Quantum Information and Continuous Variable Systems

Dissertation

zur Erlangung des Grades eines
Doktors der Naturwissenschaften

vorgelegt von

Dipl.-Phys. Géza Giedke

durchgeführt am
Institut für Theoretische Physik
der Leopold-Franzens–Universität Innsbruck bei

Prof. Dr. J. Ignacio Cirac

April 2001

Kurzzusammenfassung

Diese Arbeit befaßt sich mit Fragen der Quanteninformation mit unendlichdimensionalen Systemen [kontinuierliche Variablen (KV)]. Wir untersuchen die Separabilitätseigenschaften von Gaußschen Zuständen solcher Systeme. Das Separabilitätsproblem und das Destillierbarkeitsproblem für beliebige *Zwei*parteien-KV-Systeme in Gaußschen Zuständen werden durch Angabe eines Separabilitäts- und eines Destillierbarkeitskriteriums vollständig gelöst. Außerdem untersuchen wir Verfahren zur Verschränktheitsreinigung. Wir zeigen, daß die Standard-Verfahren für Qubits robust gegenüber fehlerhaft implementierten Quantenoperationen sind. Für Gaußsche Zustände finden wir ein universelles Verfahren zur Reinigung sämtlicher destillierbarer Zustände und machen einen konkreten Vorschlag zur quantenoptischen Implementierung eines praktikablen Reinigungsverfahrens. Für den einfachsten Fall eines *Drei*parteien-KV-Systems geben wir eine notwendige und hinreichende Bedingung, die die vollständige Klassifizierung dieser Zustände gemäß ihren Verschränktheitseigenschaften erlaubt.

Abstract

This thesis treats several questions concerning quantum information theory of infinite dimensional continuous variable (CV) systems. We investigate the separability properties of Gaussian states of such systems. Both the separability and the distillability problem for bipartite Gaussian states are solved by deriving operational ctiteria for these properties.

We consider multipartite Gaussian states and obtain a necessary and sufficient condition that allows the complete classification of three-mode tripartite states according to their separability properties.

Moreover we study entanglement distillation protocols. We show that the standard protocols for qubits are robust against inperfect implementation of the required quantum operations. For bipartite Gaussian states we find a universal scheme to distill all distillable states and propose a concrete quantum optical realization.

For this reprint (Oct. 2001) some errors in the original text have been corrected, the references have been updated, and preprints that did appear meanwhile have been reprinted in their published form.

Acknowledgments

With great pleasure I take the opportunity to thank the many people who have contributed to making my time in Innsbruck rewarding and enjoyable.

My first and greatest thanks go to Ignacio Cirac for being the perfect thesis advisor. His guidance and encouragement were essential for this work. I have benefited greatly from his wide and thorough knowledge of physics and of "doing physics" and enjoyed our many long discussions.

Sincere thanks to Peter Zoller, in whose group this work was completed. In particular I thank him for suggesting, together with Ignacio Cirac, the topic that was to become the main part of the Thesis, and for providing a challenging, stimulating, and international environment for doing research.

I thank Lu-Ming Duan and Barbara Kraus for rewarding collaboration on important parts of this Thesis.

I am grateful to many current and former members of the Quantum Optics Group for making this a pleasant, exciting, and enriching place to be – at work and after work. Many thanks to Thomas Busch, Chiara Menotti, Giovanna Morigi, Guifré Vidal, and to James Anglin, Hans Briegel, Tommaso Calarco, Peter Domokos, Lu-Ming Duan, Wolfgang Dür, Peter Fedichev, Simon Gardiner, Klaus Gheri, Peter Horak, Christian Jäkel, Dieter Jaksch, Barbara Kraus, Alberto Madrazo, Belén Paredes, Helmut Ritsch, Karl Schulze, Päivi Törmä for many interesting discussions and good company. Cheers to the Saturday Soccer Team (especially to Raju Khanal and David Tskhakaya) and the Stadtlauf-Teams for many a good kick and race.

My thanks to the staff of the institute, including Hans Embacher, Marion Grünberger, Nicole Jorda, and Julio Lamas-Knapp for making things work.

I gratefully acknowledge three years of full financial support by the Friedrich-Naumann–Stiftung funded by the German Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, and (for the first few months in Innsbruck) by the Austrian Fonds für wissenschaftliche Forschung (FWF). I thank Sam Braunstein for inviting me to the University of Wales in Bangor and the fruitful stay there.

My warmest thanks to my parents, my brothers and my sister for their love and friendship, and for making home a good place to be (when there was a chance).

Contents

1 Introduction

1.1 Quantum Information

Quantum information (QI) research combines ideas from quantum physics, information theory, and computer science to study the implications that the laws of quantum mechanics have on the capabilities of information processing devices. A quantum computer [1, 2] uses quantum mechanical two-level systems ("qubits") instead of the customary classical bits to store information and unitary transformations on the Hilbert space $\left(\mathbb{C}^2\right)^{\otimes n}$ of a n-qubit to process this information. The exponential growth of the dimension of the underlying Hilbert space with the number of qubits holds the key for the quantum-speedup compared to classical computers: A n qubit quantum register can be brought into a state representing a superposition of 2^n different numbers that can then, loosely speaking, be processed simultaneously by the quantum computer. The hard part is to access this information in an efficient way, circumventing the difficulties arising from the fact that quantum information cannot be copied ("cloned", [3]) nor accessed without degrading it. In the early 1980s it was conjectured [1] that quantum mechanics might provide major advantages over classical physics for these purposes and a few ingenious algorithms [4, 2] have meanwhile been found that can indeed make use of this "quantum parallelism" to accelerate computation. Most notable among those are Shor's algorithm for factorizing numbers [5] and Grover's algorithm for unstructured search [6]. While the potential of quantum computers is most closely related to the *superposition principle* of quantum mechanics and the way in which the dimension of coupled quantum systems grows, the *uncertainty principle* can also be put to good use: it is the foundation of protocols that allow the unconditionally secure distribution of secret random keys [7] allowing for provable secure secret communication. Of all applications of QI this is the one closest to real-life implementation [9].

While these applications are probably mostly still decades away, quantum information research has in the meantime produced many surprising insights into the properties of quantum mechanics that are of fundamental interest regardless of potential applications. Maybe the most puzzling quantum mechanical phenomenon is *entanglement*, that is the existence of unusually strong quantum correlations between the components of a composite system. Since the famous paper [11] which showed that quantum mechanics is not a complete, local realistic theory, and the later proof that one can actually experimentally test the assumptions of local realism [12] has entanglement been a major topic of research on the foundations of quantum mechanics. In recent years, the study of entanglement from the point of view of quantum information has revealed many strange and fascinating features of quantum mechanics. Many different kinds of entanglement have been discovered. We are still only beginning to understand their classification, quantification, and application. It is this aspect of QI research – the exploration of the properties of quantum states and quantum operations – that the present Thesis is mainly concerned with. In particular we will consider states of composite quantum systems, e.g. composed of the Hilbert spaces of two spatially separated parties, usually called Alice and Bob, that want to communicate with each other. Quantum correlations between Alice's and Bob's systems enable them to perform tasks not possible by classical means. Given a state ρ of a bipartite quantum system there are at least

three questions to ask corresponding to three major open problems of quantum information theory.

Is ρ separable or is it entangled? A state is called *entangled* (or *inseparable*) if there are genuine quantum correlations between the systems A and B., otherwise it is *separable*. Inseparable states shared between A and B are necessary for quantum communication tasks such as *quantum teleportation* [13] or quantum-enhanced communication and as such a valuable resource. Separable states, on the other hand, can be prepared from a *product state* by local operations and provide no advantage compared to classical communication. Currently, there is no general way known to answer this question for an arbitrary ρ. This "separability problem" is the subject of Sec. 2, and a practical solution (a "separability criterion") for the family of Gaussian states is presented in Subsec. 2.4.

If ρ is entangled – just how *entangled is it*? This question about the proper *quantification* of entanglement has received much attention and many inequivalent measures have been proposed, reflecting the various different kinds of entanglement that have been discovered. This interesting subject ([14] recet review) is not addressed in this Thesis.

A bit more technical is the third question: *If ρ is entangled – can it be transformed into a maximally entangled state by local means*? A state which can be transformed this way is called *distillable*. As will be explained in Sec. 3, which is devoted to the distillability problem, this question addresses the *usefulness* of ρ for certain quantum communication tasks. In Subsec. 3.2 we give an answer to this question for Gaussian states.

1.2 Continuous Quantum Variables

Continuous Variable (CV) systems offer an *analog* approach to quantum information processing in contrast to the more customary *digital* approach based on qubits. In a CV quantum computer the elementary unit of quantum information is represented by a system with infinite dimensional Hilbert space $\mathcal{H} = \mathrm{L}^2(\mathbb{R})$, for example a mode of the electromagnetic field. This allows to represent $x \in \mathbb{R}$ in a CV quantum register instead of the binary digit. The use of infinite dimensional systems for quantum communication was first proposed in [15], where a *quantum teleportation* scheme and a implementation with quantum optical means were suggested. The experimental realization [16] of this proposal in the same year demonstrated the technological promise of quantum optical CV quantum communication. The possibility of universal CV quantum computation was explored in [17] and it was shown that there is a small set of experimentally accessible operations that form a "universal set" in the sense that any operation on $\mathrm{L}^2(\mathbb{R}^n)$ can be approximated arbitrarily well by concatenating members of the set. Moreover it could be shown that CV quantum error correcting codes can be constructed. Only through the clever use of such codes there is hope to realize large-scale quantum computing despite the inevitable imperfections of realistic systems.

But the main advantages of CV systems such as optical modes lies in the area on *quantum communication*, especially for quantum cryptography [19, 20]. Light is probably the best choice as a carrier of information, and it is conceivable that standard telecom fibers may in the future allow for quantum communication. The potential advantages of CV quantum communication compared to qubits are mainly "technological" in nature: due to their much larger Hilbert

space, CV systems may potentially provide much higher bandwidth for quantum communication than, e.g., qubit-based setups. As an example serves the work [21] which shows how arbitrary d-level systems can be encoded in a one CV mode. This encoding is then used in [20] to devise a quantum key distribution protocol that actually makes use of the high dimensionality of the CV system, achieving a bandwidth which would only be limited by the imperfections of the technical realization. Furthermore, some interesting CV states appear to be quite robust against the most common types of noise, and lastly, the main resource needed for quantum communication, namely quantum entanglement, is surprisingly straight forward to generate in CV systems [16, 22]. This makes CV systems a good place to study entanglement and quantum nonlocality experimentally.

While this Thesis is motivated in part by applications of quantum information in communication and computation, it does not deal directly with such applications. Instead, it is concerned with the quantum mechanical resource at the heart of most communication protocols, namely entangled states of composite quantum systems. Since due to the limitations of technology, current experiments are not able to actually prepare all possible quantum states of CV systems, but only members of the family of so-called *Gaussian states*, we investigate the entanglement properties of Gaussian states of multi-party CV systems.

1.3 Outline

This Thesis collects the work done on the on the separability properties of continuous quantum systems in Gaussian states. The four sections are all structured similarly. After a brief introduction to the question addressed in the section there follow reprints of one or more publications or submitted papers, which constitute the main part of the Thesis and contain virtually all new results. **Sec. 2** discusses the separability of bipartite Gaussian states. We formulate to separability problem and derive an separability criterion for all Gaussian states. **Sec. 3** is concerned with the property of distillability and shows that all Gaussian states with negative partial transpose are distillable. In **Sec. 4** actual protocols to distill entangled Gaussian states are investigated and a practical purification protocol is presented. These results are almost entirely due to Dr. Lu-Ming Duan, the principal author of [67, 68] and are included in this Thesis only for completeness. Finally, in **Sec. 5** the separability properties of three-partite Gaussian states are studied. A criterion is obtained that allows to completely classify all tripartite Gaussian states according to their separability properties.

All these chapters make heavy use of many results on Gaussian states and quasifree quantum operations and the corresponding notation. While each publication can be read for itself, the supplementing sections make use of the definitions and lemmas that are collected in Appendix A. Some supplemental material to the subjects covered in Sections 2 to 5.2 is provided in the Appendices B to D.

2 Separability of Gaussian States

Entanglement is maybe the most genuinely "quantum" property physical systems may possess. It occurs in *composite* systems and is a consequence of the superposition principle and the fact that the proper Hilbert space to describe a composite quantum system is the *tensor product* $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ of the subsystems. This contrasts with classical systems, where the phase space of a composite system is the *direct sum* of the subsystems' phase spaces. The superposition principle immediately implies the existence of states such as the *Bell state*

$$|\Phi+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \right), \tag{1}$$

which is the most popular example of a maximally entangled state that are the essential ingredient of quantum information theory. The study of entangled states of bipartite quantum systems is the main topic of this Thesis. In this Section we provide tools to distinguish them from the "other", less interesting states, that are called *separable*.

In the first subsection we introduce the separability problem and review its status in finite dimensions. The second subsection is concerned with separability of Gaussian states of CV systems. It summarizes the results that have been obtained so far, including those of [23, 60] that are reprinted in Subsections 2.3 and 2.4. The latter contains the main result of this section, a separability criterion for all Gaussian states.

2.1 Bipartite Quantum Systems

Definition 2.1 *(Separable State)*
A state ρ of a bipartite system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is called separable *if ρ is a mixture of product states, i.e. if ρ can be written as [24]*

$$\rho = \sum_k p_k \rho_k^{(A)} \otimes \rho_k^{(B)}, \tag{2}$$

where $p_k \geq 0, \sum_k p_k = 1$, and $\rho_k^{(A)}, \rho_k^{(B)}$ are states on $\mathcal{H}_a, \mathcal{H}_B$, resp.

A separable state can be prepared by *local means*, that is by performing local quantum operations on a product state, where

Definition 2.2 *(Local Operations (LOCC))*
A linear map $\mathcal{P} : \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{B}(\mathcal{K}_A \otimes \mathcal{K}_B)$ is called a local quantum operation *and we write $\mathcal{P} \in LOCC(\mathcal{H}_A \otimes \mathcal{H}_B, \mathcal{K}_A \otimes \mathcal{K}_B)$ if*

$$\mathcal{P} = \sum_k \mathcal{P}_{ak} \otimes \mathcal{P}_{bk} \tag{3}$$

for completely positive maps $\mathcal{P}_{xk} : \mathcal{B}(\mathcal{H}_x) \to \mathcal{B}(\mathcal{K}_x), x = a, b.$

This allows for the most general transformations on the systems A and B (including unitary evolution, generalized measurements, joining of ancilla systems, and discarding of subsystems) and for coordination of these transformations by

classical communication. Since all separable states can be prepared that way, the correlations between the subsystems are purely classical in such a state: no Bell-type inequality is violated, and there is no enhancement of computational power or communication capacity.

States that are not separable are called *inseparable* or *entangled*. These states are responsible for the peculiar non-local aspects of quantum mechanics and therefore of interest for tests of quantum nonlocality as well as for applications in quantum communication and quantum computation. Consequently, these states are at the center of virtually all work on quantum information, and this Thesis is no exception.

The *separability problem* [64], that is the question whether a given state ρ of a composite quantum system is separable or not, is one of the central challenges of quantum information theory. A major effort has been devoted to this problem in recent years, as evidenced by more than 500 E-prints in the Los-Alamos archive[1] (`www.arXiv.org`) devoted to this subject.

In general it is quite difficult to determine, whether a given mixed state ρ of a bipartite system is separable or not, since there are infinitely many ways to write a general mixed state as a mixture of pure states. What one would like to have is a *separability criterion* , that is, a necessary and sufficient condition for separability that is easy to check, i.e. that can be directly calculated from the density matrix of the state. A reformulation of (2) in terms of positive maps indicates how to derive such conditions. First recall

Definition 2.3 *(Positive Maps)*
A map $\mathcal{P}$ on $\mathcal{B}(\mathcal{H})$ is called positive *if $X \geq 0 \Rightarrow \mathcal{P}(X) \geq 0$. If $\mathcal{P}$ is positive and $\mathbb{1} \otimes \mathcal{P}$ is positive on $\mathcal{B}(\mathbb{C}^n \otimes \mathcal{H})$ for all n then $\mathcal{P}$ is called* completely positive.

Positive, but not completely positive maps may reveal the inseparability of a state. We have

Theorem 2.1 *(Separability, [26])*
The state ρ is separable if and only if for all positive maps $\mathcal{P}$ on $\mathcal{B}(\mathcal{H}_A)$

$$(\mathcal{P} \otimes \mathbb{1})(\rho) \geq 0. \tag{4}$$

For any given positive (but not completely positive) map $\mathcal{P}$ this provides us with a practical sufficient condition for inseparability. But this characterization of separability is not a criterion, since there are many positive maps, and little is known about this set (although it has been studied since the 1960s, see [30]). For systems consisting of a two-level system on one side and a two- or three-level system on the other condition (4) turns into a criterion: All positive maps on $\mathbb{C}^2$ are of the form $\mathcal{C}_1 + \mathcal{C}_2\mathcal{T}$, where $\mathcal{C}_1, \mathcal{C}_2$ are completely positive and the positive map $\mathcal{T}$ is transposition [27]: $\mathcal{T}(\rho) = \rho^T$ (in some basis). Positive maps that can be decomposed in this way are called *decomposable*. Therefore we have following Theorem, which was conjectured by Peres [25] and then proved by the Horodeckis [26].

Theorem 2.2 *(Peres-Horodecki separability criterion, [25, 26])*
A state ρ of two qubits ($\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$) is separable if and only if its density

[1] At the latest count (25.4.2001) there were 511 E-prints with "separable", "separability" or "entangled", "entanglement" in the title; among those alone 397 since 1999.

matrix remains positive under partial transposition, i.e.

$$\rho \in \mathcal{B}(\mathcal{H}) \text{ separable } \Leftrightarrow \rho^{T_A} \geq 0. \tag{5}$$

States with positive partial transpose are referred to as ppt *states, states for which* $\rho^{T_A} \ngeq 0$ *are* npt *states.*

This is still true for $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^3$ systems [26] but for higher dimensional systems, no criterion is known. There exist only conditions that are either necessary or sufficient for inseparability and turn into criteria for certain families of states. A good current summary of known conditions for separability is provided in [64].

The general question of inseparability for CV systems contains all the unsolved finite dimensional cases and finding an answer to it is not attempted here. Instead we consider the family of *Gaussian states* (see App. A.1) which contains virtually all generic continuous variable states that can currently be prepared experimentally.

2.2 Separability of Gaussian States

Specializing to Gaussian states greatly simplifies the problem of separability compared to the general CV case. A Gaussian state is completely determined by its correlation matrix (CM) γ and displacement d (see App. A.1). Since any such state is locally equivalent to a state with the same CM γ and $d = 0$ all nonlocal properties of a Gaussian state are determined by its CM. Thus the study of infinite dimensional density matrices can be replaced by finite dimensional correlation matrices. We give a brief review of results on separability of Gaussian states.

The first step towards the solution of the separability problem for Gaussian states was done in [23, 59] where a separability criterion for two-mode Gaussian states was proved; the equivalence of these conditions (not only for Gaussian states) is proved in App. B.

In [23] (reprinted in Subsec. 2.3) it is shown that separable states must satisfy a stronger form of the usual uncertainty relations for the quadrature operators X_k, P_k, and that all inseparable Gaussian states of two modes do violate this relation, which thus provides a separability criterion for these states.

A more elegant approach is due to Simon [59]. He noted that the characteristic function (see A.1) of the transposed state ρ^T is obtained from that of ρ simply by multiplying all the momentum coordinates by -1. For a Gaussian state ρ with CM γ and displacement d we therefore have

$$\tilde{\gamma} = \Lambda\gamma\Lambda \quad \text{and} \quad \tilde{d} = \Lambda d, \tag{6}$$

where $\Lambda = \text{diag}(1, -1, 1, -1, \ldots, 1, -1)$. Consequently, a Gaussian state has nonpositive partial transpose if and only if the CM of the partially transposed states is not a proper CM, i.e. iff (see Subsec. A.3, Lemma A.1)

$$\tilde{\gamma}_A := (\Lambda_A \oplus \mathbb{1})\gamma(\Lambda_A \oplus \mathbb{1}) \ngeq iJ, \tag{7}$$

where Λ_A acts only on the modes of the first subsystem. Sometimes it is more convenient to apply Λ_A on the rhs of this inequality and write $\gamma \ngeq i\tilde{J}_A := i\Lambda_A J \Lambda_A$. With this, Simon showed explicitly, that npt is also necessary for inseparability of two mode Gaussian states. This can be formulated as the

Theorem 2.3 *(Peres-Horodecki Criterion for 1×1 Gaussian States, [23, 59]) A Gaussian state of two modes with CM γ is separable if and only if its partial transpose is positive, i.e. if and only if gamma does not fulfill the condition (7), i.e.*

$$\gamma \geq i\tilde{J}_A. \tag{8}$$

Using the four local invariants x_k (see Subsec. A.3, Eq. (68)) of γ, this can be expressed in very compact form: The state is separable if and only if (see Subsec. A.3, Eq. (71))

$$x_4 + 1 - x_1 - x_2 + 2x_3 \geq 0. \tag{9}$$

In general we consider Gaussian states of $N \times M$ systems consisting of N modes at A's and M modes at B's location and a $(2N + 2M) \times (2N + 2M)$ CM γ. Werner and Wolf [62] have reformulated the separability problem for Gaussian states in a very useful way. They proved

Theorem 2.4 *(Separability of Gaussian States, [62])*
A Gaussian state with CM γ is separable if and only if there exist CMs γ_A, γ_B such that

$$\gamma \geq \gamma_A \oplus \gamma_B. \tag{10}$$

This shows that a Gaussian state is separable iff it can be written as a mixture of Gaussian product states. The condition (10) does, however, not constitute a separability criterion (and thus a solution of the separability problem for Gaussian states), since it is in general not easy to decide whether such CMs γ_A, γ_B exists for a given γ.

The articles reprinted in the following two subsections prove a separability criterion for two important special cases. The elementary case of two modes in a Gaussian state (comparable to the two-qubit system in finite dimensions) is treated in Subsec. 2.3, while in Subsec. 2.4 we show how to turn the condition (10) into a practical separability criterion, which, for an arbitrary Gaussian state, enables us to directly compute whether it is separable or not. This solves the problem of separability for Gaussian states.

2.3 Inseparability criterion for continuous variable systems

Lu-Ming Duan, Géza Giedke, J. Ignacio Cirac, and Peter Zoller,

An inseparability criterion based on the total variance of a pair of Einstein-Podolsky-Rosen type operators is proposed for continuous variable systems. The criterion provides a sufficient condition for entanglement of any two-party continuous variable states. Furthermore, for all the Gaussian states, this criterion turns out to be a necessary and sufficient condition for inseparability.

Phys. Rev. Lett. **84**, 2722 (2000), E-print: quant-ph/9908056.

Inseparability Criterion for Continuous Variable Systems

Lu-Ming Duan,[1,2,*] G. Giedke,[1] J. I. Cirac,[1] and P. Zoller[1]

[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*

(Received 17 August 1999)

An inseparability criterion based on the total variance of a pair of Einstein-Podolsky-Rosen type operators is proposed for continuous variable systems. The criterion provides a sufficient condition for entanglement of any two-party continuous variable states. Furthermore, for all Gaussian states, this criterion turns out to be a necessary and sufficient condition for inseparability.

PACS numbers: 03.67.–a, 03.65.Bz, 42.50.Dv, 89.70.+c

It is now believed that quantum entanglement plays an essential role in all branches of quantum information theory [1]. A problem of great importance is then to check if a state, generally mixed, is entangled or not. Concerning this problem, Peres proposed an inseparability criterion based on partial transpose of the composite density operator [2], which provides a sufficient condition for entanglement. This criterion was later shown by Horodecki to be a necessary and sufficient condition for inseparability of the (2×2)- or (2×3)-dimensional states, but not to be necessary any more for higher-dimensional states [3,4]. Many recent protocols for quantum communication and computation are based on continuous variable quantum systems [5–11], and the continuous variable optical system has been used to experimentally realize the unconditional quantum teleportation [12]. Hence, it is desirable to know if a continuous variable state is entangled or not.

In this paper, we propose a simple inseparability criterion for continuous variable states. The criterion is based on the calculation of the total variance of a pair of Einstein-Podolsky-Rosen (EPR) type operators. We find that, for any separable continuous variable states, the 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 the state. We then investigate how strong the bound is for the set of Gaussian states, which is of great practical importance. It is shown that for a 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. Hence we obtain a necessary and sufficient inseparability criterion for all of the Gaussian continuous variable states.

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:

$$\rho = \sum_i p_i \rho_{i1} \otimes \rho_{i2}\,, \tag{1}$$

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 [13], such as $\hat{x}_1 + \hat{x}_2$ and $\hat{p}_1 - \hat{p}_2$. Therefore, 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 physically entangled continuous variable states—the two-mode squeezed states [14]—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:

$$\hat{u} = |a|\hat{x}_1 + \frac{1}{a}\hat{x}_2\,, \tag{2a}$$

$$\hat{v} = |a|\hat{p}_1 - \frac{1}{a}\hat{p}_2\,, \tag{2b}$$

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 Eqs. (2a) and (2b) 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 Eqs. (2a) and (2b) with the commutators $[\hat{x}_j, \hat{p}_{j'}] = i\delta_{jj'}$ $(j, j' = 1, 2)$ satisfies the inequality

$$\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho \geq a^2 + \frac{1}{a^2}\,. \tag{3}$$

Proof.—We can directly calculate the total variance of the $\hat{u}$ and $\hat{v}$ operators using the decomposition (1) of the density operator ρ, and finally get the following expression:

 0031-9007/00/84(12)/2722(4)$15.00 © 2000 The American Physical Society

$$\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho = \sum_i p_i(\langle\hat{u}^2\rangle_i + \langle\hat{v}^2\rangle_i) - \langle\hat{u}\rangle_\rho^2 - \langle\hat{v}\rangle_\rho^2$$
$$= \sum_i p_i\Big(a^2\langle\hat{x}_1^2\rangle_i + \frac{1}{a^2}\langle\hat{x}_2^2\rangle_i + a^2\langle\hat{p}_1^2\rangle_i + \frac{1}{a^2}\langle\hat{p}_2^2\rangle_i\Big)$$
$$+ 2\frac{a}{|a|}\Big(\sum_i p_i\langle\hat{x}_1\rangle_i\langle\hat{x}_2\rangle_i - \sum_i p_i\langle\hat{p}_1\rangle_i\langle\hat{p}_2\rangle_i\Big) - \langle\hat{u}\rangle_\rho^2 - \langle\hat{v}\rangle_\rho^2$$
$$= \sum_i p_i\Big(a^2\langle(\Delta\hat{x}_1)^2\rangle_i + \frac{1}{a^2}\langle(\Delta\hat{x}_2)^2\rangle_i + a^2\langle(\Delta\hat{p}_1)^2\rangle_i + \frac{1}{a^2}\langle(\Delta\hat{p}_2)^2\rangle_i\Big)$$
$$+ \sum_i p_i\langle\hat{u}\rangle_i^2 - \Big(\sum_i p_i\langle\hat{u}\rangle_i\Big)^2 + \sum_i p_i\langle\hat{v}\rangle_i^2 - \Big(\sum_i p_i\langle\hat{v}\rangle_i\Big)^2. \quad (4)$$

In Eq. (4), the symbol $\langle\cdots\rangle_i$ denotes the average over the product density operator $\rho_{i1}\otimes\rho_{i2}$. It follows from the uncertainty relation that $\langle(\Delta\hat{x}_j)^2\rangle_i + \langle(\Delta\hat{p}_j)^2\rangle_i \geq |[\hat{x}_j,\hat{p}_j]| = 1$ for $j = 1, 2$, and, moreover, by applying the Cauchy-Schwarz inequality $(\sum_i p_i)(\sum_i p_i\langle\hat{u}\rangle_i^2) \geq (\sum_i p_i|\langle\hat{u}\rangle_i|)^2$, we know that the last line of Eq. (4) 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 (1) can be any local operators satisfying the commutators $[\hat{x}_j,\hat{p}_{j'}] = i\delta_{jj'}$. 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 (3) 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 $|a^2 - \frac{1}{a^2}|$, which reduces to zero for $a = 1$. For separable states the much stronger bound given by Eq. (3) must be satisfied. A natural question is then how strong is the bound. Is it strong enough to ensure that, if some inequality in the form of Eq. (3) 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 [5–12], 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 of 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 (3) indeed gives a necessary and sufficient inseparability criterion for all of 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 [14]:

$$\chi^{(w)}(\lambda_1,\lambda_2) = \mathrm{tr}[\rho\exp(\lambda_1\hat{a}_1 - \lambda_1^*\hat{a}_1^\dagger + \lambda_2\hat{a}_2 - \lambda_2^*\hat{a}_2^\dagger)]$$
$$= \mathrm{tr}\{\rho\exp[i\sqrt{2}(\lambda_1^I\hat{x}_1 + \lambda_1^R p_1 + \lambda_2^I\hat{x}_2 + \lambda_2^R\hat{p}_2)]\}, \quad (5)$$

where the parameters $\lambda_j = \lambda_j^R + i\lambda_j^I$, and the annihilation operators $\hat{a}_j = \frac{1}{\sqrt{2}}(\hat{x}_j + i\hat{p}_j)$, with the quadrature amplitudes $\hat{x}_j, \hat{p}_j$ satisfying the commutators $[\hat{x}_j,\hat{p}_{j'}] = i\delta_{jj'}$ $(j, j' = 1, 2)$. 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 [14]. Without loss of generality, we can write $\chi^{(w)}(\lambda_1,\lambda_2)$ in the form

$$\chi^{(w)}(\lambda_1,\lambda_2) = \exp\Big[-\frac{1}{2}(\lambda_1^I,\lambda_1^R,\lambda_2^I,\lambda_2^R)M(\lambda_1^I,\lambda_1^R,\lambda_2^I,\lambda_2^R)^T\Big]. \quad (6)$$

In Eq. (6), 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

$$M = \begin{pmatrix} G_1 & C \\ C^T & G_2 \end{pmatrix}, \quad (7)$$

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 [15]. 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

$$M_s^{\mathrm{I}} = \begin{pmatrix} n & & c & \\ & n & & c' \\ c & & m & \\ & c' & & m \end{pmatrix}, \qquad (n, m \geq 1). \tag{8}$$

Proof.—A LLUBO on the state ρ_G transforms the correlation matrix M in the Wigner characteristic function in the following way:

$$\begin{pmatrix} V_1 & \\ & V_2 \end{pmatrix} M \begin{pmatrix} V_1^T & \\ & V_2^T \end{pmatrix}, \tag{9}$$

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. (7) 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 that the matrix C in Eq. (7) 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 no longer influences G_1' and G_2' 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 $\det M = (nm - c^2)(nm - c'^2)$, respectively.

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

$$M_s^{\mathrm{II}} = \begin{pmatrix} n_1 & & c_1 & \\ & n_2 & & c_2 \\ c_1 & & m_1 & \\ & c_2 & & m_2 \end{pmatrix}, \tag{10}$$

where the n_i, m_i, and c_i satisfy

$$\frac{n_1 - 1}{m_1 - 1} = \frac{n_2 - 1}{m_2 - 1}, \tag{11a}$$

$$|c_1| - |c_2| = \sqrt{(n_1 - 1)(m_1 - 1)} - \sqrt{(n_2 - 1)(m_2 - 1)}. \tag{11b}$$

Proof.—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:

$$M' = \begin{pmatrix} nr_1 & & \sqrt{r_1 r_2}\, c & \\ & \frac{n}{r_1} & & \frac{c'}{\sqrt{r_1 r_2}} \\ \sqrt{r_1 r_2}\, c & & mr_2 & \\ & \frac{c'}{\sqrt{r_1 r_2}} & & \frac{m}{r_2} \end{pmatrix}, \tag{12}$$

where r_1 and r_2 are arbitrary squeezing parameters. M' in Eq. (12) has the standard form M_s^{II} (10) if r_1 and r_2 satisfy the following two equations:

$$\frac{\frac{n}{r_1} - 1}{nr_1 - 1} = \frac{\frac{m}{r_2} - 1}{mr_2 - 1}, \tag{13}$$

$$\sqrt{r_1 r_2}\,|c| - \frac{|c'|}{\sqrt{r_1 r_2}} = \sqrt{(nr_1 - 1)(mr_2 - 1)} - \sqrt{\left(\frac{n}{r_1} - 1\right)\left(\frac{m}{r_2} - 1\right)}. \tag{14}$$

Our task remains to prove that Eqs. (13) and (14) 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), r_2 can be expressed as a continuous function of r_1 with $r_2(r_1 = 1) = 1$ and $r_2(r_1) \xrightarrow{r_1 \to \infty} m$. Substituting this expression $r_2(r_1)$ into Eq. (14), we construct a function $f(r_1)$ by subtracting the right-hand side of Eq. (14) from the left-hand side, i.e., $f(r_1) = \mathrm{left}(14) - \mathrm{right}(14)$. Obviously, $f(r_1 = 1) = |c| - |c'| \geq 0$, and $f(r_1) \xrightarrow{r_1 \to \infty} \sqrt{r_1 m}\,[|c| - \sqrt{n(m - \frac{1}{m})}\,] \leq 0$, 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 $f(r_1 = r_1^*) = 0$. Therefore Eqs. (13) and (14) have at least one solution. This proves lemma 2.

We remark that, corresponding to a given standard form I or II, there is a class of Gaussian states which is equivalent under LLUBOs. Note that separability or inseparability is a property not influenced by LLUBOs, so all of the Gaussian states with the same standard forms have the same separability or inseparability property. With the above preparations, we now 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 (3) is satisfied by the following two EPR type operators

$$\hat{u} = a_0 \hat{x}_1 - \frac{c_1}{|c_1|}\frac{1}{a_0}\hat{x}_2, \tag{15a}$$

$$\hat{v} = a_0 \hat{p}_1 - \frac{c_2}{|c_2|}\frac{1}{a_0}\hat{p}_2, \tag{15b}$$

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 expressions (15a) and (15b) of $\hat{u}$ and $\hat{v}$ into the inequality (3), and calculating $\langle(\Delta\hat{u})^2\rangle + \langle(\Delta\hat{v})^2\rangle$ by using the correlation matrix M_s^{II}, we get the following inequality:

$$a_0^2 \frac{n_1 + n_2}{2} + \frac{m_1 + m_2}{2a_0^2} - |c_1| - |c_2| \geq a_0^2 + \frac{1}{a_0^2}, \tag{16}$$

which, combined with Eqs. (11), yields

$$|c_1| \leq \sqrt{(n_1 - 1)(m_1 - 1)}, \tag{17a}$$

$$|c_2| \leq \sqrt{(n_2 - 1)(m_2 - 1)}. \tag{17b}$$

The inequalities (17a) and (17b) ensures that the matrix $M_s^{\mathrm{II}} - I$ is positive semidefinite. So there exists a Fourier transformation to the following normal characteristic function of the state ρ_G^{II}:

$$\begin{aligned}\chi_{\mathrm{II}}^{(n)}(\lambda_1, \lambda_2) &= \chi_{\mathrm{II}}^{(w)}(\lambda_1, \lambda_2) \exp\left[\frac{1}{2}(|\lambda_1|^2 + |\lambda_2|^2)\right] \\ &= \exp\left[-\frac{1}{2}(\lambda_1^I, \lambda_1^R, \lambda_2^I, \lambda_2^R)(M_s^{\mathrm{II}} - I)\right. \\ &\quad \left.\times (\lambda_1^I, \lambda_1^R, \lambda_2^I, \lambda_2^R)^T\right].\end{aligned} \tag{18}$$

This means that ρ_G^{II} can be expressed as

$$\rho_G^{\mathrm{II}} = \int d^2\alpha\, d^2\beta\, P(\alpha, \beta)\, |\alpha, \beta\rangle\langle\alpha, \beta|, \tag{19}$$

where $P(\alpha, \beta)$ is the Fourier transformation of $\chi_{\mathrm{II}}^{(n)}(\lambda_1, \lambda_2)$ and thus is a positive Gaussian function. Equation (19) 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 of the Gaussian states. We conclude the paper by applying this criterion to a simple example. Consider a two-mode squeezed vacuum state $e^{-r(\hat{a}_1^\dagger \hat{a}_2^\dagger - \hat{a}_1 \hat{a}_2)}|\mathrm{vac}\rangle$ with the squeezing parameter r. This state has been used in recent experiments for continuous variable quantum teleportation [12]. 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 $\overline{n}$. It is easy to show that, after time t, the standard correlation matrix for this Gaussian state has the form of Eq. (8) with $n = m = \cosh(2r)e^{-2\eta t} + (2\overline{n} + 1)(1 - e^{-2\eta t})$ and $c = -c' = \sinh(2r)e^{-2\eta t}$ [16]. Therefore the inseparability criterion means that, if the transmission time t satisfies

$$t < \frac{1}{2\eta} \ln\left(1 + \frac{1 - e^{-2r}}{2\overline{n}}\right), \tag{20}$$

the state is entangled; otherwise it becomes separable. Interestingly, Eq. (20) shows that, if there is only vacuum fluctuation noise, i.e., $\overline{n} = 0$ (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 $\overline{n} \gg 1$, the state is no longer entangled when the transmission time $t \geq \frac{1-e^{-2r}}{4\eta\overline{n}}$.

Note added.—After submission of this work, we became aware of a recent preprint by R. Simon (quant-ph/9909044), which shows that the Peres-Horodecki criterion also provides a necessary and sufficient condition for inseparability of Gaussian continuous variable quantum states.

This work was funded by the Austrian Science Foundation and by the European TMR Network Quantum Information. G. G. acknowledges support by the Friedrich-Naumann-Stiftung.

*Email address: luming.duan@uibk.ac.at

[1] C. H. Bennett, Phys. Today **48**, No. 10, 24 (1995); D. P. DiVincenzo, Science **270**, 255 (1995).
[2] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[4] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[5] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
[6] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[7] S. L. Braunstein, Nature (London) **394**, 47 (1998).
[8] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
[9] G. J. Milburn and S. L. Braunstein, quant-ph/9812018.
[10] P. Loock, A. L. Braunstein, and H. J. Kimble, quant-ph/9902030.
[11] A. S. Parkins and H. J. Kimble, quant-ph/9904062.
[12] A. Furusawa *et al.*, Science **282**, 706 (1998).
[13] A. Einstein, B. Podolsky, and R. Rosen, Phys. Rev. **47**, 777 (1935).
[14] C. W. Gardiner and P. Zoller, *Quantum Noise* (Springer-Verlag, Berlin, 1999), 2nd ed.
[15] S. L. Braunstein, quant-ph/9904002.
[16] L. M. Duan and G. C. Guo, Quantum Semiclass. Opt. **9**, 953 (1997).

2.4 Separability Criterion for all bipartite Gaussian States

Geza Giedke, Barbara Kraus, Maciej Lewenstein, and J. Ignacio Cirac,

We provide a necessary and sufficient condition for separability of Gaussian states of bipartite systems of arbitrarily many modes. The condition provides an operational criterion since it can be checked by simple computation. Moreover, it allows us to find a pure product–state decomposition of any given separable Gaussian state. Our criterion is independent of the one based on partial transposition, and is strictly stronger.

Phys. Rev. Lett. **87**, 167904 (2001); E-print: quant-ph/0104050.

Entanglement Criteria for All Bipartite Gaussian States

G. Giedke,[1] B. Kraus,[1] M. Lewenstein,[2] and J. I. Cirac[1]

[1]*Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*

[2]*Institut für Theoretische Physik, Universität Hannover, 30163 Hannover, Germany*

(Received 10 April 2001; revised manuscript received 9 July 2001; published 1 October 2001)

We provide a necessary and sufficient condition for separability of Gaussian states of bipartite systems of arbitrarily many modes. The condition provides an operational criterion since it can be checked by simple computation. Moreover, it allows us to find a pure product-state decomposition of any given separable Gaussian state. We also show that all bipartite Gaussian states with nonpositive partial transpose are distillable.

DOI: 10.1103/PhysRevLett.87.167904 PACS numbers: 03.65.Ud, 03.65.Ca, 03.67.Hk

Entanglement is the basic ingredient in the philosophical implications of quantum theory. It also plays a crucial role in some fundamental issues of this theory, such as decoherence or the measurement process. Furthermore, it is the basis of most applications in the field of quantum information. However, in spite of their importance, the entanglement properties of systems are far from being understood. In particular, we do not even know how to answer the following question [1]: given two systems A and B in a state described by a density operator ρ, are those systems entangled? This question constitutes the so-called separability problem, and it represents one of the most important theoretical challenges of the emerging theory of quantum information.

During the last few years a significant amount of work in the field of quantum information has been devoted to the separability problem [2]. Until now, the basic tool to study this problem is a *linear* map called partial transposition. Introduced in this context by Peres [3], it provides us with a necessary condition for a density operator to be separable. This condition turns out to be also sufficient in two cases: (a) A and B are two qubits or one qubit and one qutrit [4]; (b) A and B are two modes (continuous variable systems) in a Gaussian state [5]. Thus, in these cases the separability problem is fully solved. However, for higher dimensional systems as well as in the case in which A and B consist of several modes in a joint Gaussian state, partial transposition alone does not provide a general criterion for separability. In both cases, examples of states which in spite of being entangled satisfy the partial transposition criterion have been found [6,7].

In this Letter we solve the separability problem for Gaussian states of an arbitrary number of modes per site. Our method does not rely in any sense on partial transposition, and therefore is entirely different from the ones that have been introduced so far to study this problem [2]. It is based on a *nonlinear* map f: $\gamma_N \rightarrow \gamma_{N+1}$ between matrices γ_N which reveals whether a state ρ is an entangled state or not. In addition, we show that if ρ is entangled and has nonpositive partial transpose then it is distillable [2,8].

Let us start by fixing the notation and recalling some properties of correlation matrices (CMs). A Gaussian state of n modes is completely characterized by a matrix $\gamma \in M_{2n,2n}$ (the set of $2n \times 2n$ matrices), called correlation matrix [9], whose elements are directly measurable quantities. A matrix $\gamma \in M_{2n,2n}$ is a CM if it is real, symmetric, and $\gamma - iJ_n \geq 0$. Here we use [10]

$$J_n \equiv \oplus_{k=1}^{n} J_1, \qquad J_1 \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{1}$$

In the following we will consider two systems A and B, composed of n and m modes, respectively, in a Gaussian state. The corresponding CM will be written as

$$\gamma_0 = \begin{pmatrix} A_0 & C_0 \\ C_0^T & B_0 \end{pmatrix} \geq iJ_{n,m} \tag{2}$$

where $A_0 \in M_{2n,2n}$ and $B_0 \in M_{2m,2m}$ are CM themselves, $C_0 \in M_{2n,2m}$ and $J_{n,m} \equiv J_n \oplus J_m$. In order to simplify the notation, when it is clear from the context we will not write the subscripts to the matrices J and we will not specify the dimensions of the matrices involved in our derivations. In [7] it was shown that a CM of the form (2) is separable (i.e., it corresponds to a separable state) iff there exist two CMs $\gamma_{A,B}$, such that

$$\gamma_0 \geq \gamma_A \oplus \gamma_B . \tag{3}$$

This condition, even though it can be very useful to show that some particular states are entangled [7,11], cannot be directly used in practice to determine whether an arbitrary state is entangled or not, since there is no way of determining $\gamma_{A,B}$ in general. If one can determine them, however, then one can automatically construct an explicit decomposition of the corresponding density operator as a convex combination of product states [7].

Below we present a criterion which allows one to determine whether a given CM, γ_0, is separable or not. To this aim, we define a sequence of matrices $\{\gamma_N\}_{N=0}^{\infty}$ of the form (2). The matrix γ_{N+1} is determined by a discrete map defined as follows: (i) if γ_N is not a CM then $\gamma_{N+1} = 0$;

 © 2001 The American Physical Society

(ii) if γ_N is a CM then

$$A_{N+1} \equiv B_{N+1} \equiv A_N - \mathrm{Re}(X_N), \tag{4a}$$

$$C_{N+1} \equiv -\mathrm{Im}(X_N), \tag{4b}$$

where $X_N \equiv C_N(B_N - iJ)^{-1}C_N^T$ [12]. Note that for $N \geq 1$ we have that $A_N = A_N^T = B_N$ and $C_N = -C_N^T$ are real matrices. The importance of this sequence is that γ_0 is separable iff γ_N is a valid separable CM, and, after some finite number of iterations, γ_N acquires a form in which separability is simple to check. Moreover, starting from that CM we are able to construct the CMs $\gamma_{A,B}$ of Eq. (3) for the original γ_0. Now we state several propositions from which the above results follow. For two technical lemmas, see the Appendix.

First we show that if γ_N is separable, so is γ_{N+1}. Moreover, the CMs $\gamma_{A,B}$ associated to γ_N [cf. Eq. (3)] allow us to construct the corresponding CMs for γ_{N+1}.

Proposition 1: *If for some CMs $\gamma_{A,B}$, we have $\gamma_N \geq \gamma_A \oplus \gamma_B$ then $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$.*

Proof: We use the equivalence (i)–(iii) of Lemma 1 to obtain that $B_N - C_N^T(A_N - \gamma_A)^{-1}C_N \geq \gamma_B \geq iJ$, where the last inequality follows from the fact that γ_B is a CM. Using the equivalence (ii)–(iii) of Lemma 1 we obtain $\gamma_A \leq A_N - C_N(B_N - iJ)^{-1}C_N^T = A_{N+1} + iC_{N+1}$, where we have also used the map (4). According to Lemma 2, this immediately proves the proposition. ■

Now, we show that the converse of Proposition 1 is true. That is, if γ_{N+1} is separable, so is γ_N. Apart from that, the following proposition exhibits how to construct the matrices $\gamma_{A,B}$ [cf. Eq. (3)] related to γ_N starting from the ones corresponding to γ_{N+1}.

Proposition 2: *If for some CM γ_A we have $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$ then $\gamma_N \geq \gamma_A \oplus \gamma_B$ for the CM*

$$\gamma_B \equiv B_N - C_N^T(A_N - \gamma_A)^{-1}C_N. \tag{5}$$

Proof: We use Lemma 2 and the map (4) to transform the inequality $\gamma_{N+1} \geq \gamma_A \oplus \gamma_A$ into $A_N - C_N(B_N - iJ)^{-1}C_N^T \geq \gamma_A$. According to the equivalence (ii)–(iii) of Lemma 1 this implies that $\gamma_B \geq iJ$. Since it is clear from its definition (5), γ_B is also real and symmetric, it is a CM. On the other hand, using the equivalence (i)–(iii) of Lemma 1 we immediately obtain that $\gamma_N \geq \gamma_A \oplus \gamma_B$. ■

Using the fact that for $N \geq 1$, $A_N = B_N$ and the symmetry of the corresponding matrix γ_N we have

Corollary 1: *Under the conditions of Proposition 2, we have $\gamma_N \geq \tilde{\gamma}_A \oplus \tilde{\gamma}_A$, and $\tilde{\gamma}_A \equiv (\gamma_A + \gamma_B)/2 \geq iJ$ is a CM.*

The above propositions imply that γ_0 is separable iff γ_N is separable for all $N > 0$. Thus, if we find some γ_N fulfilling (3) then γ_0 is separable. Thus, we can establish now the main result of this work.

Theorem 1 (separability criterion):

(1) If for some $N \geq 1$ we have $A_N \ngeq iJ$ then γ_0 is not separable.

(2) If for some $N \geq 1$ we have

$$L_N \equiv A_N - \|C_N\|_{\mathrm{op}}\mathbb{1} \geq iJ \tag{6}$$

then γ_0 is separable [13].

Proof: (1) It follows directly from Proposition 1; (2) We will show that $\gamma_N \geq L_N \oplus L_N$, so that according to Proposition 2 γ_0 is separable. We have

$$\gamma_N = L_N \oplus L_N + \begin{pmatrix} \|C_N\|_{\mathrm{op}}\mathbb{1} & C_N \\ C_N^T & \|C_N\|_{\mathrm{op}}\mathbb{1} \end{pmatrix}, \tag{7}$$

so that we just have to prove that the last matrix is positive. But using Lemma 1 this is equivalent to $\|C_N\|_{\mathrm{op}}^2\mathbb{1} \geq C_N^T C_N$, which is always the case. ■

This theorem tells us how to proceed in order to determine if a CM is separable or not. We just have to iterate the map (4) until we find that either A_N is no longer a CM or L_N is a CM. In the first case, we have that γ_0 is not separable, whereas in the second one it is separable. If we wish to find a decomposition of the corresponding density operator as a convex sum of product vectors we simply use the construction given in Corollary 1 until $N = 1$ and then the one of Proposition 2. This will give us the CMs $\gamma_{A,B}$, such that $\gamma_0 \geq \gamma_A \oplus \gamma_B$, from which the decomposition can be easily found [7].

In order to check how fast our method converges we have taken families of CMs and applied to them our criterion. We find that typically with less than five iterations we are able to decide whether a given CM is entangled or not. The most demanding states for the criterion are those which lie very close to the border of the set of separable states (see Proposition 3 below). We challenged the criterion by applying it to states close to this border and still the convergence was very fast (always below 30 steps). Figure 1 illustrates this behavior. We have taken $n = m = 2$ modes, an entangled CM γ_a of the GHZ form [14] (Fig. 1a) and an entangled CM γ_b with positive partial transpose [7] (Fig. 1b). We produced two families of CMs as $\gamma_{a,b}(\epsilon) = \gamma_{a,b} + \epsilon\mathbb{1}$. We have determined $\epsilon_{a,b}$

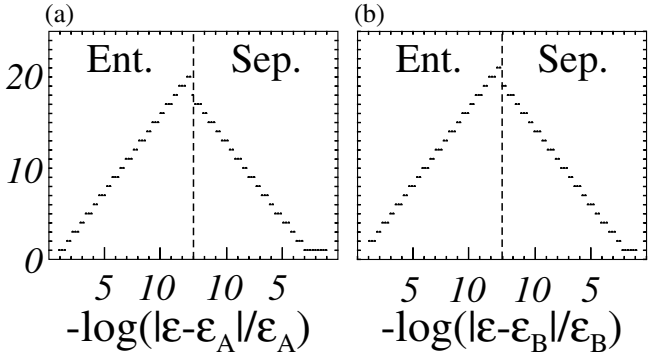

FIG. 1. Number of steps as a function ϵ for CMs of the form $\gamma_{a,b}(\epsilon) = \gamma_{a,b} + \epsilon\mathbb{1}$ where: (a) γ_a taken from Eq. (1) in Ref. [14] with $r = 1/4$, and $\epsilon_a = 0.305\,774\,915\,510(1)$; (b) γ_b taken from Eq. (9) in Ref. [7] and $\epsilon_b = 0.097\,866\,790\,222\,8(4)$.

such that $\gamma_{a,b}(\epsilon)$ become separable. In Fig. 1 we see that in both cases, as we approach $\epsilon_{a,b}$ exponentially fast, the number of needed steps increases linearly. The same behavior is found using instead of $\mathbb{1}$ other positive projectors with different ranks and for different initial CMs. Even though we have tested numerically the rapid convergence of our method, we still have to prove that, except for a zero measure set, it can decide whether a CM is entangled or not after a finite number of steps [15]. We start by considering the set of separable states, defined by $\gamma_0 \geq \gamma_A \oplus \gamma_B$ with $\gamma_{A,B} \geq iJ$. If we just consider those with $\gamma_A > iJ$, we will omit a zero measure set. But then we can show that after a *finite* number of steps these separable states will be detected by our procedure.

Proposition 3: *If* $\gamma_0 \geq \gamma_A \oplus \gamma_B$ *with* $\gamma_A \geq iJ + \epsilon\mathbb{1}$, *then there exists some*

$$N < N_0 \equiv \frac{1}{\epsilon}\left(\|A_0\|_{\mathrm{tr}} - 2n\right) + 1\,, \tag{8}$$

for which condition (6) is fulfilled.

Proof: Using Proposition 1 we have that for all N,

$$A_N - iJ \geq \epsilon\mathbb{1}\,. \tag{9}$$

Thus, $0 \leq \mathrm{Re}(X_N) = A_N - A_{N+1}$. Since all the matrices in this expression are positive, taking the trace norm we have $\|A_N\|_{\mathrm{tr}} - \|A_{N+1}\|_{\mathrm{tr}} = \|\mathrm{Re}(X_N)\|_{\mathrm{tr}}$. Adding both sides of this equation from $N = 0$ to N_0, taking into account that $\|\cdots\|_{\mathrm{tr}} \geq \|\cdots\|_{\mathrm{op}}$, and $\|\mathrm{Re}(X_N)\|_{\mathrm{op}} \geq \|C_{N+1}\|_{\mathrm{op}}$ [since $\mathrm{Re}(X_N) \geq \pm i\,\mathrm{Im}(X_N)$], we have

$$\sum_{N=0}^{N_0-1} \|C_{N+1}\|_{\mathrm{op}} \leq \|A_0\|_{\mathrm{tr}} - \|A_{N_0}\|_{\mathrm{tr}} \leq \|A_0\|_{\mathrm{tr}} - 2n\,,$$

where the last inequality is a consequence of the fact that $A_N \geq iJ$ for all N. Thus, among $\{C_N\}_{N=1}^{N_0}$ there must be at least one for which $\|C_N\|_{\mathrm{op}} \leq \epsilon$. Thus, $A_N - \|C_N\|_{\mathrm{op}}\mathbb{1} \geq A_N - \epsilon\mathbb{1} \geq 0$ where for the last inequality we have used Eq. (9), and therefore, for that particular value of N, condition (6) must be fulfilled. ■

It is worth stressing that from the proof of Proposition 3 it follows directly that if γ_0 is separable, then the sequence γ_N converges to a fixed point $\gamma_\infty = A_\infty \oplus B_\infty$, where $A_\infty = B_\infty \geq iJ$ are CMs. For the sake of completeness, we now show that if γ_0 is inseparable, then we can always detect it in a finite number of steps. We will use the fact that the CMs of inseparable Gaussian states form an open set, a fact that follows directly from condition (3). Therefore, if γ_0 is inseparable, there always exist $\epsilon_0 > 0$ such that if $\epsilon < \epsilon_0$ then $\gamma_0 + \epsilon\mathbb{1}$ is still inseparable and thus condition (6) is never fulfilled. However, if γ_0 were separable, then, according to Proposition 3, $\gamma_0 + \epsilon\mathbb{1}$ should fulfill that condition before reaching $N = N_0$. This can be summarized as follows.

Corollary 2: *If* γ *is inseparable then there exists some* $\epsilon > 0$ *such that starting out from* $\gamma_0 = \gamma + \epsilon\mathbb{1}$, *condition (6) is not fulfilled for any* $N \leq N_0 \equiv (\|A_0\|_{\mathrm{tr}} - 2n)/\epsilon$.

Together, Proposition 3 and Corollary 2 show that — whether γ_0 is separable or not, and except for a set of measure zero — we will be able to detect it in a finite number of steps. However, as mentioned above, according to our numerical calculations we see that the process always converges very fast and in practice one can directly use the method sketched after Theorem 1.

To conclude this Letter, we show that not only separability but also distillability [2,8], can be determined for all Gaussian states. The proof is based on the result that for 1×1 Gaussian states nonpositive partial transpose (npt) implies distillability [16]. This result can be extended to *all* bipartite Gaussian states, i.e., a Gaussian density matrix ρ is distillable iff its partial transpose is not positive. For the proof, it suffices to show that any $n \times m$ npt Gaussian state can be locally transformed into an 1×1 npt Gaussian state. This is achieved as follows: For Gaussian states, the npt condition is equivalent to $\gamma \not\geq i\tilde{J}$ [7]. Hence, for every npt CM γ there exists a vector $z = z_A \oplus z_B \in \mathbb{C}^{2(n+m)}$ such that for some $\epsilon > 0$ we have

$$z^\dagger(\gamma - i\tilde{J})z \leq -\epsilon < 0\,. \tag{10}$$

It is always possible to pick z such that $(\mathrm{Re}z_x)^T J\,\mathrm{Im}z_x \neq 0$ for both $x = A, B$. But then there exist symplectic maps S_A, S_B such that S_x maps $\mathrm{span}\{\mathrm{Re}z_x, \mathrm{Im}z_x\}$ to $\mathrm{span}\{e_1, e_2\}$ [17]. It follows that $\hat{z}_x \equiv S_x^{-1} z_x$ have nonzero entries only in the first two components. Thus not only is $\hat{z}^\dagger[(S_A \oplus S_B)^T \gamma (S_A \oplus S_B) - i\tilde{J}]\hat{z} < 0$ but by construction this still holds for the CM of the *reduced state* obtained by discarding all but the first mode at each side. Discarding subsystems is a local operation, hence all npt Gaussian states can be transformed locally into an npt 1×1 state and are thus distillable by [16]. ■

To summarize, we have obtained a necessary and sufficient condition for Gaussian states to be separable. The condition provides an operational criterion in that it can be easily checked by direct computation. It is worth mentioning that our criterion can be used to study the separability properties with respect to bipartite splittings of multipartite systems in Gaussian states [11,18]. Our criterion is based on a nonlinear map that is more powerful than partial transposition. In addition we proved that a bipartite Gaussian state is distillable if and only if it has nonpositive partial transpose. While in general, i.e., for non-Gaussian states, both the separability and the distillability problems remain open, these results represent a significant step towards understanding the separability problem, which is one of the most challenging problems in the field of quantum information. With the results presented here, one can decide for any bipartite Gaussian state by direct computation whether it is distillable and/or inseparable: it is distillable iff it is npt, and it is separable iff $\gamma_N \geq iJ\ \forall\ N$.

G. G. thanks the Friedrich-Naumann-Stiftung for financial support. This work was supported by the Austrian Science Found (SFB "Control and Measurement of Coherent Quantum Systems," Project 11), the EU (EQUIP,

contr. IST-1999-11053), the ESF, the Institute for Quantum Information GmbH Innsbruck, and the DFG (SFB 407 and SPP "Quanteninformationsverarbeitung").

Appendix.— In this Appendix we present the lemmas which are needed in order to prove Propositions 1 and 2. Let us consider three real matrices $0 \leq A = A^T \in M_{n,n}$, $0 \leq B = B^T \in M_{m,m}$, $C \in M_{n,m}$, and

$$M = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} = M^T \in M_{n+m,n+m}\,. \tag{11}$$

Lemma 1: *The following statements are equivalent:*
(i) $M \geq 0$.
(ii) $\ker(B) \subseteq \ker(C)$ *and* $A - CB^{-1}C^T \geq 0$.
(iii) $\ker(A) \subseteq \ker(C^T)$ *and* $B - C^TA^{-1}C \geq 0$ [12].

Proof: We will just prove the first equivalence since the other one is analogous. We use that $M \geq 0$ iff for any two real vectors $a \in \mathbb{R}^n$ and $b \in \mathbb{R}^m$

$$a^TAa + b^TBb + a^TCb + b^TC^Ta \geq 0\,. \tag{12}$$

Conversely, $A - CB^{-1}C^T \geq 0$ iff for any $a \in \mathbb{R}^n$ we have

$$a^TAa - a^TCB^{-1}C^Ta \geq 0\,. \tag{13}$$

(i) $\Rightarrow$ (ii): We assume (12). First, $\ker(B) \subseteq \ker(C)$ since otherwise we could always choose a $b \in \ker(B)$ so that $-2a^TCb > a^TAa$. Second, if we choose $b = -B^{-1}C^Ta$ then we obtain (13). (ii) $\Rightarrow$ (i): We now assume (13). Then, $A = CB^{-1}C^T + P$, where $P \geq 0$. Defining $\tilde{a} \equiv B^{-1}C^Ta$, we have that $C^Ta = B\tilde{a}$ [since $\ker(B) \subseteq \ker(C)$], and thus the left-hand side of (12) can be expressed as $a^TPa + (\tilde{a} + b)^TB(\tilde{a} + b)$, which is positive. ■

In the derivations of Propositions 1 and 2 we have not included explicitly the conditions imposed by the present lemma on the kernels of B and C. However, one can easily verify that all the problems that may arise from these kernels are eliminated by using pseudoinverses [12] instead of inverses of matrices.

Let us consider two real matrices $A = A^T \in M_{n,n}$ and $C = -C^T \in M_{n,n}$, and

$$M = \begin{pmatrix} A & C \\ C^T & A \end{pmatrix} = M^T \in M_{2n,2n}\,. \tag{14}$$

Lemma 2: $M \geq 0$ iff $A + iC \geq 0$.

Proof: This follows from the observation that M is real, and that for any pair of real vectors $a, b \in \mathbb{R}^N$ we have $(a - ib)^\dagger(A + iC)(a - ib) = (a \oplus b)^TM(a \oplus b)$. ■

[1] R. Werner, Phys. Rev. A **40**, 4277 (1989).
[2] For a review of the problem and its progress see, e.g., M. Lewenstein *et al.,* J. Mod. Opt. **47**, 2481 (2000); P. Horodecki *et al.,* J. Quant. Inf. Comp. **1**, 45 (2001).
[3] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[4] M. Horodecki *et al.,* Phys. Lett. A **223**, 1 (1996).
[5] L.-M. Duan *et al.,* Phys. Rev. Lett. **84**, 2722 (2000); R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[6] P. Horodecki, Phys. Lett. A **232**, 333 (1997); C. H. Bennett *et al.,* Phys. Rev. Lett. **82**, 5385 (1999).
[7] R. Werner *et al.,* Phys. Rev. Lett. **86**, 3658 (2001).
[8] C. Bennett *et al.,* Phys. Rev. A **54**, 3824 (1996); M. Horodecki *et al.,* Phys. Rev. Lett. **80**, 5239 (1998).
[9] If X_k, P_k are position- and momentum-like operators in each mode with canonical commutator $[X_k, P_k] = i$, we define $\gamma_{kl} \equiv 2\,\mathrm{Re}[\langle (R_k - d_k)(R_l - d_l)\rangle]$, where $d_k = \langle R_k\rangle \equiv \mathrm{tr}(\rho R_k)$ and $R_{2k-1} = X_k$ and $R_{2k} = P_k$ $(k = 1, \ldots, n)$.
[10] For convenience we use direct sum notation for matrices and vectors. That is, if $A \in M_{n,n}$ and $B \in M_{m,m}$, $A \oplus B \in M_{n+m,n+m}$ is a block diagonal matrix of blocks A and B. Similarly, if $f_1 \in \mathbb{R}^n$ and $f_2 \in \mathbb{R}^m$ are two vectors, then $f_1 \oplus f_2 \in \mathbb{R}^{n+m}$ is a vector whose first n components are given by the entries of f_1 and the last m by those of f_2.
[11] G. Giedke *et al.,* e-print quant-ph/01030137 [Phys. Rev. A (to be published)].
[12] Throughout this work we will denote by B^{-1} the pseudoinverse of B, that is, $BB^{-1} = B^{-1}B$ is the projector on the range of B.
[13] $\|A\|_{\mathrm{tr}} \equiv \mathrm{tr}(A^\dagger A)^{1/2}$ denotes the trace norm of A. The operator norm of A, $\|A\|_{\mathrm{op}}$ is the maximum eigenvalue of $(A^\dagger A)^{1/2}$.
[14] P. v. Loock *et al.,* Phys. Rev. A **63**, 022106 (2001).
[15] Note that the existence of a zero measure set which cannot be characterized in a finite number of steps is not particular for our method, but a simple consequence of finite precision. E.g., if we have a density matrix ρ for two qubits such that the partial transpose has a negative eigenvalue $-\epsilon$, it will be increasingly difficult to check whether $\rho^T \geq 0$ as $\epsilon \to 0$.
[16] G. Giedke *et al.,* e-print quant-ph/0007061 [J. Quant. Inf. Comp. (to be published)].
[17] V. I. Arnold, *Mathematical Methods of Classical Mechanics* (Springer-Verlag, New York, 1989), 2nd ed.
[18] W. Dür *et al.,* Phys. Rev. Lett. **83**, 3562 (1999); Phys. Rev. A **61**, 042314 (2000).

3 Distillability of Gaussian States

This section discusses *distillability* – a property that even more than separability determines the usefulness of quantum states for quantum communication. In the first subsection we motivate and define distillability and review the current knowledge on this topic (for this also see [64]) as the background on which the work on distillability of Gaussian states ([61], reprinted in Subsec. 3.2) was done. Section 4 then deals with actual entanglement distillation protocols.

3.1 The Distillability Problem

The fact that the state ρ of a bipartite system is inseparable shows that quantum correlations between the subsystems exist. This is necessary for ρ to offer any advantages over classical means of communication. But specific applications using entangled states for quantum communication – such as teleportation [13, 15] or quantum key distribution [8, 20] – are usually formulated for *pure* entangled states. In realistic situations, however, noise and imperfections are unavoidable, and therefore in practice one has to deal with mixed states. These can only be used directly in those protocols if they are sufficiently close to the ideal pure state. For example, if A and B want to employ an entanglement-based quantum key distribution protocol [8, 20], then, in principle, the noise might be due to an eavesdropping attempt and the protocol cannot guarantee more than a certain imperfect level of security. Therefore a mixed entangled state will in general not be directly useful, in particular if long-distance quantum communication is considered.

But if it is entangled, the mixed state ρ still represents a potentially valuable resource and the question arises, whether it can be made useful by local operations (see Def. 2.2). This is the question of distillability: if Alice and Bob are provided with a sufficiently large number of copies of the state ρ can they transform it into a "purified" state ρ' that is arbitrarily close to a pure maximally entangled state ψ by LOCC? We define

Definition 3.1 *(Distillable State)*
A state ρ of a bipartite quantum system on $\mathcal{H}_A \otimes \mathcal{H}_B$ is distillable *if $\forall \epsilon > 0$ there exists an $n > 0$ and a local quantum operation $\mathcal{P} \in LOCC(\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}, \mathcal{K}_A \otimes \mathcal{K}_B)$ such that*

$$\langle \psi | \, \mathcal{P}(\rho^{\otimes n}) \, | \psi \rangle \geq 1 - \epsilon. \tag{11}$$

for a pure maximally entangled state $|\psi\rangle \in \mathcal{K}_A \otimes \mathcal{K}_B$.

The existence of undistillable, *bound entangled* states was shown in [28, 29]. This proved that distillability is a property that has to be established independently of separability. More on entanglement distillation and its relevance for long-distance quantum communication in Sec. 4.

3.1.1 Finite dimensional systems

Up until now, no practical necessary and sufficient condition for distillability is known. Clearly, a state must be entangled if it is to be distillable. In addition, it was shown in [29] that all entanglement distillation protocols preserve ppt and that therefore npt is a necessary condition for distillability. For the special case of systems composed of a qubit and a d-level system ($\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^d$) it

was shown [37, 40] that this condition is also sufficient. Thus for this case the distillability problem is solved, but in general, it is still open.

In [29] it was shown that ρ is distillable iff for some number N of copies of ρ we can project $\rho^{\otimes N}$ into a two-dimensional subspace at either side such that the resulting state on $\mathbb{C}^2 \otimes \mathbb{C}^2$ is distillable, i.e. has npt. This condition is, however, very hard to check for a general state.

A practical sufficient condition for distillability is provided by the same authors in [39]. There the so-called *reduction criterion* (RC), a sufficient condition for inseparability, is introduced, and it is shown that this condition is also sufficient for distillability. The RC makes use of the positive map $\mathcal{P}$ defined for states on $\mathbb{C}^n$

$$\mathcal{P} : \rho \mapsto \mathrm{tr}(\rho) - \rho. \tag{12}$$

It is shown in [39] that this map is *decomposable* (see p. 7). Clearly, separable states remain positive under $\mathcal{P} \otimes \mathbb{1}$, and a negative eigenvalue of $\mathcal{P} \otimes \mathbb{1}(\rho)$ proves ρ inseparable. Formulated as a criterion for distillability, the RC then states

Theorem 3.1 *(Reduction Criterion of Distillability, [39])*
If for a bipartite state ρ on $\mathbb{C}^n \otimes \mathbb{C}^n$ it holds that

$$(\mathcal{P} \otimes \mathbb{1})(\rho) \ngeq 0 \tag{13}$$

then ρ is distillable.

For a long time all states known to be distillable satisfied Ineq. (13) and it was already shown in [39] that for certain distilliation protocols this was also a necessary condition. But very recently it was shown [42] that there are distillable states for which (13) is not fulfilled. This leaves open the question whether all npt states can be distilled. Up until now all known examples of undistillable, bound entangled states have ppt. There is evidence, though, that there are states that are undistillable, although their partial transpose is negative [40, 41]. These are the *Werner states* [24] W_d defined for pairs of d-level systems by

$$W_d = \frac{1}{d^2 - 1} \left[(1 - \lambda/d)\mathbb{1} + (\lambda - 1/d)V \right], \tag{14}$$

where V is the permutation operator, defined by $V(x \otimes y) = y \otimes x$ and $-1 \leq \lambda \leq 1$. It is shown in [40, 41] that for $d > 2$ and any finite $n > 0$ there is a finite range of values of λ for which these states are not *n-distillable* in the sense that $W_d^{\otimes n}$ cannot be projected to a 2×2 npt state. Numerical results indicate that all these states are in fact undistillable for any n. Note that the Werner states are the key to question whether npt implies distillability. This comes from the fact that any state of two d-level systems can be transformed into W_d (for some λ) by local operations [34, 40, 41] in such a way, that (non)positivity of the partial transpose is preserved. Hence, if all npt Werner states can be distilled, then all npt states can.

If there are indeed bound entangled npt states, this would have surprising consequences for quantum information [42]: it would imply that one of the most interesting measures of entanglement, *distillable entanglement* [36, 31], is not convex and not additive, which are both properties one might naively expect of entanglement measures.

3.1.2 Continuous Variable Systems

The study of distillability for infinite dimensional systems has begun only recently. However, since the most promising applications of CV states are in quantum communication and many tasks in this area are based on (pure) entangled states, it is of particular importance to identify the distillable CV states.

On the one hand it was shown that there exist generically infinite dimensional ppt bound entangled states [63] and later that there are also Gaussian ppt bound entangled states. On the other hand, entanglement distillation protocols for certain pure [66, 65] and mixed entangled states were presented [67].

In [61] (reprinted in Subsec. 3.2) we prove that for Gaussian states npt is necessary and sufficient for distillability. To this end we first extend the RC to infinite dimensions and then proceed in three steps. First, it is shown that *symmetric states* (see Subsec. A.6, p. 90) are distillable by the reduction criterion. In the second step, we show that every entangled state of two modes can be symmetrized by local operations in a way that *maintains inseparability* (and thus npt by [23, 59]). Since the proof of this step is somewhat concentrated in [61], we give some more details in App. C. In the last step we show that any npt $N \times M$ Gaussian state can be locally transformed into a distillable two-mode state. Interestingly, no collective action is needed for this step, thus all distillable Gaussian states are 1-distillable in the sense of [40]. This shows that among Gaussian states, there seem to exist only two qualitatively different types of entanglement, namely npt-entanglement (free) and ppt-entanglement (bound).

3.2 Distillability Criterion for all Gaussian States

Geza Giedke, Lu-Ming Duan, Peter Zoller, and J. Ignacio Cirac,

We prove that all inseparable Gaussian states of two modes can be distilled into maximally entangled pure states by local operations. Using this result we show that a bipartite Gaussian state of arbitrarily many modes can be distilled if and only if its partial transpose is not positive.

Quant. Inf. Comp. **1**, 79 (2001); E-print: quant-ph/0104072.

Quantum Information and Computation, Vol. 1, No. 3 (2001) 79–86
© Rinton Press

DISTILLABILITY CRITERION FOR ALL BIPARTITE GAUSSIAN STATES

GEZA GIEDKE,* LU-MING DUAN, J. IGNACIO CIRAC, AND PETER ZOLLER,
Institut für Theoretische Physik, Universität Innsbruck, Technikerstrasse 25, 6020 Innsbruck, Austria

Received July 30, 2001

We prove that all inseparable Gaussian states of two modes can be distilled into maximally entangled pure states by local operations. Using this result we show that a bipartite Gaussian state of arbitrarily many modes can be distilled if and only if its partial transpose is not positive.

Keywords: entanglement, distillation, Gaussian states

Communicated by: S Braunstein and C Fuchs

The existence of *pure* entangled states of two or more systems entails the possibility of finding new applications of Quantum Mechanics, in particular in the fields of computation and communication [1]. In practice, however, systems are exposed to interactions with the environment, that transform pure into *mixed* states, which may no longer be useful for quantum communication. Fortunately, there exist methods to recover pure entangled states from mixed ones in certain situations. These processes are called *entanglement distillation* (or purification) [2], and consist of local operations and classical communication transforming several copies of a mixed entangled state into (approximately) pure entangled states which can then be used for quantum communication. In fact, applying this method in the appropriate way one can construct quantum repeaters [3] that should allow efficient quantum communication over arbitrarily long distances even via a noisy channel.

For this reason it is important to determine whether a given state is distillable or not. In general, the answer to this question is not known. At the moment we only have conditions that are necessary or sufficient for distillability, but not both. Clearly, only inseparable states can be distilled. Moreover, as shown by Horodecki *et al.* [4], there exists a stronger necessary condition, namely that ρ must have non-positive partial transpose (npt). In fact, there are entangled states which are not distillable since their density matrices remain positive under partial transposition [5]. Furthermore, there is evidence that this condition is not sufficient, since there exist npt states that nevertheless seem to be undistillable [6]. The existence of undistillable npt states would have interesting consequences such as non-additivity and non-convexity of the entanglement of formation [7].

On the other hand, a useful sufficient criterion, the so-called reduction criterion [8], has been established. It states that, given a state ρ on the composite Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$,

*email: geza.giedke@uibk.ac.at

if there exists a vector $|\psi\rangle \in \mathcal{H}$ such that

$$\langle\psi| \operatorname{tr}_B \rho \otimes \mathbf{1} - \rho |\psi\rangle < 0. \tag{1}$$

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 (1), then one can explicitly construct a protocol to distill ρ.

Up until now, nearly all work on the distillability problem has considered states of finite dimensional systems, see [9] for a current overview. In particular it was shown that states systems consisting of one qubit and an N-level, $N \geq 2$ system are distillable if and only if (iff) they are npt [10, 6]. An alternative setting for quantum information processing, which considers infinite dimensional systems [continuous variables (CV) or "modes"] in Gaussian states is receiving increasing attention recently [11, 12]. For CV systems some distillation protocols for particular states have been proposed [13], and the existence of bound entangled states has been proved [14, 15], but the question of distillability in general has not been addressed.

In this article we answer this question completely for all Gaussian states. We will prove that

Theorem 1 *(Distillability Criterion)*
A Gaussian state of $N \times M$ modes is distillable if and only if its partial transpose is negative.

This shows that there are no npt bound entangled Gaussian states and, in particular, that for systems of $1 \times N$ modes all entangled states (npt is necessary for inseparability of such systems [15, 16, 17]) are distillable and thus useful for quantum communication. Moreover, our proof, which is based in part on the reduction criterion, provides an explicit protocol that accomplishes distillation for all those states. After introducing the necessary notation and properties of Gaussian states, the remainder of the present paper is devoted to the proof of Theorem 1.

We consider bipartite systems composed of two subsystems, A and B, which consist of N and M "modes" [distinguishable infinite dimensional quantum systems with Hilbert space $\mathrm{L}^2(\mathbf{R})$], respectively. The joint system is referred to as a "$N \times M$ system". It is convenient to describe the state ρ of such a system by its characteristic function (e.g., [18])

$$\chi(x) = \operatorname{tr}[\rho D(x)]. \tag{2}$$

Here $x = (q_1, p_1, \ldots, q_{N+M}, p_{N+M}) \in \mathbf{R}^{2N+2M}$ is a real vector and

$$D(x) = e^{-i \sum_k (q_k X_k + p_k P_k)}, \tag{3}$$

where X_k and P_k are operators satisfying the canonical commutation relations ($\hbar = 1$). A characteristic function χ uniquely defines a state ρ_χ. In the following we exclusively consider *Gaussian states*, i.e. states for which χ is a Gaussian function of x [19]

$$\chi(x) = e^{-\frac{1}{4} x^T \gamma x - i d^T x}, \tag{4}$$

where γ is the *correlation matrix* (CM) and $d \in \mathbf{R}^{2N+2M}$ the *displacement*. Thus, a Gaussian state is fully characterized by its CM γ and displacement d. These states are of particular

interest, since they comprise essentially all CV states that can be prepared in the lab with current technology.

A matrix γ is the CM of a physical state iff (e.g. [22]) it is strictly positive, real, symmetric $2(N+M)\times 2(N+M)$ and satisfies

$$\gamma \geq J^T \gamma^{-1} J, \tag{5}$$

where $J_{N+M} = \bigoplus_{k=1}^{N+M} J_1$ [20] with $J_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Simon [17] noted that for CV states partial transposition is equivalent to the orthogonal transformation $\Lambda_B(q_A, p_A, q_B, p_B) = (q_A, p_A, q_B, -p_B)$ on phase space, i.e., the momentum coordinates referring to B are inverted. For a Gaussian state this means that its CM is changed to $\tilde{\gamma} = \Lambda_B \gamma \Lambda_B$ and the displacement to $\Lambda_B d$. A Gaussian state with CM γ has negative partial transpose (npt) iff $\tilde{\gamma}$ does not satisfy Ineq. (5) [17, 15], or, equivalently, iff

$$\gamma \not\geq \tilde{J}^T \gamma^{-1} \tilde{J}, \tag{6}$$

where $\tilde{J} = \Lambda_B J \Lambda_B^T$ is the "partially transposed" J in which the J_1's corresponding to B's modes are replaced by $-J_1$.

The first part of the proof of the theorem is concerned with the special case of a bipartite two-mode Gaussian state: $N = M = 1$. Any such state can be transformed into what we called the *standard form*, using local unitary operations only [16, 17]. For a state in standard form the displacement $d = 0$ and the CM γ has the simple form

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{7}$$

where

$$A = \begin{pmatrix} n_a & 0 \\ 0 & n_a \end{pmatrix},\ B = \begin{pmatrix} n_b & 0 \\ 0 & n_b \end{pmatrix},\ C = \begin{pmatrix} k_x & 0 \\ 0 & k_p \end{pmatrix}. \tag{8}$$

The local unitaries needed to achieve this form are linear Bogoliubov transformations, i.e., generated by Hamiltonians that are at most quadratic in the operators $X_{1,2}, P_{1,2}$ The four real parameters (n_a, n_b, k_x, k_p) fully characterize a 1×1 Gaussian state up to local linear Bogoliubov transformations (LLBT). They can be easily calculated from the four LLBT-invariant determinants $\det A, \det B, \det C$, and $\det \gamma$ as follows:

$$n_a = \sqrt{\det A}, n_b = \sqrt{\det B}, k_x k_p = \det C, \tag{9a}$$

$$(n_a n_b - k_x^2)(n_a n_b - k_p^2) = \det \gamma. \tag{9b}$$

Without loss of generality we choose $k_x \geq |k_p|$. We call a state *symmetric*, if $n_a = n_b = n$, or, equivalently, if $\det A = \det B$.

Now we are prepared for the proof of Theorem 1. We state the three main steps of the proof in three lemmas, which we prove in the remainder of this article.

Lemma 1 *(Distillability of Symmetric 1×1 States)*
A symmetric 1×1 Gaussian state with non-positive partial transpose is distillable.

Lemma 2 *(Symmetrization of 1×1 States)*
Every 1×1 Gaussian state with non-positive partial transpose can be locally transformed into a symmetric npt state.

Lemma 3 *(Concentrating Inseparability in two Modes)*
Every $N \times M$ Gaussian state with non-positive partial transpose can be locally transformed into a 1×1 npt state.

Proof of Theorem 1: The "only if"-part of the Theorem was proven proven by the Horodeckis in [4]. The "if"-part is clearly implied by these three Lemmas, since by Lemma 3 the $N \times M$ case can be reduced to the 1×1 case, and that case by Lemma 2 to the symmetric case. ∎

For the proof of Lemmas 1 and 2, it is useful to re-express the conditions (5,6) for 1×1 states in terms of the parameters (9). We find that γ is CM of a physical state iff

$$(n_a n_b - k_x^2)(n_a n_b - k_p^2) + 1 \geq n_a^2 + n_b^2 + 2k_x k_p, \tag{10a}$$

$$n_a n_b - k_x^2 \geq 1, \tag{10b}$$

and that γ is CM of an inseparable (or, equivalently, npt) state, iff in addition it holds that

$$(n_a n_b - k_x^2)(n_a n_b - k_p^2) + 1 < n_a^2 + n_b^2 - 2k_x k_p. \tag{11}$$

Proof of Lemma 1: For this we use that a state is distillable, if there exists a pure state $|\psi\rangle$ such that Ineq. (1) holds. This condition was proved in [8] to be sufficient for distillability of finite dimensional systems. Its extension to infinite dimensions is straightforward: and proved in the appendix.

We show now that for any symmetric npt Gaussian state ρ Ineq. (1) is satisfied with $|\psi\rangle$ taken as the pure two-mode squeezed state $|\psi\rangle = \frac{1}{\cosh r} \sum_n \tanh^n r \, |nn\rangle$ for sufficiently large $r > 0$. Note that $|\psi\rangle$ is a symmetric Gaussian state in standard form. We denote its CM by γ_ψ and the four parameters (9) are $n_a = n_b = \cosh 2r, k_x = -k_p = \sinh 2r$. Let γ_ρ denote the CM of ρ. With these choices, Ineq. (1) becomes [21]

$$2\left[\det(\gamma_{\mathrm{tr}_B \rho} + \gamma_{\mathrm{tr}_B \psi})\right]^{-1/2} - 4\left[\det(\gamma_\rho + \gamma_\psi)\right]^{-1/2} < 0. \tag{12}$$

In the limit of large r (keeping only the leading terms in e^r) this becomes after some simple algebra

$$(n - k_x)(n + k_p) < 1. \tag{13}$$

But Ineq. (13) is implied by the inseparability criterion for symmetric states: if $n_a = n_b = n$ then Ineq. (11) simplifies to

$$|n^2 - k_x k_p - 1| < n(k_x - k_p). \tag{14}$$

For inseparable states we observe [17] that $k_x k_p < 0$, which together with Ineq. (10b) implies that the LHS of Ineq. (14) is equal to $n^2 - k_x k_p - 1$ which can be transformed to $(n - k_x)(n + k_p) + n(k_x - k_p) - 1$ from which Ineq. (13) follows immediately. ∎

Since the local operation that will be shown to achieve symmetrization involves a measurement, it is more convenient to describe the state here by its *Wigner function* [18]. It is related to the characteristic function by symplectic Fourier transformation and thus is Gaussian for Gaussian states. The Wigner CM γ_W is related to the (characteristic) CM by $\gamma_W = J^T\gamma^{-1}J$. We denote the four LLBT-invariant parameters for the Wigner CM [which are defined as in (9)] by (N_a, N_b, K_x, K_p). We use the following easily checked facts: just as the standard form of γ, the standard form of γ_W can be obtained by LLBTs. A state is symmetric iff $N_a = N_b$. The conditions (10,11) can be formulated equivalently in terms of the parameters (N_a, N_b, K_x, K_p). While (10a, 11) are identical for the Wigner parameters, in (10b) "$\geq$" is changed to "$\leq$". We refer to these conditions for the Wigner parameters as (10W, 11W) in the following.

Proof of Lemma 2: 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. This must be done without destroying the entanglement of ρ. We proceed as follows: ρ is transformed to its Wigner standard form with parameters (N_a, N_b, K_x, K_p). Now assume that $N_b < N_a$, i.e., B is the hotter side [24]. Take an ancilla mode in the vacuum state and couple it to B's mode by a beam splitter [23] with transmittivity $\cos^2\theta$. After a measuring the ancilla's X-operator [25] results a state $\tilde{\rho}$ with Wigner CM $\tilde{\gamma}_W$ of the form (7) with

$$\tilde{A} = \frac{1}{\nu}\begin{pmatrix} c^2N_a + s^2D_x & 0 \\ 0 & c^2N_a + s^2N_aN_b \end{pmatrix},$$

$$\tilde{B} = \frac{1}{\nu}\begin{pmatrix} N_b & 0 \\ 0 & [c^2N_b + s^2]\nu \end{pmatrix},\ \tilde{C} = \frac{1}{\nu}\begin{pmatrix} cK_x & 0 \\ 0 & cK_p\nu \end{pmatrix},$$

where the abbreviations $c = \cos\theta, s = \sin\theta, \nu = s^2N_b + c^2$, and $D_{x,p} = N_aN_b - K_{x,p}^2$ were used. The condition for symmetry, $\det\tilde{A} = \det\tilde{B}$ requires

$$\tan^2\theta = \frac{N_a^2 - N_b^2}{N_b - D_xN_a}. \tag{15}$$

Checking (11W) for $\tilde{\gamma}_W$ one sees that the inequality is just multiplied by $(N_b\tan^2\theta + 1)^{-1} > 0$; therefore the transformed state is inseparable iff the original one was inseparable. It remains to show that there always exists a θ to satisfy (15), i.e., that the right hand side of Eq. (15) is positive. The numerator is positive since we have chosen $N_b < N_a$, the denominator is positive since $N_b < N_a$ and the second part of condition (10W) imply that $(N_a - D_xN_b) > 0$ and the first part of (10W) assures that $(N_a - D_xN_b)(N_b - D_pN_a) \geq (N_aK_x + N_bK_p)^2 \geq 0$, hence all Gaussian states in Wigner standard form can be symmetrized this way. But since every Gaussian state can be brought into Wigner standard form by local unitaries, this completes the proof of Lemma 2. ∎

To finish the proofs, we now turn to the general case of $N \times M$ modes. Let γ be the CM of a npt state.

Proof of Lemma 3: The condition (6) is equivalent to $\gamma \not\geq i\tilde{J}$ [15]. Hence, for every npt state with CM γ there exists a vector $z \in \mathbf{C}^{2(N+M)}$ such that for some $\epsilon > 0$

$$z^\dagger(\gamma - i\tilde{J})z \leq -\epsilon < 0. \tag{16}$$

The idea of the proof is that γ can be locally transformed such that at both sides all but one mode can be discarded, and the resulting (reduced) 1×1 state is still npt. Then it is distillable by Lemmas 1 and 2.

Write z in Eq. (16) as $z = z^{(A)} \oplus z^{(B)}$ with real and imaginary parts $z_r^{(x)}, z_i^{(x)}$, $(x = A, B)$. We can always find a z such that $z_r^{(x)}$ and $z_i^{(x)}$ are not skew-orthogonal, i.e. $(z_r^{(x)})^T J z_i^{(x)} \neq 0$ for both $x = A, B$ [26].

Now we have to find two symplectic transformations $S_x, x = A, B$ that map the span of $\{z_r^{(x)}, z_i^{(x)}\}$ to the span of $\{e_1, e_2\}$, where $e_1 = (1, 0, \ldots, 0)$ etc. After performing the local transformation $S = S_A \oplus S_B$, both A and B can discard all but the first mode of their systems and still have an npt entangled (and thus distillable) state. That such symplectic transformations S_A, S_B always exist is seen as follows: let $f_1 = z_r, f_2 = -z_i/(z_r^T J z_i)$; we can always extend f_1, f_2 into a *symplectic basis* [27] $f_k : k = 1, \ldots, 2n$ such that $f_{2k}^T J f_{2l+1} = \delta_{kl}, f_{2k}^T J f_{2l} = 0 = f_{2k+1}^T J f_{2l+1}$. Then S defined by $S e_k = f_k$ is symplectic [27] and S^{-1} maps $\mathrm{span}\{z_r, z_i\}$ to $\mathrm{span}\{e_1, e_2\}$, i.e.

$$\hat{z}^{(x)} := S_x^{-1} z^{(x)} = a_x e_1 + b_x e_2, \tag{17}$$

$a_x, b_x \in \mathbf{C}$. Consequently we have for $\hat{\gamma} := (S_A \oplus S_B)^T \gamma (S_A \oplus S_B)$

$$(\hat{z}^{(A)} \oplus \hat{z}^{(B)})^\dagger (\hat{\gamma} - i\tilde{J})(\hat{z}^{(A)} \oplus \hat{z}^{(B)}) < 0. \tag{18}$$

Using Eq. (17) we see that only the matrix elements $(\hat{\gamma})_{kl}$ with $k, l = 1, 2, N+1, N+2$ contribute to the lhs of Eq. (18). Thus Ineq. (18) does not change if we replace $\hat{\gamma}$ by the two-mode CM $\hat{\gamma}_{red}$ obtained from $\hat{\gamma}$ by discarding all rows and columns referring to modes other than 1 and $N+1$. This is the CM of the state in which A and B discard all but their first mode each. Thus Ineq. (18) shows that the state ρ_{red} corresponding to $\hat{\gamma}_{red}$ is npt. But ρ_{red} is a two-mode state and thus distillable by the first part of the proof. ∎

Note that all the operations needed to transform a general $N \times M$ npt state into a symmetric 1×1 entangled state can be implemented quantum optically with current technology: they require nothing but squeezers, beam splitters, phase shifters [23], homodyne measurements, and the discarding of subsystems. Once a state has been transformed to symmetric standard form, the protocol of Ref. [8] can be used to obtain maximally entangled states in a finite dimensional Hilbert space. While a *practical* distillation protocol for such Gaussian states remains to be found (see however [13]), it is worth noting, that the main part of the universal protocol of [8], namely the filtering operation and the joint measurement, are for symmetric Gaussian states implemented by the procedure of Duan *et al.*[13]; for details see [12, ch. II.8].

In conclusion, we have answered the distillability question for all Gaussian states: such states are distillable if and only if they are npt. In particular, all entangled Gaussian states of $1 \times N$ modes are distillable, and there exist no npt bound entangled Gaussian states.

Acknowledgements

G.G. acknowledges financial support by the Friedrich-Naumann-Stiftung. This work was supported by the Austrian Science Foundation (SFB "Control and Measurement of Coherent Quantum Systems", Project 11), the EU (TMR network ERB–FMRX–CT96–0087 and the

project EQUIP, contract IST-1999-11053), the ESF, and the Institute for Quantum Information GmbH, Innsbruck.

References

1. C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett., **70**, 1895 (1993);
   A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661 (1991).
2. C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, Phys. Rev. Lett. **76**, 722 (1996); quant-ph/9511027.
   C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. A **54** 3824 (1996); quant-ph/9604024.
3. H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, *Quantum repeaters: The role of imperfect local operations in quantum communication*, Phys. Rev. Lett. **81**, 5932 (1998); quant-ph/9803056.
4. M. Horodecki, P. Horodecki, and R. Horodecki, *Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?*, Phys. Rev. Lett. **80**, 5239 (1998).
5. P. Horodecki, *Separability Criterion and inseparable mixed states with positive partial transpose*, Phys. Lett. A **232**, 333 (1997).
6. W. Dür, J.I. Cirac, M. Lewenstein, D. Bruß, *Distillability and partial transposition in bipartite systems*, Phys. Rev. A **61**, 062313 (2000), quant-ph/9910022.
   D. DiVincenzo, P.W. Shor, J.A. Smolin, B.M. Terhal, A.V. Thapliyal, *Evidence for bound entangled states with negative partial transpose*, Phys. Rev. A **61**, 062312 (2000); quant-ph/9910026.
7. P.W. Shor, J.A. Smolin, B.M. Terhal, *Nonadditivity of Bipartite Distillable Entanglement follows from Conjecture on Bound Entangled Werner States*, Phys. Rev. Lett. **86**, 2681 (2001); quant-ph/0010054.
8. M. Horodecki, P. Horodecki, *Reduction criterion of separability and limits for a class of distillation protocols*, Phys. Rev. A **59**, 4206 (1999).
9. M. Lewenstein, D. Bruß, J.I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, and R. Tarrach, *Separability and distillability in composite quantum systems – a primer*, J. Mod. Opt. **47**, 2481 (2000), quant-ph/006064.
10. M. Horodecki, P. Horodecki, and R. Horodecki, *Inseparable Two Spin-1/2 Density Matrices Can Be Distilled to a Singlet Form*, Phys. Rev. Lett. **78**, 574 (1997).
11. L. Vaidman, *Teleportation of quantum states*, Phys. Rev. A **49**, 1473 (1994).
    S.L. Braunstein and H.J. Kimble, *Teleportation of Continuous Quantum Variables*, Phys. Rev. Lett. **80**, 869 (1998);
    A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, *Unconditional Quantum Teleportation*, Science **282**, 706 (1998).
12. S. Braunstein and A. Pati (eds.), *Quantum Information Theory with Continuous Variables*, Kluwer Academic Publishers, Dodrecht 2001, in press.
13. T. Opatrný, G. Kurizki, and D.-G. Welsch, *Improvement on teleportation of continuous variables by photon subtraction via conditional measurement*, Phys. Rev. A **61**, 032302 (1999); quant-ph/9907048;
    S. Parker, S. Bose, and M.B. Plenio, *Entanglement quantification and purification in continuous variable systems*, Phys. Rev. A **61**, 032305 (1999); quant-ph/9906098;
    L.-M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, *Entanglement Purification of Gaussian Continuous Variable Quantum States*, Phys. Rev. Lett. **84**, 4002 (2000); quant-ph/9912017.
14. P. Horodecki, M. Lewenstein, *Bound Entanglement and Continuous Variables*, Phys. Rev. Lett. **85**, 2657 (2000); quant-ph/0001035.
15. R.F. Werner and M.M. Wolf, *Bound entangled Gaussian States*, Phys. Rev. Lett. **86**, 3658 (2001); quant-ph/0009118.

16. L.-M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, *Inseparability criterion for continuous variable systems*, Phys. Rev. Lett. **84**, 2722 (2000); quant-ph/9908056.
17. R. Simon, *Peres-Horodecki separability criterion for continuous variable systems*, Phys. Rev. Lett. **84**, 2726 (2000); quant-ph/9909044.
18. C. Gardiner and P. Zoller, *Quantum Noise* 2nd ed., Springer-Verlag, Berlin (1999).
19. J. Manuceau and A. Verbeure, Comm. Math. Phys. **9**, 293 (1968).
20. For convenience we use direct sum notation for matrices and vectors. That is, if A and B are $n \times n$ and $m \times m$ matrices, resp., then $A \oplus B \in M_{n+m,n+m}$ is a block diagonal matrix of blocks A and B. Similarly, if $f_1 \in \mathbf{R}^n$ and $f_2 \in \mathbf{R}^m$ are two vectors, then $f_1 \oplus f_2 \in \mathbf{R}^{n+m}$ is a vector whose first n components are given by the entries of f_1 and the last m by those of f_2.
21. H. Scutaru, *Transition Probabilities for Quasifree States*, J. Math. Phys. **39**, 6403 (1998).
22. H. Scutaru, *The states with Gaussian Wigner function are quasi-free states*, Phys. Lett. A **141**, 223 (1989).
23. We use quantum optical terminology for the following LBT: a beam splitter of transmittivity t coupling the modes k and l refers to the unitary generated by $t(P_k X_l - X_l P_k)$, a phase shifter for the kth mode is generated by $X_k^2 + P_k^2$, a squeezing transformation by $X_k P_k + P_k X_k$, and a displacement by $aX_k + bP_k$.
24. Note that since γ_W is essentially the inverse of γ, large (Wigner parameter) N_a implies *small* entropy of the reduced state, while large (characteristic function parameter) n_a implies large entropy of the reduced state; more precisely we have: $N_a = n_b/\sqrt{\det \gamma}, N_b = n_a/\sqrt{\det \gamma}$.
25. If a measurement of an observable X_k or P_k is performed, the Wigner function of the final state of the remaining modes is calculated as follows: replace the phase space coordinate referring to the measured operator by the measured result and integrate out the conjugate phase space coordinate. Note that the CM of final state is independent of the measurement outcome.
26. In case the original vectors z_r, z_i are skew-orthogonal, we can replace z_i by $z_i' = z_i + \delta J z_r$ where δ is so small that Ineq. (16) still holds for $z' = z_r + iz_i'$.
27. V.I. Arnold, *Mathematical Methods of Classical Mechanics* 2nd. ed., Springer Verlag, New York, 1989.

Appendix A

We show that Ineq. (1) implies distillability even for $\dim\mathcal{H} = \infty$. Let $\{|k\rangle : k = 0, 1, ...\}$ be an orthonormal basis of $\mathcal{H}$, let $\mathcal{H}_n = \text{span}\{|0\rangle, |1\rangle, ..., |n\rangle\}$, $P_{\mathcal{H}_n}$ the orthogonal projector on $\mathcal{H}_n$, and let ρ be a density matrix on $\mathcal{H} \otimes \mathcal{H}$. Let $\mathcal{E}(\rho) = \text{tr}_B \rho \otimes \mathbf{1} - \rho$ be the map occuring on the lefthand side of (1). Assume that $\exists\, |\psi\rangle \in \mathcal{H}, \epsilon > 0$ such that $\langle\psi| \mathcal{E}(\rho) |\psi\rangle < -\epsilon < 0$. Since $\rho_n = P_{\mathcal{H}_n} \rho P_{\mathcal{H}_n}$ converges in the weak topology to ρ, there is $N \geq 0$ such that $\langle\psi| \mathcal{E}(\rho_n) |\psi\rangle < -\epsilon/2$ for all $n \geq N$. Thus ρ can be projected by local operations onto a distillable state ρ_N and is therefore itself distillable. ∎

4 Entanglement Purification Protocols

While the previous Section was concerned with the property of distillability, we now turn to the operations by which distillable states are transformed into directly usable, (almost) pure, highly entangled states. Sequences of operations which achieve this goal are referred to as *entanglement purification* (or *distillation*) *protocols* (EPP). Again, we first review the paradigmatic case of entangled qubits and then turn to more recent work on EPPs for Gaussian States and their physical implementation.

4.1 Finite Dimensions

As discussed above, the main motivation to study entanglement purification is to restore entangled states that are necessarily degraded by their passage through a noisy communication channel back to usable, pure form.

One way to address (or rather avoid) this problem is the use of *quantum error correcting codes* (QECCs) [72]: encoding locally created maximally entangled state before transmission in a sufficiently high-dimensional code space it can be protected against all kinds of errors, and decoding it, A and B receive an entangled state as close to the original one as desired. But for this the coherent manipulation of many quantum systems, and, in effect, a full-fledged quantum computer is necessary. Moreover, QECCs are designed to protect an arbitrary *unknown* state against errors, whereas in the situation under consideration it would suffice to protect a particular, *known*, maximally entangled state. Therefore one may ask whether there are simpler methods to faithfully distribute entangled states over large distances, and this is what entanglement purification protocols help to achieve.

The EPPs that have been proposed so far [32, 33, 34, 35, 39, 43] (some of which have been realized experimentally [44]) all fall into one of three distinct classes: "filtering", "recurrence", or "hashing" protocols. Since a combination of all three is needed for the (according to current knowledge) most efficient and general protocol, all three will be sketched in the following.

4.1.1 EPPs for qubits

The conceptionally simplest EPPs are the filtering protocols [32, 33, 39]. They work as follows: Alice and Bob share a (mixed) entangled states ρ and both perform a generalized measurement and communicate the result to each other. For some measurement outcomes the resulting state is closer to the desired maximally entangled state than ρ. Alice and Bob keep only those states and discard the rest. "Closeness" is in this context measured by the *fidelity* F, i.e. the overlap $F = \langle\psi|\,\rho\,|\psi\rangle$ of the state ρ with the desired state. Depending on the initial state it is in some cases possible to choose the measurements in such a way that resulting state is as close to the maximally entangled state as desired (at the expense of this result becoming less and less probable), a simple example of this case is given in [36].

One major advantage of this kind of protocol is its simplicity: a single operation on an individual system is sufficient to achieve purification, that is, collective operations are not needed. Also, it allows in some cases to distill states

arbitrarily close to a product state and therefore vanishingly little entanglement, see e.g. [36, III.A.2].

But many states cannot be purified by individual operations. For example, it is not even possible to increase the fidelity of a Werner state W_2 by local operations on an individual pair [38]. This is where the second type of purification protocol, the "recurrence" protocol, first proposed for qubits in [34], becomes useful. The recurrence protocol allows to distill all entangled Werner of two qubits in the following way: Alice and Bob share a N identical pairs each in a Werner state with fidelity $F > 1/2$. perform collective local operations on pairs of entangled states.

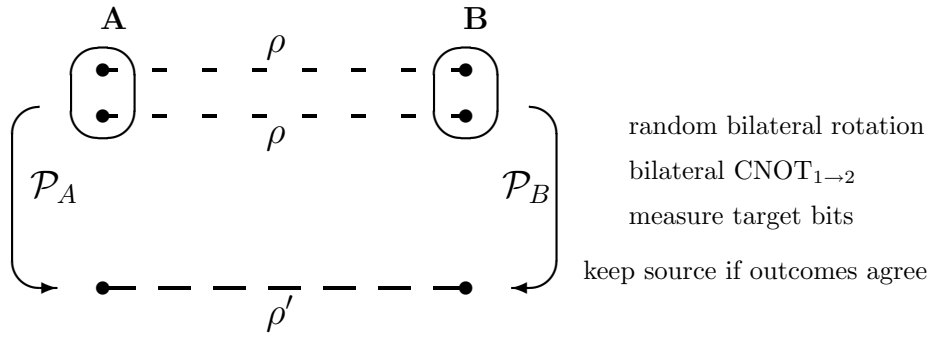

Figure 1: The "recurrence" entanglement purification protocol [34].

A distillation procedure that allows to distill every entangled two-qubit state ρ can be constructed by combining the protocols [34] and [33]. If the *fully entangled fraction* of ρ, defined as the $\max\{\langle\psi|\,\rho\,|\psi\rangle : \psi$ maximally entangled $\}$ is lager than $1/2$, then ρ can be locally transformed into a Werner state with fidelity $F > 1/2$ and then distilled by the recurrence protocol. Otherwise, there is a filtering measurement which purifies ρ into a state with fully entangled fraction $> 1/2$. In fact, this can be generalized to d-level systems. In [39] this generalized protocol – which can distill all states that are currently known to be distillable – is developed. Since it will serve as a basis for a universal EPP for Gaussian states we give a brief review in Subsec. D.1.

The main drawback of this protocol is, that it is quite "wasteful" with the resource entanglement. If a protocol allows to obtain on average m pairs of fidelity F' out of n initial pairs of fidelity F we define the yield of the protocol by $Y(F', F) = m/n$. For both the filtering and the recurrence method the $Y(F', F)$ vanishes as $F' \to 1$: their asymptotic yield of pure singlets is zero. The third class of EPPs addresses this problem. If the initial Werner state ρ has sufficiently high fidelity, then the "hashing" protocol [36] that performs collective operations on a large number of entangled pairs has $\lim_{F'\to 1} Y(F', F) = Y_0$. Y_0 is given by $Y_0 = 1 - S(F)$, where $S(F)$ is the (von Neumann) entropy of the Werner state with fidelity F. This gives a positive yield for $F > F_0 \sim 0.82$. Thus according to current knowledge the best universal purification protocol uses (if necessary) filtering to obtain states of sufficiently high fully entangled fraction and then

the recurrence protocol (actually a improved version [35]) to produce Werner states of fidelity $F > F_0$, which are then distilled by the hashing method.

First experiments realizing entanglement purification were reported in [44].

4.1.2 Bridging large distances: The Quantum Repeater

While EPPs are an important building block for long-distance quantum communication, they are, on their own, not sufficient to achieve this task. The problem that still remains is that only entangled states can be purified and that if the channel is too long and noisy, it does not allow the direct distribution of entangled pairs. Especially for long-distance communication this will inevitably be the case, since both absorption losses and depolarization errors scale exponentially with the length of the channel. For example, if the entangled state is encoded in the polarization of a pair of photons, which are then sent through an optical fiber the probability of arrival decreases exponentially with distance, as does the fidelity of the transmitted state. The central idea of the *quantum repeater* is to divide a long quantum channel into shorter segments, which are first purified separately and then "connected", building up entanglement over the longer compound channel consisting of two segments. In the repeater protocol this is done by teleporting [13] a member of the pair in the right hand segment through the pair in the left hand segment, see Fig. 2. Since teleportation through an imperfect channel degrades the output, after several connections it is necessary to purify the new pairs (that now bridge a larger distance) before further connections can be made. While the combination of purification and

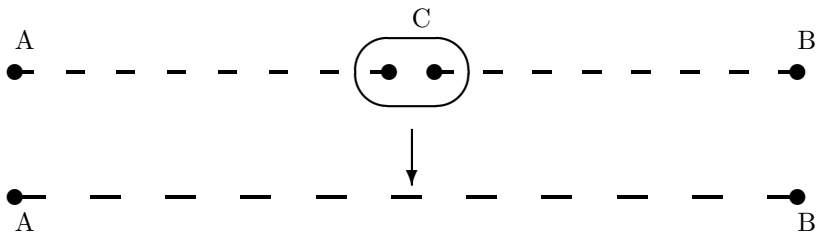

Figure 2: Entanglement swapping: C performs a teleportation of "his" member of the pair AC to B using the pair CB.

teleportation allows to create entanglement over arbitrary distance, the question remains how much this "costs": how many entangled pairs across the initial segments are necessary to obtain one high fidelity pair across the whole channel? The important point of [52] is that it shows that the needed resources grow only *polynomially* with the length of the channel. This shows that the quantum repeater is as efficient as alternative approaches to long-distance communication based on QECCs [72], but – as shown in [52] – is both less sophisticated and more robust than the latter.

4.2 Entanglement Purification with Imperfect Means

The importance of EPPs and the quantum repeater rests on the fact that they would allow to cope with the limitations and imperfections of real-life quantum communication systems, in particular with noisy channels. But the discussion of these imperfections has been incomplete so far, since we always (tacitly) assumed the local operations of which the EPP consists to be perfect. Clearly, this is an unrealistic assumption, and to complete the discussion it needs to be studied, whether purification and the repeater still work with imperfect operations. It turns out that EPPs are significantly more robust against errors than the known universal QECCs.

In [52] analytical and numerical work on the whole quantum repeater protocol (including EPP and teleportation) for a simple generic error model (the "depolarizing channel") showed that errors up to a few percent could be tolerated – much more than the threshold for universal QECCs (about 10^{-4}, [73]). Later it was shown [54] that despite transmission noise and imperfect operation the entangled states obtained in this way do actually represent a *perfectly private* quantum channel, with a potential eavesdropper's knowledge guaranteed to be smaller than any desired bound.

But one might claim that this was an unfair comparison, as the threshold for QECC is derived under much more general assumptions about the errors [73]. This motivated the work of the article [53], reprinted below, it which entanglement purification in the presence of arbitrary errors is investigated, and it is shown that even in this case purification works for errors as large as $0.5 \cdot 10^{-2}$. Therefore, entanglement purification and the quantum repeater, being both simpler and more robust than universal QECC, represent promising tools for long-distance quantum communication with realistic (imperfect) means.

4.3 Lower bounds for attainable fidelities in entanglement purification

Géza Giedke, Hans J. Briegel, J. Ignacio Cirac, and Peter Zoller,

We derive lower bounds for the attainable fidelity of standard entanglement purification protocols when local operations and measurements are subjected to errors. We introduce an error parameter which measures the distance between the ideal completely positive map describing a purification step and the one in the presence of errors. We derive non–linear maps for a lower bound of the fidelity at each purification step in terms of this parameter.

Phys. Rev. A **59**, 2641 (1999); E-print: quant-ph/9809043.

Lower bounds for attainable fidelities in entanglement purification

G. Giedke,[1] H. J. Briegel,[1,2] J. I. Cirac,[1] and P. Zoller[1]
[1]*Institut für Theoretische Physik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria*
[2]*Departamento de Fisica Aplicada, Universidad de Castilla–La Mancha, 13071 Ciudad Real, Spain*
(Received 22 September 1998)

We derive lower bounds for the attainable fidelity of standard entanglement purification protocols when local operations and measurements are subjected to errors. We introduce an error parameter which measures the distance between the ideal completely positive map describing a purification step and the one in the presence of errors. We derive nonlinear maps for a lower bound of the fidelity at each purification step in terms of this parameter. [S1050-2947(99)01104-X]

PACS number(s): 03.67.Hk, 03.65.Bz

I. INTRODUCTION

Entanglement purification [1–3] is one of the most important tools in the theory of quantum information and, in particular, in quantum communication. It allows, in principle, creation of maximally entangled states of particles at different locations, even if the channel that connects those locations is noisy [4]. These entangled particles can then be used for faithful teleportation [5] or secure quantum cryptography [6,7].

The basic idea in entanglement purification is to ''distill'' a few N' pairs of particles [quantum bits (qubits), for example, the case which we will consider exclusively in the following] in highly entangled states out of $N \geqslant N'$ pairs in a mixed state with lower fidelity of the entanglement (or, in short, fidelity) using local operations and measurements. This fidelity is defined as the maximum overlap of the density operator of a pair of qubits with a maximal entangled state. If the initial pairs are in a nonseparable state [8,9], then one can obtain asymptotically (in the limit $N \rightarrow \infty$) maximally entangled states [10] provided all local operations and measurements are perfect [2,11]. In practice, there will be errors in both the local operations and measurements. The purpose of this paper is to analyze this problem for the purification protocols introduced in Refs. [1,7]. We are interested in analyzing the conditions under which one can purify in the presence of errors, as well as in the limitations of the purification protocols. In particular, we find a nonlinear map which relates a lower bound for the fidelity at two consecutive steps of the purification protocol, which allows us to derive lower bounds for the reachable fidelity. In order to analyze this problem, we introduce a parameter δ which characterizes the errors. It measures the distance between the ideal operations and measurements and the ones in the presence of errors.

Quantum communication in the presence of errors has been considered previously by Knill and Laflamme [12] in a general context, and by Van Enk *et al.* [13] for a particular experimental setup [14]. The work of Knill and Laflamme introduced ideas of fault-tolerant quantum computation [15] to show that there exists an accuracy threshold for storage of quantum information, which also applies to the case of quantum communication. As shown by Bennett *et al.* [2] one can rephrase this result in terms of entanglement purification with *one-way classical communication*. In Ref. [16], entanglement purification together with a generic error model is used to estimate the possibilities of quantum communication over long distances using quantum repeaters. The employed entanglement purification protocols explicitly utilize *two-way classical communication*, which makes them much more efficient for quantum communication. In the present paper we use purification protocols which utilize *two-way classical communication*, and therefore our error thresholds are much less demanding than those derived from the theory of Knill and Laflamme [12]. On the other hand, we are interested in a rigorous lower bound for the achievable fidelity for arbitrary errors, and not in an estimation [16]. The results and methods developed here can be generalized to derive lower bounds for other interesting problems in which local operations and measurements are imperfect, such as quantum teleportation or quantum cryptography.

This paper is organized as follows. Section II contains a summary of the main results of this paper, and is directed to the reader who is interested neither in the technical details of the definitions of our error parameter, nor in the derivations of the nonlinear maps for the lower bound of the fidelity. In Sec. III we introduce the error parameter δ and derive some properties related to the fact that it is a distance between completely positive linear maps. Finally, in Sec. IV we derive the nonlinear map for the fidelity of entanglement in terms of this distance and sketch its dynamics.

II. SUMMARY OF THE MAIN RESULTS AND DISCUSSION

In the standard scenario of entanglement purification [1], two partners at different locations share N pairs of qubits, each pair being in a state described by a density operator ρ. A purification procedure produces $N' \leqslant N$ pairs in a state ρ' ''closer'' to a maximally entangled state ψ_{me} by only using local operations, local measurements, and classical communication between the partners. More specifically, if we define the fidelity of the entanglement

$$F(\rho) = \max_{\psi_{me}} \langle \psi_{me} | \rho | \psi_{me} \rangle, \tag{1}$$

where the maximization is taken with respect to maximally entangled states ψ_{me}, then $F(\rho') > F(\rho)$. In the following we will call $F(\rho)$ simply fidelity.

It has been shown [10] that if ρ is nonseparable (it cannot be written as a convex combination of factorized density

 ©1999 The American Physical Society

operators [8,9]) then there are purification procedures which obtain $F(\rho')=1$ in the asymptotic limit $N\to\infty$. In particular, if $F(\rho)>1/2$ one can reach this goal by using the purification procedure devised by Bennett *et al.* [1] and improved by Deutsch *et al.* [7]. It consists of a concatenation of *purification steps* involving two pairs of qubits, which give rise to a single pair with higher fidelity. In all these procedures, one assumes that the local operations and measurements are error free. In a real situation, however, there will be errors due to the coupling to the environment, imprecise apparatus, etc. Although small, they will limit the maximum attainable fidelity and will dictate whether purification is possible or not.

In this section we first briefly review the purification protocol introduced in Refs. [1,7], and define the notation that we will use later on. Then we consider the same procedure in the presence of general errors, and characterize these errors in terms of a single parameter δ, which basically expresses the departure of the purification step in the presence of errors from the ideal one. Next, we express the lowest possible fidelity (worst case) in each purification step as a function of the lowest possible fidelity in the previous step, which leads to a non-linear map. We analyze this map and discuss the conditions required for purification with imperfect means. The properties of our definitions and the technical details are presented in the following sections.

A. Error-free purification protocols

In this subsection we review the two purification procedures introduced in Refs. [1,7]. Subsequently we will refer to them as scheme I and II, respectively. We characterize them in two different ways: first, in terms of a completely positive linear map between the initial density operator and the one after the measurement; secondly, in terms of a nonlinear map relating the diagonal matrix elements of the density operator (in the Bell basis) at each step with the ones in the previous step. In the next subsection we will generalize the first characterization to the case of imperfect operations in order to introduce the parameter describing the errors, and then we will generalize the second characterization to find a lower bound for the fidelity.

Both purification protocols I and II consist of a sequence of steps in which local operations are applied to two pairs of qubits, followed by a measurement of one of the pairs which is then discarded. Depending on the outcome of the measurement, the other pair is discarded or not. In the latter case the fidelity F_1 of the remaining pair is (on average) larger than that of the original ones. This step is applied to the N pairs obtaining $N_1\leqslant N/2$ pairs of fidelity F_1. Then it is applied to the resulting N_1 pairs obtaining N_2 pairs of fidelity $F_2>F_1$. Continuing in this vein, one can reach asymptotically $F_n\to 1$ when $n\to\infty$.

Let us consider a single purification step. It starts out with two pairs 1 and 2 in the state $\rho_{12}=\rho\otimes\rho$, applies the local operations described by the superoperator $\mathcal{U}$, and then measures each of the qubits of the second pair in the basis $\{|0\rangle,|1\rangle\}$. We denote by x the outcome of the measurement: $x=0$ if the qubits are found in the state $|0\rangle_2\equiv|00\rangle_2$; $x=1$ if they are in $|1\rangle_2\equiv|11\rangle_2$; $x=2$ if they are in $|2\rangle_2\equiv|01\rangle_2$; and $x=3$ if they are in $|3\rangle\equiv|10\rangle_2$ (the subscript 2 denotes the second pair). We denote by $\mathcal{P}_x$ $(x=0,\ldots,3)$ the map defined as follows:

$$\mathcal{P}_x(\rho_{12})\equiv {}_2\langle x|\mathcal{U}(\rho_{12})|x\rangle_2. \tag{2}$$

This map is linear and completely positive. The probability of obtaining the outcome x is $p_x(\rho_{12})=\mathrm{tr}[\mathcal{P}_x(\rho_{12})]$. If the outcome is $x=2,3$, then the first pair is discarded and otherwise it is kept. In the latter case, the state of the first pair will be

$$\rho_1'=\frac{\mathcal{P}_0(\rho_{12})+\mathcal{P}_1(\rho_{12})}{p_0(\rho_{12})+p_1(\rho_{12})}. \tag{3}$$

Thus, each (successful) step of the purification protocol is completely characterized by the maps $\mathcal{P}_{0,1}$. (Note that $\mathcal{P}_x$ stand for different maps depending on whether we are discussing scheme I or scheme II.)

On the other hand, if one is only interested in the fidelity at each step, one can use a simpler characterization of each purification step in terms of four real numbers. In the purification protocols I and II, the local operations characterized by $\mathcal{U}$ consist of a bilateral controlled-NOT gate and specific single qubit rotations. In that case, the diagonal elements of the density operator ρ' in the Bell basis only depend on the diagonal elements of the density operator ρ, and therefore each purification step can be characterized by a nonlinear map between these four diagonal matrix elements. We denote by $A_n^i=\langle\phi^i|\rho_n|\phi^i\rangle$, where ρ_n is the density operator of each pair after the nth purification step and $|\phi^i\rangle$ are the elements of the Bell basis $(i=0,1,2,3)$,

$$|\phi^{0,3}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),$$

$$|\phi^{1,2}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle).$$

In particular, $A_n^0=F_n$, the entanglement fidelity at each step. For scheme II there is, according to Ref. [7], a simple nonlinear map that relates $\mathbf{A}_{n+1}$ to $\mathbf{A}_n$, namely

$$A_{n+1}^i=\frac{\langle\phi^i|\mathcal{P}_0(\rho_n\otimes\rho_n)+\mathcal{P}_1(\rho_n\otimes\rho_n)|\phi^i\rangle}{\mathrm{tr}[\mathcal{P}_0(\rho_n\otimes\rho_n)+\mathcal{P}_1(\rho_n\otimes\rho_n)]}=:\frac{f^i(\mathbf{A}_n)}{g(\mathbf{A}_n)}, \tag{4}$$

where

$$f^0(\mathbf{A}_n)=(A_n^0)^2+(A_n^1)^2, \tag{5a}$$

$$f^1(\mathbf{A}_n)=2A_n^2A_n^3, \tag{5b}$$

$$f^2(\mathbf{A}_n)=(A_n^2)^2+(A_n^3)^2, \tag{5c}$$

$$f^3(\mathbf{A}_n)=2A_n^0A_n^1, \tag{5d}$$

$$g(\mathbf{A}_n)=(A_n^0+A_n^1)^2+(A_n^2+A_n^3)^2. \tag{5e}$$

The map (4) has a fixed point at $\mathbf{A}=(1,0,0,0)$, which is reached if the initial state has $A_0^0=F>1/2$ [17]. This fact expresses that in the absence of errors, one can use this pu-

rification protocol to purify states with $F>1/2$ and reach a fidelity as close to one as we please.

Scheme I [1] is governed by a similar map. The main difference is that at the end of each step the resulting state is brought into Werner form, that is, the three diagonal elements A^1,A^2,A^3 are made equal to $(1-A^0)/3$. Therefore one can concentrate on the first diagonal element, the fidelity A^0, only. The fidelity after the nth purification step is then given by

$$A^0_{n+1}=\frac{f^0(A^0_n,(1-A^0_n)/3)}{g(A^0_n,(1-A^0_n/3)}. \tag{6}$$

Like Eq. (4), this map has an attractive fixed point at $A^0=1$, and all $A^0_0>1/2$ are attracted to it.

B. Characterization of errors

In practice, while performing the purification protocols, errors will occur, both in the local operation and in the measurements. The imperfections in the local operations can be accounted for by substituting the action of the superoperator $\mathcal{U}$ in Eq. (2) by the action of some other completely positive, trace-preserving linear map. The errors in the measurements will be related to the following fact: in practice, the outcomes $x=0,1$ will be ultimately attributed to the presence/absence of clicks in some kind of detectors. Due to imperfections, the projection operators (or, more generally, POVMs) corresponding to those clicks are not exactly the same as the ideal ones [see Eq. (2)]. Consequently, the probabilities of the outcomes $x=0,1$ as well as the state remaining after the measurement will differ from the ideal ones. In general, we can describe both these erroneous operations and measurements in terms of a single completely positive linear map $\tilde{\mathcal{P}}_x$ which does not necessarily preserve the trace (we will use tildes in the case in which there are errors). That is, if the two pairs are initially in the state $\rho_{12}=\rho\otimes\rho$, a purification step yields the outcome x with a probability $\tilde{p}_x(\rho_{12})=\mathrm{tr}[\tilde{\mathcal{P}}_x(\rho_{12})]$. The state of the pair after the measurement is

$$\tilde{\rho}'_1=\frac{\tilde{\mathcal{P}}_0(\rho_{12})+\tilde{\mathcal{P}}_1(\rho_{12})}{\tilde{p}_0(\rho_{12})+\tilde{p}_1(\rho_{12})}. \tag{7}$$

Thus, as before, the maps $\tilde{\mathcal{P}}_{0,1}$ completely characterize each purification step.

We characterize the errors by a single parameter as follows:

$$\delta:=\max_{x=0,1} d(\mathcal{P}_x,\tilde{\mathcal{P}}_x), \tag{8}$$

where $d(\mathcal{P},\tilde{\mathcal{P}})$ denotes a distance between $\mathcal{P}$ and $\tilde{\mathcal{P}}$. The explicit form of this distance is given in Eq. (13) below. We emphasize that for a given set-up, one can (in principle) perform local measurements to completely characterize $\tilde{\mathcal{P}}_x$, and therefore obtain the value of δ experimentally [18,19]. The error parameter δ has a clear physical meaning since it measures the distance between the ideal process and the erroneous one. We would like to remark here that due to the fact that there are measurements and postselection involved in the process, we have to work with maps $\mathcal{P}_x$ that do not preserve the trace. In Sec. III we discuss why it is advantageous to use those maps instead of trace-preserving maps.

Some remarks concerning the adopted description of errors are in order: We envision $\mathcal{P}$ as the reduced dynamics of the two entangled pairs coupled to some environment [20]. In taking the imperfect system dynamics to be completely positive we do (as discussed in [20]) essentially assume that there is *no initial entanglement* between the system and any environment to which it might be coupled during gate operations. There may be, however, initial entanglement of the system with another environment that is not affected by the gate operations. As in the error-free purification schemes [1,7] we also assume the two pairs that participate in a purification step to be disentangled from each other.

C. Purification with imperfect means

Once we have defined a parameter that characterizes the errors at each purification step, we can analyze the whole purification procedure [1,7] in the nonideal case. In order to do that, we define $\tilde{A}^i_n=\langle\phi^i|\tilde{\rho}_n|\phi^i\rangle$ where $\tilde{\rho}_n$ is the density operator after the nth purification step. We are particularly interested in the fidelity at each step $\tilde{A}^0_n=\tilde{F}_n$. In Sec. IV we show that for suitable initial conditions $\mathbf{A}_0$ and error parameter δ,

$$\tilde{A}^0_n\geqslant a_n,\ \ \tilde{A}^1_n\leqslant b_n\ \ (n=1,2,\ldots), \tag{9}$$

where

$$a_{n+1}=\frac{a_n^2+b_n^2-2\delta}{(a_n+b_n)^2+(1-a_n-b_n)^2+2\delta}, \tag{10a}$$

$$b_{n+1}=\frac{(1-a_n)^2/2+2\delta}{a_n^2+(1-a_n)^2-2\delta}, \tag{10b}$$

and $a_0=\tilde{A}^0_0$, $b_0=\tilde{A}^1_0$. For scheme I only the fidelity A^0_n and therefore the bound (10a) with b_n replaced by $(1-a_n)/3$ is relevant.

Equations (10) define a nonlinear map that can be iterated to yield a lower bound for the attainable fidelity $\tilde{F}_\infty\geqslant a_\infty$ which depends on the value of δ. In the following we will analyze the map (10).

Let us first concentrate on the fixed points (a_f,b_f) of this map, and consider in particular scheme II. In Fig. 1 (solid line) we have plotted a_f as a function of the error parameter δ. For small values of $\delta\lesssim 0.01$ there are three fixed points. The ones with largest and the smallest value of a_f are attractive, whereas the intermediate one is a saddle point attractive in one direction and repulsive in the others. For larger values of δ, only the smallest one survives. This means that for the appropriate initial values of a_0 and b_0 if $\delta\lesssim 0.01$ one increases the fidelity using the purification protocol II to a value larger than the one given by the right wing of the appropriate curve of Fig. 1. For example, for $\delta\simeq 0.005$ one can obtain a fidelity $F\gtrsim 0.95$.

Now, let us analyze for which initial conditions (a_0,b_0) the map converges to the fixed point with the largest a_f, i.e., for which the protocol achieves purification. In Fig. 2 we

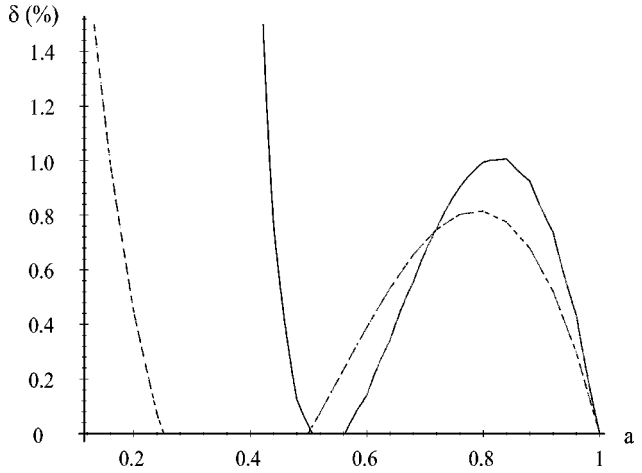

FIG. 1. The fixed points of the nonlinear map: the intersections of a horizontal line at δ with the plotted curve give the a coordinates of the fixed points for scheme I (broken) and scheme II (solid).

have plotted in the (a,b) parameter space the curve (separatrix) between the stable regions for several values of δ ($\delta_k = 0.002k$, $k=0,1,\ldots,5$). For any initial value (a_0,b_0) lying to the right of each curve, the map will converge to the corresponding fixed point (asterisks in the plot). For $\delta = 0.006$ ($k=3$ in the plot), for example, one can purify from values of $a_0 \gtrsim 0.69$ up to values of $F \geqslant a_f \approx 0.94$; for $\delta = 0.002$, one can reach $F \gtrsim 0.98$ starting from $a_0 \leqslant 0.61$. The results show that the error threshold for purification is much less restrictive than the one for quantum computation [12].

III. DISTANCE BETWEEN TWO POSITIVE MAPS

We denote by H a finite dimensional complex Hilbert space and by $L(H)$ the complex Banach space of linear operators $A:H\rightarrow H$ with the trace norm $||A|| = \mathrm{tr}(|A^\dagger A|^{1/2}) \equiv \mathrm{tr}(|A|)$ (as usual, $|A| \equiv |A^\dagger A|^{1/2}$). We denote by $C(H) \subset L(H)$ the convex set of positive linear operators ρ acting on H with $||\rho|| \leqslant 1$, and by $P(H,H')$ the set of completely positive linear maps $\mathcal{P}: C(H) \rightarrow C(H')$ fulfilling

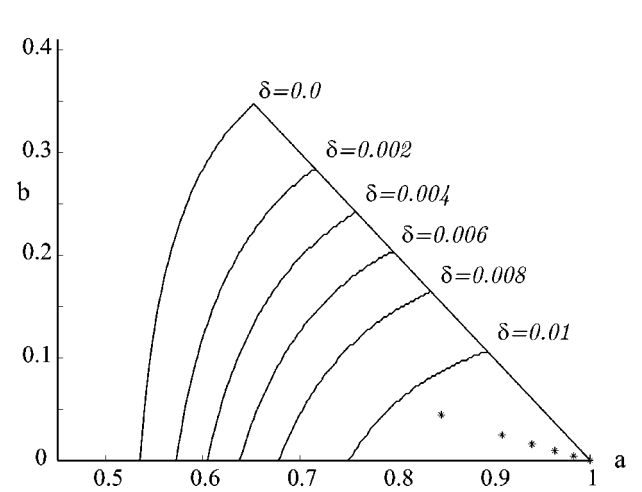

FIG. 2. The solid lines show the border between the two stable sets (the separatrix) for six values of δ. The asterisks show the corresponding (δ increasing from right to left) upper fixed points.

$$||\mathcal{P}(\rho)|| \leqslant ||\rho||. \tag{11}$$

For positive operators, the trace norm simply coincides with the trace, and therefore Eq. (11) is equivalent to

$$\mathrm{tr}[\mathcal{P}(\rho)] \leqslant \mathrm{tr}(\rho) \leqslant 1. \tag{12}$$

Given two completely positive maps $\mathcal{P},\tilde{\mathcal{P}} \in P(H,H')$, we define their distance

$$d(\mathcal{P},\tilde{\mathcal{P}}) = \max_{\rho \in C(H)} ||\mathcal{P}(\rho) - \tilde{\mathcal{P}}(\rho)||. \tag{13}$$

It is straightforward to show that d is indeed a distance by using the fact that the trace norm is a norm.

With this definition, we can characterize the errors by using the parameter δ as defined in Eq. (8). The motivation for this definition with respect to other possible definitions is that it easily gives lower bounds even for physical processes where there are measurements and postselection (as it is in the case of entanglement purification, cf. next section), i.e., when the map describing the physical process is not trace preserving. On the other hand (although we will not use this property here), it allows one to easily bound the distance between processes which are composed of several individual processes in terms of the distances between the individual processes themselves (see next subsection).

One can define other distances between trace preserving maps: for example, one can consider the map $\tilde{\mathcal{P}}'$ that transforms $\rho_{12} \rightarrow \rho_1'$, where ρ_1' is given in Eq. (7) in terms of the linear maps $\tilde{\mathcal{P}}_{0,1}$. This new map, although trace preserving, is nonlinear. If one defines distances between $\tilde{\mathcal{P}}'$ and the corresponding (trace-preserving) ideal map $\mathcal{P}'$, problems related to the nonlinearity arise: for example, it can happen that while the distance δ between the linear maps $\mathcal{P},\tilde{\mathcal{P}}$ is very small, the similarly defined distance between the nonlinear maps $\mathcal{P}',\tilde{\mathcal{P}}'$ is of the order of 1, which makes the definition useless to derive bounds. The reason is that low probability processes get ''magnified'' by the normalization and then dominate the maximization used to define the distance.

One can still define other error parameters to find sharper bounds to the fidelity in entanglement purification. However, by increasing the number of parameters one does not gain too much and the bounds become more complicated to analyze. On the other hand, $d(\mathcal{P}\otimes 1,\tilde{\mathcal{P}}\otimes 1) \neq d(\mathcal{P},\tilde{\mathcal{P}})$ [19], which would allow us to use d in processes for which the system in which we perform operations and measurements is entangled with another system, without having to include the other system in the error analysis. This may be useful, for example, in quantum computation where operations are performed on single qubits that are entangled with many other qubits. In that case, one can define other distances, as it is done in Ref. [19]. In any case, in quantum communication if we can bound the fidelity when the system is not entangled, we can automatically derive a bound for the entanglement fidelity [12,4].

A. Properties of d

In this subsection we derive some properties of the distance d introduced above. Given $\mathcal{P},\tilde{\mathcal{P}}\in P(H,H')$ we have the following.

(1) We can restrict the maximization in Eq. (13) to one dimensional projectors, i.e.,

$$d(\mathcal{P},\tilde{\mathcal{P}})=\max_{\psi\in H,\,||\,|\psi\rangle||=1}||\mathcal{P}(|\psi\rangle\langle\psi|)-\tilde{\mathcal{P}}(|\psi\rangle\langle\psi|)||. \quad (14)$$

Proof: We just have to prove that the distance as given in Eq. (14) is always larger than or equal to the one given in Eq. (13), since the converse is clearly true. For any $\rho\in C(H)$ we write $\rho=\Sigma P_i|\phi_i\rangle\langle\phi_i|$ with $\Sigma_i P_i\leq 1$ and ψ_i normalized states of H. Using the linearity of $\mathcal{P}$ and $\tilde{\mathcal{P}}$ and that $||\Sigma_i P_i A_i||\leq\max_i||A_i||$, we find that $||\mathcal{P}(\rho)-\tilde{\mathcal{P}}(\rho)||\leq\max_i||\mathcal{P}(|\phi_i\rangle\langle\phi_i|)-\tilde{\mathcal{P}}(|\phi_i\rangle\langle\phi_i|)||$. Taking the maximum with respect to ρ in this inequality completes the proof.

(2) For all $\rho\in C(H)$ and $\phi\in H$ (normalized state) we have

$$\langle\phi|\mathcal{P}(\rho)|\phi\rangle-d(\mathcal{P},\tilde{\mathcal{P}})\leq\langle\phi|\tilde{\mathcal{P}}(\rho)|\phi\rangle\leq\langle\phi|\mathcal{P}(\rho)|\phi\rangle+d(\mathcal{P},\tilde{\mathcal{P}}), \quad (15a)$$

$$\mathrm{tr}[\mathcal{P}(\rho)]-d(\mathcal{P},\tilde{\mathcal{P}})\leq\mathrm{tr}[\tilde{\mathcal{P}}(\rho)]\leq\mathrm{tr}[\mathcal{P}(\rho)]+d(\mathcal{P},\tilde{\mathcal{P}}). \quad (15b)$$

Proof: For Eq. (15a) we use

$$|\langle\phi|\mathcal{P}(\rho)-\tilde{\mathcal{P}}(\rho)|\phi\rangle|\leq||\mathcal{P}(\rho)-\tilde{\mathcal{P}}(\rho)||\leq d(\mathcal{P},\tilde{\mathcal{P}}), \quad (16)$$

whereas for Eq. (15b) we use

$$|\mathrm{tr}[\mathcal{P}(\rho)-\tilde{\mathcal{P}}(\rho)]|\leq\mathrm{tr}[|\mathcal{P}(\rho)-\tilde{\mathcal{P}}(\rho)|]=d(\mathcal{P},\tilde{\mathcal{P}}). \quad (17)$$

Next, we give a property that allows one to bound the distance when one applies sequential maps. This may be useful when one has a concatenation of processes.

(3) Given $\mathcal{P}\in P(H',H'')$ and $\mathcal{Q}\in P(H,H')$, we define $\mathcal{P}\circ\mathcal{Q}\in P(H,H'')$ according to $(\mathcal{P}\circ\mathcal{Q})(\rho)=\mathcal{P}[\mathcal{Q}(\rho)]$. Then, we have

$$d(\mathcal{P}\circ\mathcal{Q},\tilde{\mathcal{P}}\circ\tilde{\mathcal{Q}})\leq d(\mathcal{P},\tilde{\mathcal{P}})+d(\mathcal{Q},\tilde{\mathcal{Q}}). \quad (18)$$

Proof: Using the properties of a distance, we have

$$d(\mathcal{P}\circ\mathcal{Q},\tilde{\mathcal{P}}\circ\tilde{\mathcal{Q}})\leq d(\mathcal{P}\circ\mathcal{Q},\mathcal{P}\circ\tilde{\mathcal{Q}})+d(\mathcal{P}\circ\tilde{\mathcal{Q}},\tilde{\mathcal{P}}\circ\tilde{\mathcal{Q}}). \quad (19)$$

On the one hand, we have

$$d(\mathcal{P}\circ\tilde{\mathcal{Q}},\tilde{\mathcal{P}}\circ\tilde{\mathcal{Q}})=\max_{\rho\in C(H)}||\mathcal{P}[\tilde{\mathcal{Q}}(\rho)]-\tilde{\mathcal{P}}[\tilde{\mathcal{Q}}(\rho)]||\leq\max_{\rho'\in C(H')}||\mathcal{P}(\rho')]-\tilde{\mathcal{P}}(\rho')||=d(\mathcal{P},\tilde{\mathcal{P}}), \quad (20)$$

where we have used Eq. (11) for $\tilde{\mathcal{Q}}$. On the other hand,

$$d(\mathcal{P}\circ\mathcal{Q},\mathcal{P}\circ\tilde{\mathcal{Q}})=\max_{\rho\in C(H)}||\mathcal{P}[\mathcal{Q}(\rho)]-\mathcal{P}[\tilde{\mathcal{Q}}(\rho)]||=\max_{\rho\in C(H)}||\mathcal{P}[\mathcal{Q}(\rho)-\tilde{\mathcal{Q}}(\rho)]||. \quad (21)$$

Now, since $\mathcal{Q}(\rho)-\tilde{\mathcal{Q}}(\rho)$ is self-adjoint, we can substitute in this last equation its spectral decomposition

$$\mathcal{Q}(\rho)-\tilde{\mathcal{Q}}(\rho)=\sum_\phi|\phi\rangle\langle\phi|\langle\phi|\mathcal{Q}(\rho)-\tilde{\mathcal{Q}}(\rho)|\phi\rangle \quad (22)$$

obtaining

$$d(\mathcal{P}\circ\mathcal{Q},\mathcal{P}\circ\tilde{\mathcal{Q}})=\max_{\rho\in C(H)}\sum_\phi|\langle\phi|\mathcal{Q}(\rho)-\tilde{\mathcal{Q}}(\rho)|\phi\rangle|\times||\mathcal{P}(|\phi\rangle\langle\phi|)||$$

$$\leq\max_{\rho\in C(H)}\sum_\phi|\langle\phi|\mathcal{Q}(\rho)-\tilde{\mathcal{Q}}(\rho)|\phi\rangle| \quad (23)$$

$$=\max_{\rho\in C(H)}||\mathcal{Q}(\rho)-\tilde{\mathcal{Q}}(\rho)||=d(\mathcal{Q},\tilde{\mathcal{Q}}), \quad (24)$$

which completes the proof.

(4) Finally, we show that the distance d stems from a norm, which may be useful to derive some other properties. First, let us enlarge the set $C(H)$ so that it becomes a Banach space. The simplest way is to define $S(H)=\mathrm{lin}_R\{C(H)\}$, that is, the set of operators that can be written as a (finite) linear combination of positive operators with real coefficients. The real Banach space $S(H)\subset L(H)$ is simply the space of self-adjoint operators acting on H. In the same way, we can enlarge the set $P(H,H')$. First, given a map $\mathcal{P}\in P(H,H')$ we define $\hat{\mathcal{P}}:S(H)\to S(H)$ by using the linearity of $\mathcal{P}$ [that is, if $S(H)\ni A=\Sigma_i\lambda_i\rho_i$ with $\rho_i\in C(H)$, we define $\mathcal{P}(A)=\Sigma_i\lambda_i\mathcal{P}(\rho_i)$]. Then, we define $Q(H,H')=\mathrm{lin}_R\{P(H,H')\}$, which is a real vector space. Using the operator norm

$$||\mathcal{P}||_{\mathrm{op}}=\max_{A\in S(H)||A||\leq 1}||\mathcal{P}(A)||, \quad (25)$$

it becomes a real Banach space. With this definition we have

$$d(\mathcal{P},\tilde{\mathcal{P}})=||\mathcal{P}-\tilde{\mathcal{P}}||_{\mathrm{op}}. \quad (26)$$

Proof: We show that the distance given in Eq. (26) is smaller than or equal to the one defined in Eq. (13), since the converse is obviously true since $C(H)\subset S(H)$. For any $A\in S(H)$ with $||A||\leq 1$ we can write $A=\Sigma_i\lambda_i|\phi\rangle\langle\phi|$, where $\Sigma_i|\lambda_i|\leq 1$. Now, arguing as in the proof of the property (1), we obtain that $||\mathcal{P}(A)-\tilde{\mathcal{P}}(A)||\leq\max_\phi||\mathcal{P}(|\phi\rangle\langle\phi|)-\tilde{\mathcal{P}}(|\phi\rangle\langle\phi|)||$. Taking the maximum over all possible $A\in S(H)$ we complete the proof.

The distance d is not unrelated to other quantities used in the literature to characterize erroneous operations. Typically, given one of the other quantities, one can bound d (and vice versa within the respective domains of applicability). Specifically this is true for the minimum fidelity, the error amplitude [12], and the generic error model [16]. The diamond

norm introduced in [19] is a generalization of the distance used here and particularly useful to discuss operations on systems that are strongly entangled with other systems.

IV. NONLINEAR MAP FOR ENTANGLEMENT PURIFICATION

In this section we derive the nonlinear map (10) for the bounds of the diagonal matrix elements in the Bell basis of the density operator after each step of the purification process. As above, let $\tilde{A}_n^i=\langle\phi^i|\tilde{\rho}_n|\phi^i\rangle$, $i=0\ldots3$. Analogous to Eq. (4), we have

$$\tilde{A}_{n+1}^i=\frac{\langle\phi^i|\tilde{\mathcal{P}}_0(\tilde{\rho}_n\otimes\tilde{\rho}_n)+\tilde{\mathcal{P}}_1(\tilde{\rho}_n\otimes\tilde{\rho}_n)|\phi^i\rangle}{\mathrm{tr}[\tilde{\mathcal{P}}_0(\tilde{\rho}_n\otimes\tilde{\rho}_n)+\tilde{\mathcal{P}}_1(\tilde{\rho}_n\otimes\tilde{\rho}_n)]}. \tag{27}$$

Using Eq. (10) we have that

$$\frac{f^i(\tilde{\mathbf{A}}_n)-2\delta}{g(\tilde{\mathbf{A}}_n)+2\delta}\leqslant\tilde{A}_{n+1}^i\leqslant\frac{f^i(\tilde{\mathbf{A}}_n)+2\delta}{g(\tilde{\mathbf{A}}_n)-2\delta}, \tag{28}$$

where f^i and g are defined in Eq. (5). In the following subsections we will discuss the two purification schemes separately in detail.

A. Scheme I

As stated above for scheme I we can use Eq. (6) instead of f^0 and forget about the other three diagonal elements. This gives

$$\tilde{A}_{n+1}^0\geqslant\frac{(\tilde{A}_n^0)^2+[(1-\tilde{A}_n^0)/3]^2-2\delta}{[\tilde{A}_n^0+(1-\tilde{A}_n^0/3]^2+[1-\tilde{A}_n^0+(1-\tilde{A}_n^0)/3]^2+2\delta}. \tag{29}$$

Now we observe that the right hand side of Eq. (29) is monotonically increasing with $\tilde{A}_n^0$ for all $\tilde{A}_n^0\geqslant1/8$. Therefore replacing $\tilde{A}_n^0$ by $\frac{1}{8}\leqslant a_n\leqslant\tilde{A}_n^0$ in Eq. (29) yields a lower bound for $\tilde{A}_{n+1}^0$. Since the interval [1/8,1] is mapped into itself by the left hand side of Eq. (29) we arrive at the dynamical system defined by $a_0=A_0^0$ and

$$a_{n+1}=\frac{a_n^2+[(1-a_n)/3]^2-2\delta}{[a_n+(1-a_n)/3]^2+[1-a_n-(1-a_n)/3]^2+2\delta}. \tag{30}$$

For every n the value of a_n is a lower bound of the fidelity after n purification steps.

In the case $\delta=0$ the original map of Bennett *et al.* is recovered. The three fixed points of that map at $a_l(\delta)\approx0.25$, $a_i(\delta)\approx0.5$, and $a_u(\delta)\approx1$ survive even for nonzero δ and are given by the roots of the cubic polynomial

$$x^3-\frac{7}{4}x^2+\left[\frac{7}{8}+\frac{9}{4}\delta\right]x-\left[\frac{1}{8}-\frac{9}{4}\delta\right].$$

They are plotted as a function of δ in Fig. 1 (broken line). For $\delta\geqslant0.008$ only the lower fixpoint survives.

The upper and lower fixpoints are attractive, while the intermediate is repulsive. Consequently even an imperfectly implemented scheme I allows us to purify ensembles with initial fidelity $F_{\mathrm{in}}>a_i(\delta)$ up to a fidelity $F_{\mathrm{out}}\geqslant a_u(\delta)$, provided that $\delta\leqslant0.008$.

B. Scheme II

Scheme II converges faster than scheme I and can tolerate somewhat larger errors, but the analysis becomes significantly more complicated, since all four diagonal elements of the density matrix come into play. Using Eq. (28) we have

$$\tilde{A}_{n+1}^0\geqslant\frac{(\tilde{A}_n^0)^2+(\tilde{A}_n^1)^2-2\delta}{(\tilde{A}_n^0+\tilde{A}_n^1)^2+(\tilde{A}_n^2+\tilde{A}_n^3)^2+2\delta}, \tag{31a}$$

$$\tilde{A}_{n+1}^1\leqslant\frac{2\tilde{A}_n^2A_n^3+2\delta}{(\tilde{A}_n^0+\tilde{A}_n^1)^2+(\tilde{A}_n^2+\tilde{A}_n^3)^2-2\delta}. \tag{31b}$$

To proceed the same way as in the preceding subsection we need again a monotonicity property of the right hand sides of Eqs. (31) so that we can replace the values $\tilde{A}_n^i$ (which are typically not known, since their exact value depends on the unkown errors in $\tilde{\mathcal{P}}$) by lower or upper bounds, respectively.

Using $\Sigma_i\tilde{A}_n^i=1$ we can express the right hand side of Eq. (31a) in terms of $\tilde{A}_n^0,\tilde{A}_n^1$ only. It is straightforward to check that the resulting expression is monotonically increasing in $\tilde{A}_n^0$ and monotonically decreasing in $\tilde{A}_n^1$ for all $(\tilde{A}_n^0,\tilde{A}_n^1)$ fulfilling

$$\tilde{A}_n^0\geqslant\frac{1}{2}+\frac{3\delta}{1-2\delta}\ \text{ and }\ \tilde{A}_n^1\leqslant0.5. \tag{32}$$

Thus, provided that $\tilde{A}_n^0\geqslant a_n$, $\tilde{A}_n^1\leqslant b_n$, and (a_n,b_n) fulfill the condition (32), then a_{n+1} as given in Eq. (10a) is a lower bound for $\tilde{A}_{n+1}^0$.

It remains to justify Eq. (10b). Starting from Eq. (31b) we can this time express the right hand side only in terms of $\alpha_n=\tilde{A}_n^2+\tilde{A}_n^3$ and $\beta_n=\tilde{A}_n^2-\tilde{A}_n^3$ using the normalization condition

$$\tilde{A}_{n+1}^1\leqslant\frac{\frac{1}{2}(\alpha_n^2-\beta_n^2)+2\delta}{\alpha_n^2+(1-\alpha_n)^2-2\delta}.$$

Now it is easy to check that the right hand side of this inequality is monotonically increasing in α_n (for fixed β_n) and takes (for fixed α_n) its maximum at $\beta_n=0$, where we use the fact that $\alpha_n\leqslant1-\tilde{A}_n^0$ and $\tilde{A}_n^0\geqslant0.5$. Since $\alpha_n=\tilde{A}_n^2+\tilde{A}_n^3\leqslant1-\tilde{A}_n^0\leqslant1-a_n$ we arrive at Eq. (10b) by replacing $\beta_n\to0$ and $\alpha_n\to1-a_n$.

The discrete dynamical system defined by the map (10) has for $0\leqslant\delta\lesssim0.01$ three fixpoints with a coordinate around $a_l\approx0.5$, $a_i\approx0.6$, $a_u\approx1$. Figure 1 (solid line) shows them as a function of δ. For $\delta>0.01$ only the lower fixpoint survives. The exact a values are given by the real roots of a polynomial of seventh degree or equivalently by the intersections of the curves $b_{n+1}(a)$ and

$$b_{\mathrm{fix}}(a) = -a + \sqrt{a - \left(1 + \frac{3}{2a-1}\right)\delta}, \tag{33}$$

the latter of which is defined by $a_{n+1}\,(a_n, b_{\mathrm{fix}}(a_n)) = a_n$. The corresponding b coordinates are $b_{n+1}(a_x)$, where $x = l, i, u$.

As in the previous case the upper and lower fixpoints are attractive, while the intermediate one is now a saddle point, attractive in one direction and repulsive in the others. Now essentially the same argument as in the preceding subsection applies: points between intermediate and upper fixed points are purified to a final fidelity $F_{\mathrm{out}} \geq a_u$. There are, however, two complications: first, the eventual fate of a point (a,b) depends on both a and b. Second, we need to make sure that the conditions (32) are fulfilled in every step of the iteration, otherwise it is no longer valid to interpret (a_n, b_n) as bounds of the actual values $(\tilde{A}_n^0, \tilde{A}_n^1)$. For both of these complications we have been unable to find complete analytical answers. Therefore we first give the numerical results before mentioning partial analytical solutions.

Numerical calculations show that the physically meaningful set $\{(a,b): 0 \leq a \leq 1, 0 \leq b \leq 1-a\}$ is divided in two parts by a curve passing through the intermediate fixed point, the separatrix (see Fig. 2). Points to the right of that curve converge to the upper fixed point, points to the left towards the lower one. Moreover, all points to the right satisfy the conditions (32) and so do the orbits of all these points. For all ensembles described by density matrices with diagonal elements A_0^0, A_0^1 in that region, a_n, b_n as defined in Eq. (10) provide lower and upper bounds for the respective fidelities after n purification steps. For initial values to the left of the separatrix our approach allows no statement. The case $\delta = 0$ in Fig. 2 indicates how many ''good'' points our worst-case consideration misses: as shown in [17] the exact border of the set of purifiable points in the (a,b) plane is given by the straight line $a = 0.5$.

For a subset of the points to the right of the separatrix it is easy to *prove* convergence: All the points (a,b) fulfilling $a \geq a_i$, $b \leq b_i$, and $a + b \leq 1$ converge to the upper fixed point P_u (except for P_i, of course).

Proof: The proof proceeds in four steps. The main tool is the monotonic dependence of a_{n+1}, b_{n+1} on a and b. [It is easily checked by calculation that the coordinates of the intermediate fixed point satisfy the conditions (32) for all δ so that monotonicity holds.]

(i) Consider (a,b) in the set enclosed by the two curves $b_{n+1}(a)$ and $b_{\mathrm{fix}}(a)$ [Eq. (33), cf. Fig. 3]. For these points, we have for all n

$$a_{n+1} \geq a_n \quad \text{and} \quad b_{n+1} \leq b_n .$$

Since a_n and b_n are bounded by the coordinates of the upper and intermediate fixpoints, they form monotonical, bounded sequences and therefore converge. Since a_n increases and b_n decreases, they converge towards (a_u, b_u).

(ii) Similarly it is seen that all points $(a \geq a_u, b \leq b_u)$ do converge to the fixed point ''from above.''

(iii) Now, consider a point $X = (a, b \leq b_u)$ below the curve $b_{n+1}(a)$.

Let us call a point (a,b) *better* than (a',b'), if $a \geq a'$ and $b \leq b'$. Monotonicity implies that if (a,b) better than (a',b') then this will also be true for the images of these points after one iteration of the dynamical system.

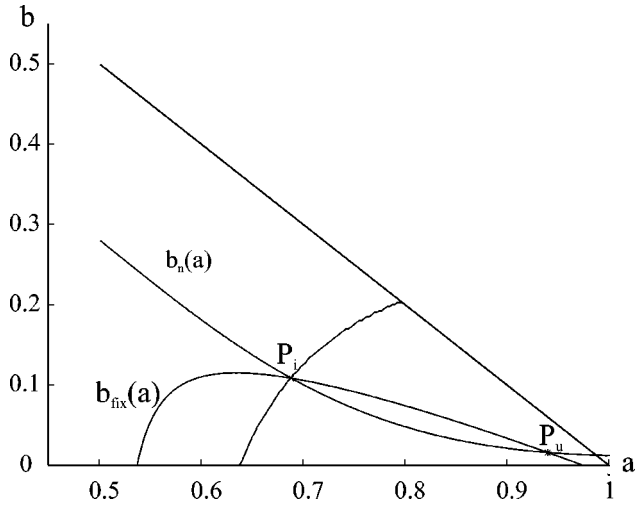

FIG. 3. For $\delta = 0.006$ the curves b_n (10b) and b_{fix} (33) are plotted. Their intersections are fixed points of the dynamical system.

Now compare X with $X' = (a' = a, b')$ between the curves but with the same a as X, and with $X'' = (a'' \geq a_u, b'' = b)$. Clearly, X is better than X' but worse than X''. Since both X' and X'' converge towards the upper fixpoint, so does X.

(iv) A similar argument applies, if we compare a point $Y = (a, b > b_{\mathrm{fix}}(a))$ with $Y' = (a' < a, b' = b)$ between the curves and $Y'' = (a'' = a, b'' \leq b)$ below the curves: the primed points converge to the upper fixpoint, and thus (a,b)—being better than Y' and worse than Y''—does so, too. This completes the proof.

V. SUMMARY

The entanglement purification protocols [1,7] in the presence of errors in gate operations and measurements have been investigated. The errors are quantified by a single parameter derived from the trace norm. We have shown that these protocols allow us to increase the fidelity of the entanglement even if implemented with imperfect quantum gates and measurements, as long as the errors are below a threshold of the order 1%. We derived a nonlinear map to calculate a lower bound for the fidelity after n purification steps. Polynomials are given, a root of which gives a lower bound for the asymptotically attainable fidelity.

The methods and definitions introduced in this work can be applied to other interesting problems in quantum information, like teleportation or quantum cryptography. Furthermore, they can be used to analyze other purification protocols which, under certain circumstances, are more efficient than the ones studied here (see, for example, Refs. [1,2]).

ACKNOWLEDGMENTS

This work was supported in part by the Österreichischer Fonds zur Förderung der wissenschaftlichen Forschung and by the European TMR Network No. ERB-FMRX-CT96-0087. G.G. thanks Wolfgang Dür for useful discussions. Part of this work was completed during the 1998 Elsag-Bailey–I.S.I. Foundation research meeting on quantum computation.

[1] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[3] N. Gisin, Phys. Lett. A **210**, 151 (1996).
[4] B. Schumacher, Phys. Rev. A **54**, 2614 (1996); B. Schumacher and M. D. Westmoreland, *ibid.* **56**, 131 (1997).
[5] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[6] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[7] D. Deutsch, A. Ekert, R. Josza, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[8] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[9] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[10] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[11] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[12] E. Knill and R. Laflamme, e-print quant-ph/9608012; E. Knill, R. Laflamme, and W. Zurek, Proc. R. Soc. London, Ser. A **454**, 365 (1998).
[13] S. Van Enk, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 4293 (1997); Science **279**, 205 (1998).
[14] J. I. Cirac, P. Zoller, J. H. Kimble, and H. Mabuchi, and Phys. Rev. Lett. **78**, 3221 (1997).
[15] P. Shor, SIAM J. Comput. **26**, 1484 (1997); e-print quant-ph/9605011; A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997); D. Gottesman, e-print quant-ph/970229.
[16] H. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998); W. Dür, H. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[17] C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
[18] J. F. Poyatos, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 390 (1997); I. Chuang and M. Nielsen, J. Mod. Opt. **44**, 2455 (1997).
[19] D. Aharonov, A. Kitaev, and N. Nisan, e-print quant-ph/9806029.
[20] As shown in P. Pechukas, Phys. Rev. Lett. **73**, 1060 (1994), reduced dynamics in general need not be completely positive (not even positive) on the whole system space. In the case of weak coupling between system and environment, short memory of the environment and time coarse graining, the description of the reduced dynamics by a completely positive map is justified even in the case of initial entanglement [see A. Royer, Phys. Rev. Lett. **77**, 3272 (1996)]. We thank D. Lidar for pointing out these references.

4.4 EPP for Gaussian States

In the CV setting there are two questions: the first – how can distillable Gaussian states be distilled in principle? – has already been answered in the distillability proof. The more interesting question concerns *implementation*: we would like to find an EPP employing only transformations that can be realized experimentally with current technology, e.g. in a quantum optical setting.

4.4.1 Linear Means: Linear Transformations, Homodyne Detection

Most interesting from the standpoint of feasibility would be a protocol that relies only on linear transformations (see Subsec. A.2).

In the most general form of such a linear EPP (LEPP) Alice and Bob would start with n pairs of modes in an entangled Gaussian state standard form (cf. 67) and m ancillas in the vacuum state each. Then they both perform suitably chosen linear transformations, corresponding to symplectic maps S_A, S_B, respectively, and finally they both measure the x-quadrature on all but the first of their respective modes, resulting .

Note that this is indeed the most general form of a LEPP since (a) the standard form can be reached by local linear transformations (LLT); (b) all pure Gaussian ancilla states can be obtained from the vacuum by LLT, and mixed ancillas, being a mixture of pure Gaussian states, can be no better than pure ancillas; (c) all homodyne measurements can be realized by a x quadrature measurement preceded by some LLT; (d) that all measurements can be delayed until after the LLTs is seen as follows: prepare an ancilla in the state $|0\rangle$, the highly squeezed vacuum (31); coupling the mode to be measured to the ancilla by a continuous CNOT-gate [18] allows to effectively perform a QND-measurement of the quadrature of the mode by measuring the quadrature of the ancilla; but since the ancilla is not involved in the other LLTs of the EPP this measurement commutes with all other operations and can thus be delayed until the end.

From this we immediately see that such a linear EPP would be *deterministic*: Since the correlation matrix of the resulting state is independent of the measurement outcome, all the states produced by such a scheme have the same amount of entanglement. While this fact is in contrast with the protocols known for qubits and may make the existence of an LEPP seem unlikely, it does not rule out such a protocol (except the case $n = 1$). Many entangled beams would be used up in such a scheme, thus expected entanglement of the output may decrease even if one more strongly entangled beam is produced with certainty. Until now neither a LEPP has been found, nor a proof that there is none. We briefly mention some unsuccessful attempts to construct a LEPP in the appendix D.2.

4.4.2 Higher-order Nonlinearities

Thus we turn to higher-order nonlinearities to find an EPP for Gaussian states. One interesting approach based on the nonlinearities introduced by photon counting was proposed by Opatrný *et al.*[66]: Alice and Bob share a pure entangled Gaussian state (as the one used in [16]), both couple their respective mode to the vacuum via a low-reflectivity beam splitter and detect the photons that are "subtracted" by measuring the photon number in the reflected beams. If both measure the same small number the resulting (pure) state was shown to

be more entangled than the original one and to lead to a higher fidelity when used for teleportation. But it is not clear whether this scheme also works for mixed states or how it could be extended to this case.

Before turning to the proposal of [23], reprinted in Subsec. 4.5, which forms the main part of this section, let us discuss briefly which kind of nonlinearities would be needed to realize in a quantum optical setting the universal EPP for all Gaussian states [56, ch. II.8] which is based on the d-level protocol of [39].

As usual for EPPs Alice and Bob initially share a large number of identically prepared entangled systems in the known state ρ.

0a.) Concentration: If ρ describes more than two modes, both A and B perform a local linear transformation as described in [61] to concentrate the entanglement in the first of their modes such that all the others can be discarded. As shown in Subsec. A.2 this requires only linear optics and hence is within reach of today's technology. Therefore we have to consider only the case of ρ being a 1×1 Gaussian state in the following.

0b.) Symmetrization: If the state does not have zero mean, i.e. if $d \neq 0$ then perform a suitable displacement to achieve $d = 0$. If the state is not symmetric (see p. 90) symmetrize it as described in Subsec. 3.2, and then bring the symmetric state into standard form (see 67). 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.

These two steps have to be performed only once, while the following steps are iterated, representing the proper recurrence procedure.

For a state in symmetric standard form the filtering operation (91) required in the EPP is unnecessary, since then ρ already satisfies Ineq. (13) with the state $|\psi\rangle \propto \lim_{\lambda\to 1} \sum_k \lambda^k |k\rangle |k\rangle$ (in the photon number basis). This gives $a_{nm} = \lim_{\lambda\to 1} \lambda^{n+m}\delta_{nm}$, 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 $N_\alpha^{\text{tot}} = N_{\alpha 1} + N_{\alpha 2}, \alpha = A, B$ on both sides. Consider the state conditional on both A and B obtaining the same result N. It differs only by a local unitary transformation[2] (namely $|n, N-n\rangle_\alpha \mapsto |n, N\rangle_\alpha$) from the one that is obtained by directly following the d-level protocol of [39] sketched in Subsec. D.1, 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. 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 $(N_f+1)^2$, where N_f is the

[2] To be precise: local unitary 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 $N_\alpha \leq N$

last successful result of the total photon number measurement. Hence with finite probability one can get arbitrarily close to a maximally entangled state in some finite dimensional space provided the initial supply of states ρ is sufficiently large.

In the following two subsections the practical EPP that allows to distill certain mixed Gaussian states into pure maximally entangled states in one step is presented and its physical implementation using high finesse cavities and cross-Kerr nonlinearities is discussed.

4.5 Entanglement purification of Gaussian continuous variable quantum states

Lu-Ming Duan, Géza Giedke, J. Ignacio Cirac, and Peter Zoller,

We describe an entanglement purification protocol to generate maximally entangled states with high efficiencies from two-mode squeezed states or from mixed Gaussian continuous entangled states. The protocol relies on a local quantum non-demolition measurement of the total excitation number of several continuous variable entangled pairs. We propose an optical scheme to do this kind of measurement using cavity enhanced cross–Kerr interactions.

Phys. Rev. Lett. **84**, 4002 (2000), E-print: quant-ph/9912017.

Entanglement Purification of Gaussian Continuous Variable Quantum States

Lu-Ming Duan,[1,2,*] G. Giedke,[1] J. I. Cirac,[1] and P. Zoller[1]
[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*
(Received 3 December 1999)

We describe an entanglement purification protocol to generate maximally entangled states with high efficiencies from two-mode squeezed states or from mixed Gaussian continuous entangled states. The protocol relies on a local quantum nondemolition measurement of the total excitation number of several continuous variable entangled pairs. We propose an optical scheme to do this kind of measurement using cavity enhanced cross-Kerr interactions.

PACS numbers: 03.67.Hk, 03.65.Bz, 42.50.–p

Quantum communication, such as quantum key distribution and quantum teleportation, is hampered by the difficulty to generate maximally entangled states between distant nodes [1]. Because of loss and decoherence, in reality we can generate only partially entangled states between distant sides [2]. Entanglement purification techniques are needed to concentrate maximally entangled states from partially entangled states [3,4]. For qubit systems, efficient entanglement purification protocols have been found [3–5]. But none of these purification schemes have been realized experimentally due to the great difficulty of performing repeated collective operations in realistic quantum communication systems. Thus, it is of interest to consider purification of continuous variable entanglement. The nonlocal Gaussian continuous variable entangled states (i.e., states whose Wigner functions are Gaussians) can be easily generated by transmitting two-mode squeezed light, and this kind of entanglement has been demonstrated in the recent experiment of continuous variable teleportation [6]. As the first choice for performing continuous entanglement purification, one would consider direct extensions of the purification schemes for qubit systems. But until now, in these extensions, no entanglement increase has been found for Gaussian continuous entangled states [7]. Thus, the discussion should be extended to a larger class of operations to purify continuous entangled states. Braunstein *et al.* [8] have proposed a simple error correction scheme for continuous variables. However, it is not clear whether it can be used for purification. In [9] 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 this paper, we present an entanglement purification scheme with the following properties: (i) For pure states it reaches the maximal allowed efficiency in the asymptotic limit (when the number of pairs of modes goes to infinity). (ii) 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 a scheme to implement this protocol experimentally using high finesse cavities and cross-Kerr nonlinearities. Our purification protocol generates maximally entangled states in finite dimensional Hilbert spaces. The entanglement in the continuous partially entangled state is transformed to the maximally entangled state with a high efficiency. We begin the paper by describing the entanglement purification protocol for pure two-mode squeezed states, then extend the protocol to include mixed Gaussian continuous states, and last describe the physical implementation of the purification protocol.

First, assume that we have generated m entangled pairs A_i, B_i $(i = 1, 2, \ldots, m)$ between two distant sides A and B. Each pair of modes A_i, B_i are prepared in the two mode squeezed state $|\Psi\rangle_{A_iB_i}$, which in the number basis has the form

$$|\Psi\rangle_{A_iB_i} = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} \lambda^n |n\rangle_{A_i} |n\rangle_{B_i}, \qquad (1)$$

where $\lambda = \tanh(r)$, and r is the squeezing parameter [10]. For and only for a pure state, the entanglement is uniquely quantified by the von Neumann entropy of the reduced density operator of its one-component. The entanglement of the state (1) is thus given by $E(|\Psi\rangle_{A_iB_i}) = \cosh^2(r)\log[\cosh^2(r)] - \sinh^2(r)\log[\sinh^2(r)]$. The joint state $|\Psi\rangle_{(A_iB_i\})}$ of the m entangled pairs is simply the product of all the $|\Psi\rangle_{A_iB_i}$, which can be rewritten as

$$|\Psi\rangle_{(A_iB_i\})} = (1 - \lambda^2)^{m/2} \sum_{j=0}^{\infty} \lambda^j \sqrt{f_j^{(m)}}\, |\, j\rangle_{(A_iB_i\})}, \qquad (2)$$

where $(A_iB_i\}$ is an abbreviation of the symbol $A_1, B_1, A_2, B_2, \ldots,$ and A_m, B_m, and the normalized state $|\, j\rangle_{(A_iB_i\})}$ is defined as

$$|\, j\rangle_{(A_iB_i\})} = \frac{1}{\sqrt{f_j^{(m)}}} \sum_{i_1,i_2,\ldots,i_m}^{i_1+i_2+\cdots+i_m=j} |i_1, i_2, \ldots, i_m\rangle_{(A_i\})} \otimes |i_1, i_2, \ldots, i_m\rangle_{(B_i\})}. \qquad (3)$$

 0031-9007/00/84(17)/4002(4)$15.00 © 2000 The American Physical Society

The function $f_j^{(m)}$ in Eqs. (2) and (3) is given by $f_j^{(m)} = \frac{(j+m-1)!}{j!(m-1)!}$. To concentrate entanglement of these m entangled pairs, we perform a quantum nondemolition (QND) measurement of the total excitation number $n_{A_1} + n_{A_2} + \cdots + n_{A_m}$ on the A side (we will describe later how to implement this measurement experimentally). The QND measurement projects the state $|\Psi\rangle_{(A_iB_i\}}$ onto a two-party maximally entangled state $|\,j\rangle_{(A_iB_i\}}$ with probability $p_j = (1-\lambda^2)^m \lambda^{2j} f_j^{(m)}$. The entanglement of the outcome 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 getting a more entangled state is quite high. It can be easily proven that, if m goes to infinity, with unit probability we would get a maximally entangled state with entanglement $mE(|\Psi\rangle_{A_iB_i})$. This ensures that this method is optimal in this limit, analogous to the purification protocol presented in [3] for the qubit case. For any finite number of entangled pairs, the present purification protocol is more efficient than that in [3], 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 $|\,j\rangle_{(A_iB_i\}}$ does not necessarily exceed that of the original state $|\Psi\rangle_{A_iB_i}$ if j is small. It is also interesting to note that a small alternation of this scheme provides a useful method for preparing GHZ-like (Greenberger-Horne-Zeilinger) states in high dimensional Hilbert spaces [11]. The key point is that the modes B_i need not be at the same side in the protocol. Assume we have two entangled pairs B, A_1 and A_2, C distributed at three sides B, A, C, with each pair being prepared in the state (1). Then a local QND measurement of the modes A_1, A_2 at the A side with the outcome $j \neq 0$ generates a three-party GHZ state in the $(j+1)$-dimensional Hilbert space. Obviously, if we have m entangled pairs, we can generate a $(m+1)$-party GHZ state using this method.

In reality, the light transmission will be unavoidably subjected to loss, and then we will not start from an ideal two-mode squeezed state, but instead from a mixed state described by the following master equation:

$$\dot{\rho} = -i(H_{\rm eff}\rho - \rho H_{\rm eff}^{\dagger}) + \sum_{i=1}^{m} (\eta_A a_{A_i}\rho a_{A_i}^{\dagger} + \eta_B a_{B_i}\rho a_{B_i}^{\dagger}), \qquad (4)$$

where ρ is the density operator of the m entangled pairs with $\rho(0) = |\Psi\rangle_{(A_iB_i\}}\langle\Psi|$, the ideal two-mode squeezed state, and the effective Hamiltonian,

$$H_{\rm eff} = -i\sum_{i=1}^{m}\left(\frac{\eta_A}{2} a_{A_i}^{\dagger}a_{A_i} + \frac{\eta_B}{2} a_{B_i}^{\dagger}a_{B_i}\right). \qquad (5)$$

In Eqs. (4) and (5), 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 based on symmetry considerations, but η_A and η_B may be different to each other.

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. In the language of quantum trajectories [10], to the first order of $\eta_A\tau$ and $\eta_B\tau$, the final state of the m entangled pairs is either $|\Psi^{(0)}\rangle_{(A_iB_i\}} \propto e^{-iH_{\rm eff}\tau}|\Psi\rangle_{(A_iB_i\}}$, with no quantum jumps occurred, or $|\Psi^{(\alpha_i)}\rangle_{(A_iB_i\}} \propto \sqrt{\eta_\alpha\tau}\, a_{\alpha_i}|\Psi\rangle_{(A_iB_i\}}$, with a jump occurred in the α_i channel ($\alpha = A, B$ and $i = 1, 2, \ldots, m$). The final density operator is a mixture of all these possible states. To purify entanglement from the mixed state, we perform QND measurements of the total excitation number on both sides A and B, and the measurement results are denoted by j_A and j_B, respectively. We then compare j_A and j_B through classical communication, 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

$$P_A^{(j)}P_B^{(j)}|\Psi^{(0)}\rangle_{(A_iB_i\}} = |\,j\rangle_{(A_iB_i\}}, \quad P_A^{(j)}P_B^{(j)}|\Psi^{(\alpha_i)}\rangle_{(A_iB_i\}} = 0. \qquad (6)$$

So, if $j_A = j_B = j$, the outcome state is the maximally entangled state $|\,j\rangle_{(A_iB_i\}}$ with entanglement $\log(f_j^{(m)})$. The probability to get the state $|\,j\rangle_{(A_iB_i\}}$ 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 for occurrence of these kinds of quantum jumps is proportional to $m^2\overline{n}^2\eta_A\eta_B\tau^2$. So the condition for small transmission noise requires $m^2\overline{n}^2\eta_A\eta_B\tau^2 \ll 1$, where $\overline{n} = \sinh^2(r)$ is the mean photon for a single mode.

In the purification for mixed entanglement, we need classical communication (CC) to confirm that the measurement outcomes of the two 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 taken in all the entanglement purification schemes which need the help of repeated CCs [4,5]. If we also make this assumption for continuous variable systems, there exists another simple configuration for the purification protocol to work. We put the generation setup for two-mode squeezed states on the A side. 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 subjected 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 for sides A and B to subject to the same nonzero times of quantum jumps should be very small. This total probability is always smaller than $\overline{n}\eta_A\tau$, despite 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 $\overline{n}\eta_A\tau \ll 1$. The loss rate η_B can be large. The probability to get the maximally entangled state $|j\rangle_{\{A_i B_i\}}$ is still given by $p_j' = (1 - \lambda^2)^m \lambda^{2j} f_j^{(m)} e^{-(\eta_A+\eta_B)\tau j}$.

For continuous variable systems, the assumption of storage with a very small loss rate is typically unrealistic. If this is the case, then we can use the following simple method to circumvent the storage problem. Note that the purpose to distill maximally entangled states is to directly apply them in some quantum communication protocols, such as in quantum cryptography or in quantum teleportation. So we can modify the above purification protocol by the following procedure: right after the state generation, we take a QND measurement of the total excitation number on side A and get a measurement result j_A. Then we do not store the outcome state on side A, but immediately use it (e.g., perform the corresponding measurement as required by a quantum cryptography protocol [12]). During this process, the modes B_i are being sent to the distant side B and, when they arrive, we take another QND measurement of the total excitation number of the modes B_i and get an 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.

To experimentally implement the above purification scheme, we need first generate Gaussian continuous entangled states between two distant sides, and then perform a local QND measurement of the total excitation number of several entangled pairs. Here we propose a promising experimental scheme, which uses a high finesse optical cavity to carry continuous entangled states and cavity enhanced cross-Kerr interactions to realize the local QND measurement. It is possible to generate Gaussian continuous entangled states between two distant cavities [13]. We can transmit and then couple the two output lights of the nondegenerate optical parametric amplifier to distant high finesse cavities. The steady state of the cavities is just a Gaussian continuous entangled state described by the solution of Eq. (4) after taking into account the propagation loss [14]. 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. 1 to attain this goal. (For convenience, we use the two-cavity measurement as an example to illustrate the method. Extension of the measurement method to multicavity cases is straightforward.)

The measurement model depicted in Fig. 1 is an example of the cascaded quantum system [10]. 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 $\langle b_{i1}'^{\dagger}(t) b_{i1}'(t')\rangle = 0$ and $\langle b_{i1}'(t) b_{i1}'^{\dagger}(t')\rangle = \delta(t - t')$. 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 medium, and thus is negligible [15,16]. In the frame rotating at the optical frequencies, the Langevin equations describing the dynamics in the two ring cavities have the form

$$\begin{aligned} \dot{b}_1 &= -i\chi n_1 b_1 - \frac{\gamma}{2} b_1 - \sqrt{\gamma}\, b_{i1}' - g\gamma\,, \\ \dot{b}_2 &= -i\chi n_2 b_2 - \frac{\gamma}{2} b_2 - \sqrt{\gamma}\, b_{i2}\,, \end{aligned} \tag{7}$$

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 photon current over the measurement time T. Choosing the phase of

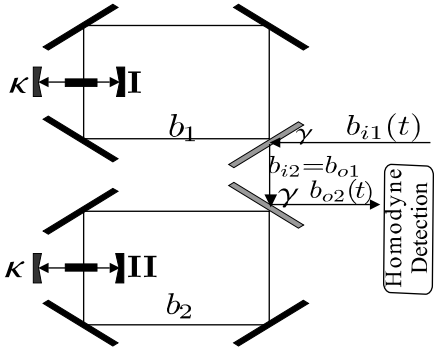

FIG. 1. Schematic experimental setup to measure the total photon number $n_1 + n_2$ contained in the cavities I and II. The cavities I and II, each with a small damping rate κ and with a cross-Kerr medium inside, are put, respectively, in a bigger ring cavity. The ring cavities with the damping rate γ are used to enhance the cross-Kerr interactions. A strong cotinuous 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.

the driving field so that $g = i|g|$, the measured observable corresponds to the operator

$$X_T = \frac{1}{T}\int_0^T \frac{1}{\sqrt{2}}[b_{o2}(t) + b_{o2}^{\dagger}(t)]\,dt \approx \frac{4\sqrt{2}\,|g|\chi}{\sqrt{\gamma}}(n_1 + n_2) + \frac{1}{\sqrt{T}}X_T^{(b)}, \qquad (8)$$

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 $b_T = 1/\sqrt{T}\int_0^T b_{i1}'(t)\,dt$. Equation (8) assumes $\gamma \gg \chi\langle n_i\rangle$ and $e^{-\gamma T} \ll 1$. There are two different contributions in Eq. (8). 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 $\delta n = \sqrt{\gamma}/(8|g|\chi\sqrt{T})$. 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

$$\frac{\gamma}{64|g|^2\chi^2} < T < \frac{1}{\kappa\langle n_i\rangle}. \qquad (9)$$

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 [15,16], the Kerr coefficient $\chi/2\pi \sim 0.1$ MHz would be obtainable [17]. We can choose the decay rates $\kappa/2\pi \sim 4$ MHz and $\gamma/2\pi \sim 100$ MHz, and let the dimensionless factor $g \sim 100$ (for a cavity with cross area $S \sim 0.5 \times 10^{-4}$ cm^2, $g \sim 100$ corresponds to a coherent driving light with intensity about 40 mW cm^{-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. (9) can be easily satisfied if we choose the measuring time $T \sim 8$ ns. More favorable values for the parameters are certainly possible.

To bring the above proposal into a real experiment, there are several imperfect effects which should be considered. These imperfections include phase instability of the driving field, imbalance between the two ring cavities, light absorption of the Kerr media 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 [18]. With the parameters given in the above paragraph, all these requirements can be met experimentally.

We thank P. Grangier and S. Parkins for discussions. This work was supported by the Austrian Science Foundation, by the European TMR network Quantum Information, and by the Institute for Quantum Information.

*Email address: luming.duan@uibk.ac.at

[1] C. H. Bennett, Phys. Today **48** No. 10, 24 (1995).
[2] J. I. Cirac *et al.*, Phys. Rev. Lett. **78**, 3221 (1997); S. J. Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998).
[3] C. H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996).
[4] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
[5] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).
[6] A. Furusawa *et al.*, Science **282**, 706 (1998).
[7] S. Parker, S. Bose, and M. B. Plenio, quant-ph/9906098.
[8] S. L. Braunstein, Nature (London) **394**, 47 (1998); Phys. Rev. Lett. **80**, 4084 (1998); S. Lloyd and J. J.-E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).
[9] T. Opatrny, G. Kurizki, and D.-G. Welsch, quant-ph/9907048.
[10] C. W. Gardiner and P. Zoller, *Quantum Noise* (Springer-Verlag, Berlin, 1999).
[11] D. Greenberger *et al.*, Am. J. Phys. **58**, 1131 (1990); J. W. Pan *et al.*, Nature (London) (to be published); G. M. D'Ariano *et al.*, quant-ph/9906067.
[12] M. Hillery, quant-ph/9909006.
[13] N. Ph. Georgiades *et al.*, Phys. Rev. Lett. **75**, 3426 (1995).
[14] A. S. Parkins and H. J. Kimble, quant-ph/9907049.
[15] A. Imamoglu *et al.*, Phys. Rev. Lett. **79**, 1467 (1997); **81**, 2836 (1998).
[16] L. V. Hau *et al.*, Nature (London) **397**, 594 (1999).
[17] In fact, Ref. [15] considered a configuration, yielding a Kerr coefficient $\chi \sim 100$ 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 $\chi/2\pi \sim 0.1$ MHz is obtainable. This value of the Kerr coefficient is large enough for performing the QND measurement.
[18] L. M. Duan *et al.* (to be published).

4.6 Physical implementation for entanglement purification of Gaussian continuous variable quantum states

Lu-Ming Duan, Géza Giedke, J. Ignacio Cirac, and Peter Zoller,

We give a detailed description of the entanglement purification protocol which generates maximally entangled states with high efficiencies from realistic Gaussian continuous variable entangled states. The physical implementation of this protocol is extensively analyzed using high finesse cavities and cavity enhanced cross Kerr nonlinearities. In particular, we take into account many imperfections in the experimental scheme and calculate their influences. Quantitative requirements are given for the relevant experimental parameters.

Phys. Rev. A **62**, 032304 (2000), E-print: quant-ph/0003116

Physical implementation for entanglement purification of Gaussian continuous-variable quantum states

Lu-Ming Duan,[1,2,*] G. Giedke,[1] J. I. Cirac,[1] and P. Zoller[1]
[1]*Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*
[2]*Department of Physics, University of Science and Technology of China, Hefei 230026, China*
(Received 6 March 2000; published 14 August 2000)

We give a detailed description of the entanglement purification protocol which generates maximally entangled states with high efficiencies from realistic Gaussian continuous variable entangled states. The physical implementation of this protocol is extensively analyzed using high finesse cavities and cavity enhanced cross Kerr nonlinearities. In particular, we take into account many imperfections in the experimental scheme and calculate their influences. Quantitative requirements are given for the relevant experimental parameters.

PACS number(s): 03.67.Hk, 42.50.−p, 03.65.Bz

I. INTRODUCTION

Quantum entanglement plays an essential role in many interesting quantum information protocols, such as in quantum key distribution and quantum teleportation [1]. To faithfully realize these protocols, first we need to generate a maximally entangled state. In reality, however, due to loss and decoherence, normally we can only generate partially entangled states between distant sides [2]. Entanglement purification is further needed which distills a maximally entangled state from several pairs of partially entangled states using local quantum operations and classical communications [3,4]. For qubit systems, efficient entanglement purification protocols have been found [4,5]. Recently, quantum information protocols have been extended from qubit systems to continuous variable systems, such as continuous variable teleportation [6,7], continuous variable computation [8], and error correction [9], continuous variable cryptography [10], and also the notions of continuous variable inseparability [11] and bound entanglement [12] have been investigated. For physical implementation, Gaussian continuous variable entangled states (i.e., states whose Wigner functions are Gaussians) can be generated experimentally by transmitting two-mode squeezed light, and this kind of entanglement has been demonstrated in the recent experiment of continuous variable teleportation [13]. Obviously, it is useful to consider purification of continuous variable entanglement, that is, to generate a desired more entangled state from some realistic continuous entangled states. We have recently proposed an efficient continuous variable entanglement purification protocol [14]. In this paper, we present the mathematical details of this purification protocol together with results on its physical implementation. In particular, we take into account many important imperfections in a realistic experimental setup, and calculate their influence on the purification scheme. Quantitative requirements are given for the relevant experimental parameters. These calculations make necessary preparations for a real experiment. We also show how to generate Gaussian continuous entangled states between two distant high finesse cavities, which is the first step for the physical implementation of the purification protocol.

It should be noted that with direct extensions of the purification protocols for qubit systems, it is possible to increase entanglement for a special class of less realistic continuous entangled states [15]. Unfortunately, with these direct extensions no entanglement increase has been found until now for realistic Gaussian continuous entangled states. In Ref. [16] 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 subtraction. For its practical realization, the efficiency, however, seems to be an issue. In contrast, the purification scheme discussed in this paper has the following favorable properties. (i) For pure states it reaches the maximal allowed efficiency in the asymptotic limit (when the number of pairs of modes goes to infinity). (ii) 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. (iii) An experimental scheme is possible for physical implementation of the purification protocol using high finesse cavities and cross Kerr nonlinearities.

The paper is arranged as follows. In Sec. II we show how to generate a Gaussian continuous entangled state between two distant cavities from the broadband squeezed light provided by a nondegenerate optical parametric amplifier (NOPA). Light transmission loss is taken into account. In Secs. III and IV we give a detailed description of the purification protocol. Section III shows how to generate a maximally entangled state from pure two-mode squeezed states based on a local quantum nondemolition (QND) measurement of the total photon number, and Sec. IV extends the purification protocol to include the mixed Gaussian continuous states which are evolved from the pure two-mode squeezed states due to the unavoidable light transmission loss. In Sec. V, we describe a cavity scheme to realize the local QND measurement of the total photon number, and deduce conditions for the QND measurement. Then, in Sec. VI, we extensively discuss many imperfections for a real experiment on QND measurements, and deduce quantitative requirements for the relevant experimental parameters. Last, we summarize the results, and give some typical parameter estimations.

*Email address: luming.duan@uibk.ac.at

 ©2000 The American Physical Society

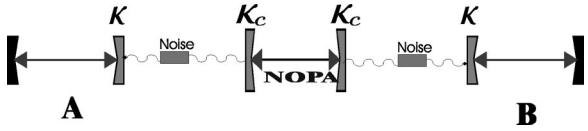

FIG. 1. Schematic setup for generating Gaussian continuous entangled states between two distant cavities.

II. GENERATION OF CONTINUOUS ENTANGLED STATES BETWEEN TWO DISTANT CAVITIES

Our source of entangled light field is taken to be a NOPA operating below threshold [17]. The light fields may be nondegenerate in polarization or in frequency. The two NOPA cavity modes c_A and c_B are assumed to have the same output coupling rate κ_c. The dynamic in the NOPA cavity is described by the Langevin equations (in the rotating frame) [18]

$$\dot{c}_A=\epsilon c_B^\dagger-\frac{\kappa_c}{2}c_A-\sqrt{\kappa_c}c_{iA},$$
$$\dot{c}_B^\dagger=\epsilon^* c_A-\frac{\kappa_c}{2}c_B^\dagger-\sqrt{\kappa_c}c_{iB}^\dagger, \tag{1}$$

where ϵ is the pumping rate with $|\epsilon|<\kappa_c/2$ (below threshold), and c_{iA} and c_{iB} are vacuum inputs. The NOPA outputs c_{oA} and c_{oB} are given, respectively, by $c_{o\alpha}=c_{i\alpha}+\sqrt{\kappa_c}c_\alpha$ $(\alpha=A,B)$. The two outputs, perhaps after a long distance propagation, are incident on distant high finesse cavities A and B. The cavities A and B are assumed to have the same damping rate κ with $\kappa\ll\kappa_c$. The schematic setup is shown by Fig. 1.

Under the condition $\kappa\ll\kappa_c$, the dynamics in the NOPA cavity is much faster than those in the cavities A and B, so we can assume a steady state for the NOPA outputs. The steady NOPA outputs are described by squeezed white noise operators with the following correlations [18]:

$$\langle c_{oA}(t)c_{oB}(t')\rangle=M\delta(t-t'),$$
$$\langle c_{o\alpha}^\dagger(t)c_{o\alpha}(t')\rangle=N\delta(t-t'),\quad(\alpha=A,B),$$
$$\langle c_{o\alpha}(t)c_{o\alpha}^\dagger(t')\rangle=(N+1)\delta(t-t'),\quad(\alpha=A,B), \tag{2}$$

where N and M, satisfying $M=\sqrt{N(N+1)}$, are determined by the NOPA coupling and pumping rates through $N=|\epsilon|^2\kappa_c^2/(\kappa_c^2/4-|\epsilon|^2)^2$ and $M=|\epsilon|\kappa_c(\kappa_c^2/4+|\epsilon|^2)/(\kappa_c^2/4-|\epsilon|^2)^2$.

To get the steady state of the cavities A and B, we note that their inputs a_{iA} and a_{iB} are, respectively, the NOPA outputs c_{oA} and c_{oB} with neglect of the losses during light propagation. The Langevin equations for the cavity modes a_A and a_B have the form

$$\dot{a}_\alpha=-\frac{\kappa}{2}a_\alpha-\sqrt{\kappa}a_{i\alpha}\quad(\alpha=A,B),$$

with the following solution:

$$a_\alpha(t)=a_\alpha(0)e^{-(\kappa/2)t}-\sqrt{\kappa}\int_0^t e^{-(\kappa/2)(t-t')}a_{i\alpha}(t')dt'. \tag{3}$$

When κt is considerably larger than 1, from Eqs. (2) and (3), it follows that

$$\langle a_A a_B\rangle=\sqrt{N(N+1)},$$
$$\langle a_\alpha^\dagger a_\alpha\rangle=N\quad(\alpha=A,B), \tag{4}$$
$$\langle a_\alpha a_\alpha^\dagger\rangle=(N+1)\quad(\alpha=A,B).$$

On the other hand, we know that two modes driven by a white noise are in Gaussian states at any time. A Gaussian state with the correlations (4) is necessarily a pure two-mode squeezed state. So the steady state of the cavity modes a_A and a_B is

$$|\Psi\rangle_{12}=S_{AB}(r)|\mathrm{vac}\rangle_{AB}, \tag{5}$$

where the squeezing operator $S_{AB}(r)=\exp[r(a_A^\dagger a_B^\dagger-a_A a_B)]$ and the squeezing parameter r is determined by $\coth(r)=\sqrt{N+1}$.

Next we include some important sources of noise in the state generation process. The noise includes the losses in the NOPA cavity and the light transmission loss from the NOPA cavity to the cavities A and B. With a small loss rate $\eta_0\ll\kappa_c$ for the modes c_A and c_B in the NOPA cavity, the Langevin equation (1) is replaced by

$$\dot{c}_A=\epsilon c_B^\dagger-\frac{\kappa_c+\eta_0}{2}c_A-\sqrt{\kappa_c}c_{iA}-\sqrt{\eta_0}v_{iA},$$
$$\dot{c}_B^\dagger=\epsilon^* c_A-\frac{\kappa_c+\eta_0}{2}c_B^\dagger-\sqrt{\kappa_c}c_{iB}^\dagger-\sqrt{\eta_0}v_{iB}^\dagger, \tag{6}$$

where v_{iA} and v_{iB} are standard vacuum white noise, and the NOPA outputs are still given by $c_{o\alpha}=c_{i\alpha}+\sqrt{\kappa_c}c_\alpha$ $(\alpha=A,B)$. On the other hand, the transmission loss of light can be described by

$$a_{i\alpha}=c_{o\alpha}\sqrt{e^{-\eta_\alpha\tau}}+v_\alpha\sqrt{1-e^{-\eta_\alpha\tau}}\quad(\alpha=A,B), \tag{7}$$

where τ is the transmission time, η_A and η_B are, respectively, the transmission loss rates for the outputs c_{oA} and c_{oB}, and v_A and v_B are standard vacuum white noise. From Eqs. (6) and (7), it follows that the inputs for the cavities A and B have the following correlations:

$$\langle a_{iA}(t)a_{iB}(t')\rangle=\sqrt{N'(N'+1)}e^{-\eta_A'+\eta_B'/2\tau}\delta(t-t'),$$
$$\langle a_{i\alpha}^\dagger(t)a_{i\alpha}(t')\rangle=N'e^{-\eta_\alpha'\tau}\delta(t-t')\quad(\alpha=A,B),$$
$$\langle a_{i\alpha}(t)a_{i\alpha}^\dagger(t')\rangle=(N'e^{-\eta_\alpha'\tau}+1)\delta(t-t')\quad(\alpha=A,B),$$

where the total loss rates $\eta_\alpha'=\eta_\alpha+(1/\tau)\ln(1+\eta_0/\kappa_c)=\eta_\alpha+\eta_0/(\kappa_c\tau)$ $(\alpha=A,B)$, and the parameter $N'=|\epsilon|^2(\kappa_c$

$+\eta_0)^2/[(\kappa_c+\eta_0)^2/4-|\epsilon|^2)^2 \approx N$. The steady state of the two cavity modes a_A and a_B is thus a Gaussian state with the nonzero correlations given by

$$\langle a_A a_B\rangle = \sqrt{N(N+1)}e^{-[(\eta'_A+\eta'_B)/2]\tau},$$

$$\langle a_\alpha^\dagger a_\alpha\rangle = Ne^{-\eta'_\alpha\tau} \quad (\alpha=A,B), \tag{8}$$

$$\langle a_\alpha a_\alpha^\dagger\rangle = (Ne^{-\eta'_\alpha\tau}+1) \quad (\alpha=A,B).$$

The Gaussian state is completely determined by these correlations. The Gaussian state (8) can be equivalently described as the solution at time $t=\tau$ of the following master equation:

$$\dot{\rho} = \eta'_A\left(a_A\rho a_A^\dagger - \frac{1}{2}a_A^\dagger a_{A1}\rho - \frac{1}{2}\rho a_A^\dagger a_A\right) + \eta'_B\left(a_B\rho a_B^\dagger - \frac{1}{2}a_B^\dagger a_B\rho - \frac{1}{2}\rho a_B^\dagger a_B\right) \tag{9}$$

with the initial state $\rho(0)=|\Psi\rangle_{AB}\langle\Psi|$, where $|\Psi\rangle_{AB}$ is defined by Eq. (5). This equivalence simplifies the physical picture in Sec. IV, where we will use the master equation (9) to describe the state generation noise.

III. ENTANGLEMENT CONCENTRATION OF PURE TWO-MODE SQUEEZED STATES

In the above, we have shown how to generate continuous partially entangled states between two distant cavities. In the case of no noise in the state generation process, the cavities are in a pure two-mode squeezed state. In this section, we will show how to concentrate continuous variable entanglement, that is, starting from several pairs of continuous entangled states, we want to get a state with more entanglement through only local operations. The section is divided into two parts. The first part describes the purification protocol for two entangled pairs, and the second part extends the protocol to include multiple pairs.

A. Concentration of two entangled pairs

Assume now we have two cavities A_1,A_2 and B_1,B_2 on each side. Each pair of cavities A_i,B_i $(i=1,2)$ are prepared in the state (5), which is now denoted by $|\Psi\rangle_{A_iB_i}$. $|\Psi\rangle_{A_iB_i}$, expressed in the number basis, has the form

$$|\Psi\rangle_{A_iB_i} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle_{A_i}|n\rangle_{B_i}, \tag{10}$$

where $\lambda=\tanh(r)$. Equation (10) is just the Schmidt decomposition of the state $|\Psi\rangle_{A_iB_i}$. For a pure state, the entanglement is uniquely quantified by the von Neumann entropy of the reduced density operator of its one-component. The entanglement of the state (10) is thus expressed as

$$E(|\Psi\rangle_{A_iB_i}) = \cosh^2 r\,\ln(\cosh^2 r) - \sinh^2 r\,\ln(\sinh^2 r). \tag{11}$$

The joint state of the two entangled pairs A_1,B_1 and A_2,B_2 is simply the product

$$|\Psi\rangle_{A_1B_1A_2B_2} = S_{A_1B_1}(r)|\mathrm{vac}\rangle_{A_1B_1}\otimes S_{A_2B_2}(r)|\mathrm{vac}\rangle_{A_2B_2} = (1-\lambda^2)\sum_{j=0}^{\infty}\lambda^j\sqrt{1+j}\,|j\rangle_{A_1A_2B_1B_2}, \tag{12}$$

where $|j\rangle_{A_1A_2B_1B_2}$ is defined as

$$|j\rangle_{A_1A_2B_1B_2} = \frac{1}{\sqrt{1+j}}\sum_{n=0}^{j}|n,j-n\rangle_{A_1A_2}|n,j-n\rangle_{B_1B_2}. \tag{13}$$

We now perform a local QND measurement of the total photon number of the two cavities A_1,A_2. There have been several proposals for doing QND measurements of the photon number, and in Sec. V, we will describe a cavity scheme for realizing the QND measurement of the total photon number of two local cavities. Here we simply assume this type of measurement can be done. After the QND measurement of the total number $n_{A_1}+n_{A_2}$, the state $|\Psi\rangle_{A_1B_1A_2B_2}$ is collapsed into $|j\rangle_{A_1A_2B_1B_2}$ with probability

$$p_j = (1-\lambda^2)^2\lambda^{2j}(j+1). \tag{14}$$

The state $|j\rangle_{A_1A_2B_1B_2}$ is a maximally entangled state between the two parties A_1,A_2 and B_1,B_2 in a $(j+1)\times(j+1)$-dimensional Hilbert space, and its entanglement is

$$E(|j\rangle_{A_1A_2B_1B_2}) = \ln(j+1). \tag{15}$$

If $E(|j\rangle_{A_1A_2B_1B_2}) > E(|\Psi\rangle_{A_iB_i})$, i.e.,

$$j > \frac{[\cosh(r)]^{\cosh(r)}}{[\sinh(r)]^{\sinh(r)}} - 1,$$

we get a two-party state with more entanglement. The quantity

$$\Gamma_j = \frac{E(|j\rangle_{A_1A_2B_1B_2})}{E(|\Psi\rangle_{A_iB_i})}$$

defines the entanglement increase ratio. Figure 2 shows the probability of success versus entanglement increase ratio for some typical values of the squeezing parameter.

An interesting feature of this entanglement purification protocol is that with 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 $|j\rangle_{A_1A_2B_1B_2}$ does not necessarily exceed that of the original state $|\Psi\rangle_{A_iB_i}$ if j is small. The state $|j\rangle_{A_1A_2B_1B_2}$ involves two pairs of cavities. If one wants to transfer the entanglement to a single pair of cavity modes, one can make a phase measurement of the cavity mode A_2. There have been some proposals for doing a phase measurement [19,20]. A phase measurement of the mode A_2 with the measurement outcome ϕ

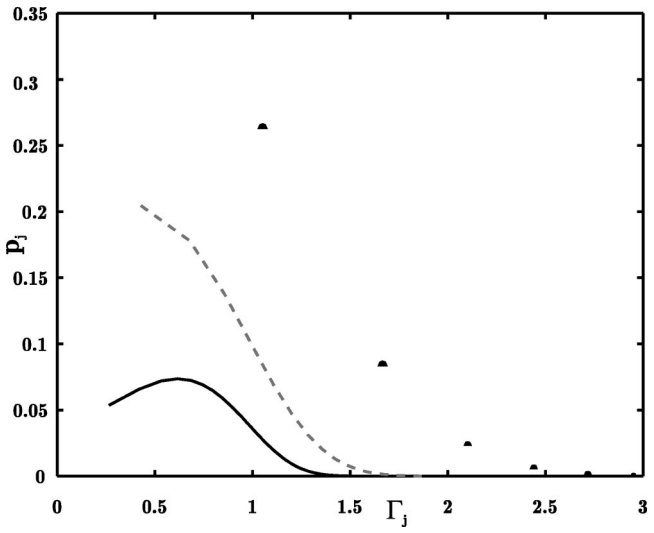

FIG. 2. The purification success probability versus entanglement increase ratio for two pairs. Dotted line for the squeezing parameter $r=0.5$, dashed line for $r=1.0$, and solid line for $r=1.5$.

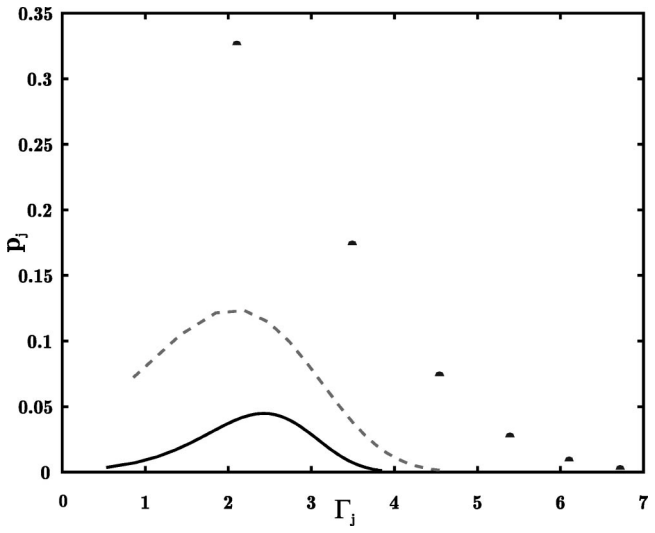

FIG. 3. The purification success probability versus entanglement increase ratio for the number of pairs $m=4$. The dotted line is for the squeezing parameter $r=0.5$, dashed line for $r=1.0$, and solid line for $r=1.5$.

will convert the state $|j\rangle_{A_1A_2B_1B_2}$ to the following maximally entangled state of a single pair of cavity modes:

$$|j\rangle_{A_1A_2}=\frac{1}{\sqrt{1+j}}\sum_{n=0}^{j}e^{i(j-n)\phi}|n\rangle_{A_1}|n\rangle_{B_1}. \tag{16}$$

B. Concentration of multiple entangled pairs

The above protocol can be extended straightforwardly to simultaneously concentrate entanglement of multiple cavity pairs. Simultaneous concentration of multiple entangled pairs is much more effective that the entanglement concentration two by two. Assume that we have m cavity pairs A_1,B_1, A_2,B_2, ..., and A_m,B_m. Each pair of cavities A_i,B_i is prepared in the state (10). The joint state of the m entangled pairs can be expressed as

$$\begin{aligned}|\Psi\rangle_{(A_iB_i\}}&=|\Psi\rangle_{A_1B_1}\otimes|\Psi\rangle_{A_2B_2}\otimes\cdots\otimes|\Psi\rangle_{A_mB_m}\\&=(1-\lambda^2)^{m/2}\sum_{j=0}^{\infty}\lambda^j\sqrt{f_j^{(m)}}|j\rangle_{(A_iB_i\}},\end{aligned} \tag{17}$$

where $(A_iB_i\}$ is abbreviation of A_1,B_1, $A_2,B_2,\ldots,A_m,B_m$, and the normalized state $|j\rangle_{(A_iB_i\}}$ is defined as

$$\begin{aligned}|j\rangle_{(A_iB_i\}}=\frac{1}{\sqrt{f_j^{(m)}}}&\sum_{\substack{i_1,i_2,\ldots,i_m\\ i_1+i_2+\ldots+i_m=j}}|i_1,i_2,\ldots,i_m\rangle_{(A_i\}}\\&\otimes|i_1,i_2,\ldots,i_m\rangle_{(B_i\}}.\end{aligned} \tag{18}$$

The function $f_j^{(m)}$ in Eqs. (17) and (18) is given by

$$f_j^{(m)}=\frac{(j+m-1)!}{j!(m-1)!}=\binom{j+m-1}{m-1}. \tag{19}$$

To concentrate the entanglement, we perform a QND measurement of the total photon number $n_{A_1}+n_{A_2}+\cdots+n_{A_m}$. This measurement projects the state $|\Psi\rangle_{(A_iB_i\}}$ onto a two-party maximally entangled state $|j\rangle_{(A_iB_i\}}$ with probability

$$p_j^{(m)}=(1-\lambda^2)^m\lambda^{2j}f_j^{(m)}. \tag{20}$$

The entanglement of the outcome state $|j\rangle_{(A_iB_i\}}$ is given by

$$E(|j\rangle_{(A_iB_i\}})=\ln(f_j^{(m)}). \tag{21}$$

Similarly, $\Gamma_j=E(|j\rangle_{(A_iB_i\}})/E(|\Psi\rangle_{A_iB_i})$ defines the entanglement increase ratio, and if $\Gamma_j>1$, we get a more entangled state. For four pairs, the probability of success versus entanglement increase ratio is shown in Fig. 3. There appears a peak in the probability curve for some entanglement increase ratio between 2 and 3.

To measure how efficient the scheme is, we define the entanglement transfer efficiency Υ with the expression

$$\Upsilon=\frac{\sum_{j=0}^{\infty}p_j^{(m)}E(|j\rangle_{(A_iB_i\}})}{mE(|\Psi\rangle_{A_iB_i})}. \tag{22}$$

It is the ratio of the average entanglement after concentration measurement to the initial total entanglement contained in the m pairs. Obviously, $\Upsilon\leqslant 1$ 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. 4.

From the 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 if m goes to infinity, with unit probability we would get a maximally entangled state with entanglement

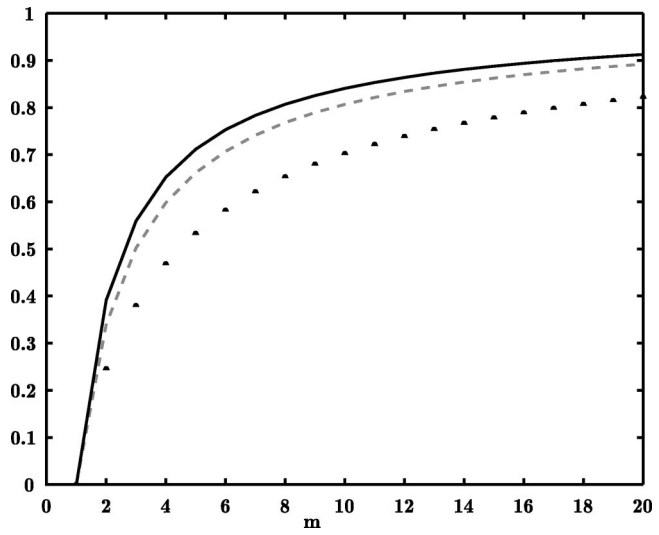

FIG. 4. The entanglement transfer efficiency versus the number of pairs m in simultaneous concentration. The dotted line is for $r=0.5$, dashed line for $r=1.0$, and solid line for $r=1.5$.

$mE(|\Psi\rangle_{A_iB_i})$. To show this, we calculate the mean value and the variance of the distribution $p_j^{(m)}$, and find

$$\bar{j}=\frac{m\lambda^2}{(1-\lambda^2)},$$
$$\overline{(\Delta j)^2}=\frac{m\lambda^2}{(1-\lambda^2)^2}. \tag{23}$$

The results show that if m tends to infinity, $\sqrt{\overline{(\Delta j)^2}}/\bar{j}\to 0$ 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 $|\bar{j}\rangle_{(A_iB_i\}}$ is

$$E(|\bar{j}\rangle_{(A_iB_i\}})\xrightarrow{m\to\infty} mE(|\Psi\rangle_{A_iB_i}), \tag{24}$$

so the entanglement transfer efficiency tends to unity. This proves that the purification method described above is optimal in the asymptotic limit ($m\to\infty$), analogous to the purification protocol presented in Ref. [4] for the qubit case. For any finite number of entangled pairs, this purification protocol is more efficient than that in Ref. [4], since it takes advantage of the special relations between the coefficients in the two-mode squeezed state.

IV. ENTANGLEMENT PURIFICATION OF MIXED GAUSSIAN CONTINUOUS ENTANGLED STATES

The assumption of noise-free preparation of partially continuous entangled states is not realistic. If we include the unavoidable light transmission loss and the NOPA cavity loss in the state generation process, in Section II we have shown that we would get a mixed Gaussian continuous entangled state between two distant cavities. The state is described by the solution at the transmission time τ of the master equation (9), with the ideal two-mode squeezed state (10) at the beginning. If we want to establish m entangled cavity pairs $A_1,B_1,A_2,B_2,\ldots$ and A_m,B_m, Eq. (9) can be extended directly to the following form

$$\dot{\rho}=-i(H_{\rm eff}\rho-\rho H_{\rm eff}^{\dagger})+\sum_{i=1}^{m}(\eta_A' a_{A_i}\rho a_{A_i}^{\dagger}+\eta_B' a_{B_i}\rho a_{B_i}^{\dagger}), \tag{25}$$

where ρ is the density operator of the whole m entangled pairs with $\rho(0)=|\Psi\rangle_{(A_iB_i\}}\langle\Psi|$, and the effective Hamiltonian

$$H_{\rm eff}=-i\sum_{i=1}^{m}\left(\frac{\eta_A'}{2}a_{A_i}^{\dagger}a_{A_i}+\frac{\eta_B'}{2}a_{B_i}^{\dagger}a_{B_i}\right). \tag{26}$$

In Eqs. (25) and (26), we assumed that the total loss rates η_A' and η_B' are the same for the m entangled pairs, but η_A' and η_B' may be different from each other. In this section, we will show how to distill entanglement from the kind of realistic continuous entangled states described by the solution of the master equation (25). There are two practical circumstances in which our entanglement purification protocol can be extended straightforwardly to generate maximally entangled states from the mixed Gaussian entangled states. We describe these two circumstances one by one.

A. Case of small state preparation noise

Though the state preparation noise is unavoidable, in many cases it is reasonable to assume that it is quite small. We take $\eta_A'\tau$ and $\eta_B'\tau$ as small factors, and solve the master equation (25) perturbatively to the first order of these small factors. It is convenient to use the quantum trajectory language to explain the perturbative solution. In this language, to the first order of $\eta_A'\tau$ and $\eta_B'\tau$, the final normalized state of the m entangled pairs is either (no jumps)

$$\begin{aligned}|\Psi^{(0)}\rangle_{(A_iB_i\}}&=\frac{1}{\sqrt{p^{(0)}}}e^{-iH_{\rm eff}\tau}|\Psi\rangle_{(A_iB_i\}}\\&=\frac{1}{\sqrt{p^{(0)}}}(1-\lambda^2)^{m/2}\sum_{j=0}^{\infty}\lambda^j e^{-[(\eta_A'+\eta_B')/2]\tau j}\\&\quad\times\sqrt{f_j^{(m)}}|j\rangle_{(A_iB_i\}},\end{aligned} \tag{27}$$

with probability

$$p^{(0)}=\frac{(1-\lambda^2)^m}{(1-\lambda^2 e^{-(\eta_A'+\eta_B')\tau})^m} \tag{28}$$

or (a jump occurred)

$$|\Psi^{(\alpha_i)}\rangle_{(A_iB_i\}}=\frac{1}{\sqrt{p^{(\alpha_i)}}}\sqrt{\eta_\alpha'\tau}\,a_{\alpha_i}|\Psi\rangle_{(A_iB_i\}},$$
$$(\alpha=A,B \text{ and } i=1,2,\ldots,m) \tag{29}$$

with probability

$$p^{(\alpha_i)} = \eta'_\alpha \tau_{(A_iB_i\}} \langle \Psi | a^\dagger_{\alpha_i} a_{\alpha_i} | \Psi \rangle_{(A_iB_i\}} = \bar{n}\, \eta'_\alpha \tau, \qquad (30)$$

where $\bar{n} = {}_{(A_iB_i\}}\langle \Psi | a^\dagger_{\alpha_i} a_{\alpha_i} | \Psi \rangle_{(A_iB_i\}} = \sinh^2(r)$ is the mean photon number for a single mode.

Similar to the pure state case, we also use QND measurements of the total photon number to distill entanglement from the mixed continuous state described by Eqs. (27)–(30). The difference is that now we perform QND measurements on both sides *A* and *B*. The measurement results are denoted by j_A and j_B, respectively. We then compare j_A and j_B through classical communication, and keep the outcome state if and only if $j_A = j_B$. It is easy to show that the final state is a maximally entangled state in a finite dimensional Hilbert space. Let $P_A^{(j)}$ and $P_B^{(j)}$ denote the projections onto the eigenspace of the corresponding total number operator $\Sigma_{i=1}^m$ and $\Sigma_{i=1}^m a^\dagger_{B_i} a_{B_i}$ with eigenvalue *j*, respectively. From Eqs. (27) and (29), it follows

$$P_A^{(j)} P_B^{(j)} |\Psi^{(0)}\rangle_{(A_iB_i\}} = |j\rangle_{(A_iB_i\}},$$

$$P_A^{(j)} P_B^{(j)} |\Psi^{(\alpha_i)}\rangle_{(A_iB_i\}} = 0, \quad (\alpha = A,B \text{ and } i = 1,2,\ldots,m). \qquad (31)$$

So if $j_A = j_B$, the outcome state is maximally entangled with entanglement $\ln(f_j^{(m)})$. The components (29) in the mixed density operator, which are not maximally entangled, are discarded through confirmation of the two-side measurement outcomes. Compared with the pure state case, the probability to get the entangled state $|j\rangle_{(A_iB_i\}}$ is now decreased to

$$p'_j = (1-\lambda^2)^m \lambda^{2j} f_j^{(m)} e^{-(\eta'_A + \eta'_B)\tau j}. \qquad (32)$$

We also note that the projection operators $P_A^{(j)} P_B^{(j)}$ cannot eliminate the state obtained from the initial state $|\Psi\rangle_{(A_iB_i\}}$ by a quantum jump on both sides *A* and *B*. The total probability for this kind of quantum jumps to occur is proportional to $m^2 \overline{n^2} \eta'_A \eta'_B \tau^2$. So the condition for small state preparation noise in fact requires

$$m^2 \overline{n^2} (\eta_A \tau + \eta_0/\kappa_c)(\eta_B \tau + \eta_0/\kappa_c) \ll 1. \qquad (33)$$

If the light transmission loss is the dominant noise, Eq. (33) reduces to $m^2 \overline{n^2} \eta_A \eta_B \tau^2 \ll 1$.

B. Case of asymmetric state preparation noise

In the above purification protocol, we need classical communication (CC) to confirm that the measurement outcomes of the two sides are the same, and during this CC, we implicitly assume that the storage noise for the cavity modes is negligible. In fact, that the storage noise during CC is much smaller than the transmission noise is a common assumption made in all the entanglement purification schemes which need the help of repeated CCs [3,5]. If we also make this assumption for continuous variable systems, there exists a simple purification protocol to generate maximally entangled states. We put the NOPA setup on the *A* side. After creation of ideal squeezed vacuum lights, we directly couple one output light of the NOPA to the cavity on side *A* without noisy propagation; and the other output of the NOPA is sent to the remote side *B*, through a long distance noisy transmission. This configuration of the setup is equivalent to setting the transmission loss rate $\eta_A \approx 0$ so that $\eta'_A \approx \eta_0/(\kappa_c \tau)$. Note that the NOPA cavity loss rate η_0 is normally much smaller than the output coupling rate κ_c, so the total loss rate η'_A can be much smaller than η'_B in this case. The purification protocol now is exactly the same as that described in the previous case. We note that the component of the mixed density operator which is kept the projection $P_A^{(j)} P_B^{(j)}$ should subject to the same times of quantum jumps on each side *A* and *B*. We want this component is a maximally entangled state. This requires that the total probability for *A* and *B* to be subjected to the same nonzero number of quantum jumps should be very small. From Eq. (30), this total probability is always smaller than $m\bar{n}\eta'_A \tau$, no matter how large the transmission loss $\eta_B \tau$ is. So the working condition of the protocol in the asymmetric transmission noise case is

$$m\bar{n}\eta_0/\kappa_c \ll 1. \qquad (34)$$

The transmission loss $\eta_B \tau$ can be above one. The probability of success for obtaining the maximally entangled state $|j\rangle_{(A_iB_i\}}$ is also given by Eq. (32).

Before concluding this section, we remark that for continuous variable systems, the information carrier is normally light, and the assumption of storage with a very small loss rate is typically unrealistic. It is interesting to note that recently there have been proposals to store light in internal states of an atomic ensemble [21,22]. If this turns out to be possible, the storage time for light can be greatly increased. Anyway, as was pointed out in Ref. [14], this purification method is in fact not essentially hampered by the difficulty to store light, since there is a simple posterior confirmation method to circumvent the storage problem. Note that the purpose to distill maximally entangled states is to directly apply them in some quantum communication protocol, such as in quantum cryptography or in quantum teleportation. So we can modify the above purification protocol by the following procedure: right after the cavity *A* attains its steady state, we make a QND measurement of the total excitation number on side *A* and get a measurement result j_A. Then we do not store the outcome state on side *A*, but immediately use it (e.g., perform the corresponding measurement as required by a quantum cryptography protocol). 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 total excitation number 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.

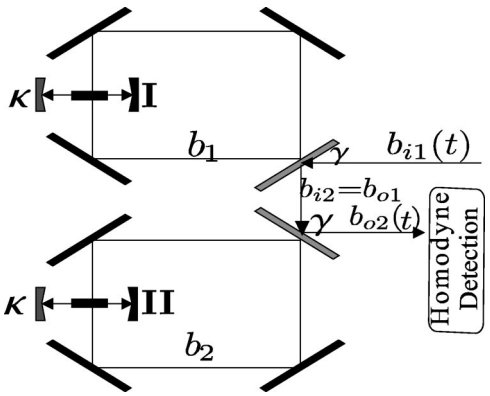

FIG. 5. Schematic experimental setup to measure the total photon number n_1+n_2 contained in cavities I and II.

V. QND MEASUREMENTS OF THE TOTAL PHOTON NUMBER OF SEVERAL CAVITIES

The QND measurement of the total photon number plays a critical role in our entanglement purification protocol. There have been some proposals for making a QND measurement of the photon number in a single cavity [23–25], such as letting some atoms pass through the cavity, and measuring the internal or external degrees of freedom of the atoms [23]. In this section, we propose a purely optical scheme for making a QND measurement of the total photon number contained in several cavities. The different optical modes interact with each other through cross phase modulation induced by a Kerr medium, and we use cavities to enhance this kind of interaction. As an illustrative example, in the following we will show how to measure the total photon number of two cavities. Extension of this scheme to include several cavities is straightforward.

The schematic setup is depicted in Fig. 5. We want to make a QND measurement of the total photon number n_1+n_2 contained in the good cavities I and II, whose damping rate κ is assumed to be very small. The cavities I and II, each with a Kerr type medium inside, are put respectively in a bigger ring cavity. The two ring cavities are assumed to damp at the same rate γ, and $\gamma \gg \kappa$. A strong coherent light b_{i1} is incident on the first ring cavity, whose output b_{o1} is directed to the second ring cavity. The output b_{o2} of the second ring cavity is continuously observed through homodyne detection, and we will show that under some realistic conditions, this detection gives a QND measurement of the total photon number operator $n_1+n_2=a_1^\dagger a_1+a_2^\dagger a_2$.

The measurement model depicted in Fig. 5 is an example of a cascaded quantum system [18].The incident light b_{i1} can be expressed as

$$b_{i1}=b'_{i1}+g\sqrt{\gamma}, \tag{35}$$

where $g\sqrt{\gamma}$ is a constant driving field, and b'_{i1} is the standard vacuum white noise, satisfying

$$\langle b'^{\dagger}_{i1}(t)b'_{i1}(t')\rangle=0,$$
$$\langle b'_{i1}(t)b'^{\dagger}_{i1}(t')\rangle=\delta(t-t'). \tag{36}$$

The Hamiltonian for the Kerr medium is assumed to be

$$H_i=\hbar\chi n_i b_i^\dagger b_i \quad (i=1,2), \tag{37}$$

where b_1 and b_2 are the annihilation operators for the ring cavity modes, and χ is the cross-phase modulation coefficient. The self-phase modulation effects will be discussed in the next section and shown to be negligible under some realistic conditions. In the rotating frame, the Langevin equations describing the dynamics in the two ring cavities have the form

$$\dot{b}_1=-i\chi n_1 b_1-\frac{\gamma}{2}b_1-\sqrt{\gamma}b'_{i1}-g\gamma,$$
$$\dot{b}_2=-i\chi n_2 b_2-\frac{\gamma}{2}b_2-\sqrt{\gamma}b_{i2}. \tag{38}$$

The boundary conditions for the two ring cavities are described by

$$b_{i2}=b_{o1}=b'_{i1}+g\sqrt{\gamma}+\sqrt{\gamma}b_1,$$
$$b_{o2}=b_{i2}+\sqrt{\gamma}b_2. \tag{39}$$

Assume $\gamma \gg \chi\langle n_i\rangle$ $(i=1,2)$, and we take adiabatic elimination, i.e., let $\dot{b}_1=\dot{b}_2=0$ in Eq. (38), obtaining

$$b_1\approx\frac{-2(g\gamma+\sqrt{\gamma}b'_{i1})}{\gamma}\left(1-\frac{2i\chi n_1}{\gamma}\right),$$
$$b_2\approx\frac{2(g\gamma+\sqrt{\gamma}b'_{i1})}{\gamma}\left(1-\frac{4i\chi n_1}{\gamma}-\frac{2i\chi n_2}{\gamma}\right). \tag{40}$$

Substituting the above result into Eq. (39), the final output field b_{o2} is expressed as

$$b_{o2}\approx-\frac{4ig\chi}{\sqrt{\gamma}}(n_1+n_2)+b'_{i1}+g\sqrt{\gamma}. \tag{41}$$

Now we measure the X component of the quadrature phase amplitudes of the output field b_{o2} through a homodyne detection. The phase of the driving field g is set according to $g=i|g|$. Suppose T is the measuring time. What we really get is the integrated photon current over time T, which, divided by T, corresponds to the following measuring operator:

$$X_T=\frac{1}{T}\int_0^T\frac{1}{\sqrt{2}}[b_{o2}(t)+b_{o2}^\dagger(t)]dt$$
$$\approx\frac{4\sqrt{2}|g|\chi}{\sqrt{\gamma}}(n_1+n_2)+\frac{1}{\sqrt{T}}X_T^{(b)}, \tag{42}$$

where $X_T^{(b)}=(1/\sqrt{2})(b_T+b_T^\dagger)$, and b_T, satisfying $[b_T,b_T^\dagger]=1$, is defined by

$$b_T=\frac{1}{\sqrt{T}}\int_0^T b'_{i1}(t)dt. \tag{43}$$

From Eq. (36), it follows that the defined mode b_T is in a vacuum state. So the first term of the right hand side of Eq. (42) represents the signal which is proportional to n_1+n_2, and the second term represents the contribution of the vacuum noise. The distinguishability of this measurement is given by

$$\delta n = \frac{\sqrt{\gamma}}{8|g|\chi\sqrt{T}}. \tag{44}$$

If $\delta n < 1$, i.e., if the measuring time

$$T > \frac{\gamma}{64|g|^2\chi^2}, \tag{45}$$

we perform an effective measurement of the total number operator n_1+n_2. During the measuring time T, the loss of the two cavities I and II should be negligible, which requires

$$\kappa\langle n_i\rangle T < 1 \quad (i=1,2). \tag{46}$$

Under this condition, n_1+n_2 is approximately a conserved observable, and we realize a QND measurement of the total photon number operator. The measurement projects the field in the cavities I and II to one of the eigenstates of n_1+n_2. Equations (45) and (46), combined together, determine the suitable choice for the measuring time.

VI. INFLUENCE OF IMPERFECTIONS IN THE QND MEASUREMENT

We have shown how to perform a QND measurement of the total photon number. The scheme described above works under ideal conditions. For a real experiment, there are always many imperfections which should be considered. For example, the phase of the driving field may be unstable, and has a small variance; the damping rates and the cross phase modulation coefficients for different ring cavities may not be exactly the same; the Kerr media and the mirrors may absorb some light; self-phase modulation effects caused by the Kerr media may have some influence on the resulting state; there may be some loss of light from the first ring cavity to the second ring cavity; the efficiency of the detector is not unity. Of course, to realize a QND measurement of the total photon number, all the imperfections must be small. But the important question is how small these imperfections should be. In this section, we will deduce quantitative requirements for all the imperfections listed above. These calculations may be helpful for a future real experiment. We will consider these imperfections one by one.

A. Phase instability of the driving field

Assume that the phase of the driving field $g\sqrt{\gamma}$ has a small variance δ, i.e., g is expressed as $g=i|g|e^{i\delta}$. Then, Eq. (42) is replaced by

$$X_T \approx \frac{4\sqrt{2}|g|\chi}{\sqrt{\gamma}}(n_1+n_2) + \frac{1}{\sqrt{T}}X_T^{(b)} - \sqrt{2}|g|\delta\sqrt{\gamma}. \tag{47}$$

The last term of Eq. (47) represents the noise due to the phase instability of the driving field. It should be negligible compared with the signal, which requires

$$\delta < \frac{4\chi}{\gamma}. \tag{48}$$

On the other hand, we know that the squared phase variance δ^2 increases linearly with time, i.e., $\delta^2=\delta_t t$, where δ_t is the increasing rate. The measuring time T is bounded from below by Eq. (45), so the increasing rate of the phase instability of the driving field is required to satisfy

$$\delta_t < \frac{1024|g|^2\chi^4}{\gamma^3}. \tag{49}$$

Equation (49) suggests it is easier to meet the requirement imposed by the phase instability with a strong driving field and a large cross phase modulation coefficient.

B. Imbalance between the ring cavities

In the previous section, we assumed that the damping rates and the cross phase modulation coefficients are exactly the same for the two ring cavities. This may be impossible in a real experiment. Here we calculate the largest allowed imbalance between the two ring cavities. The damping rates and the cross phase modulation coefficients for the ring cavities are denoted by γ_1, γ_2, and χ_1, χ_2, respectively. The Langevin equations (38) and the boundary conditions (39) are replaced respectively by the following equations

$$\dot{b}_1 = -i\chi_1 n_1 b_1 - \frac{\gamma_1}{2}b_1 - \sqrt{\gamma_1}b'_{i1} - g\gamma_1,$$
$$\dot{b}_2 = -i\chi_2 n_2 b_2 - \frac{\gamma_2}{2}b_2 - \sqrt{\gamma_2}b_{i2}, \tag{50}$$

$$b_{i2} = b_{o1} = b'_{i1} + g\sqrt{\gamma_1} + \sqrt{\gamma_1}b_1,$$
$$b_{o2} = b_{i2} + \sqrt{\gamma_2}b_2. \tag{51}$$

The final measured observable is expressed as

$$X_T \approx \frac{4\sqrt{2}|g|\chi_1}{\sqrt{\gamma_1}}(n_1+n_2) + \frac{1}{\sqrt{T}}X_T^{(b)} + 4\sqrt{2}|g|\sqrt{\gamma_1}\left(\frac{\chi_2}{\gamma_2}-\frac{\chi_1}{\gamma_1}\right)n_2, \tag{52}$$

The last term of Eq. (52) represents the noise due to the unbalance between the ring cavities, which should be negligible compared with the signal, yielding

$$\left|\frac{\chi_2\gamma_1}{\chi_1\gamma_2}-1\right|<\frac{1}{\langle n_2\rangle}. \tag{53}$$

C. Absorption and leakage of the light

Light absorption by mirrors and Kerr media and light leakage through other mirrors of the ring cavities can be described by the same Langevin equation, which has the form

$$\dot{b}_1=-i\chi n_1 b_1-\frac{\gamma}{2}b_1-\sqrt{\gamma}b'_{i1}-g\gamma-\frac{\beta_1}{2}b_1-\sqrt{\beta_1}c_{i1},$$
$$\dot{b}_2=-i\chi n_2 b_2-\frac{\gamma}{2}b_2-\sqrt{\gamma}b_{i2}-\frac{\beta_2}{2}b_2-\sqrt{\beta_2}c_{i2}, \tag{54}$$

where β_1 and β_2 are the light leakage (or absorption) rates of the first and second ring cavities, respectively, and c_{i1} and c_{i2} are the standard vacuum inputs. The boundary conditions for the ring cavities are still described by Eq. (39). The leaked (or absorbed) light fields c_{o1} and c_{o2} are expressed as

$$c_{o\alpha}=c_{i\alpha}+\sqrt{\beta_\alpha}b_\alpha \quad (\alpha=1,2). \tag{55}$$

The leakage (or absorption) of light may have two types of effects: First, it may destroy the balance between the two ring cavities; and second, the leaked light (55) may carry some information about n_1 (or n_2). Any information about n_1 (or n_2) will destroy the superposition of the different eigenstates of n_1 (or n_2), and thus lead to decoherence of the eigenstate of n_1+n_2 [note that a eigenstate of n_1+n_2 is normally a superposition of the different eigenstates of n_1 (or n_2)]. So we require that the information about n_1 (or n_2) carried by the leaked light should be completely masked by the vacuum noise. This is equivalent to require that the decoherence of the eigenstate of n_1+n_2 caused by the light leakage is negligible. To consider the first effect of the light leakage, we calculate the measured observable X_T, and find it has the form

$$X_T\approx\frac{4\sqrt{2}|g|\chi}{\sqrt{\gamma}}(n_1+n_2)+\frac{1}{\sqrt{T}}X_T^{(b)}+\frac{4\sqrt{2}|g|\chi}{\sqrt{\gamma}}\left(\frac{\beta_2^2}{\gamma^2}-\frac{\beta_1^2}{\gamma^2}\right)n_2. \tag{56}$$

The last term of Eq. (56) should be negligible compared with the signal, which requires

$$|\beta_2^2-\beta_1^2|<\frac{\gamma^2}{\langle n_2\rangle}. \tag{57}$$

To consider the decoherence effect of the light leakage, we define a similar measuring operator $X_T^{(\alpha)}$ for the leaked light (55)

$$X_T^{(\alpha)}=\frac{1}{T}\int_0^T\frac{1}{\sqrt{2}}[c_{o\alpha}(t)+c_{o\alpha}^\dagger(t)]dt \approx\frac{8\sqrt{2}|g|\chi\sqrt{\beta_\alpha}(\alpha-1)}{\gamma}(n_1+n_2)+\frac{1}{\sqrt{T}}X_T^{(c_\alpha)}-\frac{4\sqrt{2}|g|\chi\sqrt{\beta_\alpha}}{\gamma}n_\alpha \quad (\alpha=1,2), \tag{58}$$

where $X_T^{(c_\alpha)}$, similar to $X_T^{(b)}$ defined below Eq. (42), are standard vacuum noise terms. The last term of Eq. (58) bears some information about n_α, which should be completely masked by the vacuum noise term to make the decoherence effect negligible. This condition requires

$$\frac{4\sqrt{2}|g|\chi\langle n_\alpha\rangle}{\gamma}\sqrt{\beta_\alpha}<\frac{1}{\sqrt{2T}}. \tag{59}$$

On the other hand, the measuring time T is bounded from below by Eq. (45), which, combined with Eq. (59), yields the following requirement for the leakage rates

$$\beta_\alpha<\frac{\gamma}{\langle n_\alpha\rangle^2} \quad (\alpha=1,2). \tag{60}$$

Obviously, this is a much stronger requirement than that given by Eq. (57).

We should mention that there is another kind of absorption by the Kerr medium, the absorption rate of which is proportional to the cavity photon number n_α. This kind of absorption, usually termed two-photon absorption, cannot be described by Eq. (54). To incorporate the two-photon absorption, we add an imaginary part to the cross phase modulation coefficient χ, i.e., χ is replaced by $\chi+i\chi_i$, where χ_i describes the two-photon absorption rate. The two-photon absorption should be negligible compared with the cross Kerr interaction, which requires $\chi_i<\chi/\langle n_\alpha\rangle$ $(\alpha=1,2)$.

D. Self-phase-modulation effects

Normally, a Kerr medium also induces self-phase-modulation effects. However, by a suitable choice of the resonance condition for the Kerr medium, the self-phase-modulation effects can be made much smaller than the cross-phase modulation [26], then the self-phase-modulation interaction is basically negligible. Here, for completeness, we still calculate the influence of self-phase modulations. In fact, self-phase modulation of the ring cavity modes have no influence on the QND measurement. This modulation adds a term similar to $-i\chi_s b_i^\dagger b_i b_i$ $(i=1,2)$ in the Langevin equation (38), where χ_s denotes the self-phase modulation coefficient for the ring cavity modes. We know that the ring cavity modes b_1 and b_2 are in steady states under adiabatic elimination, and to a good approximation $b_i^\dagger b_i$ can be replaced by $\langle b_i^\dagger b_i\rangle=4|g|^2$. So the term $-i\chi_s b_i^\dagger b_i b_i$ simply

induces a constant phase shift for the output field b_{o2}, and it can be easily compensated by choosing the initial phase of the driving field g.

Self-phase modulation of the cavity modes a_1 and a_2 plays a more subtle role. First, it obviously has no influence on the QND measurement of n_1+n_2, but it influences the resulting state after the QND measurement. In the purification scheme for two entangled pairs (described in Sec. III A), if there is no self-phase modulation, the state after the QND measurement is given by Eq. (13); and if the self-phase modulation of the modes a_1 and a_2 is considered, the modulation Hamiltonian $\hbar\chi_s' n_i^2$ $(i=1,2)$, in which χ_s' is the corresponding self-phase-modulation coefficient, will bring the resulting state into

$$|j\rangle'_{A_1A_2B_1B_2}=\frac{1}{\sqrt{1+j}}\sum_{n=0}^{j} e^{i\chi_s' t[n^2+(j-n)^2]} \times|n,j-n\rangle_{A_1A_2}|n,j-n\rangle_{B_1B_2}, \tag{61}$$

where t is the interaction time for the self phase modulation. It is important to note that the state (61) is still a maximally entangled state with entanglement $\log(j+1)$. In this sense, self-phase modulation effects have no influence on the entanglement purification, though the resulting state is changed.

E. Imperfect coupling from the first ring cavity to the second ring cavity

If the coupling between the two ring cavities is not perfect, the relation $b_{i2}=b_{o1}$ is not valid any more, and should be replaced by

$$b_{i2}=\sqrt{\mu}b_{o1}+\sqrt{1-\mu}d_i,$$
$$d_o=\sqrt{\mu}d_i+\sqrt{1-\mu}b_{o1}, \tag{62}$$

where d_i is the standard vacuum white noise, and d_o represents the leaked light in the imperfect coupling. The quantity μ describes the coupling efficiency. This kind of imperfection is very similar to the light leakage (or absorption) described in Sec. VI C. The difference is that the imperfect coupling (62) does not cause any unbalance between the two ring cavities. The only restriction is that the decoherence effect induced by it should be negligible, which requires

$$\mu>1-\frac{1}{\langle n_1\rangle^2}. \tag{63}$$

Equation (63) suggests that loss of light from the first to the second ring cavity should be very small.

F. Detector inefficiency

The detector efficiency of course cannot attain 1. For a detector with efficiency ν, the real measured field b'_{o2} has the following relation with the output of the second ring cavity:

$$b'_{o2}=\sqrt{\nu}b_{o2}+\sqrt{1-\nu}e_i, \tag{64}$$

where e_i is the standard vacuum white noise. This imperfection is similar to the imperfect coupling considered in the previous subsection. But now the leaked light depends only on the operator sum n_1+n_2, and carries no information about the single cavity photon number n_1, so it does not induce any decoherence. The only role played by the detector inefficiency is that it decreases the signal by a factor $\sqrt{\nu}$, so Eq. (45) on the restriction of the measuring time is now replaced by

$$T>\frac{\gamma}{64\nu|g|^2\chi^2}. \tag{65}$$

Obviously, the detector inefficiency has no important influence on this QND measurement scheme.

TABLE I. List of requirements for the QND measurement.

Measuring time	$\frac{\gamma}{64\|g\|^2\chi^2}<T<\frac{1}{\kappa\langle n_i\rangle}$
Phase instability	$\delta<\frac{4\chi}{\gamma}$ or $\delta_t<\frac{1024\|g\|^2\chi^4}{\gamma^3}$
Cavity imbalance	$\left\|\frac{\chi_2\gamma_1}{\chi_1\gamma_2}-1\right\|<\frac{1}{\langle n_2\rangle}$
Absorption (leakage) rate	$\beta_\alpha<\frac{\gamma}{\langle n_\alpha\rangle^2}$, $(\alpha=1,2)$
Coupling efficiency	$\mu>1-\frac{1}{\langle n_1\rangle^2}$
Detector efficiency	$\nu>\frac{\gamma}{64\|g\|^2\chi^2T}$

VII. SUMMARY AND DISCUSSION

In summary, we have given a detailed description of the purification protocol which generates maximally entangled states in a finite dimensional Hilbert space from two-mode squeezed states or from realistic Gaussian continuous entangled states. The nonlocal Gaussian continuous entangled states are generated by feeding two distant cavities with the outputs of the NOPA. The purification operation is based on a local QND measurement of the total photon number contained in several cavities. We have extensively analyzed a cavity scheme to do this QND measurement, and have deduced its working condition. Furthermore, we have discussed many imperfections existing in a real experiment, and deduced quantitative requirements for the relevant experimental parameters. In Table I, we summarize the working conditions for the collective QND measurement, including the requirements for many types of imperfections.

To realize the QND measurement, basically we need high finesse optical cavities and strong cross Kerr interaction media. A good example for the strong cross Kerr interaction is

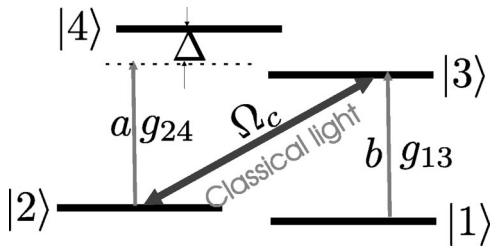

FIG. 6. Level structure of the atoms.

provided by the resonantly enhanced Kerr nonlinearity, which has been predicted theoretically [26,27] and demonstrated in recent experiments [28]. In those works, the Kerr medium is a low density cold trapped atomic gas, whose relevant energy level structure is represented by the four-state diagram shown in Fig. 6 with $|1\rangle$ being the ground state. The ring cavity mode b_i with frequency ω_b is assumed to be resonant with the $|1\rangle \rightarrow |3\rangle$ transition, and the cavity mode a_i with frequency ω_a (ω_a is quite different from ω_b) is coupled to the $|2\rangle \rightarrow |4\rangle$ transition, but with a large detuning Δ_{42}. A nonperturbative classical coupling field with frequency ω_c resonant with the $|2\rangle \rightarrow |3\rangle$ transition creates an electromagnetically induced transparency (EIT) for the cavity fields a_i and b_i. In this configuration, the one-photon absorption of the medium is eliminated due to quantum interference, and the cross Kerr nonlinearity is only limited by the two-photon absorption (the self Kerr nonlinearity is negligible provided that $|\omega_a - \omega_b| \gg \Delta_{42}$). After adiabatically eliminating all the atomic levels, the cross phase modulation coefficient is given by [26]

$$\chi \sim \frac{3|g_{13}|^2|g_{24}|^2}{\Omega_c^2 \Delta_{42}} n_{\mathrm{atom}}, \tag{66}$$

where g_{24} and g_{13} are the coupling coefficients between the atoms and the cavity modes a_i and b_i, respectively, Ω_c denotes the Rabi frequency of the coupling field, and n_{atom} is the total atom number contained in the cavity. The two-photon absorption rate χ_i is connected with χ by the relation $\chi_i/\chi = \gamma_{42}/\Delta_{42}$, where $2\gamma_{42}$ is the spontaneous emission rate from level $|4\rangle$ to level $|2\rangle$. To justify the adiabatic elimination, one requires that $|g_{13}|^2 n_{\mathrm{atom}}/\Omega_c^2 < 1$ [29,30]. As an estimation, if one takes $|g_{13}|^2 n_{\mathrm{atom}}/\Omega_c^2 \sim 0.2$, $g_{24}/2\pi \sim 10$ MHz, $\gamma_{42}/2\pi \sim 30$ MHz, and $\Delta_{42} \sim 10\gamma_{42}$, the coefficient χ is about $\chi/2\pi \sim 0.2$ MHz, and the two-photon absorption rate $\chi_i \sim 0.1\chi$. This value of the cross phase modulation coefficient χ is not large enough to realize a single-photon turnstile device [26], but it is enough for performing QND measurements of the photon number. For example, if the mean photon number $\langle n_1 \rangle = \langle n_2 \rangle = \sinh^2(r) \sim 1.4$ with the squeezing parameter $r \sim 1.0$, we choose the decay rates $\kappa/2\pi \sim 4$ MHz and $\gamma/2\pi \sim 100$ MHz (these values for decay rates are obtainable in current experiments), and let $g \sim 50$ (for a cavity with cross area $S \sim 0.5 \times 10^{-4}$ cm^2, $g \sim 50$ corresponds to a coherent driving light with intensity about 10 mW cm^{-2}). With the above parameters, all the requirements listed in Table I can be satisfied if we choose the measuring time $T \sim 8$ ns. Note that the light speed can be much reduced in the EIT medium [28] , so it is possible to get a reduced cavity decay rate κ with the same finesse mirrors, and then more favorable parameters can be given for the QND measurement. Note also that a large Kerr nonlinearity based on EIT can also be obtained in other systems, such as trapping a single atom in a high finesse cavity [31]. So the example discussed here is not the unique choice.

ACKNOWLEDGMENTS

We thank P. Grangier and S. Parkins for discussions. This work was supported by the Austrian Science Foundation, by the European TMR network Quantum Information, by the European Union Project EQUIP, and by the Institute for Quantum Information. G.G. acknowledges support by the Friedrich-Naumann-Stiftung.

[1] C. H. Bennett, Phys. Today **48** (10), 24 (1995).
[2] J. I. Cirac *et al.*, Phys. Rev. Lett. **78**, 3221 (1997); S. J. Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998).
[3] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
[4] C. H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996).
[5] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).
[6] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
[7] S. L. Braunstein and J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[8] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
[9] S. L. Braunstein, Nature (London) **394**, 47 (1998); S. Lloyd and J. J.-E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).
[10] T. C. Ralph, Phys. Rev. A **61**, 010302(R) (2000).
[11] L. M. Duan *et al.*, Phys. Rev. Lett. **84**, 2722 (2000); R. Simon, e-print quant-ph/9909044.
[12] P. Horodecki and M. Lewenstein, e-print quant-ph/0001035.
[13] A. Furusawa *et al.*, Science **282**, 706 (1998).
[14] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 4002 (2000).
[15] S. Parker, S. Bose, and M. B. Plenio, e-print quant-ph/9906098.
[16] T. Opatrny, G. Kurizki, and D.-G. Welsch, e-print quant-ph/9907048.
[17] Z. Y. Ou, *et al.*, Phys. Rev. Lett. **68**, 3663 (1992); A. S. Parkins and H. J. Kimble, e-print quant-ph/9907049.
[18] C. W. Gardiner and P. Zoller, *Quantum Noise* (Springer-Verlag, Berlin, 1999).
[19] H. M. Wiseman, Phys. Rev. Lett. **75**, 4587 (1995).
[20] S. M. Barnett and D. T. Pegg, Phys. Rev. Lett. **76**, 4148 (1996).
[21] A. E. Kozhekin, K. Molmer, and E. S. Polzik, e-print quant-ph/9912014.
[22] M. D. Lukin, S. F. Yelin, and M. Fleischhauer, Phys. Rev. Lett. **84**, 4232 (2000); L. M. Duan, J. I. Cirac, and P. Zoller (unpublished).
[23] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, Berlin, 1995).

[24] G. M. D'Ariano *et al.*, e-print quant-ph/0001065.
[25] G. Nogues *et al.*, Nature (London) **400**, 239 (1999).
[26] A. Imamoglu *et al.*, Phys. Rev. Lett. **79**, 1467 (1997); **81**, 2836 (1998).
[27] Y. Yamamoto, Nature (London) **390**, 17 (1997).
[28] L. V. Hau *et al.*, Nature (London) **397**, 594 (1999).
[29] P. Grangier, D. F. Walls, and K. M. Gheri, Phys. Rev. Lett. **81**, 2833 (1998).
[30] K. M. Gheri, W. Alge, and P. Grangier, Phys. Rev. A **60**, R2673 (1999).
[31] S. Rebic, S. M. Tan, A. S. Parkins, and D. F. Walls, Quantum Semiclassic. Opt. **1**, 490 (1999).

5 Multi-party Entanglement of Gaussian States

5.1 Multi-party Entanglement

So far we have only discussed the entanglement properties of *bipartite* systems. If more parties are considered, an even richer and still largely unexplored variety of nonlocal properties and phenomena is observed. In this setting, the problems of separability and distillability are even more formidable than for bipartite systems. This is already evident for *pure* states, where much more inequivalent types of entanglement are found than in the bipartite case [49]. E.g., even for the simplest multi-party case of three qubits and for the weakest form of equivalence (two states are called equivalent if they can be transformed into each other by local operations with finite probability – all pure bipartite entangled states are equivalent in this sense) there exist two inequivalent kinds of pure state entanglement [50].

Multi-party states exhibit many new features the investigation and understanding of which are still at their beginning. One of the earliest observations was the "refutation of local realism without inequalities" by means of the now famous GHZ-state [45]

$$|GHZ\rangle := \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle \right). \tag{15}$$

More recently mixed states of tripartite systems have been discovered that have the curious property to be separable (according to Def. 2.1) whenever two of the three parties A, B, and C are joined together – i.e., neither between AB-C nor between A-BC nor between B-AC exist quantum correlations – but nevertheless the state cannot be written as a mixture of tripartite product states [46].

The potential applications are found, of course, in the field of multi-party communication. As an example we mention *secret sharing*, a protocol based, e.g., on a three-party GHZ-state that achieves secret key distribution between A, B and C in such a way that only if B and C cooperate they can obtain the secret key [51].

For mixed multi-party entangled states few results have been obtained [46, 47, 48], most notably a scheme to completely classify the separability properties of multi-party systems [47]. This scheme will be explained and used in the following subsection on mixed three-mode Gaussian entanglement.

The field of continuous variable multi-party entanglement is still essentially unexplored. It was shown recently, that the preparation of pure GHZ-like multi-party entangled states can be achieved with encouragingly simple means, in a minimalistic set-up one pure squeezed state, $N-1$ vacuum states and $N-1$ beam splitters suffice to create N-party-entangled states that, e.g., allow teleportation between two arbitrary parties, opening the way to CV "quantum communication networks" [69, 70].

In [71], reprinted in the following subsection, we investigate and completely classify the separability properties of three-partite three-mode Gaussian states. In particular we give a directly computable criterion for the classification of theses state according to the scheme of [47]. These results represent a first example where it is possible to obtain stronger results on entanglement properties for infinite dimensional Gaussian states than on the corresponding qubit-system.

5.2 Separability Properties of Three-mode Gaussian States

Géza Giedke, Barbara Kraus, Maciej Lewenstein, and J. Ignacio Cirac,

We derive a necessary and sufficient condition for separability of tripartite three mode Gaussian states, that is easy to check for any such state. We give a classification of the separability properties of those systems and show how to determine for any state to which class it belongs. We show that there exist genuinely tripartite bound entangled states and point out how to construct and prepare such states.

Phys. Rev. A **64**, 052303 (2001); E-print: quant-ph/0103137.

Separability properties of three-mode Gaussian states

G. Giedke,[1] B. Kraus,[1] M. Lewenstein,[2] and J. I. Cirac[1]
[1]*Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*
[2]*Institut für Theoretische Physik, Universität Hannover, 30163 Hannover, Germany*
(Received 11 April 2001; published 8 October 2001)

We derive a necessary and sufficient condition for the separability of tripartite three-mode Gaussian states that is easy to check for any such state. We give a classification of the separability properties of those systems and show how to determine for any state to which class it belongs. We show that there exist genuinely tripartite bound entangled states and point out how to construct and prepare such states.

DOI: 10.1103/PhysRevA.64.052303 PACS number(s): 03.67.Hk, 03.65.Ta

I. INTRODUCTION

Entanglement of composite quantum systems is central to both the peculiarities and promises of quantum information. Consequently, the study of entanglement of bi- and multipartite systems has been the focus of research in quantum information theory. While pure state entanglement is fairly well understood, there are still many open questions related to the general case of mixed states. The furthest progress has been made in the study of systems of two qubits: it has been shown that a state of two qubits is separable if and only if its partial transpose is positive (PPT property) [1] and a closed expression for the entanglement of formation was derived [2]. Moreover, it was shown [3] that all entangled states of two qubits can be distilled into maximally entangled pure states by local operations. This property of distillability is of great practical importance, since only the distillable states are useful for certain applications such as long-distance quantum communication, quantum teleportation, or cryptography [4].

In higher dimensions much less is known: the PPT property is no longer sufficient for separability as proved by the existence of PPT entangled states (PPTES's) in $\mathbb{C}^2\otimes\mathbb{C}^4$ systems [5]. These states were later shown to be bound entangled [6]: even if two parties (Alice and Bob) share an arbitrarily large supply of such states, they cannot transform (''distill'') it into even a single pure entangled state by local quantum operations and classical communication. Meanwhile, a number of additional necessary or sufficient conditions for inseparability have been found for finite-dimensional bipartite systems, which use properties of the range and kernel of the density matrix ρ and its partial transpose ρ^{T_A} to establish separability ([7] and references therein).

When going from two to more parties, current knowledge is even more limited. Pure multipartite entanglement was first considered in [8]. A classification of N-partite mixed states according to their separability properties has been given [9]. But even for three qubits there is currently no general way to decide to which of these classes a given state belongs [10]. Results on bound entanglement [11] and entanglement distillation [12] for multiparty systems have been obtained.

Recently increasing attention was paid to infinite dimensional systems, the so-called continuous quantum variables (CV's), in particular since the experimental realization of CV quantum teleportation [13,14]. Quantum information with CV's in general is mainly concerned with the family of Gaussian states, since these comprise essentially all the experimentally realizable CV states. A practical advantage of CV systems is the relative ease with which entangled states can be generated in the laboratory [14,15]. First results on the separability and distillability of Gaussian states were reported in [16–22]. One finds striking similarities between the situations of two qubits and two one-mode CV systems in a Gaussian state: PPT is necessary and sufficient for separability [17,18], and all inseparable states are distillable [19]. Generalizing the methods reviewed in [7] it was shown that for more than two modes at either side PPT entangled states exist [20]. In [21] a computable measure of entanglement for bipartite Gaussian states was derived.

The study of CV multipartite entanglement was initiated in [23,24], where a scheme was suggested to create pure CV N-party entanglement using squeezed light and $N-1$ beam splitters. In fact, this discussion indicates that tripartite entanglement has already been created (though not investigated or detected) in a CV quantum teleportation experiment [14].

In this paper we provide a complete classification of three-mode entanglement (according to the scheme [9]) and obtain—in contrast to the finite-dimensional case—a simple, directly computable criterion that allows us to determine to which class a given state belongs. We show that none of these classes are empty and in particular provide examples of genuine tripartite bound entangled states, i.e., states of three modes A, B, and C that are separable whenever two parties are grouped together but cannot be written as a mixture of tripartite product states. Finally we show how to extend these results to states of one mode each at A and B and n modes at C.

Before we can derive our results we need to introduce some notation and collect a number of useful facts about our main object of study: Gaussian states.

II. GAUSSIAN STATES

In quantum optics and in other scenarios described by continuous quantum variables, not all states on the infinite-dimensional Hilbert space are equally accessible in current experiments. In fact, the set of Gaussian states comprises essentially all genuinely CV states that can currently be pre-

 ©2001 The American Physical Society

pared in the laboratory. This and the mathematical simplicity of these states are the reasons why CV quantum information has so far considered almost exclusively Gaussian states, as will the present paper. This section summarizes results on Gaussian states that we need in the following and introduces some notation.

We consider systems composed of n distinguishable infinite-dimensional subsystems, each with Hilbert space $\mathcal{H}=L^2(\mathbb{R})$. These could be implemented quantum optically by different modes of the electromagnetic field: hence each of these subsystems will be referred to as a ''mode.'' To each mode belong the two canonical observables X_k, P_k, $k=1,\ldots,n$, with commutation relation $[X_k,P_k]=i$. Defining $R_k=X_k$, $R_{n+k}=P_k$, these relations are summarized as $[R_k,R_l]=-iJ_{kl}$, using the antisymmetric $2n\times 2n$ matrix

$$J=\begin{pmatrix} 0 & -\mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}, \tag{2.1}$$

which plays an important role in the following calculations [25].

For such systems, it is convenient to describe the state ρ by its characteristic function

$$\chi(x)=\mathrm{Tr}[\rho D(x)]. \tag{2.2}$$

Here $x=(q,p)$, $q,p\in\mathbb{R}^n$ is a real vector, and

$$D(x)=\exp\left(-i\sum_k (q_kX_k+p_kP_k)\right). \tag{2.3}$$

The characteristic function contains all the information about the state of the system: that is, one can construct ρ knowing χ. Gaussian states are exactly those for which χ is a Gaussian function of the phase space coordinates x [26],

$$\chi(x)=e^{-x^T\gamma x/4-id^Tx}, \tag{2.4}$$

where γ is a real, symmetric, strictly positive matrix, the correlation matrix (CM), and $d\in\mathbb{R}^{2n}$ is a real vector, the displacement. Note that both γ and d are directly measurable quantities; their elements γ_{kl} and d_k are related to the expectation values and variances of the operators R_k. A Gaussian state is completely determined by γ and d. Note that the displacement of a (known) state can always be adjusted to $d=0$ by a sequence of unitaries applied to individual modes. This implies that d is irrelevant for the study of nonlocal properties. Therefore we will occasionally say, e.g., that ''a CM is separable'' when the Gaussian state with this CM is separable. Also, from now on in this paper ''state'' will always mean ''Gaussian state'' (unless stated otherwise).

Not all real, symmetric, positive matrices γ correspond to the CM of a physical state. There are a number of equivalent ways to characterize physical CM's, which will all be useful in the following. We collect them in the following lemma.

Lemma 1 (correlation matrices). For a real, symmetric $2n\times 2n$ matrix $\gamma>0$ the following statements are equivalent:

$$\gamma \text{ is the CM of a physical state,} \tag{2.5a}$$

$$\gamma+J\gamma^{-1}J\geqslant 0, \tag{2.5b}$$

$$\gamma-iJ\geqslant 0, \tag{2.5c}$$

$$\gamma=S^T(D\oplus D)S, \tag{2.5d}$$

for S symplectic [27] and $D\geqslant\mathbb{1}$ diagonal [28].

Proof. (2.5a) $\Leftrightarrow$ (2.5b), see [26]; (2.5a) $\Leftrightarrow$ (2.5c), see [20]; (2.5a) $\Leftrightarrow$ (2.5d), see [29] (proposition 4.22).

A CM corresponds to a pure state if and only if (iff) $D=\mathbb{1}$, i.e., iff $\det\gamma=1$ (e.g., [26]). It is easy to see from Eq. (2.5d) that for pure states Ineq. (2.5b) becomes an equality and $\dim[\ker(\gamma-iJ)]=n$. It is clear from Eq. (2.5d) that for every CM γ there exists a pure CM γ_0 such that $\gamma_0\leqslant\gamma$. This will allow us to restrict many proofs to pure CM's only. Note that for a pure $2n\times 2n$ CM γ it holds that $\mathrm{Tr}\,\gamma\geqslant 2n$.

A very important transformation for the study of entanglement is partial transposition [1]. Transposition is an example of a positive but not completely positive map and therefore, may reveal entanglement when applied to part of an entangled system. On phase space, transposition corresponds to the transformation that changes the sign of all the p coordinates $(q,p)\mapsto\Lambda(q,p)=(q,-p)$ [18] and leaves the q's unchanged. For γ and d this means $(\gamma,d)\mapsto(\Lambda\gamma\Lambda,\Lambda d)$. Using this, the nonpositive partial transpose (NPT) criterion for inseparability [1] translates very nicely to Gaussian states. Consider a bipartite system consisting of m modes on Alice's side and n modes on Bob's ($m\times n$ system in the following). Let γ be the CM of a Gaussian $m\times n$ state and denote by $\Lambda_A=\Lambda\oplus\mathbb{1}$ the partial transposition in Alice's system only. Then we have the following criterion for inseparability.

Theorem 1 (NPT criterion). Let γ be the CM of a $1\times n$ system, then γ corresponds to an inseparable state if and only if $\Lambda_A\gamma\Lambda_A$ is not a physical CM, i.e., if and only if

$$\Lambda_A\gamma\Lambda_A\ngeqslant iJ. \tag{2.6}$$

We say that γ ''is NPT'' if Eq. (2.6) holds.

Proof. See [18] for $N=1$ and [20] for the general case.

Occasionally it is convenient to apply the orthogonal operation Λ_A to the right-hand side of Ineq. (2.6) and write $\tilde{J}_A\equiv\Lambda_AJ\Lambda_A$.

For states of at least two modes at both sides condition (2.6) is still sufficient for inseparability, but no longer necessary as shown by Werner and Wolf, who have considered a family of 2×2 entangled states with positive partial transpose [20]. In the same paper, the following was shown.

Theorem 2 (separability of Gaussian states). A state with CM γ is separable iff there exist CM's γ_A,γ_B such that

$$\gamma\geqslant\gamma_A\oplus\gamma_B. \tag{2.7}$$

It is observed in [20] that if Ineq. (2.7) can be fulfilled, then the state with CM γ can be obtained by local operations and classical communication from the product state with CM $\gamma_p=\gamma_A\oplus\gamma_B$, namely, by mixing the states (γ_p,d) with the d's distributed according to the Gaussian distribution $\propto\exp[-d^T(\gamma-\gamma_p)^{-1}d]$.

Note that while Theorem 2 gives a necessary and sufficient condition for separability, it is not a practical criterion, since to use it, we have to prove the existence or nonexistence of CM's γ_A, γ_B. Instead, a criterion would allow us to directly calculate from γ whether the corresponding state is separable or not. Theorem 2 and its extension to the three-party situation are the starting point for the derivation of such a criterion for the case of three-mode three-party states in the following main section of this paper.

III. TRIMODE ENTANGLEMENT

When systems that are composed of $N>2$ parties are considered, there are many ''types'' of entanglement due to the many ways in which the different subsystems may be entangled with each other. We will use the scheme introduced in [9] to classify three-mode tripartite Gaussian states. The important point is that from the extension of theorem 2 we can derive a simple criterion that allows us to determine which class a given state belongs to. This is in contrast to the situation for three qubits, where up until now no such criterion is known. In particular, we show that none of these classes are empty and we provide an example of a genuine tripartite bound entangled state, i.e., a state of three modes *A*, *B*, and *C* that is separable whenever two parties are grouped together but cannot be written as a mixture of tripartite product states and therefore cannot be prepared by local operations and classical communication of three separate parties.

A. Classification

The scheme of [9] considers all possible ways to group the N parties into $m \leqslant N$ subsets, which are then themselves considered each as a single party. Now, it has to be determined whether the resulting m-party state can be written as a mixture of m-party product states. The complete record of the m-party separability of all these states then characterizes the entanglement of the N-party state.

For tripartite systems, we need to consider four cases: namely, the three bipartite cases in which *AB*, *AC*, or *BC* are grouped together, respectively, and the tripartite case in which all *A*, *B*, and *C* are separate. We formulate a simple extension to theorem 2 to characterize mixtures of tripartite product states.

Theorem 2′ (three-party separability). A Gaussian three-party state with CM γ can be written as a mixture of tripartite product states iff there exist one-mode correlation matrices $\gamma_A, \gamma_B, \gamma_C$ such that

$$\gamma - \gamma_A \oplus \gamma_B \oplus \gamma_C \geqslant 0. \tag{3.1}$$

Such a state will be called *fully separable*.

Proof. The proof is in complete analogy with that of Theorem 2.7 in [20] and is therefore omitted here.

A state for which there are a one-mode CM γ_A and a two-mode CM γ_{BC} such that $\gamma - \gamma_A \oplus \gamma_{BC} \geqslant 0$ is called an A-BC biseparable state (and similarly for the two other bipartite groupings). In total, we have the following five different entanglement classes.

Class 1. Fully inseparable states are those which are not separable for any grouping of the parties.

Class 2. One-mode biseparable states are those which are separable if two of the parties are grouped together, but inseparable with respect to the other groupings.

Class 3. Two-mode biseparable states are separable with respect to two of the three bipartite splits but inseparable with respect to the third.

Class 4. Three-mode biseparable states separable with respect to all three bipartite splits but cannot be written as a mixture of tripartite product states.

Class 5. The fully separable states can be written as a mixture of tripartite product states.

Examples for class 1 (the GHZ-like states of [24]), class 2 (two-mode squeezed vacuum in the first two and the vacuum in the third mode), and class 5 (vacuum state in all three modes) are readily given; we will provide examples for classes 3 and 4 in Sec. IV below.

How can we determine to which class a given state with CM γ belongs? States belonging to classes 1, 2, or 3 can be readily identified using the NPT criterion (Theorem 1). Denoting the partially transposed CM by $\tilde{\gamma}_x = \Lambda_x \gamma \Lambda_x$, $x = A, B, C$, we have the following equivalences.

Lemma 2 (classification):

$$\tilde{\gamma}_A \not\geqslant iJ, \tilde{\gamma}_B \not\geqslant iJ, \tilde{\gamma}_C \not\geqslant iJ \Leftrightarrow \text{class } 1, \tag{3.2}$$

$$(*)\, \tilde{\gamma}_A \not\geqslant iJ, \tilde{\gamma}_B \not\geqslant iJ, \tilde{\gamma}_C \geqslant iJ \Leftrightarrow \text{class } 2, \tag{3.3}$$

$$(*)\, \tilde{\gamma}_A \not\geqslant iJ, \tilde{\gamma}_B \geqslant iJ, \tilde{\gamma}_C \geqslant iJ \Leftrightarrow \text{class } 3, \tag{3.4}$$

$$\tilde{\gamma}_A \geqslant iJ, \tilde{\gamma}_B \geqslant iJ, \tilde{\gamma}_C \geqslant iJ \Leftrightarrow \text{class } 4 \text{ or } 5, \tag{3.5}$$

where the asterisk reminds us to consider all permutations of the indices *A*, *B*, and *C*.

The proof follows directly from the definitions of the different classes and theorem 1.

What is still missing is an easy way to distinguish between class 4 and class 5. Thus to complete the classification we now provide a criterion to determine whether a CM γ satisfying Ineqs. (3.5) is fully separable or three-mode biseparable; that is, we have to decide whether there exist one-mode CM's $\gamma_A, \gamma_B, \gamma_C$ such that Eq. (3.1) holds, in which case γ is fully separable. In the next subsection we will describe a small set consisting of no more than nine CM's among which γ_A is necessarily found if the state is separable.

B. Criterion for full separability

This subsection contains the main result of the paper: a separability criterion for PPT $1\times1\times1$ Gaussian states, i.e., states whose CM fulfills Ineqs. (3.5). We start from Theorem $2'$ and obtain in several steps a simple, directly computable necessary and sufficient condition. The reader mainly interested in this result may go directly to Theorem 3, from where she will be guided to the necessary definitions and lemmas.

Since the separability condition in Theorem $2'$ is formulated in terms of the positivity of certain matrices the following lemma will be very useful throughout the paper. We con-

sider a self-adjoint $(n+m)\times(n+m)$ matrix M that we write in block form as

$$M=\begin{pmatrix} A & C \\ C^\dagger & B \end{pmatrix}, \tag{3.6}$$

where A, B, and C are $n\times n$, $m\times m$, and $n\times m$ matrices, respectively.

Lemma 3 (positivity of self-adjoint matrices). A self-adjoint matrix M as in Eq. (3.6) with $A\geqslant 0, B\geqslant 0$ is positive if and only if for all $\epsilon>0$

$$A-C\frac{1}{B+\epsilon\mathbb{1}}C^\dagger\geqslant 0 \tag{3.7}$$

or, equivalently, if and only if

$$\ker B\subseteq\ker C \tag{3.8a}$$

and

$$A-C\frac{1}{B}C^\dagger\geqslant 0, \tag{3.8b}$$

where B^{-1} is understood in the sense of a pseudoinverse (inversion on the range).

Proof. The only difficulty in the proof arises if $\ker B\neq 0$. Therefore we consider the matrices M_ϵ, where B in Eq. (3.6) is replaced by $B_\epsilon=B+\epsilon\mathbb{1}$ $(\epsilon>0)$, which avoids this problem and which is positive $\forall\ \epsilon>0$ iff $M\geqslant 0$. In a second simplifying step we note that $M_\epsilon\geqslant 0\ \ \forall\ \ \epsilon>0$ iff $M'_\epsilon=(\mathbb{1}\oplus B_\epsilon^{-1/2})M(\mathbb{1}\oplus B_\epsilon^{-1/2})\geqslant 0$.

Now direct calculation shows the claim that we can write a general $f\oplus g$ as $f\oplus[(B_\epsilon^{-1/2}C^\dagger)h+h_\perp]$, where $h_\perp$ is orthogonal to the range of $(B_\epsilon^{-1/2}C^\dagger)$. Then $(f\oplus g)^\dagger M'_\epsilon(f\oplus g)=f^\dagger(A-CB_\epsilon^{-1}C^\dagger)f+(f+h)^\dagger CB_\epsilon^{-1}C^\dagger(f+h)+h_\perp^\dagger h_\perp$, which is clearly positive, if Eq. (3.7) holds. With the choice $h_\perp=0$ and $h=-f$ it is seen that Eq. (3.7) is also necessary.

That the second condition is equivalent is seen as follows: If Ineq. (3.7) holds, $\forall\ \epsilon>0$, there cannot be vector $\xi\in\ker B$ and $\xi\notin\ker C$ since for such a ξ we have

$$\xi^T\left(A-C\frac{1}{B+\epsilon\mathbb{1}}C^\dagger\right)\xi<0$$

for sufficiently small $\epsilon>0$, and if Eq. (3.8a) holds, then Eq. (3.7) converges to Eq. (3.8b). Conversely, if Eq. (3.8a) holds, then $CB^{-1}C^\dagger$ is well-defined and Ineq. (3.8b) implies it, $\forall\,\epsilon>0$. ■

As mentioned above, in this section we exclusively consider three-mode CM's γ that satisfy Ineqs. (3.5). We write γ in the form of Eq. (3.6) as

$$\gamma=\begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{3.9}$$

where A is a 2×2 matrix, whereas B is a 4×4 matrix. We observe that Ineqs. (3.5) impose some conditions on γ that will be useful later on:

Observation 1. Let γ satisfy Ineqs. (3.5); then,

$$\gamma\geqslant\begin{pmatrix} \sigma_A iJ & 0 & 0 \\ 0 & \sigma_B iJ & 0 \\ 0 & 0 & \sigma_C iJ \end{pmatrix}, \tag{3.10}$$

where $\sigma_x\in\{0,\pm 1\}$, $\forall x=A,B,C$.

Proof. Inequalities (3.5) say that $\gamma\pm iJ\geqslant 0$ and $\gamma\pm i\tilde{J}_x\geqslant 0\ \forall x$. By adding these positive matrices all combinations of σ_x can be obtained.

From this it follows

Observation 2. For a PPT CM γ as in Eq. (3.9),

$$\ker(B+iJ),\ker(B+i\tilde{J})\subseteq\ker C, \tag{3.11}$$

where $\tilde{J}=J\oplus(-J)$ is the partially transposed J for two modes.

Proof. Condition (3.11) on the kernels is an immediate consequence of Lemma 3 applied to the matrices $\gamma-0\oplus iJ\oplus(\pm iJ)$, which are positive by observation 1. ■

Then the matrices

$$\tilde{N}\equiv A-C\frac{1}{B-i\tilde{J}}C^T, \tag{3.12a}$$

$$N\equiv A-C\frac{1}{B-iJ}C^T \tag{3.12b}$$

are well-defined and

Observation 3. It holds that both

$$\mathrm{Tr}\,N,\mathrm{tr}\,\tilde{N}>0. \tag{3.13}$$

Proof. Condition (3.13) is true since, again by Lemma 3 and observation 1, both N and $\tilde{N}$ are positive and $N\pm iJ$, $\tilde{N}\pm iJ\geqslant 0$. This implies that $N,\tilde{N}$ cannot be zero, which is the only positive matrix with vanishing trace. Therefore $\mathrm{Tr}\,N,\mathrm{Tr}\,\tilde{N}$ are strictly positive.

The remainder of this section leads in several steps to the separability criterion. First, we simplify the condition (3.1) by reducing it to a condition which involves only one one-mode CM γ_A.

Lemma 4. A PPT three-mode CM γ is fully separable if and only if there exists a one-mode CM γ_A such that both

$$\tilde{N}\geqslant\gamma_A, \tag{3.14a}$$

$$N\geqslant\gamma_A, \tag{3.14b}$$

hold, where $N,\tilde{N}$ were defined in Eqs. (3.12). Without loss of generality we require γ_A to be a pure state CM, i.e., $\det\gamma_A=1$.

Proof. By Theorem $2'$ full separability of γ is equivalent to the existence of one-mode CMs $\gamma_A,\gamma_B,\gamma_C\geqslant iJ$ such that $\gamma-\gamma_A\oplus\gamma_B\oplus\gamma_C\geqslant 0$. Let γ_x stand for $\gamma_{A,B,C}$.

By Lemma 3 this is equivalent to $\exists\,\gamma_x$ such that

$$X_\epsilon \equiv B - C^T \frac{1}{A_\epsilon - \gamma_A} C \geq \gamma_B \oplus \gamma_C, \quad \forall \epsilon > 0,$$

where $A_\epsilon \equiv A + \epsilon \mathbb{1}$. But iff there exist such γ_x, then (Lemma 3) the inequality also holds for $\epsilon = 0$ and the kernels fulfill Eq. (3.8a). This is true iff the matrix $X \equiv X_0'$ is a CM belonging to a separable state, i.e., (Theorem 1), iff $X' \geq i\tilde{J}, iJ$. Using $B \geq i\tilde{J}, iJ$ [which holds since γ fulfills Ineqs. (3.5)] we obtain that γ is separable iff there exists $\gamma_A \geq iJ$ such that

$$\begin{pmatrix} A - \gamma_A & C \\ C^T & B_k' \end{pmatrix} \geq 0, \quad k = 1,2, \tag{3.15}$$

where $B_1' = B - iJ$ and $B_2' = B - i\tilde{J}$. Since condition (3.8a) holds, this is (Lemma 3) equivalent to Ineqs. (3.14). That we can always choose $\det \gamma_A = 1$ follows directly from Eq. (2.5d) and the remark after Lemma 1. ■

While we can always find a γ_A fulfilling Ineq. (3.14b), since γ belongs to a PPT state (and there exists a two-mode CM $\gamma_{BC} \geq iJ$ such that $\gamma_A \oplus \gamma_{BC}$ is smaller than γ), it may well happen that Ineq. (3.14a) cannot be satisfied at all, or that it is impossible to have both Ineqs. (3.14) fulfilled for one γ_A simultaneously. Note that due to Ineqs. (3.5), N and $\tilde{N}$ as above are always positive. From Ineqs. (3.14) we observe the following.

Observation 4. For the CM γ of a separable state it is necessary to have

$$\mathrm{Tr}\, N, \mathrm{Tr}\, \tilde{N} \geq 2, \tag{3.16a}$$

$$\det N, \det \tilde{N} > 0, \tag{3.16b}$$

where γ as in Eq. (3.9) and $N, \tilde{N}$ as in Eqs. (3.12).

Proof. A self-adjoint 2×2 matrix is positive iff its trace and determinant are positive. Since the Trace of the right-hand side (RHS) of both Ineqs. (3.14) is ≥ 2 (remark after Lemma 1), the same is necessary for the LHS. Also, since $\det \gamma_A = 1$, which implies that γ_A has full rank, any matrix $\geq \gamma_A$ must also have full rank [30] and thus a strictly positive determinant. ■

For a self-adjoint positive 2×2 matrix

$$R = \begin{pmatrix} a & b \\ b^* & c \end{pmatrix}, \tag{3.17}$$

we show the following.

Lemma 5. There exists a CM $\gamma_A \leq R$ if and only if there exist $(y,z) \in \mathbb{R}^2$ such that

$$\mathrm{tr}\, R \geq 2\sqrt{1 + y^2 + z^2}, \tag{3.18a}$$

$$\det R + 1 + L^T \begin{pmatrix} y \\ z \end{pmatrix} \geq \mathrm{tr}\, R \sqrt{1 + y^2 + z^2}, \tag{3.18b}$$

where

$$L = (a - c, 2\,\mathrm{Re}\, b). \tag{3.19}$$

Proof. As noted in Lemma 4 we need only look for γ_A with $\det \gamma_A = 1$. We parametrize

$$\gamma_A = \begin{pmatrix} x + y & z \\ z & x - y \end{pmatrix}, \tag{3.20}$$

with real parameters x,y,z and $x^2 = 1 + y^2 + z^2$ for purity. This is a CM iff $\gamma_A - iJ \geq 0$ (Lemma 1), that is, iff $\mathrm{Tr}\, \gamma_A = 2x \geq 0$ [where we use that positivity of the 2×2 matrix is equivalent to the positivity of its trace and determinant and $\det(\gamma_A - iJ) = 0$ by construction]. By the same argument, $R - \gamma_A \geq 0$ leads to the two conditions (3.18). ■

The Ineqs. (3.18) have a simple geometrical interpretation that will be useful for the proof of the promised criterion: Inequality (3.18a) restricts (y,z) to a circular disk $\mathcal{C}'$ of radius $\sqrt{(\mathrm{Tr}\, R)^2/4 - 1}$ around the origin, while Ineq. (3.18b) describes a (potentially degenerate) ellipse $\mathcal{E}$ (see Fig. 2), whose elements are calculated below, and the existence of a joint solution to Ineqs. (3.18) is therefore equivalent to a nonempty intersection of $\mathcal{C}'$ and $\mathcal{E}$.

Applying this now to the matrices (3.12) we find that in order to simultaneously satisfy both conditions in Lemma 4, the intersection between the two ellipses $\mathcal{E}, \tilde{\mathcal{E}}$ and the smaller of the two concentric circles $\mathcal{C}', \tilde{\mathcal{C}}'$ (which we denote in the following by $\mathcal{C}$) must be nonempty. This condition leads to three inequalities in the coefficients of the matrices $\tilde{N}, N$ which can be satisfied simultaneously if and only if the PPT trimode state is separable. Thus we can reformulate the condition for separability (Lemma 4) as follows.

Lemma 6 (reformulated separability condition). A three-mode state with CM γ satisfying Ineqs. (3.5) is fully separable if and only if there exists a point $(y,z) \in \mathbb{R}^2$ fulfilling the following inequalities:

$$\min\{\mathrm{Tr}\, N, \mathrm{Tr}\, \tilde{N}\} \geq 2\sqrt{1 + y^2 + z^2}, \tag{3.21a}$$

$$\det N + 1 + L^T \begin{pmatrix} y \\ z \end{pmatrix} \geq \mathrm{Tr}\, N \sqrt{1 + y^2 + z^2}, \tag{3.21b}$$

$$\det \tilde{N} + 1 + \tilde{L}^T \begin{pmatrix} y \\ z \end{pmatrix} \geq \mathrm{Tr}\, \tilde{N} \sqrt{1 + y^2 + z^2}. \tag{3.21c}$$

Proof. According to Lemma 4 γ belongs to a separable state iff we can find γ_A smaller than $\tilde{N}$ and smaller than N. According to Lemma 5 we can find such a γ_A iff we can find (y,z) such that Ineqs. (3.18) are satisfied for both N and $\tilde{N}$. ■

In the following paragraphs we have a closer look at the sets $\mathcal{E}$, $\tilde{\mathcal{E}}$, and $\mathcal{C}$. The goal of this discussion is to identify a few special points—directly computable from γ—among which a solution to Ineqs. (3.21) will be found iff the state under consideration is separable. This will then lead to the final practical form of the separability criterion which is stated at the end of this section.

By squaring Ineq. (3.21b) we obtain

$$\left[\begin{pmatrix} y \\ z \end{pmatrix} - \mu L\right]^T K \left[\begin{pmatrix} y \\ z \end{pmatrix} - \mu L\right] \leqslant m, \tag{3.22}$$

where $\mu = (\det N+1)/k_1$, $m = (k_2/k_1)[(\det N+1)^2 - k_1]$, and the matrix K is [31]

$$K = k_1 P_L + k_2 P_{L^\perp},$$

with the orthogonal projectors $P_L, P_{L^\perp}$ on $L, L^\perp$ and

$$k_1 = 4[\det N + (\mathrm{Im}\, b)^2],$$

$$K_2 = (\mathrm{Tr}\, N)^2.$$

Due to Ineqs. (3.16), k_1 and k_2 are strictly positive, μ, m are well defined, and K is a positive matrix of rank 2. Let us now distinguish the cases $m<0$ and $m \geqslant 0$. For $m<0$, Ineq. (3.22) can never be fulfilled since K is a positive matrix. In the case $m \geqslant 0$, Ineq. (3.22) describes an ellipse $\mathcal{E}$ which is centered at $m_e = \mu L$ with major axis L and minor axis $L^\perp$ of lengths $\sqrt{m/k_1} \geqslant \sqrt{m/k_2}$, respectively. From Ineq. (3.21c) we obtain the same equations for the tilded quantities derived from $\tilde{N}$.

The final argument for the derivation of the separability criterion is as follows. By Lemma 6 the state is separable if and only if the three sets described by Ineqs. (3.21a)–(3.21c) have a common intersection, i.e., iff $I \equiv \mathcal{E} \cap \tilde{\mathcal{E}} \cap \mathcal{C} \neq \emptyset$. The border of I is contained in the union of the borders of the ellipses and circle: $\partial I \subseteq \partial\mathcal{E} \cup \partial\tilde{\mathcal{E}} \cup \partial\mathcal{C}$. Now we can distinguish two cases, both of which allow one to calculate a definite solution to the Ineqs. (3.21) if the state is separable: Either ∂I has nonempty intersections with the borders of two of the sets $\mathcal{E}$, $\tilde{\mathcal{E}}$, $\mathcal{C}$, or ∂I coincides with the border of one of the three. In the latter case this whole set is contained in I. In the former case, at least one of the points at which the borders intersect must be in I and thus a solution. If no solution is found this way, the state is inseparable. This argument is made more precise in the final theorem. Formulas for the nine candidate solutions—the centers $m_c, m_e, m_{\tilde{e}}$ and the intersections points $i^{\pm}_{e\tilde{e}}, i^{\pm}_{ce}, i^{\pm}_{c\tilde{e}}$—are given in the Appendix.

Theorem 3 (criterion for full separability). A three-mode state corresponding to the CM γ satisfying Ineq. (3.5) is fully separable if and only if Ineq. (3.16b) holds and there exists a point ξ_{sol},

$$\xi_{\mathrm{sol}} \in \{m_c, m_e, m_{\tilde{e}}, i^{\pm}_{e\tilde{e}}, i^{\pm}_{ce}, i^{\pm}_{c\tilde{e}}\}, \tag{3.23}$$

fulfilling the Ineqs. (3.21).

Proof. We already saw (observation 4) that $\det N, \det \tilde{N} > 0$ are necessary for separability. If this holds, the quantities used in Eqs. (3.21) and (3.23) and in their derivation are all well-defined.

According to Lemma 6, γ is fully separable iff there exists a point $(y,z)^T$ such that the Ineqs. (3.21) are fulfilled. Therefore, if one of the points (3.23) satisfies Ineqs. (3.21), then it determines a γ_A fulfilling Ineqs. (3.14) thus proving that the state is separable. To complete the proof, we show that if the state is separable, then we find a solution to Ineqs. (3.21) among the points (3.23).

As pointed out before, the condition that Ineqs. (3.21) can simultaneously be satisfied has the geometrical interpretation that the circle $\mathcal{C}$ and the two ellipses $\mathcal{E}, \tilde{\mathcal{E}}$ have a nonempty intersection, i.e., $I \equiv \mathcal{E} \cap \tilde{\mathcal{E}} \cap \mathcal{C} \neq \emptyset$.

Thus it remains to prove that if I is nonempty then one of the nine points in (3.23) lies in I. But if $I \neq \emptyset$ there are only the following two possibilities: since all the sets considered are convex and closed, either the border of I coincides with that of one of the sets $\mathcal{C}, \mathcal{E}, \tilde{\mathcal{E}}$ (which means that one of these sets, call it $\mathcal{S}$, is contained in both others) or at least two of the borders $\partial\mathcal{C}, \partial\mathcal{E}, \partial\tilde{\mathcal{E}}$ contribute to ∂I, in which case the points at which these two intersect belong to ∂I and thus to I.

In the former case, the center of $\mathcal{S}$ is a solution and given by one of the Eqs. (A1); in the latter, one can find a solution among the intersections of the borders of the sets $\mathcal{E}, \tilde{\mathcal{E}}, \mathcal{C}$. That these are given by the $i^{\pm}_x$ is shown in Appendix A. ■

If a CM γ belongs to a separable state according to the above theorem then the point ξ_{sol} provides us with a pure one-mode CM γ_A such that $N, \tilde{N} \geqslant \gamma_A$. By construction $\gamma' = B - C(A - \gamma_A)^{-1} C^T$ is a separable 2×2 CM and by repeating a similar procedure as above with γ' we can calculate a pure product-state decomposition of the original state with CM γ.

IV. EXAMPLES OF BOUND ENTANGLED STATES

In this section we construct states belonging to Classes 3 and 4. Our construction makes use of ideas that were first applied in finite dimensional quantum systems to find PPT entangled states (PPTES) [5] and then generalized in [32] to construct so-called edge states, i.e. states on the border of the convex set of states with positive partial transpose. Similarly, one can define ''edge CMs'' as those that lie on the border of the convex set of PPT CMs (they are called ''minimal PPT CMs'' in [20]).

This section is divided into three subsections. In the first one we define ''edge CMs'' and characterize them. In the second and third subsections we present two different families of CMs which contain edge CMs. We also show that within those families we have CMs belonging to all classes.

A. Edge CM's

In the following we will consider CM's γ corresponding to PPT states, i.e., fulfilling

$$\gamma - i\tilde{J}_x \geqslant 0, \quad \text{for all } x = 0, A, B, C, \tag{4.1}$$

where $\tilde{J}_0 \equiv J$.

Definition 1 (edge correlation matrices). A CM γ is an edge CM if it corresponds to a nonseparable state, fulfills Eq. (4.1), and $\gamma' \equiv \gamma - P$ does not fulfill Eq. (4.1) for all real operators P with $0 \neq P \geqslant 0$.

Note that a state with an edge CM automatically belongs to class 4 (i.e., edge CM's correspond to three-mode biseparable states). In order to fully characterize them, we will need the following definition. Let us consider the complex vector space $V \subseteq \mathbb{C}^6$ of dimension d spanned by the vectors belong-

ing to the kernels of all $\gamma - i\tilde{J}_x$ ($x=0,A,B,C$). We will define $K(\gamma)$ as a real vector space which is spanned by the real parts and imaginary parts of all the vectors belonging to V. More specifically, let us denote by $B=\{f_R^k + i f_I^k\}_{k=1}^d$ a basis of V, such that f_R^k and f_I^k are real. We define

$$K(\gamma)=\left\{ \sum_k \lambda_k f_R^k + \mu_k f_I^k, \lambda_k, \mu_k \in \right\} \subseteq \mathbb{R}^6, \qquad (4.2)$$

that is, the real span of the vectors f_R^k and f_I^k. Note that this definition does not depend on the chosen basis B. [As is pointed out in Appendix B, $K(\gamma)$ coincides with the real vector space spanned by all the vectors in the kernels of $\gamma + \tilde{J}_x \gamma^{-1} \tilde{J}_x$.] We then have the following theorem.

Theorem 4 (characterization of $1\times1\times1$ edge CM's). A CM γ fulfilling Eq. (4.1) is an edge CM if and only if there exist no CM's $\gamma_A, \gamma_B, \gamma_C$ such that $\gamma = \gamma_A \oplus \gamma_B \oplus \gamma_C$ and $K = \mathbb{R}^6$.

Proof. We will use the fact [31] that, given two positive matrices $A,B \neq 0$, there exists some $\epsilon > 0$ such that $A - \epsilon B \geqslant 0$ iff $\mathrm{ran}(B) \subseteq \mathrm{ran}(A)$. According to Definition 1 we cannot subtract any real positive matrix from γ without violating the conditions (4.1). This is equivalent to imposing that there be no real vector in the intersection of the ranges of the matrices $\gamma - i\tilde{J}_x$. This is again equivalent to saying that there is no real vector orthogonal to all the $\ker(\gamma - i\tilde{J}_x)$, which in turn is equivalent to $K=\mathbb{R}^6$, since that vector should be orthogonal to all the real and imaginary parts of the vectors spanned by those kernels. Now, if γ corresponds to an entangled state, it is clear that $\gamma \neq \gamma_A \oplus \gamma_B \oplus \gamma_C$. Conversely, if $\gamma \neq \gamma_A \oplus \gamma_B \oplus \gamma_C$ was separable, then there must exist some real positive P such that $\gamma - P = \gamma_A \oplus \gamma_B \oplus \gamma_C$ is separable, and therefore fulfills Eq. (4.1), which is not possible. ■

Note that this theorem generalizes easily to the cases of more than three parties and more than one mode at each site.

In the construction of the following two examples of tripartite bound entangled states we are going to use this theorem. The idea is to take a CM γ_0 of a pure entangled state [which, of course, does not fulfill Eq. (4.1)] and add real positive matrices until the conditions (4.1) as well as $K = \mathbb{R}^6$ are fulfilled. If the resulting CM is not of the form $\gamma_A \oplus \gamma_B \oplus \gamma_C$, then Theorem 4 implies that it is an edge CM. In fact, we can add more real positive matrices keeping the state entangled [and fulfilling Eq. (4.1)]. In order to see how much we can add, we can use the criterion derived in the previous section.

This method of constructing CM's belonging to class 4 also indicates how the corresponding states may be prepared experimentally. Adding a positive matrix P to the CM γ_0 corresponds to the following preparation process: start with an ensemble of states with CM γ_0, and displace them randomly by d according to the Gaussian probability distribution with covariance matrix given by the inverse of P. This is a local operation (that potentially needs to be supplemented by classical communication) on each individual mode. The state produced by this randomization has CM $\gamma + P$ [20].

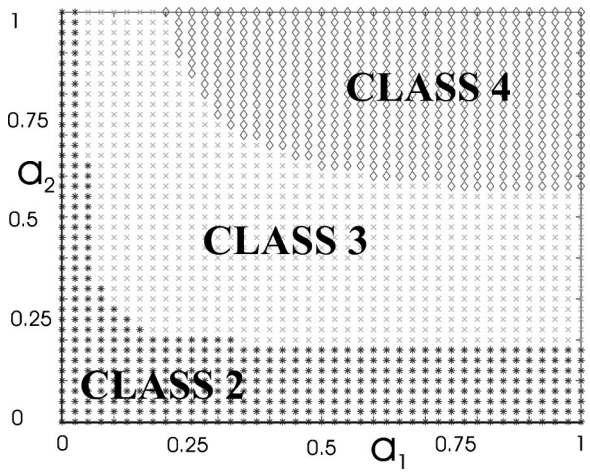

FIG. 1. The entanglement classes of γ_{a_1,a_2}.

B. Example 1

In the first example we start out with an entangled state between the two parties Alice and Bob and the vacuum state in Charlie and add two projectors to the corresponding CM. More specifically, we consider CM's of the form $\gamma_{a_1,a_2} = \gamma + a_1 P_1 + a_2 P_2$, where

$$\gamma = \gamma_{AB} \oplus \mathbb{1}_C \qquad (4.3)$$

and

$$\gamma_{AB} = \begin{pmatrix} a & 0 & c & 0 \\ 0 & a & 0 & -c \\ c & 0 & a & 0 \\ 0 & -c & 0 & a \end{pmatrix}, \qquad (4.4)$$

with $a=\sqrt{1+c^2}$ and c can take any value different from zero. Here, $P_1 = \tilde{p}_1 \tilde{p}_1^T$ and $P_2 = \tilde{p}_1 \tilde{p}_1^T$, where $\tilde{p}_1 = (0,1,0,1,1,2)^T$ and $\tilde{p}_2 = (1,0,-1,0,0,1)^T$.

In order to explain why the CM γ_{a_1,a_2} achieves our purposes, let us first consider the two-mode case in which the correlation matrix is γ_{AB}. We denote now by $p = p_1 + i p_2$ [where $p_1 = (0,1,0,1)^T$ and $p_2 = (1,0,-1,0)^T$] the eigenvector corresponding to the negative eigenvalue of $\gamma_{AB} - i\tilde{J}_A$ [25]. Since $(-i\tilde{J}_A)^* = -i\tilde{J}_B$, we have that the eigenvector corresponding to the negative eigenvalue of $\gamma_{AB} - i\tilde{J}_B$ is $p^* = p_1 - i p_2$. By adding a sufficiently large multiple of the projectors onto those vectors, we obtain a CM whose partial transposes are positive. Note that in this case (just two modes) this would already make the state separable.

In the case of three modes with a correlation matrix γ the same argumentation applies, namely, that by adding some projectors we can make the partial transposes with respect to A and B positive. However, we have to involve C and thereby smear out the initial entanglement between A and B among all three parties. This is exactly what is achieved by adding the projectors P_1 and P_2. If we choose now, for instance, $c=0.3$, $a_1=1$, and $a_2 \approx 0.553\,109\,5$, then one can show that the set $K(\gamma_{a_1,a_2})$ defined as in Eq. (4.2) spans $\mathbb{R}^6$.

As mentioned at the end of the previous subsection, since the resulting CM is not of the form $\gamma_A \oplus \gamma_B \oplus \gamma_C$ it corresponds to an edge CM.

In Fig. 1 we illustrate to which class γ_{a_1,a_2} belongs as a function of the parameters $a_{1,2}$. In order to determine this, we have used the criterion derived in the previous section. It is worth noting that γ_{a_1,a_2} never becomes separable. This follows from Theorem 3 and the fact that both $m=\tilde{m}=0$ for all values of $a_{1,2}$, as can be easily verified. This implies that the two ellipses [cf. Ineq. (3.22)] are just two points [which coincide with the centers given in Eq. (A1)]. Thus, the only possibility that the circle and the two ellipses intersect is that the centers of the ellipses are the same and lie inside the circle. It is easy to show that for all values of a_1 and a_2 the centers of the two ellipses are never the same. Thus the state corresponding to the CM γ_{a_1,a_2} is never separable and is a PPTES for all values of a_1, a_2 for which the partial transposes are positive.

C. Example 2

Here we present a family of states which belong either to class 1, 4, or 5. The states of this family are obtained from a pure GHZ-like state [24] by adding a multiple of the identity, i.e.,

$$\gamma_\alpha = \gamma + \alpha \mathbb{1}, \tag{4.5}$$

where

$$\gamma = \begin{pmatrix} a & 0 & c & 0 & c & 0 \\ 0 & b & 0 & -c & 0 & -c \\ c & 0 & a & 0 & c & 0 \\ 0 & -c & 0 & b & 0 & -c \\ c & 0 & c & 0 & a & 0 \\ 0 & -c & 0 & -c & 0 & b \end{pmatrix}, \tag{4.6}$$

with $a>1$ and

$$b = \frac{1}{4}(5a - \sqrt{9a^2-8}), \tag{4.7}$$

$$c = \frac{1}{4}(a - \sqrt{9a^2-8}). \tag{4.8}$$

For the following discussion, we pick $a=1.2$. It is clear that for $\alpha=0$ the state is fully inseparable: i.e., it belongs to class 1, whereas for $\alpha \geqslant 1$ the state will be fully separable (class 5). We will show now that for $\alpha_0 \leqslant \alpha \leqslant \alpha_1$, where $\alpha_0 \approx 0.297\,56$ and $\alpha_1 \approx 0.313\,55$, the state is biseparable and belongs therefore to class 4.

The CM γ_α is symmetric with respect to permutations between the parties, and therefore the negative eigenvalues of the matrices $\gamma - i\tilde{J}_x$, $x=A,B,C$, are the same. We denote its absolute value by $\alpha_0 \approx 0.297\,56$. It is easy to determine the real and imaginary parts of the corresponding eigenvectors. One finds that all those vectors are linearly independent.

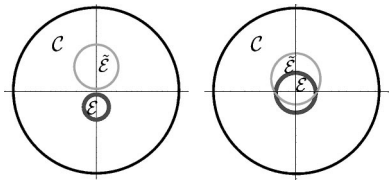

FIG. 2. (a) The circle and the two ellipses do not have a joint intersection: therefore the state corresponding to γ_α is a PPTES. (b) The circle and the two ellipses have a joint intersection: therefore the state corresponding to γ_α is separable.

If we add now $\alpha_0 \mathbb{1}$ to γ, then all those vectors belong to $K(\gamma_{\alpha_0})$ which immediately implies that $K(\gamma_{\alpha_0}) = \mathbb{R}^6$. Since $\gamma_{\alpha_0} \neq \gamma_A \oplus \gamma_B \oplus \gamma_C$, we have that it is an edge CM.

Let us now use Theorem 3 in order to determine α_1. First of all, we show, independently of the discussion above, that γ_{α_0} belongs to class 4. In particular, we find that $m=\tilde{m}=0$ [cf. Eq. (3.22)], which implies that there exists a solution to Ineqs. (3.21) only if the centers of the two ellipses are the same and lie within the circle. Here one can also show that the two centers are not the same and so the state corresponding to the CM γ_{α_0} is a PPTES. Let us determine the values of α for which it is still the case that there exists no intersection of the two ellipses and the circle given by Ineqs. (3.21). It is easy to show that if $\alpha > \alpha_0$, then $\mathrm{Tr}\, N \leqslant \mathrm{Tr}\, \tilde{N}$, which implies that the circle that has to be considered has radius $r_c = \sqrt{(\mathrm{Tr}\, N)^2/4 - 1}$. One can also easily verify that the two ellipses never intersect the border of the circle, which simplifies the problem. The ellipses must always lie inside the circle (since if they were outside it would never be possible to obtain a separable state even for $\alpha > 1$). Thus, the problem reduces to check at which point the ellipses intersect each other. This occurs when $\alpha = \alpha_1 \approx 0.313\,55$. Thus the CM γ_α, where $\alpha_0 \leqslant \alpha < \alpha_1$ corresponds to a PPTES, whereas for $\alpha \geqslant \alpha_1$, the corresponding state is fully separable. In Fig. 2 we have plotted the circle and the two ellipses, which are almost circles in this case, for (a) $\alpha < \alpha_1$ and (b) $\alpha > \alpha_1$.

V. CONCLUSIONS

We have discussed nonlocal properties of Gaussian states of three tripartite modes. We have distinguished five classes with different separability properties and given a simple necessary and sufficient criterion that allows us to determine which of these classes a given Gaussian state belongs to. The first three classes contain only NPT states and positivity of a state under the three partial transpositions suffices to determine to which of those it belongs. The separability criterion, which allows us to distinguish PPT entangled states from separable states, is the main result of this paper. For the case of three qubits such a criterion is still missing. Last, we have constructed examples for all the classes and in particular for tripartite entangled states with positive partial transpose.

It is interesting to note that the results presented above can be extended to cover the case of n modes at location C by using the separability criterion for multimode bipartite

Gaussian states [22]. Nothing changes in the argumentation to distinguish three-party biseparable from fully separable states [the additional modes are taken care of automatically in Eqs. (3.12)]. However, the separability criterion of [22] is now necessary to determine the properties under bipartite splitting, since for *AB*-*C* we deal with a $2\times n$ state and PPT is then no longer sufficient for biseparability [20].

It is worth pointing out that the separability criterion can be checked experimentally. The CM γ can be measured, and thus the criterion is entirely formulated in terms of quantities that are measurable with current technology.

Gaussian CV states promise to be a fruitful testing ground for quantum nonlocality: Pure entanglement is comparatively easy to create in quantum optical experiments, as described in [24]. Likewise, tripartite bound entangled states are experimentally accessible: the states discussed in the examples Secs. IV B and IV C can be obtained by mixing differently displaced pure Gaussian states.

The study of the entanglement of multiparty Gaussian states is still in a very early stage. For example, no work has, to our knowledge, been done on the interesting cases of more parties and modes. But even for the simple three-mode case there are important open questions. In particular nothing is known about the distillability of tripartite states. As in Ref. [9] for qubits, it is easy to see that Gaussian states in classes 3 and 4 cannot be distilled at all and are therefore bound entangled. For this, we consider N copies of a class 3 state ρ, and apply an arbitrary local quantum operation $\mathcal{P}_{locc}$ consisting of a classically correlated sequence of operations of the form $\mathcal{P}=\mathcal{P}_A\otimes\mathcal{P}_B\otimes\mathcal{P}_C$. Since ρ is in class 3, we can write $\rho^{\otimes N}$ as a mixture of *AB*-*C* product states $\Sigma_k p_k \rho^{(N)}_{AB,k}\otimes\rho^{(N)}_{C,k}$ and as a mixture of *AC*-*B* product states $\Sigma_k p'_k \rho^{(N)}_{AC,k}\otimes\rho^{(N)}_{B,k}$. After applying an operation such as $\mathcal{P}$ the resulting state $\tilde{\rho}=\mathcal{P}(\rho^{\otimes N})$ will still be separable along these cuts, and no sequence of operations $\mathcal{P}$ can change this. Thus ρ is bound entangled.

Whether all states in class 2 may be distilled to maximally entangled states between the two nonseparable parties is an open question. If this were shown, it would follow that all states in class 1 could be distilled into arbitrary tripartite entangled states.

ACKNOWLEDGMENTS

G.G. acknowledges financial support by the Friedrich-Naumann-Stiftung. B.K. and J.I.C. thank the University of Hannover for hospitality. M.L., B.K., and J.I.C. acknowledge the hospitality of the Erwin Schrödinger Institute. 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 No. IST-1999-11053), the European Science Foundation, the Institute for Quantum Information GmbH, Innsbruck, and the Deutsche Forschungsgemeinschaft (SFB 407 and Schwerpunkt ''Quanteninformationsverarbeitung'').

APPENDIX A: POINTS OF INTERSECTION

As shown in Theorem 3 a state is separable iff solutions to Ineqs. (3.21) are found among the points of intersection of the curves described by the *equalities* (3.21) or the centers of the three sets. Here we give the formulas to directly calculate these points from γ.

The centers of circle and the ellipses have already been shown to be

$$m_c=(0,0)^T,$$

$$m_e=\frac{\det N+1}{k_1}L,$$

$$m_{\tilde{e}}=\frac{\det\tilde{N}+1}{\tilde{k}_1}\tilde{L}, \tag{A1}$$

where $N,\tilde{N}$ were defined in Eq. (3.12), L in Eq. (3.19), and $k_1,\tilde{k}_1$ after Eq. (3.22). The intersections of the borders of $\mathcal{C},\mathcal{E},\tilde{\mathcal{E}}$ are calculated as follows. Consider first the two ellipses, whose borders are defined by the equalities (3.21b) and (3.21c). Dividing by $\mathrm{Tr}\,N$, respectively, by $\mathrm{Tr}\,\tilde{N}$ and subtracting the two equalities we find that a point on both $\partial\mathcal{E}$ and $\partial\tilde{\mathcal{E}}$ must lie on the straight line $\mathcal{G}_{e\tilde{e}}$ defined by

$$(\det N+1+L^T\xi)/\mathrm{Tr}\,N=(\det\tilde{N}+1+\tilde{L}^T\xi)/\mathrm{Tr}\,\tilde{N}, \tag{A2}$$

where $\xi=(y,z)$. $\mathcal{G}_{e\tilde{e}}$ can be parametrized with $s\in\mathbb{R}$ as $g_{e\tilde{e}}+sf_{e\tilde{e}}$, where

$$g_{e\tilde{e}}=\left(\frac{\det N+1}{\mathrm{Tr}\,N}-\frac{\det\tilde{N}+1}{\mathrm{Tr}\,\tilde{N}}\right)L'/\|L'\|^2, \tag{A3}$$

where $L'=\tilde{L}/\mathrm{Tr}\,\tilde{N}-L/\mathrm{Tr}\,N$ [33] and $f_{e\tilde{e}}$ is a vector orthogonal to L'.

Inserting $\mathcal{G}_{e\tilde{e}}$ in Eq. (3.21b) for $\partial\mathcal{E}$ we obtain a quadratic polynomial in s, whose roots $s^{\pm}_{e\tilde{e}}$ (if they are real) give the intersection points. For the intersection of $\partial\mathcal{C}$ with the ellipses we proceed similarly. In summary, we get for the intersection points

$$i^{\pm}_{e\tilde{e}}=g_{e\tilde{e}}+s^{\pm}_{e\tilde{e}}f_{e\tilde{e}}, \tag{A4}$$

$$i^{\pm}_{ce}=g_{ce}+s^{\pm}_{ce}f_{ce}, \tag{A5}$$

$$i^{\pm}_{c\tilde{e}}=g_{c\tilde{e}}+s^{\pm}_{c\tilde{e}}f_{c\tilde{e}}, \tag{A6}$$

where the vectors g_x, $x=ce,c\tilde{e}$ are

$$g_{ce}=(\mathrm{Tr}\,N\sqrt{r_c^2+1}-\det N-1)L/\|L\|^2, \tag{A7}$$

f_{ce} is a vector orthogonal to L, and r_c is the smaller of the two radii:

$$r_c=\min\{\sqrt{(\mathrm{Tr}\,N)^2/4-1},\sqrt{(\mathrm{Tr}\,\tilde{N})^2/4-1}\}. \tag{A8}$$

$g_{c\tilde{e}},f_{e\tilde{e}}$ are defined likewise for tilded quantities. And, finally, by $s^{\pm}_{e\tilde{e}},s^{\pm}_x$ we denote the real roots of the quadratic polynomials:

$$P_{e\tilde{e}}(s)=(L^T(g_{e\tilde{e}}+sf_{e\tilde{e}})+\det N+1)^2 - (\mathrm{Tr}\,N)^2(1+\|g_{e\tilde{e}}+sf_{e\tilde{e}}\|^2), \quad \text{(A9a)}$$

$$P_x(s)=r_c^2-\|g_x+sf_x\|^2, \quad x=ce,c\tilde{e}. \quad \text{(A9b)}$$

Thus all nine candidates are given in terms of $N,\tilde{N}$ which can be directly obtained from γ.

APPENDIX B: CHARACTERIZATION OF *K*

Here we show that $K(\gamma)$ as defined in Eq. (4.2) coincides with the (real) span of the vectors belonging to the kernels of $\gamma+\tilde{J}_x\gamma^{-1}\tilde{J}_x$. This fact automatically follows from the following.

Lemma 7 [characterization of $K(\gamma)$]. Let $f=f_R+if_I$, where f_R and f_I are real. Then $f\in\ker(\gamma-i\tilde{J}_x)$ iff $f_I=\gamma^{-1}\tilde{J}_xf_R$ and both f_R and f_I belong to the kernel of $\gamma+\tilde{J}_x\gamma^{-1}\tilde{J}_x$.

Proof. Taking the real and imaginary parts of the equation $(\gamma-i\tilde{J}_x)f=0$ we find $\gamma f_R+\tilde{J}_xf_I=0$ and $\gamma f_I-\tilde{J}_xf_R=0$. Since γ must be invertible, we obtain from the second equation that $f_I=\gamma^{-1}\tilde{J}_xf_R$. Using now the first equation we find that $(\gamma+\tilde{J}_x\gamma^{-1}\tilde{J}_x)f_R=0$. Analogously, $(\gamma+\tilde{J}_x\gamma^{-1}\tilde{J}_x)f_I=0$. The same argumentation holds for the other direction of the proof.

[1] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[2] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[4] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998); C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, *ibid.* **70**, 1895 (1993); A. Ekert, *ibid.* **67**, 661 (1991).
[5] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[6] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[7] M. Lewenstein, D. Bruss, J. I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, and R. Tarrach, J. Mod. Opt. **47**, 2481 (2000).
[8] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[9] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999); W. Dür and J. I. Cirac, Phys. Rev. A **61**, 042314 (2000).
[10] See, however, A. Acin, D. Bruss, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **87**, 040401 (2001); e-print quant-ph/0103025; and Ref. [9].
[11] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[12] W. Dür and J. I. Cirac, Phys. Rev. A **62**, 022302 (2000); e-print quant-ph/0002028; P. W. Shor, J. A. Smolin, and A. V. Thapliyal, e-print quant-ph/0005117.
[13] L. Vaidman, Phys. Rev. A **49**, 1473 (1994); S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[14] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).
[15] Ch. Silberhorn, P. K. Lam, O. Weiss, F. König, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **86**, 4267 (2001); e-print quant-ph/0103002.
[16] M. D. Reid, Phys. Rev. A **40**, 913 (1989).
[17] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
[18] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[19] G. Giedke, L.-M. Duan, J. I. Cirac, and P. Zoller, Quant. Inf. Comp. (to be published); e-print quant-ph/0104072.
[20] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001); e-print quant-ph/0009118.
[21] G. Vidal and R. F. Werner, e-print quant-ph/0102117.
[22] G. Giedke, B. Fraus, M. Lewenstein, and J. I. Cirac, e-print quant-ph/0104050.
[23] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000).
[24] P. van Loock and S. L. Braunstein, Phys. Rev. A **63**, 022106 (2001).
[25] To be precise, we should define J with an index n to keep track of the dimension of the space $\mathbb{R}^{2n}$ on which it acts. But since n will always be clear from the context we will omit this index and just use J to make the expressions more readable.
[26] J. Manuceau and A. Verbeure, Commun. Math. Phys. **9**, 293 (1968).
[27] A linear transformation S on phase space is called *symplectic* if it preserves J, i.e., if $SJS^T=J$ holds. The symplectic transformations contain those physical operations on CV states that can currently be routinely realized in the laboratory. They comprise all unitary operations generated by a Hamiltonian quadratic in the canonical operators X_k, P_k, i.e., in quantum optical terms, beam splitter, phase shifter, and squeezer.
[28] In the following, it is convenient to use the notation $A\oplus B$ for block-diagonal matrices: if A and B are $n\times n$ and $m\times m$ square matrices, respectively, then $A\oplus B$ is the $(n+m)\times(n+m)$ square matrix $\left(\begin{smallmatrix}A & 0\\ 0 & B\end{smallmatrix}\right)$.
[29] G. B. Folland, *Harmonic Analysis in Phase Space* (Princeton University Press, Princeton, 1989).
[30] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000).
[31] The following definitions assume that $L,\tilde{L}\neq 0$. [If one of them is 0, the corresponding ellipse degenerates into a circle around (0,0) and we can take an arbitrary $L\neq 0$ to make sense of P_L.] The criterion is not affected by this assumption, since it relies on Ineqs. (3.21).
[32] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000); e-print quant-ph/0005014.
[33] In the case $L'=0$ the borders of the ellipses either do not intersect at all or coincide. In both cases we have to look for solutions among the remaining seven candidates.

A States and Transformations

This appendix collects a number of definitions and lemmas on the Hilbert spaces, algebras, and transformations that are the main object of study of the present thesis.

We consider systems composed of n distinguishable infinite dimensional subsystems, each with Hilbert space $\mathcal{H}_0 = \mathrm{L}^2(\mathbb{R})$. These subsystems are referred to as *modes* [3] and the Hilbert space of the whole n-mode system is $\mathcal{H} = \mathrm{L}^2(\mathbb{R}^n)$. To each mode belong the two (dimensionless) canonical observables $X_k, P_k, k = 1, \ldots, n$ (also called *quadrature operators* in the quantum optical literature) with commutation relation

$$[X_k, P_k] = i.$$

Defining $R_k = X_k, R_{n+k} = P_k$ these commutation relations can be conveniently summarized as

$$[R_k, R_l] = -iJ_{kl}, \quad k, l = 1, ..., 2n \tag{16}$$

using the antisymmetric $2n \times 2n$ matrix

$$J_n = \begin{pmatrix} \mathbb{O}_n & -\mathbb{1}_n \\ \mathbb{1}_n & \mathbb{O}_n \end{pmatrix}. \tag{17}$$

which is sometimes called the *complex structure*. Here $\mathbb{O}_n, \mathbb{1}_n$ are the n-dimensional zero and identity matrix, respectively. We omit the index n whenever the dimension is clear from the context in order to make the expressions more readable. From the quadratures we define *creation and annihilation operators* $a_k^\dagger, a_k$ for the kth mode in the usual way:

$$a_k = \frac{X_k + iP_k}{\sqrt{2}}, \quad a_k^\dagger = \frac{X_k - iP_k}{\sqrt{2}}, \tag{18}$$

implying $[a_k, a_k^\dagger] = \mathbb{1}$. The unbounded operators $R_k, k = 1, \ldots 2n$ generate all the observables of the n-mode quantum system. But it is often useful to consider a bounded (unitary) family of operators, the *Weyl operators* $\mathcal{W}(x)$ instead, which are defined for all $x \in H := \mathbb{R}^{2n}$ in terms of the R_k by

$$\mathcal{W}(x) = \exp[-ix^T R]. \tag{19}$$

The Weyl operators satisfy the exponentiated form of the canonical commutation relation, see, e.g., [79]:

$$\mathcal{W}(x)\mathcal{W}(y) = e^{-\frac{i}{2}\sigma(x,y)}\mathcal{W}(x+y) = e^{-i\sigma(x,y)}\mathcal{W}(y)\mathcal{W}(x), \tag{20}$$

also called the *Weyl relations*. Here $\sigma(x, y) := x^T Jy$. This is a *symplectic form* (cf. [79]) and (H, σ) forms a symplectic space, the classical phase space.

The Weyl operators generate the C*-algebra of canonical commutation relations (CCR- or Weyl-algebra), the algebra of (bounded) observables on $\mathcal{H} \equiv \mathrm{L}^2(\mathbb{R}^n)$. This and the commutation relation Eq. (20) imply that a state ρ on $\mathcal{H}$ is completely determined by the expectation values of all the $\mathcal{W}(x)$, i.e. by its *characteristic function*

[3] This name is used since a possible implementation of $\mathrm{L}^2(\mathbb{R}^n)$ are n modes of the electromagnetic field or normal modes of a chain of ions in a harmonic trap. Another promising implementation is the total spin of an ensemble of many polarized atoms[89]

Definition A.1 (Characteristic Function) *The characteristic function χ of the state ρ on $\mathcal{F}_+(H)$ is given by the expectation values of the Weyl operators $\mathcal{W}(x)$*

$$\chi(x) = \mathrm{tr}[\rho\mathcal{W}(x)]. \tag{21}$$

In fact, the density matrix of ρ can be written in terms of χ and the Weyl operators as

$$\rho = (2\pi)^{-n} \int_{\mathbb{R}^{2n}} \chi(x)\mathcal{W}(-x)\, dx. \tag{22}$$

The expectation values of all polynomials in R_k can be obtained from χ by differentiation[4]. E.g., we have for the mean values of the quadratures $\langle R_k \rangle$

$$\mathrm{tr}(R_k\rho) := (-i)\frac{\partial}{\partial t}\chi_\rho(te_k)|_{t=0} \tag{23}$$

and in general for the mth order correlations $\langle R_{k_1} \dots R_{k_m} \rangle$

$$\mathrm{tr}\left(\Pi_{k=1}^m R_{k_i}\rho\right) = (-i)^m \frac{\partial^m}{\partial t_1 \dots \partial t_m} \mathrm{tr}\left[\mathcal{W}(t_1 e_{k_1}) \dots \mathcal{W}(t_m e_{k_m})\rho\right] |_{t_1=\dots=t_m=0}. \tag{24}$$

Using the Weyl relations Eq. (20) these can be expressed via the characteristic function as

$$(-i)^m \frac{\partial^m}{\partial t_1 \dots \partial t_m} \left(\exp[-\frac{i}{2}\sum_{j<l} t_j t_l \sigma(e_{k_j}, e_{k_l})]\chi(\sum_l t_l e_{k_l}) \right) |_{t_1=\dots=t_m=0}.$$

Of particular importance in the following are the second order correlations ($m = 2$), which form the $2n \times 2n$ *correlation matrix* (or covariance matrix) (CM) γ. In general, a (analytical) state ρ on $\mathcal{H}$ is determined by *all* the mth order correlations. But for the important class of *Gaussian states*, the first and second moments are sufficient to characterize the state completely. Moreover, Gaussian states are by far the most easily prepared states of the physical systems currently considered for CV quantum information and, in fact, comprise nearly all the genuine CV states that can be generated in the lab with present technology. This is directly related to the fact that the set of quantum operations on $\mathcal{H}$ that can be performed in practice is essentially limited to *linear transformations*, i.e. transformations generated by Hamiltonians that are quadratic in the canonical operators X_k, P_k. Because of this fortunate coincidence of mathematical simplicity and experimental relevance these states and transformations have been considered almost exclusively in CV quantum information and so does this Thesis. This following subsection collects results and conventions related to Gaussian states that are used in the main parts of the Thesis.

A.1 Gaussian States

Definition A.2 (Gaussian States) *A state ρ is called* Gaussian *or* quasifree, *if its characteristic function is Gaussian, i.e. it is of the form*

$$\chi(x) = \exp\left[-\frac{1}{4}x^T\gamma x + id^T x\right] \tag{25}$$

[4]More precisely, these expectation values exist and are given by Eq. (24) for all *analytical states* on CCR(H), i.e., states for which $\mathbb{R} \ni t \mapsto \phi(\mathcal{W}(tx))$ is analytical for all $x \in H$; cf. [79].

for a real, strictly positive, symmetric $2n \times 2n$ *matrix* γ *and* $d \in \mathbb{R}^{2n}$.

The *displacement* d is given by Eq. (23) and the *correlation matrix* γ by Eq. (24). Because of its importance in the remainder of this section we give the relation of the displacement and the correlation matrix to the moments of the R_k's explicitely. From Eqs. (24) and (25) it follows for $m = 1$ that

$$d_k = \mathrm{tr}(\rho R_k), \tag{26a}$$

and for $m = 2$ that

$$\gamma_{kl} = 2\mathrm{tr}\left[\rho(R_k - d_k)(R_l - d_l)\right] + iJ_{kl}. \tag{26b}$$

Not every matrix γ is the correlation matrix of a physical state. Rather, it has to satisfy one of the following equivalent conditions.

Lemma A.1 (Correlation Matrix of a Physical State) *The following conditions are equivalent:*
(i) γ *defines a state via Eq. (25)*
(ii) γ *satisfies*

$$\gamma + iJ \geq 0. \tag{27a}$$

(iii) γ *satisfies the inequality*

$$J\gamma J^T \geq \gamma^{-1}; \tag{27b}$$

(iv) γ *is of the form*

$$\gamma = S(D \oplus D)S^T, \tag{27c}$$

where $D \geq \mathbb{1}$ *has diagonal form and* S *satisfies* $SJS^T = J$, *cf. Subsec. A.2.*

Proof: (i)⇔(ii) see [79, Lemma 3.2]; (ii)⇔(iii) follows from the Lemmas A.11 and A.12, p. 93; (iv)⇒(ii) is seen by direct calculation, using that $S^{-1}J(S^{-1})^T = J$ and $d \geq iJ$; (ii)⇒(iv) follows from $\gamma = \gamma^T > 0$ and from symplectic diagonalization (Lemma A.13, p. 93). ∎

Pure Gaussian states are easily characterized:

Lemma A.2 (Pure Gaussian States) *A Gausian state with CM* $\gamma \geq iJ$ *is pure iff one of the following (equivalent) conditions hold:*
(i) $\det\gamma = 1$.
(ii) $\gamma = S^T S$ *for some* $s \in Sp(n)$.
(iii) $\gamma J \gamma J^T = \mathbb{1}$.

Proof: see, e.g., [78, 77].

Examples for the most important families of one-mode Gaussian states include (see, e.g., [81] for details):

- the *thermal states* ρ_T of temperature $T \geq 0$

$$\gamma_T = (1 - e^{-\kappa})^{-1}\mathbb{1}, \quad d = 0, \tag{28}$$

where $\kappa = \frac{\hbar\omega}{k_B T}$,

- the *coherent states* $|\alpha\rangle$ with amplitude $\alpha \in \mathbb{C}$

$$\gamma = \mathbb{1}, \quad d = \sqrt{2}(\mathrm{Re}\alpha, \mathrm{Im}\alpha)^T, \tag{29}$$

  $|0\rangle\langle 0| \equiv \rho_{T=0}$ is called the *vacuum state*.

- and the *squeezed states* with squeezing $r \in \mathbb{R}$

$$\gamma = R(\theta)^T \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^2 r \end{pmatrix} R(\theta), \quad d \in \mathbb{R}^2, \tag{30}$$

  where $R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is a rotation by θ in the phase plane. For $d = 0$ these states are called *squeezed vacuum states*. In such a state the variance of the operator $X_\theta := \cos\theta X + \sin\theta P$ is reduced (for $r > 0$) by a factor of e^r, while the variance of canonically conjugate operator $P_\theta := \cos\theta P - \sin\theta X$ is increased (stretched) by the same factor such that the product of the two is consistent with the minimal value permitted by the uncertainty relation $\left\langle (\Delta X_\theta)^2 \right\rangle \left\langle (\Delta P_\theta)^2 \right\rangle \geq \frac{1}{4}$.

- The "*computational basis states*" $|x\rangle, x \in \mathbb{R}$ used in [17, 18] for quantum computation with continuous variables are defined as the (improper) eigenstates of X

$$X|x\rangle = x|x\rangle \tag{31}$$

  They can be approximated by *displaced*, strongly squeezed vacua with $r \to \infty$ and $d = (x, 0)^T$.

Given two states ρ, ρ' their *overlap* $\mathrm{tr}(\rho\rho')$ is a useful quantity to quantify the "closeness" of two states. If ρ is pure then $\mathrm{tr}(\rho\rho')$ is also called the *fidelity* of ρ' with respect to ρ and denoted by $F_\rho(\rho')$. The fidelity takes values in $[0, 1]$ and gives the probability with which ρ' "will behave as if it were ρ" in an experiment. For Gaussian states the overlap can be directly calculated from the CM and displacement of ρ, ρ'.

Lemma A.3 (Overlap of two Gaussian states) *The overlap* $\mathrm{tr}(\rho\rho')$ *between two n mode Gaussian states with correlation matrices* γ, γ' *and displacements* d, d'*, resp., is given by*

$$\left[\det\left(\frac{\gamma+\gamma'}{2}\right)\right]^{-1/2} \exp\left[-(d-d')^T(\gamma+\gamma')^{-1}(d-d')\right].$$

PROOF: [76] ∎

Clearly, the Gaussian state ρ' that maximizes the overlap with the Gaussian state with ρ (with CM γ and displacement d) has always the same displacement $d' = d$ as ρ.

The above formula directly provides a simple expression for the *purity* of Gaussian states. The purity of ρ is defined as $\mathcal{P}(\rho) = \mathrm{tr}(\rho^2)$ and $\mathcal{P}(\rho) = 1$ iff ρ is pure. For a Gaussian state with CM γ we get

$$\mathcal{P}(\gamma) = (\det\gamma)^{-1/2}. \tag{32}$$

Lemma A.4 (Decomposition of the Correlation Matrix) *Every matrix γ is of the form*

$$\gamma = S^T \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} S, \tag{33}$$

where S is a symplectic matrix and $D \geq \mathbb{1}$ is a positive diagonal matrix.

PROOF: Follows from $\gamma = \gamma^T > 0$ and Lemma A.13. ∎

As becomes clear in the following subsection, the physical interpretation of this is that every quasifree state can be obtained from a thermal state (described by the diagonal correlation matrix $\mathbb{1}_2 \otimes D$) by performing a unitary *quasifree transformation* U_S. More on the preparation of Gaussian states can be found on p. 85.

Other "representations" of ρ

Besides the characteristic function there are additional phase space distributions that uniquely describe a state on $\mathcal{H}$ and will be used in the following. Particularly useful is the *Wigner function* W. One way to define it is via the characteristic function χ: The Wigner function is the symplectic Fourier transform of the characteristic function, namely

$$W(x) := \left(\frac{1}{2\pi}\right)^{2n} \int_{\mathbb{R}^{2n}} e^{i\sigma(x,v)} \chi(v) dv. \tag{34}$$

Using Lemma A.10 it follows that the Wigner function of a quasifree state is a Gaussian:

$$W(x) = \frac{1}{\pi^n} \frac{1}{\sqrt{|M_W|}} \exp\left[-(x - d_W)^T M_W (x - d_W)\right], \tag{35}$$

where the Wigner correlation matrix M_W and the Wigner displacement d_W are related to γ, d by

$$\begin{aligned} M_W &= J\gamma^{-1}J^T, \\ d_W &= Jd_\chi, \end{aligned} \tag{36}$$

thus with Ineq. (27b) we see that a symmetric matrix M is a proper Wigner correlation matrix if and only if $1 \geq M_W > 0$ and

$$(M_W)^{-1} \geq J M_W J^T. \tag{37}$$

For some calculations the *normally ordered characteristic function*

$$\chi_N(x) := \operatorname{tr}\left[: \mathcal{W}(x) : \rho\right] = \chi(x) e^{-\frac{1}{4}\|x\|^2} \tag{38}$$

is useful. Here $: \mathcal{W}(x) :$ denotes the normally ordered Weyl operator

$$: \mathcal{W}(x) := e^{-i\frac{x_1 + ix_2}{\sqrt{2}} a^\dagger} e^{-i\frac{x_1 - ix_2}{\sqrt{2}} a},$$

and the last equality in Eq. (38) follows from the Baker-Campbell-Hausdorff formula

$$e^{A+B} = e^A e^B e^{-[A,B]/2}, \tag{39}$$

which holds whenever $[A, B]$ commutes with both A and B. For Gaussian states we clearly have

$$\chi_N(x) = \exp\left[-\frac{1}{4}x^T M_N x + i d_N^T x\right], \tag{40}$$

where

$$\begin{array}{rcl} M_N & = & \gamma - \mathbb{1}, \\ d_N & = & d. \end{array} \tag{41}$$

It is also useful to relate the *position representation* $\rho(x, y) = \langle x|\, \rho\, |y\rangle$ of a Gaussian state ρ to its Wigner function. Writing $x = (q, p)$ we have according to the definition of the Wigner function (e.g. [80])

$$W(q,p) = \left(\frac{1}{\pi}\right)^n \int_{\mathbb{R}^n} d^n u \rho(q+u, q-u) e^{-i2pu}$$

$q, p \in \mathbb{R}^n$ it follows that

$$\rho(x,y) = \frac{1}{2^n}\int_{\mathbb{R}^n} d^n p W(\frac{x+y}{2}, \frac{p}{2}) e^{i\frac{x-y}{2}p}, \tag{42}$$

and for a Gaussian state with Wigner correlation matrix

$$M_W = \begin{pmatrix} M_x & M_{xp} \\ M_{xp}^T & M_p \end{pmatrix} \tag{43}$$

the position representation takes the form

$$\rho(x,y) = \exp\left[-\frac{1}{4}\begin{pmatrix} x \\ y \end{pmatrix}^T M_{pos} \begin{pmatrix} x \\ y \end{pmatrix}\right],$$

where

$$\begin{aligned} M_{pos} &= \begin{pmatrix} M_x + \frac{1}{M_p} & M_x - \frac{1}{M_p} \\ M_x - \frac{1}{M_p} & M_x + \frac{1}{M_p} \end{pmatrix} \\ &\quad - \begin{pmatrix} M_{xp}\frac{1}{M_p}M_{xp}^T & M_{xp}\frac{1}{M_p}M_{xp}^T \\ M_{xp}\frac{1}{M_p}M_{xp}^T & M_{xp}\frac{1}{M_p}M_{xp}^T \end{pmatrix} + i \begin{pmatrix} M_{xp}\frac{1}{M_p} + \frac{1}{M_p}M_{xp}^T & -M_{xp}\frac{1}{M_p} + \frac{1}{M_p}M_{xp}^T \\ M_{xp}\frac{1}{M_p} - \frac{1}{M_p}M_{xp}^T & -M_{xp}\frac{1}{M_p} - \frac{1}{M_p}M_{xp}^T \end{pmatrix} \end{aligned}$$

Conversely, a Gaussian state with

$$M_{pos} = \begin{pmatrix} M_1 & M_{12} \\ M_{21} & M_2 \end{pmatrix}$$

has the Wigner correlation matrix M_W as in Eq. (43), with

$$\begin{array}{rcl} M_p & = & 2\left[\mathrm{Re}(M_1 - M_{12})\right]^{-1} \\ M_{xp} & = & \mathrm{Im}\,(M_1 - M_{12})\left[\mathrm{Re}(M_1 - M_{12})\right]^{-1} \\ M_x & = & \mathrm{Re}\,(M_1) - M_p^{-1} + M_{xp}M_p^{-1}M_{xp}^T \end{array}$$

Another useful representation is that of the density matrix of a Gaussian state as the exponential of a quadratic expression in the quadrature operators.

$$\rho \propto \exp\left[-\frac{1}{2}R^T \Gamma R\right] \tag{44}$$

(for zero-mean states). The matrix Γ is simply related to the correlation matrix γ of ρ. Using Lemma A.1 (iv), $\gamma = S^T D T$ and the fact [80] that the thermal state of temperature T has the density matrix

$$\rho_T = (1-e^{-\kappa})\exp\left[-\kappa a^\dagger a\right] = 2\sinh(\kappa/2)\exp\left[-\frac{1}{2}\kappa(X^2+P^2)\right], \tag{45}$$

where $\kappa = \frac{\hbar\omega}{k_B T}$ and k_B Boltzmann's constant has CM $\gamma_T = \tau\mathbb{1}$, where $\tau = (1-e^{-\kappa})^{-1}$ we can relate

$$\Gamma_T = \kappa\mathbb{1} \leftrightarrow \gamma_T = (1-e^{-\kappa})^{-1}\mathbb{1}. \tag{46}$$

From this it follows that the Gaussian state with CM $\gamma = S^T(\mathcal{T}\oplus\mathcal{T})S$, where $\mathcal{T}$ is the diagonal matrix with entries τ_k, has a "quadrature operator representation" as in Eq. (44) with

$$\Gamma = S^{-1}(\mathcal{K}\oplus\mathcal{K})(S^{-1})^T, \tag{47}$$

where $\mathcal{K}$ is diagonal with entries κ_k. This can be proved by observing that the state with CM $\gamma' = S^T\gamma S$ is obtained from that with CM γ through a unitary operation $\rho \to U_S \rho U_S^\dagger$ and, as seen below (cf. Eq. (51)), $U_S R_k U_S^\dagger = \sum_l (S^{-1})_{lk} R_l$. From Eq. (44) it is straightforward to rewrite ρ using creation and annihilation operators ("$a - a^\dagger$-representation"):

$$\rho \propto \exp\left[-\frac{1}{4}(a_1, a_1^\dagger, a_2 \ldots, a_n, a_n^\dagger)^T M_a (a_1, a_1^\dagger, a_2 \ldots, a_n, a_n^\dagger)\right], \tag{48}$$

with

$$M_a = \begin{pmatrix} \mathbb{1} & i\mathbb{1} \\ \mathbb{1} & -i\mathbb{1} \end{pmatrix}^T \Gamma \begin{pmatrix} \mathbb{1} & i\mathbb{1} \\ \mathbb{1} & -i\mathbb{1} \end{pmatrix}. \tag{49}$$

E.g., the thermal state ρ_T has a simple form in this representation ($\kappa = \hbar\omega/k_B T$):

$$\rho_T = (1-e^{-\kappa})e^{-\kappa a^\dagger a}.$$

A.2 Linear Transformations

This Subsection collects some definitions and lemmas on an important subset of transformations on $\mathcal{B}(\mathcal{H})$, closely related to Gaussian states.

A.2.1 Unitary Linear Transformations

Unitary operations on $\mathcal{H}$ that transform the canonical operators R_k (cf. p. 76) into a linear combinations of all the R_l's

$$URU^\dagger = MR$$

are in quantum optics often called *linear transformations* (LTs). They are of particular importance, since most unitary time-evolutions that can currently be realized experimentally belong to this class. Not all matrices M are compatible with the unitarity of U, rather, in order to preserve the commutation relations Eq. (16) it is necessary and sufficient for M to be *symplectic*.

Definition A.3 (Symplectic Map) *A map $S : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ is called symplectic if for J as in Eq. (17) it holds that*

$$SJS^T = J. \tag{50}$$

We then write $S \in Sp(n)$.

Note that $S \in Sp(n)$ preserves the symplectic form σ (cf. Eq. (20)), i.e. $\sigma(Sx, Sy) = \sigma(x, y)$ for all $x, y \in \mathbb{R}^{2n}$. Also observe that Eq. (50) implies that if S is symplectic then $\det S = 1$ and both S^{-1} and S^T are symplectic as well.

This prepares the definition of linear transformations, which we introduce by their action on the Weyl operators.

Definition A.4 (Linear Transformations (LT)) *Unitary operations U_S on $\mathcal{B}(\mathcal{H})$ defined by*

$$U_S^\dagger \mathcal{W}(x) U_S = \mathcal{W}(Sx) \tag{51}$$

where $S \in Sp(n)$ are called linear transformations*. (Sometimes also* linear Bogoliubov transformations *or* quasifree transformations*.)*

Clearly, Eq. (51) implies that $U_S^\dagger = U_{S^{-1}}$ and with Eq. (19) that

$$U_S^\dagger R U_S = S^T R, \tag{52}$$

for $R = (X_1, X_2, \ldots, X_n, P_1, \ldots, P_n)^T$. For a state ρ we have that

$$\chi_{U_S \rho U_S^\dagger}(x) = \operatorname{tr}\left[U_S \rho U_S^\dagger \mathcal{W}(x)\right] = \chi(Sx). \tag{53}$$

Note that for a Gaussian state with CM γ and displacement d it follows that $\tilde{\rho} = U_S \rho U_S^\dagger$ is still a Gaussian state with CM $\tilde{\gamma} = S\gamma S^T$ and $\tilde{d} = S^T d$.

These transformations are particularly interesting, because there exists a selfadjoint operator H_S that is *quadratic in the field operators* such that

$$U_S = \exp\left[iH_S\right]$$

and quadratic Hamiltonians are relatively easy to implement experimentally, e.g., in a quantum optical setting.

Restricting to Gaussian states and quasifree transformations reduces the problem of studying states and operations on an infinite dimensional Hilbert space to a more tractable problem in finite dimensions.

Before giving the Hamiltonian H_S that implements U_S, we note two useful ways to decompose an arbitrary symplectic map S.

Lemma A.5 (Decomposition of Symplectic Maps) *(1) Every symplectic S can be decomposed into a positive diagonal matrix M and two orthogonal and symplectic maps O, O' such that:*

$$S = O \begin{pmatrix} M & 0 \\ 0 & M^{-1} \end{pmatrix} O'. \tag{54}$$

(2) In addition, there exists a unique polar decomposition *of S as*

$$S = OS_+ \tag{55}$$

for O orthogonal and symplectic and $S_+ = S_+^T \geq 0$ symplectic. We can write

$$S_+ = \tilde{O} \begin{pmatrix} M & 0 \\ 0 & M^{-1} \end{pmatrix} \tilde{O}^T = \tilde{O} \Big[\cosh(L \oplus L) + \tilde{I} \sinh(L \oplus L) \Big] \tilde{O}^T,$$

with $\tilde{O}$ symplectic and orthogonal, an antilinear involution $\tilde{I} = \tilde{O}[\mathbb{1} \oplus (-\mathbb{1})]\tilde{O}^T$, $M \geq 0$ and diagonal, and $\cosh L = (M + M^{-1})/2$.

(3) Symplectic and orthogonal maps always have the form

$$O = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix}, \tag{56}$$

where $X - iY$ is unitary on $\mathbb{C}^n$.

Proof: (1) see, e.g., [74, 75, 76] and references therein. For (2), see [83]. (3) is seen as follows: being orthogonal and symplectic, O preserves both the symplectic form $\sigma(x, y) = x^T J y$ and the scalar product $\langle x, y \rangle_r = x^T y$ on $\mathbb{R}^{2n}$. Embedding $\mathbb{C}^n$ in $\mathbb{R}^{2n}$ via $\mathbb{C}^n \ni z \leftrightarrow \mathrm{Re}(z) \oplus \mathrm{Im}(z) \in \mathbb{R}^{2n}$ the complex structure J represents "multiplication with i" and thus σ can be seen as the imaginary part of the scalar product on $\mathbb{C}^n$, while $\langle x, y \rangle_r$ represents the real part. If both are preserved, the corresponding linear transformation is unitary. By the above embedding U on $\mathbb{C}^n$ corresponds to

$$O = \begin{pmatrix} \mathrm{Re}U & -\mathrm{Im}U \\ \mathrm{Im}U & \mathrm{Re}U \end{pmatrix} \qquad \text{on } \mathbb{R}^{2n}. \qquad \blacksquare$$

One may extend the class of linear transformations by including the *displacement* of a state, i.e. the maps

$$\chi(x) \overset{D(d)}{\mapsto} \chi(x) e^{+id^T x}. \tag{57}$$

In fact, this transformation is achieved by the Weyl operators: $\mathrm{tr}(\mathcal{W}(d)\rho\mathcal{W}(d)^\dagger \mathcal{W}(x)) = \mathrm{tr}(\rho \mathcal{W}(x)) e^{i(Jd)^T x}$. However, we define the *displacement operator* $D(d)$ slightly differently (in accordance with the use in the quantum optical literature [81]) as follows

$$D(d) := \mathcal{W}(\sqrt{2} J^T d). \tag{58}$$

For a single mode this leads to the usual definition $D(\alpha) := \exp\big[\alpha a^\dagger - \alpha * a\big]$. We will usually include displacements when talking of quasifree transformations.

Before turning to two classes of non-unitary transformations we give a brief review on how these unitary operations may be implemented quantum optically.

A.2.2 Physical realization of quasifree transformations and state generation

Here we list the Hamiltonians which generate the most frequently used linear transformations and give the corresponding symplectic maps S. The transformed quadrature operators $e^{iH}Re^{-iH}$ are then given by S^TR and the CM and displacement of the transformed state $e^{-iH}\rho e^{iH}$ by $(S^T\gamma S, S^Td)$. We consider only ideal realizations, i.e. assume that there is no absorption.

- Beam splitter: $H = \pm\theta(X_2P_1 - X_1P_2)$

$$S_{BS}(\theta) = \begin{pmatrix} \cos\theta & \sin\theta & & \\ -\sin\theta & \cos\theta & & \\ & & \cos\theta & \sin\theta \\ & & -\sin\theta & \cos\theta \end{pmatrix}.$$

  $T = \cos\theta$ and $R = \sin\theta$ are called the transmittivity and reflectivity of the beam splitter, respectively.

- Displacement: $H = r_1X + r_2P, r = (r_1, r_2) \in \mathbb{R}^2$

$$(X, P) \to (X + r_1, P + r_2),$$

$$(\gamma, d) \to (\gamma, d + Jr).$$

  This can be implemented by using a beam splitter of tiny transmittivity $T \to 0$ and a strong coherent beam of amplitude $\alpha \to \infty$ such that $T*\alpha \to r_1 + ir_2$.

- Phase shift: $H = \phi(X^2 + P^2)$

$$R(\phi) = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}.$$

  Since H is essentially the free Hamiltonian of the electromagnetic field a delay of the mode considered (relative to the other modes), e.g., via a longer path in an interferometer or via a phase plate implements the phase shift.

- Squeezer: $H = \pm r(XP + PX)$

$$S_{sq}(r) = \begin{pmatrix} e^{\pm r} & 0 \\ 0 & e^{\mp r} \end{pmatrix}.$$

The first three of these Hamiltonians are sometimes called *passive* LTs to distinguish them from the *active* LTs, which also make use of the squeezing Hamiltonian, which makes use of a higher-order process, e.g., parametric down-conversion.

Given n modes and the ability to apply all of these Hamiltonians to each mode for an arbitrary amount of time it is possible to realize *any* unitary time-evolution generated by a Hamiltonian quadratic in the R_k's but no other. To be able to approximate an arbitrary evolution, it is sufficient to add one Hamiltonian of higher order, e.g., $H = (X^2 + P^2)^2$ [17]. Concatenating only passive

LTs, all unitaries U_O, where O is orthogonal and symplectic, can be constructed [75, 17].

Now it is also clear how to generate Gaussian states. There are two major sources of light used in the lab: The *laser* can be used to produce coherent states $|\alpha\rangle$. (See [86] for a detailed discussion of the state produced by a laser.) Before the advent of the laser, the typical sources of light (such as light bulbs or discharge lamps) produced thermal states.

In view of Lemma A.1, (iv), Lemma A.5 and Eq. (57) it is clear that all Gaussian states can be produced from these two classes of states by applying LTs. O and O' of Eq. (54) can be realized by beam splitters and phase shifters, while the diagonal matrix $M \oplus M^{-1}$ represents the effect of n one-mode squeezers. Thus this decomposition means that every symplectic transformation is a concatenation of linear time-evolutions, a collection of one-mode squeezers, and again linear evolution.

A.2.3 Quadrature Measurements

Consider an n-mode state ρ with Wigner function W. After measuring the x quadrature in the last m modes (result $z \in \mathbb{R}^m$), the state of the remaining modes has the Wigner function

$$W_z(x' = (q', p')) \propto \int_{\mathbb{R}^m} d^m u \; W(\begin{pmatrix} q' \\ z \end{pmatrix}, \begin{pmatrix} p' \\ u \end{pmatrix}). \tag{59}$$

For a quasifree state with displacement $d = (d', d'')$ and the $2n \times 2n$ CM

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{60}$$

where the $2(n-m) \times 2(n-m)$ block

$$A = \begin{pmatrix} A_x & A_{xp} \\ A_{xp}^T & A_p \end{pmatrix}$$

refers to the first $n-m$ modes (that are not measured), while the $2m \times 2m$ block B refers to the m measured modes ($C \in M_{2m \times 2(n-m)}$) this implies

$$W_z(x') = e^{-(x'-d')^T \left[A - \binom{B_{px}}{B_p} \frac{1}{C_p} (B_{xp} B_p)\right] (x'-d')} e^{-2\left[\binom{B_x}{B_{xp}} - \binom{B_{px}}{B_p} \frac{1}{C_p} C_{px}\right] (z - d_x'')^T (x'-d')}.$$

Thus the state remains quasifree.

Quadrature measurements can be approximated by homodyne detection [81]. To measure the quadrature operator $X_\theta = \cos\theta X + \sin\theta P$ one proceeds as follows: a strong coherent light field of amplitude $a(\cos\theta + i \sin\theta), a >> 1$ (the so-called local oscillator) is coupled at a 50:50 beam splitter to the signal field that is to be measured. At both output ports of the beam splitter then intensity is measured with photon counters. Subtracting the two results gives (in the limit of infinite a) a result in $\mathbb{R}$ that can be taken to represent the result of an X_θ measurement in the following sense: the statistics of the experiment are (in the limit of strong local oscillator and perfect photo detection) exactly those to be expected from an X_θ measurement [87].

A.2.4 The Effect of Noise

The effect of noise can be described by coupling the system in question to a bath of harmonic oscillators at temperature T with a coupling constant η. It is shown in [88] that in the Markov approximation the reduced state of the system after a time t has the normally ordered characteristic function

$$\tilde{\chi}_N(x,t) = \chi_N(e^{-\eta t}x)e^{-\langle N\rangle||x||^2},$$

where $\langle N\rangle = \left(e^{\beta}-1\right)^{-1}$ is the particle number expectation value in the thermal bath and $\beta = \hbar\omega/(kT)$ gives the temperature.

Thus the normally ordered correlation matrix of a Gaussian state being (for a time t) subject to Markovian thermal noise (each mode coupled to its own reservoir with coupling constant η_k for photon number expectation value $\tau_k = \langle N_k\rangle$) is given by

$$\tilde{M}_N = \mathcal{N} M_N \mathcal{N} + (\mathbb{1} - \mathcal{N}^2)\mathcal{T}, \tag{61}$$

where

$$\mathcal{N}_t = \begin{pmatrix} e^{-\eta_1 t}\mathbb{1}_2 & 0 & \cdots & 0 \\ 0 & e^{-\eta_2 t}\mathbb{1}_2 & & 0 \\ & & \ddots & \\ 0 & 0 & & 0 \\ 0 & \cdots & & e^{-\eta_n t}\mathbb{1}_2 \end{pmatrix},$$

$$\mathcal{T} = \begin{pmatrix} \tau_1\mathbb{1}_2 & 0 & \cdots & 0 \\ 0 & \tau_2\mathbb{1}_2 & & 0 \\ & & \ddots & \\ 0 & 0 & & 0 \\ 0 & \cdots & & \tau_n\mathbb{1}_2 \end{pmatrix}.$$

Thus "application of Markovian noise" enlarges the family of physical operations that leave the set of Gaussian states invariant. From Eqs. (61) and (41) we see immediately the (characteristic function) CM γ of the state after the interaction with the heat bath is

$$\tilde{\gamma} = \mathcal{N}\gamma\mathcal{N} + (\mathbb{1} - \mathcal{N}^2)(\mathbb{1} + \mathcal{T}). \tag{62}$$

Every "noisy" time evolution of a quantum system with Hilbert space $\mathcal{H}$ can be described by a unitary (noiseless) evolution on a larger Hilbert space $\mathcal{H}\otimes\mathcal{E}$ and subsequent "tracing out" the environment $\mathcal{H}_E$. "Tracing out" describes the fact thet the environmental degrees of freedom are considered to be not accessible by experiment, i.e., that all relevant observables are of the form $A\otimes\mathbb{1}_{\mathcal{E}}$. The state $\rho_{red} := \mathrm{tr}_{\mathcal{E}}(\rho)$ is called the *reduced state* of the system. If the composite system is in a Gaussian state, then the state of the reduced system is Gaussian, too, and its CM can be simply obtained from that of the composite system by discarding all rows and columns refering to modes belonging to $\mathcal{E}$. This directly follows from using only Weyl operators of the form $\mathcal{W}(x\oplus 0) = \mathcal{W}(x)\otimes\mathbb{1}_{\mathcal{E}}$. Consequently, for an n-mode Gaussian state with CM γ as in Eq. (60), the reduced state of the first $n-m$ modes has the CM $\gamma_{red} = A$.

Another source of "noise" that maps Gaussian states to Gaussian states is the mixing of states with different γ and d with an appropriate probability distribution P. The simplest example was pointed out in [62], where it was

shown that given two CMs $\gamma_1 \geq \gamma_2$ then the Gaussian state with CM γ_1 can be written as a mixture of Gaussian states with CM γ_2 and displacement x, where x is distributed according to the Gaussian probability distribution

$$P(x) = \exp\left[-x^T \Delta x\right],$$

where $\Delta = (\gamma_1 - \gamma_2)^{-1}$ (in the sense of the pseudo-inverse). In particular it is then clear from Cond. (iv) in Lemma A.1, p. 78 that every Gaussian state is a mixture of pure Gaussian states ($S^T D S \geq S^T S$ for $D \geq 1$).
It is not known (to me) whether the method described above is the only way in which Gaussian states may be mixed to obtain a Gaussian result. (On the other hand, it is clear that there other ways of mixing (any sort of) states to obtain a Gaussian state, e.g., the eigenstates of ρ, which are not Gaussian, but (symplectically transformed) number states (as evident from Eq. (27c), p. 78).

A.3 Bipartite Systems

Most ofthis Thesis deals wioth the properties of *bipartite* systems in Gaussian states. This subsection contains sme useful properties of such states.

The tensor product structure of the Hilbert space of composite quantum systems translates into a *direct sum* on the phase space of those systems. Thus the CM γ of a system composed of n modes at Alice's location and m modes at Bob's ("$n \times m$ system") is a $2n + 2m$ square matrix which we write in the following block matrix form

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}. \tag{63}$$

Here A (B) are $2n$ ($2m$) CMs themselves and describe the reduced state of the system at A (B). The $2n \times 2m$ matrix C describes the (quantum and classical) correlations between A and B. Clearly, the displacement d of the composite system is given by $d_a \oplus d_B$, the direct sum of the individual displacements.

A very important concept when discussing the properties of states of bi- or multipartite systems is local equivalence:

Definition A.5 (Local Equivalence) *Two states ρ, ρ' on $\mathcal{H}_A \otimes \mathcal{H}_B$ are called* locally equivalent[5] *if there exists unitaries U_A, U_B on $\mathcal{H}_A, \mathcal{H}_B$, resp., such that $\rho' = U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$.*

States that are locally equivalent in this sense are identical as far as their entanglement properties are concerned. E.g., Gaussian states with identical CM but different displacements are locally equivalent, since local displacement operations (see p. 84) can convert them into each other. Therefore displacements play no role in our study of entanglement properties of Gaussian states. Next we study local equivalence of states with different CMs.

Using the fact that every positive definite matrix can be diagonalized by a symplectic transformation (see [74]) we can choose $S = S_A \otimes S_B$ such that

$$\begin{aligned} S_A^T A S_A &= D_A \oplus D_A, \\ S_B^T B S_B &= D_B \oplus D_B, \end{aligned}$$

[5] In other contexts different notions of local equivalence are used.

$D_A, D_B \geq \mathbb{1}$. Thus every CM γ brought by local unitary operations to the form

$$\begin{pmatrix} \mathbb{1}_2 \otimes D_A & K \\ K^T & \mathbb{1}_2 \otimes D_B \end{pmatrix}, \tag{64}$$

where $D_{A(B)} \geq \mathbb{1}_n$ is a $n \times n$ ($m \times m$) diagonal matrix. Now consider the case $m = n$. The only transformations that are in general still possible without changing the diagonal blocks are symplectic and orthogonal maps on the individual modes, i.e., phase shifts of the individual modes:

$$O_{x,k} = \begin{pmatrix} \cos\phi_{x,k} & \sin\phi_{x,k} \\ -\sin\phi_{x,k} & \cos\phi_{x,k} \end{pmatrix}, \quad x = \mathrm{A,B}, k = 1, \ldots, n.$$

This allows to diagonalize the 2×2 blocks on the diagonal of K, bringing K to the form

$$K = \begin{pmatrix} c_{11} & 0 & c_{13} & \cdots & & c_{1n} \\ 0 & c_{22} & c_{23} & \cdots & & c_{2n} \\ c_{31} & c_{32} & c_{33} & 0 & c_{35} & \cdots \\ c_{41} & c_{42} & 0 & c_{44} & c_{45} & \cdots \\ \vdots & & & & & \\ c_{n1} & & & \cdots & 0 & c_{nn} \end{pmatrix},$$

thus leaving in general $2n + (4n^2 - 2n) = 4n^2$ independent parameters.

In the case $n = 1$ these O_x are *all* the orthogonal transformations on $\mathbb{R}^2$:

Lemma A.6 (Orthogonal transformations on $\mathbb{R}^2$) *All orthogonal transformations O on $\mathbb{R}^2$ are of the form*

$$O = S \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \tag{65}$$

where S is symplectic.

PROOF: Let $O = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then orthogonality, i.e., $O^T O = \mathbb{1} = O O^T$ implies that $a^2 + b^2 = 1, b^2 = c^2, a^2 = d^2$, and $ac + bd = 0$. From these equations follows (a) in case that $a = 0$ that $d = 0, bc = \pm 1$ or (b) if $a \neq 0$ that $c = -bd/a, d = \pm a, c = \mp b$, i.e.,

$$O = \begin{pmatrix} a & \mp b \\ b & \pm a \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \tag{66}$$

and $a^2 + b^2 = 1$. It is easy to see that $O^T J O = \pm(a^2 + b^2) J = \pm J$, i.e. O is symplectic for the upper sign. ∎

With this result, we can prove the existence of a very simple standard form for all 1×1 Gaussian states. Since states in standard represent all entanglement classes of 1×1 systems (up to local unitaries) we spend some time to study their properties.

Lemma A.7 (Standard Form of Bipartite two-mode Gaussian States) *Every 1×1 Gaussian state with CM γ can be transformed into the state with CM*

$$\gamma_{std} = \begin{pmatrix} n_a & 0 & k_x & 0 \\ 0 & n_a & 0 & k_p \\ k_x & 0 & n_b & 0 \\ 0 & k_p & 0 & n_b \end{pmatrix} \tag{67}$$

$k_x \geq |k_p|$ by local quasifree transformations. The four parameters characterizing this state can be directly calculated for any given matrix γ. Four independent invariants under local quasifree transformations are, e.g.,

$$\begin{aligned} x_1 &= \det A, \\ x_2 &= \det B, \\ x_3 &= \det C, \\ x_4 &= \det \gamma, \end{aligned} \tag{68}$$

and then we have

$$\begin{aligned} n_a &= \sqrt{x_1}, \\ n_b &= \sqrt{x_2}, \\ k_x k_p &= x_3, \\ \alpha := k_x + k_p &= \sqrt{\frac{(\sqrt{x_1 x_2} + x_3)^2 - x_4}{\sqrt{x_1 x_2}}}, \\ k_x &= \frac{1}{2}\left(\alpha + \sqrt{\alpha^2 - 4x_3}\right), \\ k_p &= \frac{1}{2}\left(\alpha - \sqrt{\alpha^2 - 4x_3}\right). \end{aligned}$$

PROOF: From Eq. (64) it follows that both A and B can be made proportional to $\mathbb{1}$ by symplectic transformations S_A, S_B. Then we can always find orthogonal transformations O_A, O_B that effect the singular value decomposition of $\tilde{C} = S_A^T C S_B$ [85] without changing the diagonal blocks. It remains to be shown, that O_A, O_B can be chosen symplectic. Let $K = O_A^T \tilde{C} O_B$ be the singular value decomposition of $\tilde{C}$. Then it is clear from Eq. (65) that

$$\tilde{K} := \begin{pmatrix} 1 & 0 \\ 0 & \sigma \end{pmatrix} K \begin{pmatrix} 1 & 0 \\ 0 & \sigma \end{pmatrix} =: \tilde{O}_A^T C \tilde{O}_B$$

is diagonal, too, and $\tilde{O}_A, \tilde{O}_B$ are symplectic *and* orthogonal. ∎

The parameters n_a, n_b are directly related to the temperature of the reduced state at A resp. B: in standard form, the reduced states are both thermal states (cf. p. 78) with temperatures $kT_{A,B}/\hbar\omega = 1/\ln(1 + 1/n_{a,b})$, i.e. the larger n the higer the temperature. We define symmetric states as those wher the "local temperatures" T_A, T_B are the same:

Definition A.6 (Symmetric Bipartite Gaussian States) *A Gaussian state is called* symmetric*, if $x_1 = x_2$.*
It is called fully symmetric*, if it is symmetric and in addition $k_p = -k_x$.*

For states in standard form it is very easy to check whether the CM γ remains a physical CM under partial transposition.

Lemma A.8 (Conditions on the invariants of a CM) *A matrix γ in standard form (67) is a CM of a physical state if and only if the parameters n_a, n_b, k_x, k_p fulfill*

$$n_a n_b - k_{x,p}^2 \geq 1, \tag{69a}$$

$$d_x d_p + 1 \geq n_a^2 + n_b^2 + 2k_x k_p. \tag{69b}$$

The latter inequality can be expressed in terms of the four invariants x_k:

$$x_4 + 1 - x_1 - x_2 - 2x_3 \geq 0. \tag{70}$$

PROOF: The eigenvalues of $J^T \gamma J - \gamma^{-1}$ for γ as in Eq. (67) are

$$\begin{aligned} e_{1,2} &= \frac{1}{2}(a_x + c_x) \pm \frac{1}{2}\sqrt{(a_x + c_x)^2 - 4(a_x c_x - b_x^2)} \\ e_{3,4} &= \frac{1}{2}(a_p + c_p) \pm \frac{1}{2}\sqrt{(a_p + c_p)^2 - 4(a_p c_p - b_p^2)} \end{aligned}$$

where

$$\begin{aligned} d_{x,p} &:= n_a n_b - k_{x,p}^2, \\ a_{x,p} &:= n_a - \frac{n_b}{d_{x,p}}, \\ c_{x,p} &:= n_b - \frac{n_a}{d_{x,p}}, \\ b_{x,p} &:= k_{p,x} + \frac{k_{x,p}}{d_{x,p}}. \end{aligned}$$

They are all positive iff $a_{x,p} + c_{x,p} \geq 0$ and $a_{x,p} c_{x,p} - b_{x,p}^2 \geq 0$, which implies Eqs. (69). ∎

From this we can obtain a very compact form of the separability criterion for two-mode Gaussian states. If a CM is "partially transposed" this flips the sign of x_3 but leaves the invariants $x_{1,2,4}$ unchanged. Therefore we have

Lemma A.9 (Separability Criterion for 1×1 Gaussian states) *A bipartite two-mode Gaussian state whose CM is characterized by the four invariants x_1, x_2, x_3, x_4 as in Eqs. (68) is separable if and only if*

$$x_4 + 1 - x_1 - x_2 + 2x_3 \geq 0. \tag{71}$$

PROOF: Follows directly from Ineq. (70) and the fact that partial transposition does change the sign of x_3 while it leaves the other invariants unchanged [59]. ∎

From Eq. (36) follows a simple relation between the standard form of the Wigner correlation matrix and the characteristic correlation matrix:

$$\chi_{n_a,n_b,k_x,k_p} \leftrightarrow W_{(n_b,n_a,k_x,k_p)/\sqrt{|\gamma|}}, \tag{72a}$$

$$W_{N_a,N_b,K_x,K_p} \leftrightarrow \chi_{(N_b,N_a,K_x,K_p)/\sqrt{|M_W|}}. \tag{72b}$$

From this it is evident that if a state that is symmetric (according to Def. A.6 then the standard form of its Wigner CM satisfies the same symmetry condition.

Moreover, we can now easily express the physicality and inseparability conditions Ineqs. (70) and (71) in terms of the parameters X_1, X_2, X_3, X_4 defined in analogy to Eqs. (68) for the Wigner CM. It follows that $W_{(N_a,N_b,K_x,K_p)}$ describes a physical state iff

$$X_4 + 1 \geq X_1 + X_2 + 2X_3, \tag{73a}$$

$$D_x, D_p \leq 1, \tag{73b}$$

$$N_a N_b \geq K_x^2, K_p^2, \tag{73c}$$

and it is inseparable iff it is physical and in addition

$$X_4 + 1 < X_1 + X_2 - 2X_3. \tag{74}$$

The two-mode CM in standard form is a central object in continuous variable quantuminformation, therefore we note here some of its elementary properties. The matrix γ of Eq. (67) has the eigenvalues

$$\frac{1}{2}(n_a + n_b) \pm \frac{1}{2}\sqrt{(n_a + n_b)^2 - 4(n_a n_b - k_x^2)}, \tag{75a}$$

$$\frac{1}{2}(n_a + n_b) \pm \frac{1}{2}\sqrt{(n_a + n_b)^2 - 4(n_a n_b - k_p^2)}. \tag{75b}$$

Its *symplectic eigenvalues* (cf. Lemma A.13, p. 93) are

$$\left[n_a^2 + n_b^2 + 2k_x k_p \pm \sqrt{(n_a^2 - n_b^2)^2 + 4(n_a^2 + n_b^2)k_x k_p + 4n_a n_b(k_x^2 + k_p^2)}\right]^{1/2} /\sqrt{2}, \tag{76}$$

where the discriminant can be simplified to

$$(n_a^2 + n_b^2 + 2k_x k_p)^2 - 4[(n_a n_b - k_x^2)(n_a n_b - k_p^2)].$$

Finally, the partially transposed CM [cf. Sec. 7, Eq. (7), p. 8] of $\tilde{\gamma}_A = \Lambda_A \gamma \Lambda_A$ is of interest. If one of its symplectic eigenvalues is smaller than one, then γ is the CM of an inseparable state [59, 62, 23]. The symplectic eigenvalues of $\tilde{\gamma}_A$ are, of course, obtained by just replacing k_p by $-k_p$, i.e., they are

$$\left[n_a^2 + n_b^2 - 2k_x k_p \pm \sqrt{(n_a^2 + n_b^2 - 2k_x k_p)^2 - 4[(n_a n_b - k_x^2)(n_a n_b - k_p^2)]}\right]^{1/2} /\sqrt{2}. \tag{77}$$

It is straight forward to see that the smaller of the two symplectic eigenvalues of $\tilde{\gamma}_A$ is smaller than one iff condition (71) is fulfilled, as it must be.

A.4 Some useful Lemmas

Lemma A.10 (Gaussian Integrals) *Consider a real strictly positive symmetric $n \times n$ matrix A and a vector $b \in \mathbb{C}^n$. Then it holds that*

$$\int_{\mathbb{R}^n} \exp\left[-x^T A x + i2b^T x\right]\, d^n x = \sqrt{\frac{\pi^n}{\det A}} \exp\left[-b^T \frac{1}{A} b\right]. \tag{78}$$

Proof: Eq. (78) follows directly from the well-known one-dimensional formula $\int_{\mathbb{R}} \exp\left[-ax^2 + i2bx\right]\, dx = \sqrt{\frac{\pi}{a}} \exp\left[-\frac{b^2}{a}\right]$ and the orthogonal transformation into the eigenbasis of A. ∎

Now we collect some useful Lemmas on positive matrices, that originally were proved in [71, 60].

We consider a selfadjoint $(n+m) \times (n+m)$ matrix M that we write in block form as

$$M = \begin{pmatrix} A & C \\ C^\dagger & B \end{pmatrix}, \tag{79}$$

where A, B, C are $n \times n, m \times m$, and $n \times m$ matrices, respectively.

Lemma A.11 (Positivity of selfadjoint matrices) *A selfadjoint matrix M as in (79) with $A \geq 0, B \geq 0$ is positive if and only if for all $\epsilon > 0$*

$$A - C\frac{1}{B+\epsilon\mathbb{1}}C^\dagger \geq 0, \tag{80}$$

or, equivalently, if and only if

$$\ker B \subseteq \ker C \tag{81a}$$

and

$$A - C\frac{1}{B}C^\dagger \geq 0, \tag{81b}$$

where B^{-1} is understood in the sense of a pseudo-inverse (inversion on the range).

The last conditions can equivalently be formulated with the roles of A and B exchanged: $\ker(A) \subseteq \ker(C^T)$ *and* $B - C^T A^{-1} C \geq 0$

PROOF: The only difficulty in the proof arises if $\ker B \neq 0$. Therefore we consider the matrices M_ϵ, where B in (79) is replaced by $B_\epsilon = B + \epsilon\mathbb{1}$ ($\epsilon > 0$), which avoid this problem and which are positive $\forall\epsilon > 0$ iff $M \geq 0$. In a second simplifying step we note that $M_\epsilon \geq 0$ $\forall\epsilon > 0$ iff $M'_\epsilon = (\mathbb{1} \oplus B_\epsilon^{-1/2})M(\mathbb{1} \oplus B_\epsilon^{-1/2}) \geq 0$.

Now direct calculation shows the claim: we can write a general $f \oplus g$ as $f \oplus \left[(B_\epsilon^{-1/2}C^\dagger)h + h_\perp\right]$, where $h_\perp$ is orthogonal to the range of $(B_\epsilon^{-1/2}C^\dagger)$. Then $(f\oplus g)^\dagger M'_\epsilon(f\oplus g) = f^\dagger(A - CB_\epsilon^{-1}C^\dagger)f + (f+h)^\dagger CB_\epsilon^{-1}C^\dagger(f+h) + h_\perp^\dagger h_\perp$, which is clearly positive, if (80) holds. With the choice $h_\perp = 0$ and $h = -f$ it is seen that (80) is also necessary.

That the second condition is equivalent is seen as follows: If Ineq. (80) holds $\forall\epsilon > 0$ there cannot be vector $\xi \in \ker B$ and $\xi \notin \ker C$ since for such a ξ we have $\xi^T\left(A - C\frac{1}{B+\epsilon\mathbb{1}}C^\dagger\right)\xi < 0$ for sufficiently small $\epsilon > 0$, and if (81a) holds then (80) converges to (81b). Conversely, if (81a) holds, then $CB^{-1}C^\dagger$ is well-defined and Ineq. (81b) implies it $\forall\epsilon > 0$. ∎

Lemma A.12 *For two real matrices $A = A^T \in M_{n,n}$ and $C = -C^T \in M_{n,n}$, and*

$$M = \begin{pmatrix} A & C \\ C^T & A \end{pmatrix} = M^T \in M_{2n,2n}. \tag{82}$$

we have that

$$M \geq 0 \text{ if and only if } A + iC \geq 0.$$

PROOF: This follows from the observation that M is real, and that for any pair of real vectors $a, b \in \mathbb{R}^n$ we have $(a-ib)^\dagger(A+iC)(a-ib) = (a\oplus b)^T M(a\oplus b)$.∎

Lemma A.13 (Symplectic Diagonalization) *Given $M_{2n}(\mathbb{R}) \ni A = A^T > 0$ there exists $S \in Sp(2n)$ and a diagonal $D \in M_n(\mathbb{R})$ diagonal and strictly positive such that*

$$SAS^T = D \oplus D, \tag{83}$$

where D is diagonal. S and D are unique up to permutations of the eigenvalues of D.

PROOF: We prove the Lemma by construction. Eq. (83) implies that $S = \sqrt{D \oplus D} O \sqrt{A^{-1}}$, where $OO^T = \mathbb{1}$. Then $SJS^T = J$ is equivalent to $OA^{-1/2}JA^{-1/2}O^T = \begin{pmatrix} 0 & D^{-1} \\ -D^{-1} & 0 \end{pmatrix}$. Note that $A^{-1/2}JA^{-1/2}$ is antisymmetric and there always exist $D^{-1} > 0$ diagonal and O orthogonal such that the above equation holds. Thus $S = \sqrt{D \oplus D} O \sqrt{A^{-1}}$ is the symplectic transformation that diagonalizes A. ∎

The eigenvalues of D are called the *symplectic eigenvalues* of A and can be calculated from the eigenvalues of iJA [84].

B Equivalence of the Inseparability Conditions of [23] and [59]

In [23] we consider observables $A_{x,p}, B_{x,p}$ that obey the canonical commutation relations $[A_x, A_p] = i$. Then it is shown that for any separable state ρ the variances of the nonlocal observables

$$u_a = \frac{1}{\sqrt{2}} \left(a A_x \mp a^{-1} B_x \right), \tag{84a}$$

$$v_a = \frac{1}{\sqrt{2}} \left(a A_p \pm a^{-1} B_p \right), \tag{84b}$$

satisfy

$$\left\langle (\Delta u_a)^2 \right\rangle_\rho + \left\langle (\Delta v_a)^2 \right\rangle_\rho \geq a^2 + a^{-2} \tag{85}$$

for all $a > 0$, while for any inseparable state there exists an a such that this inequality is violated.

Simon [59] showed that the Peres-Horodecki criterion (2.2) can be adapted to the continuous case and is a necessary and sufficient condition for inseparability of Gaussian states of two modes. The transpose of a state ρ can, e.g., easily be calculated using the Wigner function. The Wigner function of the transposed state corresponds to that of the original state with the sign of the momentum variables flipped:

$$W_{\rho^T}(q,p) = W_\rho(q,-p). \tag{86}$$

Simon the showed that the state ρ is separable iff the partially transposed state satisfies the generalized uncertainty relations for operators $X(d) \equiv d^T R = d_1 X_A + d_3 P_A + d_2 X_B + d_4 P_B$, that is iff

$$\left\langle (\Delta X(d))^2 \right\rangle_\rho + \left\langle (\Delta X(d'))^2 \right\rangle_\rho \leq |\sigma(d_A, d'_A)| + |\sigma(d_B, d'_B)|, \tag{87}$$

where $d_A = (d_1, d_3), d_B = (d_2, d_4)$, $\Delta X = X - \langle X \rangle$, and $\sigma(x,y) = x^T J y$ is the symplectic form.

For non-Gaussian states (85) and (87) are still necessary conditions for separability. That they are equivalent to each other is seen as follows:

That (85) is implied by (87) is evident for $d = (a, 0, \pm a^{-1}, 0)$ and $d' = (0, a, 0 \mp a^{-1})$. The converse is seen in three steps: (i) if $X(d), X(d')$ violate (87) then $\sigma(d_A, d'_A)\sigma(d_B, d'_B) < 0$, since otherwise the RHS of (87) is equal to $|\sigma(d_A, d'_A) + \sigma(d_B, d'_B)|$, and the inequality with this RHS (Ineq. (8) in [59]) is satisfied for all states. This implies that d_A, d'_A and d_B, d'_B may not be

proportional to each other. (ii) Without loss of generality we can multiply d, d' by $\lambda \in \mathbb{R}$ such that RHS of (87) $= 1$ and $\sigma(d_A, d'_A) > 0$. Then choose $a = \sqrt{\sigma(d_A, d'_A)}$. (iii) For this choice of a there exist symplectic transformations S_A, S_B such that $S_A(a,0) = d_A, S_A(0,a) = d'_A$ and the same for B with $a \to a^{-1}$. Thus with $A_x = X(d_A) = X(S_A[1,0]^T), A_p = X(d'_A) = X(S_A[0,1]^T)$ and $B_x = X(d_B) = X(S_B[1,0]^T), B_p = X(d'_B) = X(S_B[0,1]^T)$ the operators u_a, v_a of Eqs. (84) violate of (85).

C Proof: Symmetrization of npt two-mode Gaussian States

This section contains a more readable extended version of the proof in [61], reprinted in Subsec. 3.2 that all npt Gaussian states can be symmetrized in a way that preserves the npt property.

Consider ρ in Wigner standard form with parameters (N_a, N_b, K_x, K_p). If the state is not symmetric, i.e., $N_a \neq N_b$, it means that one side is (looking at the reduced density matrix) "hotter" than the other. The idea of the symmetrization procedure is to bring it in contact with a (pure) vacuum state to cool it down. Assume that $N_a > N_b$, i.e side B is "hotter" in the above sense. Bob then uses an an ancillary mode in the vacuum state and couples it with his member of the entangled pair via a beam splitter with transmission coefficient $\cos\theta$, to be given below. Then he measures the P quadrature of the ancilla mode. We consider the case that the measurement result is 0. Otherwise a displacement operation conditional on the result brings the state into the desired form of vanishing mean. Before the measurement the three-mode state has the correlation matrix $\tilde{M}$

$$\begin{pmatrix} N_a & 0 & cK_x & sK_x & 0 & 0 \\ 0 & N_a & 0 & 0 & cK_p & sK_p \\ cK_x & 0 & c^2N_b + s^2 & sc(N_b-1) & 0 & 0 \\ sK_x & 0 & sc(N_b-1) & c^2 + s^2N_b & 0 & 0 \\ 0 & cK_p & 0 & 0 & c^2N_b + s^2 & sc(N_b-1) \\ 0 & sK_p & 0 & 0 & sc(N_b-1) & c^2 + s^2N_b \end{pmatrix},$$

where $c = \cos\theta, s = \sin\theta$. Define the block matrices

$$\tilde{M}_{AB} = \begin{pmatrix} N_a & 0 & cK_x & 0 \\ 0 & N_a & 0 & cK_p \\ cK_x & 0 & c^2N_b + s^2 & 0 \\ 0 & cK_p & 0 & c^2N_b + s^2 \end{pmatrix},$$

$$\tilde{M}_{anc} = \begin{pmatrix} c^2 + s^2N_b & 0 \\ 0 & c^2 + s^2N_b \end{pmatrix},$$

and

$$\tilde{M}_{AB,anc} = \begin{pmatrix} cK_x & sK_x & 0 & 0 \\ 0 & 0 & cK_p & sK_p \end{pmatrix}.$$

Then according to section A.2.3 the Wigner function after measuring $p_{anc} = 0$ (and tracing out the ancilla) is given by setting $p_{anc} = 0$ and integrating out x_{anc}. Thus the final correlation matrix given is:

$$M_{out} = \tilde{M}_{AB} - \tilde{M}^T_{AB,anc}|_{p_{anc}=0} \tilde{M}^{-1}_{anc}|_{p_{anc}=0} \tilde{M}_{AB,anc}|_{p_{anc}=0},$$

where the notation $M|_{p_{anc}=0}$ means that all matrix entries relating to p_{anc} are set to zero. Hence M_{out} consists of the 2×2 block matrices

$$(M_{out})_A = \begin{pmatrix} N_a & 0 \\ 0 & N_a \end{pmatrix} - \frac{1}{\nu(\theta)} \begin{pmatrix} s^2 K_x & 0 \\ 0 & 0 \end{pmatrix},$$

$$(M_{out})_B = \begin{pmatrix} c^2 N_b + s^2 & 0 \\ 0 & c^2 N_b + s^2 \end{pmatrix} - \frac{1}{\nu(\theta)} \begin{pmatrix} s^2 c^2 (N_b - 1)^2 & 0 \\ 0 & 0 \end{pmatrix},$$

$$(M_{out})_{AB} = c \begin{pmatrix} K_x & 0 \\ 0 & K_p \end{pmatrix} - \frac{1}{\nu(\theta)} \begin{pmatrix} s^2 c K_x (N_b - 1) & 0 \\ 0 & 0 \end{pmatrix},$$

where we used $\nu(\theta) = s^2 N_b + c^2$. The four parameters $x_1, \ldots, x_4$ after the operation are:

$$X_1 = N_a \frac{N_a + D_x u}{1 + N_b u}, \tag{88a}$$

$$X_2 = N_b \frac{N_b + u}{1 + N_b u}, \tag{88b}$$

$$X_3 = K_x K_p \frac{1}{1 + N_b u}, \tag{88c}$$

$$X_4 = D_x \frac{D_p + N_a u}{1 + N_b u}, \tag{88d}$$

where $u = \tan^2 \theta$. For the resulting state to be symmetric, (i.e. to have $X_1 = X_2$) we have to choose

$$u = \frac{N_a^2 - N_b^2}{N_b - D_x N_a}. \tag{89}$$

Since $u > 0$ this is (in the case $N_a > N_b$ under consideration) only possible, if $N_b - D_x N_a > 0$. That this is the case for all physical states (i.e. for all sets of parameters satisfying (37)) is seen like this: $N_b - D_x N_a > 0 \Leftrightarrow (N_b - D_x N_a)(N_a - D_p N_b) > 0$ (since $N_a > N_b, D_p \leq 1$). Expanding the product this gives $N_a N_b (D_x D_p + 1) - N_a N_b (N_a^2 + N_b^2) + N_a^2 K_x^2 + N_b^2 K_p^2$. Using (37) we see that this is $\geq N_a N_b (N_a^2 + N_b^2 + 2 K_x K_p) - N_a N_b (N_a^2 + N_b^2) + N_a^2 K_x^2 + N_b^2 K_p^2 = (N_a K_x + N_b K_p)^2 \geq 0$. ∎

Thus all physical states can be symmetrized this way, it remains to be shown that inseparability is never lost in this process. The inseparability criterion for the output state can be expressed using the parameters X_k [cf. Ineq. (74)]:

$$I_{out} = X_4 - X_1 - X_2 + 2X_3 + 1 \stackrel{!}{<} 0 \tag{90}$$

Inserting the expressions (88) we get: $(D_x D_p + 1 - N_a^2 - N_b^2 + 2 K_x K_p + 1)/(N_b u + 1) \stackrel{!}{<} 0$. Since the denominator is > 0 and the numerator represents the lhs of Ineq. (74) which is negative iff the original state was inseparable. So the "local temperatures" can always be equalized by local means without changing the inseparability property of the state. Since it is shown in [61] that all symmetric states can be distilled, this proves that all inseparable Gaussian states are distillable. ∎

Using the result of [62] that npt is necessary and sufficient for inseparability of $1 \times n$ Gaussian states, we can extend our proof to cover all those states:

D Entanglement Purification

D.1 A protocol for d-level systems [39]

Let a density matrix ρ and the pure state $|\psi\rangle = \sum_{n,m} a_{nm} |n\rangle \otimes |m\rangle$ fulfill the condition (13), p. 21, where the vectors $|n\rangle$ form an orthonormal basis. The coefficients a_{nm} define a matrix $A = (a_{nm})$ satisfying $AA^\dagger = \mathrm{tr}_B(|\psi\rangle\langle\psi|)$. 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 [82]. Conditional on the measurement outcome corresponding to $AA^\dagger \otimes \mathbb{1}$ we obtain the state

$$\tilde{\rho} = A^\dagger \otimes \mathbb{1} \rho A \otimes \mathbb{1} / \mathrm{tr}(\rho A A^\dagger \otimes \mathbb{1}), \tag{91}$$

which still satisfies (13) 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, (13) implies $\mathrm{tr}(\tilde{\rho} |\Phi_+^N\rangle\langle\Phi_+^N|) > 1/N$.
A state satisfying this inequality can be distilled by a generalization of the recurrence protocol of Ref. [34], 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 $\mathrm{XOR}_N : |k\rangle |l\rangle \mapsto |k\rangle |(l+k) \mathrm{mod} N\rangle$ 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 stated converges to the maximally entangled state $|\Phi_+^N\rangle$. To achieve finite yield one can proceed as follows: after reaching a sufficiently high fidelity the states are locally projected into a 2×2 subspace and then further purified e.g. by hashing protocol of [36].

D.2 Linear Entanglement Purification Protocols

As discussed in Sec. 4 an EPP based on linear transformations would be desirable. Here we present some unsuccessful attempts to construct such a protocol.

D.2.1 "Translating" Qubit-EPPs?

This attempt was motivated by surprising fact that some quantum error correcting codes could be simply "translated" from the qubit to the CV setting [18]. The "dictionary" provided there tells us to replace a qubit CNOT-gate by addition in the computational basis (31) $|x\rangle |y\rangle \mapsto |x\rangle |y+x\rangle$ and the Hadamard transformation ... by the Fourier transformation $|x\rangle \mapsto \int e^{ipx} |p\rangle \, dp$, both LTs. An obvious question to ask is then: Can the protocols of Bennett *et al.*[34] or Deutsch *et al.*[35] be "translated" to the CV case in a similar way?

This is not the case. We considered the protocol [35], since for [34] the realization of the depolarization operation presents a problem as using only LTs for depolarization is not enough. Then in addition to the continuous CNOT-gate the "translation" of the single qubit rotation $|0\rangle \mapsto |0\rangle - i\,|1\rangle\,, |1\rangle \mapsto |1\rangle - i\,|0\rangle$ to the CV case is needed, for which there is no obvious candidate. Using passive linear transformations for this step of the "translated" protocol does not lead to entanglement purification. (Proof for pure states, fully symmetric mixed states).

D.2.2 QEC-enhanced Entanglement Swapping

It has been shown [65] that teleporting one member of a locally prepared (and therefore highly entangled) EPR-pair via a pure, finitely squeezed EPR channel never leads to entanglement purification: the resulting pair is never more entangled than the one used up. The measurements and local transformations needed for CV teleportation [15] are all linear. Therefore if this protocol would work it would, according to Subsec. 4.4.1, increase entanglement with probability 1, contradicting the fact that entanglement cannot be increased on average. ([65] argues like this for a pure "channel" state, but this clearly extends to mixed Gaussian channels, too.)

One might think, however, that the combination of entanglement swapping with quantum error correction might constitute an EPP: the codes introduced by Braunstein [18] can be implemented with quasifree transformations and entanglement swapping requires only homodyne detection. The argument of the previous paragraph doesn't apply here, since now many entangled pairs are used up, to produce one purified pair. Nevertheless, calculations show that using a Gaussian channel and a pure EPR-like state input, this procedure does not lead to EP. This is not due to a failure of the QECCs, which work fine, but to the following: reducing the amount of errors (i.e. increasing the entanglement in the channel) makes it at some point necessary to increase the entanglement of the input state as well – since it has to be more entangled than the channel (otherwise even perfect teleportation would not effect EP). Stronger entanglement means more stronger squeezing, but the stronger the squeezing, the less reliable becomes teleportation; higher order errors are not negligible, can even become dominant.

Consider for simplicity a *symmetric* Gaussian channel state in standard form (i.e., $N_1 = N_2 = N, K_1 = -K_2 = K$). If a state with Wigner function W_{in} is teleported through that channel, the Wigner function of the teleported state is

$$W_{tel}(\xi) = \left(W_{in} * \exp\left(-F||\cdot||^2\right)\right)(\xi) \tag{92}$$

($F = (N_1 + N_2 - K^2)/(N_1 + N_2 - 2K)$). From this we see that

$$W_{tel}(\xi) \propto \int d^2u e^{-F||u||^2} S_{\vec{u}}^{(k)} W_{in}(\xi),$$

i.e., the teleported state is a mixture of displaced input states with Gaussian weight centered at displacement 0. Using

$$\sqrt{\frac{F}{\pi}} e^{-Fx^2} = \frac{1}{2} \sum_{n \geq 0} \left(\frac{1}{2F}\right)^n \frac{1}{2n!!} \delta_0^{(2n)}(x),$$

($\delta_0^{(n)}(x)$ being the nth derivative of the delta function at $x = 0$).

This allows us now to start with a Gaussian six-mode state W_{in} (a pure EPR-pair one member of which has been encoded using the 5-mode code). Then the teleported state will look as follows:

$$\begin{aligned}
\rho_{tel} &= \int d^{10}u \left(\sqrt{\frac{F}{\pi}}\right)^{10} e^{-F||u||^2} \rho(S_{\vec{u}} W_{in}) \\
&= \int d^{10}u \left(\Pi_{k=1}^{10} \frac{1}{2} \sum_{n \geq 0} \left(\frac{1}{2F}\right)^n \frac{1}{2n!!} \delta_0^{(2n)}(x_k) \right) \rho(S_{\vec{u}} W_{in}) \\
&= \sum_{k=1}^{5} \int d^2 u_k e^{-F||u_k||^2} \rho(S_{\vec{u}_k}^{(k)} W_{in}) \\
&+ \int d^{10}u \underbrace{\sum_{n_1, m_1 \geq 0} \cdots \sum_{n_5, m_5 \geq 0}}_{\substack{\text{at least 2 indices w/} \\ \text{diff. subscript} \neq 0}} \Pi_{k=1}^{5} \frac{\left(\frac{1}{2F}\right)^{n_k + m_k}}{(2n_k)!!(2m_k)!!} \delta_0^{(2n_k)}((u_k)_1) \delta_0^{(2m_k)}((u_k)_2) \rho(S_{\vec{u}} W_{in}).
\end{aligned}$$

The first line in the last equation represents the first order errors (and the error-free part) - this can be completely corrected by the QECC. The second line contains all the higher order errors, which cannot be corrected by one layer of QECC.

Note the derivatives of the delta-function of order $\sum_k n_k + m_k \geq 2$. Going to the Wigner representation we see that the error terms are of order

$$\left(\frac{1}{2F}\right)^{n_k + m_k} d^{2m_k} d'^{2n_k},$$

where the d, d' terms come from taking the derivative of the Gaussian and d, d' are of the order of the squeezing in the input state, which is supposed to be larger than that of the channel state, which determines F. Thus for strong squeezing of the input state, the errors of order $\gtrsim 1$ are by no means negligible and therefore QECC does not help.

This argument shows that the usual reasoning for the effectiveness of QECC – demonstrating that the leading order of errors is removed – fails here. This indicates (but does not prove) that no entanglement purification is possible this way. And indded, calculating numerically the fidelity and the coherent teleportation fidelity (see below) of a state "purified" this way shows no improvement.

D.2.3 Random Search for a LEPP

We have performed an extensive numerical search for a general LEPP as described at the beginning of Subsec. 4.4.1, allowing for up to 5 pairs of entangled modes and up to 5 ancillas. This has not produced any example in which the LLTs "improved" the state. In order to evaluate the performance of the LEPP we made use of two quantities, which quantify nonlocal properties of a state ρ: the *coherent teleportation fidelity* $F_{tel}^{coh}(\rho)$, which measures how good the state ρ is as a quantum channel, and the fidelity with respect to the maximally entangled state F_{EPR}, which quantifies how close ρ is to the maximally entangled state $|\mathrm{EPR}_{00}\rangle$.

Both quantities represent only very crude ways to measure the success of EPPs, since neither is an entanglement monotone. Nevertheless in both cases it holds that as $F(\rho)$ approaches 1 the state approaches the desired maximally entangled state $|\mathrm{EPR}_{00}\rangle$.

Overlap with an ideal EPR-state

In the case of qubits, the *fidelity* of state with respect to a maximally entangled state is very useful to quantify entanglement. While it provides an entanglement monotone only when maximized over all maximally entangled states (or, in this case equivalently: maximized over all local transformations of the state) it is useful in particular to prove that an entanglement purification protocol produces asymptotically maximally entangled states.

This motivates us to try out the overlap of a given state ρ with an ideal EPR state (e.g. $|\mathrm{EPR}_{00}\rangle = |x_A + x_B = 0, p_A - p_B = 0\rangle$ the one with Wigner function $\delta(x_A + x_B)\delta(p_A - p_B)$) as a means to quantify the entanglement of ρ.

$$\tilde{F}_{EPR}(\rho) = \langle \mathrm{EPR}_{00}| \, \rho \, |\mathrm{EPR}_{00}\rangle$$

For a Gaussian state with zero mean $\tilde{F}_{EPR}$ is given by

$$\sqrt{\frac{|M|}{|M_A + M'_B + 2M'_{AB}|}}, \tag{93}$$

where $M'_B = \begin{pmatrix} (M_B)_{11} & -(M_B)_{12} \\ -(M_B)_{12} & (M_B)_{22} \end{pmatrix}$ and $M'_{AB} = \begin{pmatrix} -(M_{AB})_{11} & (M_{AB})_{12} \\ -(M_{AB})_{21} & (M_{AB})_{22} \end{pmatrix}$. If M is in standard form, this becomes

$$\sqrt{\frac{(N_1N_2 - K_1^2)(N_1N_2 - K_2^2)}{(N_1 + N_2 - 2K_1)(N_1 + N_2 + 2K_2)}}.$$

Defining the quantities F_1, F_2 as

$$F_{1(2)} = \frac{N_1N_2 - K_{1(2)}^2}{N_1 + N_2 - (+)2K_{1(2)}} \tag{94}$$

we finally get

$$\tilde{F}_{EPR} = \sqrt{F_1F_2}. \tag{95}$$

Teleportation Fidelity

One of the major applications of entangled CV states will probably be the teleportation of CV states, e.g. using the VBK scheme [15] as did the pioneering experiment [16]. Thus the quality with which a state can be teleported using this scheme may serve as a measure of quality for the channel state used (assuming perfect operations[6]).

Using a two-mode Gaussian state in standard form N_1, N_2, K_1, K_2 as a channel, teleportation of a state with Wigner function W_{in} proceeds as follows: Initially we have a three-mode state with Wigner function

$$W_{in}(\xi_{in})W_{ch}(\xi_A, \xi_B) \tag{96}$$

[6]It has been observed [58] that for many typical imperfections teleportation with imperfect operations may be described by teleportation with perfect operations using a (more) noisy channel state.

A couples her two modes at a 50:50 beam splitter to obtain

$$W_{in}(\frac{1}{\sqrt{2}}(\xi_A - \xi_{in}))W_{ch}(\frac{1}{\sqrt{2}}(\xi_A + \xi_{in}), \xi_B) \tag{97}$$

Then Alice measures $X_A = z_1, P_{in} = z_2$, the state of Bob's mode then has the Wigner function

$$\int_{\mathbb{R}^2} d^2r W_{in}(\frac{1}{\sqrt{2}}\begin{pmatrix} z_1 - r_1 \\ r_2 - z_2 \end{pmatrix}),$$
$$\exp\left[-\begin{pmatrix} (z_1+r_1)/\sqrt{2} \\ q_B \end{pmatrix}^T M_q \begin{pmatrix} (z_1+r_1)/\sqrt{2} \\ q_B \end{pmatrix} - \begin{pmatrix} (z_2+r_2)/\sqrt{2} \\ p_B \end{pmatrix}^T M_p \begin{pmatrix} (z_2+r_2)/\sqrt{2} \\ p_B \end{pmatrix}\right]$$

where $w = \sqrt{2}(z_1, -z_2)$. This equals

$$\begin{aligned} &\exp\left[-(M_q)_{22}q_B^2 - (M_p)_{22}p_B^2\right] \int_{\mathbb{R}^2} d^2u W_{in}(u) \\ &\times \exp\left[-(M_q)_{11}(w_1-u_1)^2 - (M_p)_{11}(w_2-u_2)^2 - 2(M_q)_{12}q_B(w_1-u_1) + 2(M_p)_{12}p_B(w_2-u_2)\right] \\ &= \exp\left[-\frac{|M_q|}{(M_q)_{11}}q_B^2 - \frac{|M_p|}{(M_p)_{11}}p_B^2\right]\left(W_{in} * e^{-(M_q)_{11}(\cdot)^2 - (M_p)_{11}(\cdot)^2}\right)(w_1 + \frac{(M_q)_{12}}{(M_q)_{11}}q_B, w_2 - \frac{(M_p)_{12}}{(M_p)_{11}}p_B) \end{aligned} \tag{98}$$

i.e. Bob's state after teleportation is the input state convoluted with a Gaussian, then displaced, stretched, and damped with a Gaussian. In the last step Bob processes his state conditioned on Alice's measurement result, namely he displaces it by (w_1, w_2). Defining diagonal 2x2 matrices O_1, O_2, O_3

$$\begin{aligned} O_1 &= \begin{pmatrix} \frac{|M_q|}{(M_q)_{11}} & 0 \\ 0 & \frac{|M_p|}{(M_p)_{11}} \end{pmatrix} \\ O_2 &= \begin{pmatrix} (M_q)_{11} & 0 \\ 0 & (M_p)_{11} \end{pmatrix} \\ O_3 &= \begin{pmatrix} (M_q)_{12} & 0 \\ 0 & -(M_p)_{12} \end{pmatrix}(O_2)^{-1} \end{aligned}$$

the teleported state can be written as

$$W_{tel}(\xi_B) = e^{-(\xi_B - w)^T O_1 (\xi_B - w)}\left(W_{in} * e^{-\langle \cdot, O_2 \cdot \rangle}\right)[(1 - O_3)w + O_3\xi_B]. \tag{99}$$

Averaging over the measurement results leads to a simple expression for W_{out}. (Note that by performing this average one may deteriorate the overall state, if the teleported mode is entangled with other systems.)

$$\sqrt{\frac{|\tilde{O}|}{\pi^2}}\left(W_{in} * e^{-\langle \cdot, \tilde{O} \cdot \rangle}\right), \tag{100}$$

and

$$\tilde{O} = \begin{pmatrix} \frac{(M_q)_{11}|M_q|}{|M_q| + ((M_q)_{12} - (M_q)_{11})^2} & 0 \\ 0 & \frac{(M_p)_{11}|M_p|}{|M_p| + ((M_p)_{12} + (M_p)_{11})^2} \end{pmatrix}.$$

In the case of W_{ch} in standard form the two entries of $\tilde{O}$ are F_1, F_2 as in Eq. (94) So the output state is the input state convoluted with a Gaussian. Clearly, as $F_k \to \infty$ this state approximates the input state as well as desired.

How to define a fidelity? As discussed in [57] there are many ways to define a meaningful *teleportation fidelity* by choosing a set $\mathcal{S}$ of pure states and considering the fidelity with which these states can be teleported.

The fidelity, i.e. the overlap of the teleported state with a pure input state is given in the Wigner representation as

$$F_{tel}(W_{in}) = 2\pi \int_{\mathbb{R}^2} d^2\xi W_{in}(\xi) W_{tel}(\xi). \tag{101}$$

Now one can define the *$\mathcal{S}$-teleportation fidelity of the channel* $F_{tel}^{\mathcal{S}}(\rho)$ either as the minimum over all states, or, given some a priori distribution on $\mathcal{S}$, as the average over $\mathcal{S}$.

1. $\mathcal{S}_c$ = coherent states
   for $W_{in} = \pi^{-1} \exp\left[-||\xi - \xi_0||^2\right]$ the fidelity of the teleported state is

   $$F_{tel}^{coh}(\xi_0, F) = \left[(1 + \frac{1}{2F_1})(1 + \frac{1}{2F_2})\right]^{-1/2}, \tag{102}$$

   i.e. it is independent of the free parameters ξ_0. Thus in this case, average and minimum teleportation fidelity are the same. In the symmetric case $F_1 = F_2$, hence $F_{tel}^{coh} = 2F/(2F+1)$. The condition for better-than-classical teleportation [57] $F_{tel}^{coh} > 1/2$ translates in this case to $F > 0.5 \Leftrightarrow n + K > 1 \Leftrightarrow \rho$ inseparable.

2. $\mathcal{S}_{s,r}^0$ = squeezed vacuum states with squeezing $\leq r$
   $W_{in}(\xi) = \pi^{-1} \exp\left[-||S\xi||^2\right]$; as mentioned in subsection A.2, S can be written as $S = OS_\lambda O'$, where O, O' are orthogonal and S_λ is diagonal with eigenvalues $\lambda, \lambda^{-1} > 0$. For the fidelity we obtain

   $$F_{tel}^{sqvac,r} = \sqrt{\frac{F_1 F_2}{|\frac{1}{2}S_\lambda^2 + O'FO'^T|}}. \tag{103}$$

   In the special case $F_1 = F_2$ this becomes $\sqrt{(1 + \frac{\lambda^2}{2F_1})(1 + \frac{\lambda^{-2}}{2F_2})}$. Minimum for $\lambda = r_{max}, r_{max}^{-1}$. Averaging over $r \in \mathbb{R}_+$ vanishes.

3. $\mathcal{S}_{s,r}$ = arbitrary squeezed states with squeezing $< r$

   $$W_{in} = \exp\left[-(x-d)^T S^T S (x-d)\right],$$

   S symplectic.

4. another possibility, which is not explored here, is to consider how well *entanglement* is teleported? E.g., one could calculate entanglement fidelity for the case that one member of a zero-mean EPR pair is teleported and use this to measure the quality of the teleportation channel.

To obtain an entanglement monotone, however, it would be necessary to maximize the above expressions over all local transformations. More tractable might be the concept of "linear" or "quasifree" entanglement monotone in which the maximasation is performed over linear transformations and generalized homodyne measurements only. Is it always optimal to take the entangled state ρ_{ch} in standard form? In general not, as shown in [58].

E Notation and Abbreviations

$\oplus$	direct sum (of vector spaces, operators, vectors, ...).
$\otimes$	tensor product (of Hilbert spaces, operators, vectors, ...).
$:=, =:$	definition: the defined object is indicated by the colon
$M \ni x$	same as $x \in M$
$\mathcal{H}, \mathcal{K}, \ldots$	Hilbert spaces
$\mathcal{B}(\mathcal{H})$	bounded linear operators on the Hilbert space $\mathcal{H}$.
$Sp(n)$	symplectic maps on $\mathbb{R}^{2n}$
$M_{n,m}(\mathbb{K})$	n by m matrix with entries in $\mathbb{K} = \mathbb{R}, \mathbb{C}$; $M_n \equiv M_{n,n}$
$\mathcal{W}x$	Weyl operator
ρ	density matrix of a state
J	complex structure on $\mathbb{R}^{2n}$: $\bigoplus_{k=1}^{n} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
Λ_A	partial transposition on phases space: $(q_A, p_A, q_B, p_B) \mapsto (q_A, -p_A, q_B, p_B)$.
$\tilde{M}_A$	$= \Lambda_A M \Lambda_A$.
$\mathbb{1}_n, \mathbb{0}_n$	identity, null operator on $\mathbb{C}^n$
X_k, P_k	canonical operators of the kth mode
R	vector whose components are $X_k, P_k, k = 1, \ldots n$
$\|EPR_{qp}\rangle$	(improper) simultaneous eigenstate of $X_A + X_B$ and $P_A - P_B$ with eigenvalues q, p, resp.
γ	correlation matrix of a Gaussian state
$\chi(x)$	characteristic function
npt, ppt state	state, whose density matrix has (non)positive partial transpose
CM	correlation matrix, see p. 77
LT	linear transformation, see (p. 83)
LLT	local linear transformation
EPP	entanglement purification protocol, see p. 32

References

[1] P. Benioff, The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines, J. Stat. Phys. **22**, pp. 563 (1980).

R. Feynman, Simulating physics with computers, J. Theoret. Phys. **21**, pp.467 (1982).

R. Feynman, Quantum mechanical Computers, Found. Phys. **16**, 507 (1986).

D. Deutsch, Quantum Theory, the Church-Turing principle and the universal quantum computer, Proc. Roy. Soc. A **400**, pp.96-117 (1985).

[2] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, UK (2000).

[3] W.K. Wootters and W.H. Zurek, A single quantum cannot be cloned, Nature **299**, 802 (1982).

[4] for a review on quantum algorithms see [2] or, e.g.,

A. Ekert and R. Josza, Quantum computation and Shor's factoring algorithm, Rev. Mod. Phys. **68**, 733(1996).

P.W. Shor, Introduction to Quantum Algorithms, quant-ph/0005003.

[5] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comp. **26**, 1484 (1997).

[6] L. Grover, Quantum Mechanics Helps in Searching for a Needle in a Haystack, Phys. Rev. Lett. **79**, 325 (1997); quant-ph/9706033.

[7] S. Wiesner, Conjugate Coding, Sigact. News **15**, 78 (1983).

C.H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, in Proc. IEEE International Conference on Computers, Systems, and Signal Processing, IEEE Press, Los Alamitos, Calif. (1984), p. 175.

[8] A. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[9] R.J. Hughes, G.L. Morgan, and C.G. Peterson, Practical quantum key distribution over a 48-km optical fiber network, J. Mod. Opt. **47**, 533 (2000);

P.D. Townsend, Opt. Fiber Technol. **4**, 345 (1998);

[10] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Quantum Cryptography with entangled photons, Phys. Rev. Lett. **84**, 4729 (2000); quant-ph/9912117.

D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol, Phys. Rev. Lett. **84**, 4733 (2000).

W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Quantum Cryptography Using Entangled Photons in Energy-Time Bell States, Phys. Rev. Lett. **84**, 4737 (2000).

[11] A. Einstein, B. Podolsky, N. Rosen, Can Quantum Mechanical Description of Physical reality be considered complete?, Phys. Rev. **47**, 777 (1935).

[12] J.S. Bell, On the problem of hidden variables in quantum theory, Rev. Mod. Phys. **38**, 447 (1996).

[13] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett., **70**, 1895 (1993).

[14] M. Horodecki, Entanglement measures, Quant. Inf. Comp. **1**, 3 (2001).

[15] L. Vaidman, Teleportation of quantum states, Phys. Rev. A **49**, 1473 (1994).

S.L. Braunstein and H.J. Kimble, Teleportation of Continuous Quantum Variables, Phys. Rev. Lett. **80**, 869 (1998).

[16] A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Unconditional Quantum Teleportation, Science **282**, 706 (1998).

[17] S. Lloyd and S.L. Braunstein, Quantum Computing over Continuous Variables, Phys. Rev. Lett. **82**, 1784 (1999).

[18] S.L. Braunstein, Error correction for continuous quantum variables, Phys. Rev. Lett. **80**, 4084 (1998).

S.L. Braunstein, Quantum error correction for communication with linear optics, Nature **394**, 47 (1998).

[19] T.C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 061303R (2000); quant-ph/9907073.
T.C. Ralph, Security of continuous variable quantum cryptography, Phys. Rev. A **62**, 062307 (2000); quant-ph/0007024.

M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000); quant-ph/9909006.

M. Reid, Phys. Rev. A **62**, 062308 (2000); quant-ph/9909030.

S.F. Pereira, Z.Y. Ou, and H.J. Kimble, Quantum communication with correlated nonclassical states, Phys. Rev. A. **62**, 042311 (2000);

N.J. Cerf, M. Levy, and G. van Assche, Quantum key distribution of Gaussian keys with squeezed states, quant-ph/0008058.

[20] D. Gottesman and J. Preskill, Secure quantum key distribution using squeezed states Phys. Rev. A **63** 22309 (2001); quant-ph/0008046

[21] D. Gottesman, A. Kitaev, and J. Preskill, Encoding a qudit in an oscillator, Phys. Rev. A **64**, 012310 (2001); quant-ph/0008040.

[22] Ch. Silberhorn, P.K. Lam, O. Weiss, F. Koenig, N. Korolkova, and G. Leuchs, accepted by Phys. Rev. Lett.; Preprint quant-ph/0103002.

[23] L.-M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, Inseparability criterion for continuous variable systems, Phys. Rev. Lett. **84**, 2722 (2000); quant-ph/9908056.

[24] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989).

[25] A. Peres, Separability Criterion for Density Matrices, Phys. Rev. Lett. **77**, 1413 (1996).

[26] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[27] S.L. Woronowicz, Positive maps of low dimensional matrix algebras, Rep. Math. Phys. **10**, 165 (1976).

[28] P. Horodecki, Separability Criterion and inseparable mixed states with positive partial transpose, Phys. Lett. A **232**, 333 (1997).

[29] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?, Phys. Rev. Lett. **80**, 5239 (1998).

[30] E. Størmer, Positive Linear Maps of Operator Algebras, Acta Math. **110**, 233 (1963).

M.-D. Choi, Positive Linear Maps on C*-Algebras, Can. J. Math. **24**, 520 (1972).

B.M. Terhal, A family of indecomposable positive linear maps based on entangled quantum states, Lin. Al. Apll. **323**, 61 (2000); quant-ph/9810091.

[31] E.M. Rains, Rigorous treatment of distillable entanglement, Phys. Rev. A **60**, 173 (1999).

[32] S. Popescu, Bell's Inequalities and Density Matrices: Revealing "Hidden" Nonlocality, Phys. Rev. Lett. **74**, 2619 (1995).

[33] N. Gisin, Hidden quantum nonlocality revealed by local filters, Phys. Lett. A **210**, 151 (1996).

[34] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996); quant-ph/9511027.

[35] D. Deutsch, A. Ekert, R. Josza, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels, Phys. Rev. Lett. **77**, 2818 (1996); Phys. Rev. Lett. **80**, 2022 (1998); C. Macchiavello, On the analytical convergence of the QPA procedure, Phys. Lett. A **246**, 385 (1998).

[36] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54** 3824 (1996); quant-ph/9604024.

[37] M. Horodecki, P. Horodecki, and R. Horodecki, Inseparable Two Spin-1/2 Density Matrices Can Be Distilled to a Singlet Form, Phys. Rev. Lett. **78**, 574 (1997).

[38] N. Linden, S. Massar, and S. Popescu, Purifying noisy entanglement requires collective measurements, Phys. Rev. Lett. **81**, 3279 (1998).

[39] M. Horodecki, P. Horodecki, Reduction criterion of separability and limits for a class of distillation protocols, Phys. Rev. A **59**, 4206 (1999).

[40] W. Dür, J.I. Cirac, M. Lewenstein, D. Bruß, Distillability and partial transposition in bipartite systems, Phys. Rev. A **61**, 062313 (2000), quant-ph/9910022.

[41] D. DiVincenzo, P.W. Shor, J.A. Smolin, B.M. Terhal, A.V. Thapliyal, Evidence for bound entangled states with negative partial transpose, Phys. Rev. A **61**, 062312 (2000); quant-ph/9910026.

[42] P.W. Shor, J.A. Smolin, B.M. Terhal, Nonadditivity of Bipartite Distillable Entanglement follows from Conjecture on Bound Entangled Werner States, Phys. Rev. Lett. **86**, 2681 (2001); quant-ph/0010054.

[43] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, Phys. Rev. A **53**, 2046 (1996).

H. Bechmann-Pasquinucci, B. Huttner, N. Gisin, Phys. Lett. A **242**, 198 (1998); quant-ph/9708040.

S. Bose, V. Vedral, P. L. Knight, Purification via entanglement swapping and conserved entanglement Phys.Rev. A **60**, 194 (1999).

E.N. Maneva, J.A. Smolin, Improved two-party and multi-party purification protocols, quant-ph/0003099.

J.-W. Pan, C. Simon, C. Brukner, A. Zeilinger, Feasible Entanglement Purification for Quantum Communication, Nature **410**, 1067 (2001); quant-ph/0012026.

G. Alber, A. Delgado, N. Gisin, and I. Jex, Efficient bipartite quantum state purification in arbitrary dimensions, quant-ph/0102035.

[44] P.G. Kwiat, S. Barraza-Lopez, A. Stefanov, and N. Gisin, Experimental entanglement distillation and "hidden" non-locality, Nature **409**, 1014 (2001).

[45] D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, A. Zeilinger, Observation of three-photon Greenberger-Horne-Zeilinger entanglement, Phys. Rev. Lett. **82** 1345 (1999); quant-ph/9810035.

[46] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, Unextendible Product Bases and Bound Entanglement, Phys. Rev. Lett. **82**, 5385 (1999).

[47] W. Dür, J.I. Cirac, and R. Tarrach, Separability and Distillability of Multiparticle Quantum Systems, Phys. Rev. Lett. **83**, 3562 (1999); quant-ph/9903018.

W. Dür, and J.I. Cirac, Classification of multiqubit mixed states: Separability and distillability properties, Phys. Rev. A **61**, 042314 (2000); quant-ph/9911044.

[48] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Classification of mixed three-qubit states, quant-ph/0103025.

[49] N. Linden and S. Popescu, On multi-particle entanglement, Fort. Phys. **46**, 567 (1998); quant-ph/9711016;

J. Kempe, Multi-particle entanglement and its applications to cryptography, Phys. Rev. A **60**, 910 (1999); quant-ph/9902036.

C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin, A.V. Thapliyal, Exact and Asymptotic Measures of Multipartite Pure State Entanglement, Phys. Rev. A **63**, 012307 (2001); quant-ph/9908073.

N. Linden, S. Popescu, B. Schumacher, M. Westmoreland, Reversibility of local transformations of multiparticle entanglement, quant-ph/9912039.

H.A. Carteret and A. Sudbery, Local symmetry properties of pure 3-qubit states, J. Phys. A **33**, 4981 (2000); quant-ph/0001091.

A. Sudbery, On local invariants of pure three-qubit states, J. Phys. A **34**, 643 (2001); quant-ph/0001116.

A. Acín, A. Andrianov, L. Costa, E. Jané, J.I. Latorre, and R. Tarrach, Generalized Schmidt decomposition and classification of three-quantum-bit states, Phys. Rev. Lett. **85**, 1560 (2000); quant-ph/0003050.

H. A. Carteret, A. Higuchi, and A. Sudbery, Multipartite generalisation of the Schmidt decomposition, J. Math. Phys. **41**, 7932 (2000); quant-ph/0006125.

A. Acín, A. Andrianov, E. Jané, and R. Tarrach, Three-qubit pure-state canonical forms, quant-ph/0009107.

H. Barnum and N. Linden, Monotones and invariants for multi-particle quantum states, quant-ph/0103155.

[50] W. Dür, G. Vidal, and J.I. Cirac, Three qubits can be entangled in two inequivalent ways, Phys. Rev. A **62**, 062314 (2000);

[51] M. Hillery, V. Buzek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999); quant-ph/9806063.

W. Tittel, H. Zbinden, and N. Gisin, Experimental demonstration of quantum secret sharing, Phys. Rev. A **63**, 042301 (2001).

[52] H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication, Phys. Rev. Lett. **81**, 5932 (1998); quant-ph/9803056.

W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Quantum repeaters based on entanglement purification, Phys. Rev. A **59**, 169 (1999); quant-ph/9808065.

[53] G. Giedke, H.-J. Briegel, J.I. Cirac, and P. Zoller, Lower bounds for attainable fidelities in entanglement purification, Phys. Rev. A **59**, 2641 (1999); quant-ph/9809043.

[54] H. Aschauer and H.J. Briegel, Secure quantum communication over arbitrary distances, quant-ph/0008051.

[55] D. Bouwmeester, J.-W. Pan, M. Daniel, H. Weinfurter and A. Zeilinger, Experimental Quantum Teleportation, Nature **390**, 575, (1997).

D. Boschi, S. Branca, F. DeMartini, L. Hardy, S. Popescu, Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels, Phys. Rev. Lett. **80**, 1121 (1998).

[56] S.L. Braunstein and A.K. Pati (eds.), *Quantum Information Theory with Continuous Variables*, Kluwer Academic (to be published).

[57] S.L. Braunstein, C.A. Fuchs, and H.J. Kimble, Criteria for Continuous Variable Teleportation, J. Mod. Opt. **47**, 267 (2000); quant-ph/9910030;

S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and P. v. Loock, Quantum versus Classical Domains for Teleportation with Continuous Variables, quant-ph/0012001 (2000).

[58] M. S. Kim and J. Lee, Asymmetric quantum channel for quantum teleportation, Phys. Rev. A **64**, 012309 (2001); quant-ph/0005022.

[59] R. Simon, Peres-Horodecki separability criterion for continuous variable systems, Phys. Rev. Lett. **84**, 2726 (2000); quant-ph/9909044.

[60] G. Giedke, B. Kraus, M. Lewenstein, and J.I. Cirac, Separability Criterion for all bipartite Gaussian States, Phys. Rev. Lett. **87**, 167904 (2001); quant-ph/0104050.

[61] G. Giedke, L.-M. Duan, P. Zoller, and J.I. Cirac, Distillability Criterion for all bipartite Gaussian States, Quant. Inf. Comp. **1**, 79 (2001); quant-ph/0104072.

[62] R.F. Werner and M.M. Wolf, Bound entangled Gaussian States, Phys. Rev. Lett. **86**, 3658 (2001); quant-ph/0009118.

[63] P. Horodecki and M. Lewenstein, Bound Entanglement and Continuous Variables, Phys. Rev. Lett. **85**, 2657 (2000); quant-ph/0001035.

[64] M. Lewenstein, D. Bruß, J.I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, and R. Tarrach, Separability and distillability in composite quantum systems – a primer, J. Mod. Opt. **47**, 2481 (2000), quant-ph/006064.

[65] S. Parker, S. Bose, and M.B. Plenio, Entanglement quantification and purification in continuous variable systems, Phys. Rev. A **61**, 032305 (1999); quant-ph/9906098.

[66] T. Opatrný, G. Kurizki, and D.-G. Welsch, Improvement on teleportation of continuous variables by photon subtraction via conditional measurement, Phys. Rev. A **61**, 032302 (1999); quant-ph/9907048.

[67] L.-M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, Entanglement Purification of Gaussian Continuous Variable Quantum States, Phys. Rev. Lett. **84**, 4002 (2000); quant-ph/9912017.

[68] L.-M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, Physical implementation for entanglement purification of Gaussian continuous-variable quantum states, Phys. Rev. A **62**, 032304 (2000).

[69] P. van Loock and S.L. Braunstein, Multipartite Entanglement for Continuous Variables: A Quantum Teleportation Network, Phys. Rev. Lett. **84**, 3482 (2000).

[70] P. van Loock and S.L. Braunstein, Greenberger-Horne-Zeilinger nonlocality in phase space, Phys. Rev. A **63**, 022106 (2001).

[71] G. Giedke, B. Kraus, M. Lewenstein, and J.I. Cirac, Separability Properties of Three-mode Gaussian States, Phys. Rev. A **64** 052303 (2001); quant-ph/0103137.

[72] P.W. Shor, Fault-tolerant quantum computation, Proceedings of the 37th Symposion on the Foundations of Computation, IEEE Comp. Soc. Press (1996); quant-ph/9605011.

Fault-tolerant quantum computation with constant error, D. Aharonov and M. Ben-Or, Proceedings of the 37th Symposion on the Foundations of Computation, IEEE Comp. Soc. Press (1996); quant-ph/9611025.

E. Knill and R. Laflamme, Theory of quantum error-correcting codes, Phys. Rev. A **55**, 900 (1997).

[73] E. Knill, R. Laflamme, and W.H. Zurek, Resilient Quantum Computation: Error Models and Thresholds, Proc. Roy. Soc. A **454**, 365 (1998); quant-ph/9702058;

[74] G.B. Folland, *Harmonic Analysis in Phase Space*, Princeton University Press, Princeton, 1989.

[75] S.L. Braunstein, Squeezing as an irreducible resource, quant-ph/9904002.

[76] H. Scutaru, Transition Probabilities for Quasifree States, J. Math. Phys. **39**, 6403 (1998).

[77] H. Scutaru, The states with Gaussian Wigner function are quasi-free states, Phys. Lett. A **141**, 223 (1989).

[78] J. Manuceau and A. Verbeure, Quasi-Free States of the C.C.R.–Algebra and Bogoliubov Transformations, Comm. Math. Phys. **9**, 293 (1968).

[79] D. Petz, *An Invitation to the Algebra of Canonical Commutation Relations*, Leuven University Press, Leuven (1990);

[80] C.W. Gardiner and P. Zoller, *Quantum Noise* 2nd ed., Springer-Verlag, Berlin (1999).

[81] D.F. Walls and G.J. Milburn, *Quantum Optics*, Springer-Verlag, Berlin (1994).

[82] C. Helstrom, *Quantum detection and estimation theory*, Associate Press, London (1976).

[83] R. Honegger, A. Rieckers, Squeezing Bogoliubov transformations on the ininite mode CCR-algebra, J. Math. Phys. **37**, 4292 (1996).

[84] G. Vidal and R.F. Werner, A computable measure of entanglement, quant-ph/0102117.

[85] R. Horne, C. Johnson, *Matrix Analysis*, Cambridge University Press, 1985.

[86] K. Mølmer, Optical coherence: A convenient fiction, Phys. Rev. A **55**, 3195 (1997);

T. Rudolph and B.C. Sanders, Requirement of optical coherence for continuous-variable quantum teleportation, quant-ph/0103147;

S.J. van Enk and C.A. Fuchs, The quantum state of a laser field, quant-ph/0104036v2.

[87] H.P. Yuen and H. Shapiro, Quantum statistics of homodyne and heterodyne detection, in *Coherence and Quantum Optics, Proc. of the Fourth Rochester Conference*, L. Mandel and E. Wolf (eds.), Plenum Press, New York (1978), pp. 719-727;

S.L. Braunstein, Homodyne Statistics, Phys. Rev. A **42**, 474 (1990);

W. Vogel and J. Grabow, Statistics of difference events in homodyne detection, Phys. Rev. A **47**, 4227 (1993).

[88] L.-M. Duan and G. Guo, Influence of noise on the entanglement fidelity of states, Quant. Semiclass. Opt. **9**, 953 (1997).

[89] E.S. Polzik, Einstein-Podolsky-Rosen–correlated atomic ensembles, Phys. Rev. A **59**, 4202 (1999).

A.E. Kozekhin, K. Mølmer, and E.S. Polzik, Quantum Memory for Light, Phys. Rev. A **62**, 033809 (2000); quant-ph/9912014.

M.D. Lukin, S.F. Yelin, and M. Fleischhauer, Entanglement of Atomic Ensembles by Trapping Correlated Photon States Phys. Rev. Lett. **84**, 4232 (2000); quant-ph/9912046.

L.-M. Duan, J.I. Cirac, P. Zoller, and E.S. Polzik, Quantum communication between atomic ensembles using coherent light, Phys. Rev. Lett. **85**, 5643 (2000); quant-ph/0003111.

A. Sørensen, L.-M. Duan, J.I. Cirac, and P. Zoller, Many-particle entanglement with Bose-Einstein-Condensates, Nature **409**, 63 (2001); quant-ph/0006111.

L.-M. Duan, A. Sørensen, J.I. Cirac, and P. Zoller, Squeezing and entanglement of atomic beams, Phys. Rev. Lett. **85**, 3991 (2000); quant-ph/0007048.

A. Kuzmich and E.S. Polzik, Atomic Quantum State Teleportation and Swapping, Phys. Rev. Lett. **85**, 5639 (2000).

D.F. Philips, A. Fleischhauer, A. Mair, R.L. Walsworth, and M.D. Lukin, Storage of Light in Atomic Vapor, Phys. Rev. Lett. **86**, 783 (2001); quant-ph/0012138.

C. Liu, Z. Dutton, C.H. Beroozy, and L.V. Hau, Coherent optical information storage in an atomic medium using halted light pulses, Nature **409**, 490 (2001).

Index