible to employ a non-linear interaction between two channels to create entanglement. Apart from the self-phase modulation effect used for squeezing generation, the Kerr nonlinearity also results in cross-phase modulation if optical fields of different polarizations or different frequencies are involved. For instance, back-action evading measurement schemes with colliding solitons are based on the cross-Kerr-effect [25]. The non-linear Kerr interaction between two channels entangles two pulses, the signal pulse and the probe pulse, and hence a QND measurement of the signal photon number can be performed. In one scheme the non-linear inter-channel interaction leads to a non-local quantum correlation between the photon-number of the signal pulse, n_s and a phase shift of the probe pulse, $\Delta\phi_p$, [25, 26]. A non-local quantum correlation between the signal photon number n_s and a frequency shift Δf_p of the probe emerges in another scheme [14, 15]. In terms of observables it corresponds to a correlation between the photon number (\hat{n}_s) and the momentum \hat{p}_p of the probe pulse. Applying a spectral filtering technique, this correlation can be transferred into a photon number - photon number correlation between the signal (n_s) and the spectrally filtered probe pulses (n_p). Continuous variable entanglement generated in QND interaction can also be employed for quantum communication purposes. Recently, a quantum teleportation scheme was proposed using quantum nondemolition technique

[27], where the QND interaction of coherent input fields was discussed as well as QND coupling of squeezed beams aiming at improved teleportation quality.

Continuous variable EPR-paradox. EPR-entanglement and ideas of QND-measurement [27, 28, 29] are closely related. A clear insight in this tight connection can be found in the characterization of quantum correlations.

The quality of the quantum correlations between the signal \hat{A}_s and probe \hat{B}_p variables at the output of the QND-device is associated with the quality of the state preparation. An experimental measure for this is the variance in the signal output given a measured value for the probe field, e.g. the variance of the difference of the measured values of the two correlated variables. It is the variance of the relevant conditional probability distribution and is conventionally referred to as the conditional variance [28]:

$$V_{cond}(\hat{A}_s|\hat{B}_p) = \frac{V(\hat{A}_s)}{V(\hat{A}_{s,\text{SN}})} \left(1 - C^2(\hat{A}_s, \hat{B}_p)\right) \quad (24.1)$$

with

$$C^2(\hat{A}_s, \hat{B}_p) = \frac{|\langle \hat{A}_s \hat{B}_p \rangle - \langle \hat{A}_s \rangle \langle \hat{B}_p \rangle|^2}{V(\hat{A}_s) V(\hat{B}_p)} \quad (24.2)$$

where $V(\hat{A})$ denotes a variance $\langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2$ of an observable \hat{A} and $C^2(\hat{A}_s, \hat{B}_p)$ is the correlation coefficient. The variance $V(\hat{A}_{s,\text{SN}})$ corresponds to the shot noise, i.e. vacuum noise level which marks a boundary between classical and quantum regime. Equivalently $V_{cond}(\hat{A}_s|\hat{B}_p)$ can be expressed in terms of the normalized variance of $\hat{A}_s + g\hat{B}_p$ for an optimal gain g :

$$V_{cond}(\hat{A}_s|\hat{B}_p) = \min_g \frac{V(\hat{A}_s + g\hat{B}_p)}{V(\hat{A}_{s,\text{SN}})}. \quad (24.3)$$

In a QND regime the conditional variance (24.3) should be nonclassical revealing a degree of quantum correlations which is better than the vacuum noise level of a signal beam:

$$V_{cond}(\hat{A}_s|\hat{B}_p) = \min_g \frac{V(\hat{A}_s + g\hat{B}_p)}{V(\hat{A}_{s,\text{SN}})} < 1. \quad (24.4)$$

The notion of continuous EPR-like correlations of the amplitude and phase quadratures is related to the demonstration of the EPR-paradox for continuous variables introduced by Reid and Drummond in 1988 [24]. If two spatially separated beams are correlated in their amplitude $\hat{X}_j = \hat{a}_j^\dagger + \hat{a}_j$ and phase $\hat{Y}_j = i(\hat{a}_j^\dagger - \hat{a}_j)$ quadratures, it is possible to infer e.g. X_2 by a measurement of \hat{X}_1

or Y_2 by \hat{Y}_1 . The quality of this continuous variable entanglement is restricted by finite squeezing values so that there will always be a limit in this inference. This was originally referred to as an inference error $V_{inf}(\hat{X}_j)$, $V_{inf}(\hat{Y}_j)$ [24]. To minimize the error, a variable gain g [24, 25, 28] is introduced:

$$\begin{aligned} V_{inf}^{\pm}(\hat{X}_1) &= \frac{V\left(\hat{X}_1 \pm g_X \hat{X}_2\right)}{V(\hat{X}_{1,\text{SN}})}, \\ V_{inf}^{\mp}(\hat{Y}_1) &= \frac{V\left(\hat{Y}_1 \mp g_Y \hat{Y}_2\right)}{V(\hat{Y}_{1,\text{SN}})}. \end{aligned} \quad (24.5)$$

The upper signs are used if the amplitudes are anti-correlated and the phases are correlated and the lower signs are for the reversed situation.

Note, that for the optimal gains $g_X = g_X^{opt}$, $g_Y = g_Y^{opt}$ the inference errors (24.5) in the derivation of the EPR-paradox are equivalent to the conditional variances (24.1,24.3):

$$\begin{aligned} V_{cond}^{\pm}(\hat{X}_1|\hat{X}_2) &= \min_{g_X} V_{inf}^{\pm}(\hat{X}_1), \\ V_{cond}^{\mp}(\hat{Y}_1|\hat{Y}_2) &= \min_{g_Y} V_{inf}^{\mp}(\hat{Y}_1). \end{aligned} \quad (24.6)$$

Consider now the quantum noise limit for the measurement of conjugate quadratures of a single field which is given by the Heisenberg relation:

$$V(\hat{X})V(\hat{Y}) \geq 1. \quad (24.7)$$

The continuous variable EPR-paradox is related to an apparent violation of this fundamental limit [24]. In our notation (24.6), the demonstration of the EPR-paradox requires simultaneous non-classical values of the respective conditional variances:

$$V_{cond}^{\pm}(\hat{X}_1|\hat{X}_2) < 1, \quad V_{cond}^{\mp}(\hat{Y}_1|\hat{Y}_2) < 1; \quad (24.8)$$

$$V_{cond}^{\pm}(\hat{X}_1|\hat{X}_2) V_{cond}^{\mp}(\hat{Y}_1|\hat{Y}_2) < 1. \quad (24.9)$$

This specifies the ability to infer "at a distance" either of the two non-commuting signal observables with a precision below the shot noise level of the signal beam [24], (24.4). Condition (24.9) defines the EPR boundary for a non-local quantum correlation and provides a sufficient condition for a state to be entangled. Hence, if the quantum correlation is stronger than a certain threshold one refers to EPR-entanglement and this is closely related to the idea of a QND measurement.

Non-separability criterion for continuous variables. It is important to define accurately the relation between notions "correlated systems" and "entangled systems". Which kind of correlations implies entanglement? In the paragraph above we have defined EPR-correlations in terms of the EPR-*Gedankenexperiment* introduced for amplitude and phase quadrature operators by Reid [24]. This represents a sufficient entanglement criterion. Are there other ways which allow one to draw the line between classical correlations and entanglement for continuous variable systems more precisely? The conventional notion of entanglement for pure states is intrinsically related to quantum inseparability which means that in general it is not possible to assign a single state vector to either of two systems which have interacted in the past [9]. For mixed states it was first formulated by Werner [30]: "A state of a composite quantum system is called classically correlated if it can be approximated by convex combinations of product states, and Einstein-Podolsky-Rosen correlated otherwise".

Hence, a separable state of a joint system described by a density matrix $\hat{\rho}$ can be written as:

$$\hat{\rho} = \sum_i p_i \hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \quad (24.10)$$

where $\hat{\rho}_{i1}$, $\hat{\rho}_{i2}$ denote density matrices of two subsystems 1 and 2 (see also [30]). In contrast, an entangled state is a non-separable quantum state of a system which cannot be represented as a convex sum of product states of two subsystems. For discrete variables, i.e. for the Hilbert space of 2×2 and 2×3 dimensions, a necessary and sufficient criterion for separability is the requirement that the partial transpose $\hat{\rho}^T$ of the density matrix is positive which is known as the Peres-Horodecki criterion.

Recently, the Peres-Horodecki criterion was extended to higher dimensions of the Hilbert space, i.e. for continuous variables, using two different approaches (for details see [31, 32] and chapters 13 and 14 of the present book). The analysis of Simon [31] is accomplished using the formalism of the phase space Wigner function $W(x, p)$ [21, 33]. It is based on the recognition that the partial transpose $\hat{\rho}^T$ is equivalent to a mirror reflection in phase space. If $\hat{\rho}$ is separable, its Wigner distribution necessarily goes over into a Wigner distribution under the phase space mirror reflection [31]:

$$\hat{\rho} \longrightarrow \hat{\rho}^T \iff W(x, p) \longrightarrow W(x, -p). \quad (24.11)$$

Here x, p are the canonical variables position and momentum. This recognition (24.11) leads to uncertainty principles to be obeyed by all separable states. For all bipartite Gaussian states, the continuous variable Peres-Horodecki criterion can then be written, which turns out to be a necessary and sufficient condition for separability [31]. The criterion of Simon corresponds to the necessary and

sufficient form of the criterion derived by Duan et al [32]. The rest of this section is devoted to this latter criterion first in its sufficient and then in its necessary and sufficient form as it allows one to use the conventional tools of experimental quantum optics and is more convenient for the experimental verification of entanglement of intense beams.

Duan et al [32] are deriving the non-separability criterion in the spirit of two-mode squeezing [33]:

$$V(\hat{x}_1 + \hat{x}_2) \rightarrow 0, \quad V(\hat{p}_1 - \hat{p}_2) \rightarrow 0. \quad (24.12)$$

They introduce the EPR-like operators in the form of joint variables:

$$\hat{u} = |a| \hat{x}_1 + \frac{1}{a} \hat{x}_2, \quad \hat{v} = |a| \hat{p}_1 - \frac{1}{a} \hat{p}_2; \quad (24.13)$$

$$[\hat{x}_j, \hat{p}_k] = i\delta_{jk} \quad (j, k = 1, 2) \quad (24.14)$$

where a is an arbitrary non-zero real number. Then the total variance of \hat{u} and \hat{v} is derived under the assumption that (24.10) holds. The lower bound for this total variance is calculated which represents a separability condition. A sufficient criterion for non-separability of an arbitrary two-mode state is obtained whenever the following inequality is fulfilled [32]:

$$V(\hat{u})_\rho + V(\hat{v})_\rho < a^2 + \frac{1}{a^2}. \quad (24.15)$$

For a bipartite Gaussian state this inequality can also give a necessary and sufficient condition for non-separability. For this purpose both beams should be transformed into a canonical form by performing local linear Bogolubov operations on them and by using an optimal gain (see [32] and next subsection for details). The criterion of Duan et al [32] (24.15) and the equivalent to its necessary and sufficient form criterion of Simon [31] have an advantage for experimental quantum communication as they can be expressed in terms of measurable quantities. In Eqn. (24.15) the variances $V(\hat{u})$, $V(\hat{v})$ are presented without any additional normalization. For the analytical analysis the normalization is not needed: the reference level is the noise variance of the coherent beam or equivalently of the coherent vacuum which is equal to $1/2$ in the notation of (24.13-24.15). However, in an experiment the respective reference is represented by the shot noise level and has to be always explicitly determined in each measurement run. To account for this, we rewrite the Peres-Horodecki non-separability criterion (24.15) for continuous variables quadrature amplitudes $\hat{X}_j = \hat{a}_j^\dagger + \hat{a}_j$, $\hat{Y}_j = i(\hat{a}_j^\dagger - \hat{a}_j)$ with $[\hat{X}_j, \hat{Y}_k] = 2i\delta_{jk}$, $j, k = 1, 2$ of two subsystems, beams 1 and 2. We introduce the joint variables $\hat{X} = \hat{X}_1 + g\hat{X}_2$ and $\hat{Y} = \hat{Y}_1 - g\hat{Y}_2$ of two bright beams analogously to (24.13), where g is a variable gain like in the description of continuous variable EPR-paradox presented above. The quadrature correlations between two beams can

be characterized by the normalized squeezing variances $V_{sq}^{\pm}(\hat{X})$, $V_{sq}^{\mp}(\hat{Y})$ which are known from the context of two-mode squeezing [33]:

$$V_{sq}^{\pm}(\hat{X}) = \frac{V(\hat{X}_1 \pm g \hat{X}_2)}{V(\hat{X}_{1,\text{SN}} + g \hat{X}_{2,\text{SN}})}, \quad (24.16)$$

$$V_{sq}^{\mp}(\hat{Y}) = \frac{V(\hat{Y}_1 \mp g \hat{Y}_2)}{V(\hat{Y}_{1,\text{SN}} + g \hat{Y}_{2,\text{SN}})}. \quad (24.17)$$

The field modes are denoted by the respective subscripts and SN denotes the shot noise limit of the respective beam and $g_X = g_Y = g$ by the argument of symmetry. Apart for a difference in the normalization, the variances in (24.15) correspond to the squeezing variances in (24.16, 24.17). The joint variables (24.13) for the optical beams are expressed in terms of amplitude and phase quadratures.

To rewrite the non-separability criterion (24.15) in terms of measured variances of quadrature operators, let us consider the amplitude quadratures \hat{X}_j first. If we are dealing with bright beams, we can write:

$$\hat{a}_j = \alpha + \delta\hat{a}_j \quad \hat{n}_j \approx n_j + \alpha_j \delta\hat{X}_j \quad (24.18)$$

where $\alpha_j \gg 1$ is a strong classical coherent amplitude, $\alpha = \langle a \rangle$; $\delta\hat{a}_j$ is an operator with zero mean which describes the quantum uncertainty and \hat{n}_j is a photon number operator of the respective beam with mean value n_j . The expression for \hat{n}_j is written using the linearization approach, omitting terms in the second order of $\delta\hat{X}_j$ ($\delta\hat{X}_j = \delta\hat{a}_j^\dagger + \delta\hat{a}_j$) and higher. The direct photo detection in each beam 1 and 2 yields photo currents containing the measurement results of \hat{n}_j which are then used to determine the relevant shot noise reference and the combined variance of two beams (see (24.18)). The shot noise variance is related to the strong coherent amplitude and equals:

$$V_{\text{SN}}(\hat{n}_1 + g \hat{n}_2) = \alpha_1^2 + g^2 \alpha_2^2. \quad (24.19)$$

The variance of the combined variables read out by means of photo detection is given by (24.18):

$$V(\hat{n}_1 + g \hat{n}_2) = V(\alpha_1 \delta\hat{X}_1 + g \alpha_2 \delta\hat{X}_2) \quad (24.20)$$

To facilitate the comparison with (24.15), it can be expressed as

$$V(\hat{n}_1 + g \hat{n}_2) = g\alpha_1\alpha_2 V\left(\sqrt{\frac{\alpha_1}{g\alpha_2}} \delta\hat{X}_1 + \sqrt{\frac{g\alpha_2}{\alpha_1}} \delta\hat{X}_2\right). \quad (24.21)$$

The variance $V_{sq}^+(\hat{X})$ corresponding to that of the joint variables of (24.13) [32] is then obtained in the form:

$$V_{sq}^+(\hat{X}) = \frac{V(\hat{n}_1 + g \hat{n}_2)}{V_{SN}(\hat{n}_1 + g \hat{n}_2)} = \frac{V\left(\sqrt{\frac{\alpha_1}{g\alpha_2}} \delta\hat{X}_1 + \sqrt{\frac{g\alpha_2}{\alpha_1}} \delta\hat{X}_2\right)}{\frac{\alpha_1}{g\alpha_2} + \frac{g\alpha_2}{\alpha_1}}. \quad (24.22)$$

For two beams 1 and 2 of equal intensity it takes a simple form discussed by Reid in 1989 while relating their EPR criterion [24] for continuous variables amplitude and phase to two-mode squeezing:

$$V_{sq}^+(\hat{X}) = \frac{V\left(\delta\hat{X}_1 + g \delta\hat{X}_2\right)}{1 + g^2}. \quad (24.23)$$

Compare (24.22) to (24.13, 24.15):

$$V_{sq}^+(\hat{X}) = 2 \frac{V(\hat{u})}{a^2 + \frac{1}{a^2}} \quad \text{for } a = \sqrt{\frac{\alpha_1}{g\alpha_2}} \quad (24.24)$$

where the factor 2 comes from different normalizations used: $[\hat{x}_j, \hat{p}_k] = i\delta_{jk}$ in (24.13) and $[\hat{X}_j, \hat{Y}_k] = 2i\delta_{jk}$ for quadrature operators, i.e. $V(\hat{x}_j) = V\left(\frac{\delta\hat{X}_j}{\sqrt{2}}\right)$. The latter normalization for quadratures is convenient in the current context while it corresponds to the Heisenberg uncertainty relation bounded by unity and the two-mode squeezing condition of $V_{sq}^+(\hat{X}) < 1$. Analogously,

$$V_{sq}^-(\hat{Y}) = 2 \frac{V(\hat{v})}{a^2 + \frac{1}{a^2}} \quad \text{for } a = \sqrt{\frac{\alpha_1}{g\alpha_2}}. \quad (24.25)$$

Compiling (24.16, 24.17, 24.24, 24.25, 24.15), we can write the non-separability criterion [31, 32] in terms of measurable squeezing variances of two bright beams:

$$V_{sq}^\pm(\hat{X}) + V_{sq}^\mp(\hat{Y}) < 2. \quad (24.26)$$

This is a sufficient criterion for non-separability for any two-mode bipartite state (24.15) put in the form suitable for the experiments where the observables are continuous variables, amplitude and phase quadrature operators. A state obeying (24.26) we refer to as a two-mode non-separable state.

Necessary and sufficient criterion, covariance matrix, correlation matrix and separability criterion for all bipartite Gaussian state. For a certain class of Gaussian two-mode states, inequality (24.26) can give a necessary and sufficient condition for a state being entangled [32, 35]. This is, for

example, the case for bright entangled beams generated in our experiment [11] (Sec. 3.) and it corresponds to a particular choice of the \hat{X}_j , \hat{Y}_j basis ensuring maximal available correlations and to the optimized gain g^{opt} [32]. In general, a Gaussian state of n modes is completely characterized by a covariance matrix [34] or a correlation matrix [35], the elements of which are measurable quantities, covariances of Gaussian probability distributions describing the correlations between all relevant conjugate variables in and between all involved modes of a Gaussian bipartite state. Separability and the positivity of the partial transpose of any Gaussian bipartite state can be characterized in terms of the correlation matrix [34, 35]. The necessary and sufficient condition for separability [32, 35] and distillability criterion [35] for all Gaussian bipartite states have been recently derived using this formalism (see also chapters 13-15 of this book). The experimental determination of the correlation matrix for bright beams is rather evolved as it requires the use of strong, phase-matched local oscillators or other techniques for tomographic measurements of all quadrature operators. In our current experiments, we thus restrict ourselves to the entanglement characterization using Eq. (24.26) [32]. However, the correlation matrix is an important tool for describing Gaussian states. The development of experimental methods to record it are in progress.

Entanglement quantification and types of entanglement. We aim at entanglement applications in quantum communication with bright beams. For this purpose the following paragraph establishes entanglement measures which are reliably observable in an experiment. We use the notions of two-mode squeezing [33], of non-separability [31, 32] and of the continuous variable EPR paradox [24] to define experimental criteria which are well-suited for the evaluation of continuous entanglement produced in the linear interaction of squeezed fields, in any non-linear interaction, or in QND-interactions. In what follows, the optimal gain is taken to be $g_X^{\text{opt}} = g_Y^{\text{opt}} = g$ assuming a symmetry between the beams in the quantum uncertainties inherent to entangled states and a symmetry in optical powers [24, 11].

1. Squeezed-state entanglement. Squeezed-state-entanglement (SSE in Table 24.1) defines a non-separable [30, 31, 32] two-mode state which satisfies the conditions

$$V_{sq}^{\pm}(\hat{X}) = \frac{V(\hat{X}_1 \pm g \hat{X}_2)}{V(\hat{X}_{1,\text{SN}} + g \hat{X}_{2,\text{SN}})} < 1, \quad (24.27)$$

$$V_{sq}^{\mp}(\hat{Y}) = \frac{V(\hat{Y}_1 \mp g \hat{Y}_2)}{V(\hat{Y}_{1,\text{SN}} + g \hat{Y}_{2,\text{SN}})} < 1 \quad (24.28)$$

for the variances (24.16), (24.17) of conjugate variables with the field modes denoted by the respective subscripts.

Table 24.1 Types of continuous variable non-local correlations.

<i>Generating process</i>	<i>Inter-channel coupling</i>	<i>Correlated variables</i>	<i>Correlation type</i>
OPO type II; Ou et al. [10].	non-linear	$\delta X_1 \propto \delta X_2$ $\delta Y_1 \propto -\delta Y_2$	EPR and/or SSE
OPO type I; Furusawa et al. [22].	linear	$\delta X_1 \propto \delta X_2$ $\delta Y_1 \propto -\delta Y_2$	EPR and/or SSE
Kerr nonlinearity in fibre; Silberhorn et al. [11].	linear	$\delta X_1 \propto -\delta X_2$ $\delta Y_1 \propto \delta Y_2$	EPR and/or SSE
QND (phase shift); Friberg et al. [26].	non-linear	$\Delta\phi_p \propto n_s$ $\Delta\phi_s \propto n_p$	QND; one-way EPR
QND (spectral shift); König et al. [14].	non-linear	$\Delta f_p \propto n_s$ ($p_p \propto n_s$) $\Delta f_s \propto n_p$ ($p_s \propto n_p$)	QND
QND (spectral filtering); König et al. [14].	non-linear	$\delta n_p \propto \delta n_s$	QND
QND (squeezed light beam splitter $V(X_p^{in}) < 1$); Bruckmeier et al. [37].	linear	$X_p \propto X_s$	QND

To test for squeezed-state entanglement one has to determine experimentally the variances (24.16), (24.17) of normalized sum and difference photo currents of the fields 1 and 2 for both amplitude and phase quadratures. For instance, if sum squeezing for the amplitude quadrature is given by $V_{sq}^+(\hat{X}) < 1$ and difference squeezing for the phase by $V_{sq}^-(\hat{Y}) < 1$ then this implies squeezed-state entanglement of the fields 1 and 2. The output state has the nature of the two-mode squeezed state [33], hence its name "squeezed-state entanglement".

Note, that this definition of squeezed-state entanglement refers to the quantum properties of the output fields and can be verified experimentally in a straightforward measurement. In the literature, "squeezed-state entanglement"

Table 24.2 Various boundaries for non-separable states.

<i>Relevant criterion</i>	<i>Physical meaning</i>
	non-separability criterion:
1. $V_{sq}^{\pm}(\hat{X}) + V_{sq}^{\mp}(\hat{Y}) < 2$	always sufficient [32] and for a certain class of Gaussian states also necessary [31, 32, 35]
3. $V_{sq}^{\pm}(\hat{X})V_{sq}^{\mp}(\hat{Y}) < 4$	a sufficient criterion for non-separability [36]
4. $V_{cond}^{\pm}(\hat{X}_1 \hat{X}_2)V_{cond}^{\mp}(\hat{Y}_1 \hat{Y}_2) < 1$	demonstration of the EPR <i>Gedankenexperiment</i> [24]
5. $V_{sq}^{\pm}(\hat{X}) < 1 \wedge V_{sq}^{\mp}(\hat{Y}) < 1$	squeezed-state entanglement
6. $V_{cond}^{\pm}(\hat{X}_1 \hat{X}_2) < 1 \wedge V_{cond}^{\mp}(\hat{Y}_1 \hat{Y}_2) < 1$	EPR entanglement

is sometimes related to the way how entanglement is produced, namely by the interference of two squeezed beams. This is difficult to quantify experimentally. We prefer the definition based on the output properties as this is essentially what counts for further applications.

2. EPR-entanglement. The EPR-entanglement (EPR in Table 24.1) defines a non-separable [30, 31, 32] two-mode state which obeys the inequality (24.9) and which satisfies both conditions (24.8) for the conditional variances of conjugate variables.

The demonstration of the EPR-entanglement implies the experimental observation that the two conditional variances are both well below the quantum

limit:

$$V_{cond}(\hat{X}_1|\hat{X}_2) = \frac{V(\hat{X}_1 \pm g_X^{opt} \hat{X}_2)}{V(\hat{X}_{1,SN})} < 1, \quad (24.29)$$

$$V_{cond}(\hat{Y}_1|\hat{Y}_2) = \frac{V(\hat{Y}_1 \mp g_Y^{opt} \hat{Y}_2)}{V(\hat{Y}_{1,SN})} < 1. \quad (24.30)$$

To test experimentally for EPR entanglement one has to measure the sum and difference photo currents, but a different normalization has to be used compared to (24.16), (24.17). The sum and difference photo currents for both amplitude and phase quadratures are normalized to the shot noise variance of the beam described by the first variable in the argument of V_{cond} .

Requiring quantumness for both conjugate variables. The feasibility of EPR entanglement applications in quantum communication and computation purposes requires:

$$V(\hat{X}_1 \pm g_X^{opt} \hat{X}_2) \ll V(\hat{X}_{j,SN}), \quad V(\hat{Y}_1 \pm g_Y^{opt} \hat{Y}_2) \ll V(\hat{Y}_{j,SN}) \quad (24.31)$$

where the sign " \ll " emphasizes the ability to reliably differentiate between the measured correlation level and the quantum/classical boundary $V(\hat{X}, \hat{Y}_{SN})$. The limit of maximally entangled beams would imply

$$V(\hat{X}_1 \pm g_X^{opt} \hat{X}_2) \rightarrow 0, \quad V(\hat{Y}_1 \pm g_Y^{opt} \hat{Y}_2) \rightarrow 0. \quad (24.32)$$

The closer the continuous entanglement is to the maximal entanglement (24.32), the better is the efficiency and the quality of the information processing based upon it. However, this limit (24.32) is never achieved for continuous variables because it would require an infinite degree of squeezing and therefore an infinite energy content in the system.

The non-separability condition (24.26) is very close to our definition of squeezed-state entanglement. Note, however, that the Peres-Horodecki criterion is not requesting both variances of conjugate variables to drop below the quantum limit. Analogously, the demonstration of the EPR paradox also does not demand each variance of the product to be non-classical. These conditions set limits on the *sum or product* of two variances.

In contrast, the definitions of squeezed-state and EPR-entanglement impose more stringent requirements on the degree of a quantum correlation which are needed for an experimental implementation of quantum communication protocols in accordance with (24.31, 24.32). Both conjugate variables have to exhibit a quantum correlation to guarantee a secure quantum key distribution. A quantum correlation of both conjugate variables is also preferable for the reconstruction of an unknown state in quantum teleportation.

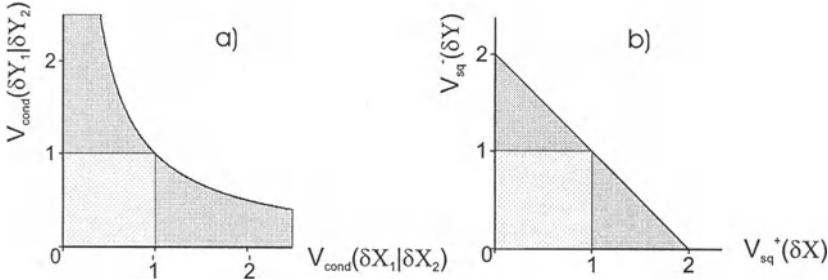


Figure 24.1 Different boundaries for the continuous variable entanglement and respective entanglement regions in terms of conditional and squeezing variances: (a) Demonstration of the EPR-Gedankenexperiment [24] (dark grey region below the curve) and EPR-entanglement (light grey square); (a) Non-separable quantum states [32, 31] (dark grey region below the line) and squeezed-state entanglement (light grey square). The gain is taken to be $g_X = g_Y = g = 1$ to facilitate the comparison. Note, however, that this gain corresponds to the optimal one only on the diagonal of the squares where $V_{\text{cond}}(\delta \hat{X}_1 | \delta \hat{X}_2) = V_{\text{cond}}(\delta \hat{Y}_1 | \delta \hat{Y}_2)$ and $V_{\text{sq}}^+(\delta \hat{X}) = V_{\text{sq}}^-(\delta \hat{Y})$. Thus all the depicted boundaries are sufficient conditions for a quantum state to be entangled.

The discussed limits are summarized in Table 24.2. The mutual relations between these different boundaries is illustrated in Fig. 24.1. Figure 24.1 assumes $g_X^{opt} = g_Y^{opt} = g$, as well as the whole discussion in this paragraph does. Note that for entangled beams asymmetric in terms of uncertainties, different optimal gains might be required for different quadratures. Moreover, to be able to verify the non-separability condition 24.26 in its necessary and sufficient form, local linear unitary Bogoliubov operations should be applied to the two-mode quantum state in this case, i.e. local squeezing transformation together with some rotations [32].

The boundaries (24.27), (24.28), (24.29), (24.30) seem to be the most conservative and reliable experimental criteria for the evaluation of the continuous variable entanglement for quantum communication purposes.

3. QND-entanglement. The QND-entanglement (QND in Table 24.1) defines a non-separable two-mode state [30, 31, 32] which obeys at least one of the inequalities of the type of (24.9) for a QND variable A_s of the signal and an observable B_p of the probe:

$$V_{\text{cond}}^\pm(\hat{A}_s | \hat{B}_p) = \frac{V(\hat{A}_s \pm g \hat{B}_p)}{V(\hat{A}_{s,\text{SN}})} < 1 . \quad (24.33)$$

Here, the conditions

$$[\hat{H}_0, \hat{A}_s] = 0 , \quad [\hat{H}_I, \hat{A}_s] = 0 \quad (24.34)$$

have to be satisfied for the relevant signal variable(s) where $\hat{H} = \hat{H}_0 + \hat{H}_I$ is the total Hamiltonian of the measurement interaction (for explanations and details about a QND measurement see part 3 of this chapter and references therein). An example of such entanglement and its application in quantum communication is the quantum teleportation scheme based on QND-entanglement between field quadratures of bright light [27]. Further examples are considered thoroughly in part 3, where the QND-entanglement emerging in soliton collisions in different schemes is presented.

In analogy to the definitions of EPR versus squeezed-state entanglement, consider the situation when the condition (24.8) is replaced by (24.27), (24.28):

$$V_{sq}^{sp} = \frac{V(\hat{A}_s \pm g \hat{B}_p)}{V(\hat{A}_{s,SN} + g \hat{B}_{p,SN})} < 1. \quad (24.35)$$

That would imply a quantum correlation between signal and probe variables, however, without necessarily the possibility to infer the signal variable \hat{A}_s with a precision below the quantum noise limit by a measurement of the probe \hat{B}_p . In this case the generated entanglement might be too weak for obtaining a QND readout.

The interesting question which still has to be answered is how the EPR-entanglement and the QND-entanglement are related to each other (see Fig. 24.2). One can introduce two sub-classes of the EPR-entanglement important for understanding EPR and QND properties. **Two-way EPR-entanglement** of some conjugate pairs of variables $X_1, Y_1; X_2, Y_2$ obeys not only the EPR conditions stated as:

$$V_{cond}(\hat{X}_1|\hat{X}_2) < 1 \wedge V_{cond}(\hat{Y}_1|\hat{Y}_2) < 1 \quad (24.36)$$

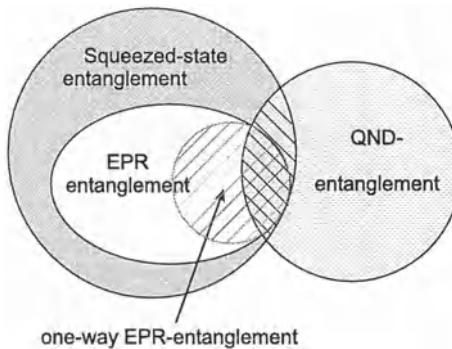


Figure 24.2 Relation between the different types of continuous variable entanglement.

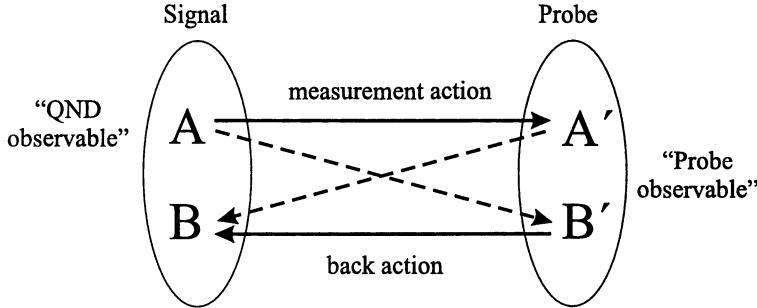


Figure 24.3 QND interaction as one-way EPR-entanglement. Solid and dashed lines correspond to two possible pairs of correlated variables in Eq. 24.38, 24.39.

or

$$V_{cond}(\hat{X}_1|\hat{Y}_2) < 1 \wedge V_{cond}(\hat{Y}_1|\hat{X}_2) < 1 \quad (24.37)$$

but also the same relations under exchange of indices ("second way"). The schemes for continuous entanglement generation involving OPO [10, 24] and interference of squeezed beams [11, 22] all are examples of two-way entanglement.

For **one-way EPR-entanglement** holds (note the order of the indices!):

$$V_{cond}(\hat{X}_1|\hat{X}_2) < 1 \wedge V_{cond}(\hat{Y}_1|\hat{Y}_2) < 1 \quad (24.38)$$

or

$$V_{cond}(\hat{X}_1|\hat{Y}_2) < 1 \wedge V_{cond}(\hat{X}_2|\hat{Y}_1) < 1. \quad (24.39)$$

Though QND-entanglement does not mean EPR entanglement per definition, in many schemes the situation does appear symmetrical for signal and probe pulse and the EPR condition (24.38, 24.39) is satisfied. EPR-entanglement generated in QND interactions always belongs to the sub-class one-way EPR entanglement. A fundamental reason for that is illustrated in diagram of Fig. 24.3. The signal acts on the probe system, modifying the probe observable in accordance with the QND observable. Each measurement imposes an unavoidable back action on the signal system. The peculiar feature of the QND interaction is that the QND observable evades the back action ("back action evading measurement of a signal") channeling the back action of the probe into a signal variable conjugate to the QND one (Fig. 24.3). For details see part 3 of this chapter devoted to the QND measurements. Here we briefly discuss the example of a QND scheme with colliding optical fibre solitons [14, 25, 26]. There the EPR-criterion is satisfied: the phase of the probe pulse is entangled with the photon number of the signal and its photon number is in turn entangled with

the signal phase (see Table 1). However, there is a certain asymmetry which comes from the QND-requirements set on the signal variable. It means, one can conclude on the signal photon number from the measurement of the probe phase. It is also possible to infer the information of the probe phase from the measurement of the signal photon number but it is not possible to do that with a precision below the vacuum noise level. That would contradict the conditions (24.34) set on the QND-variable of the signal. Thus this QND entanglement represents the one-way EPR entanglement between conjugate variables.

For the aim of the QND measurement itself, however, it is not important whether the EPR condition is satisfied or not. What is of interest is the entanglement between the relevant variable of the signal and the observable of the probe. Therefore, in many QND experiments the behaviour of the conjugate pair of the variables was not at all addressed. Are there always two entangled pairs of conjugate variables arising in a QND interaction? Note, that even if there appears to be only one entangled pair, e.g. $\hat{X}_1 \propto \hat{X}_2$ but \hat{Y}_1 is not quantum correlated with \hat{Y}_2 , the situation may change by moving into the other basis, for example, $\hat{X}_1 \cos \theta + \hat{Y}_1 \sin \theta$ and $\hat{X}_2 \cos \phi + \hat{Y}_2 \sin \phi$. In general, the quantum state can be non-separable in only one variable (in each subsystem) and in this sense it can be entangled in one variable. This can be readily seen from the non-separability criterion (24.26) which can be satisfied if only one of the conditional variances obeys the condition (24.33) for EPR-like quantum correlations.

An example of a QND scheme where there seems to be only one entangled pair of variables, i.e. which is not an EPR-entanglement, is a QND measurement of an amplitude quadrature of the signal field via an interference on a beam splitter with an amplitude-squeezed probe field [37]. In the limit of perfect squeezing and assuming a 50/50 beam splitter, the correlation coefficients for both quadratures are equal to unity, $\hat{X}_p^{out} \propto \hat{X}_s^{in=out}$ and $\hat{Y}_s^{out} \propto \hat{Y}_p^{out}$, but the corresponding conditional variances are given by:

$$V_{cond}(\hat{X}_s^{in=out}|\hat{X}_p^{out}) \rightarrow 0, \quad V_{cond}(\hat{Y}_p^{out}|\hat{Y}_s^{out}) \rightarrow 1 \quad (24.40)$$

thus implying the QND-entanglement (24.26, 24.33) but satisfying neither of the EPR conditions (Tab. 24.1).

Figure 24.2 illustrates, how the different entanglement types defined in this paragraph relate to each other. Table 24.1 completes this comparison with examples of various entanglement schemes.

The quality of EPR-entanglement is a critical parameter in quantum communication applications. In the case of continuous variables there are inherent advantages and disadvantages in this respect, as discussed in the introduction. The main advantages are the high efficiency of sources and detectors and the controllable generation process. The main disadvantages are fragility against losses and finite degree of entanglement. In what follows, we attempt

to review the bright entanglement schemes which can deliver a high degree of entanglement, making full use of the advantages discussed in the introduction and exhibiting experimental feasibility with the prospects for technological applications.

3. BRIGHT EPR-ENTANGLEMENT WITH SQUEEZED FIBRE OPTICAL SOLITONS

The generation of entanglement with continuous variables typically uses optical parametric down conversion in a below threshold OPO. This process creates two vacuum states with quantum correlated amplitude and anti-correlated phase quadratures or vice versa [10, 22]. However, because of this entanglement generation being phase sensitive, one has to apply additional more complicated phase locking techniques to the dark output beams to obtain a long-term stable source for EPR-entanglement, which is costly in terms of squeezing. A new promising scheme for the generation of EPR-entangled beams employs the Kerr-nonlinearity of an optical fibre to produce two bright amplitude squeezed pulsed light fields. These fields are made to interfere at a beam splitter with the phase adjusted to obtain two bright output beams of equal power. In this way EPR-entanglement with anti-correlated amplitude and correlated phase quadrature is established between these beams.

3.1 ENTANGLEMENT SCHEME

The scheme, on which the experiment is based, utilizes the superposition of two independently squeezed bright light fields to create quantum correlations between the two output ports [23]. For this purpose the optical phases of the incoming fields are chosen such that the initial fields overlap at the outputs with a phase difference of 90° . Fig.24.4 illustrates this interference graphically in a phase space representation. The ellipses and circles depict the quantum uncertainties of the optical fields (i. e. the half-height contours of Wigner functions) and the sticks relate to the strong classical amplitudes. The uncertainty areas of the input fields are spanned by orthogonal phasors in amplitude and phase direction each contributing respectively to the uncertainties at the outputs. EPR-entanglement is obtained only if quantum correlations for two conjugate quadratures, like amplitude and phase in the described experiment, can be proven (see Eq. (24.29, 24.30)). The anti-squeezed phase quadratures of the inputs dominate the uncertainty areas at the outputs and are responsible for the output correlations. The squeezed amplitude quadratures introduce the errors in the emerging correlations. The 90° phase difference between the interfering fields in Fig. 24.4 guarantees the most precise mapping of the uncertainties of the output beams with minimum errors, which yields the best achievable quantum correlations.

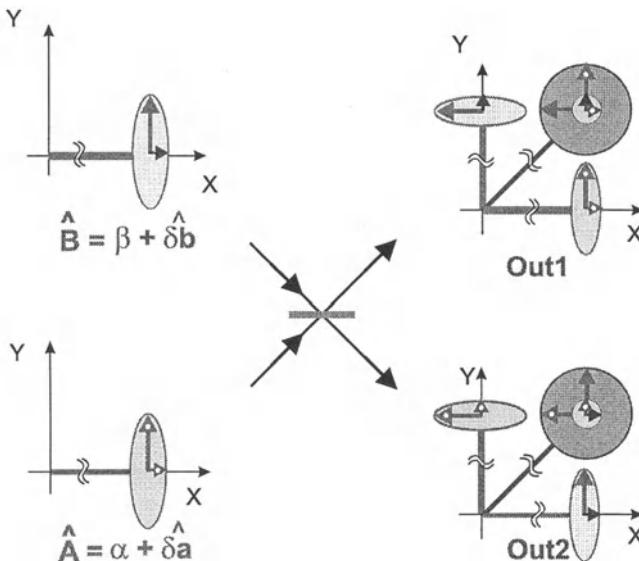


Figure 24.4 Generation of EPR entanglement: interference of two amplitude squeezed beams where the beam splitter is taken to be symmetric ($t = 1/\sqrt{2}$, $r = i/\sqrt{2}$).

In Fig. 24.4 this mapping is illustrated with the help of the input phasors in phase direction (large arrows) spanning the uncertainty regions at the outputs. The classical fields add vectorially and form a new amplitude direction 45° to the input fields. The projections of the phase uncertainties of the incident fields onto the new amplitude direction of the output beams show strict anti-correlations, those onto the new phase direction strict correlations. This would correspond to perfect entanglement. However, the finite amplitude uncertainties of the squeezed input beams reduce the correlations as indicated by the small light circles at the outputs. According to this the sum variance of the two entangled output beams, reflecting the amplitude uncertainties, is decreasing linearly with the squeezing at the inputs. Respectively, the difference variance for the phase uncertainties is growing linearly. The phase diagrams in Fig 24.4 describe the interference of two single mode fields. The reasoning leading to entanglement also holds in the more complex case of squeezed multi-mode fields such as amplitude squeezed pulses [23].

3.2 "TWO-IN-ONE" SQUEEZER FOR SQUEEZED-STATE-ENTANGLEMENT

In the experiment the first task is to produce two independently squeezed beams, which are also optically coherent. An asymmetric fibre Sagnac interferometer [38, 39, 40] can be used to provide directly detectable amplitude

squeezing (photon-number squeezing) of a single beam. This squeezing is highly robust and can be long term stable. The Sagnac interferometer consists of a highly asymmetric beam splitter with a splitting ratio around 90/10 and a polarization maintaining fibre. Polarization maintaining fibres are birefringent with two distinct orthogonal main axes, along which light travels at different speeds. The cross-talk between the corresponding polarizations is negligible in such fibres. Therefore it is possible to build up a "two-in-one squeezer" out of one Sagnac interferometer by adjusting the polarization of the incoming beam to 45° with respect to the slow and fast fibre axes [41]. The energy is then equally distributed between the two corresponding polarizations and two squeezed output beams of orthogonal polarization can be obtained. They can be separated by a polarizing beam splitter.

Fig 24.5 shows the associated experimental setup. A mode-locked Cr⁴⁺:YAG

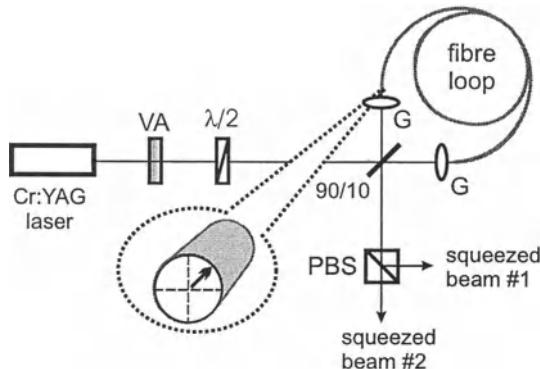


Figure 24.5 Schematic of the experimental setup of a two-in-one-squeezer for the generation of two squeezed beams. VA: variable attenuator, $\lambda/2$: half-wave plate, G: gradient index lens, PBS: polarizing beam splitter, 90/10: beam splitter with 90% reflectivity. Insert shows the polarization direction of the beam at the input of the fibre with respect to the main axes.

laser serves as a source for linearly polarized hyperbolic-secant (sech) shaped optical pulses. After a variable attenuation and the proper orientation of their polarizations by a half wave plate the pulses are launched into the Sagnac interferometer. In order to run the fibre Sagnac interferometer on both axes the splitting ratio has to be approximately the same for all polarizations. Therefore the angle of incidence at the asymmetric beam splitter is chosen to be sufficiently close to 0° to ensure that the mirror reflectivities are the same for both polarization. Thus a strong and a weak pulse counter-propagate through the Sagnac loop for each polarization. Due to the different propagation speeds along the fibre axes each of the two co-propagating pulses of the incoming beam will separate quickly after only a few centimeters inside the fibre. This

ensures the independence of the squeezing of the two output beams, which was checked experimentally.

The Kerr nonlinearity induces an intensity dependent phase shift during the propagation of the pulses along the fibre. This in turn provides a relative phase shift between the strong and weak counter-propagating pulses having the same polarization and it influences the quantum characteristics of the strong pulse. In a single mode model the circular shaped phase space uncertainty of a coherent light field is formed into an ellipse by the Kerr effect during the propagation along the fibre [42, 43]. However, in order to be able to detect the amplitude-squeezing in direct detection, the uncertainty ellipse has to be realigned. The interference of the strong pulse with the weak one at the output of a fibre Sagnac interferometer implements this re-orientation due to the Kerr-induced relative phase shift between the strong and weak counter-propagating pulses [42]. Still, the intensity dependent phase of the interference has to be matched and hence the directly detectable amplitude squeezing depends on the pulse energy. To detect the squeezing, the light is equally distributed to a pair of balanced photo diodes of high efficiency and the generated photo currents are added and subtracted. The noise variances of the sum and difference signals give the noise of the output beam and the corresponding shot noise level. Fig. 24.6 shows the results for the output ports of the described "two-in-one" squeezer. The noise powers in Fig. 24.6 are recorded as a function of the input energy and the grey areas indicate energy ranges where squeezing occurs.

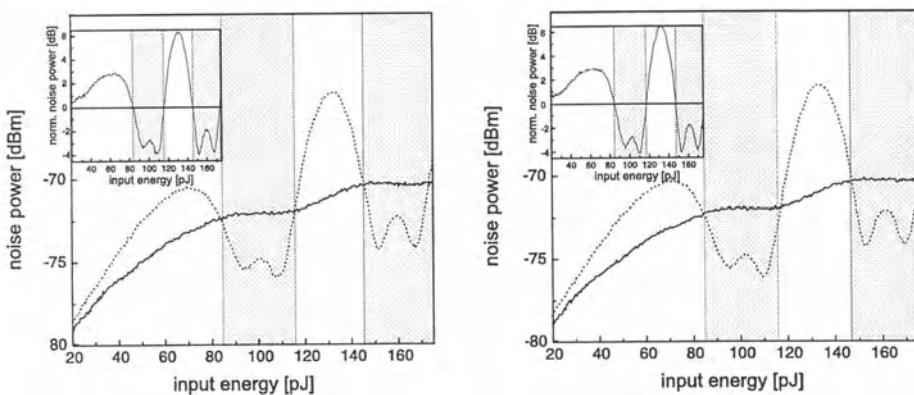


Figure 24.6 Noise powers of the outputs of a "two-in-one" squeezer as a function of the input energy; doted line: noise of the output beams; solid line: corresponding shot noise levels as derived from the difference signal and verified by attenuation measurements. Inserts show the normalized variances of the respective traces.

3.3 GENERATION OF EPR CORRELATIONS BY LINEAR INTERFERENCE

In order to obtain the interference of the two squeezed beams emerging from the Sagnac interferometer one has to have temporal, spatial, polarization and spectral overlaps of the outgoing pulses. Therefore the traveling time difference of the pulses inside the fibre is compensated for by an appropriate delay line. A half wave plate corrects the polarization and the phase is controlled by using the DC output signals of the detectors. In the following again only the single mode picture of Fig. 24.4 is used to model the conditions of the superposition of the independently squeezed light fields at the beam splitter. However, because of the beam splitter being a linear element, it is possible to extrapolate all conclusions directly from the single-mode situation to the multi-mode one by the superposition principle. In this consideration the Raman effect is ignored, which introduces a spectral shift of the sub-picosecond pulses and decreases the spectral overlap of the pulses during the interference.

To evaluate the EPR-entanglement and its dependence on squeezing, the noise variance of the input and output beams are calculated using the ansatz of a strong coherent amplitude and the linearized treatment of the uncertainties. The annihilation operator of the field is given by $\hat{a} = \alpha + \delta\hat{a}$ with α being the coherent amplitude of a classical mean field and the operator $\delta\hat{a}$ describing the quantum uncertainty. To model a superposition on the beam splitter, the classical parts of the input fields are both taken to be real with no relative phase difference. The beam splitter in Fig. 24.4 introduces a phase shift of 90° for each reflection, whereas the transmitted beams do not experience any phase shift. This gives the output fields $\hat{a} = r\hat{A} + t\hat{B}$ and $\hat{b} = t\hat{A} + r\hat{B}$ with reflection $r = i\frac{1}{\sqrt{2}}$ and transmission $t = \frac{1}{\sqrt{2}}$ coefficients corresponding to the situation of Fig. 24.4. If the amplitude quadrature is denoted by $\hat{X}_a = \hat{a}^\dagger(t) + \hat{a}(t)$ and the phase quadrature by $\hat{Y}_a = i(\hat{a}^\dagger(t) - \hat{a}(t))$ the spectral variances of the beams $V(\hat{X}_a) = V(\hat{X}_a(\omega)) = \langle |\delta\hat{a}(\omega) + \delta\hat{a}^\dagger(\omega)|^2 \rangle$ and $V(\hat{Y}_a) = V(\hat{Y}_a(\omega)) = \langle |\delta\hat{a}(\omega) - \delta\hat{a}^\dagger(\omega)|^2 \rangle$ can be calculated via Fourier transformation. In the experiment the amplitude anti-correlations of the output beams are demonstrated by directly detecting the sum and difference photo currents at the two output ports. Fig 24.7 shows the expected noise variances of the output beams (normalized to their respective shot noise level) as a function of the squeezing of the input beams calculated for minimum uncertainty input states.

The experimental data for the amplitude anti-correlation are recorded similar to the squeezing results, where the noise powers of the different traces are plotted versus the input power of the Sagnac interferometer [11]. In Fig. 24.8, traces 1 and 2 indicate the noise powers of the sum and the difference of the two output beams. Traces 3 and 4 show the noise of the individual beams, and

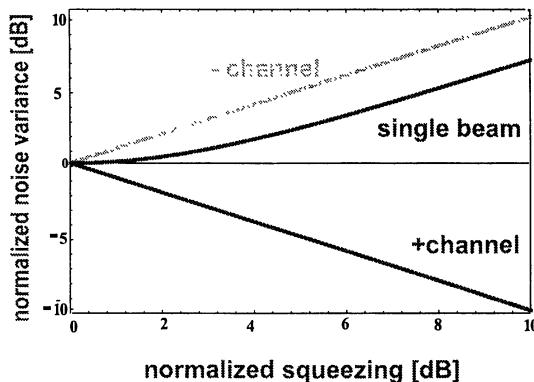


Figure 24.7 Calculated noise variances of the output beams at the beam splitter versus the squeezing of the input beams for minimum uncertainty states.

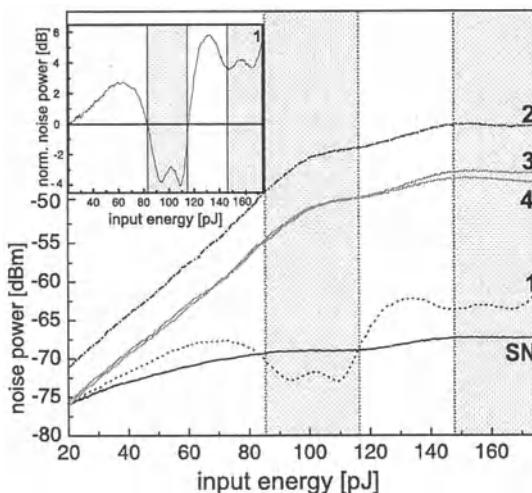


Figure 24.8 Experimental data: noise measurements of the output beams at the beam splitter; insert shows normalized variance of the sum of the output beams demonstrating amplitude quantum correlation

the trace labeled SN gives the shot noise level, which corresponds to the optical power of the combined output beams. The grey areas mark energy regions, where the fields entering the input ports of the beam splitter are amplitude-squeezed (see Figs. 24.7 and 24.8).

The calculations (see Fig. 24.7) predict no correlations for coherent states with shot noise limited uncertainty for amplitude and phase. In the experimental data of Fig. 24.6 and Fig. 24.8 these states should be found at the boundaries of

the grey areas, which correspond to 0 dB input squeezing. However, in Fig. 24.8 the noise levels of the sum, difference and single beam signals (traces 1 - 4) at 0 dB input squeezing differ significantly from each other indicating still existing classical anti-correlation of the amplitude quadratures. This phenomenon can be understood by additional noise in the phase quadrature of the input beams due to the interaction of the photon pulse with thermal phonons in the fibre, which leads to classical amplitude anti-correlation in addition to the quantum effects. This classical anti-correlation can result in high correlation coefficients, but the conditional variance as the figure of merit for the quantum correlation will never drop below unity. The enlarged phase noise is present for all energies and explains the high noise powers of the individual output beams as well as the noise trace for the difference photo current. In contrast, calculations for the sum photo current show, that the noise variance of the sum is not affected by the additional phase noise. The noise power of the sum photo currents was observed to drop up to 4.0 ± 0.2 dB below the shot noise level, the quantum limit for the anti-correlation. As expected, this quantum anti-correlation is limited by the squeezing of the input beams, as seen by the comparison of Fig. 24.6 and Fig. 24.7.

Simultaneous squeezing of the input beams is also recorded for higher energies. However, in that region the sum variance of the amplitudes lies above the quantum limit. There are two possible explanations. Firstly, the interference was optimized for lower energies and, secondly, the detection of the quantum amplitude anti-correlation is very sensitive to the balance of the photo-detector pair. In the ideal situation traces 3 and 4 for the single beams in Fig. 24.8 should coincide for all energies, but they separate for the high energy range. This can be attributed to an imbalance of the photo detectors which were calibrated for the lower energy band around 100 pJ.

For the complete determination of the EPR-entanglement in addition the quantum phase correlation has to be investigated. In order to directly measure the phase quadrature variances, strong optical local oscillators with matched spectra and wavefronts are required. To circumvent the experimental difficulties involved when applying this technique to bright light pulses an interferometric measurement scheme for the characterization of the state was invented.

In Fig. 24.9 the source of the EPR-entanglement is treated as a black box with two output beams. These beams are made to interfere at yet another 50/50 beam splitter with the relative phase of the beams being scanned (Fig. 24.10). To prove the non-separability of the state it is now sufficient to record the amplitude noise variance in addition to the shot noise of one of the resulting output beams \hat{c} and \hat{d} . Calculations show, that for a suitable interference phase the reduced amplitude noise of a single output beam is equivalent to the measurement of $\frac{1}{4} \left(V(\hat{X}_a + \hat{X}_b) + V(\hat{Y}_a - \hat{Y}_b) \right)$. The shot noise levels

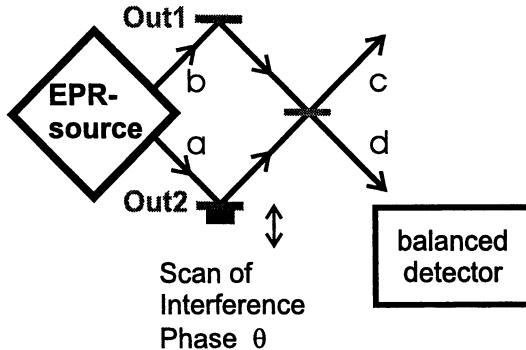


Figure 24.9 Schematic for indirect measurement for the phase quadrature correlation

$V(\hat{X}_{1,SN} + \hat{X}_{2,SN})$ and $V(\hat{Y}_{1,SN} + \hat{Y}_{2,SN})$ are both equivalent to twice the shot noise $V(X_{c/d,SN})$ of \hat{c} or \hat{d} . Thus the normalized amplitude noise of the beams \hat{c} and \hat{d} is given by

$$\frac{1}{4} \left(\frac{V(\hat{X}_a + \hat{X}_b) + V(\hat{Y}_a - \hat{Y}_b)}{V(\hat{X}_{c,d,SN})} \right) = \frac{1}{2} \left(V_{sq}^+(\hat{X}) + V_{sq}^-(\hat{Y}) \right).$$

That means the described setup permits the direct detection of the Peres-Horodecki non-separability criterion for continuous variables (see Eq.24.26):

$$V_{sq}^+(\hat{X}) + V_{sq}^-(\hat{Y}) < 2.$$

In the experiment a value of $V_{sq}^+(\hat{X}) + V_{sq}^-(\hat{Y}) = 0.80 \pm 0.03$ was observed, demonstrating the high non-separability of the state. Fig.24.10 represents the corresponding experimental data.

Provided the variance of the sum of the amplitude of beams \hat{a} and \hat{b} is already known, the quantum phase correlation can be inferred from the measured amplitude noise of \hat{c} or \hat{d} . A quantum phase correlation of up to 4.0 ± 0.4 dB was verified from the data of Fig. 24.10.

Note, that all indicated experimental values describe the noise statistics of the light without correction for linear losses. The photo-detectors showed a detection efficiency of around $92 \pm 5\%$ and the noise powers were recorded for a detection frequency of 10 MHz with a resolution bandwidth of 300 kHz. The measured data are corrected for the electronic noise of the photo-detectors and the spectrum analysers. For quantum information applications the dark noise can limit the availability of the entanglement. If one corrects only the shot noise level for electronic noise to evaluate the quantum limit and for an uncorrected signal noise, the value of $1.12 \pm 0.06 < 2$ was observed in the experiment for the Peres-Horodecki criterion.

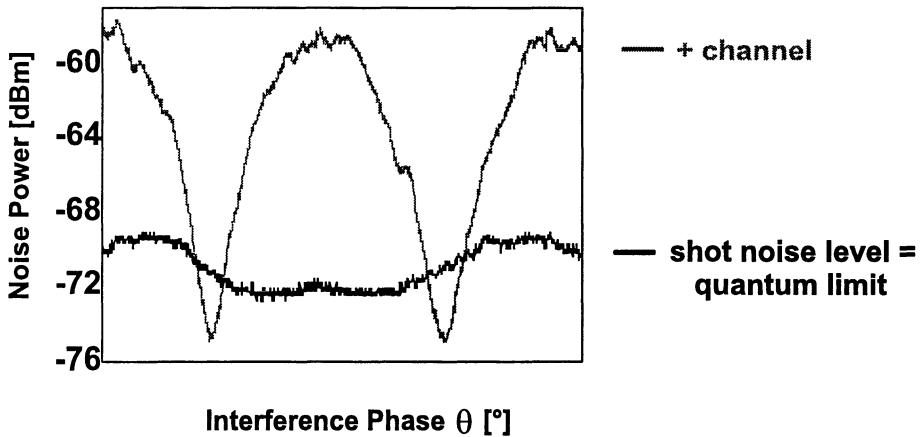


Figure 24.10 Experimental data: Amplitude noise variances for the indirect detection of the phase correlation. For these data the initial squeezed light beams forming the entangled pair interfere with a phase difference of $\phi = 30^\circ$. For $\phi = 90^\circ$ phase difference the noise variance detected in "+" channel will be below shot noise for all phase angles θ (see Fig. 24.9).

3.4 DEMONSTRATION OF THE EPR-PARADOX AND QUANTUM COMMUNICATION

After determining the quantum correlations of the two conjugate variables, amplitude and phase, in addition to the Peres-Horodecki criterion the figures of merit for the demonstration of EPR-entanglement can be calculated (see Eqn. (24.8, 24.9 and 24.29, 24.30)). For the sum of the amplitude quadratures squeezing of up to 4.0 ± 0.2 dB was observed. For the squeezed-state entanglement (24.27, 24.16) this gives $V^+(\hat{X}) = 0.40 \pm 0.02 < 1$. This corresponds to a quantum anti-correlation with a non-classical conditional variance of $V_{cond}(\hat{X}_a|\hat{X}_b) = \frac{V(\delta\hat{X}_a + \delta\hat{X}_b)}{V(\hat{X}_{a,SN})} = 0.80 \pm 0.03 < 1$. Due to the enlarged phase noise of the input fields in this case the optimal gain for (24.8) was $g_X^{opt} = 1$. Similarly, for the phase quadrature difference squeezing (24.28, 24.17) of also up to 4.0 ± 0.4 dB was associated with $V^-(\hat{Y}) = 0.40 \pm 0.04 < 1$. This indicates a quantum correlation with the same non-classical conditional variance of $V_{cond}(\hat{Y}_a|\hat{Y}_b) = \frac{V(\delta\hat{Y}_a - \delta\hat{Y}_b)}{V(\hat{Y}_{a,SN})} = 0.80 \pm 0.07 < 1$ (the optimal gain is again $g_Y^{opt} = 1$). Thus the EPR-paradox for continuous variables (24.9) was demonstrated:

$$V_{cond}(\hat{X}_a|\hat{X}_b) V_{cond}(\hat{Y}_a|\hat{Y}_b) = 0.64 \pm 0.08 \quad (24.41)$$

with a quantum limit of

$$V_{cond}(\hat{X}_a|\hat{X}_b) V_{cond}(\hat{Y}_a|\hat{Y}_b) = 1 \quad (24.42)$$

Equation (24.41) gives an appropriate measure of the EPR-entanglement from the point view of both, fundamental research and experimental applications. In recent years, the study of quantum correlations in quantum optics has experienced a resurgence of interest focusing nowadays more and more on applications in optical transmission systems and signal processing. Soliton squeezing discussed above is being tested for applicability in fibre-optical communication systems [43]. The upward trend towards novel optical technologies has led to new paradigms also for the research in the field of quantum entanglement. The utilization of EPR correlations is evolving from the purely fundamental tests of the validity of quantum mechanics to applications in quantum information processing and communication. These set also other requirements for the correlation measures with a particular emphasis on quantifying the efficiency of the resulting applications, e.g. in optical and quantum communication. Such a "pragmatic" approach leads to defining the quality of correlations by means of signal-to-noise ratios, efficiency of noise reduction in optical signal detection, fidelity of state reconstruction in quantum teleportation, or efficiency and security of quantum key distribution systems. The measures (24.27-24.35) which we have discussed here lie also within this trend. This constitutes a new link between the fundamental and applied aspects of continuous variable quantum correlation.

4. QND EXPERIMENTS WITH OPTICAL SOLITONS

'Quantum nondemolition' (QND) devices are among the basic building blocks of quantum information processing, because of their wide-ranging applications. QND measurements were proposed for entanglement purification for continuous variable entanglement [44], for an eavesdropping attack in the context of quantum cryptography [45, 46], for a quantum optical bus system [47] and for monitoring in quantum computing [48]. Many applications for a back-action evading (BAE) measurement can be derived because it is a paradigm for a quantum mechanical measurement.

The concept of a QND measurement is briefly recalled in section 4.1. In section 4.2 it is described how the interaction of solitons leads to QND measurements. Section 4.3 explains the QND detection scheme with collision induced phase shifts together with the experiments. Finally, in section 4.4 the novel frequency shift QND detection scheme and recent experiments are reviewed.

4.1 CONCEPT OF A QND MEASUREMENT IN QUANTUM OPTICS

Originally the concept of QND detection was introduced by Braginsky and Vorontsov [49] for the quantum mechanical measurement of very small deflections of a massive mechanical resonator for gravitational wave detection (see also [29]). Later this idea was extended from mechanical to optical harmonic oscillators in quantum optics to detect a quadrature component \hat{X}_s of a light field [50, 51, 52].

A QND measurement involves two quantum mechanical systems described by the conjugate pairs \hat{X}_s, \hat{Y}_s for the signal system S and \hat{X}_p, \hat{Y}_p for the probe system P , respectively. The observable to be measured, \hat{X}_s , is referred to as ‘signal’. The state of the system $S + P$ prior to the measurement is given by $|\psi^S\rangle \otimes |\psi^P\rangle$, where $|\psi^S\rangle$ and $|\psi^P\rangle$ are the respective state vectors of S and P . In a first step the signal system S is coupled to the probe system P to establish a correlation between S and P , such that \hat{X}_s can be inferred from a direct measurement on P . Through this correlation S and P are entangled and the system $S + P$ is in a non-separable state. Finally, the state P is directly and destructively measured to infer \hat{X}_s , and thus to reduce the signal state to an eigenstate of \hat{X}_s .

The coupling between S and P is described by the total Hamiltonian $\hat{H} = \hat{H}_0 + \hat{H}_I$ composed of the interaction part \hat{H}_I and the free evolution part \hat{H}_0 of the individual systems S and P . The measurement \hat{H} and the QND variable \hat{X}_s must satisfy certain conditions to allow for a QND measurement [51, 53]. A QND variable \hat{X}_s is required to be a constant of motion ($[\hat{H}_0, \hat{X}_s] = 0$ and $[\hat{H}_I, \hat{X}_s] = 0$)¹ for the unperturbed system described by \hat{H}_0 as well as the interaction \hat{H}_I . The QND measurement is accomplished through a coupling to \hat{Y}_p , i.e. $[\hat{H}_I, \hat{Y}_p] \neq 0$, where \hat{H}_I depends on \hat{X}_s . In this way \hat{Y}_p is affected by \hat{X}_s .

4.2 QND INTERACTIONS OF OPTICAL SOLITONS

Solitons are exact, analytical, and robust solutions of the nonlinear Schrödinger equation, describing pulse propagation in a fibre with group-velocity dispersion and Kerr-effect nonlinearity [55]. In the classical model, solitons are stationary solutions. These particle-like wavepackets recover their shape, velocity and energy after a collision.

In quantum field theory, coherent solitons are non-stationary solutions. The soliton mode is described by the four soliton parameters photon number n , phase ϕ , momentum p and position x [56]. As a QND observable the photon number is most suitable, since it is practically preserved in the evolution of a soliton in a fibre² [43, 57, 58]. This is verified using the Hamilton operator in

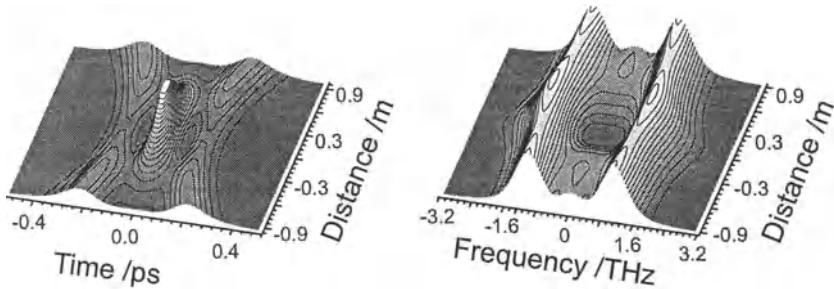


Figure 24.11 Time and frequency domain interaction of two fundamental solitons. The intensity of the field is displayed in a reference frame moving with the center of mass of the solitons.

the fibre [51, 59]:

$$\hat{H} = \hat{H}_s + \hat{H}_p + \hat{H}_I = \hbar\chi_s \hat{n}_s^2 + \hbar\chi_p \hat{n}_p^2 + \hbar\chi_I \hat{n}_s \hat{n}_p; \quad (24.43)$$

it can immediately be seen that the signal photon number is preserved, i.e. $[\hat{H}_s, \hat{n}_s] = 0$. If the photon numbers are as large as 10^8 , a linearized description of the field fluctuations can be used [60]. In terms of quadratures the photon number or amplitude quadrature can then be written as $\hat{X}_s = \hat{n}_s / (2\sqrt{\langle \hat{n}_s \rangle})$ and the conjugate phase quadrature as $\hat{Y}_s = \sqrt{\langle \hat{n}_s \rangle} \hat{\Phi}_s$.³

The Kerr effect couples two copropagating and interacting modes in a fibre by an intensity dependent phase modulation (XPM). In soliton QND schemes XPM coupling is achieved by a soliton interaction, i.e. the collision of a signal with a probe soliton. This is depicted in Fig. 24.11 in the time and in the frequency domain. The colliding pair is described by an unbound solution of the nonlinear Schrödinger equation. Maximum pulse overlap occurs in the center of the collision at $z = 0$. Before the pulses begin to overlap they propagate with unaltered shape as expected from single solitons. The collision transiently disturbs the envelopes of the pulses, which retrieve their pulse envelope, energy, and momentum after the interaction. Therefore only two of the four soliton parameters, the photon number and momentum, are conserved. The photon number preservation during the interaction can be verified with the Hamiltonian of Eq. 24.43, $[\hat{H}_I, \hat{n}_s] = 0$. From the pulse trajectories an acceleration of the pulses towards each other is visible, causing a subsisting shift in phase and position, which depends on the intensity of the other soliton. The probe soliton phase shift is a possible readout for the signal amplitude, because \hat{H}_I is a function of \hat{n}_s and $[\hat{H}_I, \hat{Y}_p] \neq 0$ ($[\hat{Y}_p, \hat{n}_p] \neq 0$) [25, 63]. For a small phase shift, \hat{Y}_p represents the probe phase shift, which can be read out by an interference with an additional phase reference soliton. This type of QND interaction is explained in section 4.3. Transient changes in the solitons

during the collision such as the change in relative velocity of the pulses can be used for a QND readout as well: Because of the chromatic dispersion of the fibre a relative group-velocity increase corresponds to a transient increase in the spectral separation of the pulses (Fig.24.11). Note, that in the center of the collision the spectral density at line center approaches zero. This holds for any relative velocity and phase of the solitons provided they have equal amplitudes. Detecting the spectral shift of the probe pulse serves as a QND readout of the amplitude of the signal soliton, as explained in section 4.4. To date, these two are the only schemes for a QND measurement with solitons in fibres. XPM provides the cross talk mechanism to write the signal intensity information into the probe system without degrading the signal-to-noise ratio of the signal. Thus XPM generates the desired entanglement of the signal and the probe system. The back-action noise introduced by the measurement is fed into the signal phase and position only (Fig. 24.3).

QND measurements based on the Kerr effect were among the first proposals for QND measurements in optics [50, 51, 52]. The first QND experiment was realized using the Kerr effect in fibres [64]. Fibre-optical experiments aiming at back-action evading measurements of a quantum-limited signal intensity are listed in Table 24.3. The experiments used shot-noise limited intensity

Table 24.3 Experiments aiming at fibre QND detection of a shot noise limited signal beam. Pump light denotes the signal/probe power or pulse energy and center wavelength. The correlation coefficient C is the fraction of probe readout photocurrent rms noise due to signal shot noise. L_{eff} is the effective interaction length, different from fibre length due to resonator finesse [65] or pulse walk-off [14, 26, 66].

Pump light	C	ϕ_{XPM} (rad)	Fibre length	L_{eff}	Experimental configuration	Ref.
phase modulated CW, 130 mW@676 nm/ 60 mW@647 nm	0.37	no data	114 m 2 K	114 m	linear travelling wave	[64]; [67]
CW, 15 mW@676 nm/ 16 mW@647 nm	0.26 ^a	no data	13 m	100 m	resonant ring	[65]
solitons, 2.6 ps, 15 pJ @1460.7 nm/3.6 ps, 6 pJ@1455 nm	0.39	1.22	400 m	110 m	linear travelling wave	[26]
solitons, 200 fs, 40 pJ @1495 nm/200 fs, 40 pJ@1510 nm	0.27	0.71	6.3 m	0.9 m	linear travelling wave	[14]

^a Results for temporarily optimum polarization conditions.

fluctuations as a quantum signal (quantum-modulation or quantum-information transfer). A dual successive back-action evading measurement based on the experiment of Ref.[26] was reported as well [66]. The QND experiments of Refs. [26, 64, 65, 67] were limited by background phase noise contaminating the probe phase readout for the signal photon number. The latest experiment [14] was limited by the internal noise structure of the probe solitons (see section 4.4). The general state of the art in QND detection is a conditional noise reduction of the shot-noise limited signal of 3.5 dB(55%) with cold atoms in a trap [68]. A similar result was obtained with an OPA system [69].

4.3 PHASE-SHIFT QND DETECTION

This section discusses the QND detection using the probe phase shift and the optimum field quadrature for a readout. The only experiment so far using phase detection is reviewed. The section summarizes the corresponding discussion given by Sizmann and Leuchs [43]. The phase quadrature of the probe soliton is changed by the collision with the signal soliton and provides information on the signal amplitude quadrature. Investigating small fluctuations in the quadrature field, the input-output relations are:

$$\delta\hat{X}_s^{out} = \delta\hat{X}_s^{in}, \quad \delta\hat{Y}_p^{out} = \delta\hat{Y}_p^{in} + \sigma\delta\hat{X}_p^{in} + \gamma\delta\hat{X}_s^{in}. \quad (24.44)$$

Here γ is the QND gain and σ the self phase modulation (SPM) coefficient. Note that both depend on the interaction lengths. The probe readout quadrature $\delta\hat{Y}_p^{out}$ contains the signal $\delta\hat{X}_s^{in}$. The inevitable back-action noise due to the measurement is channeled into the quadrature \hat{Y}_s , conjugate to \hat{X}_s . However, one typically finds that $\sigma > \gamma$ and the probe observable is contaminated by SPM noise.

The corresponding fibre QND scheme is shown in Fig. 24.12. In order to evaluate the performance of a certain QND device, transfer coefficients are practical quantities for the determination of the signal degradation and information transfer to the probe observable [28, 70, 71]. They are measureable quantities even in a single stage BAE measurement. In the case of uncorrelated input states, i.e. $\langle\hat{X}_s^{in}\hat{Y}_s^{in}\rangle_{sym} = 0$, the transfer coefficients can be derived directly from the correlation coefficients [28]:

$$\begin{aligned} T_s &= C^2(\hat{S}^{in}, \hat{S}^{out}) = \frac{|\langle\hat{S}^{in}\hat{S}^{out}\rangle_{sym}|^2}{\langle\hat{S}^{in 2}\rangle\langle\hat{S}^{out 2}\rangle} \\ T_p &= C^2(\hat{S}^{in}, \hat{P}^{out}) = \frac{|\langle\hat{S}^{in}\hat{P}^{out}\rangle_{sym}|^2}{\langle\hat{S}^{in 2}\rangle\langle\hat{P}^{out 2}\rangle} \end{aligned} \quad (24.45)$$

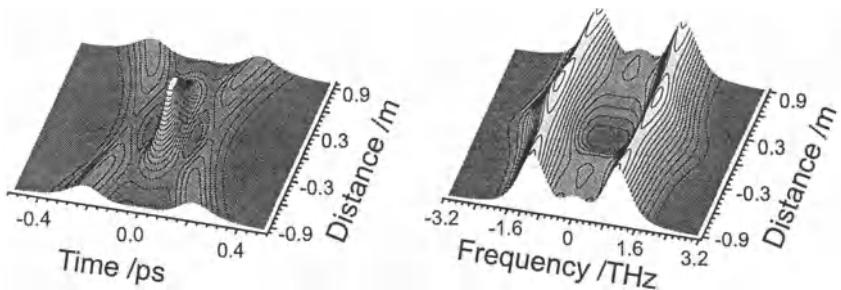


Figure 24.12 QND scheme using XPM induced phase changes in optical fibres. The signal-intensity dependent refractive index changes the phase of a probe pulse and vice versa. A QND measurement of the signal amplitude can be performed via a probe phase detection, leaving the signal amplitude unperturbed (after Sizmann and Leuchs [43]).

Here \hat{S}^{in} , \hat{S}^{out} and \hat{P}^{out} refer to the observables in a general QND measurement. The inequality

$$T_s + T_p > 1 \quad (24.46)$$

characterizes a quantum measurement, in which the signal information is noiselessly amplified. Using Eq. 24.44 we can calculate the transfer coefficients for a coherent signal and a coherent probe input ($V(\hat{X}_s^{in}) = V(\hat{X}_p^{in}) = V(\hat{Y}_p^{in}) = 1$):

$$T_s + T_p = C^2(\delta\hat{X}_s^{in}, \delta\hat{X}_s^{out}) + C^2(\delta\hat{X}_s^{in}, \delta\hat{Y}_p^{out}) = 1 + \frac{\gamma^2}{1 + \gamma^2 + \sigma^2} \quad (24.47)$$

Without self-phase modulation acting on the probe ($\sigma = 0$) a nearby perfect QND measurement can be performed by increasing the probe power ($\gamma \rightarrow \infty$). In this case the ‘macroscopic’ phase change of the probe due to the signal dominates over the small phase uncertainty of the probe itself. In practice, however, $\sigma \neq 0$ and self-phase modulation (SPM) phase noise increases proportional to probe power. Photon-number fluctuations of the coherent probe input feed into phase fluctuations via SPM. This way the probe transfer coefficient is degraded, since $\sigma > \gamma$.

To eliminate the SPM noise in Eq. 24.47 for a noiseless QND experiment the probe observable can be changed to a linear combination of phase and amplitude

quadratures [72, 73]. The probe output fluctuations are then measured in the quadrature B_p :

$$\delta \hat{B}_p^{out}(\psi) = \delta \hat{X}_p^{out} \cos(\psi) + \delta \hat{Y}_p^{out} \sin(\psi)$$

and for optimized angle ψ_0 [43]:

$$\delta \hat{B}_p^{out}(\psi_0) = (1 + \sigma^2)^{-1/2} (\delta \hat{Y}_p^{in} + \gamma \delta \hat{X}_s^{in}). \quad (24.48)$$

The probe observable, δB_p^{out} then contains only the probe input phase quadrature noise and the QND copy of the signal. In analogy to Eq.24.47 the sum of the transfer coefficients is:

$$T_s + T_p = 1 + \frac{\gamma^2}{1 + \gamma^2}. \quad (24.49)$$

This semiclassical analysis shows that an SPM-noise-free QND measurement is possible when using a combined amplitude and phase detection.

Experiment with colliding solitons using phase shift detection. In what follows, the experiment with colliding solitons is reviewed which uses phase detection of the probe pulse [26], see also Table 24.3.

In this QND measurement of the signal amplitude one detects the phase change of the probe soliton using a reference soliton which does not interact with the signal soliton, as is shown in Fig. 24.13. A detailed study of this soliton-collision interferometer was performed [74] and with this experiment, Friberg, Machida and Yamamoto [26] realized the first QND measurement with optical solitons in fibres. Signal ($\tau_{FWHM} = 2.6$ ps), probe and reference (each 3.6 ps) pulses were spectrally filtered out from a single pulse of higher energy, which was SPM-broadened to up to 10 nm spectral width in an additional fibre [26]. The timing of the pulses was adjusted such that a complete collision between signal and probe occurred in the 400 m long fibre leaving the reference pulse unaffected. GAWBS⁴ noise was eliminated by a differential technique. The probe soliton followed the reference soliton with a delay of only 30 ps so that both pulses experience the same GAWBS phase fluctuations [76]. On the detection side the signal was separated from probe and reference pulses by a grating and the QND signal was extracted in a Mach-Zehnder interferometer (Fig. 24.13).

The experiment showed a 0.25 dB noise reduction below the combined noise level due to the correlation between signal amplitude and probe phase, where the signal photon number was shot-noise limited. The total transfer $T_s + T_p$ is larger than unity (quantum domain) or just below unity (classical domain) depending on whether or not the losses for the signal are included [26, 43].

An advantage of soliton QND experiments is the straight forward extension to repeated BAE detection. In a double-collision experiment [26, 66] it took

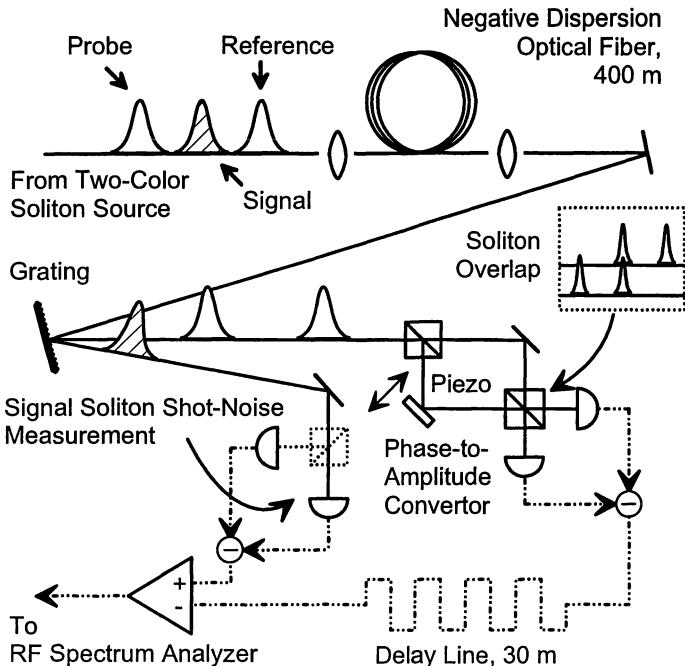


Figure 24.13 Outline of a soliton QND measurement. After the probe-signal collision in the fibre, the phase difference between probe and reference is a readout of the signal soliton photon number. For phase detection, probe and reference interfere with a $\pi/2$ relative phase delay in addition to the group delay (after Friberg et al. [26]).

only a different pulse sequence and a longer fibre to realize two collisions. In the experiment it was shown that probe and reference, when both colliding with the signal, experience the same XPM to within 13 dB. However, repeated BAE detection requires individual readouts of the two probe pulses of the two collisions, which can be implemented in this scheme with two additional solitons which do not collide with the signal soliton.

The soliton QND experiments discussed so far were limited by detection efficiency and by SPM noise of the probe system. The two limitations were inherent in the Mach-Zehnder and the pulse delay detection scheme. The SPM noise limitation leads to a predicted conditional variance which is at best 0.8, corresponding to $T_s + T_p = 1.2$ in this case [72]. To get closer to an ideal soliton QND experiment the probe would have to be detected with a linear combination of amplitude and phase quadratures [72, 77, 78]. A different detection scheme [73] could reduce both classical GAWBS noise and quantum SPM noise simultaneously.

4.4 FREQUENCY-SHIFT QND DETECTION

This section is about the fibre-optical QND scheme using frequency shift detection by spectral filtering. In a first paragraph the historical evolution and the mechanism of the novel approach is considered. Then the experimental realization is reviewed.

Despite the stationary properties of solitons used in the phase shift detecting QND scheme, a coherent quantum soliton propagating in a fibre is nonstationary, i.e. the quantum fluctuations of the field do change. The coherent soliton can be described as a superposition of Fock state solitons, each propagating stationary and experiencing different nonlinear phase shifts (SPM). This led on the one hand to soliton quadrature squeezing experiments [79, 80] and on the other hand to the squeezed state generation by spectral filtering [81]. In further investigations of the latter with shorter fundamental solitons, the multimode quantum correlation structure of a soliton was discovered which was found to be responsible for the observed squeezing [82, 83]. Largely enhanced nonclassical correlations compared to the fundamental soliton were predicted in the case of bound higher order solitons, because of the interaction of its different soliton components [84]. These spectral correlations between soliton components are used in the novel QND detection scheme.

The soliton collision (see Fig. 24.11) corresponds to an unbound second order soliton where the soliton components are the colliding signal and probe pulses. The spectral shift of the two pulses shown in Fig. 24.11 is due to XPM. If the pulse spectra do not overlap, the shift mainly depends on the respective amplitudes of the pulses and the relative group velocity $V = v_s - v_p$. Thus, the frequency shift of one pulse is a measure of the photon number of the other pulse: $\Delta f_p \propto n_s / |V|$. Experimentally, the frequency shift is measured by detecting the part of the probe pulse, which is transmitted through a spectral low- or high-pass filter. The QND conditions (see section 4.1) for the signal photon number conservation are valid for this scheme as well. The interaction depends again on the signal photon number \hat{n}_s . The probe observable is the probe momentum \hat{p}_p , which is proportional to \hat{v}_p . The change in probe velocity in the interaction is related to $[\hat{H}_I, \hat{p}_p] \neq 0$.

Compared to the phase shift QND scheme this scheme provides the following advantages: It creates directly detectable photon number entanglement, it is not affected by thermal or quantum phase diffusion noise (SPM), and it has a higher energy efficiency because no third pulse is required as a phase reference. On the other hand, a drawback of this scheme is a limited QND performance found in the simulation of the experiments [14].

Frequency shift QND experiment. The experimental realization with pulses in the sub-ps regime is shown in Fig. 24.14. The laser source is a modelocked

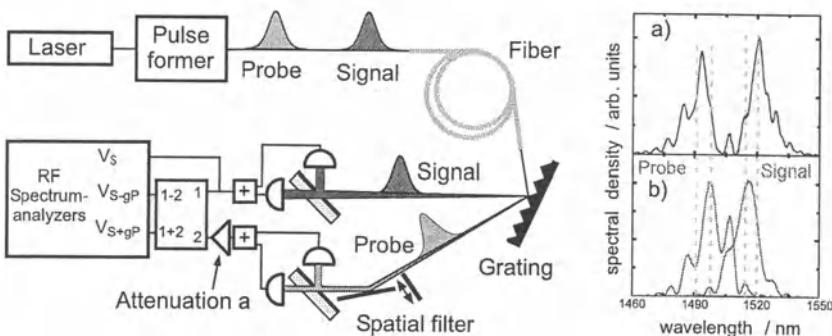


Figure 24.14 The QND experiment using frequency shift detection (left). Experimental spectra (right) (a) of two colliding pulses in the center of the collision and (b) of the pulses without a collision.

solid-state laser emitting 150-fs pulses with 163 MHz repetition rate at the wavelength of 1.5 μm . Each laser pulse is separated spatially by a dichroic mirror into two shot noise limited and uncorrelated signal and probe pulses, each 14 nm in spectral width and spectrally separated by 15 nm. Because of the short length of the pulses only a short interaction length is required to produce spectral correlations [85]. The timing of the pulses is adjusted such that they fully overlap at the end of the fibre. This locates the center of the collision. Output spectra of colliding pulses (a) as well as of non-colliding pulses (b) are displayed in Fig. 24.14 (right). The spectral shift of the respective signal and probe spectra is clearly visible and amounts to approximately half the spectral width of the single pulses (7 nm). In addition to this a modulation appears in the spectrum due to interference with a dispersive background wave created by the slight chirp of the input pulses.

After the pulses leave the fibre they are separated using a grating. In addition, the probe pulse is spectrally filtered by a subsequent spatial slit. Note that the photon number of the probe pulse is preserved in the interaction. The spectral filtering then induces losses to the probe pulse and the transmitted photon number is taken as the probe output. Correlations between the signal and the probe outputs are detected as follows: The photocurrent of the probe is attenuated by an amount a (variable gain g in Fig. 24.14) and added to the signal photocurrent. The input-output relations can be written as

$$\delta\hat{n}_p^{out} = \delta\hat{n}_p^{out,un} + \theta\delta\hat{n}_s^{in}, \quad (24.50)$$

where $\delta\hat{n}_p^{out,un}$ is the uncorrelated part of the photon-number fluctuations of the probe. Assuming $\delta\hat{n}_s^{out} = \delta\hat{n}_s^{in}$, the added mode photocurrent noise is

proportional to:

$$V(\hat{n}_s^{out} + a\hat{n}_p^{out}) = V(\hat{n}_s^{in})(1 + 2\theta a + \theta^2 a^2) + a^2 V(\hat{n}_p^{out,un}), \quad (24.51)$$

where $V(\hat{A})$ denotes a variance $\langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2$ of an observable \hat{A} . An anticorrelation ($\theta < 0$) between signal and filtered probe photon number is anticipated for frequency low-pass filtering of the probe pulse. In that case the combined currents exhibit a noise reduction as a function of a for small a . Results are shown in Fig. 24.15. The variances of the photocurrents are measured simultaneously with two RF spectrum analyzers at 20 MHz with a 300 kHz-resolution bandwidth. A clear noise reduction below the signal noise is found in the

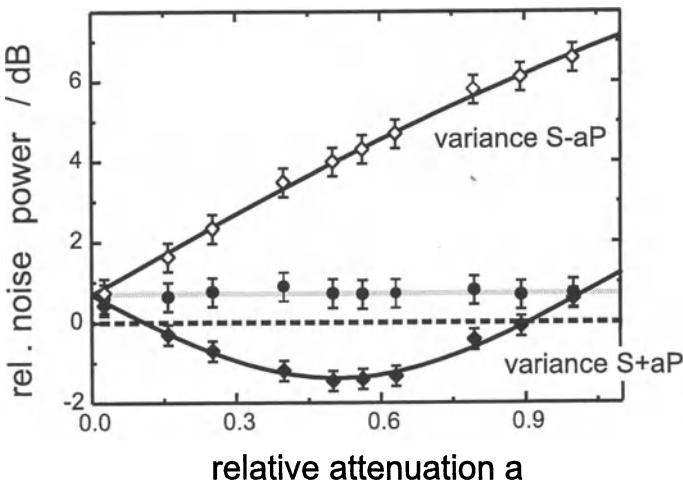


Figure 24.15 Reduction of the signal noise power below the signal shot noise level. A conditional variance of 0.73 results.

added current noise levels, as expected for anticorrelations. Furthermore, the noise reduces by 1.37 dB even below the shot noise level of the signal. This corresponds to a conditional variance smaller than unity and indicates operation in the quantum domain [28]. The noise levels of the plus and minus channels are fitted to a parabola according to Eq. 24.51 (solid lines). The conditional variance of $V_{cond}(n_s|n_p) = 0.73$ is obtained for the measurement in Fig. 24.15, thus satisfying the quantum-state reduction criterion for QND measurements. A strong negative correlation of $C = -0.62$ can be inferred [14]. The small amount of additional noise introduced to the signal is attributed to the experimental inaccuracy and the influence of the stimulated Raman effect. The second criterion for a QND measurement refers to the transfer coefficients which have recently been measured to be in the QND region [14]. Thus the measurement performed so far does fulfill the two QND criteria. Based on the

probe measurement the signal photon number fluctuations could be reduced 27% below the shot noise limit.

The amount of noise reduction in this experiment is limited for several reasons. Firstly, the data were all obtained with a finite detection efficiency. The linear losses were larger than 20% due to finite performance of lenses, grating, beam splitters, mirrors and detectors. In a theoretical investigation it was simulated, however, that the performance of such a system will ultimately be limited by the internal noise structure of the solitons [14]. Compared to the phase measuring QND scheme this scheme shows improved performance due to robustness against phase noise. Although the QND scheme using quadrature detection is predicted to yield better results, the frequency shift QND measurement discussed above achieved the best performance of the soliton QND measurements reported so far.

The soliton QND experiments demonstrate that a spectral filter in a nonlinear optical fibre transmission line can introduce crosstalk between information channels, represented by different carrier frequencies. The technological challenge is to utilize this effect for optical switching, optical tapping and ultrafast nonlinear optical gates. The function of a quantum optical tap of the photon number was demonstrated [14, 26, 66] but other functions might be implemented as well. These are the basic building blocks of any quantum communication system.

Acknowledgments

The authors are grateful to R. Loudon, D. Ostrowsky, R. Werner, B. Buchler, S. Lorenz and T. C. Ralph for fruitful discussions and their support.

Notes

1. In principle deterministic perturbations of \hat{X}_s are allowed [29, 54].
2. In fibres the absorption is typically as low as 0.2 dB/km at $\lambda = 1.5 \mu\text{m}$.
3. For a discussion of the phase operator, see [61, 62].
4. GAWBS = Guided Acoustic Wave Brillouin Scattering [75]

References

- [1] E. Schrödinger, *Naturwiss.*, **23**, 807 (1935).
- [2] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [3] D. Bohm, *Quantum Theory*. Prentice Hall, Englewood Cliffs, NJ, 1951.
- [4] J. S. Bell, *Physics* **1**, 195 (1964).
- [5] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Rev. Prog. Phys.* **23**, 880 (1969); J. F. Clauser and A. Shimony, *Rev. Prog. Phys.* **41**, 1881

- (1978).
- [6] A. Aspect, P. Grangier, and G. Roger, *Phys. Rev. Lett.* **47**, 460 (1981); A. Aspect, J. Dalibard, and G. Roger, *Phys. Rev. Lett.* **49**, 1804 (1982).
 - [7] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993); C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptology* **5**, 3 (1992).
 - [8] For a review see W. Tittel, G. Ribordy, and N. Gisin, *Physics World*, 41 (March 1998); N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145-195 (2002).
 - [9] D. Bouwmeester, A. Ekert, A. Zeilinger (Eds.), *Physics of Quantum Information*. Springer, Berlin, 2000.
 - [10] Z. Y. Ou, S. F. Pereira, H. J. Kimble, K. C. Peng, *Phys. Rev. Lett.* **68**, 3663 (1992).
 - [11] Ch. Silberhorn, P. K. Lam, O. Weiß, F. König, N. Korolkova, and G. Leuchs, *Phys. Rev. Lett.* **86**, 4267 (2001) and quant-ph/0103002.
 - [12] Y. Zhang, H. Wang, X. Li, J. Jing, C. Xie, and K. Peng, *Phys. Rev. A* **62**, 023813 (2000).
 - [13] K. Bencheikh, J. A. Levenson, Ph. Grangier, O. Lopez, *Phys. Rev. Lett.* **75**, 3422 (1995).
 - [14] F. König, B. Buchler, T. Rechtenwald, G. Leuchs, and A. Sizmann, "Soliton back-action evading measurement using spectral filtering", *Phys. Rev. A*, submitted; F. König, T. Rechtenwald, M. A. Zielonka, R. Steidl, G. Leuchs, and A. Sizmann, "Quantum-nondemolition measurement using spectral correlations between fibre-optical pulses." *Conference on Lasers and Electro-Optics/ Quantum Electronics and Laser Science Conference CLEO/QELS'2000*, San Francisco, California, May 7-12, 2000, Technical digest, QThI28, p. 206.
 - [15] F. König, M. A. Zielonka, and A. Sizmann, "Transient photon-number correlations of interacting solitons", *Phys. Rev. A* **66**, in print (2002); A. Sizmann, F. König, M. A. Zielonka, R. Steidl, and T. Rechtenwald, "Quantum correlations of colliding solitons", in *Massive WDM and TDM Soliton Transmission Systems (A ROSC Symposium)*. A. Hasegawa (Ed.), Kluwer Academic Publishers, Dordrecht 2000, p. 289-298.
 - [16] A. Kuhn, M. Hennrich, T. Bondo, and G. Rempe, *Appl. Phys.*, **69**, 373 (1999); M. Hennrich, T. Legero, A. Kuhn, and G. Rempe, *Phys. Rev. Lett.* **85**, 4872 (2000).
 - [17] C. K. Law and H. J. Kimble, *J. Mod. Opt.* **44**, 2067 (1997).
 - [18] B. Huttner and J. Brendel, "Photon-counting techniques for fiber measurements", *Lightwave*, August 2000, pp. 112-120.

- [19] A. Karlsson, M. Bourennane, G. Ribordy, H. Zbinden, J. Bendel, J. Rarity, and P. Tapster, "A single-photon counter for log-haul telecom", *IEEE Circuits & Devices*, November 1999, p. 34.
- [20] S. Lloyd and S. L. Braunstein, *Phys. Rev. Lett.* **82**, 1784 (1999).
- [21] U. Leonhardt, *Measuring the quantum state of light*. Cambridge University Press, 1997.
- [22] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, *Science* **283**, 706 (1998).
- [23] G. Leuchs, T. C. Ralph, C. Silberhorn, and N. Korolkova, *J. Mod. Opt.* **46**, 1927 (1999); G. Leuchs and N. Korolkova, "Entangling fiber solitons: Quantum noise engineering for interferometry and communication", *Optics & Photonic News*, February 2002, p. 64-69.
- [24] M. D. Reid, and P.D. Drummond, *Phys. Rev. Lett.* **60**, 2731 (1988); M. D. Reid, *Phys. Rev. A* **40**, 913 (1989); M. D. Reid, The Einstein-Podolsky-Rosen Paradox and entanglement 1: Signatures of EPR correlations for continuous variables, quant-ph/0112038 (2001).
- [25] H. A. Haus, K. Watanabe, Y. Yamamoto, *J. Opt. Soc. Am. B* **6**, 113 (1989).
- [26] S.R. Friberg, S. Machida, and Y. Yamamoto, *Phys. Rev. Lett.* **69**, 3165 (1992); S. R. Friberg, S. Machida, M. J. Werner, A. Levanon, and T. Mukai, *Phys. Rev. Lett.* **77**, 3775 (1996).
- [27] D. B. Horoshko and S. Ya. Kilin, *Phys. Rev. A* **61**, 032304 (2000).
- [28] M. J. Holland, M.J. Collett, D. F. Walls, and M. D. Levenson, *Phys. Rev. A* **42**, 2995 (1990); J.-P. Poizat, J.-F. Roch, and P. Grangier, *Ann. Phys. Fr.* **19**, 265 (1994).
- [29] V. B. Braginsky, Y. I. Vorontsov and K. S. Thorne, *Science* **209**, 547 (1980).
- [30] R. F. Werner, *Phys. Rev. A* **40**, 4277 (1989).
- [31] R. Simon, *Phys. Rev. Lett.* **84**, 2726 (2000).
- [32] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **84**, 2722 (2000).
- [33] D. F. Walls, G. J. Milburn, *Quantum Optics*. Springer, Berlin, 1995.
- [34] R. F. Werner and M. M. Wolf, *Phys. Rev. Lett.* **86**, 3658 (2001).
- [35] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, *Phys. Rev. Lett.* **87**, 167904 (2001); G. Giedke, L.-M. Duan, J. I. Cirac, and P. Zoller, *Quant. Inf. Comp.* **1**, 79 (2001); G. Giedke and J. I. Cirac, "The characterization of Gaussian operations and Distillation of Gaussian States", quant-ph/0204085.
- [36] S. Mancini, V. Giovannetti, D. Vitali, and P. Tombesi, Entangling macroscopic oscillators exploiting radiation pressure, quant-ph/0108044.

- [37] R. Bruckmeier, H. Hansen, S. Schiller, and J. Mlynek, *Phys. Rev. Lett.* **79**, 43 (1997).
- [38] S. Schmitt, J. Ficker, M. Wolff, F. König, A. Sizmann, and G. Leuchs, *Phys. Rev. Lett.* **81**, 2446 (1998).
- [39] D. Krylov, and K. Bergman, *Optics Lett.* **23**, 1390 (1998).
- [40] M. J. Werner, *Phys. Rev. Lett.* **81**, 4232 (1998).
- [41] N. Korolkova, G. Leuchs, S. Schmitt, C. Silberhorn, A. Sizmann, M. Stratmann, O. Weiß, and H. A. Bachor, *Nonlinear Optics*, **24**, 223 (2000).
- [42] M. Kitagawa, and Y. Yamamoto, *Phys. Rev. A* **34**, 3974 (1986).
- [43] A. Sizmann and G. Leuchs, in: E.Wolf (ed.), *Progress in Optics XXXIV*. Elsevier Science Publishers B. V., Amsterdam, 1999, p. 373.
- [44] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **84**, 4002 (2000).
- [45] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002); N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (2000); G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).
- [46] J. A. Levenson, I. Abram, T. Rivera, P. Fayolle, J. C. Garreau, and P. Grangier, *Phys. Rev. Lett.* **70**, 267 (1993); J. Ph. Poizat and P. Grangier, *Phys. Rev. Lett.* **70**, 271 (1993); E. Goobar, A. Karlsson, and G. Björk, *Phys. Rev. Lett.* **71**, 2002 (1993).
- [47] Ph. Grangier, *International Quantum Electronics Conference IQEC'2000*, Nice, September 10-15, 2000, Tutorial talk.
- [48] M. Ozawa, *Phys. Rev. Lett.* **80**, 631 (1998).
- [49] V. B. Braginsky and Y. I. Vorontsov, Sov. Phys.-Usp. **17**, 644 (1974).
- [50] G. J. Milburn and D. F. Walls, *Phys. Rev. A* **28**, 2065 (1983).
- [51] N. Imoto, H. A. Haus, and Y. Yamamoto, *Phys. Rev. A* **32**, 2287 (1985).
- [52] B. Yurke, *J. Opt. Soc. Am. B* **2**, 732 (1985).
- [53] C. M. Caves, *Phys. Rev. Lett.* **45**, 75 (1980).
- [54] W. G. Unruh, *Phys. Rev. D* **19**, 2888 (1979).
- [55] G. P. Agrawal, *Nonlinear Fiber Optics*. Academic Press, Inc., San Diego, California, 1995.
- [56] Y. Lai and H. A. Haus, *Phys. Rev. A* **40**, 854 (1989).
- [57] P. D. Drummond, R. M. Shelby, S. R. Friberg, and Y. Yamamoto, *Nature* **365**, 307 (1993).
- [58] Ph. Grangier, J. A. Levenson, and J.-P. Poizat, *Nature* **396**, 537 (1998).
- [59] M. Kitagawa, N. Imoto, and Y. Yamamoto, *Phys. Rev. A* **35**, 5270 (1987).

- [60] H. A. Haus and Y. Lai, *J. Opt. Soc. Am. B* **7**, 386 (1990).
- [61] P. Carruthers and M. Nieto, *Phys. Rev. Lett.* **14**, 387 (1965).
- [62] W. Vogel and D.-G. Welsch, *Lectures on Quantum Optics*. Akademie Verlag, Berlin, 1994.
- [63] V. E. Zakharov and A. B. Shabat, *Zh. Eksp. Teor. Fiz.* **61**, 118 (1971), [*Sov. Phys. JETP* **34**, 62 (1972)].
- [64] M. D. Levenson, R. M. Shelby, M. Reid, and D. F. Walls, Y. Yamamoto, *Phys. Rev. Lett.* **57**, 2473 (1986).
- [65] H. A. Bachor, M. S. Levenson, D. F. Walls, S. H. Perlmutter, and R. M. Shelby, *Phys. Rev. A* **38**, 180 (1988).
- [66] S. R. Friberg, T. Mukai, and S. Machida, *Phys. Rev. Lett.* **84**, 59 (2000).
- [67] M. D. Levenson and R. M. Shelby, *J. Mod. Opt.* **34**, 775 (1987).
- [68] J.-F. Roch, K. Vigneron, P. Grelu, A. Sinatra, J.-P. Poizat, and Ph. Grangier, *Phys. Rev. Lett.* **78**, 634 (1997).
- [69] B. Buchler, P. K. Lam, H. A. Bachor, U. Anderson and T. C. Ralph, *Phys. Rev. A* **65**, 011803(R).
- [70] N. Imoto and S. Saito, *Phys. Rev. A* **39**, 675 (1989).
- [71] Ph. Grangier, J. M. Courty, and S. Reynaud, *Opt. Commun.* **89**, 99 (1992).
- [72] P. D. Drummond, J. Breslin, and R. M. Shelby, *Phys. Rev. Lett.* **73**, 2837 (1994).
- [73] J.M. Courty, S. Spälter, F. König, A. Sizmann, and G. Leuchs, *Phys. Rev. A* **58**, 1501 (1998).
- [74] Y. Sakai, R. J. Hawkins, and S. R. Friberg, *Opt. Lett.* **15**, 239 (1990).
- [75] R. M. Shelby, M. D. Levenson, and P. W. Bayer, *Phys. Rev. Lett.* **54**, 939 (1985); R. M. Shelby, M. D. Levenson, and P. W. Bayer, *Phys. Rev. B* **31**, 5244 (1985).
- [76] P. D. Townsend and A. J. Poustie, R. M. Shelby, *Opt. Lett.* **20**, 37 (1995).
- [77] S. S. Yu and Y. Lai, "Quantum non-demolition measurements of the photon number with a fiber ring: enhancement of the correlation through multiple soliton collisions", in *International Quantum Electronics Conference Technical digest*, OSA Technical Digest Series, Sidney, Australia, 1996, **V. 20**, p. 246.
- [78] S. Spälter, P. van Loock, A. Sizmann, and G. Leuchs, *Appl. Phys. B* **64**, 213 (1997).
- [79] S. J. Carter, P. D. Drummond, M. D. Reid, and R. M. Shelby, *Phys. Rev. Lett.* **58**, 1841 (1987).
- [80] M. Rosenbluh and R. M. Shelby, *Phys. Rev. Lett.* **66**, 153 (1991).

- [81] S. R. Friberg, S. Machida, M. J. Werner, A. Levenson, and T. Mukai, *Phys. Rev. Lett.* **77**, 3775 (1996).
- [82] S. Spälter, N. Korolkova, F. König, A. Sizmann, and G. Leuchs, *Phys. Rev. Lett.* **81**, 786 (1998).
- [83] M. Werner and S. Friberg, *Phys. Rev. Lett.* **79**, 4143 (1997).
- [84] E. Schmidt, L. Knöll, D.-G. Welsch, M. Zielonka, F. König, and A. Sizmann, *Phys. Rev. Lett.* **85**, 3801 (2000).
- [85] S. Spälter, M. Burk, U. Strößner, A. Sizmann, and G. Leuchs, *Optics Express* **2**, 77 (1998).

Index

- Abrams-Lloyd, 42
- Algorithm
 - Abrams-Lloyd, 42
 - Deutsch-Jozsa, 7, 32
 - Grover, 8, 33
 - Shor, 7, 41
- Anticline, 284
- BB84 protocol, 332
- Beam splitter, 27, 112, 117, 256, 285–286
- Bell inequality, 5
- Bell-state, 63, 78, 86
- Bit error rate, 298, 302
- Bit, 4
- Cauchy-Schwarz inequality, 123
- Characteristic function, 175
- Check pairs, 327
- CHSH inequality, 133
- Circuit
 - quantum, 116
- Classical teleportation, 89
- Clifford
 - algebra, 49
 - group, 49–50
- Cloning, 277
 - fidelity, 283, 286
- CNOT, 48, 50, 116, 281
- Coherent
 - amplitude, 71
 - state, 71, 300
- Commutation relation, 106
- Completely-positive, 280
- Computational complexity, 7
- Concatenation of cloners, 286
- Conditional variance, 382
- Conjugate observables, 278
- Correlation matrix, 138, 175
- Covariance maxtix, 175
- Covariant, 280
- CSS code, 330
- Damping channel, 348
- Decoherence, 40
- Dense coding, 64, 95
- Deutsch-Jozsa, 7, 32
- Displacement-covariant, 280
- Distillability, 174
- Down conversion, 79
- Eavesdropper, 290
- Efficient simulation, 47
- Entanglement, 60, 250
 - bipartite, 112
 - bound, 174, 180, 211, 213, 218
 - distillation, 173, 207, 323
 - entropy, 194
 - fidelity, 73
 - measure, 61, 194
 - mixed, 115
 - multipartite, 111–112, 114, 125
 - partial, 141
 - purification, 65, 173, 193, 323
 - quantification, 194
 - swapping, 64
- EPR, 59, 68, 255, 382, 390, 396, 400, 404
 - beams, 81, 97
 - pair, 62, 78
 - state, 69, 281
- Error
 - correction, 19
 - probability, 298, 305
- Excess noise, 279
- Exponential speedup, 43
- Factorize, 7
- Feed-forward, 111
- Fidelity, 68, 79, 89
 - cloning, 283, 286
- Fourier, 117
- Gate
 - Pauli, 48
 - phase, 48, 51
 - SUM, 50, 52
- Gaussian, 43, 70, 219

- additive-noise, 289
- cloner, 278, 280, 283
- distribution, 288
- noise, 283
- operation, 207
- raw key, 289
- state, 105, 114, 141, 174, 384
- Generalized uncertainty principle, 297, 299
- GHZ, 105, 114–115
 - operator, 106
 - paradox, 105
 - state, 108
- Gottesman-Knill, 47
- Group
 - Clifford, 49–50
 - Heisenberg-Weyl, 49
 - Pauli, 49
- Grover, 8, 33
- Hadamard, 20, 48, 116
- Hamiltonian, 10
 - Kerr, 12
 - quadratic, 11
- Harmonic oscillator, 38
- Heisenberg-Weyl group, 49
- Homodyne, 99, 120
 - detection, 111
 - measurement, 179
- Hybrid, 37, 40
- Inequality
 - Bell, 5
 - Cauchy-Schwarz, 123
 - CHSH, 133
- Information exclusion principle, 291
- Inseparability, 121, 177–178, 384, 387, 402
 - multipartite, 112, 116
- Joint measurement, 278
- Kerr, 121
 - effect, 14, 399, 407
 - Hamiltonian, 12
 - nonlinearity, 13, 187, 381, 396
- Key pairs, 327
- Kraus operators, 62
- Linear optics, 112, 120
- Local-hidden variable, 105
- Local-realistic theories, 113
- LOCC, 60, 65, 211
- Loss, 307
- Majorization, 114
- Momentum, 116
- Multipartite inseparability, 112, 116
- Mutual information, 100, 304
- Nat, 13
- Non-splitter, 27
- Nonlocality, 105, 131, 137
- OPO, 81, 381
- Optical fibre, 381, 408
- Parity operator, 132
- Partial transpose, 113–114, 180, 218
- Pauli
 - gate, 48
 - group, 49
 - operator, 323
- Phase gate, 48, 51
- Phase-insensitive amplifier, 285–286
- Photon absorption, 345
- Position, 116
- Privacy amplification, 305
- QND, 26, 182, 187, 244–245, 248–250, 381, 405
- Quadrature, 111, 116, 382
- Quantum
 - entanglement, 5
 - circuit, 116
 - cloning, 277
 - communication, 111
 - computation, 4
 - fault-tolerant, 15
 - universal, 10
 - cryptography, 288, 295
 - duty, 71, 89
 - error correction, 15, 21
 - floating point, 10
 - key distribution, 288, 317
 - noise, 84, 296
 - parallelism, 6
 - repeater, 174
 - teleportation, 312
 - uncertainty, 78, 388, 396, 400
- Quasifree transformation, 176
- Qubit, 5, 32, 38
- Qudit, 71–72
- Qunat, 13, 32, 38
- Reconciliation protocol, 290
- Reduction criterion, 174
- Rotation-covariant, 283
- Sagnac interferometer, 397
- Schmidt
 - decomposition, 61, 112, 114
 - number, 61, 220, 224
- Separability
 - full, 123
 - partial, 123
- Separable state, 384
- Shannon theory, 289
- Shor, 7, 41
- Signal transfer coefficient, 302, 309
- Signal-to-noise ratio, 289
- Soliton, 406
 - collision, 407
- Spin squeezing, 244
- Spin states
 - coherent, 234
 - EPR, 235
 - squeezed, 234
- SPM, 410

- Squeezed
 - light, 112, 308
 - state, 42, 112, 180, 236, 284, 319, 388, 413
 - vacuum, 13, 81
- Stabilizer, 48
 - generators, 320
- Standard form, 176
- State swapping, 260
- SUM gate, 50, 52
- Symplectic, 176
- Syndrome, 25–26
- Telecloning, 130
- Teleportation, 63, 67, 77, 255, 258
 - classical, 89
- Theorem
 - Gottesman-Knill, 47
 - no-cloning, 278
 - virial, 26
- Transfer coefficient, 409
- Transform
 - discrete Fourier, 287
 - Fourier, 20, 282
 - Hadamard, 20
- Transpose
 - partial, 113–114, 180, 218
- Tritter, 27
- Two-mode cat state, 202
- Vacuum fluctuations, 82, 283
- Virial theorem, 26
- Von Neumann entropy, 62, 96, 113, 116
- W state, 115
- Wave-packet, 22
- Weyl operator, 175
- Wigner
 - function, 68, 73, 99, 128, 384, 396
 - representation, 128
- XOR, 21, 33, 243–244
- XPM coupling, 407