REVIEWS OF MODERN PHYSICS, VOLUME 77, APRIL 2005

Quantum information with continuous variables

Samuel L. Braunstein

Computer Science, University of York, York YO10 5DD, United Kingdom

Peter van Loock

National Institute of Informatics (NII), Tokyo 101-8430, Japan and Institute of Theoretical Physics, Institute of Optics, Information and Photonics (Max-Planck Forschungsgruppe), Universität Erlangen-Nürnberg, D-91058 Erlangen, Germany

(Published 29 June 2005)

Quantum information is a rapidly advancing area of interdisciplinary research. It may lead to real-world applications for communication and computation unavailable without the exploitation of quantum properties such as nonorthogonality or entanglement. This article reviews the progress in quantum information based on continuous quantum variables, with emphasis on quantum optical implementations in terms of the quadrature amplitudes of the electromagnetic field.

CONTENTS

I. INTRODUCTION

Quantum information is a relatively young branch of physics. One of its goals is to interpret the concepts of quantum physics from an information-theoretic point of view. This may lead to a deeper understanding of quan-

0034-6861/2005/77(2)/513(65)/$50.00

tum theory. Conversely, information and computation are intrinsically physical concepts, since they rely on physical systems in which information is stored and by means of which information is processed or transmitted. Hence physical concepts, and at a more fundamental level quantum physical concepts, must be incorporated in a theory of information and computation. Furthermore, the exploitation of quantum effects may even prove beneficial for various kinds of information processing and communication. The most prominent examples of this are quantum computation and quantum key distribution. *Quantum computation* means in particular cases, in principle, computation faster than any known classical computation. *Quantum key distribution* makes possible, in principle, unconditionally secure communication as opposed to communication based on classical key distribution.

From a conceptual point of view, it is illuminating to consider *continuous quantum variables* in quantum information theory. This includes the extension of quantum communication protocols from discrete to continuous variables and hence from finite to infinite dimensions. For instance, the original discrete-variable quantum teleportation protocol for qubits and other finite-dimensional systems (Bennett *et al.*, 1993) was soon after its publication translated into the continuous-variable setting (Vaidman, 1994). The main motivation for dealing with continuous variables in quantum information, however, originated in a more practical observation: efficient implementation of the essential steps in quantum communication protocols, namely, preparing, unitarily manipulating, and measuring (entangled) quantum states, is achievable in quantum optics utilizing continuous quadrature amplitudes of the quantized electromagnetic field. For example, the tools for measuring a quadrature with near-unit efficiency or for displacing an optical mode in phase space are provided by homodyne-detection and feedforward techniques, respectively. Continuous-variable entanglement can be efficiently produced using squeezed light [in which the squeezing of a quadrature's quantum fluctuations is due to a nonlinear optical interaction (Walls and Milburn, 1994)] and linear optics.

A valuable feature of quantum optical implementations based upon continuous variables, related to their high efficiency, is their *unconditionalness*. Quantum resources such as entangled states emerge from the nonlinear optical interaction of a laser with a crystal (supplemented if necessary by some linear optics) in an unconditional fashion, i.e., every inverse bandwidth time. This unconditionalness is hard to obtain in discrete-variable qubit-based implementations using single-photon states. In that case, the desired preparation due to the nonlinear optical interaction depends on particular (coincidence) measurement results ruling out the unwanted (in particular, vacuum) contributions in the outgoing state vector. However, the unconditionalness of the continuous-variable implementations has its price: it is at the expense of the quality of the entanglement of the prepared states. This entanglement and hence any entanglement-based quantum protocol is always imperfect, the degree of imperfection depending on the amount of squeezing of the laser light involved. Good quality and performance require large squeezing which is technologically demanding, but to a certain extent [about 10 dB (Wu *et al.*, 1986)] already state of the art. Of course, in continuous-variable protocols that do not rely on entanglement, for instance, coherent-state-based quantum key distribution, these imperfections do not occur.

To summarize, in the most commonly used optical approaches, the continuous-variable implementations always work pretty well (and hence efficiently and unconditionally), but never perfectly. Their discrete-variable counterparts only work sometimes (conditioned upon rare successful events), but they succeed, in principle, perfectly. A similar tradeoff occurs when optical quantum states are sent through noisy channels (optical fibers), for example, in a realistic quantum key distribution scenario. Subject to losses, the continuous-variable states accumulate noise and emerge at the receiver as contaminated versions of the sender's input states. The discrete-variable quantum information encoded in single-photon states is reliably conveyed for each photon that is not absorbed during transmission.

Due to the recent results of Knill, Laflamme, and Milburn (Knill *et al.*, 2001), it is now known that efficient quantum information processing is possible, in principle, solely by means of linear optics. Their scheme is formulated in a discrete-variable setting in which the quantum information is encoded in single-photon states. Apart from entangled auxiliary photon states, generated off-line without restriction to linear optics, conditional dynamics (feedforward) is the essential ingredient in making this approach work. Universal quantum gates such as a controlled-NOT gate can, in principle, be built using this scheme without need of any Kerr-type nonlinear optical interaction (corresponding to an interaction Hamiltonian quartic in the optical modes' annihilation and creation operators). This Kerr-type interaction would be hard to obtain on the level of single photons. However, the off-line generation of the complicated auxiliary states needed in the Knill-Laflamme-Milburn scheme seems impractical too.

Similarly, in the continuous-variable setting, when it comes to more advanced quantum information protocols, such as universal quantum computation or, in a communication scenario, entanglement distillation, it turns out that tools more sophisticated than mere Gaussian operations are needed. In fact, the Gaussian operations are effectively those described by interaction Hamiltonians at most quadratic in the optical modes' annihilation and creation operators, thus leading to linear input-output relations as in beam-splitter or squeezing transformations. Gaussian operations, mapping Gaussian states onto Gaussian states, also include homodyne detections and phase-space displacements. In contrast, the non-Gaussian operations required for advanced continuous-variable quantum communication (in particular, long-distance communication based on entanglement distillation and swapping, quantum memory, and teleportation) are due either to at least cubic nonlinear optical interactions or to conditional transformations depending on non-Gaussian measurements such as photon counting. It seems that, at this very sophisticated level, the difficulties and requirements of the discrete- and continuous-variable implementations are analogous.

In this review, our aim is to highlight the strengths of the continuous-variable approaches to quantum information processing. Therefore we focus on those protocols that are based on Gaussian states and their feasible manipulation through Gaussian operations. This leads to continuous-variable proposals for the implementation of the simplest quantum communication protocols, such as quantum teleportation and quantum key distribution, and includes the efficient generation and detection of continuous-variable entanglement.

Before dealing with quantum communication and computation, in Sec. II, we first introduce continuous quantum variables within the framework of quantum optics. The discussions about the quadratures of quantized electromagnetic modes, about phase-space representations, and about Gaussian states include the notations and conventions that we use throughout this article. We conclude Sec. II with a few remarks on linear and nonlinear optics, on alternative polarization and spin representations, and on the necessity of a phase reference in continuous-variable implementations. The notion of entanglement, indispensable in many quantum protocols, is described in Sec. III in the context of continuous variables. We discuss pure and mixed entangled states, entanglement between two (bipartite) and between many (multipartite) parties, and so-called bound (undistillable) entanglement. The generation, measurement, and verification (both theoretical and experimental) of continuous-variable entanglement are here of particular interest. As for the properties of the continuous-variable entangled states related with their inseparability, we explain how the nonlocal character of these states is revealed. This involves, for instance, violations of Bell-type inequalities imposed by local realism. Such violations, however, cannot occur when the measurements considered are exclusively of continuous-variable type. This is due to the strict positivity of the Wigner function of the Gaussian continuous-variable entangled states, which allows for a hidden-variable description in terms of the quadrature observables.

In Sec. IV, we describe the conceptually and practically most important quantum communication protocols formulated in terms of continuous variables and thus utilizing the continuous-variable (entangled) states. These schemes include quantum teleportation and entanglement swapping (teleportation of entanglement), quantum (super)dense coding, quantum error correction, quantum cryptography, and entanglement distillation. Since quantum teleportation based on nonmaximum continuous-variable entanglement, using finitely squeezed two-mode squeezed states, is always imperfect, teleportation criteria are needed both for the theoretical and for the experimental verification. As is known from classical communication, light, propagating at high speed and offering a broad range of different frequencies, is an ideal carrier for the transmission of information. This applies to quantum communication as well. However, light is less suited for the storage of information. In order to store quantum information, for instance, at the intermediate stations in a quantum repeater, atoms are more appropriate media than light. Significantly, as another motivation to deal with continuous variables, a feasible light-atom interface can be built via free-space interaction of light with an atomic ensemble based on the alternative polarization and spin-type variables. No strong cavity QED coupling is needed as with single photons. The concepts of this transfer of quantum information from light to atoms and vice versa, as the essential ingredients of a quantum memory, are discussed in Sec. IV.F

Section V is devoted to quantum cloning with continuous variables. One of the most fundamental (and historically one of the first) "laws" of quantum information theory is the so-called no-cloning theorem (Dieks, 1982; Wootters and Zurek, 1982). It forbids the exact copying of arbitrary quantum states. However, arbitrary quantum states can be copied approximately, and the resemblance (in mathematical terms, the *overlap* or *fidelity*) between the clones may attain an optimal value independent of the original states. Such optimal cloning can be accomplished locally by sending the original states (together with some auxiliary system) through a local unitary quantum circuit. Optimal cloning of Gaussian continuous-variable states appears to be more interesting than that of general continuous-variable states, because the latter can be mimicked by a simple coin toss. We describe a non-entanglement-based implementation for the optimal local cloning of Gaussian continuous-variable states. In addition, for Gaussian continuous-variable states, an optical implementation exists of optimal cloning at a distance (telecloning). In this case, the optimality requires entanglement. The corresponding multiparty entanglement is again producible with nonlinear optics (squeezed light) and linear optics (beam splitters).

Quantum computation over continuous variables, discussed in Sec. VI, is a more subtle issue than the in some sense straightforward continuous-variable extensions of quantum communication protocols. At first sight, continuous variables do not appear well suited for the processing of digital information in a computation. On the other hand, a continuous-variable quantum state having an infinite-dimensional spectrum of eigenstates contains a vast amount of quantum information. Hence it might be promising to adjust the continuous-variable states theoretically to the task of computation (for instance, by discretization) and yet to exploit their continuous-variable character experimentally in efficient (optical) implementations. We explain in Sec. VI why universal quantum computation over continuous variables requires Hamiltonians at least cubic in the position and momentum (quadrature) operators. Similarly, any quantum circuit that consists exclusively of unitary gates from the continuous-variable Clifford group can be efficiently simulated by purely classical means. This is a continuous-variable extension of the discrete-variable Gottesman-Knill theorem in which the Clifford group elements include gates such as the Hadamard (in the continuous-variable case, Fourier) transform or the controlled NOT (CNOT). The theorem applies, for example, to quantum teleportation which is fully describable by CNOT's and Hadamard (or Fourier) transforms of some eigenstates supplemented by measurements in that eigenbasis and spin or phase flip operations (or phase-space displacements).

Before some concluding remarks in Sec. VIII, we present some of the experimental approaches to squeezing of light and squeezed-state entanglement generation in Sec. VII.A. Both quadratic and quartic optical nonlinearities are suitable for this, namely, parametric down conversion and the Kerr effect, respectively. Quantum teleportation experiments that have been performed already based on continuous-variable squeezed-state entanglement are described in Sec. VII.D. In Sec. VII, we further discuss experiments with long-lived atomic entanglement, with genuine multipartite entanglement of optical modes, experimental dense coding, experimental quantum key distribution, and the demonstration of a quantum memory effect.

II. CONTINUOUS VARIABLES IN QUANTUM OPTICS

For the transition from classical to quantum mechanics, the position and momentum observables of the particles turn into noncommuting Hermitian operators in the Hamiltonian. In quantum optics, the quantized electromagnetic modes correspond to quantum harmonic oscillators. The modes' quadratures play the roles of the oscillators' position and momentum operators obeying an analogous Heisenberg uncertainty relation.

A. The quadratures of the quantized field

From the Hamiltonian of a quantum harmonic oscillator expressed in terms of (dimensionless) creation and annihilation operators and representing a single mode k, $\hat{H}_k=\hbar\omega_k(\hat{a}_k^\dagger\hat{a}_k+\frac{1}{2})$, we obtain the well-known form written in terms of "position" and "momentum" operators (unit mass),

$$\hat{H}_k=\frac{1}{2}(\hat{p}_k^2+\omega_k^2\hat{x}_k^2), \tag{1}$$

with

$$\hat{a}_k=\frac{1}{\sqrt{2\hbar\omega_k}}(\omega_k\hat{x}_k+i\hat{p}_k), \tag{2}$$

$$\hat{a}_k^\dagger=\frac{1}{\sqrt{2\hbar\omega_k}}(\omega_k\hat{x}_k-i\hat{p}_k), \tag{3}$$

or, conversely,

$$\hat{x}_k=\sqrt{\frac{\hbar}{2\omega_k}}(\hat{a}_k+\hat{a}_k^\dagger), \tag{4}$$

$$\hat{p}_k=-i\sqrt{\frac{\hbar\omega_k}{2}}(\hat{a}_k-\hat{a}_k^\dagger). \tag{5}$$

Here, we have used the well-known commutation relation for position and momentum,

$$[\hat{x}_k,\hat{p}_{k'}]=i\hbar\delta_{kk'}, \tag{6}$$

which is consistent with the bosonic commutation relations $[\hat{a}_k,\hat{a}_{k'}^\dagger]=\delta_{kk'}$, $[\hat{a}_k,\hat{a}_{k'}]=0$. In Eq. (2), we see that up to normalization factors the position and the momentum are the real and imaginary parts of the annihilation operator. Let us now define the dimensionless pair of conjugate variables,

$$\hat{X}_k\equiv\sqrt{\frac{\omega_k}{2\hbar}}\hat{x}_k=\mathrm{Re}\,\hat{a}_k,\quad \hat{P}_k\equiv\frac{1}{\sqrt{2\hbar\omega_k}}\hat{p}_k=\mathrm{Im}\,\hat{a}_k. \tag{7}$$

Their commutation relation is then

$$[\hat{X}_k,\hat{P}_{k'}]=\frac{i}{2}\delta_{kk'}. \tag{8}$$

In other words, the dimensionless position and momentum operators, $\hat{X}_k$ and $\hat{P}_k$, are defined as if we set $\hbar=1/2$. These operators represent the quadratures of a single mode k, in classical terms corresponding to the real and imaginary parts of the oscillator's complex amplitude. In the following, by using $(\hat{X},\hat{P})$ or equivalently $(\hat{x},\hat{p})$, we shall always refer to these dimensionless quadratures as playing the roles of position and momentum. Hence $(\hat{x},\hat{p})$ will also stand for a conjugate pair of dimensionless quadratures.

The Heisenberg uncertainty relation, expressed in terms of the variances of two arbitrary noncommuting observables $\hat{A}$ and $\hat{B}$ for an arbitrary given quantum state,

$$\langle(\Delta\hat{A})^2\rangle\equiv\langle(\hat{A}-\langle\hat{A}\rangle)^2\rangle=\langle\hat{A}^2\rangle-\langle\hat{A}\rangle^2,$$

$$\langle(\Delta\hat{B})^2\rangle\equiv\langle(\hat{B}-\langle\hat{B}\rangle)^2\rangle=\langle\hat{B}^2\rangle-\langle\hat{B}\rangle^2, \tag{9}$$

becomes

$$\langle(\Delta\hat{A})^2\rangle\langle(\Delta\hat{B})^2\rangle\geqslant\frac{1}{4}|\langle[\hat{A},\hat{B}]\rangle|^2. \tag{10}$$

Inserting Eq. (8) into Eq. (10) yields the uncertainty relation for a pair of conjugate quadrature observables of a single mode k,

$$\hat{x}_k=(\hat{a}_k+\hat{a}_k^\dagger)/2,\quad \hat{p}_k=(\hat{a}_k-\hat{a}_k^\dagger)/2i, \tag{11}$$

namely,

$$\langle(\Delta\hat{x}_k)^2\rangle\langle(\Delta\hat{p}_k)^2\rangle\geqslant\frac{1}{4}|\langle[\hat{x}_k,\hat{p}_k]\rangle|^2=\frac{1}{16}. \tag{12}$$

Thus, in our units, the quadrature variance for a vacuum or coherent state of a single mode is $1/4$. Let us further illuminate the meaning of the quadratures by looking at a single frequency mode of the electric field (for a single polarization),

$$\hat{E}_k(\mathbf{r},t) = E_0[\hat{a}_k e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \hat{a}_k^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}]. \tag{13}$$

The constant E_0 contains all the dimensional prefactors. By using Eq. (11), we can rewrite the mode as

$$\hat{E}_k(\mathbf{r},t) = 2E_0[\hat{x}_k \cos(\omega_k t - \mathbf{k}\cdot\mathbf{r}) + \hat{p}_k \sin(\omega_k t - \mathbf{k}\cdot\mathbf{r})]. \tag{14}$$

Clearly, the position and momentum operators $\hat{x}_k$ and $\hat{p}_k$ represent the in-phase and out-of-phase components of the electric-field amplitude of the single mode k with respect to a (classical) reference wave $\propto\cos(\omega_k t - \mathbf{k}\cdot\mathbf{r})$. The choice of the phase of this wave is arbitrary, of course, and a more general reference wave would lead us to the single-mode description

$$\hat{E}_k(\mathbf{r},t) = 2E_0[\hat{x}_k^{(\Theta)} \cos(\omega_k t - \mathbf{k}\cdot\mathbf{r} - \Theta) + \hat{p}_k^{(\Theta)} \sin(\omega_k t - \mathbf{k}\cdot\mathbf{r} - \Theta)], \tag{15}$$

with the more general quadratures

$$\hat{x}_k^{(\Theta)} = (\hat{a}_k e^{-i\Theta} + \hat{a}_k^\dagger e^{+i\Theta})/2, \tag{16}$$

$$\hat{p}_k^{(\Theta)} = (\hat{a}_k e^{-i\Theta} - \hat{a}_k^\dagger e^{+i\Theta})/2i. \tag{17}$$

These new quadratures can be obtained from $\hat{x}_k$ and $\hat{p}_k$ via the rotation

$$\begin{pmatrix} \hat{x}_k^{(\Theta)} \\ \hat{p}_k^{(\Theta)} \end{pmatrix} = \begin{pmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{pmatrix} \begin{pmatrix} \hat{x}_k \\ \hat{p}_k \end{pmatrix}. \tag{18}$$

Since this is a unitary transformation, we again end up with a pair of conjugate observables fulfilling the commutation relation (8). Furthermore, because $\hat{p}_k^{(\Theta)} = \hat{x}_k^{(\Theta+\pi/2)}$, the whole continuum of quadratures is covered by $\hat{x}_k^{(\Theta)}$ with $\Theta\in[0,\pi)$. This continuum of observables is indeed measurable by relatively simple means. Such a so-called homodyne detection works as follows.

A photodetector measuring an electromagnetic mode converts the photons into electrons and hence into an electric current, called the photocurrent $\hat{i}$. It is therefore sensible to assume $\hat{i}\propto\hat{n}=\hat{a}^\dagger\hat{a}$ or $\hat{i}=q\hat{a}^\dagger\hat{a}$ where q is a constant (Paul, 1995). In order to detect a quadrature of the mode $\hat{a}$, the mode must be combined with an intense local oscillator at a 50:50 beam splitter. The local oscillator is assumed to be in a coherent state with large photon number, $|\alpha_{\mathrm{LO}}\rangle$. It is therefore reasonable to describe this oscillator by a classical complex amplitude α_{LO} rather than by an annihilation operator $\hat{a}_{\mathrm{LO}}$. The two output modes of the beam splitter, $(\hat{a}_{\mathrm{LO}}+\hat{a})/\sqrt{2}$ and $(\hat{a}_{\mathrm{LO}}-\hat{a})/\sqrt{2}$ (see Sec. II.D), may then be approximated by

$$\hat{a}_1 = (\alpha_{\mathrm{LO}} + \hat{a})/\sqrt{2}, \quad \hat{a}_2 = (\alpha_{\mathrm{LO}} - \hat{a})/\sqrt{2}. \tag{19}$$

This yields the photocurrents

$$\hat{i}_1 = q\hat{a}_1^\dagger\hat{a}_1 = q(\alpha_{\mathrm{LO}}^* + \hat{a}^\dagger)(\alpha_{\mathrm{LO}} + \hat{a})/2,$$

$$\hat{i}_2 = q\hat{a}_2^\dagger\hat{a}_2 = q(\alpha_{\mathrm{LO}}^* - \hat{a}^\dagger)(\alpha_{\mathrm{LO}} - \hat{a})/2. \tag{20}$$

The actual quantity to be measured will be the difference photocurrent

$$\delta\hat{i} \equiv \hat{i}_1 - \hat{i}_2 = q(\alpha_{\mathrm{LO}}^*\hat{a} + \alpha_{\mathrm{LO}}\hat{a}^\dagger). \tag{21}$$

By introducing the phase Θ of the local oscillator, $\alpha_{\mathrm{LO}} = |\alpha_{\mathrm{LO}}|\exp(i\Theta)$, we recognize that the quadrature observable $\hat{x}^{(\Theta)}$ from Eq. (16) is measured (without mode index k). Now adjustment of the local oscillator's phase $\Theta\in[0,\pi]$ enables us to detect any quadrature from the whole continuum of quadratures $\hat{x}^{(\Theta)}$. A possible way to realize quantum tomography (Leonhardt, 1997), i.e., the reconstruction of the mode's quantum state given by its Wigner function, relies on this measurement method, called (balanced) *homodyne detection*. A broadband rather than a single-mode description of homodyne detection can be found in the work of Braunstein and Crouch (1991), who also investigate the influence of a quantized local oscillator.

We have now seen that it is not too hard to measure the quadratures of an electromagnetic mode. Unitary transformations such as quadrature displacements (phase-space displacements) can also be relatively easily performed via the so-called feedforward technique, as opposed to, for example, photon number displacements. This simplicity and the high efficiency when measuring and manipulating continuous quadratures are the main reasons why continuous-variable schemes appear more attractive than those based on discrete variables such as the photon number.

In the following, we shall refer mainly to the conjugate pair of quadratures $\hat{x}_k$ and $\hat{p}_k$ (position and momentum, i.e., $\Theta=0$ and $\Theta=\pi/2$). In terms of these quadratures, the number operator becomes

$$\hat{n}_k = \hat{a}_k^\dagger\hat{a}_k = \hat{x}_k^2 + \hat{p}_k^2 - \frac{1}{2}, \tag{22}$$

using Eq. (8).

Let us finally review some useful formulas for the single-mode quadrature eigenstates,

$$\hat{x}|x\rangle = x|x\rangle, \quad \hat{p}|p\rangle = p|p\rangle, \tag{23}$$

where we have now dropped the mode index k. They are orthogonal,

$$\langle x|x'\rangle = \delta(x-x'), \quad \langle p|p'\rangle = \delta(p-p'), \tag{24}$$

and complete,

$$\int_{-\infty}^{\infty} |x\rangle\langle x|dx = \mathbb{1}, \quad \int_{-\infty}^{\infty} |p\rangle\langle p|dp = \mathbb{1}. \tag{25}$$

Just as for position and momentum eigenstates, the quadrature eigenstates are mutually related to each other by a Fourier transformation,

$$|x\rangle = \frac{1}{\sqrt{\pi}}\int_{-\infty}^{\infty} e^{-2ixp}|p\rangle dp, \tag{26}$$

$$|p\rangle = \frac{1}{\sqrt{\pi}}\int_{-\infty}^{\infty} e^{+2ixp}|x\rangle dx. \tag{27}$$

Despite being unphysical and not square integrable, the quadrature eigenstates can be very useful in calculations involving the wave functions $\psi(x)=\langle x|\psi\rangle$, etc., and in idealized quantum communication protocols based on continuous variables. For instance, a vacuum state infinitely squeezed in position may be expressed by a zero-position eigenstate $|x=0\rangle=\int|p\rangle dp/\sqrt{\pi}$. The physical, finitely squeezed states are characterized by the quadrature probability distributions $|\psi(x)|^2$, etc., of which the widths correspond to the quadrature uncertainties.

B. Phase-space representations

The Wigner function is particularly suitable as a "quantum phase-space distribution" for describing the effects on the quadrature observables that may arise from quantum theory and classical statistics. It behaves partly as a classical probability distribution, thus enabling us to calculate measurable quantities such as mean values and variances of the quadratures in a classical-like fashion. On the other hand, in contrast to a classical probability distribution, the Wigner function can become negative.

The Wigner function was originally proposed by Wigner in his 1932 paper "On the quantum correction for thermodynamic equilibrium" (Wigner, 1932). There, he gave an expression for the Wigner function in terms of the position basis which reads (with x and p being a dimensionless pair of quadratures in our units with $\hbar=1/2$ as introduced in the previous section; Wigner, 1932)

$$W(x,p) = \frac{2}{\pi}\int dy e^{+4iyp}\langle x-y|\hat{\rho}|x+y\rangle. \tag{28}$$

Here and throughout, unless otherwise specified, the integration will be over the entire space of the integration variable (i.e., here the integration goes from $-\infty$ to ∞). We gave Wigner's original formula for only one mode or one particle [Wigner's (1932) original equation was in N-particle form] because it simplifies the understanding of the concept behind the Wigner function approach. The extension to N modes is straightforward.

Why does $W(x,p)$ resemble a classical-like probability distribution? The most important attributes that explain this are the proper normalization,

$$\int W(\alpha)d^2\alpha = 1, \tag{29}$$

the property of yielding the correct marginal distributions,

$$\int W(x,p)dx = \langle p|\hat{\rho}|p\rangle, \qquad \int W(x,p)dp = \langle x|\hat{\rho}|x\rangle, \tag{30}$$

and the equivalence to a probability distribution in classical averaging when mean values of a certain class of operators $\hat{A}$ in a quantum state $\hat{\rho}$ are to be calculated,

$$\langle\hat{A}\rangle = \mathrm{Tr}(\hat{\rho}\hat{A}) = \int W(\alpha)A(\alpha)d^2\alpha, \tag{31}$$

with a function $A(\alpha)$ related to the operator $\hat{A}$. The measure of integration is in our case $d^2\alpha=d(\mathrm{Re}\,\alpha)d(\mathrm{Im}\,\alpha)=dxdp$ with $W(\alpha=x+ip)\equiv W(x,p)$, and we shall use $d^2\alpha$ and $dxdp$ interchangeably. The operator $\hat{A}$ represents a particular class of functions of $\hat{a}$ and $\hat{a}^\dagger$ or $\hat{x}$ and $\hat{p}$. The marginal distribution for p, $\langle p|\hat{\rho}|p\rangle$, is obtained by changing the integration variables $(x-y=u, x+y=v)$ and using Eq. (26), that for x, $\langle x|\hat{\rho}|x\rangle$, by using $\int\exp(+4iyp)dp=(\pi/2)\delta(y)$. The normalization of the Wigner function then follows from $\mathrm{Tr}(\hat{\rho})=1$.

For any symmetrized operator (Leonhardt, 1997), the so-called Weyl correspondence (Weyl, 1950),

$$\mathrm{Tr}[\hat{\rho}\mathcal{S}(\hat{x}^n\hat{p}^m)] = \int W(x,p)x^n p^m dxdp, \tag{32}$$

provides a rule for calculating quantum-mechanical expectation values in a classical-like fashion according to Eq. (31). Here, $\mathcal{S}(\hat{x}^n\hat{p}^m)$ indicates symmetrization. For example, $\mathcal{S}(\hat{x}^2\hat{p})=(\hat{x}^2\hat{p}+\hat{x}\hat{p}\hat{x}+\hat{p}\hat{x}^2)/3$ corresponds to x^2p (Leonhardt, 1997).

Such a classical-like formulation of quantum optics in terms of quasiprobability distributions is not unique. In fact, there is a whole family of distributions $P(\alpha,s)$ of which each member corresponds to a particular value of a real parameter s,

$$P(\alpha,s) = \frac{1}{\pi^2}\int \chi(\beta,s)\exp(i\beta\alpha^* + i\beta^*\alpha)d^2\beta, \tag{33}$$

with the s-parametrized characteristic functions

$$\chi(\beta,s) = \mathrm{Tr}[\hat{\rho}\exp(-i\beta\hat{a}^\dagger - i\beta^*\hat{a})]\exp(s|\beta|^2/2). \tag{34}$$

The mean values of operators normally and antinormally ordered in $\hat{a}$ and $\hat{a}^\dagger$ may be calculated via the so-called P function $(s=1)$ and Q function $(s=-1)$, respectively. The Wigner function $(s=0)$ and its characteristic function $\chi(\beta,0)$ are perfectly suited to provide expectation values of quantities symmetric in $\hat{a}$ and $\hat{a}^\dagger$ such as the quadratures. Hence the Wigner function, though not always positive definite, appears to be a good compromise in describing quantum states in terms of quantum phase-space variables such as single-mode quadratures. We may formulate various quantum states relevant to continuous-variable quantum communication by means of the Wigner representation. These particular quantum states exhibit extremely nonclassical features such as entanglement and nonlocality. Yet their Wigner functions are positive definite, and thus belong to the class of Gaussian states.

C. Gaussian states

Multimode Gaussian states may represent optical quantum states that are potentially useful for quantum communication or computation purposes. They are efficiently producible in the laboratory, available on demand in an unconditional fashion. Their corresponding Wigner functions are normalized Gaussian distributions of the form (for zero mean)

$$W(\xi) = \frac{1}{(2\pi)^N \sqrt{\det V^{(N)}}} \exp\left\{ -\frac{1}{2}\xi [V^{(N)}]^{-1} \xi^T \right\}, \tag{35}$$

with the $2N$-dimensional vector ξ having the quadrature pairs of all N modes as its components,

$$\xi = (x_1, p_1, x_2, p_2, \dots, x_N, p_N), \tag{36}$$

$$\hat{\xi} = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \dots, \hat{x}_N, \hat{p}_N), \tag{37}$$

and with the $2N \times 2N$ correlation matrix $V^{(N)}$ having as its elements the second moments symmetrized according to the Weyl correspondence Eq. (32),

$$\begin{aligned} \mathrm{Tr}[\hat{\rho}(\Delta\hat{\xi}_i \Delta\hat{\xi}_j + \Delta\hat{\xi}_j \Delta\hat{\xi}_i)/2] &= \langle (\hat{\xi}_i \hat{\xi}_j + \hat{\xi}_j \hat{\xi}_i)/2 \rangle \\ &= \int W(\xi) \xi_i \xi_j d^{2N}\xi = V_{ij}^{(N)}, \end{aligned} \tag{38}$$

where $\Delta\hat{\xi}_i = \hat{\xi}_i - \langle \hat{\xi}_i \rangle = \hat{\xi}_i$ for zero mean values. The last equality defines the correlation matrix for any quantum state. For Gaussian states of the form of Eq. (35), the Wigner function is completely determined by the second-moment correlation matrix.

For a classical probability distribution over the classical $2N$-dimensional phase space, every physical correlation matrix is real, symmetric, and positive, and conversely, any real, symmetric, and positive matrix represents a possible physical correlation matrix. Apart from reality, symmetry, and positivity, the Wigner correlation matrix (of any state), describing the quantum phase space, must also comply with the commutation relation from Eq. (8) (Simon, 2000; Werner and Wolf, 2001),

$$[\hat{\xi}_k, \hat{\xi}_l] = \frac{i}{2}\Lambda_{kl}, \quad k,l = 1,2,3, \dots, 2N, \tag{39}$$

with the $2N \times 2N$ matrix Λ having the 2×2 matrix J as diagonal entry for each quadrature pair, for example, for $N=2$,

$$\Lambda = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{40}$$

A direct consequence of this commutation relation and the non-negativity of the density operator $\hat{\rho}$ is the following N-mode uncertainty relation (Simon, 2000; Werner and Wolf, 2001):

$$V^{(N)} - \frac{i}{4}\Lambda \geqslant 0. \tag{41}$$

This matrix equation means that the matrix sum on the left-hand side has only non-negative eigenvalues. Note that this N-mode uncertainty relation applies to any state, not only Gaussian states. Any physical state has to obey it. For Gaussian states, however, it is not only a necessary condition, but also sufficient to ensure the positivity of $\hat{\rho}$ (Werner and Wolf, 2001). In the simplest case $N=1$, Eq. (41) is reduced to the statement det $V^{(1)} \geqslant 1/16$, which is a more precise and complete version of the Heisenberg uncertainty relation in Eq. (12). For any N, Eq. (41) becomes exactly the Heisenberg uncertainty relation of Eq. (12) for each individual mode, if $V^{(N)}$ is diagonal. The purity condition for an N-mode Gaussian state is given by det $V^{(N)} = 1/16^N$.

D. Linear optics

In passive optical devices such as beam splitters and phase shifters, the photon number is preserved and the modes' annihilation operators are transformed only linearly. This linear-optics toolbox provides essential tools for generating particular quantum states and for manipulating and measuring them.

A beam splitter can be considered as a four-port device with the input-output relations in the Heisenberg picture,

$$(\hat{a}_1' \hat{a}_2')^T = U(2)(\hat{a}_1 \hat{a}_2)^T. \tag{42}$$

The matrix $U(2)$ must be unitary, $U^{-1}(2) = U^\dagger(2)$, in order to ensure that the commutation relations are preserved,

$$[\hat{a}_i', \hat{a}_j'] = [(\hat{a}_i')^\dagger, (\hat{a}_j')^\dagger] = 0, \quad [\hat{a}_i', (\hat{a}_j')^\dagger] = \delta_{ij}. \tag{43}$$

This unitarity reflects the fact that the total photon number remains constant for a lossless beam splitter. Any unitary transformation acting on two modes can be expressed by the matrix (Bernstein, 1974; Danakas and Aravind, 1992)

$$U(2) = \begin{pmatrix} e^{-i(\phi+\delta)} \sin\theta & e^{-i\delta} \cos\theta \\ e^{-i(\phi+\delta')} \cos\theta & -e^{-i\delta'} \sin\theta \end{pmatrix}. \tag{44}$$

An ideal phase-free beam-splitter operation is then simply given by the linear transformation

$$\begin{pmatrix} \hat{a}_1' \\ \hat{a}_2' \end{pmatrix} = \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}, \tag{45}$$

with the reflectivity and transmittance parameters $\sin\theta$ and $\cos\theta$. Thus the general unitary matrix describes a sequence of phase shifts and phase-free beam-splitter rotations,

$$U(2) = \begin{pmatrix} e^{-i\delta} & 0 \\ 0 & e^{-i\delta'} \end{pmatrix} \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} \begin{pmatrix} e^{-i\phi} & 0 \\ 0 & 1 \end{pmatrix}. \tag{46}$$

Not only the above 2×2 matrix can be decomposed into phase shifting and beam-splitting operations. Any N

$\times N$ unitary matrix as it appears in the linear transformation

$$\hat{a}_i' = \sum_j U_{ij}\hat{a}_j \tag{47}$$

may be expressed by a sequence of phase shifters and beam splitters (Reck *et al.*, 1994). This means that any mixing between optical modes described by a unitary *matrix* can be implemented with linear optics. In general, it does not mean that any unitary *operator* acting on the Hilbert space of optical modes (or a subspace of it) is realizable via a fixed network of linear optics. Conversely, however, any such network can be described by the linear transformation in Eq. (47).

The action of an ideal phase-free beam-splitter operation on two modes can be expressed in the Heisenberg picture by Eq. (45). The input operators are changed, whereas the input states remain invariant. The corresponding unitary operator must satisfy

$$\begin{pmatrix} \hat{a}_1' \\ \hat{a}_2' \end{pmatrix} = \hat{B}_{12}^\dagger(\theta)\begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}\hat{B}_{12}(\theta). \tag{48}$$

In the Schrödinger representation, we have correspondingly $\hat{\rho}' = \hat{B}_{12}(\theta)\hat{\rho}\hat{B}_{12}^\dagger(\theta)$ or, for pure states, $|\psi'\rangle = \hat{B}_{12}(\theta)|\psi\rangle$. Note that $\hat{B}_{12}(\theta)$ acts on the position eigenstates as

$$\begin{aligned} \hat{B}_{12}(\theta)|x_1,x_2\rangle &= |x_1 \sin\theta + x_2\cos\theta, x_1\cos\theta - x_2\sin\theta\rangle \\ &= |x_1',x_2'\rangle. \end{aligned} \tag{49}$$

In Eq. (49), $|x_1,x_2\rangle \equiv |x_1\rangle|x_2\rangle \equiv |x_1\rangle_1 \otimes |x_2\rangle_2$ which we shall use interchangeably throughout. The position wave function is transformed according to

$$\begin{aligned} \psi(x_1,x_2) &\to \psi'(x_1',x_2') \\ &= \psi(x_1'\sin\theta + x_2'\cos\theta, x_1'\cos\theta - x_2'\sin\theta). \end{aligned} \tag{50}$$

Analogous linear beam-splitter transformation rules apply to the momentum wave function, the probability densities, and the Wigner function. Finally, we note that any unitary operator $\hat{U}$ that describes a network of passive linear optics acting upon N modes corresponds to a quadratic Hamiltonian such that $\hat{U} = \exp(-i\vec{\hat{a}}^\dagger H \vec{\hat{a}})$, where $\vec{\hat{a}} = (\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_N)^T$, $\vec{\hat{a}}^\dagger = (\hat{a}_1^\dagger, \hat{a}_2^\dagger, \ldots, \hat{a}_N^\dagger)$, and H is an $N \times N$ Hermitian matrix.

E. Nonlinear optics

An important tool of many quantum communication protocols is entanglement, and the essential ingredient in the generation of continuous-variable entanglement is squeezed light. In order to squeeze the quantum fluctuations of the electromagnetic field, nonlinear optical effects are needed. This squeezing of optical modes is sometimes also referred to as a *linear optical process*, because the corresponding interaction Hamiltonian is quadratic in $\hat{a}$ and $\hat{a}^\dagger$, which yields a linear mixing between annihilation and creation operators in the input-output relations. In the previous section, we discussed how a process that truly originates from linear optics (based only on passive elements such as beam splitters and phase shifters) is expressed by Eq. (47). Such a process is given by linear input-output relations, but it does not involve mixing between the $\hat{a}$'s and $\hat{a}^\dagger$'s. The most general linear transformation combining elements from passive linear optics and nonlinear optics is the so-called *linear unitary Bogoliubov transformation* (Bogoliubov, 1947),

$$\hat{a}_i' = \sum_j A_{ij}\hat{a}_j + B_{ij}\hat{a}_j^\dagger + \gamma_i, \tag{51}$$

with the matrices A and B satisfying the conditions $AB^T = (AB^T)^T$ and $AA^\dagger = BB^\dagger + \mathbb{1}$ due to the bosonic commutation relations for $\hat{a}_i'$. This input-output relation describes any combination of linear optical elements (multiport interferometers), multimode squeezers, and phase-space displacements or, in other words, any interaction Hamiltonian quadratic in $\hat{a}$ and $\hat{a}^\dagger$. The linear unitary Bogoliubov transformations are equivalent to the Gaussian transformations that map Gaussian states onto Gaussian states.

In general, squeezing refers to the reduction of quantum fluctuations in one observable below the standard quantum limit (the minimal noise level of the vacuum state) at the expense of an increased uncertainty of the conjugate variable. In the remainder of this section, we shall briefly discuss squeezing schemes involving a nonlinear optical $\chi^{(2)}$ interaction, describable by a quadratic interaction Hamiltonian. Other schemes, based on a $\chi^{(3)}$ nonlinearity and a quartic Hamiltonian, are among the topics discussed in Sec. VII.

The output state of degenerate parametric amplification, in which the signal and idler frequencies both equal half the pump frequency, corresponds to a single-mode squeezed state. This effect of single-mode squeezing can be calculated with an interaction Hamiltonian quadratic in the creation and annihilation operators,

$$\hat{H}_{\text{int}} = i\hbar\frac{\kappa}{2}(\hat{a}^{\dagger 2}e^{i\Theta} - \hat{a}^2 e^{-i\Theta}). \tag{52}$$

This Hamiltonian describes the amplification of the signal mode $\hat{a}$ at half the pump frequency in an interaction picture (without explicit time dependence due to the free evolution). The coherent pump mode is assumed to be classical (the so-called parametric approximation), its real amplitude $|\alpha_{\text{pump}}|$ is absorbed in κ, and the pump phase is Θ. The parameter κ also contains the susceptibility, $\kappa \propto \chi^{(2)}|\alpha_{\text{pump}}|$. The fully quantum-mechanical Hamiltonian is $\hat{H}_{\text{int}} \propto \hat{a}^{\dagger 2}\hat{a}_{\text{pump}} - \hat{a}^2\hat{a}_{\text{pump}}^\dagger$, and with the parametric approximation we assume $\hat{a}_{\text{pump}} \to \alpha_{\text{pump}} = |\alpha_{\text{pump}}|e^{i\Theta}$ (Scully and Zubairy, 1997). In the interaction picture, we can insert $\hat{H}_{\text{int}}$ into the Heisenberg equation of motion for the annihilation operator and obtain (taking zero pump phase $\Theta = 0$)

$$\frac{d}{dt}\hat{a}(t)=\frac{1}{i\hbar}[\hat{a}(t),\hat{H}_{\mathrm{int}}]=\kappa\hat{a}^{\dagger}(t). \tag{53}$$

This equation is solved by

$$\hat{a}(t)=\hat{a}(0)\mathrm{cos}h(\kappa t)+\hat{a}^{\dagger}(0)\sinh(\kappa t). \tag{54}$$

The quadrature operators evolve correspondingly into

$$\hat{x}(t)=e^{+\kappa t}\hat{x}(0),\quad \hat{p}(t)=e^{-\kappa t}\hat{p}(0). \tag{55}$$

This is in fact the expected result. Due to the unitary evolution, the uncertainty of the p quadrature decreases, whereas that of the x quadrature grows:

$$\langle[\Delta\hat{x}(t)]^2\rangle=e^{+2\kappa t}\langle[\Delta\hat{x}^{(0)}]^2\rangle,$$

$$\langle[\Delta\hat{p}(t)]^2\rangle=e^{-2\kappa t}\langle[\Delta\hat{p}^{(0)}]^2\rangle. \tag{56}$$

Here we have chosen vacuum-state inputs and replaced the initial quadratures by those of the vacuum labeled by a superscript (0). The evolving states remain minimum uncertainty states, but they have p fluctuations below and x fluctuations above the vacuum noise level. They have become quadrature squeezed states. According to the unitary evolution

$$\hat{U}(t,t_0)=\exp\left[-\frac{i}{\hbar}\hat{H}(t-t_0)\right], \tag{57}$$

with the Hamiltonian from Eq. (52) and $t_0=0$, let us now introduce the *unitary squeezing operator* or *squeeze operator* $\hat{S}(\zeta)$ by defining $\zeta\equiv -r\exp(i\Theta)$ with the squeezing parameter $r\equiv\kappa t$ (a dimensionless effective interaction time),

$$\hat{U}(t,0)=\exp\left[\frac{\kappa}{2}(\hat{a}^{\dagger 2}e^{i\Theta}-\hat{a}^{2}e^{-i\Theta})t\right]$$

$$\equiv\hat{S}(\zeta)=\exp\left(\frac{\zeta^*}{2}\hat{a}^2-\frac{\zeta}{2}\hat{a}^{\dagger 2}\right). \tag{58}$$

The squeezing operator obviously satisfies $\hat{S}^{\dagger}(\zeta)=\hat{S}^{-1}(\zeta)=\hat{S}(-\zeta)$. Applying it to an arbitrary initial mode $\hat{a}(0)\equiv\hat{a}$ yields the transformations

$$\hat{S}^{\dagger}(\zeta)\hat{a}\hat{S}(\zeta)=\hat{a}\cosh r+\hat{a}^{\dagger}e^{i\Theta}\sinh r,$$

$$\hat{S}^{\dagger}(\zeta)\hat{a}^{\dagger}\hat{S}(\zeta)=\hat{a}^{\dagger}\cosh r+\hat{a}e^{-i\Theta}\sinh r. \tag{59}$$

For the rotated mode

$$\hat{x}^{(\Theta/2)}+i\hat{p}^{(\Theta/2)}=(\hat{x}+i\hat{p})e^{-i\Theta/2}=\hat{a}e^{-i\Theta/2}, \tag{60}$$

the squeezing transformation results in

$$\hat{S}^{\dagger}(\zeta)[\hat{x}^{(\Theta/2)}+i\hat{p}^{(\Theta/2)}]\hat{S}(\zeta)=\hat{a}e^{-i\Theta/2}\cosh r$$

$$+\hat{a}^{\dagger}e^{+i\Theta/2}\sinh r$$

$$=e^{+r}\hat{x}^{(\Theta/2)}+ie^{-r}\hat{p}^{(\Theta/2)}. \tag{61}$$

Thus the effect of the squeezing operator on an arbitrary pair of quadratures, as generally defined in Eqs. (16) and (17), is the attenuation of one quadrature and the amplification of the other. We have seen that the squeezing operator effectively represents the unitary evolution due to the optical parametric amplifier Hamiltonian. The corresponding expressions for the resulting Heisenberg quadrature operators (with $\Theta=0$ and vacuum inputs),

$$\hat{x}(r)=e^{+r}\hat{x}^{(0)},\quad \hat{p}(r)=e^{-r}\hat{p}^{(0)}, \tag{62}$$

as in Eq. (55) squeezed in p for $t>0$ ($r>0$), will prove extremely useful for the following investigations. Note that time reversal ($r<0$) just swaps the squeezed and the antisqueezed quadrature. Throughout this review, we will always use $r\geqslant 0$, and hence describe a position-squeezed mode via the Heisenberg equations

$$\hat{x}(r)=e^{-r}\hat{x}^{(0)},\quad \hat{p}(r)=e^{+r}\hat{p}^{(0)}, \tag{63}$$

where $r>0$. The quadrature squeezing, mathematically defined through the squeezing operator $\hat{S}(\zeta)$ and physically associated with the optical parametric amplifier interaction, is commonly referred to as "ordinary" squeezing. Other kinds of squeezing will be mentioned in Sec. VII.

The Heisenberg equations (62) correspond to a squeezed vacuum state, in the Schrödinger representation given by the Hilbert vector $\hat{S}(\zeta)|0\rangle$ (with $\Theta=0$). More generally, all minimum uncertainty states are displaced squeezed vacua,

$$|\alpha,\zeta\rangle=\hat{D}(\alpha)\hat{S}(\zeta)|0\rangle, \tag{64}$$

with the unitary displacement operator

$$\hat{D}(\alpha)=\exp(\alpha\hat{a}^{\dagger}-\alpha^*\hat{a})=\exp(2ip_{\alpha}\hat{x}-2ix_{\alpha}\hat{p}), \tag{65}$$

where $\alpha=x_{\alpha}+ip_{\alpha}$ and $\hat{a}=\hat{x}+i\hat{p}$. The displacement operator acting on $\hat{a}$ (as a unitary transformation in the Heisenberg picture) yields a displacement by the complex number α,

$$\hat{D}^{\dagger}(\alpha)\hat{a}\hat{D}(\alpha)=\hat{a}+\alpha. \tag{66}$$

The position wave function for the displaced position-squeezed vacuum is given by

$$\psi(x)=\left(\frac{2}{\pi}\right)^{1/4}e^{r/2}\exp[-e^{2r}(x-x_{\alpha})^2+2ip_{\alpha}x-ix_{\alpha}p_{\alpha}]. \tag{67}$$

The corresponding Wigner function is then

$$W(x,p)=\frac{2}{\pi}\exp[-2e^{+2r}(x-x_{\alpha})^2-2e^{-2r}(p-p_{\alpha})^2], \tag{68}$$

where the quadrature variances here are $\sigma_x=e^{-2r}/4$ and $\sigma_p=e^{+2r}/4$. In the limit of infinite squeezing, $r\to\infty$, the position probability density, $|\psi(x)|^2=\sqrt{2/\pi}e^r\exp[-2e^{2r}(x-x_{\alpha})^2]$, becomes a delta function, $\lim_{\epsilon\to 0}\exp[-(x-x_{\alpha})^2/\epsilon^2]/\epsilon\sqrt{\pi}=\delta(x-x_{\alpha})$, with $\epsilon=e^{-r}/\sqrt{2}$. The squeezed vacuum wave function in that limit, $\psi(x)\propto\delta(x)$, describes a zero-position eigenstate, $\int dx\,\psi(x)|x\rangle\propto|0\rangle$. The mean photon number of an infinitely squeezed state becomes infinite, because for the displaced squeezed vacuum we have

$$\langle \hat{n} \rangle = \langle \hat{x}^2 \rangle + \langle \hat{p}^2 \rangle - \frac{1}{2} = |\alpha|^2 + \sinh^2 r, \tag{69}$$

using Eq. (22).

Later, we shall show that the simplest quantum teleportation protocol based on continuous variables utilizes two-mode squeezing. The physical process for producing a two-mode squeezed state via a nondegenerate optical parametric amplifier is a generalization of the nonlinear interaction involved in degenerate optical parametric amplification. This interaction relies on the Hamiltonian

$$\hat{H}_{\text{int}} = i\hbar\kappa(\hat{a}_1^\dagger \hat{a}_2^\dagger e^{i\Theta} - \hat{a}_1 \hat{a}_2 e^{-i\Theta}), \tag{70}$$

where $\hat{a}_1$ and $\hat{a}_2$ refer to the signal and idler modes emerging at two sidebands around half the pump frequency and having different polarizations. Here, we still assume $\kappa \propto \chi^{(2)}|\alpha_{\text{pump}}|$. Mathematically, two-mode squeezing may be defined analogously to single-mode squeezing by the unitary two-mode squeeze operator

$$\begin{aligned} \hat{U}(t,0) &= \exp[\kappa(\hat{a}_1^\dagger \hat{a}_2^\dagger e^{i\Theta} - \hat{a}_1 \hat{a}_2 e^{-i\Theta})t] \\ &\equiv \hat{S}(\zeta) = \exp(\zeta^* \hat{a}_1 \hat{a}_2 - \zeta \hat{a}_1^\dagger \hat{a}_2^\dagger), \end{aligned} \tag{71}$$

with the same definitions and conventions as above. The solution for the output modes, calculated as above for single-mode squeezing, is (with $\Theta = 0$)

$$\begin{aligned} \hat{a}_1(r) &= \hat{a}_1 \cosh r + \hat{a}_2^\dagger \sinh r, \\ \hat{a}_2(r) &= \hat{a}_2 \cosh r + \hat{a}_1^\dagger \sinh r. \end{aligned} \tag{72}$$

These output modes are entangled and exhibit quantum correlations between the quadratures. More realistically, these correlations cover a finite range of sideband frequencies. This broadband two-mode squeezing will be briefly discussed in Sec. VII. A two-mode squeezed state, produced by the nondegenerate optical parametric amplifier interaction, is equivalent to two single-mode squeezed states (with perpendicular squeezing directions and produced via the degenerate optical parametric amplifier interaction or alternatively via a $\chi^{(3)}$ interaction; see Sec. VII) combined at a beam splitter (van Loock *et al.*, 2000). This equivalence will be explained in Sec. III.

We have discussed the generation of squeezed light within the framework of nonlinear optics and the manipulation of electromagnetic modes by linear optics using beam splitters. Squeezers and beam splitters are the resources and building blocks of quantum communication protocols based on continuous variables, because they represent tools for creating the essential ingredient of most of these protocols: continuous-variable entanglement, introduced in detail in Sec. III.

F. Polarization and spin representations

The field of quantum information with continuous variables grew out of the analysis of quadrature-squeezed optical states. However, in order for this field to mature into one yielding a usable technology, methods for storing continuous quantum information will be required. In particular, it seems clear that continuous quantum variables that can be compatible with the collective state of a set of atomic systems will be needed to perform this task. Here we briefly discuss a useful alternative encoding for continuous quantum information in terms of collective spinlike variables.

Optically, we shall be interested in encoding the continuous quantum information onto the collective Stokes (polarization) variables of an optical field. Let $\hat{a}_+(t-z/c)$ and $\hat{a}_-(t-z/c)$ be the annihilation operators for circularly polarized beams of light propagating along the positive z axis. Then the Stokes operators may be defined as

$$\begin{aligned} \hat{S}_x &= \frac{c}{2}\int_0^T d\tau' [\hat{a}_+^\dagger(\tau')\hat{a}_-(\tau') + \hat{a}_-^\dagger(\tau')\hat{a}_+(\tau')], \\ \hat{S}_y &= \frac{-ic}{2}\int_0^T d\tau' [\hat{a}_+^\dagger(\tau')\hat{a}_-(\tau') - \hat{a}_-^\dagger(\tau')\hat{a}_+(\tau')], \\ \hat{S}_z &= \frac{c}{2}\int_0^T d\tau' [\hat{a}_+^\dagger(\tau')\hat{a}_+(\tau') - \hat{a}_-^\dagger(\tau')\hat{a}_-(\tau')]. \end{aligned} \tag{73}$$

Given the usual equal-time commutation relations for the annihilation operators $\hat{a}_\pm(t,z)$ as $[\hat{a}_i(t,z),\hat{a}_j(t,z')] = \delta_{ij}\delta(z-z')$, where $i,j=\pm$, the commutation relations for these Stokes operators correspond to those of the usual spin operators, namely, $[\hat{S}_j,\hat{S}_k] = i\epsilon_{jkl}\hat{S}_l$.

Now suppose we restrict our states to those for which $\langle \hat{S}_x \rangle$ is near its maximum value. In this case, to a good approximation, we may write $\hat{S}_x \simeq \langle \hat{S}_x \rangle$. For states restricted in this manner, the resulting commutation relations for $\hat{S}_y$ and $\hat{S}_z$ are a good approximation (up to rescaling) of the canonical commutation relations for the usual phase-space variables $\hat{x}$ and $\hat{p}$. Thus states with near-maximum Stokes' polarization correspond to those on a patch of phase space with $\hat{S}_y$ and $\hat{S}_z$ playing the role of $\hat{x}$ and $\hat{p}$. Taking the state with maximum $\langle \hat{S}_x \rangle$ to represent the phase-space vacuum state, the whole set of usual coherent, squeezed, and continuous-variable entangled states may be constructed via displacements and squeezing transformations based on this operator translation.

An analogous representation may be constructed for the collective spin of a set of N spin-$\frac{1}{2}$ atoms. Defining the collective spin variables as $\hat{F}_i = (1/N)\Sigma_{n=1}^N \hat{F}_i^{(n)}$, with the usual spin commutation relations, we find for the collective spin variables $[\hat{F}_j,\hat{F}_k] = i\epsilon_{jkl}\hat{F}_l$. In a similar manner, we shall consider states with near maximal polarization along the negative z axis, i.e., states corresponding to small variations about $|F,-F\rangle$. Again, for such a subset of states, the variables $\hat{F}_x$ and $\hat{F}_y$ have commutation relations (up to rescaling) that are excellent approximations to those of the phase-space variables $\hat{x}$ and $\hat{p}$. Thus, within these phase-space patches, we may encode continuous quantum information as spin-coherent, spin-squeezed, etc., states. A coherent spin state would then be a minimum uncertainty state that satisfies equality in the corresponding Heisenberg uncertainty relation, for instance, according to Eq. (10),

$$\langle(\Delta\hat{F}_x)^2\rangle\langle(\Delta\hat{F}_y)^2\rangle \geqslant \frac{1}{4}|\langle\hat{F}_z\rangle|^2. \tag{74}$$

For a state with mean polarization along the z axis, $|\langle\hat{F}_z\rangle| = F$, the vacuum variance would correspond to $\langle(\Delta\hat{F}_x)^2\rangle = \langle(\Delta\hat{F}_y)^2\rangle = F/2$.

G. Necessity of phase reference

The quantum information of continuous variables is stored as phase-space distributions. Almost all such distributions (and hence quantum states) depend on the orientation of the phase-space coordinate frame. Physically, this corresponds to a phase of the quantum field being used to encode the quantum information.

Typically, this phase corresponds to a choice of phase of the single-mode annihilation operator via

$$\hat{a} \to e^{-i\phi}\hat{a}, \tag{75}$$

or equivalently the phase shift on a single-mode state (or wave function) via

$$|\psi\rangle \to e^{-i\phi\hat{a}^\dagger\hat{a}}|\psi\rangle. \tag{76}$$

When we measure such states to extract some of their quantum information we shall typically use phase-sensitive detection schemes such as homodyne detection. However, this entails picking some phase reference.

In this case, the phase reference comes from a strong local oscillator. However, the local oscillator itself has phase freedom. So where is this freedom actually tied down in any given experiment?

The trick that has been used for decades is both to construct and to manipulate the phase-sensitive states from the same phase reference that one uses to make the measurements. Physically, one splits up the local oscillator into several pieces, each of which controls a different aspect of any given experiment. However, so long as each process is done within the local oscillator's dephasing time the common phase cancels out from the response of the detectors. Thus quantum information with continuous variables involves experiments that typically are going to require a phase reference. In quantum-optics experiments, for example, this local oscillator is just a strong laser beam that is shared amongst the various parties (such as sender and receiver) in the laboratory.

Does the phase reference of the local oscillator correspond to a quantum or a classical channel that must be shared between users? One can expect that, since multiple copies are being used, the resource must actually be relying on no more than clonable and hence presumably classical information.

This whole picture is well appreciated by experimentalists, but has recently led to some discussion about the validity of this paradigm. In particular, Rudolph and Sanders (2001) have recently argued that since we cannot know the local oscillator's phase ϕ (Mølmer, 1997), we should average over it,

$$\hat{\rho}_{\text{PEF}} = \int_0^{2\pi} \frac{d\phi}{2\pi}\text{Pr}(\phi)||\alpha|e^{-i\phi}\rangle\langle|\alpha|e^{-i\phi}| \tag{77}$$

$$= \int_0^{2\pi} \frac{d\phi}{2\pi}||\alpha|e^{-i\phi}\rangle\langle|\alpha|e^{-i\phi}| \tag{78}$$

$$= e^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{|\alpha|^{2n}}{n!}|n\rangle\langle n|, \tag{79}$$

where they implicitly took the prior distribution $\text{Pr}(\phi)$ to be uniform. Invoking the partition ensemble fallacy (Kok and Braunstein, 2000) they then argued that the decomposition of Eq. (77) into coherent states, as opposed to number states, was not appropriate in interpreting experiments.

A number of people have argued against this as counter to common sense (Gea-Banacloche, 1990; Wiseman and Vaccaro, 2001; van Enk and Fuchs, 2002). However, Nemoto and Braunstein (2003) noted a flaw in the argument of Rudolph and Sanders: although choosing $\text{Pr}(\phi)$ as uniform seems eminently reasonable, if ϕ is truly unobservable as they presume and as is generally accepted (Mølmer, 1997), then Rudolph and Sanders's choice of $\text{Pr}(\phi)$ is untestable. Indeed, any choice of $\text{Pr}(\phi)$ would lead to completely equivalent predictions for all possible experiments. The implication of this is that states of the form of Eq. (77) actually form an equivalence class—any member of which may be chosen to represent the class. One of these members is just a coherent state. Thus the conventional experimental interpretation falls out and the long-standing interpretations do not in fact involve any fallacy.

III. CONTINUOUS-VARIABLE ENTANGLEMENT

Historically, the notion of entanglement (*Verschränkung*) first appeared explicitly in the literature in 1935, long before the dawn of the relatively young field of quantum information, and without any reference to discrete-variable qubit states. In fact, the entangled states treated in this paper by Einstein, Podolsky, and Rosen (EPR; Einstein *et al.*, 1935) were two-particle states quantum-mechanically correlated with respect to their positions and momenta. Although important milestones in quantum information theory have been derived and expressed in terms of qubits or discrete variables, the notion of quantum entanglement itself came to light in a continuous-variable setting.[1] Einstein, Pod-

[1] More explicitly, the notion of entanglement was introduced by Schrödinger (1935), inspired by the EPR paper.

olsky, and Rosen (Einstein *et al.*, 1935) considered the position wave function $\psi(x_1,x_2)=C\delta(x_1-x_2-u)$ with a vanishing normalization constant C. Hence the corresponding quantum state,

$$\int dx_1 dx_2 \psi(x_1,x_2)|x_1,x_2\rangle \propto \int dx|x,x-u\rangle, \tag{80}$$

describes perfectly correlated positions ($x_1-x_2=u$) and momenta (total momentum zero, $p_1+p_2=0$), but this state is unnormalizable and unphysical. However, it can be thought of as the limiting case of a regularized, properly normalized version in which the positions and momenta are correlated only to some finite extent given by a (Gaussian) width. Such regularized versions are, for example, two-mode squeezed states, since the position and momentum wave functions for the two-mode squeezed vacuum state are (Leonhardt, 1997)

$$\begin{aligned}\psi(x_1,x_2) &= \sqrt{\frac{2}{\pi}}\exp[-e^{-2r}(x_1+x_2)^2/2 \\ &\quad - e^{+2r}(x_1-x_2)^2/2],\\ \tilde{\psi}(p_1,p_2) &= \sqrt{\frac{2}{\pi}}\exp[-e^{-2r}(p_1-p_2)^2/2 \\ &\quad - e^{+2r}(p_1+p_2)^2/2],\end{aligned} \tag{81}$$

approaching $C\delta(x_1-x_2)$ and $C\delta(p_1+p_2)$, respectively, in the limit of infinite squeezing $r\to\infty$. The corresponding Wigner function of the two-mode squeezed vacuum state is then (Bell, 1964; Walls and Milburn, 1994; Braunstein and Kimble, 1998a)

$$\begin{aligned}W(\xi) &= \frac{4}{\pi^2}\exp\{-e^{-2r}[(x_1+x_2)^2+(p_1-p_2)^2] \\ &\quad - e^{+2r}[(x_1-x_2)^2+(p_1+p_2)^2]\},\end{aligned} \tag{82}$$

with $\xi=(x_1,p_1,x_2,p_2)$. This Wigner function approaches $C\delta(x_1-x_2)\delta(p_1+p_2)$ in the limit of infinite squeezing $r\to\infty$, corresponding to the original (perfectly correlated and maximally entangled, but unphysical) EPR state (Einstein *et al.*, 1935). From the Wigner function, the marginal distributions for the two positions or the two momenta are obtained by integration over the two momenta or the two positions, respectively,

$$\begin{aligned}\int dp_1 dp_2 W(\xi) &= |\psi(x_1,x_2)|^2 \\ &= \frac{2}{\pi}\exp[-e^{-2r}(x_1+x_2)^2 - e^{+2r}(x_1-x_2)^2],\\ \int dx_1 dx_2 W(\xi) &= |\tilde{\psi}(p_1,p_2)|^2 \\ &= \frac{2}{\pi}\exp[-e^{-2r}(p_1-p_2)^2 - e^{+2r}(p_1+p_2)^2].\end{aligned} \tag{83}$$

Though having well-defined relative position and total momentum for large squeezing, the two modes of the two-mode squeezed vacuum state exhibit increasing uncertainties in their individual positions and momenta as the squeezing grows. In fact, upon tracing (integrating) out either mode of the Wigner function in Eq. (82), we obtain the thermal state

$$\int dx_1 dp_1 W(\xi) = \frac{2}{\pi(1+2\bar{n})}\exp\left[-\frac{2(x_2^2+p_2^2)}{1+2\bar{n}}\right], \tag{84}$$

with mean photon number $\bar{n}=\sinh^2 r$. Instead of the continuous-variable position or momentum basis, the two-mode squeezed vacuum state may also be written in the discrete (though, of course, still infinite-dimensional) photon number (Fock) basis. Applying the two-mode squeeze operator with $\Theta=0$, as defined in Eq. (71), to two vacuum modes, we obtain the following expression:

$$\begin{aligned}\hat{S}(\zeta)|00\rangle &= e^{r(\hat{a}_1^\dagger\hat{a}_2^\dagger-\hat{a}_1\hat{a}_2)}|00\rangle \\ &= e^{\tanh r\hat{a}_1^\dagger\hat{a}_2^\dagger}\left(\frac{1}{\cosh r}\right)^{\hat{a}_1^\dagger\hat{a}_1+\hat{a}_2^\dagger\hat{a}_2+1} \\ &\quad\times e^{-\tanh r\hat{a}_1\hat{a}_2}|00\rangle = \sqrt{1-\lambda}\sum_{n=0}^{\infty}\lambda^{n/2}|n\rangle|n\rangle,\end{aligned} \tag{85}$$

where $\lambda=\tanh^2 r$. In the second line of Eq. (85), we have used the disentangling theorem of Collett (1988). The form in Eq. (85) reveals that the two modes of the two-mode squeezed vacuum state are also quantum correlated in photon number and phase.

The two-mode squeezed vacuum state, as produced by the unitary two-mode squeeze operator in Eq. (71) corresponding to the non-degenerate optical parametric amplifier interaction Hamiltonian in Eq. (70), is equivalent to the two-mode state emerging from a 50:50 beam splitter with two single-mode squeezed vacuum states at the input. The simplest way to see this is in the Heisenberg representation. A single-mode vacuum state squeezed in p as in Eq. (59) with $\Theta=0$,

$$\hat{a}_1 = \hat{a}_1^{(0)}\cosh r + \hat{a}_1^{(0)\dagger}\sinh r, \tag{86}$$

and another one squeezed in x,

$$\hat{a}_2 = \hat{a}_2^{(0)}\cosh r - \hat{a}_2^{(0)\dagger}\sinh r, \tag{87}$$

are combined at a 50:50 beam splitter,

$$\begin{aligned}\hat{b}_1 &= (\hat{a}_1+\hat{a}_2)/\sqrt{2} = \hat{b}_1^{(0)}\cosh r + \hat{b}_2^{(0)\dagger}\sinh r,\\ \hat{b}_2 &= (\hat{a}_1-\hat{a}_2)/\sqrt{2} = \hat{b}_2^{(0)}\cosh r + \hat{b}_1^{(0)\dagger}\sinh r,\end{aligned} \tag{88}$$

where $\hat{b}_1^{(0)}=(\hat{a}_1^{(0)}+\hat{a}_2^{(0)})/\sqrt{2}$ and $\hat{b}_2^{(0)}=(\hat{a}_1^{(0)}-\hat{a}_2^{(0)})/\sqrt{2}$ are again two vacuum modes. The resulting state is a two-mode squeezed state as in Eq. (72) with vacuum inputs. The quadrature operators of the two-mode squeezed vacuum state can be written as

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

$$\hat{x}_2 = (e^{+r}\hat{x}_1^{(0)} - e^{-r}\hat{x}_2^{(0)})/\sqrt{2},$$

$$\hat{p}_2 = (e^{-r}\hat{p}_1^{(0)} - e^{+r}\hat{p}_2^{(0)})/\sqrt{2}, \tag{89}$$

where $\hat{b}_k = \hat{x}_k + i\hat{p}_k$ and $\hat{a}_k^{(0)} = \hat{x}_k^{(0)} + i\hat{p}_k^{(0)}$. Whereas the individual quadratures $\hat{x}_k$ and $\hat{p}_k$ become very noisy for large squeezing r, the relative position and the total momentum,

$$\hat{x}_1 - \hat{x}_2 = \sqrt{2}e^{-r}\hat{x}_2^{(0)},$$

$$\hat{p}_1 + \hat{p}_2 = \sqrt{2}e^{-r}\hat{p}_1^{(0)}, \tag{90}$$

become quiet, $\langle(\hat{x}_1-\hat{x}_2)^2\rangle = e^{-2r}/2$ and $\langle(\hat{p}_1+\hat{p}_2)^2\rangle = e^{-2r}/2$.

The two-mode squeezed vacuum state is the quantum optical representative for bipartite continuous-variable entanglement. In general, we may refer to continuous-variable entanglement whenever the entangled states are defined in an infinite-dimensional Hilbert space—for instance, that of two discrete quantized modes having position-momentum and number-phase quantum correlations. The Gaussian entangled states are then an important subclass of the continuous-variable entangled states. More general results on the creation of bipartite Gaussian continuous-variable entanglement were presented by Wolf *et al.* (2003) and by Kraus *et al.* (2003).

Complementary to its occurrence in quantum optical states, let us illuminate the notion of continuous-variable entanglement and, in particular, the entanglement of Gaussian states from the perspective and with the tools of quantum information theory. This leads to a rigorous definition of entanglement, necessarily given in the Schrödinger picture as a property of composite state vectors or, more generally, density operators. The link between this definition and the typical measurable quantities in a continuous-variable implementation, namely, the Gaussian moments of the quadratures, is provided by continuous-variable inseparability criteria or EPR-type nonlocality proofs, which are expressed in terms of the elements of the second-moment correlation matrix for the quadrature operators. We begin with the entanglement shared by only two parties.

A. Bipartite entanglement

1. Pure states

Bipartite entanglement, the entanglement of a pair of systems shared by two parties, is easy to handle for pure states. For any pure two-party state, orthonormal bases of each subsystem exist, $\{|u_n\rangle\}$ and $\{|v_n\rangle\}$, so that the total state vector can be written in the *Schmidt decomposition* (Schmidt, 1906) as

$$|\psi\rangle = \sum_n c_n|u_n\rangle|v_n\rangle, \tag{91}$$

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

$$|\psi\rangle = \sum_{mk} a_{mk}|m\rangle|k\rangle = \sum_{nmk} u_{mn}c_{nn}v_{kn}|m\rangle|k\rangle$$

$$= \sum_n c_n|u_n\rangle|v_n\rangle, \tag{92}$$

with $c_{nn} \equiv c_n$. In the first step, the matrix a with complex elements a_{mk} is diagonalized, $a = ucv^T$, where u and v are unitary matrices and c is a diagonal matrix with non-negative elements. In the second step, we define $|u_n\rangle \equiv \Sigma_m u_{mn}|m\rangle$ and $|v_n\rangle \equiv \Sigma_k v_{kn}|k\rangle$, which form orthonormal sets due to the unitarity of u and v and the orthonormality of $|m\rangle$ and $|k\rangle$. A pure state of two d-level systems, or *qudits*, is now maximally entangled when the Schmidt coefficients of its total state vector are all equal. Since the eigenvalues of the reduced density operator upon tracing out one-half of a bipartite state are the Schmidt coefficients squared,

$$\hat{\rho}_1 = \mathrm{Tr}_2\hat{\rho}_{12} = \mathrm{Tr}_2|\psi\rangle_{12}\langle\psi| = \sum_n c_n^2|u_n\rangle_1\langle u_n|, \tag{93}$$

tracing out either qudit of a maximally entangled state leaves the other half in the maximally mixed state $\mathbb{1}/d$. A pure two-party state is factorizable (not entangled) if and only if the number of nonzero Schmidt coefficients, the *Schmidt rank*, is 1.

A unique measure of bipartite entanglement for pure states is given by the partial von Neumann entropy, the von Neumann entropy $[S(\hat{\rho}) = -\mathrm{Tr}\hat{\rho}\ln\hat{\rho}]$ of the remaining system after tracing out either subsystem (Bennett, Bernstein, *et al.*, 1996): $E_{\text{v.N.}} = -\mathrm{Tr}\hat{\rho}_1\log_d\hat{\rho}_1 = -\mathrm{Tr}\hat{\rho}_2\log_d\hat{\rho}_2 = -\Sigma_n c_n^2\log_d c_n^2$, ranging between zero and one (in units of "edits"), with $\mathrm{Tr}_2\hat{\rho}_{12} = \hat{\rho}_1$, $\mathrm{Tr}_1\hat{\rho}_{12} = \hat{\rho}_2$. This entropy corresponds to the number of maximally entangled states contained in a given pure state. For example, $E_{\text{v.N.}} = 0.4$ means that asymptotically 1000 copies of the state can be transformed into 400 maximally entangled states via deterministic state transformations using local operations and classical communication (LOCC; Nielsen and Chuang, 2000).

According to Eq. (85), the Fock basis corresponds to the Schmidt basis of the two-mode squeezed vacuum state. In this Schmidt form, we can quantify the entanglement of the two-mode squeezed vacuum state via the partial von Neumann entropy (van Enk, 1999),

$$E_{\text{v.N.}} = -\ln(1-\lambda) - \lambda\ln\lambda/(1-\lambda)$$

$$= \cosh^2 r\ln(\cosh^2 r) - \sinh^2 r\ln(\sinh^2 r). \tag{94}$$

Note that any pure two-mode Gaussian state can be transformed into the canonical two-mode squeezed-state form via local linear unitary Bogoliubov transformations and hence its entanglement can be quantified as in Eq. (94). More generally, any bipartite pure multimode Gaussian state corresponds to a product of two-mode squeezed states up to local linear unitary Bogoliubov transformations (Botero and Reznik, 2003; Giedke, Eisert, *et al.*, 2003). In addition, the partial von Neumann entropy of a pure two-mode Gaussian state, corresponding to the entropy of an arbitrary single-mode Gaussian state, can be also directly computed (Agarwal, 1971).

In general, an important sign of entanglement is the violation of inequalities imposed by local realistic theories (Bell, 1964). Any pure two-party state is entangled if and only if, for suitably chosen observables, it yields a violation of such inequalities. The main features of *pure-state bipartite entanglement* will be summarized by

$$\text{entangled} \Leftrightarrow \text{Schmidt rank} > 1,$$

$$\text{entangled} \Leftrightarrow \text{partial von Neumann entropy} > 0,$$

$$\text{entangled} \Leftrightarrow \text{violations of local realism}. \tag{95}$$

All these conditions are necessary and sufficient.

2. Mixed states and inseparability criteria

The definition of pure-state entanglement via the nonfactorizability of the total state vector is generalized to mixed states through nonseparability (or inseparability) of the total density operator. A general quantum state of a two-party system is separable if its total density operator is a mixture (a convex sum) of product states (Werner, 1989),

$$\hat{\rho}_{12} = \sum_i \eta_i \hat{\rho}_{i,1} \otimes \hat{\rho}_{i,2}. \tag{96}$$

Otherwise, it is inseparable.[2] In general, it is a nontrivial question whether a given density operator is separable or inseparable. Nonetheless, a very convenient method of testing for inseparability is Peres's (1996) partial-transpose criterion. For a separable state as in Eq. (96), transposition of either density matrix yields again a legitimate non-negative density operator with unit trace,

$$\hat{\rho}'_{12} = \sum_i \eta_i (\hat{\rho}_{i,1})^T \otimes \hat{\rho}_{i,2}, \tag{97}$$

since $(\hat{\rho}_{i,1})^T = (\hat{\rho}_{i,1})^*$ corresponds to a legitimate density matrix. This is a necessary condition for a separable state, and hence a single negative eigenvalue of the partially transposed density matrix is a sufficient condition for inseparability (transposition is a so-called positive, but not completely positive map, which means its application to a subsystem may yield an unphysical state when the subsystem is entangled with other subsystems). In general, for states with arbitrary dimension, negative partial transpose (npt) is only sufficient for inseparability (Horodecki *et al.*, 1996a). Similarly, for arbitrary mixed states, the occurrence of violations of inequalities imposed by local realism is also only a sufficient, but not a necessary condition for inseparability (Werner, 1989). To summarize, for general *mixed-state bipartite inseparability*, the following statements hold:

$$\text{inseparable} \Leftarrow \text{npt},$$

$$\text{inseparable} \Leftarrow \text{violations of local realism}. \tag{98}$$

However, there are classes of states in which negative partial transpose becomes both necessary and sufficient, namely,

$$(2 \times 2)\text{-dimensional, inseparable} \Leftrightarrow \text{npt},$$

$$(2 \times 3)\text{-dimensional, inseparable} \Leftrightarrow \text{npt},$$

$$(1 \times N)\text{-mode Gaussian, inseparable} \Leftrightarrow \text{npt}. \tag{99}$$

Other sufficient inseparability criteria include an entropic inequality $[E_{\text{v.N.}}(\hat{\rho}_1) > E_{\text{v.N.}}(\hat{\rho}_{12})$, again with $\hat{\rho}_1 = \text{Tr}_2 \hat{\rho}_{12}$; Horodecki *et al.*, 1996b] and a condition based on the theory of majorization (Nielsen and Kempe, 2001). In the context of bound entanglement and distillability, the so-called reduction inseparability criterion (Horodecki and Horodecki, 1999) proves very useful (see below).

In Eq. (99), we made a statement about the inseparability of Gaussian states in terms of the partial-transpose criterion. What does partial transposition applied to bipartite Gaussian or, more generally, continuous-variable states actually mean? Due to the Hermiticity of a density operator, transposition corresponds to complex conjugation. Moreover, as for the time evolution of a quantum system described by the Schrödinger equation, complex conjugation is equivalent to time reversal, $i\hbar\partial/\partial t \to -i\hbar\partial/\partial t$. Hence, intuitively, transposition of a density operator means time reversal, or, in terms of continuous variables, sign change of the momentum variables. This observation and its application to the inseparability problem of continuous-variable states was a result of Simon (2000). Thus, in phase space, transposition is described by $\xi^T \to \Gamma \xi^T = (x_1, -p_1, x_2, -p_2, \ldots, x_N, -p_N)^T$, i.e., by transforming the Wigner function $W(x_1, p_1, x_2, p_2, \ldots, x_N, p_N) \to W(x_1, -p_1, x_2, -p_2, \ldots, x_N, -p_N)$. This general transposition rule for continuous variables is in the case of Gaussian states as in Eq. (35) reduced to $V^{(N)} \to \Gamma V^{(N)} \Gamma$ (where the first moments are not relevant to the separability properties, since they can be eliminated via LOCC).

Expressing partial transposition of a bipartite Gaussian system by $\Gamma_a \equiv \Gamma \oplus \mathbb{1}$ (where $A \oplus B$ means the block-diagonal matrix with the matrices A and B as diagonal entries, and A and B are, respectively, $2N \times 2N$ and $2M \times 2M$ square matrices applicable to N modes at a's

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

side and M modes at b's side), the condition that the partially transposed Gaussian state described by $\Gamma_a V^{(N+M)}\Gamma_a$ is unphysical [see Eq. (41)],

$$\Gamma_a V^{(N+M)}\Gamma_a \ngeq \frac{i}{4}\Lambda, \tag{100}$$

is sufficient for the inseparability between a and b (Simon, 2000; Werner and Wolf, 2001). For Gaussian states with $N=M=1$ (Simon, 2000) and for those with $N=1$ and arbitrary M (Werner and Wolf, 2001), this condition is necessary and sufficient. The simplest example in which the condition is no longer necessary for inseparability involves two modes at each side, $N=M=2$. In that case, entangled states with positive partial transpose, so-called bound entangled Gaussian states (see below), exist (Werner and Wolf, 2001). For the general bipartite $N\times M$ case of Gaussian states, there is also a necessary and sufficient condition: the correlation matrix $V^{(N+M)}$ corresponds to a separable state if and only if a pair of correlation matrices $V_a^{(N)}$ and $V_b^{(M)}$ exists such that (Werner and Wolf, 2001)

$$V^{(N+M)} \geqslant V_a^{(N)} \oplus V_b^{(M)}. \tag{101}$$

Since it is in general hard to find such a pair of correlation matrices $V_a^{(N)}$ and $V_b^{(M)}$ for a separable state or to prove the nonexistence of such a pair for an inseparable state, this criterion in not very practical. A more practical solution was proposed by Giedke, Kraus, *et al.* (2001b). For them, the operational criteria for Gaussian states, computable and testable via a finite number of iterations, are entirely independent of the npt criterion. They rely on a nonlinear map between the correlation matrices rather than a linear one such as the partial transposition, and, in contrast to the npt criterion, they witness also the inseparability of bound entangled states. Thus the separability problem for bipartite Gaussian states with arbitrarily many modes at each side is, in principle, completely solved.

Let us now consider arbitrary bipartite two-mode states. According to the definition of the N-mode correlation matrix $V^{(N)}$ in Eq. (38), we can write the correlation matrix of an arbitrary bipartite two-mode system in block form,

$$V^{(2)} = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{102}$$

where A, B, and C are real 2×2 matrices. Simon's continuous-variable version of the Peres-Horodecki partial-transpose criterion reads as follows (Simon, 2000):

$$\det A \det B + \left(\frac{1}{16} - |\det C|\right)^2 - \mathrm{Tr}(AJCJBJC^TJ) \geqslant \frac{1}{16}(\det A + \det B), \tag{103}$$

where J is the 2×2 matrix from Eq. (40). Any separable bipartite state satisfies the inequality of Eq. (103), so that it represents a necessary condition for separability, and hence its violation is a sufficient condition for inseparability. The inequality (103) is a consequence of the fact that the two-mode uncertainty relation, Eq. (41) with $N=2$, is preserved under partial transpose, $W(x_1,p_1,x_2,p_2)\to W(x_1,p_1,x_2,-p_2)$, provided the state is separable.

We may now define the following two standard forms for the correlation matrix:

$$V_{\mathrm{I}}^{(2)} = \begin{pmatrix} a & 0 & c & 0 \\ 0 & a & 0 & c' \\ c & 0 & b & 0 \\ 0 & c' & 0 & b \end{pmatrix} \tag{104}$$

and

$$V_{\mathrm{II}}^{(2)} = \begin{pmatrix} a_1 & 0 & c_1 & 0 \\ 0 & a_2 & 0 & c_2 \\ c_1 & 0 & b_1 & 0 \\ 0 & c_2 & 0 & b_2 \end{pmatrix}, \tag{105}$$

where the elements of the second standard form $V_{\mathrm{II}}^{(2)}$ satisfy

$$\begin{aligned} &\frac{a_1 - 1/4}{b_1 - 1/4} = \frac{a_2 - 1/4}{b_2 - 1/4}, \\ &|c_1| - |c_2| = \sqrt{(a_1 - 1/4)(b_1 - 1/4)} \\ &\qquad - \sqrt{(a_2 - 1/4)(b_2 - 1/4)}. \end{aligned} \tag{106}$$

Any correlation matrix can be transformed into the first standard form $V_{\mathrm{I}}^{(2)}$ via appropriate local canonical transformations (Simon, 2000); i.e., via local linear unitary Bogoliubov transformations like that given in Eq. (51). From the first standard form $V_{\mathrm{I}}^{(2)}$, two appropriate local squeezing operations can always lead to the second standard form $V_{\mathrm{II}}^{(2)}$ (Duan, Giedke, *et al.*, 2000a).

For the standard form $V_{\mathrm{I}}^{(2)}$, the necessary separability condition of Eq. (103) simplifies to

$$16(ab - c^2)(ab - c'^2) \geqslant (a^2 + b^2) + 2|cc'| - \frac{1}{16}. \tag{107}$$

Simon's criterion does not rely on that specific standard form and can, in fact, be applied to an arbitrary (even non-Gaussian) state using Eq. (103). For Gaussian two-mode states, however, Eq. (103) turns out to be both a necessary and a sufficient condition for separability (Simon, 2000).

A similar inseparability criterion, applicable to two-mode continuous-variable systems and expressed in terms of an inequality for certain variances involving position and momentum operators, was derived by Duan, Giedke, *et al.* (2000a) using a strategy independent of the partial transpose. This criterion relies upon the standard form $V_{\mathrm{II}}^{(2)}$ to follow through as a necessary and sufficient condition for two-mode Gaussian states. Expressed in terms of the elements of $V_{\mathrm{II}}^{(2)}$, the necessary and sufficient condition for the separability of two-mode Gaussian states reads

$$\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho \geq \frac{a_0^2}{2} + \frac{1}{2a_0^2}, \tag{108}$$

where

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

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

$$a_0^2 = \sqrt{\frac{b_1 - 1/4}{a_1 - 1/4}} = \sqrt{\frac{b_2 - 1/4}{a_2 - 1/4}}, \tag{109}$$

and the bipartite state of interest $\hat{\rho}$ has been labeled ρ. Without the assumption of Gaussian states, an alternative approach (Duan, Giedke, *et al.*, 2000a), based solely on the Heisenberg uncertainty relation of position and momentum and on the Cauchy-Schwarz inequality, leads to an inequality similar to Eq. (108). It represents only a necessary condition for the separability of arbitrary states,

$$\begin{aligned}\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho &\geq \bar{a}^2|\langle[\hat{x}_1,\hat{p}_1]\rangle_\rho| + |\langle[\hat{x}_2,\hat{p}_2]\rangle_\rho|/\bar{a}^2\\ &= \frac{\bar{a}^2}{2} + \frac{1}{2\bar{a}^2},\end{aligned} \tag{110}$$

with

$$\hat{u} = |\bar{a}|\hat{x}_1 - \frac{1}{\bar{a}}\hat{x}_2,$$

$$\hat{v} = |\bar{a}|\hat{p}_1 + \frac{1}{\bar{a}}\hat{p}_2. \tag{111}$$

Here, $\bar{a}$ is an arbitrary nonzero real parameter. Let us also mention that a similar inseparability criterion was derived by Tan (1999), namely, the necessary condition for any separable state,

$$\langle(\Delta\hat{u})^2\rangle_\rho\langle(\Delta\hat{v})^2\rangle_\rho \geq \frac{1}{4}, \tag{112}$$

with $\bar{a}=1$ in Eq. (111). This criterion is simply the product version of the sum condition in Eq. (110) (with $\bar{a}=1$). A generalization of these two-party separability conditions can be found in the work of Giovannetti *et al.* (2003), including a discussion on how they are related to each other. In this respect, defining the general linear combinations

$$\hat{u} \equiv h_1\hat{x}_1 + h_2\hat{x}_2, \quad \hat{v} \equiv g_1\hat{p}_1 + g_2\hat{p}_2, \tag{113}$$

let us only note here that, for any separable state, we have

$$\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho \geq (|h_1g_1| + |h_2g_2|)/2, \tag{114}$$

whereas for a potentially entangled state, this bound is changed to

$$\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho \geq (|h_1g_1 + h_2g_2|)/2. \tag{115}$$

The h_l and g_l are arbitrary real parameters. When choosing, for instance, $h_1=-h_2=g_1=g_2=1$, the bound for a separable state becomes 1, whereas that for an entangled state drops to 0. In fact, with this choice, $\hat{u}=\hat{x}_1-\hat{x}_2$ and $\hat{v}=\hat{p}_1+\hat{p}_2$, quantum mechanics allows the observables $\hat{u}$ and $\hat{v}$ to simultaneously take on arbitrarily well-defined values because of the vanishing commutator,

$$[\hat{x}_1 - \hat{x}_2,\hat{p}_1 + \hat{p}_2] = 0. \tag{116}$$

The inseparability criteria discussed above are fulfilled by the two-mode squeezed vacuum state for any nonzero squeezing. For example, according to Eqs. (82) and (35), its correlation matrix is given by

$$V^{(2)} = \frac{1}{4}\begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0\\ 0 & \cosh 2r & 0 & -\sinh 2r\\ \sinh 2r & 0 & \cosh 2r & 0\\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix}. \tag{117}$$

This matrix is in standard form $V_{\mathrm{I}}^{(2)}$. Hence one can easily verify that Simon's separability condition (107) is violated for any $r>0$. Even simpler is the application of Eq. (90) for the two-mode squeezed vacuum state to the condition in Eq. (110), which is also violated for any $r>0$.

Separability conditions similar to those above can also be derived in terms of the polarization Stokes operators from Eq. (73) (Bowen *et al.*, 2002; Korolkova *et al.*, 2002; Korolkova and Loudon, 2005). When doing this, in general, one must take into account the operator-valued commutator of the Stokes operators $[\hat{S}_j,\hat{S}_k]=i\epsilon_{jkl}\hat{S}_l$. Analogously, a possible sum condition in terms of the collective spin variables of two atomic ensembles [see Eq. (74)], always satisfied for separable systems, is (Kuzmich and Polzik, 2003)

$$\begin{aligned}&\langle[\Delta(\hat{F}_{x1} + \hat{F}_{x2})]^2\rangle_\rho + \langle[\Delta(\hat{F}_{y1} + \hat{F}_{y2})]^2\rangle_\rho\\ &\quad\geq |\langle\hat{F}_{z1}\rangle_\rho| + |\langle\hat{F}_{z2}\rangle_\rho|.\end{aligned} \tag{118}$$

Note that, in contrast to the conditions in Eq. (110) or (114), the condition in Eq. (118) has, in general, a state-dependent bound due to the operator-valued commutator $[\hat{F}_j,\hat{F}_k]=i\epsilon_{jkl}\hat{F}_l$. However, as discussed in Sec. II.F, within the subset of states with a large classical mean polarization along the z axis, the commutators of $\hat{F}_x$ and $\hat{F}_y$ resemble those of $\hat{x}$ and $\hat{p}$. One may choose two spins with opposite classical orientation, $\langle\hat{F}_{z1}\rangle=-\langle\hat{F}_{z2}\rangle=F$, yielding

$$\langle[\Delta(\hat{F}_{x1}+\hat{F}_{x2})]^2\rangle_\rho + \langle[\Delta(\hat{F}_{y1}+\hat{F}_{y2})]^2\rangle_\rho \geqslant 2F. \qquad (119)$$

With this choice, and using $\hat{F}_{zj}\simeq\langle\hat{F}_{zj}\rangle$, $j=1,2$, the vanishing commutator

$$[\hat{F}_{x1}+\hat{F}_{x2},\hat{F}_{y1}+\hat{F}_{y2}] = i(\hat{F}_{z1}+\hat{F}_{z2}) = 0 \qquad (120)$$

permits an arbitrarily large violation of Eq. (119) for entangled states. As in Eq. (110), where (for $\bar{a}=1$) the bound is four vacuum units corresponding to uncorrelated quadratures of the two modes, entanglement is present according to Eq. (119) when the total spin variances are smaller than those of uncorrelated atoms in two collective vacuum states, each with $\langle(\Delta\hat{F}_x)^2\rangle = \langle(\Delta\hat{F}_y)^2\rangle = F/2$ [see Eq. (74)].

As for the quantification of bipartite mixed-state entanglement, there are various measures available such as the *entanglement of formation* and distillation (Bennett, DiVincenzo, *et al.*, 1996). Only for pure states do these measures coincide and equal the partial von Neumann entropy. In general, the entanglement of formation is hard to compute. However, apart from the qubit case (Wootters, 1998), for symmetric two-mode Gaussian states given by a correlation matrix in Eq. (104) with $a = b$, the entanglement of formation can be calculated via the total variances in Eq. (110) (Giedke, Wolf, *et al.*, 2003). A Gaussian version of the entanglement of formation was proposed by Wolf *et al.* (2004). Another computable measure of entanglement for any mixed state of an arbitrary bipartite system, including bipartite Gaussian states, is the "logarithmic negativity" based on the negativity of the partial transpose (Vidal and Werner, 2002).

B. Multipartite entanglement

Multipartite entanglement, the entanglement shared by more than two parties, is a subtle issue even for pure states. In that case, for pure multiparty states, a Schmidt decomposition does not exist in general. The total state vector then cannot be written as a single sum over orthonormal basis states. Let us first consider discrete-variable multipartite entanglement.

1. Discrete variables

There is one very important representative of multipartite entanglement that does have the form of a multiparty Schmidt decomposition, namely, the Greenberger-Horne-Zeilinger (GHZ) state (Greenberger *et al.*, 1990),

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \qquad (121)$$

here given as a three-qubit state. Although there is no rigorous definition of maximally entangled multiparty states due to the lack of a general Schmidt decomposition, the form of the GHZ state with all Schmidt coefficients equal suggests that it exhibits maximum multipartite entanglement. In fact, there are various reasons for describing as "maximally entangled" the N-party GHZ states, $(|000\cdots000\rangle+|111\cdots111\rangle)/\sqrt{2}$. For example, they yield the maximum violations of multiparty inequalities imposed by local realistic theories (Mermin, 1990; Klyshko, 1993; Gisin and Bechmann-Pasquinucci, 1998). Further, their entanglement heavily relies on all parties, and, if examined pairwise, they do not contain simple bipartite entanglement (see below).

For the case of three qubits, any pure and fully entangled state can be transformed to either the GHZ state or the so-called W state (Dür, Vidal, and Cirac, 2000),

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle), \qquad (122)$$

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

$$\mathrm{Tr}_1|W\rangle\langle W| = \frac{1}{3}(|00\rangle\langle 00| + |10\rangle\langle 10| + |01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01|) \qquad (123)$$

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

$$\mathrm{Tr}_1|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}| = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|). \qquad (124)$$

Maximum bipartite entanglement is available from the GHZ state through a local measurement of one party in the conjugate basis $\{|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}\}$ (plus classical communication about the result),

$$\frac{|\pm\rangle_{11}\langle\pm|\mathrm{GHZ}\rangle}{\||\pm\rangle_{11}\langle\pm|\mathrm{GHZ}\rangle\|} = |\pm\rangle_1 \otimes |\Phi^\pm\rangle. \qquad (125)$$

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

What can be said about arbitrary mixed entangled states of more than two parties? There is of course an immense variety of inequivalent classes of multiparty mixed states, e.g., five classes of three-qubit states of which the extreme cases are the fully separable, $\sum_i \eta_i \hat{\rho}_{i,1}\otimes\hat{\rho}_{i,2}\otimes\hat{\rho}_{i,3}$, and the genuinely tripartite inseparable states (Dür, Cirac, and Tarrach, 1999).

2. Genuine multipartite entanglement

The term *genuine multipartite entanglement* refers to states in which none of the parties can be separated from any other party in a mixture of product states. In general, multiparty inseparability criteria cannot be formulated in such a compact form as for two parties. In order to verify genuine N-party entanglement, one has to rule out any possible partially separable form. In principle, this can be done by considering all possible bipartite splittings (or groupings) and, for instance, applying the npt criterion. Moreover, the quantification of multipartite entanglement, even for pure states, is still the subject of current research. Violations of multiparty inequalities imposed by local realism do not necessarily imply genuine multiparty inseparability. The following statements hold for pure or mixed multipartite entangled states (both discrete and continuous variables):

$$\begin{array}{ccc} \text{partially entangled} & \Leftarrow & \text{violations of } N\text{-party} \\ & & \text{Bell-type inequalities,} \\ \text{genuinely} & \not\Leftarrow & \text{violations of } N\text{- party} \\ \text{multipartite entangled} & & \text{Bell-type inequalities.} \end{array} \qquad (126)$$

An example of the last statement is the pure genuinely N-party entangled state

$$|\psi\rangle = \cos\alpha|00\cdots 0\rangle + \sin\alpha|11\cdots 1\rangle, \qquad (127)$$

which for $\sin 2\alpha \leqslant 1/\sqrt{2^{N-1}}$ does not violate any N-party Bell inequality (Bell, 1964), if N odd, and does not violate Mermin-Klyshko inequalities (Mermin, 1990; Klyshko, 1993; Gisin and Bechmann-Pasquinucci, 1998) for any N. Genuine multipartite entanglement can be verified only via sufficiently large violations (Seevinck and Uffink, 2001) of Mermin-Klyshko inequalities. Another sufficient condition for the genuine N-party entanglement of an N-qubit state $\hat{\rho}$ exists, namely, $\langle \mathrm{GHZ}|\hat{\rho}|\mathrm{GHZ}\rangle > 1/2$ (Seevinck and Uffink, 2001).

3. Separability properties of Gaussian states

As for the continuous-variable case, the criteria of Giedke, Kraus, *et al.* (2001c) determine to which of five possible classes of fully and partially separable, and fully inseparable states a three-party three-mode Gaussian state belongs. Hence genuine tripartite entanglement, if present, can be unambiguously identified. The classification is mainly based on the npt criterion for continuous-variable states. For three-party three-mode Gaussian states, the only partially separable forms are those with a bipartite splitting of 1×2 modes. Hence already the npt criterion is necessary and sufficient.

The classification of tripartite three-mode Gaussian states (Giedke, Kraus, *et al.* 2001c),

$$\text{class 1:}\quad \bar{V}_1^{(3)} \not\geqslant \frac{i}{4}\Lambda, \bar{V}_2^{(3)} \not\geqslant \frac{i}{4}\Lambda, \bar{V}_3^{(3)} \not\geqslant \frac{i}{4}\Lambda;$$

$$\text{class 2:}\quad \bar{V}_k^{(3)} \geqslant \frac{i}{4}\Lambda, \bar{V}_m^{(3)} \not\geqslant \frac{i}{4}\Lambda, \bar{V}_n^{(3)} \not\geqslant \frac{i}{4}\Lambda;$$

$$\text{class 3:}\quad \bar{V}_k^{(3)} \geqslant \frac{i}{4}\Lambda, \bar{V}_m^{(3)} \geqslant \frac{i}{4}\Lambda, \bar{V}_n^{(3)} \not\geqslant \frac{i}{4}\Lambda;$$

$$\text{class 4 or 5:}\quad \bar{V}_1^{(3)} \geqslant \frac{i}{4}\Lambda, \bar{V}_2^{(3)} \geqslant \frac{i}{4}\Lambda, \bar{V}_3^{(3)} \geqslant \frac{i}{4}\Lambda, \qquad (128)$$

is solely based on the npt criterion, where $\bar{V}_j^{(3)} \equiv \Gamma_j V^{(3)} \Gamma_j$ denotes the partial transposition with respect to one mode j. In classes 2 and 3, every permutation of modes (k,m,n) must be considered. Class 1 corresponds to the fully inseparable states. Class 5 contains the fully separable states. A Gaussian state described by $V^{(3)}$ is fully separable if and only if one-mode correlation matrices $V_1^{(1)}$, $V_2^{(1)}$, and $V_3^{(1)}$ exist such that $V^{(3)} \geqslant V_1^{(1)} \oplus V_2^{(1)} \oplus V_3^{(1)}$. In general, fully separable quantum states can be written as a mixture of tripartite product states, $\Sigma_i \eta_i \hat{\rho}_{i,1} \otimes \hat{\rho}_{i,2} \otimes \hat{\rho}_{i,3}$. In class 2, we have the one-mode biseparable states, in which only one particular mode is separable from the remaining pair of modes. This means in the Gaussian case that only for one particular mode k, $V^{(3)} \geqslant V_k^{(1)} \oplus V_{mn}^{(2)}$ with some two-mode correlation matrix $V_{mn}^{(2)}$ and one-mode correlation matrix $V_k^{(1)}$. In general, such a state can be written as $\Sigma_i \eta_i \hat{\rho}_{i,k} \otimes \hat{\rho}_{i,mn}$ for one mode k. Class 3 contains those states in which two but not three bipartite splittings are possible, i.e., two different modes k and m are separable from the remaining pair of modes (two-mode biseparable states). The states of class 4 (three-mode biseparable states) can be written as a mixture of products between any mode 1, 2, or 3 and the remaining pair of modes, but not as a mixture of three-mode product states. Obviously, classes 4 and 5 are not distinguishable via the npt criterion. An additional criterion for this distinction of class 4 and 5 Gaussian states is given by Giedke, Kraus, *et al.* (2001c), deciding whether one-mode correlation matrices $V_1^{(1)}$, $V_2^{(1)}$, and $V_3^{(1)}$ exist such that $V^{(3)} \geqslant V_1^{(1)} \oplus V_2^{(1)} \oplus V_3^{(1)}$. For the identification of genuinely tripartite entangled Gaussian states, only class 1 has to be distinguished from the rest. Hence the npt criterion alone suffices.

What about more than three parties and modes? Even for only four parties and modes, the separability issue becomes more subtle. The one-mode bipartite splittings, $\Sigma_i \eta_i \hat{\rho}_{i,klm} \otimes \hat{\rho}_{i,n}$, can be tested and possibly ruled out via the npt criterion with respect to any mode n. In the Gaussian language, if $\bar{V}_n^{(4)} \not\geqslant (i/4)\Lambda$ for any n, the state cannot be written in the above form. Since we consider here the bipartite splitting of 1×3 modes, the npt condition is necessary and sufficient for Gaussian states. However, a state of the form $\Sigma_i \eta_i \hat{\rho}_{i,kl} \otimes \hat{\rho}_{i,mn}$ also leads to negative partial transpose with respect to any of the four modes when the two pairs (k,l) and (m,n) are each entangled. Thus npt with respect to any individual mode is necessary but not sufficient for genuine four-party entanglement. One also has to consider the partial transposition with respect to any pair of modes. For this 2×2 mode case, however, we know that entangled Gaussian states with positive partial transpose exist (Werner and Wolf, 2001). But the npt criterion is still sufficient for inseparability between any two pairs. As for a necessary and sufficient condition, one can use those given by Giedke, Kraus, *et al.* (2001b). In any case, in order to confirm genuine four-party or even N-party entanglement, one has to rule out any possible partially separable form. In principle, this can be done by considering all possible bipartite splittings (or groupings) and applying either the npt criterion or the stronger operational criteria of Giedke, Kraus, *et al.* (2001b). Although a full theoretical characterization including criteria for entanglement classification has not been considered yet for more than three parties and modes, the presence of genuine multipartite entanglement can be confirmed, once the complete $2N\times 2N$ correlation matrix is given.

4. Generating entanglement

In this section, we show how to generate genuine multipartite continuous-variable entanglement of arbitrarily many modes from finitely squeezed sources. The resulting states are nonmaximally entangled due to finite squeezing. How measurements on the maximally entangled basis of arbitrarily many modes can be performed with linear optics and homodyne detections will be discussed in the next section.

Let us consider a family of genuinely N-party entangled continuous-variable states. The members of this family are those states that emerge from a particular sequence of $N-1$ phase-free beam splitters (an N splitter) with N squeezed-state inputs (van Loock and Braunstein, 2000a). The recipe for the generation of these states stems from the quantum circuit for creating qubit GHZ states.

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

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), \quad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle), \tag{129}$$

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

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle,$$
$$|10\rangle \to |11\rangle, \quad |11\rangle \to |10\rangle. \tag{130}$$

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

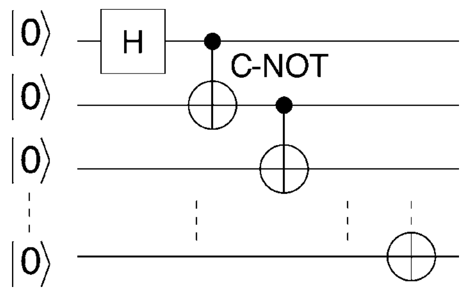

FIG. 1. Quantum circuit for generating the N-qubit Greenberger-Horne-Zeilinger (GHZ) state. The gates (unitary transformations) are a Hadamard gate ("H") and pairwise-acting controlled-NOT gates.

Let us translate the qubit quantum circuit to continuous variables (van Loock and Braunstein, 2000a). For this purpose, it is convenient to consider position and momentum eigenstates. We may replace the Hadamard by a Fourier transform,

$$\hat{\mathcal{F}}|x\rangle_{\text{position}} = \frac{1}{\sqrt{\pi}}\int_{-\infty}^{\infty} dy e^{2ixy}|y\rangle_{\text{position}} = |p=x\rangle_{\text{momentum}}, \tag{131}$$

and the controlled-NOT gates by appropriate beam splitter operations.[3] The input states are taken to be zero-position eigenstates $|x=0\rangle$. The sequence of beam-splitter operations $\hat{B}_{jk}(\theta)$ is provided by a network of ideal phase-free beam splitters (with typically asymmetric transmittance and reflectivity) acting on the position eigenstates of two modes as in Eq. (49).

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

$$\hat{B}_{N-1N}(\pi/4)\hat{B}_{N-2N-1}(\sin^{-1}1/\sqrt{3}) \times \cdots \times \hat{B}_{12}(\sin^{-1}1/\sqrt{N}), \tag{132}$$

to a zero-momentum eigenstate $|p=0\rangle \propto \int dx|x\rangle$ of mode 1 (the Fourier-transformed zero-position eigenstate) and $N-1$ zero-position eigenstates $|x=0\rangle$ in modes 2 through N. We obtain the entangled N-mode state $\int dx|x,x,\ldots,x\rangle$. This state is an eigenstate with total momentum zero and all relative positions $x_i-x_j=0$ $(i,j=1,2,\ldots,N)$. It is clearly an analog to the qubit GHZ state with perfect correlations among the quadratures. However, it is an unphysical and unnormalizable state. Rather than sending infinitely squeezed position eigen-

[3] A possible continuous-variable generalization of the controlled-NOT gate is $|x_1,x_2\rangle \to |x_1,x_1+x_2\rangle$, where the addition modulo two of the qubit CNOT, $|y_1,y_2\rangle \to |y_1,y_1\oplus y_2\rangle$, with $y_1,y_2=0,1$, has been replaced by the normal addition. However, for the quantum circuit here, a beam-splitter operation as described by Eq. (49) is a suitable substitute for the generalized controlled-NOT gate.

states through the entanglement-generating circuit, we shall now use finitely squeezed states.

In the Heisenberg representation, an ideal phase-free beam-splitter operation acting on two modes is described by Eq. (45). Let us now define a matrix $B_{kl}(\theta)$ which is an N-dimensional identity matrix with the entries I_{kk}, I_{kl}, I_{lk}, and I_{ll} replaced by the corresponding entries of the beam- splitter matrix in Eq. (45). Thus the matrix for the N splitter becomes

$$\mathcal{U}(N) \equiv B_{N-1N}\left(\sin^{-1}\frac{1}{\sqrt{2}}\right)B_{N-2N-1}\left(\sin^{-1}\frac{1}{\sqrt{3}}\right) \times \cdots \times B_{12}\left(\sin^{-1}\frac{1}{\sqrt{N}}\right). \tag{133}$$

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

$$(\hat{a}_1'\hat{a}_2'\cdots\hat{a}_N')^T = \mathcal{U}(N)(\hat{a}_1\hat{a}_2\cdots\hat{a}_N)^T, \tag{134}$$

where the input modes are squeezed according to

$$\hat{a}_1 = \cosh r_1\hat{a}_1^{(0)} + \sinh r_1\hat{a}_1^{(0)\dagger},$$

$$\hat{a}_i = \cosh r_2\hat{a}_i^{(0)} - \sinh r_2\hat{a}_i^{(0)\dagger}, \tag{135}$$

with $i=2,3,\ldots,N$. In terms of the input quadratures, we have

$$\hat{x}_1 = e^{+r_1}\hat{x}_1^{(0)}, \quad \hat{p}_1 = e^{-r_1}\hat{p}_1^{(0)},$$

$$\hat{x}_i = e^{-r_2}\hat{x}_i^{(0)}, \quad \hat{p}_i = e^{+r_2}\hat{p}_i^{(0)}, \tag{136}$$

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

$$\langle(\hat{x}_k' - \hat{x}_l')^2\rangle = e^{-2r_2}/2,$$

$$\langle(\hat{p}_1' + \hat{p}_2' + \cdots + \hat{p}_N')^2\rangle = Ne^{-2r_1}/4, \tag{137}$$

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

The output states from Eq. (134) are pure N-mode states, totally symmetric under interchange of modes, and they retain the Gaussian character of the input states. Hence they are entirely described by their second-moment correlation matrix,

$$V^{(N)} = \frac{1}{4}\begin{pmatrix} a & 0 & c & 0 & c & 0 & \cdots \\ 0 & b & 0 & d & 0 & d & \cdots \\ c & 0 & a & 0 & c & 0 & \cdots \\ 0 & d & 0 & b & 0 & d & \cdots \\ c & 0 & c & 0 & a & 0 & \cdots \\ 0 & d & 0 & d & 0 & b & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}, \tag{138}$$

where

$$a = \frac{1}{N}e^{+2r_1} + \frac{N-1}{N}e^{-2r_2},$$

$$b = \frac{1}{N}e^{-2r_1} + \frac{N-1}{N}e^{+2r_2},$$

$$c = \frac{1}{N}(e^{+2r_1} - e^{-2r_2}),$$

$$d = \frac{1}{N}(e^{-2r_1} - e^{+2r_2}). \tag{139}$$

For squeezed vacuum inputs, the multimode output states have zero mean and their Wigner function is of the form Eq. (35). The particularly simple form of the correlation matrix in Eq. (138) is, in addition to the general correlation matrix properties, symmetric with respect to all modes and contains no intermode or intramode x-p correlations (hence only the four parameters a, b, c, and d appear in the matrix). However, the states of this form are in general biased with respect to x and p $(a \neq b)$. Only for a particular relation between the squeezing values (r_1,r_2) (van Loock, 2002; van Loock and Braunstein, 2003),

$$e^{\pm 2r_1} = (N-1) \times \sinh 2r_2\left[\sqrt{1 + \frac{1}{(N-1)^2\sinh^2 2r_2}} \pm 1\right], \tag{140}$$

are the states unbiased (all diagonal entries of the correlation matrix equal), thus having minimum energy at a given degree of entanglement or, in other words, maximum entanglement for a given mean photon number (Bowen, Lam, and Ralph, 2003). The other N-mode states of the family (van Loock, 2002; van Loock and Braunstein, 2003) can be converted into the minimum-energy state via local squeezing operations (Bowen, Lam, and Ralph, 2003). Only for $N=2$ do we obtain $r=r_1=r_2$. In this case, the matrix $V^{(N)}$ reduces to that of a two-mode squeezed state, which is the maximally entangled state of two modes at a given mean energy with the correlation matrix given in Eq. (117). For general N, the first squeezer with r_1 and the $N-1$ remaining squeezers with r_2 have different squeezing. In the limit of large squeezing $(\sinh 2r_2 \approx e^{+2r_2}/2)$, we obtain approximately (van Loock, 2002; van Loock and Braunstein, 2003)

$$e^{+2r_1} \approx (N-1)e^{+2r_2}. \tag{141}$$

We see that in order to produce the minimum-energy N-mode state, the single r_1 squeezer is, in terms of the squeezing factor, $N-1$ times as squeezed as each r_2 squeezer. However, in this general N-mode case, the other N-mode states of the family can also be converted into the minimum-energy state via local squeezing operations.

Why is the N-mode state described by the correlation matrix in Eq. (138) genuinely N-partite entangled?

Simple arguments already suffice to confirm this. One such argument is that the Wigner function of the N-mode state is not even partially factorizable. Neither the Wigner function of a single mode nor that of a group of modes can be factored out from the total Wigner function. This argument depends on the purity of the N-mode state, since the Wigner function of a mixed and only classically correlated state is not factorizable either. The N-mode state described by Eq. (138) is indeed pure, because it is built from N pure single-mode states via linear optics. Apart from its purity, taking into account its total symmetry, the presence of any kind of (partial) entanglement proves the genuine N-partite entanglement of the state (van Loock, 2002). For example, according to Eq. (138), upon tracing out all modes except one, we see that the remaining single-mode correlation matrix satisfies $\det V^{(1)} > 1/16$ for any N and any $r_1 > 0$ or $r_2 > 0$. The remaining mode is then in a mixed state, thus proving its entanglement with at least some of the other modes. Hence due to the purity and symmetry, the total state is genuinely N-partite entangled. Note that this holds true even for $r_1 > 0$ and $r_2 = 0$. Thus only one squeezed state suffices to make genuine N-partite entanglement via linear optics (van Loock and Braunstein, 2000a). For three parties and modes, $N=3$, checking the npt criterion is simple too. One has to apply transposition only with respect to each mode 1, 2, and 3, in order to rule out any partially separable form $\Sigma_i \eta_i \hat{\rho}_{i,k} \otimes \hat{\rho}_{i,mn}$. Due to the symmetry, npt with respect to mode 1 is sufficient (and necessary) for genuine tripartite entanglement. The resulting three-mode state belongs to the fully inseparable class 1 in Eq. (128).

The separability properties of mixed versions of the three-mode state in Eq. (138) with $N=3$, having the same correlation matrix contaminated by some noise, $V^{(3)}_{\text{noisy}} = V^{(3)} + \mu \mathbb{1}/4$, are more subtle. In that case, for given squeezing $r = r_1 = r_2 > 0$, the state becomes three-mode biseparable [class 4 in Eq. (128)] above some threshold value μ_0, $\mu \geqslant \mu_0 > 0$, and fully separable [class 5 in Eq. (128)] above some greater value μ_1, $\mu \geqslant \mu_1 > \mu_0$ (Giedke, Kraus, *et al.*, 2001c). Note that due to symmetry, the state described by $V^{(3)}_{\text{noisy}}$ can only belong to the classes 1, 4, and 5. Classes 4 and 5 are not distinguishable via partial transpose, but the full separability (class 5) is proven if and only if one-mode correlation matrices $V^{(1)}_1$, $V^{(1)}_2$, and $V^{(1)}_3$ exist such that $V^{(3)}_{\text{noisy}} \geqslant V^{(1)}_1 \oplus V^{(1)}_2 \oplus V^{(1)}_3$ (Giedke, Kraus, *et al.*, 2001c). In particular, for $\mu \geqslant 1$, we have $V^{(1)}_1 = V^{(1)}_2 = V^{(1)}_3 = \mathbb{1}/4$, thus confirming the full separability of the state in that case.

How do the GHZ-like continuous-variable states described by Eq. (138) behave compared to the qubit GHZ states? For finite squeezing, they actually behave more like the qubit W state in Eq. (122) than the maximally entangled qubit GHZ state in Eq. (121) (van Loock and Braunstein, 2003). For three parties, for instance, bipartite two-mode mixed-state entanglement is readily available upon tracing out one mode (van Loock, 2002; van Loock and Braunstein, 2003; see also the very recent results on Gaussian multipartite entanglement by Adesso *et al.*, 2004 and by Adesso and Illuminati, 2004).

5. Measuring entanglement

In addition to the generation of entangled states, an important task is the measurement of multiparty entanglement, i.e., projection onto the basis of maximally entangled multiparty states. For qubits, it is well known that this can be achieved simply by inverting the above entanglement-generating circuit (Fig. 1). A similar strategy also works for d-level systems (Dušek, 2001).

For creating continuous-variable entanglement, we replaced the controlled-NOT gates in Fig. 1 by appropriate beam-splitter operations. The same strategy, after inverting the circuit in Fig. 1, also enables one to measure continuous-variable entanglement. In other words, a projection onto the continuous-variable GHZ basis can be performed by applying an inverse N splitter followed by a Fourier transform of one mode and by subsequently measuring the positions of all modes (van Loock, 2002). The simplest example is the continuous-variable Bell measurement, needed, for instance, in continuous-variable quantum teleportation (see Sec. IV.A). It can be accomplished by using a symmetric beam splitter and detecting the position of one output mode and the momentum of the other output mode.

We see that the requirements of a Bell-state analyzer and, more generally, a GHZ-state analyzer for continuous variables are easily met by current experimental capabilities. This is in contrast to Bell- and GHZ-state analyzers for photonic qubits (Lütkenhaus *et al.*, 1999; Vaidman and Yoran, 1999; van Loock and Lütkenhaus, 2004). Although arbitrarily high efficiencies can be approached, in principle, using linear optics, photon number detectors, and feedforward, one would need sufficiently many highly entangled auxiliary photons and detectors, resolving correspondingly large photon numbers (Dušek, 2001; Knill *et al.*, 2001). Neither of these requirements is met by current technology. Of course, the controlled-NOT gates of a qubit Bell- and GHZ-state measurement device can, in principle, be implemented via the cross Kerr effect using nonlinear optics. However, on the single-photon level, the required optical nonlinearities are hard to obtain.

The efficient and unconditional generation of (multipartite) entanglement, though nonmaximum for finite squeezing, and the simple and feasible linear-optics schemes for measuring maximum (multipartite) continuous-variable entanglement demonstrate the power of quantum optical entanglement manipulation based on continuous variables. However, the capabilities of such purely continuous-variable-based schemes, which rely exclusively on Gaussian operations such as beam splitting, homodyne detection, and squeezing, are not unlimited. This is revealed, in particular, by the no-go results for continuous-variable entanglement distillation (see Sec. IV.E).

C. Bound entanglement

There are two big issues related to composite mixed quantum states: separability and distillability. The former was the subject of the previous sections. For continuous variables, the separability problem is, in general, not completely solved yet. In the special case of Gaussian states, however, we mentioned that necessary and sufficient inseparability criteria (different from the npt criterion) for bipartite states of arbitrarily many modes exist. The situation is similar with regard to distillability. The distillability of general continuous-variable states is an open question, whereas that of bipartite Gaussian states with arbitrarily many modes is completely characterized by the partial-transpose criterion: any $N\times M$ Gaussian state is distillable if and only if it is npt (Giedke, Kraus, *et al.*, 2001a, 2001b). A state is distillable if a sufficiently large number of copies of the state can be converted into a pure maximally entangled state (or arbitrarily close to it) via local operations and classical communication. Entanglement distillation [or "purification" (Bennett, Brassard, *et al.*, 1996)] is essential for quantum communication when the two halves of a supply of entangled states are distributed through noisy channels, distilled, and subsequently used, for instance, for high-fidelity quantum teleportation.

In general, any inseparable state with positive partial transpose cannot be distilled to a maximally entangled state, thus representing a so-called bound entangled state (Horodecki *et al.*, 1998). In other words, npt is necessary for distillability. Is it in general sufficient too? There are conjectures that this is not the case and that undistillable (bound) npt states exist (DiVincenzo *et al.*, 2000; Dür, Cirac, *et al.*, 2000). On the other hand, any state $\hat{\rho}_{12}$ that satisfies the so-called reduction criterion, $\hat{\rho}_1\otimes\mathbb{1}-\hat{\rho}_{12}\not\geq 0$ or $\mathbb{1}\otimes\hat{\rho}_2-\hat{\rho}_{12}\not\geq 0$, where $\hat{\rho}_1=\mathrm{Tr}_2\,\hat{\rho}_{12}$, etc., is both inseparable and distillable (Horodecki and Horodecki, 1999). The reduction criterion is sufficient for distillability, but it has been shown not to be a necessary condition (Shor *et al.*, 2001). The known criteria for distillability are summarized by the following statements:

$$\begin{gathered}
\text{general states, distillable} \Rightarrow \text{npt}\\
\text{general states, distillable} \overset{?}{\not\Leftarrow} \text{npt}\\
\text{general states, distillable} \Leftarrow \hat{\rho}_1\otimes\mathbb{1}-\hat{\rho}_{12}\not\geq 0\\
\text{general states, distillable} \not\Rightarrow \hat{\rho}_1\otimes\mathbb{1}-\hat{\rho}_{12}\not\geq 0\\
\text{Gaussian states, distillable} \Leftrightarrow \text{npt}.
\end{gathered}\tag{142}$$

Bound entangled npt Gaussian states definitely do not exist (Giedke, Kraus, *et al.*, 2001a, 2001b). Hence the set of Gaussian states is fully explored, consisting only of npt distillable, positive partial-transpose entangled (undistillable), and separable states. The simplest bound entangled Gaussian states are those with two modes at each side, $N=M=2$. Explicit examples were constructed by Werner and Wolf (2001). An example of tripartite bound entangled states are the Gaussian three-mode states of class 4 in Eq. (128). These states are positive partial transpose with respect to any of the three modes, but nonetheless entangled. Unfortunately, the distillation of npt Gaussian states to maximally entangled finite-dimensional states, though possible in principle, is not very feasible with current technology. It relies upon non-Gaussian operations (see Sec. IV.E). As for the existence of generic bound entanglement of non-Gaussian continuous-variable states, examples were discussed by Horodecki and Lewenstein (2000) and Horodecki *et al.* (2001).

D. Nonlocality

We mentioned earlier that the notion of entanglement was introduced in 1935 by Schrödinger in his reply (Schrödinger, 1935) to the EPR paper (Einstein *et al.*, 1935). The EPR argument itself, based on the continuous-variable entangled state in Eq. (80), already contains as an essential ingredient the notion of *nonlocality*. More precisely, the reasoning behind the EPR paradox relies upon two major assumptions: first, there is something like an objective reality, and second, there is no action at a distance. Objective reality becomes manifest: "if without in any way disturbing the system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this quantity." Now two particles sharing the entangled state of Eq. (80) are perfectly correlated in their positions and momenta. Measuring, say, the position of one particle means that the result obtainable in a subsequent position measurement of the other particle can be predicted with certainty. If there is no action at a distance, this prediction is made without disturbing the second particle. Hence, due to EPR's realism, there must be a definite predetermined position of that particle. The same arguments apply to the momenta, leading also to a definite predetermined momentum for the second particle. Since quantum theory does not allow for such states of definite position and momentum, EPR conclude that the quantum-mechanical description is incomplete. Similar to the inseparability criteria for continuous-variable states, which need to be expressed in terms of position and momentum, EPR's conclusion (local realism implies incompleteness of quantum theory) also crucially depends on the presence of correlations in both conjugate variables. Hence, as discussed earlier, the nature of these correlations must be quantum rather than classical.

Later, in 1964, by extending the EPR program John Bell showed that nonlocality can be revealed via the constraints that local realism imposes on the statistics of two physically separated systems (Bell, 1964). These constraints, expressed in terms of the Bell inequalities, can be violated by quantum mechanics. There are, then, three possible conclusions that can be drawn when inequalities imposed by local realism are violated: the correlations of the relevant quantum state contradict locality or realism or both. What is today loosely called "nonlocality" includes these three alternatives.

As for a demonstration of this nonlocality, several quantum optical experiments have been performed. The first detection of violations of Bell-type inequalities was based on discrete-variable two-photon states (Aspect *et al.*, 1982; Ou and Mandel, 1988). These states are analogous to the spin-entangled states used by Bohm (1951) in his discrete-variable version of the EPR paradox. Such single-photon-based discrete-variable experiments rely on photon counting.

1. Traditional EPR-type approach

A quantum optical continuous-variable experiment more reminiscent of the original EPR paradox and distinct from tests of Bell inequalities was carried out by Ou *et al.* (1992a, 1992b) based on the quantum correlations of position and momentum in a two-mode squeezed state. In this experiment, the quantities determined were the quadrature variances of one mode conditioned upon the results obtainable in quadrature measurements of the other mode (inferred variances). This quantum optical demonstration of the original EPR paradox was based on a proposal by Reid (1989), who extended the EPR scenario to the case of finite quantum correlations using the inferred quadrature variances

$$\begin{aligned}\mathrm{Var}_{\mathrm{inf}}^{\hat{x}} \equiv \mathrm{Var}(\hat{x}_1 - \hat{x}_1^{\mathrm{est}}) &= \mathrm{Var}(\hat{x}_1 - g_x\hat{x}_2)\\ &= \langle(\hat{x}_1 - g_x\hat{x}_2)^2\rangle - \langle\hat{x}_1 - g_x\hat{x}_2\rangle^2,\end{aligned} \tag{143}$$

where $\hat{x}_1^{\mathrm{est}}=g_x\hat{x}_2$ is the inferred estimate of mode 1's position $\hat{x}_1$ based on the scaled readout $\hat{x}_1^{\mathrm{est}}$ of mode 2's position $\hat{x}_2$. The scaling parameter g_x may then be chosen optimally in order to ensure the most accurate inference. The smaller the deviation of $\hat{x}_1^{\mathrm{est}}$ from the true values $\hat{x}_1$, the better $\hat{x}_1$ may be determined at a distance by detecting $\hat{x}_2$. On average, this deviation is quantified by $\mathrm{Var}_{\mathrm{inf}}^{\hat{x}}$. Similarly, one can define $\mathrm{Var}_{\mathrm{inf}}^{\hat{p}}$, the inferred variance for the momentum, with $\hat{x}\to\hat{p}$ throughout. By calculating $\partial\mathrm{Var}_{\mathrm{inf}}^{\hat{x}}/\partial g_x=0$, we obtain the optimal scaling factor

$$g_x = \frac{\langle\hat{x}_1\hat{x}_2\rangle - \langle\hat{x}_1\rangle\langle\hat{x}_2\rangle}{\mathrm{Var}(\hat{x}_2)} = \frac{\langle\Delta\hat{x}_1\Delta\hat{x}_2\rangle}{\mathrm{Var}(\hat{x}_2)}, \tag{144}$$

with $\Delta\hat{x}_i\equiv\hat{x}_i-\langle\hat{x}_i\rangle$. For the momentum, we have correspondingly $g_p=\langle\Delta\hat{p}_1\Delta\hat{p}_2\rangle/\mathrm{Var}(\hat{p}_2)$. With these scaling factors, the optimal (minimal) value for the inferred variance becomes

$$[\mathrm{Var}_{\mathrm{inf}}^{\hat{x}}]_{\min} = \mathrm{Var}(\hat{x}_1)\left(1 - \frac{\langle\Delta\hat{x}_1\Delta\hat{x}_2\rangle^2}{\mathrm{Var}(\hat{x}_1)\mathrm{Var}(\hat{x}_2)}\right) \equiv \mathrm{Var}_{\mathrm{cond}}^{\hat{x}}, \tag{145}$$

and similarly for $[\mathrm{Var}_{\mathrm{inf}}^{\hat{p}}]_{\min}\equiv\mathrm{Var}_{\mathrm{cond}}^{\hat{p}}$ with $\hat{x}\to\hat{p}$ throughout in Eq. (145). The minimal inferred variances are also referred to as conditional variances $\mathrm{Var}_{\mathrm{cond}}^{\hat{x}}$ and $\mathrm{Var}_{\mathrm{cond}}^{\hat{p}}$, a measure of the noise degrading the otherwise perfect correlations between the two modes.

Following the EPR program and assuming now that the two modes 1 and 2 are spatially separated, but also that there is no action at a distance, one would have to assign to mode 1 predetermined values for $\hat{x}_1$ and $\hat{p}_1$ up to, on average, some noise $\mathrm{Var}_{\mathrm{inf}}^{\hat{x}}$ and $\mathrm{Var}_{\mathrm{inf}}^{\hat{p}}$, respectively. Thus if this leads to a state in which $\hat{x}_1$ and $\hat{p}_1$ are defined to an accuracy of

$$\mathrm{Var}_{\mathrm{inf}}^{\hat{x}}\mathrm{Var}_{\mathrm{inf}}^{\hat{p}} < \frac{1}{16}, \tag{146}$$

a contradiction of the Heisenberg uncertainty relation, Eq. (12), would occur. In fact, the EPR condition in Eq. (146) is satisfied with the two-mode squeezed (vacuum) state for any nonzero squeezing $r>0$, since its correlation matrix in Eq. (117) using Eq. (145) yields the conditional variances

$$\mathrm{Var}_{\mathrm{cond}}^{\hat{x}} = \mathrm{Var}_{\mathrm{cond}}^{\hat{p}} = \frac{1}{4\cosh 2r}. \tag{147}$$

The optimal scaling factors to ensure the best inference and hence to fulfill Eq. (146) for any nonzero squeezing are $g_x=\tanh 2r$ and $g_p=-\tanh 2r$.

Apparently, EPR nonlocality as given by Eq. (146) and inseparability as indicated by a violation of Eq. (112) are equivalent for pure Gaussian states such as two-mode squeezed states. In general, however, EPR nonlocality is only a sufficient (Reid, 2001; Kim *et al.*, 2002) and not a necessary condition for inseparability. This is similar to the relation between inseparability and nonlocality as expressed by violations of Bell inequalities. As mentioned earlier, except for pure states, entanglement does not automatically imply Bell nonlocality, but the converse holds true in general. For instance, the qubit Werner states are mixed states which can be inseparable without violating any (noncollective) Bell inequality (Werner, 1989). Hence the two formally distinct approaches of EPR and Bell nonlocality both lead to criteria generally stricter than those for inseparability. Due to this similarity and the fact that the EPR concept, initially designed for continuous variables (Einstein *et al.*, 1935), was later translated into the discrete-variable domain (Bohm, 1951), one may ask whether the concept of Bell nonlocality, originally derived in terms of discrete variables (Bell, 1964), is completely describable in terms of continuous variables too. Bell argued that the original EPR state directly reveals a local hidden-variable description in terms of position and momentum, since its Wigner function is positive everywhere and hence serves as a classical probability distribution for the hidden variables (Bell, 1987). Thus attempts to derive homodyne-based continuous-variable violations of Bell inequalities for the two-mode squeezed state with its positive Gaussian Wigner function must fail. However, whether the nonlocality (for pure-state entanglement always present) is uncovered depends on the observables and the measurements considered in a specific Bell inequality and not only on the quantum state itself. In fact, it was shown by Banaszek and Wódkiewicz (1998) how to demonstrate the nonlocality of the two-mode squeezed vacuum state: it violates a Clauser-Horne-Shimony-Holt (CHSH) inequality (Clauser *et al.*, 1969) when measurements of photon number parity are considered.

2. Phase-space approach

Following Bell (1987), an always positive Wigner function can serve as the hidden-variable probability distribution with respect to measurements corresponding to any linear combination of $\hat{x}$ and $\hat{p}$. In this sense, one will not obtain a violation of the CHSH inequality for the two-mode squeezed-state Wigner function of Eq. (82) when restricted to such measurements (Banaszek and Wódkiewicz, 1998). The same applies to the always positive Wigner function of the Gaussian N-party entangled N-mode state with correlation matrix given by Eq. (138). Thus in order to reveal the nonlocality of these Gaussian states, non-Gaussian measurements, which are not only based upon homodyne detection, must be considered.

For their analysis using photon number parity measurements, Banaszek and Wodkiewicz exploited the fact that the Wigner function is proportional to the quantum expectation value of a displaced parity operator (Royer, 1977; Banaszek and Wódkiewicz, 1998). Extending this observation from two to an arbitrary number of N modes, one obtains

$$W(\boldsymbol{\alpha}) = \left(\frac{2}{\pi}\right)^N \langle \hat{\Pi}(\boldsymbol{\alpha})\rangle = \left(\frac{2}{\pi}\right)^N \Pi(\boldsymbol{\alpha}), \tag{148}$$

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

$$\hat{\Pi}(\boldsymbol{\alpha}) = \mathop{\otimes}_{i=1}^{N} \hat{\Pi}_i(\alpha_i) = \mathop{\otimes}_{i=1}^{N} \hat{D}_i(\alpha_i)(-1)^{\hat{n}_i}\hat{D}_i^\dagger(\alpha_i). \tag{149}$$

The operator $\hat{D}_i(\alpha_i)$ is the displacement operator of Eq. (65) acting on mode i. Thus $\hat{\Pi}(\boldsymbol{\alpha})$ is a product of displaced parity operators corresponding to the measurement of an even (parity +1) or an odd (parity −1) number of photons in mode i. Each mode is then characterized by a *dichotomic variable* similar to the spin of a spin-1/2 particle or the single-photon polarization. Different spin or polarizer orientations from the original qubit-based Bell inequality are replaced by different displacements in phase space. The nonlocality test then simply relies on this set of two-valued measurements for each different setting.

In order to expose the nonlocal two-party correlations of the two-mode squeezed state, one may then consider the combination (Banaszek and Wódkiewicz, 1998)

$$\mathcal{B}_2 = \Pi(0,0) + \Pi(0,\beta) + \Pi(\alpha,0) - \Pi(\alpha,\beta), \tag{150}$$

which satisfies $|\mathcal{B}_2| \leqslant 2$ for local realistic theories according to the CHSH inequality (Clauser *et al.*, 1969)

$$|C(a_1,a_2) + C(a_1,a_2') + C(a_1',a_2) - C(a_1',a_2')| \leqslant 2. \tag{151}$$

Here, $C(a_1,a_2)$ are the correlation functions of measurements on particles 1 and 2 for two possible measurement settings (denoted by a_i and a_i' for each particle i).

By writing the two-mode squeezed state according to Eq. (148) for $N=2$ as $\Pi(\alpha_1,\alpha_2)$ and inserting it into Eq. (150) with, for example, $\alpha=\beta=i\sqrt{\mathcal{J}}$ (where $\mathcal{J}\geqslant 0$ is a real displacement parameter), one obtains $\mathcal{B}_2=1+2\exp(-2\mathcal{J}\cosh 2r)-\exp(-4\mathcal{J}e^{+2r})$. In the limit of large r (with $\cosh 2r \approx e^{+2r}/2$) and small $\mathcal{J}$, $\mathcal{B}_2$ is maximized for $\mathcal{J}e^{+2r}=(\ln 2)/3$, yielding $\mathcal{B}_2^{\max}\approx 2.19$ (Banaszek and Wódkiewicz, 1998), which is a clear violation of the inequality $|\mathcal{B}_2|\leqslant 2$. A similar analysis, using Eq. (148), reveals the nonlocal N-party correlations of the multipartite entangled Gaussian N-mode state with correlation matrix in Eq. (138) (van Loock and Braunstein, 2001a). In this case, the nonlocality test is possible using N-particle generalizations of the two-particle Bell-CHSH inequality (Klyshko, 1993; Gisin and Bechmann-Pasquinucci, 1998). For a growing number of parties and modes of the N-mode state in Eq. (138), its nonlocality represented by the maximum violation of the corresponding Mermin-Klyshko-type inequality seems to increase nonexponentially (van Loock and Braunstein, 2001a). This is different from the qubit GHZ states which show an exponential increase of the violations as the number of parties grows (Mermin, 1990; Klyshko, 1993; Gisin and Bechmann-Pasquinucci, 1998). Correspondingly, an exponential increase can also be obtained by considering the maximally entangled N-party states defined via the two-dimensional parity-spin ("pseudospin") subspace of the infinite-dimensional Hilbert space for each electromagnetic mode (Chen and Zhang, 2002).

3. Pseudospin approach

Alternatively and distinct from the phase-space approach of Banaszek and Wódkiewicz (1998), one can also reveal the nonlocality of the continuous-variable states by introducing a pseudospin operator (Chen *et al.*, 2002), $\vec{s}=(\hat{s}_x,\hat{s}_y,\hat{s}_z)^T$, similar to the spin operator of spin-$\frac{1}{2}$ systems, $\vec{\sigma}=(\sigma_1,\sigma_2,\sigma_3)^T$, with the Pauli matrices σ_i (Preskill, 1998). The components of the pseudospin operator are then defined in the photon number basis as (Halvorson, 2000; Chen *et al.*, 2002)

$$\hat{s}_z = (-1)^{\hat{n}}, \quad \hat{s}_+ = \hat{s}_-^\dagger = \sum_{n=0}^{\infty} |2n\rangle\langle 2n+1|, \tag{152}$$

where $\hat{s}_x \pm i\hat{s}_y = 2\hat{s}_\pm$. Hence $\hat{s}_z$ and $\hat{s}_\pm$ are the photon number parity and parity-flip operators, respectively. They obey the commutation relations

$$[\hat{s}_z,\hat{s}_\pm] = \pm 2\hat{s}_\pm, \quad [\hat{s}_+,\hat{s}_-] = \hat{s}_z, \tag{153}$$

equivalent to those of spin-$\frac{1}{2}$ systems which satisfy the Pauli matrix algebra, $[\hat{s}_i,\hat{s}_j]=2i\epsilon_{ijk}\hat{s}_k$ and $\hat{s}_i^2=1$, with $(i,j,k)\leftrightarrow(x,y,z)$. The two-valued measurements for the nonlocality test are now represented by the Hermitian operator $\vec{a}\cdot\vec{s}$ with eigenvalues ±1. The unit vector $\vec{a}$ describes the direction along which the parity spin $\vec{s}$ is measured. As in the well-known qubit context, different measurement settings correspond to different (parity) spin orientations. In the CHSH inequality (151), for instance, by substituting the setting parameters a_1, a_2, a_1', and a_2' by the vectors $\vec{a}_1$, $\vec{a}_2$, $\vec{a}_1'$, and $\vec{a}_2'$, respectively, one finds that the correlation functions now become $\langle(\vec{a}_1\cdot\vec{s}_1)\otimes(\vec{a}_2\cdot\vec{s}_2)\rangle \equiv C(\vec{a}_1,\vec{a}_2)$ (Chen *et al.*, 2002). By parametrizing the unit vectors in terms of spherical coordinates and choosing the right angles, it can be shown (Chen *et al.*, 2002) that the two-mode squeezed vacuum state of Eq. (85) maximally violates the CHSH inequality in the limit of infinite squeezing. For this maximum violation, the left-hand side of Eq. (151) with correlation functions $C(\vec{a}_1,\vec{a}_2)$ takes on a value of $2\sqrt{2}$, the upper (Cirel'son) bound for any continuous-variable quantum state (Cirel'son, 1980; Chen *et al.*, 2002). Recently, a comparison was made between the different formalisms for revealing the nonlocality of the continuous-variable states (Jeong *et al.*, 2003), in particular, using a generalized version (Wilson *et al.*, 2002) of the phase-space formalism of Banaszek and Wódkiewicz (1998). It turns out that after generalizing the formalism of Banaszek and Wodkiewicz (Banaszek and Wódkiewicz, 1998; Wilson *et al.*, 2002), the two-mode squeezed vacuum state even in the limit of infinite squeezing, though yielding larger violations than before the generalization, cannot maximally violate the Bell-CHSH inequality. Thus in order to reveal the maximum violation of the original EPR state as the limiting case of the two-mode squeezed vacuum state, the parity-spin formalism of Chen *et al.* (2002) must be employed. Similarly, the nonlocality of a two-mode squeezed state is more robust against a dissipative environment such as an absorbing optical fiber when it is based on the parity-spin formalism (Filip and Mišta, 2002) rather than the phase-space formalism (Jeong *et al.*, 2000).

As for an experimental implementation of these nonlocality tests, both the measurement of the photon number parity alone and that of the entire parity-spin operator are difficult. The former already requires detectors capable of resolving large photon numbers. However, there are reports on an experimental nonlocality test of the optical EPR state (made via a nonlinear $\chi^{(2)}$ interaction with ultrashort pump pulses) utilizing homodyne-type measurements with weak local oscillators (Kuzmich *et al.*, 2000, 2001). Since the measured observables in this experiment are not reducible to the field quadratures [as in the experiment of Ou *et al.* (1992a, 1992b), in which a strong local oscillator was used], a local hidden-variable model for the measurements cannot be simply constructed from the Wigner function of the state. Hence Bell-type violations of local realism are detected, similar to those proposed by Grangier *et al.* (1988). Nonlocality of the kind discussed by Banaszek and Wódkiewicz (1998) becomes manifest in this experiment too.

The advantage of the nonlocality tests in the continuous-variable domain is that the entangled Gaussian states are easy to build from squeezed light, though the required measurements are difficult to perform (as they are not truly continuous variable, but rather are of discretized dichotomic form). Conversely, other continuous-variable approaches to quantum nonlocality are based on feasible measurements of states for which no generation scheme is yet known. An example of this is the Hardy-type (Hardy, 1992) nonlocality proof in the continuous-variable domain involving simple position and momentum, i.e., quadrature measurements (Yurke *et al.*, 1999). Yet another approach is the proposal of Ralph *et al.* (2000), which relies on states built from optical parametric amplification in the low-squeezing (polarization-based discrete-variable) limit and utilizes efficient homodyne detections. Further theoretical work on quantum nonlocality tests using homodyne-type continuous-variable measurements were published recently by Banaszek *et al.* (2002) and by Wenger *et al.* (2003).

As for proposals for revealing the nonlocality of multiparty entangled continuous-variable states, there is a similar tradeoff between the feasibility of the state generation and that of the measurements. For instance, as discussed previously, applying the phase-space approach of Banaszek and Wódkiewicz (1998) to the N-party Mermin-Klyshko inequalities using the Gaussian N-mode state with correlation matrix in Eq. (138) (van Loock and Braunstein, 2001a) requires measurements of the photon number parity. In contrast, more feasible position and momentum measurements can be used to construct a GHZ paradox (Greenberger *et al.*, 1990) for continuous variables (Massar and Pironio, 2001), but the states involved in this scheme are not simply producible from squeezers and beam splitters. Similarly, one may consider the N-party N-mode eigenstates of the parity-spin operator for different orientations $\vec{a}\cdot\vec{s}$. These states take on a form identical to that in Eq. (121), now for each mode defined in the two-dimensional parity-spin subspace of the infinite-dimensional Hilbert space of the electromagnetic mode (Chen and Zhang, 2002). They are, in strict analogy to the qubit GHZ states, maximally entangled N-party states, and thus lead to an exponential increase of violations of the N-party Mermin-Klyshko inequalities as the number of parties grows (Chen and Zhang, 2002). Hence the nonexponential increase of violations for the Gaussian N-mode states with correlation matrix in Eq. (138) may be due to the limited phase-space formalism of Banaszek and Wódkiewicz (1998) rather than the nonmaximum W-type entanglement of these states for finite squeezing. However, it has not yet been shown whether the maximally entangled parity-spin GHZ states of Chen and Zhang (2002) are obtainable as the infinite-squeezing limit of the Gaussian N-mode states with correlation matrix in Eq. (138). Only in the two-party case is it known that the state that maximally violates the parity-spin CHSH inequality (Chen *et al.*, 2002) is the infinite-squeezing limit of the two-mode squeezed vacuum state.

E. Verifying entanglement experimentally

So far we have discussed the notion of entanglement primarily from a theoretical point of view. How may one verify the presence of entanglement experimentally? In general, theoretical tests might be applicable as well to experimental verification. For instance, measuring a violation of inequalities imposed by local realism confirms the presence of entanglement. In general, any theoretical test is applicable when the experimentalist has full information about the quantum state after measurements on an ensemble of identically prepared states [e.g., by quantum tomography (Leonhardt, 1997)]. In the continuous-variable setting, for the special case of Gaussian states, the presence of (even genuine multipartite) entanglement can be confirmed, once the complete correlation matrix is given. In this case one can apply, for instance, the npt criterion, as discussed in Secs. III.A.2 and III.B.3.

The complete measurement of an N-mode Gaussian state is accomplished by determining the $2N\times 2N$ second-moment correlation matrix. This corresponds to $N(1+2N)$ independent entries taking into account the symmetry of the correlation matrix. Kim *et al.* (2002) recently demonstrated how to determine all these entries in the two-party two-mode case using beam splitters and homodyne detectors. Joint homodyne detections of the two modes yield intermode correlations such as $\langle\hat{x}_1\hat{x}_2\rangle-\langle\hat{x}_1\rangle\langle\hat{x}_2\rangle$, $\langle\hat{x}_1\hat{p}_2\rangle-\langle\hat{x}_1\rangle\langle\hat{p}_2\rangle$, etc. Determining the local intramode correlations such as $\langle\hat{x}_1\hat{p}_1+\hat{p}_1\hat{x}_1\rangle/2-\langle\hat{x}_1\rangle\langle\hat{p}_1\rangle$ is more subtle and requires additional beam splitters and homodyne detections (or, alternatively, heterodyne detections). Once the 4×4 two-mode correlation matrix is known, the npt criterion can be applied as a necessary and sufficient condition for bipartite Gaussian two-mode inseparability (see Sec. III.A.2). In fact, the entanglement can then also be quantified for a given correlation matrix (Kim *et al.*, 2002; Vidal and Werner 2002). For three-party three-mode Gaussian states, one may pursue a similar strategy. After measuring the 21 independent entries of the correlation matrix [for example, by extending the scheme of Kim *et al.* (2002) to the three-mode case], the necessary and sufficient criteria of Giedke, Krauss, *et al.* (2001c) can be applied (see Sec. III.B.3).

However, even for Gaussian states, such a verification of entanglement via a complete state determination is very demanding to the experimentalist, in particular, when the state to be determined is a potentially multiparty entangled multimode state. Alternatively, rather than detecting all the entries of the correlation matrix, one may measure only the variances of appropriate linear combinations of the quadratures of all modes involved. This may still be sufficient to verify unambiguously the presence of (genuine multipartite) entanglement. For example, the sufficient inseparability criteria from Sec. III.A.2, expressed by violations of Eq. (112) or Eq. (114), can be used for witnessing entanglement experimentally. The indirect experimental confirmation of the presence of entanglement then relies, for example, on the detection of the quadrature variances $\langle[\Delta(\hat{x}_1-\hat{x}_2)]^2\rangle$ and $\langle[\Delta(\hat{p}_1+\hat{p}_2)]^2\rangle$ after combining the two relevant modes at a beam splitter (Tan, 1999). As for a more direct verification, the measured quadratures of the relevant state can also be combined electronically (Furusawa and Kimble, 2003).

Similarly, for three parties and modes, one may attempt to detect violations of inequalities of the form (van Loock and Furusawa, 2003)

$$\langle(\Delta\hat{u})^2\rangle_\rho+\langle(\Delta\hat{v})^2\rangle_\rho\geqslant f(h_1,h_2,h_3,g_1,g_2,g_3), \tag{154}$$

where

$$\hat{u}\equiv h_1\hat{x}_1+h_2\hat{x}_2+h_3\hat{x}_3, \quad \hat{v}\equiv g_1\hat{p}_1+g_2\hat{p}_2+g_3\hat{p}_3. \tag{155}$$

The h_l and g_l are again arbitrary real parameters. For (at least partially) separable states, the following statements hold (van Loock and Furusawa, 2003):

$$\hat{\rho}=\sum_i \eta_i\hat{\rho}_{i,km}\otimes\hat{\rho}_{i,n}\Rightarrow f(h_1,h_2,h_3,g_1,g_2,g_3)$$
$$=(|h_ng_n|+|h_kg_k+h_mg_m|)/2. \tag{156}$$

Here, $\hat{\rho}_{i,km}\otimes\hat{\rho}_{i,n}$ indicates that the three-party density operator is a mixture of states i in which parties (modes) k and m may be entangled or not, but party n is not entangled with the rest, and in which (k,m,n) is any triple of (1,2,3). Hence the fully separable state is also included in the above statements. In fact, for the fully separable state, we have (van Loock and Furusawa, 2003)

$$\hat{\rho}=\sum_i \eta_i\hat{\rho}_{i,1}\otimes\hat{\rho}_{i,2}\otimes\hat{\rho}_{i,3}\Rightarrow f(h_1,h_2,h_3,g_1,g_2,g_3)$$
$$=(|h_1g_1|+|h_2g_2|+|h_3g_3|)/2, \tag{157}$$

which is always greater than or equal to any of the boundaries in Eq. (156). By detecting violations of the conditions in Eq. (154) with Eq. (156), one can rule out any partially separable (biseparable) form of the state in question and hence verify genuine tripartite entanglement. An experiment in which this verification was achieved will be briefly described in Sec. VII.

The advantage of all these continuous-variable inseparability criteria is that, though still relying upon the rigorous definition of entanglement in terms of states as given in Secs. III.A and III.B, they can be easily checked via efficient homodyne detections of the quadrature operator statistics.

IV. QUANTUM COMMUNICATION WITH CONTINUOUS VARIABLES

When using the term quantum communication, we refer to any protocol in which the participants' ability to communicate is enhanced due to the exploitation of quantum features such as nonorthogonality or entanglement. Such an enhancement includes, for instance, the secure transmission of classical information from a sender ("Alice") to a receiver ("Bob") based on the transfer of nonorthogonal quantum states. This quantum key distribution (Bennett and Brassard, 1984; Ekert, 1991; Bennett, 1992) is the prime example of a full quantum solution to an otherwise unsolvable classical problem, namely, that of unconditionally secure communication. The, in principle, unconditional security of quantum cryptography is provided by the fact that an eavesdropper is revealed when she ("Eve") is trying to extract the classical information from the quantum system being transmitted. Eve would have to perform measurements, and thereby (at least for some measurements) inevitably disturb and alter the quantum system. In general, a solution to a classical communication problem provided by a quantum-based protocol should be *complete* (Lütkenhaus, 2002), connecting the classical world of Alice with that of Bob. For example, a secure quantum cryptographic communication scheme also relies on the classical one-time pad. By contrast, there are quantum subroutines (Lütkenhaus, 2002) that run entirely on the quantum level. A prime example for this is quantum teleportation, whereby the quantum information encoded in nonorthogonal (arbitrary or unknown) quantum states is reliably transferred from Alice to Bob using shared entanglement and classical communication. In order to teleport a qubit, two bits of classical information must be sent. As an application of quantum teleportation, one may imagine the reliable connection of the nodes in a network of quantum computers.

Nonorthogonal quantum states when sent directly through a quantum communication channel are in any realistic situation subject to environmentally induced noise, i.e., the quantum channel is noisy. The coherent superposition of the signal then turns into an incoherent mixture, a process called decoherence. There are various methods to circumvent the effect of decoherence, all of which were originally proposed for discrete-variable systems. These methods are quantum teleportation, combined with a purification of the distributed entanglement (Bennett, Brassard, *et al.*, 1996), or quantum error correction [originally proposed for reducing decoherence in a quantum computer (Shor, 1995) rather than in a quantum communication channel]. They make possible in principle, completely reliable transmission of quantum information.

Apart from the above-mentioned quantum communication scenarios in which Alice and Bob benefit from using quantum resources, there are also fundamental results of quantum communication on the restrictions imposed by quantum theory on classical communication via quantum states. A very famous result in this context is that of Holevo (1998), sometimes referred to as the "fundamental law of quantum communication" (Caves and Drummond, 1994). It places an upper bound ("Holevo bound") on the mutual information of Alice and Bob,

$$I(A\!:\!B) \leqslant S(\hat{\rho}) - \sum_a p_a S(\hat{\rho}_a) \leqslant S(\hat{\rho}), \tag{158}$$

where $S(\hat{\rho})$ is the von Neumann entropy, $\hat{\rho}$ is the mean channel state, and $\hat{\rho}_a$ are the signal states with *a priori* probabilities p_a. In this relation, equality is achievable if Alice sends pure orthogonal signal states.

Even assuming an ideal (noiseless) channel, any attempt by Bob to retrieve the classical information sent from Alice introduces "noise" when the signal states are nonorthogonal. In fact, there is an optimum of "accessible information," depending on the measurement strategy that Bob employs. The most general measurement strategy is described by so-called generalized measurements or positive operator-valued measures (POVM's). Such POVM's $\hat{E}_b$ are generalizations of projection operators and satisfy

$$\hat{E}_b = \hat{E}_b^{\dagger} \geqslant 0, \quad \sum_b \hat{E}_b = \hat{\mathbb{1}}. \tag{159}$$

When Bob is presented with a state $\hat{\rho}_a$ representing letter a from Alice's alphabet, he will find instead letter b from his own alphabet with a conditional probability given by

$$p_{b|a} = \mathrm{Tr}\, \hat{E}_b \hat{\rho}_a. \tag{160}$$

From this, one may compute the mutual information $I(A\!:\!B)$, as we shall show in Sec. IV.B in the context of dense coding. In this protocol, the roles of the classical and quantum channels are interchanged relative to those in quantum teleportation. Instead of reliably transferring quantum information through a classical channel using entanglement as in teleportation, in a dense-coding scheme the amount of classical information transmitted from Alice to Bob is increased when Alice sends quantum information (her half of an entangled state shared with Bob) through a quantum channel to Bob. For instance, two bits of classical information can be conveyed by sending just one qubit. Like quantum teleportation, dense coding also relies on preshared entanglement. Thus dense coding is still in agreement with Holevo's rule that at most one classical bit can be transmitted by sending one qubit, because, taking into account Bob's half of the entangled state transmitted to him prior to the actual communication ("off-peak"), in total two qubits must be sent to Bob. This entanglement-based dense coding is sometimes referred to as superdense coding, as opposed to the dense-coding or quantum-coding schemes introduced by Schumacher (1995). The latter enable Alice and Bob to approach the Holevo bound even for nonorthogonal or mixed signal states via appropriate encoding of the classical information into these states. These issues of quantum coding, including the results of Holevo, may be considered as an extension of Shannon's classical information theory (applied to communication) to the quantum realm (Preskill, 1998). A brief introduction to the mathematical description of classical information *á la* Shannon (1948) will be given in Sec. IV.B.

The following review of quantum communication protocols with continuous variables mainly contains entanglement-based schemes. From the preceding sections we know that, in the continuous-variable domain, not only the generation of continuous-variable entanglement, but also its *manipulation* via (local) measurements and unitary operations, turns out to be very easy. For instance, distinguishing exactly between maximally entangled states through a suitable measurement, as needed for quantum teleportation, is not possible with photonic qubit Bell states using only linear optics (Lütkenhaus *et al.*, 1999; Vaidman and Yoran, 1999). In contrast, such a complete Bell detection for continuous variables only requires a beam splitter and homodyne detections. Similarly, unitary transformations such as phase-space displacements can be easily performed for the continuous quadrature amplitudes using feedforward techniques. Homodyne-based Bell detection and feedforward are the main tools in both continuous-variable quantum teleportation and continuous-variable dense coding.

The continuous-variable quantum communication schemes presented below include entanglement-based protocols for quantum teleportation (Sec. IV.A) and (super)dense coding (Sec. IV.B). A potentially important application of quantum teleportation, the teleportation of one-half of an entangled state (entanglement swapping), will also be discussed in the continuous-variable setting. Entanglement swapping is an essential ingredient of potential long-distance implementations of quantum communication: the two remote ends of a noisy quantum channel are then provided with good entanglement after purifying the noisy entanglement in different segments of the channel and combining the segments via entanglement swapping. Several continuous-variable approaches to entanglement distillation (including the purification of mixed entangled states and the concentration of pure nonmaximally entangled states) will be discussed in Sec. IV.E. Apart from quantum teleportation combined with entanglement purification, alternatively, quantum error-correction codes can be used to protect quantum information from decoherence when being sent through a noisy quantum communication channel. A possible continuous-variable implementation of quantum error correction for communication based on linear optics and squeezed light will be discussed in Sec. IV.C. As for quantum communication schemes not necessarily based on entanglement, we shall review some continuous-variable approaches to secure communication (continuous-variable quantum key distribution) in Sec. IV.D. In Sec. IV.F, we shall also briefly mention the proposals for potential atom-light interfaces for the storage of continuous-variable quantum information (quantum memory) in a quantum repeater.

A. Quantum teleportation

Quantum teleportation, in general, is the reliable transfer of quantum information through a classical communication channel using shared entanglement. The teleportation of continuous quantum variables such as position and momentum of a particle, as first proposed by Vaidman (1994), relies on the entanglement of the states in the original EPR paradox (Einstein *et al.*, 1935). In quantum optical terms, the observables analogous to the two conjugate variables position and momentum of a particle are the quadratures of a single mode of the electromagnetic field, as we have discussed in Sec. II. By considering the finite quantum correlations between these quadratures in a two-mode squeezed state, a realistic implementation for the teleportation of continuous quantum variables was proposed by Braunstein and Kimble (1998a). Based on this proposal, in fact, quantum teleportation of arbitrary coherent states has been achieved with a fidelity $F=0.58\pm0.02$ (Furusawa *et al.*, 1998). Without using entanglement, by purely classical communication, an average fidelity of 0.5 is the best that can be achieved if the alphabet of input states includes potentially all coherent states with equal weights (Braunstein, Fuchs, and Kimble, 2000). We shall discuss the issue of delineating a boundary between classical and quantum domains for teleportation in more detail later. The scheme based on the continuous quadrature amplitudes enables the realization of quantum teleportation in an unconditional fashion with high efficiency (Braunstein and Kimble, 1998a), as reported by Braunstein *et al.* (1998) and by Furusawa *et al.* (1998). In this experiment, the following three criteria necessary for quantum teleportation were achieved:

(1) An "unknown" quantum state enters the sending station for teleportation.

(2) A teleported state emerges from the receiving station for subsequent evaluation or exploitation.

(3) The degree of overlap between the input and teleported states is higher than that which could be achieved if the sending and receiving stations were linked only by a classical channel.

There are several aspects of quantum teleportation that are worth pointing out:

(1) The arbitrary input state can even be unknown to both Alice and Bob. If Alice knew the state, she could send her knowledge classically to Bob and Bob could prepare the state. Hence, in quantum teleportation, the state remains completely unknown to both Alice and Bob throughout the entire teleportation process.

(2) The input system does not remain in its initial state because of the Bell measurement. This fact ensures that the no-cloning rule is not violated.

(3) A contradiction to special relativity is avoided because the classical communication required between Alice and Bob is restricted by the speed of light.

Let us now describe the teleportation of continuous quantum variables in the simplest way, considering just (discrete) single modes of the electromagnetic field. The generalization to a realistic broadband description, in particular, with respect to the mentioned teleportation experiment, is straightforward and will be briefly discussed in Sec. VII. In the teleportation scheme of a single mode of the electromagnetic field, the shared entanglement resource is a two-mode squeezed state [e.g., as in Eq. (89); in the original proposal (Braunstein and Kimble 1998a), equivalently, the Wigner function of the

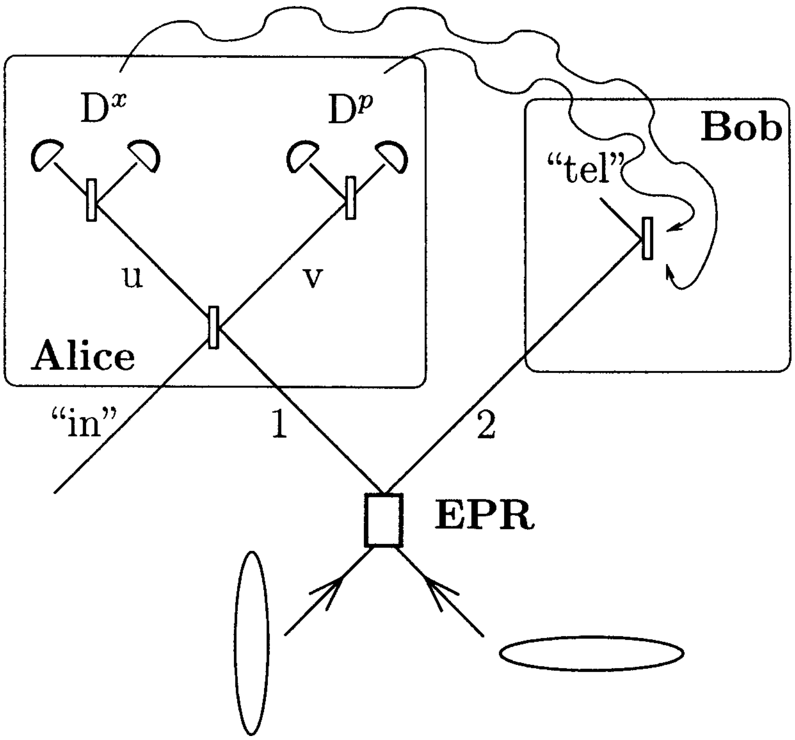

FIG. 2. Teleportation of a single mode of the electromagnetic field. Alice and Bob share the entangled state of modes 1 and 2. Alice combines the mode "in" to be teleported with her half of the Einstein-Podolsky-Rosen (EPR) state at a beam splitter. The homodyne detectors D^x and D^p yield classical photocurrents for the quadratures x_{u} and p_{v}, respectively. Bob performs phase-space displacements of his half of the EPR state depending on Alice's classical results. The entangled state EPR, eventually shared by Alice and Bob, may be produced by combining two single-mode squeezed states at a beam splitter or directly via a nonlinear two-mode squeezing interaction.

finitely squeezed EPR state of Eq. (82) was used]. The entangled state is sent in two halves: one to Alice (the teleporter or sender) and the other to Bob (the receiver), as illustrated in Fig. 2. In order to perform the teleportation, Alice has to couple the input mode she wants to teleport with her "EPR mode" at a beam splitter. The *Bell detection* of the x quadrature at one beam-splitter output, and of the p quadrature at the other output, yields the classical results to be sent to Bob via a classical communication channel. In the limit of an infinitely squeezed EPR source, these classical results contain no information about the mode to be teleported. This is analogous to the Bell measurement of the spin-$\frac{1}{2}$-particle pair by Alice for the teleportation of a spin-$\frac{1}{2}$-particle state. The measured Bell state of the spin-$\frac{1}{2}$-particle pair determines, for instance, whether the particles have equal or different spin projections. The spin projection of the individual particles, i.e., Alice's EPR particle and her unknown input particle, remains completely unknown. According to this analogy, we call Alice's quadrature measurements for the teleportation of the state of a single-mode "Bell detection." This detection corresponds to a projection onto the maximally entangled continuous-variable basis of two modes. As a result of the Bell detection and the entanglement between Alice's EPR mode and Bob's EPR mode, suitable phase-space displacements of Bob's mode convert it into a replica of Alice's unknown input mode (a perfect replica for infinite squeezing). In order to perform the right displacements, Bob needs the classical results of Alice's Bell measurement.

Quantum teleportation is a conceptually remarkable phenomenon. However, as a potential application it becomes significant only when combined with entanglement purification protocols (Sec. IV.E). In this case, instead of sending quantum information directly through a noisy channel, a more reliable transfer can be achieved by first distributing entanglement through the same channel, purifying it, and eventually exploiting it in a quantum teleportation protocol. We shall now turn to the continuous-variable protocol for quantum teleportation in more detail.

1. Teleportation protocol

The simplest formalism to describe continuous-variable quantum teleportation is based on the *Heisenberg representation*. In Eq. (89), modes 1 and 2 are entangled to a finite degree, corresponding to a (pure) nonmaximally entangled state. In the limit of infinite squeezing, $r\to\infty$, the individual modes become infinitely noisy, but the EPR correlations between them also become ideal: $(\hat{x}_1-\hat{x}_2)\to 0$, $(\hat{p}_1+\hat{p}_2)\to 0$. Now mode 1 is sent to Alice and mode 2 is sent to Bob (Fig. 2). Alice's mode is then combined at a (phase-free) 50:50 beam splitter with the input mode "in":

$$\hat{x}_{\mathrm{u}}=\frac{1}{\sqrt{2}}\hat{x}_{\mathrm{in}}-\frac{1}{\sqrt{2}}\hat{x}_1,\quad \hat{p}_{\mathrm{u}}=\frac{1}{\sqrt{2}}\hat{p}_{\mathrm{in}}-\frac{1}{\sqrt{2}}\hat{p}_1,$$

$$\hat{x}_{\mathrm{v}}=\frac{1}{\sqrt{2}}\hat{x}_{\mathrm{in}}+\frac{1}{\sqrt{2}}\hat{x}_1,\quad \hat{p}_{\mathrm{v}}=\frac{1}{\sqrt{2}}\hat{p}_{\mathrm{in}}+\frac{1}{\sqrt{2}}\hat{p}_1. \tag{161}$$

Using Eqs. (161) and (89), we may write Bob's mode 2 as

$$\hat{x}_2=\hat{x}_{\mathrm{in}}-(\hat{x}_1-\hat{x}_2)-\sqrt{2}\hat{x}_{\mathrm{u}}=\hat{x}_{\mathrm{in}}-\sqrt{2}e^{-r}\hat{x}_2^{(0)}-\sqrt{2}\hat{x}_{\mathrm{u}},$$

$$\hat{p}_2 = \hat{p}_{\text{in}} + (\hat{p}_1 + \hat{p}_2) - \sqrt{2}\hat{p}_{\text{v}} = \hat{p}_{\text{in}} + \sqrt{2}e^{-r}\hat{p}_1^{(0)} - \sqrt{2}\hat{p}_{\text{v}}. \tag{162}$$

Alice's Bell detection yields certain classical values x_{u} and p_{v} for $\hat{x}_{\text{u}}$ and $\hat{p}_{\text{v}}$. The quantum variables $\hat{x}_{\text{u}}$ and $\hat{p}_{\text{v}}$ become classically determined, random variables x_{u} and p_{v}. Now, due to the entanglement, Bob's mode 2 collapses into states that for $r \to \infty$ differ from Alice's input state only in (random) classical phase-space displacements. After receiving Alice's classical results x_{u} and p_{v}, Bob displaces his mode,

$$\hat{x}_2 \to \hat{x}_{\text{tel}} = \hat{x}_2 + g\sqrt{2}\hat{x}_{\text{u}},$$
$$\hat{p}_2 \to \hat{p}_{\text{tel}} = \hat{p}_2 + g\sqrt{2}\hat{p}_{\text{v}}, \tag{163}$$

thus accomplishing the teleportation. The parameter g describes a gain for the transformation from classical photocurrent to complex field amplitude. For $g=1$, Bob's displacements eliminate $\hat{x}_{\text{u}}$ and $\hat{p}_{\text{v}}$ in Eq. (162). The teleported mode then becomes

$$\hat{x}_{\text{tel}} = \hat{x}_{\text{in}} - \sqrt{2}e^{-r}\hat{x}_2^{(0)},$$
$$\hat{p}_{\text{tel}} = \hat{p}_{\text{in}} + \sqrt{2}e^{-r}\hat{p}_1^{(0)}. \tag{164}$$

For an arbitrary gain g, we obtain

$$\hat{x}_{\text{tel}} = g\hat{x}_{\text{in}} - \frac{g-1}{\sqrt{2}}e^{+r}\hat{x}_1^{(0)} - \frac{g+1}{\sqrt{2}}e^{-r}\hat{x}_2^{(0)},$$
$$\hat{p}_{\text{tel}} = g\hat{p}_{\text{in}} + \frac{g-1}{\sqrt{2}}e^{+r}\hat{p}_2^{(0)} + \frac{g+1}{\sqrt{2}}e^{-r}\hat{p}_1^{(0)}. \tag{165}$$

Note that these equations do not take into account Bell detector inefficiencies.

Consider the case $g=1$. For infinite squeezing $r \to \infty$, Eqs. (164) describe perfect teleportation of the quantum state of the input mode. On the other hand, for the classical case of $r=0$, i.e., no squeezing and hence no entanglement, each of the teleported quadratures has two additional units of vacuum noise compared to the original input quadratures. These two units are so-called *quantum duties*, or *quduties*, which have to be paid when crossing the border between quantum and classical domains (Braunstein and Kimble, 1998a). The two quduties represent the minimal tariff for every classical teleportation scheme (Braunstein, Fuchs, and Kimble, 2000). One quduty, the unit of vacuum noise due to Alice's detection, arises from her attempt to simultaneously measure the two conjugate variables x_{in} and p_{in} in an Arthurs-Kelly measurement (Arthurs and Kelly, 1965). This is the standard quantum limit for the detection of both quadratures when attempting to gain as much information as possible about the quantum state. The standard quantum limit yields a product of the measurement accuracies that is twice as large as the Heisenberg minimum uncertainty product. This product of the measurement accuracies contains the intrinsic quantum limit, the Heisenberg uncertainty of the mode to be detected, plus an additional unit of vacuum noise due to the detection. In other words, when measuring the input Wigner function the resulting distribution is the Wigner function convoluted with one unit of vacuum, i.e., the Q function [see Eqs. (33) and (34)]. The second quduty arises when Bob uses the information of Alice's detection to generate the state at amplitude $\sqrt{2}x_{\text{u}}+i\sqrt{2}p_{\text{v}}$ (Braunstein and Kimble, 1998a). It can be interpreted as the standard quantum limit imposed on state broadcasting.

The original proposal for the quantum teleportation of continuous variables with a finite degree of entanglement based on two-mode squeezed states used the *Wigner representation* and its convolution formalism (Braunstein and Kimble, 1998a). With the EPR-state Wigner function from Eq. (82), $W(\xi) \equiv W_{\text{EPR}}(\alpha_1, \alpha_2)$, the whole system after combining the "in" mode [which is in an unknown arbitrary quantum state described by $W_{\text{in}}(x_{\text{in}}, p_{\text{in}})$] with mode 1 at a phase-free 50:50 beam splitter (having the two outgoing modes $\alpha_{\text{u}}=x_{\text{u}}+ip_{\text{u}}$ and $\alpha_{\text{v}}=x_{\text{v}}+ip_{\text{v}}$) can be written, according to the transformation rules for Wigner functions under linear optics, as

$$W(\alpha_{\text{u}}, \alpha_{\text{v}}, \alpha_2) = \int dx_{\text{in}}dp_{\text{in}}W_{\text{in}}(x_{\text{in}}, p_{\text{in}})$$
$$\times W_{\text{EPR}}\left[\alpha_1 = \frac{1}{\sqrt{2}}(\alpha_{\text{v}} - \alpha_{\text{u}}), \alpha_2\right]$$
$$\times \delta\left[\frac{1}{\sqrt{2}}(x_{\text{u}} + x_{\text{v}}) - x_{\text{in}}\right]$$
$$\times \delta\left[\frac{1}{\sqrt{2}}(p_{\text{u}} + p_{\text{v}}) - p_{\text{in}}\right]. \tag{166}$$

Alice's Bell detection on the maximally entangled basis, i.e., homodyne detections of $x_{\text{u}}=(x_{\text{in}}-x_1)/\sqrt{2}$ and $p_{\text{v}} =(p_{\text{in}}+p_1)/\sqrt{2}$, is described via integration over x_{v} and p_{u}:

$$\int dx_{\text{v}}dp_{\text{u}}W(\alpha_{\text{u}}, \alpha_{\text{v}}, \alpha_2) = \int dxdpW_{\text{in}}(x,p)W_{\text{EPR}}[x - \sqrt{2}x_{\text{u}}$$
$$+ i(\sqrt{2}p_{\text{v}} - p), \alpha_2]. \tag{167}$$

Bob's displacements are now incorporated by the substitution $\alpha_2 = x_2' - \sqrt{2}x_{\text{u}} + i(p_2' - \sqrt{2}p_{\text{v}})$ in W_{EPR} in Eq. (167). Finally, integration over x_{u} and p_{v} yields the teleported ensemble state (for an ensemble of input states),

$$W_{\text{tel}}(\alpha_2') = \frac{1}{\pi e^{-2r}}\int d^2\alpha W_{\text{in}}(\alpha)\exp\left(-\frac{|\alpha_2' - \alpha|^2}{e^{-2r}}\right)$$
$$\equiv W_{\text{in}} \circ G_{\sigma}. \tag{168}$$

The teleported state is a convolution of the input state with the complex Gaussian $G_{\sigma}(\alpha) \equiv [1/(\pi\sigma)]\exp(-|\alpha|^2/\sigma)$ with the complex variance $\sigma=e^{-2r}$. This convolution adds the excess noise variance $e^{-2r}/2$ to each quadrature of the input state.

As for a description of continuous-variable quantum teleportation in the *Schrödinger representation*, there are several references. Milburn and Braunstein (1999) considered two different teleportation protocols referring to two different kinds of Bell measurements made by Alice. Depending on this choice, measuring either relative position and total momentum or photon-number difference and phase sum, the entire protocol, including the two-mode squeezed vacuum resource, is written in the position or in the Fock basis, respectively (Milburn and Braunstein, 1999). The protocol based on number-difference and phase-sum measurements was later modified and extended by Clausen *et al.* (2000) and by Cochrane *et al.* (2000, 2002). The extended continuous-variable quantum teleportation protocol of Opatrný *et al.* (2000) is based on quadrature Bell measurements and leads to an enhancement of the teleportation fidelity (see the next section) via subtraction of single photons. This protocol is also formulated in the Schrödinger representation. Using the approach of Opatrný *et al.* (2000), i.e., making conditional measurements on two-mode squeezed states, Cochrane *et al.* (2002) have demonstrated that the teleportation fidelity can be improved in both the quadrature-measurement-based and the number-difference and phase-sum measurement-based schemes. In particular, for quantifying the performance of continuous-variable quantum teleportation of discrete-variable (non-Gaussian) states such as Fock states, the transfer-operator formalism in the Schrödinger picture by Hofmann *et al.* (2000) and by Ide *et al.* (2001) is very useful. In this formalism, the first step is writing the continuous-variable Bell states in the Fock basis, $\hat{D}(\beta)\otimes\mathbb{1}(1/\sqrt{\pi})\Sigma_{n=0}^{\infty}|n\rangle|n\rangle$, where $\hat{D}(\beta)$ is the displacement operator and $\beta=u+iv$ is the measurement result. After projecting Alice's input state $|\phi\rangle_{\rm in}$ and her half of the two-mode squeezed vacuum state in Eq. (85) onto this Bell basis and reversing the measured displacement in Bob's half, one transfers $|\phi\rangle$ to Bob's location in the form (Hofmann *et al.*, 2000)

$$|\phi_{\rm tel}(\beta)\rangle = \hat{T}(\beta)|\phi\rangle, \tag{169}$$

with the transfer operator

$$\hat{T}(\beta) = \hat{D}(\beta)\mathcal{D}(\lambda)\hat{D}(-\beta), \tag{170}$$

and the distortion operator

$$\mathcal{D}(\lambda) = \sqrt{\frac{1-\lambda}{\pi}}\sum_{n=0}^{\infty}\lambda^{n/2}|n\rangle\langle n|. \tag{171}$$

Here, the teleported state $|\phi_{\rm tel}(\beta)\rangle$ is unnormalized and $\langle\phi_{\rm tel}(\beta)|\phi_{\rm tel}(\beta)\rangle$ is the probability for obtaining result β. The imperfection of the entanglement resource is expressed by the distortion operator, where the factors $\sqrt{1-\lambda}\lambda^{n/2}$ are the Schmidt coefficients of the finitely squeezed, only for the nonmaximally entangled two-mode squeezed vacuum state in Eq. (85). Note that for infinite squeezing, $\lambda\to 1$, the distortion operator, and hence the transfer operator too, becomes proportional to the identity operator. The teleported state $|\phi_{\rm tel}(\beta)\rangle$ corresponds to a single shot (a single teleportation event). Thus the teleported ensemble state, averaged over all measurement results for an ensemble of input states, becomes

$$\hat{\rho}_{\rm tel} = \int d^2\beta|\phi_{\rm tel}(\beta)\rangle\langle\phi_{\rm tel}(\beta)|, \tag{172}$$

corresponding to $W_{\rm tel}(\alpha_2')$ in Eq. (168). The distortion operator has also been used by Braunstein, D'Ariano, *et al.* (2000) to describe the effect of the nonmaximally entangled EPR channel. Moreover, using a universal formalism in the Schrödinger picture, it has been shown by Braunstein, D'Ariano, *et al.* (2000) that in both discrete- and continuous-variable quantum teleportation, Bob's local unitary operation means twisting the shared entanglement relative to the entangled state measured in the Bell detection. The transfer-operator description of continuous-variable quantum teleportation in Eq. (169) corresponds to a completely positive map and $\hat{T}(\beta)$ is just a Kraus operator (Kraus, 1983). This map projects the input state onto the conditional teleported state. Upon averaging over all results β, the map becomes completely positive and trace preserving (CPTP), yielding the normalized teleported state $\hat{\rho}_{\rm tel}$ in Eq. (172). A position-momentum basis description of this transfer-operator or CP-map formalism was given by Takeoka *et al.* (2002). The CP map derived in this paper is also more general, including mixed entangled states as a resource for quantum teleportation. Another alternative formulation of nonideal continuous-variable quantum teleportation was proposed by Vukics *et al.* (2002), utilizing the coherent-state basis.

2. Teleportation criteria

The teleportation scheme with Alice and Bob is complete without any further measurement. The teleported state remains unknown to both Alice and Bob and need not be demolished in a detection by Bob as a final step. However, maybe Alice and Bob are cheating. Suppose that instead of using an EPR channel they try to get away without entanglement and use only a classical channel. In particular, for a realistic experimental situation with finite squeezing and inefficient detectors where perfect teleportation is unattainable, how may we verify that successful quantum teleportation has taken place? To make this verification we shall introduce a third party, "Victor" (the verifier), who is independent of Alice and Bob (Fig. 3). We assume that he prepares the initial input state (drawn from a fixed set of states) and passes it on to Alice. After accomplishing the supposed teleportation, Bob sends the resulting teleported state back to Victor. Victor's knowledge about the input state and detection of the teleported state enable him to verify whether quantum teleportation has really occurred. For this purpose, however, Victor needs some measure that helps him to assess when the similarity between the teleported state and the input state exceeds a boundary that is only exceedable with entanglement.

One such measure[4] is the so-called *fidelity F*, for an arbitrary input state $|\phi_{\rm in}\rangle$ defined by (Braunstein, Fuchs, and Kimble, 2000)

[4] Apart from the fidelity, we also use the symbol F for the mean value of a collective spin. We stick with this notation in both cases to be consistent with the common notation in the literature.

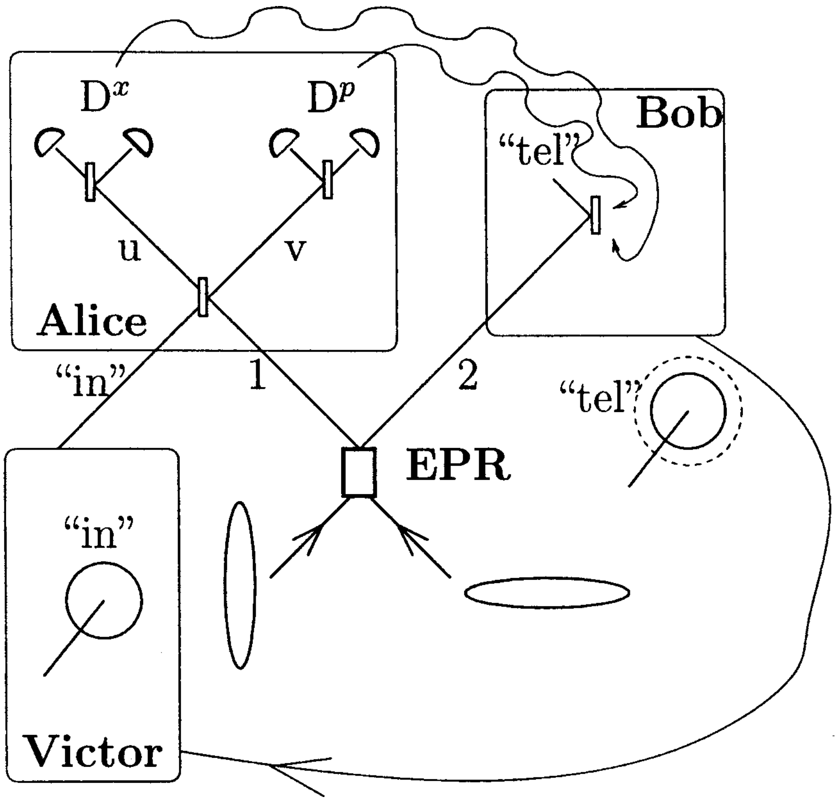

FIG. 3. Verification of quantum teleportation. The verifier "Victor" is independent of Alice and Bob. Victor prepares the input states which are known to him, but unknown to Alice and Bob. After a supposed quantum teleportation from Alice to Bob, the teleported states are given back to Victor. Due to his knowledge of the input states, Victor can compare the teleported states with the input states.

$$F\equiv\langle\phi_{\rm in}|\hat{\rho}_{\rm tel}|\phi_{\rm in}\rangle. \tag{173}$$

It equals one only if $\hat{\rho}_{\rm tel}=|\phi_{\rm in}\rangle\langle\phi_{\rm in}|$. Now Alice and Bob know that Victor draws his states $|\phi_{\rm in}\rangle$ from a fixed set, but they do not know which particular state is drawn in a single trial. Therefore an average fidelity should be considered (Braunstein, Fuchs, and Kimble, 2000),

$$F_{\rm av}=\int P(|\phi_{\rm in}\rangle)\langle\phi_{\rm in}|\hat{\rho}_{\rm tel}|\phi_{\rm in}\rangle d|\phi_{\rm in}\rangle, \tag{174}$$

where $P(|\phi_{\rm in}\rangle)$ is the probability of drawing a particular state $|\phi_{\rm in}\rangle$, and the integral runs over the entire set of input states. If the set of input states contains all possible quantum states in an infinite-dimensional Hilbert space (i.e., the input state is completely unknown apart from its infinite Hilbert-space dimension), the best average fidelity $F_{\rm av}$ achievable by Alice and Bob without using entanglement is zero. The corresponding best average fidelity if the set of input states contains all possible quantum states in a d-dimensional Hilbert space is $F_{\rm av}=2/(1+d)$ (Barnum, 1998). Thus one obtains $F_{\rm av}=0$ for $d\to\infty$, and the qubit boundary $F_{\rm av}=2/3$ for $d=2$. If the input alphabet is restricted to coherent states of amplitude $\alpha_{\rm in}=x_{\rm in}+ip_{\rm in}$ and $F=\langle\alpha_{\rm in}|\hat{\rho}_{\rm tel}|\alpha_{\rm in}\rangle$, on average, the fidelity achievable in a purely classical scheme (when averaged across the entire complex plane for arbitrary coherent-state inputs) is bounded by (Braunstein, Fuchs, and Kimble, 2000)

$$F_{\rm av}\leqslant\frac{1}{2}. \tag{175}$$

Let us apply the fidelity criterion to the single-mode teleportation equations (165) and assume an input alphabet containing all coherent states with equal probability. Up to a factor π, the fidelity $F=\langle\alpha_{\rm in}|\hat{\rho}_{\rm tel}|\alpha_{\rm in}\rangle$ is the Q function of the teleported mode evaluated for $\alpha_{\rm in}$. This Q function is, in general, a bivariate Gaussian with mean value $g(x_{\rm in}+ip_{\rm in})$,

$$\begin{aligned}F&=\pi Q_{\rm tel}(\alpha_{\rm in})\\&=\frac{1}{2\sqrt{\sigma_x\sigma_p}}\exp\left[-(1-g)^2\left(\frac{x_{\rm in}^2}{2\sigma_x}+\frac{p_{\rm in}^2}{2\sigma_p}\right)\right],\end{aligned} \tag{176}$$

where g is the gain and σ_x and σ_p are the variances of the Q function of the teleported mode for the corresponding quadratures. The Q function is a convolution of the Wigner function with a Gaussian of one unit of vacuum [Eqs. (33) and (34)], i.e., we have to add this unit to the actual variances of the teleported quadratures. According to Eq. (165), for a coherent-state input, the variances of the Q function are then given by

$$\sigma_x=\sigma_p=\frac{1}{4}(1+g^2)+\frac{e^{+2r}}{8}(g-1)^2+\frac{e^{-2r}}{8}(g+1)^2. \tag{177}$$

Teleporting states with a coherent amplitude as reliably as possible requires unit-gain teleportation (unit gain in Bob's final displacements). Only in this case do the coherent amplitudes of the teleported states always match those of the input states provided by Victor. For classical teleportation ($r=0$) and $g=1$, we obtain $\sigma_x=\sigma_p=1$ and indeed $F=F_{\rm av}=1/2$. In order to obtain a better fidelity, entanglement is needed. Then, if $g=1$, we obtain $F=F_{\rm av}>1/2$ for any $r>0$. For this unit-gain teleportation, we have seen that the teleported state W_{tel} is a convolution of the input W_{in} with a complex Gaussian of variance e^{-2r} [Eq. (168)]. Classical teleportation with $r=0$ then means the teleported mode has an excess noise of two complex units of vacuum, $1/2+1/2$, relative to the input; any $r>0$ beats this classical scheme. Hence if the input state is always recreated with the right amplitude and less than two units of vacuum excess noise, Alice and Bob must have employed entanglement as a resource.

Let us also write the fidelity in terms of the transfer operator of Eq. (170). Using Eqs. (172), (169), and (173), with a coherent-state input, leads to

$$F=\int d^2\beta|\langle\alpha_{\mathrm{in}}|\hat{T}(\beta)|\alpha_{\mathrm{in}}\rangle|^2=\frac{1+\sqrt{\lambda}}{2}. \tag{178}$$

Here we used $\hat{D}(-\beta)|\alpha\rangle=|\alpha-\beta\rangle$ and $|\langle n|\alpha\rangle|^2=|\alpha|^{2n}e^{-|\alpha|^2}/n!$. This fidelity becomes independent of α_{in}, because the transfer operator of Eq. (170) corresponds to unit-gain teleportation. Hence with $\lambda=\tanh^2 r$, we obtain $F=F_{\mathrm{av}}=1/(1+e^{-2r})$, identical to the result for $g=1$ using Eqs. (176) and (177).

In Sec. III.B, we found that one squeezed state is a sufficient resource for generating entanglement between an arbitrary number of parties. In fact, applied to the two-party teleportation scenario, the entanglement from only one squeezed state makes possible quantum teleportation with $F_{\mathrm{av}}>1/2$ for any nonzero squeezing (van Loock and Braunstein, 2000a). Unless Alice and Bob have access to additional local squeezers,[5] the maximum fidelity of coherent-state teleportation achievable with one single-mode squeezed state is $F_{\mathrm{av}}=1/\sqrt{2}$ in the limit of infinite squeezing (van Loock and Braunstein, 2000a).

Alternative criteria for quantum teleportation were proposed by Ralph and Lam (1998). Reminiscent of the criteria (Holland *et al.*, 1990) for quantum nondemolition measurements (Caves *et al.*, 1980), these are expressed in terms of two inequalities for the conditional variances [Eq. (145)] and the so-called signal transfer coefficients of both conjugate quadratures. The boundary between classical and quantum teleportation defined by the criteria of Ralph and Lam (1998) differs from that in Eq. (175) in terms of fidelity. According to Ralph and Lam, the best classical protocol permits output states completely different from the input states, corresponding to zero fidelity. This can be achieved, for instance, via an asymmetric detection scheme, where the lack of information in one quadrature leads, on average, to output states with amplitudes completely different from those of the input states. However, certain correlations between the input and the teleported quadratures can still attain the optimal value allowed without using entanglement. By contrast, the best classical protocol in terms of fidelity always achieves output states pretty similar to the input states. The fidelity boundary in Eq. (175) is exceeded for any squeezing in the EPR channel, whereas fulfillment of the teleportation criteria of Ralph and Lam (1998) requires more than 3 dB squeezing.

Finally, Grosshans and Grangier (2001) propose $F_{\mathrm{av}}\leqslant 2/3$ as the fidelity boundary between classical and quantum teleportation of arbitrary coherent states. Exceeding this bound would also require an EPR channel with more than 3 dB squeezing. The reasoning by Grosshans and Grangier (2001) is that only when Bob receives a state with $F_{\mathrm{av}}>2/3$ is it guaranteed that nobody else (neither Alice nor an eavesdropper Eve) can have an equally good or better copy. Otherwise, two copies of the unknown input state with $F_{\mathrm{av}}>2/3$ would exist, which contradicts the no-cloning boundary for coherent-state duplication (see Sec. V). On the other hand, when Bob receives, for example, a state with $1/2<F_{\mathrm{av}}<2/3$, Alice might have locally made two asymmetric copies, one with $F_{\mathrm{av}}>2/3$ and one with $1/2<F_{\mathrm{av}}<2/3$. She might have sent the worse copy to Bob via a perfectly entangled (or sufficiently entangled) EPR channel and kept the better copy. Thus, according to Grosshans and Grangier (2001), the "quantum faxing" region, $1/2<F_{\mathrm{av}}\leqslant 2/3$, does not indicate true quantum teleportation of coherent states. Similarly, one would have to give the region $2/3<F_{\mathrm{av}}\leqslant 5/6$ (where $5/6$ is the qubit duplication limit; see Sec. V) an analogous status of only quantum faxing when teleportation of arbitrary qubits is considered. By contrast, the fidelity boundary between classical and quantum teleportation of arbitrary qubit states, analogous to that of arbitrary coherent states in Eq. (175), is $F_{\mathrm{av}}\leqslant 2/3$ (Barnum, 1998). A detailed discussion of the different fidelity boundaries for coherent-state teleportation can be found in the work of Braunstein, Fuchs, *et al.* (2001).

What are the "right" criteria for continuous-variable quantum teleportation among those discussed above? The most appropriate criteria in a specific scenario certainly depend on the particular task that is to be fulfilled by quantum teleportation. For example, using quantum teleportation of coherent states as a subroutine for quantum cryptography, the security is (to some extent) ensured by $F_{\mathrm{av}}>2/3$ (Grosshans and Grangier, 2001). However, for an input alphabet of coherent states to be transferred, a rigorous boundary that unambiguously separates entanglement-based quantum teleportation schemes from schemes based solely on classical commu-

[5] Using additional local squeezers, Alice and Bob can transform the shared entangled state built from one squeezed state into the canonical two-mode squeezed state (van Loock, 2002; Bowen, Lam, and Ralph, 2003; van Loock and Braunstein, 2003). Note that such local squeezing operations do not change the amount of entanglement. The resulting two-mode squeezed state obviously can approach unit fidelity when used for quantum teleportation. Though conceptually interesting (the amount of entanglement inherent in an entangled state built with one squeezer is arbitrarily large for sufficiently large squeezing and hence there is no fidelity limit), this would not be the most practical way to achieve high-fidelity quantum teleportation. The entire teleportation process would require three squeezers with squeezing $2r$, r, and r, instead of only the two r squeezers needed to produce the canonical two-mode squeezed state (van Loock, 2002; Bowen, Lam, and Ralph, 2003; van Loock and Braunstein, 2003).

nication is given by $F_{\mathrm{av}} \leqslant 1/2$, Eq. (175) [see also the very recent proofs of this fidelity boundary by Krüger *et al.* (2004) and by Hammerer *et al.* (2004)].

Another possible way to assess whether a continuous-variable teleportation scheme is truly quantum is to check to what extent nonclassical properties such as squeezing or photon antibunching can be preserved in the teleported field (Li, Li, *et al.*, 2002). Once Alice and Bob do not share entanglement [for instance, when the pure two-mode squeezed vacuum state becomes mixed in a thermal environment (Lee *et al.*, 2000)], nonclassical properties can no longer be transferred from Alice to Bob. Let us now consider the teleportation of a truly quantum-mechanical system, namely, an electromagnetic mode entangled with another mode. This entanglement will be transferred to a third mode via quantum teleportation.

3. Entanglement swapping

In three optical teleportation experiments in Innsbruck (Bouwmeester *et al.*, 1997), Rome (Boschi *et al.*, 1998), and Pasadena (Furusawa *et al.*, 1998), the nonorthogonal input states to be teleported were single-photon polarization states (Bouwmeester *et al.*, 1997; Boschi *et al.*, 1998) and coherent states (Furusawa *et al.*, 1998). From a true quantum teleportation device, however, we would also require the capability of teleporting the entanglement source itself. This teleportation of one-half of an entangled state, *entanglement swapping*, was first introduced for single-photon polarization states (Zukowski *et al.*, 1993). In general, it allows for the entanglement of two quantum systems that have never directly interacted with each other. A demonstration of entanglement swapping with single photons was reported by Pan *et al.* (1998). Practical uses of entanglement swapping have been suggested (Bose *et al.*, 1998, 1999; Briegel *et al.*, 1998; Dür, Briegel, *et al.*, 1999) and it has also been generalized to multiparticle systems (Bose *et al.*, 1998). All these investigations have referred exclusively to discrete-variable systems.

There have been several theoretical proposals for an entanglement swapping experiment involving continuous variables. Polkinghorne and Ralph (1999) suggested teleporting polarization-entangled states of single photons using squeezed-state entanglement (in the limit of small squeezing) in which output correlations are verified via Bell inequalities. Tan (1999) and van Loock and Braunstein (2000b) considered the unconditional teleportation (without postselection of "successful" events by photon detections) of one-half of a two-mode squeezed state using quadrature Bell measurements and different verification schemes. van Loock and Braunstein (2000b) verified entanglement swapping through a second quantum teleportation process utilizing the entangled output state. Tan (1999) verified output entanglement via Eq. (112) using unit-gain displacements and hence requiring more than 3 dB squeezing. The gain, however, can be optimized, enabling a verification of entanglement swapping for any squeezing (van Loock and Braunstein, 2000b; van Loock, 2002).

Choosing the right gain is essential in entanglement swapping, for instance, in order to optimize the fidelity in a second round of teleportation (van Loock and Braunstein, 2000b) or to maximize the violations of Bell inequalities at the output in the low-squeezing (single-photon) limit (Polkinghorne and Ralph, 1999). The explanation for this is as follows: if the conditional states are displaced with the right gain, they no longer depend on the Bell measurement results, always being transformed to the same canonical two-mode squeezed state. The optimal scheme then leads to a pure ensemble output state. Even after averaging over all incoming states and measurement results, the output remains a pure two-mode squeezed vacuum state with a new squeezing parameter R modified by (van Loock, 2002)

$$\tanh R = \tanh r \tanh r' . \tag{179}$$

Up to a phase-space displacement, the resulting ensemble state is the same as the projected displaced two-mode squeezed state for a single shot of the continuous-variable Bell measurement. In Eq. (179), r and r' are the squeezing parameters of the two initial entangled two-mode squeezed states. For any nonzero squeezing and hence entanglement in both input states, $r>0$ and $r'>0$, entanglement swapping occurs, i.e., $R>0$. However, the quality of the entanglement always deteriorates, $R<r$ and $R<r'$, unless either of the input states approaches a maximally entangled state, $r\to\infty$ and hence $R=r'$, or $r'\to\infty$, thus $R=r$.

As a consequence, in a quantum repeater (Briegel *et al.*, 1998), connecting many segments of a quantum channel via continuous-variable entanglement swapping, after purifying the mixed entangled states in each segment to pure ones (two-mode squeezed states), will produce never vanishing, but increasingly small entanglement between the ends of the channel. This statement, however, is restricted to an entanglement swapping protocol based on continuous-variable (quadrature) Bell measurements.

B. Dense coding

Dense coding aims to use shared entanglement to increase the capacity of a communication channel (Bennett and Wiesner, 1997). Relative to quantum teleportation, in dense coding the roles played by the quantum and classical channels are interchanged. Dense coding was translated to continuous quantum variables by Ban (1999) and by Braunstein and Kimble (2000). It was shown that by utilizing the entanglement of a two-mode squeezed state one can always beat coherent communication (based on coherent states; Braunstein and Kimble, 2000). The continuous-variable scheme attains a capacity approaching (in the limit of large squeezing) twice that theoretically achievable in the absence of entanglement (Braunstein and Kimble, 2000). Before we discuss how dense coding can be implemented with continuous variables, let us review the ideas behind quantifying information for communication.

1. Information: A measure

In classical information theory one constructs a measure of information that tries to capture the "surprise" attached to receiving a particular message. Thus messages that are common occurrences are assumed to contain very little useful information, whereas rare messages are deemed to be valuable and to contain more information. This concept suggests that the underlying symbols or letters or alphabet used to transmit the message are themselves unimportant, but not the probabilities of these symbols or messages.

In addition to this conceptual framework, it turns out that the measure of information is essentially unique if one takes it to be additive for independent messages.

To formalize the idea of an alphabet we define it to be a set $A=\{a:a\in A\}$ of symbols a each of which has an associated probability p_a. The information content of such an alphabet will be denoted $I(A)$. The average information content per letter in alphabet A is given by

$$I(A)=-\sum_a p_a \ln p_a. \tag{180}$$

This result is the unique measure of average information per letter.

2. Mutual information

In order to quantify the information in a communication channel we must introduce a measure of information corresponding to the amount of information accessible to the receiver which contains information about the message sent. This suggests we attempt to quantify the information mutual (or common) to a pair of alphabets A and B. If these two alphabets have letters with probabilities given by p_a and p_b, respectively, and if the joint alphabet AB has letters with probabilities p_{ab} (we no longer assume these alphabets are independent), then the natural information-theoretic measures for these three quantities are given by

$$I(A)=-\sum_a p_a \ln p_a,$$

$$I(B)=-\sum_b p_b \ln p_b,$$

$$I(A,B)=-\sum_{ab} p_{ab} \ln p_{ab}. \tag{181}$$

The so-called mutual information $I(A:B)$ in a pair of alphabets is given by

$$I(A:B)=I(A)+I(B)-I(A,B)=\sum_{ab} p_{ab} \ln\left(\frac{p_{ab}}{p_a p_b}\right). \tag{182}$$

The idea behind this equation is that the sum $I(A)+I(B)$ accounts for the joint information in both alphabets, but double counts that part which is mutual to both alphabets. By subtracting the correct expression for the joint information $I(A,B)$ we are left solely with the information that is common or mutual.

3. Classical communication

We are now in a position to apply our expression for the mutual information to quantify the information received through a communication channel that contains information or that is mutual or common to the information actually sent.

Let us suppose the sender, Alice, has a source alphabet A with probabilities p_a. For each letter a sent the receiver, Bob, tries to determine its value through observation at his end of the channel. However, because of whatever source of noise or imprecision in general Bob will see an alphabet B that is not identical to Alice's.

For simplicity, we shall suppose that the channel has no memory, so that each signal sent is independent of earlier or later channel usage. In this case, we may characterize the channel by the conditional probabilities $p_{b|a}$, for the probability of observing letter b in Bob's alphabet, given that Alice sent letter a. The joint probability is therefore given by

$$p_{ab}=p_{b|a}p_a. \tag{183}$$

Given these expressions the mutual information content, per usage of the channel, in Bob's received data about Alice's messages is

$$I(A:B)=\sum_{ab} p_{b|a}p_a \ln\left(\frac{p_{b|a}}{p_b}\right). \tag{184}$$

If we optimize this expression over Alice's alphabet, we can determine the maximum achievable throughput per usage. This is called the *channel capacity* and is given by

$$C=\max_{\{p_a\}} I(A:B). \tag{185}$$

4. Classical communication via quantum states

Ultimately, Alice must use some physical carrier to represent the letters she sends. For simplicity of notation we shall tie the physical states she generates together with any modifying effects from the channel. Thus we shall say that to represent a letter a from her alphabet A, Alice produces a quantum state $\hat{\rho}_a$. Since letter a is generated with probability p_a, the mean channel state is simply

$$\hat{\rho}=\sum_a p_a\hat{\rho}_a. \tag{186}$$

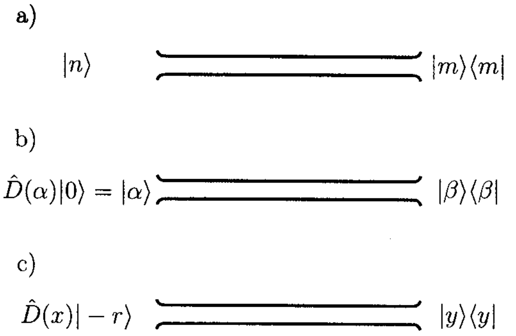

FIG. 4. Communication channel with (a) optimal number-state alphabet; (b) coherent-state alphabet; and (c) squeezed-state alphabet.

Now let us suppose that Bob uses some generalized measurement (POVM) $\hat{E}_b$, satisfying Eq. (159), to try to extract information about the letter Alice was trying to send. When Bob is presented with a state $\hat{\rho}_a$ representing letter a from Alice's alphabet, he will find instead letter b from his own alphabet with a conditional probability given by Eq. (160), from which one may compute the mutual information $I(A:B)$ using Eq. (184).

The famous result from Holevo (1998) allows us to place an upper bound on this mutual information via Eq. (158). We note that either bound is independent of Bob's measurement strategy, so an achievable upper bound will allow us to determine the channel capacity for transmitting classical information using quantum states. In fact, when this strategy works it reduces the calculation of the channel capacity to one of performing a maximum-entropy calculation.

When the states used to send information are from an infinite-dimensional Hilbert space (such as a single-mode bosonic field), we must place some constraint on the channel usage in order to get a finite value for this capacity. The canonical constraint in such circumstances is to presume that there is a constraint on the mean number of quanta that may pass down the channel per usage $\langle\hat{n}\rangle=\bar{n}$. For this constraint, the maximum entropy may be interpreted as the channel capacity achieved when Alice uses an alphabet of number states distributed according to a thermal distribution (Yuen and Ozawa, 1993; Caves and Drummond, 1994). In this case, the channel capacity is given by

$$C = (1+\bar{n})\ln(1+\bar{n}) - \bar{n}\ln\bar{n} \simeq 1 + \ln\bar{n}, \tag{187}$$

for large $\bar{n}$.

Given a constraint on the mean number of photons per channel usage $\langle\hat{n}\rangle=\bar{n}$ we shall now compare three choices of alphabets for transmission by Alice (see Fig. 4). Figure 4(a) shows the optimal strategy using an input alphabet of number states and ideal photon-number detection. Figure 4(b) shows the channel with the same constraint operating with an input alphabet of coherent states and a heterodyne detection. With this extra constraint on the input alphabet the maximal throughput is given by (Gordon, 1962; She, 1968; Yamamoto and Haus, 1986)

$$C^{\mathrm{coh}} = \ln(1+\bar{n}) \simeq \ln\bar{n}. \tag{188}$$

Finally, if Alice uses a strategy involving a squeezed-state alphabet (labeled by the displacements x) and homodyne detection, see Fig. 4(c), the maximal throughput is given by (Yamamoto and Haus, 1986)

$$C^{\mathrm{sq}} = \ln(1+2\bar{n}) \simeq \ln 2 + \ln\bar{n}. \tag{189}$$

We can see that for large $\bar{n}$ each of these schemes has a capacity that differs by only around one bit per usage!

5. Dense coding

In dense coding, Alice and Bob communicate via two channels, however, Alice only needs to modulate one of them. The second channel is used to transmit one-half of a standard (entangled) state to Bob; since this channel is not modulated it may be sent at any time, including prior to its need for communication. In this way, part of the communication channel may be run *off-peak*. Classically there is no way to achieve this sort of operation.

In general, Alice's local action is sufficient to span a system with the square of the Hilbert-space dimension of the piece she holds. Since information is essentially the logarithm of the number of distinguishable states,

$$\log(n^2) = 2\log n, \tag{190}$$

one can generally expect a doubling of the channel capacity. This accounting assumes that the off-peak usage required to transmit the shared entanglement, or to otherwise generate it, comes at no cost.

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

$$W_{\mathrm{EPR}}(\alpha_1,\alpha_2) = \frac{4}{\pi^2}\exp[-e^{-2r}(\alpha_1-\alpha_2)_R^2 - e^{2r}(\alpha_1-\alpha_2)_I^2 - e^{2r}(\alpha_1+\alpha_2)_R^2 - e^{-2r}(\alpha_1+\alpha_2)_I^2], \tag{191}$$

where the subscripts R and I refer to real and imaginary parts of the field amplitude α, respectively.

As shown in Fig. 5, signal modulation is performed only on Alice's mode, with the second mode treated as an overall shared resource by Alice and Bob. The modulation scheme that Alice chooses is simply to displace her mode by an amount α. This leads to a displaced Wigner function given by $W_{\mathrm{EPR}}(\alpha_1-\alpha,\alpha_2)$, corresponding to the field state that is sent via the quantum channel from Alice to Bob.

Upon receiving this transmitted state (consisting of Alice's modulated mode), Bob's final step in the dense-coding protocol is to combine it with the shared resource he holds and to retrieve the original classical signal α with as high a fidelity as possible. As indicated in Fig. 5, this demodulation can be performed with a simple 50:50 beam splitter that superposes these modes to yield output fields that are the sum and difference of the input

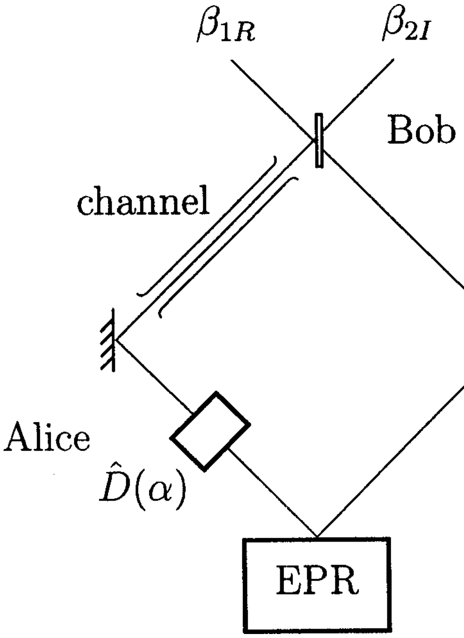

FIG. 5. Schematic of dense-coding scheme: An EPR pair is created and one-half sent to Bob. The other half is given to Alice, who modulates it by performing a phase-space translation by the amount α. This half is now passed on to Bob, who recombines the two halves and performs a pair of homodyne measurements on the sum and difference fields. These signals β_{1R} and β_{2I} will closely mimic α for a sufficiently strongly entangled state.

fields and that we label as β_1 and β_2, respectively. The resulting state emerging from Bob's beam splitter has the following Wigner function:

$$W_{\text{sum/diff}}(\beta_1,\beta_2) = W_{\text{EPR}}[(\beta_1+\beta_2)/\sqrt{2}-\alpha, (\beta_1-\beta_2)/\sqrt{2}]. \tag{192}$$

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

$$p_{\beta|\alpha} = \frac{2e^{2r}}{\pi}\exp(-2e^{2r}|\beta-\alpha/\sqrt{2}|^2), \tag{193}$$

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

$$p_\alpha = \frac{1}{\pi\sigma^2}\exp(-|\alpha|^2/\sigma^2). \tag{194}$$

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

$$\bar{n} = \sigma^2 + \sinh^2 r. \tag{195}$$

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

$$p_\beta = \frac{2}{\pi(\sigma^2+e^{-2r})}\exp\left(\frac{-2|\beta|^2}{\sigma^2+e^{-2r}}\right). \tag{196}$$

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

$$\begin{aligned} I^{\text{dense}}(A:B) &= \int d^2\beta d^2\alpha p_{\beta|\alpha} p_\alpha \ln\left(\frac{p_{\beta|\alpha}}{p_\beta}\right) \\ &= \ln(1+\sigma^2 e^{2r}). \end{aligned} \tag{197}$$

For a fixed $\bar{n}$ in Eq. (195) this information is optimized when $\bar{n}=e^r\sinh r$, i.e., when $\sigma^2=\sinh r\cosh r$, yielding a dense-coding capacity of

$$C^{\text{dense}} = \ln(1+\bar{n}+\bar{n}^2), \tag{198}$$

which for large squeezing r becomes

$$C^{\text{dense}} \sim 4r. \tag{199}$$

How efficient is this dense coding in comparison to single-channel coding? Let us place a common constraint of having a fixed mean number of photons $\bar{n}$ that can be modulated. The maximal channel capacity as given in Eq. (187) and substituting $\bar{n}=e^r\sinh r$ gives

$$C \sim 2r, \tag{200}$$

for large squeezing r. This is just one-half of the asymptotic dense-coding mutual information [see Eq. (199)]. Thus asymptotically, at least, the dense-coding scheme allows twice as much information to be encoded within a given state, although it has the extra expense (not included within the simple constraint $\bar{n}$) of requiring shared entanglement.

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

$$r_{\text{break-even}} \simeq 0.7809, \tag{201}$$

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

A fairer comparison is against single-mode coherent-state communication with heterodyne detection. Here the channel capacity is given by Eq. (188) and is always beaten by the optimal dense-coding scheme described by Eq. (198).

An improvement on coherent-state communication is squeezed-state communication with a single mode. The channel capacity of this channel is given by Eq. (189)

and is beaten by the dense-coding scheme of Eq. (198) for $\bar{n}>1$, i.e., the break-even squeezing required is

$$r^{\text{sq}}_{\text{break-even}} \simeq 0.5493, \tag{202}$$

which corresponds to 4.77 dB.

Note that this continuous-variable protocol should allow for high-efficiency, unconditional transmission with encoded information sent every inverse bandwidth time. This situation is in contrast to implementations that employ weak parametric down conversion, where transmission is achieved conditionally and relatively rarely. In fact, Mattle *et al.* (1996) obtained rates of only 1 in 10^7 per inverse bandwidth time (Weinfurter, 1998). In the limit of strong down conversion and using continuous-variable entanglement, much higher efficiency should be achievable.

It should be noted that one feature about dense coding is our assumption that the shared entanglement may be sent off-peak. This implicitly assumes that entanglement can be stored (possibly for long periods of time). Continuous-variable entanglement has now been shown to be easy to create in collective atomic states and to be efficiently transformable back and forth to optical entanglement (Julsgaard *et al.*, 2001; see Sec. IV.F). Thus although the storage times are still very small, there is potential for a high-bandwidth technology here.

C. Quantum error correction

Let us now proceed with a few remarks on an alternative method for the reliable transmission of quantum information, which is not based on shared entanglement such as quantum teleportation combined with entanglement distillation (the latter is the subject of Sec. IV.E). This method is called *quantum error correction* (Shor, 1995).

In a quantum error-correction scheme used for communication purposes, quantum states are sent directly through a potentially noisy channel after encoding them into a larger system that contains additional auxiliary subsystems. When this larger system is subject to errors during its propagation through the quantum channel, under certain circumstances these errors can be corrected at the receiving station and the input quantum state can be retrieved, in principle, with unit fidelity.

For discrete variables, a lot of theoretical work on quantum error correction has been done, for example, by Shor, 1995; Calderbank *et al.*, 1997; and Knill and Laflamme, 1997. Shortly after the proposal for the realization of continuous-variable teleportation, the known qubit quantum error-correction codes were translated to continuous variables (Braunstein, 1998a; Lloyd and Slotine, 1998). These schemes appeared to require active nonlinear operations such as quantum nondemolition coupling for the implementation of the controlled-NOT gate (Braunstein, 1998a). However, it later turned out that continuous-variable quantum error-correction codes also can be implemented using only linear optics and resources of squeezed light (Braunstein, 1998b). This was shown for the nine-wave-packet code (Braunstein, 1998b), the analog of Shor's nine-qubit code (Shor, 1995). It is still an open question how to implement the five-wave-packet code using only linear optics and squeezed light.

A more robust set of quantum error-correcting codes over continuous variables was proposed by Gottesman *et al.* (2001). These codes protect discrete-variable quantum information, i.e., states of a finite-dimensional system, from decoherence by encoding it into the infinite-dimensional Hilbert space of a continuous-variable system (an "oscillator"). The advantage of this variation over the codes described above is that the codes from Gottesman *et al.* (2001) allow effective protection against small "diffusive" errors, which are closer to typical realistic loss mechanisms. In the codes discussed above, small errors comparable to or smaller than readout errors cannot be corrected and are additive with each "protective" operation.

D. Quantum cryptography

In this section, we give an overview of the various proposals of continuous-variable quantum cryptography (or quantum key distribution). We further discuss absolute theoretical security and verification of the experimental security of continuous-variable quantum key distribution. Finally, we conclude this section with a few remarks on quantum secret sharing with continuous variables.

1. Entanglement-based versus prepare and measure

For qubit-based quantum cryptography there have been two basic schemes. Those involving the sending of states from nonorthogonal bases, such as the original "BB84 protocol" (Bennett and Brassard, 1984), and those based on sharing entanglement between the sender and receiver, such as Ekert's scheme (Ekert, 1991). The protocols without entanglement may be termed "prepare and measure" schemes, in which Alice randomly prepares a sequence of nonorthogonal states to be sent to Bob and Bob measures these states in a randomly chosen basis. In general, the entanglement-based schemes, without Ekert's approach using Bell inequalities, can also be interpreted as state preparation at a distance. As a result of entanglement, the states nonlocally prepared at the receiving station should be correlated to the sender's states, which are measured in a randomly chosen basis. The entanglement-based schemes are then equivalent to schemes such as the BB84 protocol (Bennett *et al.*, 1992).

Conversely, it has been shown that the presence of entanglement in the quantum state effectively distributed between Alice and Bob is a necessary precondition for any secure quantum key distribution protocol (Curty *et al.*, 2004). In this sense, the notion of entanglement can be recovered in the prepare and measure schemes which do not appear to rely upon entanglement. The crucial point is that the correlations given by the classical data of Alice's and Bob's measurements, described by a joint classical probability distribution $P(A,B)$, must not be consistent with a separable state (Curty *et al.*, 2004). This requirement is independent of the particular physical implementation, though the prepare and measure schemes usually seem more practical than those based on the distribution of entanglement. Thus a first test of secure quantum key distribution is to check for (optimal) *entanglement witnesses* (observables that detect entanglement), given a set of local operations and a corresponding classical distribution $P(A,B)$ (Curty *et al.*, 2004). An example of such an entanglement witness would be the violation of Bell inequalities as in Ekert's scheme (Ekert, 1991). However, even if there are no such violations, a suitable entanglement witness to prove the presence of quantum correlations may still be found. In the continuous-variable case, a particularly practical witness is given by the Duan criterion in Eq. (110) or Eq. (114), based solely upon efficient homodyne detection. Now bearing in mind that any secure quantum key distribution scheme must rely upon the effective distribution of entanglement, a similar categorization into prepare and measure schemes and those based on entanglement can be made for the various proposals of continuous-variable quantum cryptography.

2. Early ideas and recent progress

The schemes that do not rely on entanglement are mostly based on alphabets involving (nonorthogonal) coherent states as the signal states. For example, Mu *et al.* (1996) utilize four coherent states and four specific local oscillator settings for homodyne detection, enabling the receiver to conclusively identify a bit value. Huttner *et al.* (1995) use generalized measurements (POVM's) instead, which may sometimes yield inconclusive results for a bit value encoded in a weak coherent state. The scheme of Huttner *et al.* is actually a combination of the BB84 (Bennett and Brassard, 1984) and "B92" (Bennett, 1992) qubit protocols, the latter of which requires just two arbitrary nonorthogonal states. The basic idea behind this combination is to make the two states in each pair of basis states, which are orthogonal in BB84, nonorthogonal instead as in B92. By using nonorthogonal states in each pair, one gets the additional advantage of the B92 protocol, namely, that an eavesdropper, Eve, cannot deterministically distinguish between the two states in each basis. The usual disadvantage of not being able to create single-photon states, but rather weak coherent-state pulses (where pulses on average contain fewer than one photon), is then turned into a virtue. Distinguishing between two coherent signal states for these coherent-state schemes was shown by Banaszek (1999) to be possible for a receiver using a simple optical arrangement.

The use of squeezed states rather than coherent states was investigated by Hillery (2000). His analysis of security, explicitly including the effects of loss, is in some sense realistic, though ignoring collective attacks.[6] He did, however, study, two kinds of eavesdropper attack: man-in-the-middle (or intercept-resend) attacks measuring a single quadrature; and quantum-tap attacks using a beam splitter, after which again only a single quadrature is measured. Hillery found that losses produce a significant degradation in performance, but suggested that this problem could be ameliorated by preamplification.

The entanglement-based quantum cryptographic schemes within the framework of continuous-variable quantum optics rely on correlations of the quadratures of two-mode squeezed states. Cohen (1997) considered the idealized case with an unphysical infinite amount of squeezing to give perfect correlations. More realistically, Pereira *et al.* (2000; in an article that was first circulated as a preprint in 1993) considered cryptography based on finitely squeezed two-mode light beams. Their paper described a scheme more reminiscent of dense coding than of a standard quantum cryptographic protocol, since it is based on preshared entanglement and the transmission of one-half of the entangled state.

Ralph (2000a) has considered continuous-variable quantum cryptography in two variations: first, a scheme in which the information is encoded onto just a single (bright) coherent state; and second, an entanglement-based scheme, in which the bit strings are impressed on two (bright) beams squeezed orthogonally to each other before being entangled via a beam splitter (i.e., becoming entangled in a two-mode squeezed state). In assessing these schemes, Ralph considered three noncollective attacks by Eve. The first two involved the eavesdropper's acting as man in the middle, in one by measuring a fixed quadrature via homodyne detection, and in the other by measuring both quadratures via heterodyne detection [or an Arthurs-Kelly-type double homodyne detection (Arthurs and Kelly, 1965)] and reproducing the signal based on the measured values. The third used a highly asymmetric beam splitter as a quantum tap on the communication channel, after which simultaneous detection of both quadratures [again *à la* Arthurs and Kelly (1965)] was used to maximize information retrieval.

In his former, entanglement-free scheme, Ralph found that the third of his three eavesdropping strategies allowed Eve to obtain significant information about the coherent state sent with only minimal disturbance in the bit-error rate observed between Alice and Bob. Thus this first scheme proved inferior in security to normal qubit scenarios. By contrast, his entanglement-based scheme apparently gave comparable security to qubit schemes when analyzed against the same three attacks.

[6] Commonly, a distinction is made between three different classes of attacks (Lütkenhaus, 2002). In an individual attack, each signal is coupled to a probe, and each probe is measured independently of the others. In a collective attack, several probes are collected and measured jointly. The most general attack, is the coherent attack, in which many signals are coupled to many probes followed by a collective measurement of the probes.

Indeed, for this entanglement-based scheme a potential eavesdropper is revealed through a significant increase in the bit-error rate (for a sample of data sent between Alice and Bob). Ralph also considered an eavesdropping strategy based on quantum teleportation (Ralph, 2000b) and showed again that there is a favorable tradeoff between the extractable classical information and the disturbance of the signals passed on to the receiver. We note, however, that enhanced security in this entanglement-based scheme requires high levels of squeezing and low levels of loss in the channel. Ralph's latter work (Ralph, 2000b) includes an analysis of losses.

Reid (2000) has considered a similar scheme, exploiting the Heisenberg correlations [Eq. (146)] between the modes of a two-mode squeezed state. In fact, this scheme is directly analogous to Ekert's qubit scheme (Ekert, 1991), in which the protection against Eve is provided by Alice and Bob's being able to observe a Bell inequality violation. The security analysis was limited to studying a quantum-tap-based attack using a beam splitter and measurement of a single quadrature. In addition, like Hillery and Ralph, Reid includes losses in her analysis.

Finally, we note two other theoretical works, by Silberhorn, Korolkova, and Leuchs (2002; an entanglement-based protocol) and by Grosshans and Grangier (2002; a protocol relying solely upon the nonorthogonality of coherent states). Very recently, the latter scheme based on coherent states was implemented experimentally (Grosshans *et al.*, 2003). It has also been demonstrated by Grosshans *et al.* (2003) that this protocol is, in principle, secure for any value of the line transmission rate. Initially, a line transmission below 50%, corresponding to line loss above 3 dB, was thought to render secure key distribution impossible. Conversely, a scheme with line loss $\leqslant 3$ dB was considered secure (to some extent), because the no-cloning bound for coherent states (Sec. V) prevents Eve from obtaining better signals than Bob (when Eve replaces the lossy channel by a perfect one and employs beam-splitter-based cloning of the coherent signals as the supposedly optimal eavesdropping strategy). As for the existence of secure schemes beyond the 3-dB loss limit, one should realize that the entanglement of a continuous-variable resource (two-mode squeezed states), though degraded, never vanishes completely for any degree of the loss (Duan, Giedke, *et al.*, 2000a; Braunstein, Fuchs, *et al.*, 2001).[7] In other words, the necessary precondition for secure key distribution according to the theorem of Curty *et al.* (2004), namely, the presence of quantum correlations, can be satisfied for any line loss. Let us briefly discuss how this potential security of schemes beyond 3-dB loss may be exploited, especially by utilizing classical techniques.

The information-theoretic condition for secure communication, i.e., for enabling extraction of a secure key using privacy amplification (Bennett *et al.*, 1995) and error-correction techniques (Brassard and Salvail, 1994), is given by the following relation for the mutual information [Eq. (182)] between participants:

$$I(A{:}B) > \max\{I(A{:}E), I(E{:}B)\}. \tag{203}$$

In other words, the mutual information between Alice and Bob, $I(A:B)$, must exceed the information that either of them shares with Eve. For losses beyond 3 dB, the condition $I(A:B) > I(A:E)$ is always violated using the standard classical techniques. However, there are methods to beat this 3-dB loss limit. One such method is using, in addition to the classical techniques, entanglement purification and quantum memories, which are both presently not available in a feasible form (see Secs. IV.E and IV.F). Alternatively, one may use a *reverse reconciliation protocol*, which is the method proposed by Grosshans *et al.* (2003). This protocol enables, in principle, security of the scheme used by Grosshans *et al.* (2003) for arbitrarily small line transmission rates. Reverse reconciliation basically means that Alice tries to guess what was received by Bob instead of a protocol in which Bob guesses what was sent by Alice. Another promising method for beating the 3-dB loss limit is based on a postselection procedure (Silberhorn, Ralph, *et al.*, 2002). The implementation of error-correction techniques in this scheme might be less demanding than in the scheme of Grosshans *et al.* (2003). For the signals in the postselection-based scheme of Silberhorn, Ralph, *et al.* (2002), as in the scheme of Grosshans *et al.* (2003), simple coherent states suffice. Note that for the above schemes, although it seems likely that a cloning-based beam-splitting attack would be the optimal attack by Eve, an absolute proof of security would require analyzing more general attacks [including non-Gaussian attacks; see Grosshans and Cerf (2004), where it is shown that for the scheme of Grosshans *et al.* (2003), under certain reasonable assumptions, the individual Gaussian attack is optimal, being superior to any non-Gaussian coherent attack. Note that this analysis excludes the alternative protocol of Silberhorn, Ralph, *et al.* (2002) based on postselection].

3. Absolute theoretical security

From the single-wave-packet noncollective attacks considered above there has been great progress recently for continuous-variable quantum cryptography. A detailed proof of absolute theoretical security for one scheme (Gottesman and Preskill, 2001; Gottesman *et al.*, 2001) stand out. This scheme is the continuous-variable analog of the original BB84 scheme. Following the Shor and Preskill (2000) proof of absolute security for the original qubit proposal, Gottesman and Preskill (2001) have generalized the proof.

[7] Note that this statement no longer holds true when excess noise is present as well (Duan, Giedke, *et al.*, 2000a; Braunstein, Fuchs, *et al.*, 2001). Correspondingly, in the presence of any finite excess noise, a loss limit for secure key distribution does exist for any coherent-state-based continuous-variable scheme (Namiki and Hirano, 2004).

The key theoretical construct is to embed the communication into the context of quantum error-correction codes. These are not actually needed to run the protocol, but greatly simplify the proof. Then given provable bounds to the quantity of information the eavesdropper can have about the key, classical error-correction codes and classical privacy amplification are used to reduce this quantity by any desired amount. This works within some bounds of information captured by the eavesdropper. Further, imperfect resources may be treated as a channel defect (or as an effect of eavesdropping) and so are also easily included.

In the protocol considered, a signal is sent as a squeezed state with either positive or negative squeezing (which corresponds to squeezing around conjugate quadratures). It is proved that if the noise in the quantum channel is weak, squeezed signal states of just 2.51 dB are sufficient in principle to ensure the protocol's security (Gottesman and Preskill, 2001). For nonsqueezing-based coherent-state schemes, such a proof of unconditional security is not yet available (see Grosshans and Cerf, 2004).

Heuristically, it appears that the original rough and ready reasoning of security based on single-shot noncollective attacks really does impart absolute security. This strongly suggests that the protocols discussed previously will be found to be similarly absolutely secure when enhanced or supplemented by classical error correction and privacy amplification.

The remaining issues appear to be as follows:

(1) Reanalysis of this proof in a broadband context. In particular, can the protocol be run in a continuous-wave (cw) manner or do complications occur which necessitate pulsed operation? For example, in cw operation the signal switching limitations must be accounted for in addition to limitations in the detection process. The answers to this would have a sizable impact on the potential bit rates available.

(2) Attempts to use the Shor-Preskill and Gottesman-Preskill approaches to try to complete the proofs of absolute theoretical security for the various schemes considered previously. Detailed criteria could then be established for each protocol. This analysis could be of potential benefit by providing significant flexibility and hence allow for resolution of various implementation-related design tensions.

(3) Experimental verifiability of the claims of absolute security. This last point will be considered now.

4. Verifying experimental security

We have seen that there are already approaches to theoretical proofs for absolute security. Unfortunately, such theoretical proofs must be treated somewhat skeptically. Questions must still be asked about how the theoretical ideas were implemented. Were extra Hilbert-space dimensions written into during the sending or receiving processes by Alice and Bob? It appears that the only acceptable approach to truly resolving this problem is through experimental criteria. One way of thinking about this is in terms of an arms race. We have been hurriedly building the defenses, but have perhaps neglected some subtle loopholes because of unintended mismatches between ideal conceptualization and actual realization. The question remains: can an eavesdropper find a way through our defenses? To find out, it makes most sense to take seriously the position of devil's advocate in the laboratory and work towards serious eavesdropping scenarios in order to put the intended ideally secure schemes through their paces.

To that end a natural first approach for the eavesdropper (in the absence of a full quantum computer) would be to consider an asymmetric cloning strategy, whereby as little or as much information gain versus disturbance could be produced. It should be noted that Ralph (2000a) suggested using teleportation as an eavesdropping strategy. This strategy deserves more consideration, but it unnecessarily limits the eavesdropper to noncollective attacks. By contrast, general cloning strategies should encompass the same performance, but without imposing this restriction.

Cerf *et al.* (2001) have applied optimal asymmetric cloning to the question of eavesdropping on Gaussian channels. For an individual attack based on measuring a random quadrature, the quantum information gain versus disturbance was investigated. They showed that the information gained by the eavesdropper was, in this case, equal to that lost by the receiver. This sort of analysis forms a basis for experimentally implementable verification schemes. The immediate further work here is to convert the quantum circuits into realizable quantum optics hardware. This translation is considered in Sec. V on the cloning of continuous-variable quantum states.

In summary, there is now one theoretically proven secure quantum cryptographic scheme involving quantum continuous variables (Gottesman and Preskill, 2001). It seems likely that those schemes which appear secure based on individual attacks will be shown to be generally secure in a similar manner. If true this would give freedom in the approaches taken to implement any final scheme. Questions still remain about the translation of theoretical protocols into real implementations and whether new loopholes will not be created during this phase.

5. Quantum secret sharing

Quantum secret sharing can be thought of as a multiparty generalization of quantum cryptography in which a message is not only protected against potential eavesdroppers, but can only be retrieved from several people who collaborate. The first quantum secret-sharing scheme was proposed for qubits using GHZ states as an entanglement resource (Hillery *et al.*, 1999). The GHZ states are used to split information in such a way that if one is in possession of all of the subsystems, the information can be recovered, but if one has only some of the subsystems, it cannot. This statement applies both to classical and to quantum information (Hillery *et al.*, 1999). In the former case, a key can be established between all participants, and using the key requires that all participants work together. An eavesdropper would introduce errors and could be detected. In the latter case, for example, a qubit could be recovered after its quantum information had been split into two or more parts (obviously, the former scenario is a multiparty extension of what is known as quantum key distribution).

In the context of continuous variables, the analog of the qubit GHZ state, the maximally entangled N-mode state $\int dx|x,x,\ldots,x\rangle$, is indeed suitable for quantum secret sharing. We know that this state is an eigenstate with total momentum zero and all relative positions $x_i - x_j = 0$ $(i,j=1,2,\ldots,N)$. These correlations may be exploited in a manner similar to the two-mode correlations in entanglement-based quantum cryptography schemes. In fact, their use is equivalent to the two-party sender-receiver scenario when all participants except for the sender team up and share information about local momentum measurements to yield a total "receiver momentum." This would enable one to secretly share classical information protected against eavesdropping. Of course, in a more realistic scenario, the finite squeezing that affects the quantum correlations of the continuous-variable multiparty entangled states [Eq. (137)] must be taken into account.

Continuous-variable secret sharing of quantum information was proposed by Tyc and Sanders (2002). In their scheme, as opposed to the communication scenario considered by Hillery *et al.* (1999), quantum information is to be shared locally and only sufficiently large (but arbitrary) subgroups of all the participants can have access to the secret quantum information. The multimode entangled states used in the scheme of Tyc and Sanders (2002) are also producible with squeezed light and beam splitters. It has already been demonstrated experimentally how a coherent state can be shared using continuous-variable tripartite entanglement, in which any two of three parties can reconstruct the state to some extent, but a single party cannot (Lance *et al.*, 2004).

E. Entanglement distillation

In order to transfer quantum information reliably in the presence of loss, quantum teleportation must be combined with entanglement distillation protocols. The common security proofs for quantum cryptography are based on entanglement distillation as well.

In general, the term *entanglement distillation* refers to any procedure that aims at distilling from a particular number of imperfectly entangled states a smaller number of better entangled states using local operations and classical communication. Commonly, a distinction is made between distillation schemes for purifying mixed entangled states after their two halves have been distributed through noisy channels [*entanglement purification* (Bennett, Brassard, *et al.*, 1996)] and those schemes which concentrate a number of pure nonmaximally entangled states into a smaller number of better entangled pure states [*entanglement concentration* (Bennett, Bernstein, *et al.*, 1996)].

As for the concentration of pure nonmaximally entangled states, there are various approaches (Bennett, Bernstein, *et al.*, 1996; Bose *et al.*, 1999; Nielsen, 1999; Nielsen and Chuang, 2000). For example, entanglement swapping may serve as an entanglement concentration protocol capable of turning two copies of a nonmaximally entangled state into one maximally entangled copy with nonzero probability (Bose *et al.*, 1999). The original proposal of entanglement concentration included the Schmidt projection and the "Procrustean" methods (Bennett, Bernstein, *et al.*, 1996).

The Schmidt projection method requires at least two nonmaximally entangled pairs and becomes efficient for large numbers of pairs. It is based on a collective measurement [of the "Hamming weight" (Kaye and Mosca, 2001)] of all qubits at one side, projecting all pairs onto a subspace spanned by states having a common Schmidt coefficient. The measurement result is then classically communicated to the other side (alternatively, the same collective measurement performed on the other side would yield the same result and make classical communication dispensable). This method also works for dimensions $d>2$ (Bennett, Bernstein, *et al.*, 1996). In the asymptotic limit, turning the total state vector of n nonmaximally entangled input pairs into that of m maximally entangled output pairs can be described via the majorization criterion for deterministic entanglement transformations (Nielsen, 1999; Nielsen and Chuang, 2000). In entanglement concentration, we have $m<n$.

Another method of entanglement concentration is the so-called *Procrustean method*, which represents a filter operation applied to just a single copy of a nonmaximally entangled state (Bennett, Bernstein, *et al.*, 1996). With some nonzero probability (even for higher finite dimensions) a successful filter operation leads to maximum entanglement.

What is known about the distillation of continuous-variable entangled states? As for the concentration of entanglement, we have seen in Sec. IV.A.3 that continuous-variable entanglement swapping based on Gaussian (quadrature) Bell measurements does not lead to an enhancement of the initial entanglement (Parker *et al.*, 2000). In fact, the output entanglement becomes even worse than that of the inputs. As opposed to entanglement swapping with qubits (Bose *et al.*, 1999), there is no probabilistic element in continuous-variable entanglement swapping that might sometimes lead to better and sometimes to worse entanglement. An example of probabilistic entanglement concentration of a single copy of a pure Gaussian two-mode squeezed state into a more highly entangled non-Gaussian (but still infinite-dimensional) state via non-Gaussian operations (subtracting photons) was presented by Opatrný *et al.* (2000).

As for the general distillation of entanglement including purification, a continuous-variable protocol was proposed by Duan, Giedke, *et al.* (2000b) based on local photon number quantum nondemolition measurements. The entanglement of bipartite Gaussian states can be both concentrated and purified using this scheme (Duan, Giedke, *et al.*, 2000b). Its applicability to all bipartite Gaussian states was proven by Giedke, Duan, *et al.* (2001) using the reduction criterion. In the pure-state case, the scheme corresponds to the Schmidt projection method. However, though feasible (Duan, Giedke, *et al.*, 2000c), its experimental realization is very difficult. Moreover, in this scheme, the distilled entangled states end up in a finite-dimensional Hilbert space. Another continuous-variable entanglement concentration protocol based on a cross Kerr interaction was proposed by Fiurášek *et al.* (2003).

How to distill Gaussian entangled states in a feasible way to obtain better Gaussian or continuous-variable entanglement is a very subtle question. Recently it was proven, using Gaussian CPTP maps, that entanglement distillation within the class of Gaussian states cannot be achieved by applying Gaussian operations (which are those particularly feasible, such as beam splitting, homodyne detection, etc., Eisert *et al.*, 2002; Fiurášek, 2002; Giedke and Cirac, 2002). In a continuous-variable distillation scheme, at some stage non-Gaussian states, and hence non-Gaussian operations, must be part of the protocol. A possible approach to this is to apply a first non-Gaussian step, for instance, via a measurement that discriminates between the vacuum state and states containing photons. Subsequently, further Gaussian operations may be used. Through this kind of protocol, proposed by Browne *et al.* (2003) and by Eisert *et al.* (2004), continuous-variable entangled states can be distilled into highly entangled approximately Gaussian states.

F. Quantum memory

A way of storing continuous quantum information is a crucial component of a fully integrated technology. In order to be able to store such information for extended periods, it seems clear that any suitable scheme will require a way of storing it in atomic states. A natural way of achieving this is via the collective spin of an atomic ensemble, as discussed in Sec. II.F. If the ensemble is highly polarized, then small excursions of the collective spin away from some fixed axis will mimic the phase-space structure of a harmonic oscillator. As the size of the ensemble increases, the patch approximating an ideal flat phase space will also increase.

A beam-splitter-like coupling between optical Stokes operators and the collective atomic spin can be achieved for strongly polarized off-resonant coupling. In particular, for light propagating along the z axis, the coupling is well described by the Jaynes-Cummings model. For a sufficiently off-resonant interaction, no population transfer will occur. Thus only second-order transitions can produce any effect, leading to an effective Hamiltonian (Brune *et al.*, 1992)

$$\hat{H}_{\text{eff}} \propto \hat{S}_z \hat{F}_z . \tag{204}$$

It has been noted that this yields a quantum nondemolition probe of $\hat{F}_z$ of the atomic sample (Happer and Mathur, 1967).

In the limit of small interaction times, the equations of motion are

$$\begin{aligned} \hat{F}_x^{(\text{out})} &\simeq \hat{F}_x^{(\text{in})} - a\hat{S}_z^{(\text{in})}\hat{F}_y^{(\text{in})}, \\ \hat{F}_y^{(\text{out})} &\simeq \hat{F}_y^{(\text{in})} + a\hat{S}_z^{(\text{in})}\hat{F}_x^{(\text{in})}, \\ \hat{F}_z^{(\text{out})} &\simeq \hat{F}_z^{(\text{in})}, \end{aligned} \tag{205}$$

and similar equations with $\hat{S}_j$ interchanged with $\hat{F}_j$ throughout. The constant a depends on several parameters, which include, for example, the spontaneous emission rate of the atoms and the transverse cross section and the detuning of the light beam. A beam-splitter-like coupling may be obtained, for example, between $\hat{F}_y$ and $\hat{S}_z$ when the atomic sample is highly polarized along the x axis and for a strongly x-polarized optical beam. By having the beam propagate through the sample along different directions, any suitable beam-splitter coupling between components may be made. This is the basis for a series of beautiful continuous-variable experiments involving spin-squeezed atomic samples (Kuzmich and Polzik, 2003). We shall briefly discuss these experiments in Secs. VII.B and VII.G.

V. QUANTUM CLONING WITH CONTINUOUS VARIABLES

In this section, we investigate the consequences of the famous quantum no-cloning theorem, independently found by Wootters and Zurek (1982) and by Dieks (1982), for continuous quantum variables. As mentioned in Sec. IV.D, a potential application of continuous-variable quantum cloning is to implement eavesdropping strategies for continuous-variable quantum cryptography.

A. Local universal cloning

We now consider the possibility of approximately copying an unknown quantum state at a given location using a particular sequence of unitary transformations (a quantum circuit). Entanglement as a potentially nonlocal resource is therefore not necessarily needed, but it might be an ingredient at the intermediate steps of the cloning circuit.

1. Beyond no-cloning

The no-cloning theorem, originally derived for qubits, in general forbids exact copying of unknown nonorthogonal (or simply arbitrary) quantum states (Dieks, 1982; Wooters and Zurek, 1982). The first papers that went “beyond the no-cloning theorem” and considered the possibility of approximately copying nonorthogonal quantum states initially referred to qubits and later, more generally, to finite-dimensional systems (Bužek and Hillery, 1996; Gisin and Massar, 1997; Bruß, DiVincenzo, *et al.*, 1998; Bruß, Ekert, and Macchiovello, 1998; Werner 1998). Based on these results, a cloning experiment has been proposed for qubits encoded as single-photon states (Simon *et al.*, 2000), and two other optical qubit cloning experiments have already been realized (Martini and Mussi, 2000; Huang *et al.*, 2001).

What about the situation when we have N quantum systems of arbitrary dimension, each prepared in the same but arbitrary input state, and we want to convert them into M ($M>N$) systems that are each in a quantum state as similar as possible to the input state? By using an axiomatic approach,[8] Werner (1998) was able to derive the cloning map that yields the optimal N-to-M cloning fidelities for d-dimensional states,

$$F=\frac{N(d-1)+M(N+1)}{M(N+d)}\equiv F_{\mathrm{clon},N,M}^{\mathrm{univ},d}. \tag{206}$$

For this optimum cloning fidelity, we use the superscript "univ" to indicate that any d-dimensional quantum state is universally copied with the same fidelity. Let us now further investigate universal cloning machines, for both discrete and continuous variables.

2. Universal cloners

A universal cloner is capable of optimally copying arbitrary quantum states with the same fidelity independent of the particular input state. Buzek and Hillery's universal 1-to-2 qubit cloner (Bužek and Hillery, 1996) leads to two identical copies $\hat{\rho}_a$ and $\hat{\rho}_b$. It is a symmetric universal cloner. An asymmetric universal 1-to-2 cloner would distribute the quantum information of the input state unequally among the two output states. The fidelity of one output state is then better than the optimum value for symmetric cloning, whereas the fidelity of the other output state has become worse. Such a potentially asymmetric cloning device represents a quantum information distributor that generates output states of the form (Braunstein, Bužek, and Hillery, 2001)

$$\hat{\rho}_a=(1-A^2)|s\rangle_{aa}\langle s|+\frac{A^2}{d}\mathbb{1}_a,$$

$$\hat{\rho}_b=(1-B^2)|s\rangle_{bb}\langle s|+\frac{B^2}{d}\mathbb{1}_b, \tag{207}$$

for an arbitrary d-dimensional input state $|s\rangle_a=\Sigma_{n=0}^{d-1}c_n|n\rangle_a$. The parameters A and B are related via $A^2+B^2+2AB/d=1$ (Braunstein, Bužek, and Hillery, 2001). The two extreme cases occur when the entire quantum information is kept by the original system ($A=0$) and when it is completely transferred to the other system ($B=0$). It follows directly from the covariant form of the above density operators that the fidelity of the information transfer is input-state independent. The second term proportional to $\mathbb{1}/d$ in each density operator represents noise added by the information transfer process (Braunstein, Bužek, and Hillery, 2001).

It was shown by Braunstein, Bužek, and Hillery (2001) that the above quantum information distributor can be constructed from a single family of quantum circuits. This kind of quantum circuit was previously used as a quantum computational network for universal qubit cloning, in which case it consists of four controlled-NOT gates acting pairwise on the input qubit a and two qubits b and c in an entangled state (Bužek *et al.*, 1997). For arbitrary dimensions, the analogous circuit can be used with controlled-NOT operations generalized to d dimensions, $|n\rangle|m\rangle\rightarrow|n\rangle|n\oplus m\rangle$, and a corresponding d-dimensional entangled state of systems b and c (Braunstein, Bužek, and Hillery, 2001). In a discretized phase space (x_k,p_k) (Bužek *et al.*, 1992, 1995; Opatrný *et al.*, 1995), the entangled state has the form $|\chi\rangle_{bc}=A|x_0\rangle_b|p_0\rangle_c+B(\Sigma_{k=0}^{d-1}|x_k\rangle_b|x_k\rangle_c)/\sqrt{d}$, where $|x_0\rangle$ and $|p_0\rangle$ are zero-position and zero-momentum eigenstates, respectively. The continuous limit for this state is then obvious, and its regularized form consists of quadrature squeezed vacuum states and a two-mode squeezed vacuum state of squeezing r (Braunstein, Bužek, and Hillery, 2001). The parameters A and B are then related as $A^2+B^2+4AB/\sqrt{4+2\sinh^2 2r}=1$ and the controlled-NOT operations become conditional shifts in phase space, $|x\rangle|y\rangle\rightarrow|x\rangle|x+y\rangle$ (Braunstein, 1998a). Expressed in terms of position and momentum operators, the sequence of four generalized controlled-NOT operations[9] acting on modes a (the original), b, and c, can be written as (Cerf *et al.*, 2000; Braunstein, Bužek, and Hillery 2001)

$$\hat{U}_{abc}=\exp[-2i(\hat{x}_c-\hat{x}_b)\hat{p}_a]\exp[-2i\hat{x}_a(\hat{p}_b+\hat{p}_c)]. \tag{208}$$

[8] It is pointed out by Werner (1998) that the "constructive" approach (the coupling of the input system with an apparatus or "ancilla" described by a unitary transformation, and then tracing out the ancilla) consists of completely positive trace-preserving (CPTP) operations. Therefore any constructively derived quantum cloner is in accordance with the axiomatic definition that an admissible cloning machine must be given by a linear CPTP map. Conversely, any linear CPTP map can be constructed via the constructive approach.

[9] Note that the controlled-NOT operation $|n\rangle|m\rangle\rightarrow|n\rangle|n\oplus m\rangle$ is its own inverse only for qubits ($d=2$). For higher dimensions, $\hat{U}_{ab}=\Sigma_{n,m=0}^{d-1}|n\rangle_{aa}\langle n|\otimes|n\oplus m\rangle_{bb}\langle m|$ and $\hat{U}_{ab}^{\dagger}$ differ, describing conditional shifts in opposite directions. The same applies to the continuous-variable controlled-NOT operation $|x\rangle|y\rangle\rightarrow|x\rangle|x+y\rangle$ (Braunstein, 1998a). Therefore there is a slight modification in the sequence of four CNOT's from $d=2$ to $d>2$: $\hat{U}_{ca}\hat{U}_{ba}^{\dagger}\hat{U}_{ac}\hat{U}_{ab}$. Making the CNOT its own inverse $\hat{U}=\hat{U}^{\dagger}$ could be achieved by defining $|x\rangle|y\rangle\rightarrow|x\rangle|x-y\rangle$ (Alber *et al.*, 2000).

Here, $\exp(-2i\hat{x}_k\hat{p}_l)$ corresponds to a single controlled-NOT operation with control mode k and target mode l (l shifted conditioned upon k). After applying $\hat{U}_{abc}$ to mode a and the regularized state of modes b and c, the resulting fidelities of the universal continuous-variable quantum information distributor in the limit of large squeezing turn out to be $F=B^2$ for mode a and $F=A^2$ for mode b. Symmetric cloning with $A=B$ then means $A^2=B^2=1/2$ for infinite squeezing and hence a duplication fidelity of $1/2$ (Braunstein, Bužek, and Hillery 2001).

Similarly, for universal symmetric N-to-M cloning of arbitrary continuous-variable states, one obtains the optimum cloning fidelity (Braunstein, Bužek, and Hillery, 2001)

$$F_{\mathrm{clon},N,M}^{\mathrm{univ},\infty}=\frac{N}{M}, \tag{209}$$

which is exactly the infinite-dimensional limit $d\to\infty$ of Werner's result in Eq. (206). This result looks suspiciously classical. In fact, in the continuous limit, the universal cloner simply reduces to a *classical probability distributor*. For example, the optimum 1-to-2 cloner can be mimicked by a completely classical device that relies on a coin toss. From the two input states of that device, the original input state and an entirely random state (ideally an infinite-temperature thermal state), either state is sent to output a and the other one to output b or vice versa depending on the result of the coin toss. Then, on average, with a small overlap between the original input state and the random state, the two output clones have a cloning fidelity of $1/2$ (Braunstein, Bužek, and Hillery, 2001). These observations are further confirmed by the fact that there is no entanglement between systems a and b at the output of the universal continuous-variable cloner, as opposed to any universal finite-dimensional cloner (Braunstein, Bužek, and Hillery, 2001).

Let us summarize at this point: we have discussed fidelity boundaries for universal N-to-M cloners. These boundaries, the optimal cloning fidelities, can in fact be attained by means of a single family of quantum circuits. There is a universal design for these quantum circuits in any Hilbert-space dimension, and for a given dimension these circuits represent universal cloning machines copying arbitrary input states with the same optimal fidelity. Furthermore, we have seen that the universal continuous-variable cloner is not very interesting, since it is a purely classical device. Does a continuous-variable cloning machine possibly become nonclassical and hence more interesting when it is designed to copy quantum states drawn from a limited alphabet? We now turn to this question.

B. Local cloning of Gaussian states

1. Fidelity bounds for Gaussian cloners

In the first papers that considered continuous-variable cloning, the set of input states to be copied was restricted to Gaussian states (Cerf and Iblisdir, 2000a; Cerf *et al.*, 2000). The optimal cloning fidelity for turning N identical but arbitrary coherent states into M identical approximate copies,

$$F_{\mathrm{clon},N,M}^{\mathrm{coh\ st},\infty}=MN/(MN+M-N), \tag{210}$$

was derived by Cerf and Iblisdir (2000a). The approach of Cerf and Iblisdir was to reduce the optimality problem of the $N\to M$ cloner to the task of finding the optimal $1\to\infty$ cloner, an approach previously applied to universal qubit cloning (Bruß, Ekert, and Macchiavello, 1998). Let us briefly outline the derivation for qubits in order to reveal the analogy with that for coherent states.

The operation of the universal $N\to M$ qubit cloner can be characterized by a shrinking factor $\eta_{\mathrm{clon}}(N,M)$, shrinking the Bloch vector of the original input state (Preskill, 1998),

$$\hat{\rho}_a^{\mathrm{in}}=\frac{1}{2}(\mathbb{1}_a+\vec{s}_a^{\,\mathrm{in}}\cdot\vec{\sigma}), \tag{211}$$

so that the output density operator of each copy becomes (for example, for a)

$$\hat{\rho}_a^{\mathrm{out}}=\frac{1}{2}[\mathbb{1}_a+\eta_{\mathrm{clon}}(N,M)\vec{s}_a^{\,\mathrm{in}}\cdot\vec{\sigma}]. \tag{212}$$

The optimal cloners are those with maximum $\eta_{\mathrm{clon}}(N,M)\equiv\bar{\eta}_{\mathrm{clon}}(N,M)$. The derivation of the fidelity boundaries then relies on two facts: the shrinking factors for concatenated cloners multiply and the optimum cloning shrinking factor for infinitely many copies $\bar{\eta}_{\mathrm{clon}}(N,\infty)$ equals the shrinking factor for the optimal quantum state estimate through measurements $\bar{\eta}_{\mathrm{meas}}(N)$ given N identical input states. This leads to the inequality $\eta_{\mathrm{clon}}(N,M)\eta_{\mathrm{clon}}(M,L)\leqslant\bar{\eta}_{\mathrm{clon}}(N,L)$ and also (with $L\to\infty$) $\eta_{\mathrm{clon}}(N,M)\bar{\eta}_{\mathrm{clon}}(M,\infty)\leqslant\bar{\eta}_{\mathrm{clon}}(N,\infty)$, which gives the lowest upper bound

$$\eta_{\mathrm{clon}}(N,M)\leqslant\frac{\bar{\eta}_{\mathrm{clon}}(N,\infty)}{\bar{\eta}_{\mathrm{clon}}(M,\infty)}=\frac{\bar{\eta}_{\mathrm{meas}}(N)}{\bar{\eta}_{\mathrm{meas}}(M)}. \tag{213}$$

Because the optimal shrinking factor $\bar{\eta}_{\mathrm{meas}}(N)=N/(N+2)$ due to a measurement (Massar and Popescu, 1995), we obtain

$$\bar{\eta}_{\mathrm{clon}}(N,M)=\frac{N}{M}\frac{M+2}{N+2}. \tag{214}$$

This result for qubits yields the correct optimum $N\to M$ cloning fidelity given by Eq. (206) for dimension $d=2$, when inserted into

$$F=\langle\psi_{\theta_0,\phi_0}|\hat{\rho}_{\mathrm{out}}|\psi_{\theta_0,\phi_0}\rangle=\frac{1}{2}+\frac{\bar{\eta}_{\mathrm{clon}}(N,M)}{2}=F_{\mathrm{clon},N,M}^{\mathrm{univ},2}, \tag{215}$$

for arbitrary qubit states (Preskill, 1998)

$$|\psi_{\theta_0,\phi_0}\rangle = \cos\frac{\theta_0}{2}e^{-i\phi_0/2}|0\rangle + \sin\frac{\theta_0}{2}e^{+i\phi_0/2}|1\rangle. \qquad (216)$$

In fact, the resulting fidelities do not depend on the particular values of θ_0 and ϕ_0.

An analogous approach for the derivation of the optimum coherent-state cloning fidelities is based on the fact that the excess noise variances in the quadratures due to the cloning process sum up when an $N \to L$ cloner is described by two cloning machines, an $N \to M$ and an $M \to L$, operating in sequence, $\lambda_{\text{clon}}(N,L) = \lambda_{\text{clon}}(N,M) + \lambda_{\text{clon}}(M,L)$. With the optimum (minimal) excess noise variances defined by $\bar{\lambda}_{\text{clon}}(N,L)$, we now find the largest lower bound,

$$\lambda_{\text{clon}}(N,M) \geqslant \bar{\lambda}_{\text{clon}}(N,\infty) - \bar{\lambda}_{\text{clon}}(M,\infty). \qquad (217)$$

The quantity $\bar{\lambda}_{\text{clon}}(N,\infty)$ can be inferred from quantum estimation theory (Holevo, 1982), because it equals the quadrature variance of an optimal joint measurement of $\hat{x}$ and $\hat{p}$ on N identically prepared systems, $\bar{\lambda}_{\text{clon}}(N,\infty) = \bar{\lambda}_{\text{meas}}(N) = 1/2N$ (Cerf and Iblisdir, 2000a). For instance, the optimal simultaneous measurement of $\hat{x}$ and $\hat{p}$ on a single system $N=1$ yields for each quadrature a variance of $\bar{\lambda}_{\text{meas}}(1) = 1/2 = 1/4 + 1/4$ (Arthurs and Kelly, 1965), corresponding to the intrinsic minimum-uncertainty noise (one unit of vacuum) of the input state plus one extra unit of vacuum due to the simultaneous measurement. Reconstructing a coherent state based on that measurement gives the correct coherent-state input plus two extra units of vacuum [this is exactly the procedure Alice and Bob follow in classical teleportation with an optimal average fidelity of 1/2 for arbitrary coherent states, Eq. (175)]. Since infinitely many copies can be made this way, the optimal measurement can be viewed as a potential $1 \to \infty$ or, in general, an $N \to \infty$ cloner. In fact, analogously to the qubit case (Bruß, Ekert, and Macchiavello, 1998), the optimal measurement (optimal state estimate) turns out to be the optimal $N \to \infty$ cloner, and hence $\bar{\lambda}_{\text{clon}}(N,\infty) = \bar{\lambda}_{\text{meas}}(N) = 1/2N$. This result combined with the inequality of Eq. (217) gives the optimum (minimal) excess noise induced by an $N \to M$ cloning process (Cerf and Iblisdir, 2000a),

$$\bar{\lambda}_{\text{clon}}(N,M) = \frac{M-N}{2MN}. \qquad (218)$$

Inserting this excess noise into Eq. (176) with $g=1$ and a coherent-state input [where $\sigma_x = \sigma_p = 1/2 + \bar{\lambda}_{\text{clon}}(N,M)$] leads to the correct fidelity in Eq. (210). Note that this optimal fidelity does not depend on the particular coherent amplitude of the input states. Any ensemble of N identical coherent states is cloned with the same fidelity. The M output clones are in covariant form. This means the cloning machine can be considered state independent with respect to the limited alphabet of arbitrary coherent states (it treats all coherent states equally well). Of course, this does not hold when the cloner is applied to arbitrary infinite-dimensional states without any restriction to the alphabet. In this sense, the optimal covariant coherent-state cloner is nonuniversal.[10]

When the coherent-state alphabet is extended to squeezed-state inputs, optimality is provided only if the excess cloning noise is squeezed by the same amount as the input state. However, this requires knowledge about the input state's squeezing, making the cloner state dependent when applied to all Gaussian states. Yet Gaussian input states with fixed and known squeezing r, of which the coherent-state alphabet is just the special case $r=0$, are optimally cloned in a covariant fashion.

To summarize, for arbitrary qubits, the optimal cloner shrinks the input state's Bloch vector by a factor $\bar{\eta}_{\text{clon}}(N,M)$ without changing its orientation; the output clones all end up in the same mixed state. For arbitrary coherent states, the optimal (Gaussian) cloner adds an excess noise $\bar{\lambda}_{\text{clon}}(N,M)$ to the input state without changing its mean amplitude; the coherent-state copies are all in the same mixed state. In both cases, this ensures covariance and optimality.

What kind of transformation do we need to achieve optimal coherent-state cloning? In fact, the four-controlled-NOT transformations in Eq. (208) can be used to construct an optimal $1 \to 2$ coherent-state cloner, covariant under displacement and rotation in phase space (Cerf *et al.*, 2000). The entangled state of modes b and c then has to be (in our units; Cerf *et al.*, 2000)

$$|\chi\rangle_{bc} \propto \int dx dy \exp(-x^2 - y^2)|x\rangle|x+y\rangle. \qquad (219)$$

An alternative, non-entanglement-based, optical circuit for the optimal local $N \to M$ (Gaussian) cloning of coherent states will be discussed in the next section.

2. An optical cloning circuit for coherent states

So far, we have only discussed the fidelity boundaries for the $N \to M$ coherent-state cloner. In general, finding an optimal cloning transformation and proving that it achieves the maximum fidelities is a fundamental issue in quantum information theory. In the case of coherent states, implementing an $N \to M$ symmetric cloning transformation that attains Eq. (210) only requires a phase-insensitive linear amplifier and a series of beam splitters (Braunstein, Cerf, *et al.*, 2001; Fiurášek, 2001).

As the simplest example, let us focus on coherent-state duplication ($N=1, M=2$). The coherent state to be cloned is given by the annihilation operator $\hat{a}_0$, and an additional ancilla mode is similarly represented by $\hat{a}_z$. The optimal duplication can be implemented in two steps via two canonical transformations,

[10] The optimal cloning via minimizing excess noise variances, as discussed here, obviously only refers to Gaussian cloners based solely on Gaussian operations. Note that by including non-Gaussian operations, one may indeed exceed the 2/3 fidelity limit for $1 \to 2$ cloning of coherent states and attain the optimum value of approximately 0.6826 (Cerf, 2003; Demkowicz-Dobrzański *et al.*, 2004; Krüger *et al.*, 2004).

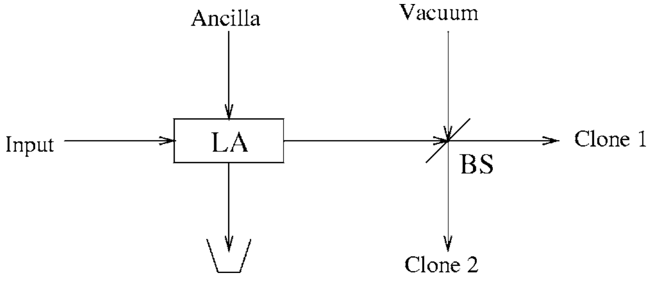

FIG. 6. Implementation of a 1→2 continuous-variable cloning machine. LA stands for linear amplifier, and BS represents a phase-free 50:50 beam splitter.

$$\hat{a}_0' = \sqrt{2}\hat{a}_0 + \hat{a}_z^\dagger, \quad \hat{a}_z' = \hat{a}_0^\dagger + \sqrt{2}\hat{a}_z,$$

$$\hat{a}_0'' = \frac{1}{\sqrt{2}}(\hat{a}_0' + \hat{a}_1), \quad \hat{a}_1'' = \frac{1}{\sqrt{2}}(\hat{a}_0' - \hat{a}_1), \tag{220}$$

where the mode described by $\hat{a}_1$ is another "blank" mode assumed to be in the vacuum state. These transformations preserve the bosonic commutation rules for two clones, modes $0''$ and $1''$.

As shown in Fig. 6, the interpretation of these transformations is straightforward: the first step (which transforms $\hat{a}_0$ and $\hat{a}_z$ into $\hat{a}_0'$ and $\hat{a}_z'$) corresponds to a phase-insensitive amplifier whose (power) gain G is equal to 2, while the second step (which transforms $\hat{a}_0'$ and $\hat{a}_1$ into $\hat{a}_0''$ and $\hat{a}_1''$) is a phase-free 50:50 beam splitter (Cerf and Iblisdir, 2000b; Ralph, 2000c). As discussed by Caves (1982), the ancilla z involved in linear amplification can always be chosen such that $\langle\hat{a}_z\rangle=0$, so that we have $\langle\hat{a}_0''\rangle=\langle\hat{a}_1''\rangle=\langle\hat{a}_0\rangle$ as required. Finally, the optimality of our cloner can be confirmed from known results on linear amplifiers. For an amplifier of (power) gain G, each quadrature's excess noise variance is bounded by (Caves, 1982)

$$\lambda_{LA} \geqslant (G-1)/4. \tag{221}$$

Hence the optimal amplifier of gain $G=2$ yields $\lambda_{LA}=1/4$. This leads to quadrature variances of both clones equal to $1/2$, corresponding to one extra unit of vacuum due to the cloning procedure. This one extra unit is indeed the optimal (minimal) amount according to Eq. (218) for $N=1$ and $M=2$. The corresponding optimal fidelity is $2/3$ [Eq. (210)]. Let us now turn from local cloning of continuous-variable quantum states to cloning at a distance.

C. Telecloning

What about conveying quantum information simultaneously to several receivers via a *multiuser quantum channel*? The no-cloning theorem that generally forbids perfect cloning of unknown nonorthogonal quantum states then also disallows cloning over a distance. This prevents the multiuser quantum channel from being able to produce exact clones of the sender's input state at all receiving stations. It can, however, provide each receiver with at least a part of the input quantum information and distribute *approximate* clones with non-unit fidelity (Bužek and Hillery, 1996). This cloning at a distance or *telecloning* may be seen as the "natural generalization of teleportation to the many-recipient case" (Murao *et al.*, 1999).

For qubits, telecloning has been studied theoretically, first with one input sent to two receivers (Bruß, DiVincenzo, *et al.*, 1998), and more generally, with one input (Murao *et al.*, 1999) and N identical inputs (Dür and Cirac, 2000) distributed among M receivers. The telecloning scenario with one input copy and M receivers has been extended to d-level systems (Murao *et al.*, 2000).

Clearly a telecloner needs entanglement as soon as its fidelity is greater than the maximum fidelity attainable by classical teleportation F_{class}. In fact, for universal $1\to M$ qubit cloning we have $F_{\text{clon},1,M}^{\text{univ},2}>F_{\text{class}}=2/3$ [Eq. (206)], whereas for $1\to M$ cloning of coherent states we have $F_{\text{clon},1,M}^{\text{coh st},\infty}>F_{\text{class}}=1/2$ [Eq. (210); for the bounds on classical teleportation, see Sec. IV.A.2]. Optimal telecloning therefore cannot be achieved by "classical telecloning," i.e., by simply measuring the input state and sending copies of the classical result to all receivers. On the other hand, in the limit $M\to\infty$, both $F_{\text{clon},1,M}^{\text{univ},2}\to F_{\text{class}}=2/3$ and $F_{\text{clon},1,M}^{\text{coh st},\infty}\to F_{\text{class}}=1/2$, which implies that no entanglement is needed for infinitely many copies [this observation reflects the previously discussed relations $\bar{\eta}_{\text{clon}}(N,\infty)=\bar{\eta}_{\text{meas}}(N)$ and $\bar{\lambda}_{\text{clon}}(N,\infty)=\bar{\lambda}_{\text{meas}}(N)$ with $N=1$]. Thus only the optimal telecloning to an infinite number of receivers is achievable via classical telecloning. Otherwise, for a finite number of receivers, entanglement is needed.

The most wasteful scheme would be a protocol in which the sender locally created M optimum clones and perfectly teleported one clone to each receiver using M maximally entangled two-party states (Murao *et al.*, 1999, 2000). A much more economical strategy would be for all participants to share an appropriate multipartite entangled state as a quantum channel. Such states can be found both for discrete variables (Bruß, DiVincenzo, *et al.*, 1998; Murao *et al.*, 1999, 2000; Dür and Cirac, 2000) and for continuous variables (van Loock and Braunstein, 2001b).

The recipe for building such a multiuser quantum channel for continuous variables is as follows (van Loock and Braunstein, 2001b): First, make a bipartite entangled state by combining two squeezed vacua with squeezing parameter r, in which one is squeezed in x and the other in p, at a phase-free 50:50 beam splitter. Then keep one-half (say, mode 1) and send the other half together with $M-1$ vacuum modes through an M splitter, Eq. (132). Mode 1 is now given to the sending station, and the M output modes of the M splitter are distributed among the M receivers. The symmetric $1\to M$ telecloning protocol then works similarly to the $1\to 1$ teleportation protocol. The sender performs a continuous-variable Bell measurement on mode 1 and on the input mode to be transferred and sends the results via classical channels to all receivers. Eventually, each receiver can produce an optimal clone by applying the corresponding phase-space displacements to his mode. For coherent-state inputs, the optimal cloning fidelities $F_{\mathrm{clon},1,M}^{\mathrm{coh\ st},\infty}$, Eq. (210) with $N=1$, are attained by adjusting the squeezing parameter according to

$$e^{-2r} = \frac{\sqrt{M}-1}{\sqrt{M}+1}. \tag{222}$$

Hence the generation of the multiuser quantum channel requires no more than two $|10\log_{10}[(\sqrt{M}-1)/(\sqrt{M}+1)]|$ dB squeezed states and M beam splitters. This is about 7.7 dB for $M=2$, 5.7 dB for $M=3$, 4.8 dB for $M=4$, and 4.2 dB for $M=5$. That the squeezing and hence the entanglement approaches zero as M increases is consistent with the convergence of the optimum cloning fidelity $F_{\mathrm{clon},1,M}^{\mathrm{coh\ st},\infty}=M/(2M-1)$ to $F_{\mathrm{class}}=1/2$. Conversely, for optimal $1\to 1$ quantum teleportation attaining unit fidelity, infinite squeezing is needed.

More generally, using the above multiuser quantum channel with the squeezing parameter given by Eq. (222), arbitrary quantum states can be transferred from a sender to M receivers with equal minimum excess noise in each output state. This can enable one, for instance, to teleport entanglement to all receivers (van Loock and Braunstein, 2001b). Further, the protocol based on the multiuser quantum channel forms a (Gaussian) cloning circuit (an optimal one for coherent states) with no need to amplify the input.

Let us finally emphasize that the continuous-variable telecloning scheme discussed above works without maximum bipartite entanglement (corresponding to the unphysical case of infinite squeezing), whereas the existing discrete-variable schemes rely on maximum two-party entanglement (Murao *et al.*, 1999, 2000; Dür and Cirac, 2000). The only known exception is the $1\to 2$ qubit telecloner of Bruß, DiVincenzo, *et al.* (1998), which uses nonmaximum entanglement.

VI. QUANTUM COMPUTATION WITH CONTINUOUS VARIABLES

We now consider the necessary and sufficient conditions for constructing a universal quantum computer using continuous variables. As an example, it is shown how a universal quantum computer for the amplitudes of the electromagnetic field might be constructed using linear optics, squeezers, and at least one further nonlinear optical element such as the Kerr effect.

A. Universal quantum computation

Ordinarily, a universal quantum computer applies local operations that affect only a few variables at a time (such operations are called *quantum logic gates*): by repeated application of such local operations it can effect any unitary transformation over a finite number of those variables to any desired degree of precision (DiVincenzo, 1995; Lloyd, 1995a).[11]

However, since an arbitrary unitary transformation over even a single continuous variable requires an infinite number of parameters to define, it typically cannot be approximated by any finite number of quantum operations, each of which would be specified by a finite number of parameters. At first sight therefore it might seem that quantum computation over continuous variables would be an ill-defined concept. Despite this difficulty, it is nonetheless possible to define a notion of universal quantum computation over continuous variables for various subclasses of transformations, such as those that correspond to Hamiltonians that are polynomial functions of the operators corresponding to the continuous variables: A set of continuous quantum operations will be termed *universal* for a particular set of transformations if one can by a finite number of applications of the operations approach arbitrarily closely to any transformation in the set.

Consider a single continuous variable corresponding to the dimensionless operator $\hat{x}$, with conjugate variable $\hat{p}$ satisfying $[\hat{x},\hat{p}]=i/2$. We first investigate the problem of constructing Hamiltonians that correspond to arbitrary polynomials of $\hat{x}$ and $\hat{p}$. It is clearly necessary that one be able to apply the Hamiltonians $\pm\hat{x}$ and $\pm\hat{p}$ themselves. In the Heisenberg picture, applying a Hamiltonian $\hat{H}$ gives a time evolution for an operator $\hat{A}$ as $\hat{A}(t)=e^{i\hat{H}t}A(0)e^{-i\hat{H}t}$. Accordingly, applying the Hamiltonian $\hat{x}$ for time t takes $\hat{x}\to\hat{x}$, $\hat{p}\to\hat{p}-t/2$, and applying $\hat{p}$ for time t takes $\hat{x}\to\hat{x}+t/2$, $\hat{p}\to\hat{p}$: the Hamiltonians $\hat{x}$ and $\hat{p}$ have the effect of shifting the conjugate variable by a constant.

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

$$e^{-i\hat{A}\delta t}e^{-i\hat{B}\delta t}e^{i\hat{A}\delta t}e^{i\hat{B}\delta t} = e^{[\hat{A},\hat{B}]\delta t^2} + O(\delta t^3), \tag{223}$$

in the limit $\delta t\to 0$, the result is the same as if one had applied the Hamiltonian $-i[\hat{A},\hat{B}]$ for time δt^2. Similarly, since

$$e^{i\hat{A}\delta t/2}e^{i\hat{B}\delta t/2}e^{i\hat{B}\delta t/2}e^{i\hat{A}\delta t/2} = e^{i(\hat{A}+\hat{B})\delta t} + O(\delta t^3), \tag{224}$$

in the limit $\delta t\to 0$, the result is the same as if one had applied the Hamiltonian $\hat{A}+\hat{B}$ for time δt. In general, then, if one can apply a set of Hamiltonians $\{\pm\hat{H}_i\}$, one can construct any Hamiltonian that is a linear combination of Hamiltonians of the form $\pm i[\hat{H}_i,\hat{H}_j]$, $\pm[\hat{H}_i,[\hat{H}_j,\hat{H}_k]]$, etc. (Deutsch *et al.*, 1995; Lloyd, 1995b;

[11] This definition of quantum computation corresponds to the normal "circuit" definition of quantum computation as in, e.g., Deutsch (1989) and Yao (1995).

Ramakrishna *et al.*, 1995), and no other Hamiltonians. That is, one can construct the Hamiltonians in the algebra generated from the original set by commutation. This result makes it relatively straightforward to determine the set of Hamiltonians that can be constructed from simpler operations.

Now apply this result to the continuous variables introduced above. The application of the boost $\pm\hat{x}$ and translation $\pm\hat{p}$ for short periods of time clearly allows the construction of any Hamiltonian $a\hat{x}+b\hat{p}+c$ that is linear in $\hat{x}$ and $\hat{p}$; this is all that it allows. To construct more complicated Hamiltonians one must also be able to perform operations that are higher-order polynomials in $\hat{x}$ and $\hat{p}$. Suppose now that one can apply the quadratic Hamiltonian

$$\hat{H} = \hat{x}^2 + \hat{p}^2. \tag{225}$$

Application of this Hamiltonian for time t takes

$$\hat{x} \to \cos t\hat{x} - \sin t\hat{p},$$

$$\hat{p} \to \cos t\hat{p} + \sin t\hat{x}. \tag{226}$$

For an electromagnetic field, such an operation corresponds to a simple phase shift. Note that since $e^{i\hat{H}t}$ is periodic with period $1/4\pi$, one can effectively apply $-\hat{H}$ for a time δt by applying $\hat{H}$ for a time $4\pi-\delta t$. The simple commutation relations between $\hat{H}$, $\hat{x}$, and $\hat{p}$ imply that the addition of $\pm\hat{H}$ to the set of operations that can be applied allows the construction of Hamiltonians of the form $a\hat{H}+b\hat{x}+c\hat{p}+d$.

Suppose that in addition to translations and phase shifts one can apply the quadratic Hamiltonian $\pm\hat{S}$ with

$$\hat{S} = \hat{x}\hat{p} + \hat{p}\hat{x}. \tag{227}$$

Applying the Hamiltonian $\hat{S}$ takes

$$\hat{x} \to e^{t}\hat{x},$$

$$\hat{p} \to e^{-t}\hat{p}. \tag{228}$$

Colloquially, $\hat{S}$ stretches $\hat{x}$ and squeezes $\hat{p}$ by some amount. In the case of the electromagnetic field, $\hat{S}$ corresponds to a squeezer operating in the parametric approximation. It is easily verified that

$$[\hat{H},\hat{S}] = 2i(\hat{x}^2 - \hat{p}^2). \tag{229}$$

Looking at the algebra generated from $\hat{x}$, $\hat{p}$, $\hat{H}$, and $\hat{S}$ by commutation, one sees that translations, phase shifts, and squeezers allow the construction of any Hamiltonian that is quadratic in $\hat{x}$ and $\hat{p}$, and of no Hamiltonian of higher order.

To construct higher-order Hamiltonians, nonlinear operations are required. One such operation is the Kerr Hamiltonian

$$\hat{H}^2 = (\hat{x}^2 + \hat{p}^2)^2, \tag{230}$$

corresponding to a $\chi^{(3)}$ process in nonlinear optics. This higher-order Hamiltonian has the key feature of typically increasing its order when it is commuted with a polynomial in $\hat{x}$ and $\hat{p}$. By evaluating a few commutators, e.g.,

$$[\hat{H}^2,\hat{x}] = -2i(\hat{x}^2\hat{p} + \hat{p}^3) + \text{lower-order terms},$$

$$[\hat{H}^2,\hat{p}] = 2i(\hat{x}\hat{p}^2 + \hat{x}^3) + \text{lower-order terms},$$

$$[\hat{x},[\hat{H}^2,\hat{S}]] = -8\hat{p}^3 + \text{lower-order terms},$$

$$[\hat{p},[\hat{H}^2,\hat{S}]] = 8\hat{x}^3 + \text{lower-order terms}, \tag{231}$$

one sees that the algebra generated by $\hat{x}$, $\hat{p}$, $\hat{H}$, $\hat{S}$, and $\hat{H}^2$ by commutation includes all third-order polynomials in $\hat{x}$ and $\hat{p}$. A simple inductive proof now shows that one can construct Hamiltonians that are arbitrary Hermitian polynomials in any order of $\hat{x}$ and $\hat{p}$. Suppose that one can construct a polynomial of order M consisting of any specific term

$$\hat{x}^{M-n}\hat{p}^{n}, \quad n \leq M. \tag{232}$$

Since we may already create any quadratic Hermitian Hamiltonian and since

$$[\hat{x}^2,\hat{x}^{M-n}\hat{p}^{n}] = \frac{ni}{2}\hat{x}^{M-(n-1)}\hat{p}^{(n-1)} + \text{lower-order terms},$$

$$[\hat{p}^2,\hat{x}^{M-n}\hat{p}^{n}] = \frac{-(M-n)i}{2}\hat{x}^{M-(n+1)}\hat{p}^{(n+1)} + \text{lower-order terms}, \tag{233}$$

then it is easy to see that we may create *all* polynomials of order M. Further, since we may create the Hamiltonians $\hat{x}^3$ or $\hat{p}^3$ and since

$$[\hat{x}^3,\hat{x}^{n}\hat{p}^{m}] = \frac{3mi}{2}\hat{x}^{n+2}\hat{p}^{m-1} + \text{lower-order terms},$$

$$[\hat{x}^3,\hat{x}^{n}\hat{p}^{m}] = \frac{-3ni}{2}\hat{x}^{n-1}\hat{p}^{m+2} + \text{lower-order terms}, \tag{234}$$

we can by judicious commutation of $\hat{x}^3$ and $\hat{p}^3$ with monomials of order M construct any monomial of order $M+1$. Since any polynomial of order $M+1$ can be constructed from monomials of order $M+1$ and lower, by applying linear operations and a single nonlinear operation a finite number of times one can construct polynomials of arbitrary order in $\hat{x}$ and $\hat{p}$ to any desired degree of accuracy. Comparison with similar results for the discrete case (Lloyd, 1996) shows that the number of operations required grows as a small polynomial in the order of the polynomial to be created, the accuracy to which that polynomial is to be enacted, and the time over which it is to be applied.

The use of the Kerr Hamiltonian $\hat{H}^2$ was not essential: any higher-order Hamiltonian would be satisfactory. Note that commutation of a polynomial in $\hat{x}$ and $\hat{p}$ with $\hat{x}$ and $\hat{p}$ themselves (which have order 1) always reduces the order of the polynomial by at least 1. Commutation with $\hat{H}$ and $\hat{S}$ (which have order 2) never increases the order, and commutation with a polynomial of order 3 or higher typically increases the order by at least 1. Judicious commutation of $\hat{x}$, $\hat{p}$, $\hat{H}$, and $\hat{S}$ with an applied Hamiltonian of order 3 or higher therefore allows the construction of arbitrary Hermitian polynomials of any order in $\hat{x}$ and $\hat{p}$. Alternatively, it has recently been proposed that a measurement-induced nonlinearity (using ideal photodetection) could be used in an optical scheme without the need for nonlinear materials (Gottesman *et al.*, 2001; Bartlett and Sanders, 2002). The physical realization of such nonlinearities is an important quest for quantum information theory over continuous variables.

The above set of results shows that simple linear operations, together with a single nonlinear operation, allow one to construct arbitrary polynomial Hamiltonian transformations of a single quantum variable. Let us now turn to more than one variable, e.g., the case of an interferometer in which many modes of the electromagnetic field interact. Suppose now that there are many variables, $\{\hat{x}_i,\hat{p}_i\}$, on each of which the simple single-variable operations described above can be performed. Now let the variables interact with each other. For simplicity, we assume that we can apply interaction Hamiltonians $\pm\hat{B}_{ij}$ with $\hat{B}_{ij}=(\hat{p}_i\hat{x}_j-\hat{x}_i\hat{p}_j)$: a more complicated interaction Hamiltonian can always be used to generate interactions of this form by combining it with single-variable operations. This operation has the effect of taking

$$\begin{aligned}\hat{A}_i &\to \cos t\hat{A}_i+\sin t\hat{A}_j,\\ \hat{A}_j &\to \cos t\hat{A}_j-\sin t\hat{A}_i,\end{aligned}\qquad(235)$$

where $\hat{A}_i=\{\hat{x}_i,\hat{p}_i\}$ and $\hat{A}_j=\{\hat{x}_j,\hat{p}_j\}$. For the electromagnetic field, $\hat{B}_{ij}$ functions as a beam splitter, linearly mixing together the two modes i and j. By repeatedly taking commutators of $\hat{B}_{ij}$ with polynomials in $\hat{x}_i$ and $\hat{p}_i$, for different i, it can be easily seen by the same algebraic arguments as above that it is possible to build up arbitrary Hermitian polynomials in $\{\hat{x}_i,\hat{p}_i\}$.

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

In analogy with information over classical continuous variables, which is measured in units of *nats* (1 nat $=\log_2 e$ bits), the unit of continuous quantum information will be called the *qunat*. Two continuous variables in the pure state $|\psi\rangle_{12}$ possess $-\mathrm{Tr}\,\hat{\rho}_1\ln\hat{\rho}_1$ qunats of entanglement, where $\hat{\rho}_1=\mathrm{Tr}_2|\psi\rangle_{12}\langle\psi|$. For two squeezed vacua (squeezed by an amount e^{-r}) entangled using a beam splitter, the entropy so computed from the approximate EPR state is given by

$$S(\hat{\rho})=(1+\bar{n})\ln(1+\bar{n})-\bar{n}\ln\bar{n}\ \text{qunats},\qquad(236)$$

with $\bar{n}=e^r\sinh r$. For example, $e^{2r}=10$ gives 10 dB of squeezing in power, corresponding to $r=1.151$. According to Eq. (236), two continuous variables entangled using a 10-dB squeezer then possess 2.607 qunats of shared, continuous quantum information, equivalent to 3.762 qubits of discrete quantum information. This is comparable to the degree of entanglement currently available using ion-trap quantum computers.

Quantum computation over continuous variables can be thought of as the systematic creation and manipulation of qunats. Universal quantum computation for polynomial transformations of continuous variables effectively allows one to perform quantum floating-point manipulations on those variables. For example, it is clearly possible using linear operations alone to take the inputs $\hat{x}_1$, $\hat{x}_2$ and to map them to $\hat{x}_1$, $a\hat{x}_1+b\hat{x}_2+c$. Similarly, application of the three-variable Hamiltonian $2\hat{x}_1\hat{x}_2\hat{p}_3$ takes

$$\begin{aligned}\hat{x}_1 &\to \hat{x}_1,\\ \hat{x}_2 &\to \hat{x}_2,\\ \hat{x}_3 &\to \hat{x}_3+\hat{x}_1\hat{x}_2t,\end{aligned}\qquad(237)$$

that is, this operation allows one to multiply $\hat{x}_1$ and $\hat{x}_2$ and place the result in the "register" $\hat{x}_3$. A wide variety of quantum floating-point operations are possible.

The ability to create and manipulate qunats depends crucially on the strength of squeezing and of the nonlinearities that one can apply. Currently 10-dB squeezers (6 dB after attenuation in the measurement apparatus) exist (Wu *et al.*, 1986). High-Q cavity quantum electrodynamics can supply a strong Kerr effect in a relatively lossless context, and quantum logic gates constructed for qubits could be used to provide the nonlinearity for continuous quantum variables as well (Turchette *et al.*, 1995). Here the fact that only single-mode nonlinearities are required for universal quantum computation simplifies the problem of effecting continuous quantum logic. Nonetheless, the difficulty of performing repeated nonlinear operations in a coherent and loss-free manner is likely to limit the possibilities for quantum computation over the amplitudes of the electromagnetic field. Vibrational modes of ions in traps or excitations of a Bose-Einstein condensate might provide the long-lived, lossless states required for quantum computation over continuous variables.

B. Extension of the Gottesman-Knill theorem

Quantum mechanics allows for information processing that could not be performed classically. In particular, it may be possible to perform an algorithm efficiently on a quantum computer that cannot be performed efficiently on a classical one. The Gottesman-Knill theorem (Gottesman, 1999) for discrete-variable (qubit) quantum information provides a valuable tool for assessing the classical complexity of a given process. Essentially, it states that any quantum algorithm that starts in the computational basis and employs only a restricted class of gates (Hadamard, phase, controlled-NOT, and Pauli gates), along with projective measurements in the computational basis, can be efficiently simulated on a classical computer (Nielsen and Chuang, 2000). The Gottesman-Knill theorem reveals that a large class of quantum algorithms do not provide a speedup over classical processes.

Here we develop the continuous-variable extension to the Gottesman-Knill theorem. This result helps us understand what algorithms performed by a continuous-variable quantum computer may be efficiently simulated by a conventional classical computer. By contrast, it is exactly the algorithms for which such an efficient simulation is impossible which are the major subject of attention of quantum computation.

We note that the issue of efficient classical simulation of a continuous-variable process is more involved than for the discrete case. Continuous-variable quantum states will typically only be defined for some limited precision. For example, the states used in continuous-variable experiments are approximations to the idealized computational basis. These basis states are infinitely squeezed states, whereas any experimental implementation will involve only finitely squeezed states (Lloyd and Braunstein, 1999). Furthermore, measurements are part of the quantum computation and, even in the computational basis, are subject to experimental constraints (such as detection efficiency). A good classical simulation must be robust against such imperfections.

Despite these complications, we shall present a set of sufficient conditions for a continuous-variable quantum information process to ensure that it can be efficiently simulated classically. To prove this theorem, we employ the techniques of stabilizers (Nielsen and Chuang, 2000) that are used for qubits. Using this formalism, it is possible to simulate a quantum algorithm by following the evolution of the set of stabilizers, rather than the evolution of quantum states. For a nontrivial set of algorithms, this procedure requires only a short description at each step and so may be simulated efficiently without recourse to the exponential overhead of explicitly recording all terms of a quantum superposition (which even for a single continuous variable could require an infinite number of terms). For continuous-variable processes the stabilizer formalism is particularly simple when expressed in terms of their generators.

We first must identify the continuous-variable analog to the qubit computational basis. Here we take it to be the set of position eigenstates $|x\rangle$ (Braunstein, 1998a, 1998b; Lloyd and Braunstein, 1999). Next, given this choice we must identify the continuous-variable analogs to each of the operations that are considered in the qubit version of the Gottesman-Knill theorem. For qubits the so-called Pauli gates perform bit flips, phase flips, or a combination of the two. For continuous-variable states, the natural analog would be to perform position translations, momentum kicks, or combinations thereof. Thus, for a single continuous-variable, the Pauli operator analogs are

$$\hat{X}(x) \equiv e^{-2ix\hat{p}}, \quad \hat{Z}(p) \equiv e^{2ip\hat{x}}, \tag{238}$$

for x, p both real. These operators are noncommutative, obeying

$$\hat{X}(x)\hat{Z}(p) = e^{-2ixp}\hat{Z}(p)\hat{X}(x). \tag{239}$$

On the computational basis these operators act as

$$\hat{X}(x')|x\rangle = |x+x'\rangle, \quad \hat{Z}(p)|x\rangle = e^{2ipx}|x\rangle. \tag{240}$$

We define the SUM gate as the continuous-variable analog of the controlled-NOT gate. It provides the basic interaction gate for a pair of continuous-variable systems i and j via

$$\widehat{\mathrm{SUM}}_{ij} \equiv e^{-2i\hat{x}_i \otimes \hat{p}_j}. \tag{241}$$

Referring to Eq. (238) the action of this gate on the Pauli operators is given by

$$\begin{aligned}\widehat{\mathrm{SUM}}_{ij}: \quad & \hat{X}_i(x) \otimes \hat{\mathbb{1}}_j \to \hat{X}_i(x) \otimes \hat{X}_j(x),\\ & \hat{Z}_i(p) \otimes \hat{\mathbb{1}}_j \to \hat{Z}_i(p) \otimes \hat{\mathbb{1}}_j,\\ & \hat{\mathbb{1}}_i \otimes \hat{X}_j(x) \to \hat{\mathbb{1}}_i \otimes \hat{X}_j(x),\\ & \hat{\mathbb{1}}_i \otimes \hat{Z}_j(p) \to \hat{Z}_i(p)^{-1} \otimes \hat{Z}_j(p).\end{aligned} \tag{242}$$

This gate describes the unitary transformation used in a backaction-evading or quantum nondemolition process.

The Fourier transform $\hat{\mathcal{F}}$ is the continuous-variable analog of the Hadamard transformation [Eq. (131)]. It can also be defined as

$$\hat{\mathcal{F}} \equiv e^{i\pi(\hat{x}^2+\hat{p}^2)/2}, \tag{243}$$

and its action on the Pauli operators is

$$\begin{aligned}\hat{\mathcal{F}}: \quad & \hat{X}(x) \to \hat{Z}(x),\\ & \hat{Z}(p) \to \hat{X}(p)^{-1}.\end{aligned} \tag{244}$$

The "phase gate" $\hat{P}(\eta)$ is a squeezing operation for continuous-variables, defined by

$$\hat{P}(\eta) \equiv e^{i\eta\hat{x}^2}, \tag{245}$$

and its action on the Pauli operators is given by

$$\hat{P}(\eta): \quad \hat{X}(x) \to e^{i\eta x^2}\hat{X}(x)\hat{Z}(\eta x), \qquad \hat{Z}(p) \to \hat{Z}(p), \tag{246}$$

which is analogous to that of the discrete-variable phase gate $\hat{\mathcal{P}}$ (Gottesman *et al.*, 2001).

For the continuous-variable operators defined above, SUM, $\hat{\mathcal{F}}$, $\hat{P}(\eta)$, $\hat{X}(x)$, and $\hat{Z}(p)$ are sufficient to simulate all possible quadratic Hermitian Hamiltonians, as we saw in the last section.

We now have the necessary components to prove our main result. We employ the stabilizer formalism used for discrete variables and follow the evolution of generators of these stabilizers rather than the states. To start with, let us consider the ideal case of a system with an initial state in the computational basis of the form $|x_1,x_2,\ldots,x_n\rangle$. This state may be fully characterized by the eigenvalues of the generators of n Pauli operators $\{\hat{x}_1,\hat{x}_2,\ldots,\hat{x}_n\}$. Any continuous-variable process or algorithm can then be modeled by following the evolution of the generators of these n Pauli operators, rather than by following the evolution of the states in the infinite-dimensional Hilbert space $\mathcal{L}^2(\mathbb{R}^n)$. If we restrict ourselves to the gate operations SUM, $\hat{\mathcal{F}}$, $\hat{P}(\eta)$, $\hat{X}(x)$, and $\hat{Z}(p)$ our job is straightforward, since each of the stabilizers evolves only to a simple tensor product of Pauli operators. In other words, these operations map linear combinations of Pauli operator generators to linear combinations of Pauli operator generators (each $\hat{x}_i$ and $\hat{p}_i$ is mapped to sums of $\hat{x}_j$, $\hat{p}_j$, $j=1,\ldots,n$, in the Heisenberg picture). For each of the n generators describing the initial state, one must keep track of $2n$ real coefficients describing this linear combination. To simulate such a system, then, requires following the evolution of $2n^2$ real numbers.

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

Measurement in the computational basis plus feedforward during the computation may also be easily simulated for a sufficiently restricted class of feedforward operations; in particular, operations corresponding to feedforward displacement (not rotation or squeezing, though this restriction will be dropped below) by an amount proportional to the measurement result. Such feedforward operations may be simulated by the Hamiltonian that generates the SUM gate with measurement in the computational basis delayed until the end of the computation. In other words, feedforward from measurement can be treated by employing conditional unitary operations with delayed measurement (Nielsen and Chuang, 2000), thus reducing feedforward to the case already treated.

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

$$\hat{S}_1(r_1) \otimes \hat{S}_2(r_2) \otimes \cdots \otimes \hat{S}_n(r_n)|0,0,\ldots,0\rangle, \tag{247}$$

where $|0\rangle$ is a vacuum state and $\hat{S}(r)$, with $r \in \mathbb{R}$, is the squeezing operation. Now the vacuum states may also be described by stabilizers generated by $\{\hat{x}_1+i\hat{p}_1,\hat{x}_2+i\hat{p}_2,\ldots,\hat{x}_n+i\hat{p}_n\}$, which are now complex linear combinations of the earlier generators. Although these generators are non-Hermitian, the operators obtained by their exponentiation do indeed behave as stabilizers. Combining the initial squeezing operators into the computation, a classical simulation of a gate array consisting of operations from the set SUM, $\hat{\mathcal{F}}$, $\hat{P}(\eta)$, $\hat{X}(x)$, and $\hat{Z}(p)$ requires following the evolution of $4n^2$ numbers (twice that of infinitely squeezed inputs due to the real and imaginary parts). Measurements in the computational basis are again easily simulated in terms of this Heisenberg evolution, by treating each of the x_i and p_i as random numbers independently sampled from a Gaussian distribution with widths described by the vacuum state. Simulation of measurement plus feedforward follows exactly the same prescription as before.

Furthermore, the condition for ideal measurements can be relaxed. Finite-efficiency detection can be modeled by a linear-loss mechanism (Yuen and Shapiro, 1980). Such a mechanism may be described by quadratic Hamiltonians and hence simulated by quadratic Hamiltonians and hence the allowed gate elements. Note that these allowed gate elements are precisely those that preserve Gaussian states; i.e., they transform Gaussians to Gaussians; this observation allows us to remove our earlier restriction on feedforward gates and allow for classical feedforward of any allowed gate operation. Note that non-Gaussian components to the states cannot be modeled in this manner.

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

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

Thus algorithms that produce entanglement between systems may still satisfy the conditions of the Gottesman-Knill theorem and thus may be simulated efficiently on a classical computer; included are those used for continuous-variable quantum teleportation (Braunstein and Kimble, 1998a; Furusawa *et al.*, 1998), quantum cryptography (Hillery, 2000; Ralph, 2000a; Reid, 2000; Gottesman and Preskill, 2001), and error correction (Braunstein, 1998a, 1998b). Although these processes are fundamentally quantum in nature and involve entanglement between systems, the extended Gottesman-Knill theorem demonstrates that they do not provide any speedup over a classical simulation. This theorem therefore provides a valuable tool in assessing the classical complexity of simulating these quantum processes.

As shown in the previous section, in order to generate all unitary transformations given by an arbitrary polynomial Hermitian Hamiltonian (as is necessary to perform universal continuous-variable quantum computation), one must include a gate described by a Hamiltonian other than an inhomogeneous quadratic one in the canonical operators, such as a cubic or higher-order polynomial. Transformations generated by these Hamiltonians do not preserve the linear structure of the generators of the stabilizers and thus cannot be described efficiently by the stabilizer formalism. These nonlinear transformations can be used in continuous-variable algorithms and may provide a significant speedup over any classical process.

VII. EXPERIMENTS WITH CONTINUOUS QUANTUM VARIABLES

In this section, we discuss some experiments based on continuous quantum variables. These include the generation of squeezed-state EPR entanglement via optical parametric amplification and via the Kerr effect. Qualitatively different manifestations of continuous-variable entanglement are that between two atomic ensembles, created in an experiment in Copenhagen (Julsgaard *et al.*, 2001), and that between more than two optical modes, experimentally generated and verified in Tokyo for three modes (Aoki *et al.*, 2003). Quantum teleportation of coherent states has been achieved already in Pasadena (Furusawa *et al.*, 1998; Zhang *et al.*, 2003) and in Canberra (Bowen, Treps, *et al.*, 2003). We shall briefly show how to describe these experiments in a realistic broadband fashion. Further important continuous-variable experiments include the dense-coding experiment of Li *et al.* utilizing bright EPR beams (Li, Pan, *et al.*, 2002), the coherent-state-based quantum key distribution experiment by Grangier and his group (Grosshans *et al.*, 2003), and the demonstration of a quantum memory effect by the Polzik group (Schori *et al.*, 2002).

A. Generation of squeezed-state EPR entanglement

The generation of discrete-variable qubit entanglement can be achieved experimentally via weak down conversion producing polarization-entangled single photons. The resulting maximum entanglement is then "polluted" by a large vacuum contribution (Braunstein and Kimble, 1998b). The consequence of this is that entanglement never emerges from these optical devices in an event-ready fashion. Since successful (postselected) events occur very rarely, one has to cope with very low efficiency in these single-photon schemes. However, there are also some advantages of the single-photon-based approaches to entanglement generation and quantum communication, as we discussed in Sec. I. Great progress has been made in generating single-photon entanglement, for the cases of both two qubits (Bouwmeester *et al.*, 1997) and three qubits (Bouwmeester *et al.*, 1999).

In the continuous-variable setting, the generation of entanglement, for instance, occurring every inverse bandwidth time at the output of an optical parametric amplifier, is more efficient than in the single-photon schemes. When making an entangled two-mode squeezed state, one need not exclude the vacuum contribution that originates from the down-conversion source via postselection. It is still contained in the resulting nonmaximally entangled output state, as expressed by Eq. (85) in an idealized discrete-mode description. We shall now discuss a more realistic description of the resulting broadband entangled state that emerges from an optical parametric amplifier. This type of quadrature entanglement was used in recent continuous-variable quantum communication experiments (Furusawa *et al.*, 1998; Li, Pan, *et al.*, 2002; Bowen, Treps, *et al.*, 2003; Zhang *et al.*, 2003). The first experiment to produce continuous-variable broadband EPR correlations of this kind was performed by Ou *et al.* (1992a, 1992b). Recently, this "conventional" quadrature entanglement was also transformed into continuous-variable polarization entanglement exhibiting correlations in the Stokes operators of two beams (Bowen *et al.*, 2002). Another recent scheme to create continuous-variable broadband entanglement was based on a different nonlinear optical interaction, namely, the Kerr effect in an optical fiber (Silberhorn *et al.*, 2001).

1. Broadband entanglement via optical parametric amplification

A broadband entangled state is generated either directly by *nondegenerate optical parametric amplification* in a cavity (also called *nondegenerate parametric down conversion*) or by combining at a beam splitter two independently squeezed fields produced via degenerate down conversion. This observation is the broadband extension of the fact that a two-mode squeezed state is equivalent to two single-mode squeezed states combined at a 50:50 beam splitter. Just as for the two discrete modes in Eqs. (88) and (89), this can be easily seen in the "continuum" representation (Caves and Schumaker, 1985) of the quadrature operators,

$$\hat{x}(\Omega) = \frac{1}{2}\left[\sqrt{1+\frac{\Omega}{\omega_0}}\hat{b}(\omega_0+\Omega) + \sqrt{1-\frac{\Omega}{\omega_0}}\hat{b}^\dagger(\omega_0-\Omega)\right],$$

$$\hat{p}(\Omega) = \frac{1}{2i}\left[\sqrt{1+\frac{\Omega}{\omega_0}}\hat{b}(\omega_0+\Omega) - \sqrt{1-\frac{\Omega}{\omega_0}}\hat{b}^\dagger(\omega_0-\Omega)\right], \quad (248)$$

where ω_0 is the optical central frequency and $\Omega > 0$ some small modulation frequency. Here, the annihilation and creation operators (now no longer dimensionless, but each in units of root time, $\sqrt{t}$) satisfy the commutation relation $[\hat{b}(\omega),\hat{b}^\dagger(\omega')] = \delta(\omega-\omega')$. The commutators for the quadratures are (Caves and Schumaker, 1985)

$$[\hat{x}(\Omega),\hat{x}(\Omega')] = [\hat{x}(\Omega),\hat{p}(\Omega')] = [\hat{p}(\Omega),\hat{p}(\Omega')] = 0,$$

$$[\hat{x}(\Omega),\hat{x}^\dagger(\Omega')] = [\hat{p}(\Omega),\hat{p}^\dagger(\Omega')] = \frac{\Omega}{2\omega_0}\delta(\Omega-\Omega'),$$

$$[\hat{x}(\Omega),\hat{p}^\dagger(\Omega')] = [\hat{x}^\dagger(\Omega),\hat{p}(\Omega')] = \frac{i}{2}\delta(\Omega-\Omega'). \quad (249)$$

This is a suitable formalism for analyzing two-photon devices such as the parametric amplifier. As a result of the nonlinear optical interaction, a pump photon at frequency $2\omega_0$ can be annihilated to create two photons at the frequencies $\omega_0 \pm \Omega$ and, conversely, two photons can be annihilated to create a pump photon. Thus the light produced by the amplifier always consists of pairs of modes at frequencies $\omega_0 \pm \Omega$.

Now it is convenient to define upper-case operators in the rotating frame about the optical central frequency ω_0 (for the nondegenerate parametric amplification, half the pump frequency),

$$\hat{B}(t) = \hat{b}(t)e^{i\omega_0 t}. \quad (250)$$

Using the Fourier transform

$$\hat{B}(\Omega) = \frac{1}{\sqrt{2\pi}}\int dt\hat{B}(t)e^{i\Omega t}, \quad (251)$$

the fields may then be described as functions of the modulation frequency Ω with the commutation relation

$$[\hat{B}(\Omega),\hat{B}^\dagger(\Omega')] = \delta(\Omega-\Omega'). \quad (252)$$

In the rotating frame, using $\hat{b}(\omega_0\pm\Omega) = \hat{B}(\pm\Omega)$ and the approximation $\Omega \ll \omega_0$, the frequency-resolved "broadband" quadrature amplitudes of Eq. (248) for a mode k (for instance, a spatial or a polarization mode) may be written in a form more reminiscent of the discrete quadratures in Eq. (11) as (Ou *et al.*, 1992a)

$$\hat{X}_k(\Omega) = \frac{1}{2}[\hat{B}_k(\Omega) + \hat{B}_k^\dagger(-\Omega)],$$

$$\hat{P}_k(\Omega) = \frac{1}{2i}[\hat{B}_k(\Omega) - \hat{B}_k^\dagger(-\Omega)], \quad (253)$$

with the broadband annihilation operators $\hat{B}_k(\Omega)$. The only nontrivial commutation relations for the non-Hermitian quadratures are now

$$[\hat{X}(\Omega),\hat{P}^\dagger(\Omega')] = [\hat{X}^\dagger(\Omega),\hat{P}(\Omega')] = \frac{i}{2}\delta(\Omega-\Omega'). \quad (254)$$

The actually measurable quantities are the Hermitian real and imaginary parts of these quadratures, satisfying the usual commutation relations

$$[\mathrm{Re}\,\hat{X}(\Omega),\mathrm{Re}\,\hat{P}(\Omega')] = [\mathrm{Im}\,\hat{X}(\Omega),\mathrm{Im}\,\hat{P}(\Omega')] = \frac{i}{4}\delta(\Omega-\Omega'). \quad (255)$$

Using the quadrature squeezing spectra,

$$\langle\Delta\hat{X}_1^\dagger(\Omega)\Delta\hat{X}_1(\Omega')\rangle = \langle\Delta\hat{P}_2^\dagger(\Omega)\Delta\hat{P}_2(\Omega')\rangle = \delta(\Omega-\Omega')|S_+(\Omega)|^2/4,$$

$$\langle\Delta\hat{X}_2^\dagger(\Omega)\Delta\hat{X}_2(\Omega')\rangle = \langle\Delta\hat{P}_1^\dagger(\Omega)\Delta\hat{P}_1(\Omega')\rangle = \delta(\Omega-\Omega')|S_-(\Omega)|^2/4, \quad (256)$$

one can describe two independently squeezed fields coming from two degenerate optical parametric oscillators as

$$\hat{X}_1(\Omega) = S_+(\Omega)\hat{X}_1^{(0)}(\Omega), \quad \hat{P}_1(\Omega) = S_-(\Omega)\hat{P}_1^{(0)}(\Omega),$$

$$\hat{X}_2(\Omega) = S_-(\Omega)\hat{X}_2^{(0)}(\Omega), \quad \hat{P}_2(\Omega) = S_+(\Omega)\hat{P}_2^{(0)}(\Omega), \quad (257)$$

where $|S_-(\Omega)| < 1$ refers to quiet quadratures and $|S_+(\Omega)| > 1$ to noisy ones, and the superscript (0) denotes vacuum modes. These fields can be used as a broadband EPR source when they are combined at a beam splitter (van Loock *et al.*, 2000):

$$\hat{X}_1'(\Omega) = \frac{1}{\sqrt{2}}S_+(\Omega)\hat{X}_1^{(0)}(\Omega) + \frac{1}{\sqrt{2}}S_-(\Omega)\hat{X}_2^{(0)}(\Omega),$$

$$\hat{P}_1'(\Omega) = \frac{1}{\sqrt{2}}S_-(\Omega)\hat{P}_1^{(0)}(\Omega) + \frac{1}{\sqrt{2}}S_+(\Omega)\hat{P}_2^{(0)}(\Omega),$$

$$\hat{X}_2'(\Omega) = \frac{1}{\sqrt{2}}S_+(\Omega)\hat{X}_1^{(0)}(\Omega) - \frac{1}{\sqrt{2}}S_-(\Omega)\hat{X}_2^{(0)}(\Omega),$$

$$\hat{P}_2'(\Omega) = \frac{1}{\sqrt{2}}S_-(\Omega)\hat{P}_1^{(0)}(\Omega) - \frac{1}{\sqrt{2}}S_+(\Omega)\hat{P}_2^{(0)}(\Omega). \quad (258)$$

In this state, the upper and lower sidebands around the central frequency exhibit EPR-type correlations similar to those in Eq. (90),

$$\hat{U}(\Omega) \equiv \hat{X}_1'(\Omega) - \hat{X}_2'(\Omega) = \sqrt{2}S_-(\Omega)\hat{X}_2^{(0)}(\Omega),$$

$$\hat{V}(\Omega) \equiv \hat{P}_1'(\Omega) + \hat{P}_2'(\Omega) = \sqrt{2}S_-(\Omega)\hat{P}_1^{(0)}(\Omega), \qquad (259)$$

and therefore

$$\langle \Delta\hat{U}^\dagger(\Omega)\Delta\hat{U}(\Omega')\rangle = \delta(\Omega-\Omega')|S_-(\Omega)|^2/2,$$

$$\langle \Delta\hat{V}^\dagger(\Omega)\Delta\hat{V}(\Omega')\rangle = \delta(\Omega-\Omega')|S_-(\Omega)|^2/2. \qquad (260)$$

The corresponding sum condition, Eq. (110) with $\bar{a}=1$, necessarily satisfied by any separable state, is now violated for that range of modulation frequencies for which the resources are squeezed,[12]

$$\langle \Delta\hat{U}^\dagger(\Omega)\Delta\hat{U}(\Omega')\rangle + \langle \Delta\hat{V}^\dagger(\Omega)\Delta\hat{V}(\Omega')\rangle = \delta(\Omega-\Omega')|S_-(\Omega)|^2. \qquad (261)$$

In recent experiments, such violations at some squeezing frequency were detected for the verification of continuous-variable quadrature entanglement (Silberhorn *et al.*, 2001; Furusawa and Kimble, 2003) or, similarly, of continuous-variable polarization entanglement (Bowen *et al.*, 2002). Exactly these violations were also needed for accomplishing the recent quantum communication protocols (Furusawa *et al.*, 1998; Li, Pan, *et al.*, 2002; Bowen, Treps, *et al.*, 2003; Zhang *et al.*, 2003).

If the squeezed fields for entanglement generation come from two optical parametric oscillators, the nonlinear optical interaction is due to a $\chi^{(2)}$ medium. In general, Eq. (256) may define arbitrary squeezing spectra of two statistically identical but independent broadband squeezed states. Before obtaining the broadband EPR state, the squeezing of the two initial fields may be generated by any suitable nonlinear interaction. The optical Kerr effect, based on a $\chi^{(3)}$ interaction, may also serve as such a suitable interaction.

2. Kerr effect and linear interference

The first light-squeezing experiment was published in 1985 (Slusher *et al.*, 1985). In this experiment, squeezed light was generated via four-wave mixing. Though involving the production of photon pairs as in parametric down conversion, the process of four-wave mixing is based on a $\chi^{(3)}$ interaction.

Initially, the main conceptual difficulty in creating a detectable squeezing effect via a $\chi^{(3)}$ interaction was that such a process is very weak in all transparent media. In particular, in order to achieve measurable quantum noise reduction against additional classical (thermal) noise, large light energy density and long interaction lengths are required. These requirements led to the proposal to use an optical fiber for nondegenerate four-wave mixing (Levenson *et al.*, 1985). The proposal referred to a dispersionless cw type of four-wave mixing. In the response of the fiber material to an external field, the dominant nonlinear contribution corresponds to a $\chi^{(3)}$ interaction (the Kerr effect), because the $\chi^{(2)}$ susceptibility vanishes in a glass fiber (Agrawal, 1995). The Kerr effect is equivalent to an intensity-dependent refractive index. A squeezing experiment confirming the cw theory of four-wave mixing in a single-mode fiber (Levenson *et al.*, 1985) was successfully conducted by Shelby *et al.* (1986). Soon after this experiment, the quantum theory of light propagation and squeezing in an optical fiber was extended to include pulsed pump fields and group velocity dispersion (Carter *et al.*, 1987).

Using stochastic equations to describe the classical propagation plus the evolution of quantum noise in a fiber, Carter *et al.* (1987) proposed the squeezing of quantum fiber solitons. This theory was then experimentally confirmed by Rosenbluh and Shelby (1991).

What is the potential advantage of using optical fibers and light pulses with respect to applications in quantum communication? At the communication wavelength of 1.55 μm, glass fibers have an absorption minimum with very low losses and negative dispersion which enables one to use stable soliton pulses (Drummond *et al.*, 1993; Agrawal, 1995). A fiber-based quantum communication system can be potentially integrated into existing fiber-optics communication networks. Moreover, an optical fiber naturally offers long interaction times for producing squeezed light. Short light pulses and solitons have large peak power and photon number density, which enhances the effective $\chi^{(3)}$ nonlinearity in the fiber and hence the potential squeezing.

The Kerr interaction Hamiltonian,

$$\hat{H}_{\text{int}} = \hbar\kappa\hat{a}^{\dagger 2}\hat{a}^2 = \hbar\kappa\hat{n}(\hat{n}-1), \qquad (262)$$

with κ proportional to $\chi^{(3)}$, is quartic rather than quadratic [see Eq. (52)] as for optical parametric amplification or for conventional four-wave mixing. For the quartic Hamiltonian, the Kerr interaction would turn a coherent state into a "banana-shaped" state, which after a suitable phase-space displacement has reduced number and increased phase uncertainty though essentially still a number-phase minimum uncertainty state (Kitagawa and Yamamoto, 1986). This state corresponds to a photon number squeezed state with sub-Poissonian statistics, as opposed to the ordinary quadrature squeezed state. The state is closer to a Fock state than to a quadrature eigenstate. However, in the regime of large photon number and small nonlinearity [which, for example, applies to quantum solitons for sufficiently small propagation distances (Kärtner and Boivin, 1996)], quantum fluctuations higher than those of second order can be neglected. The quartic Hamiltonian is then effectively reduced to a quadratic one (note that squeezing due to the former preserves the photon number, whereas that due to the latter does not). In fact, the fiber Kerr nonlinearity is so small that the radius of curvature of the "banana" state is far larger than its length. The difference between such a state and an ordinary

[12] There is actually no rigorous broadband derivation of the inseparability criteria in the literature, including the corresponding broadband analog to the sum condition (110). Here we give only the continuum equations for the broadband EPR state and apply it directly to the discrete sum condition at the squeezing frequencies.

squeezed state with an "elliptic" phase-space distribution is therefore negligible.

Recently, bipartite continuous-variable entanglement was created through an optical fiber with optical pulses squeezed via the Kerr $\chi^{(3)}$ nonlinearity (Silberhorn *et al.*, 2001). The entanglement-generating mechanism in this experiment was indeed similar to that used for the creation of the broadband EPR state in Eq. (258) by combining the two squeezed fields in Eq. (257): first, the Kerr nonlinearity in the fiber was exploited to produce two independent squeezed beams (more precisely, an asymmetric fiber Sagnac interferometer was used to make two amplitude or photon number squeezed beams of orthogonal polarization). The squeezed fields were then combined outside the fiber at a beam splitter. As described, in order to obtain Kerr-induced squeezing, the beams must have nonzero intensity, and they must be bright, as opposed to the squeezed vacuum states in Eq. (257).

B. Generation of long-lived atomic entanglement

In Sec. III, in particular Sec. III.B.4, we discussed how to make entanglement from sources of nonclassical light such as squeezed states using a network of beam splitters. In fact, in order to create continuous-variable entanglement using linear optics at least one of the input modes must be in a nonclassical state. Otherwise, if all the input modes are in a vacuum or coherent state, the output state that emerges from the beam splitters will always remain separable. Similarly, entanglement-based quantum communication schemes utilizing atom-light interactions also seem to rely upon nonclassical light as a resource [see, for instance, the protocol of Kuzmich and Polzik (2000)]. Moreover, other atom-light protocols require that the atoms be trapped in high-Q optical cavities (see, for example, Parkins and Kimble, 1999). However, remarkably, entanglement between free-space atomic ensembles may also be created using only coherent light, as was proposed by Duan, Cirac, *et al.* (2000). The quantum nondemolition coupling given in Eq. (205) is a suitable interaction to achieve this. After the successive transmission of a light beam through two separate atomic ensembles, the light is detected such that the atomic states are reduced to an entangled state, corresponding to a nonlocal Bell measurement (Duan, Cirac, *et al.*, 2000). Such an experiment, along the lines of the proposal of Duan, Cirac, *et al.* (2000), was performed in Copenhagen (Julsgaard *et al.*, 2001). The long-lived entanglement generated in this experiment was between two clouds of atoms, each consisting of a cesium gas containing about 10^{12} atoms. The creation of this entanglement between material objects is an important step towards storing quantum information in an (optical) communication protocol and proves the feasibility of using light-atom quantum interfaces in a similar approach. Further experimental investigations towards a quantum memory, also based on this kind of approach, will be briefly described in Sec. VII.G.

The experiment for creating atomic entanglement (Julsgaard *et al.*, 2001) is based on the polarization and spin representation for continuous-variable quantum information, as discussed in Sec. II.F. Hence the light and the atoms are described via the Stokes operators and the operators for the collective spin, respectively. More precisely, if the atomic samples are spin polarized along the x axis with a large classical value, and similarly for the light, the only quantum variables used for entanglement generation are the atomic operators $\hat{F}_y$ and $\hat{F}_z$ and the light operators $\hat{S}_y$ and $\hat{S}_z$. In other words, the y and z components of spin and polarization play the roles of the effective phase-space variables for the atomic and light systems.

Now when an off-resonant light pulse classically polarized along the x axis $(\hat{S}_x \simeq \langle \hat{S}_x \rangle \equiv S)$ is transmitted along the z axis through two atomic samples with opposite classical spins along the x axis, $\hat{F}_{xj} \simeq \langle \hat{F}_{xj} \rangle$, $j=1,2$, $\langle \hat{F}_{x1} \rangle = -\langle \hat{F}_{x2} \rangle \equiv F$, the input-output relations are given by [see Eq. (205)]

$$\hat{S}_y^{(\text{out})} = \hat{S}_y^{(\text{in})} + aS(\hat{F}_{z1}^{(\text{in})} + \hat{F}_{z2}^{(\text{in})}),$$

$$\hat{S}_z^{(\text{out})} = \hat{S}_z^{(\text{in})},$$

$$\hat{F}_{y1}^{(\text{out})} = \hat{F}_{y1}^{(\text{in})} + aF\hat{S}_z^{(\text{in})}, \quad \hat{F}_{y2}^{(\text{out})} = \hat{F}_{y2}^{(\text{in})} - aF\hat{S}_z^{(\text{in})},$$

$$\hat{F}_{z1}^{(\text{out})} = \hat{F}_{z1}^{(\text{in})}, \quad \hat{F}_{z2}^{(\text{out})} = \hat{F}_{z2}^{(\text{in})}. \tag{263}$$

These equations show that for a sufficiently large value of the quantity aS, a measurement of $\hat{S}_y^{(\text{out})}$ reveals the value of the total z spin in a quantum nondemolition fashion, $\hat{F}_{z1}^{(\text{in})} + \hat{F}_{z2}^{(\text{in})} = \hat{F}_{z1}^{(\text{out})} + \hat{F}_{z2}^{(\text{out})}$. At the same time, the total y spin is conserved as well, neither being changed by the interaction, $\hat{F}_{y1}^{(\text{in})} + \hat{F}_{y2}^{(\text{in})} = \hat{F}_{y1}^{(\text{out})} + \hat{F}_{y2}^{(\text{out})}$, nor affected by the measurement thanks to the vanishing commutator $[\hat{F}_{y1} + \hat{F}_{y2}, \hat{F}_{z1} + \hat{F}_{z2}] = 0$. Upon repeating this procedure with a different light pulse, but now measuring the total y spin in a quantum nondemolition fashion (which will not change the previously measured value of the total z spin), both the total z spin and the total y spin may be precisely determined. Thus the resulting state of the two atomic samples has arbitrarily small variances for both y and z components of the total spin,

$$\langle [\Delta(\hat{F}_{y1} + \hat{F}_{y2})]^2 \rangle + \langle [\Delta(\hat{F}_{z1} + \hat{F}_{z2})]^2 \rangle \to 0. \tag{264}$$

This would, in the ideal case, lead to a maximal violation of the necessary separability condition in Eq. (119) (for x and z components interchanged). Under realistic experimental conditions, however, with imperfections caused by, for instance, losses of the light on the way from one sample to the other and spin-state decay between the two measurements, the resulting atomic state does not become perfectly entangled. Moreover, the vacuum noise of the incoming light pulse prevents the creation of a maximally entangled state. The outgoing state, prepared after the measurements, is then similar to a nonmaximally entangled two-mode squeezed state.

In the experiment in Copenhagen, the protocol described above was slightly modified by adding a magnetic field oriented along the x axis. Using only a single entangling light pulse, both the y and z spin projections can be measured this way. The generated entangled state was maintained for more than 0.5 ms. This relatively long lifetime is due to the high symmetry of the state. The entanglement is based on the collective properties of the two atomic ensembles such that the coherence of the entangled superposition state is not destroyed when only a few atoms interact with the environment. This kind of robustness would not be obtainable in a maximally entangled multiparticle state. The degree of entanglement verified in the Copenhagen experiment corresponds to a fidelity of $F\approx 0.55$ when using the entangled state for teleporting an atomic sample in a coherent spin state. This clearly exceeds the classical boundary of $F=0.5$.

Although the entanglement produced in Copenhagen was bipartite, i.e., between two atomic clouds, one can easily think of an extension to more atomic samples. As for an experiment in which the creation of such a genuine multipartite entanglement has been accomplished already, we now return to the all-optical regime of squeezed-light resources and linear-optics transformations.

C. Generation of genuine multipartite entanglement

We have seen that a particularly efficient way to generate entanglement between electromagnetic modes is to let squeezed light beams interfere using linear optics. For instance, the generation of tripartite entanglement, the entanglement between three optical modes, only requires combining three input modes at two beam splitters, where at least one of these input modes is in a squeezed state (see Sec. III.B.4). The resulting entangled modes, even when spatially separated, exhibit quantum correlations, as described by Eq. (137) for $N=3$. However, due to experimental imperfections, the three-mode states generated in the laboratory become noisy mixed states that might be partially or even fully separable. Therefore one has to verify experimentally that the generated state is indeed fully inseparable, exhibiting genuine tripartite entanglement. Such an unambiguous verification can be achieved even without determining the entire correlation matrix of the generated Gaussian three-mode state. It is sufficient to detect a set of suitable linear combinations of the quadratures (see Sec. III.E). However, these must contain the positions and momenta of all modes involved.

In an experiment in Tokyo (Aoki *et al.*, 2003), such a continuous-variable tripartite entangled state was created by combining three independent squeezed vacuum states at two beam splitters. For verification, the variances of the entangled state's relative positions and total momentum were measured. The following total variances were obtained (Aoki *et al.*, 2003):

$$\begin{aligned}
\text{I}.\quad & \langle[\Delta(\hat{x}_1-\hat{x}_2)]^2\rangle+\langle[\Delta(\hat{p}_1+\hat{p}_2+\hat{p}_3)]^2\rangle \\
&=0.851\pm 0.062<1, \\
\text{II}.\quad & \langle[\Delta(\hat{x}_2-\hat{x}_3)]^2\rangle+\langle[\Delta(\hat{p}_1+\hat{p}_2+\hat{p}_3)]^2\rangle \\
&=0.840\pm 0.065<1, \\
\text{III}.\quad & \langle[\Delta(\hat{x}_3-\hat{x}_1)]^2\rangle+\langle[\Delta(\hat{p}_1+\hat{p}_2+\hat{p}_3)]^2\rangle \\
&=0.867\pm 0.062<1.
\end{aligned} \tag{265}$$

These results clearly show the nonclassical correlations among the three modes. Moreover, according to van Loock and Furusawa (2003), the above inequalities unambiguously prove the full inseparability of the generated tripartite entangled state. In fact, the measured variances correspond to violations of the conditions in Eq. (154) with Eqs. (155) and (156). Any partially separable form is thus ruled out, and the generated state can only be fully inseparable. It can therefore be used as a resource in a quantum teleportation network, as proposed by van Loock and Braunstein (2000a) and also experimentally demonstrated by Yonezawa *et al.* (2004).

D. Quantum teleportation of coherent states

In the discrete-variable teleportation experiments in Innsbruck (Bouwmeester *et al.*, 1997) and in Rome (Boschi *et al.*, 1998), the teleported states were single-photon polarization states. Continuous-variable quantum teleportation of coherent states has been achieved in Pasadena (Furusawa *et al.*, 1998; Zhang *et al.*, 2003) and in Canberra (Bowen, Treps, *et al.*, 2003). A realistic broadband description of these experiments can be obtained from the Heisenberg equations for continuous-variable quantum teleportation (van Loock *et al.*, 2000), as given in Sec. IV.A.1.

For the teleportation of an electromagnetic field with finite bandwidth, the EPR state shared by Alice and Bob is a broadband two-mode squeezed state as in Eq. (258). The incoming electromagnetic field to be teleported, $\hat{E}_{\text{in}}(z,t)=\hat{E}_{\text{in}}^{(+)}(z,t)+\hat{E}_{\text{in}}^{(-)}(z,t)$, traveling in the positive-z direction and having a single unspecified polarization, can be described by its positive-frequency part,

$$\begin{aligned}
\hat{E}_{\text{in}}^{(+)}(z,t)&=[\hat{E}_{\text{in}}^{(-)}(z,t)]^\dagger \\
&=\int_W d\omega\frac{1}{\sqrt{2\pi}}\left(\frac{u\hbar\omega}{2cA_{\text{tr}}}\right)^{1/2}\hat{b}_{\text{in}}(\omega)e^{-i\omega(t-z/c)}.
\end{aligned} \tag{266}$$

The integral runs over a relevant bandwidth W centered on ω_0 and A_{tr} represents the transverse structure of the field. The parameter u is a unit-dependent constant. By Fourier transforming the incoming field in the rotating frame, we obtain the input modes as a function of the modulation frequency Ω, $\hat{B}_{\text{in}}(\Omega)$. As for the transverse structure and the polarization of the input field, we assume that both are known to Alice and Bob.

Using the broadband EPR state of Eq. (258) for her Bell detection, Alice combines mode 1 with the unknown input field at a 50:50 beam splitter. She obtains the quadratures $\hat{X}_{\mathrm{u}}(\Omega)=(1/\sqrt{2})\hat{X}_{\mathrm{in}}(\Omega)-(1/\sqrt{2})\hat{X}_1(\Omega)$ and $\hat{P}_{\mathrm{v}}(\Omega)=(1/\sqrt{2})\hat{P}_{\mathrm{in}}(\Omega)+(1/\sqrt{2})\hat{P}_1(\Omega)$ to be measured. The photocurrent operators for the two homodyne detections, $\hat{i}_{\mathrm{u}}(t)\propto\hat{X}_{\mathrm{u}}(t)$ and $\hat{i}_{\mathrm{v}}(t)\propto\hat{P}_{\mathrm{v}}(t)$, can be written (without loss of generality we assume $\Omega>0$) as

$$\hat{i}_{\mathrm{u}}(t)\propto\int_W d\Omega h_{\mathrm{el}}(\Omega)[\hat{X}_{\mathrm{u}}(\Omega)e^{-i\Omega t}+\hat{X}_{\mathrm{u}}^{\dagger}(\Omega)e^{i\Omega t}],$$

$$\hat{i}_{\mathrm{v}}(t)\propto\int_W d\Omega h_{\mathrm{el}}(\Omega)[\hat{P}_{\mathrm{v}}(\Omega)e^{-i\Omega t}+\hat{P}_{\mathrm{v}}^{\dagger}(\Omega)e^{i\Omega t}], \qquad (267)$$

assuming a noiseless, classical local oscillator and with $h_{\mathrm{el}}(\Omega)$ representing the detectors' responses within their electronic bandwidths $\Delta\Omega_{\mathrm{el}}$: $h_{\mathrm{el}}(\Omega)=1$ for $\Omega\leqslant\Delta\Omega_{\mathrm{el}}$ and zero otherwise. We assume that the relevant bandwidth W ($\sim$1 MHz) is fully covered by the electronic bandwidth of the detectors ($\sim$1 GHz). Therefore $h_{\mathrm{el}}(\Omega)\approx 1$ in Eq. (267) is a good approximation. The two photocurrents are measured and fed forward to Bob via a classical channel with sufficient rf bandwidth. They can be viewed as complex quantities in order to respect the rf phase. Any relative delays between the classical information conveyed by Alice's and Bob's EPR beam must be such that $\Delta t\ll 1/\Delta\Omega$ with the inverse bandwidth of the EPR source $1/\Delta\Omega$. Bob's final amplitude and phase modulations correspond to

$$\hat{X}_2(\Omega)\to\hat{X}_{\mathrm{tel}}(\Omega)=\hat{X}_2(\Omega)+g(\Omega)\sqrt{2}\hat{X}_{\mathrm{u}}(\Omega),$$

$$\hat{P}_2(\Omega)\to\hat{P}_{\mathrm{tel}}(\Omega)=\hat{P}_2(\Omega)+g(\Omega)\sqrt{2}\hat{P}_{\mathrm{v}}(\Omega), \qquad (268)$$

with a frequency-dependent gain $g(\Omega)$.

For unit gain, $g(\Omega)\equiv 1$, the teleported field is

$$\hat{X}_{\mathrm{tel}}(\Omega)=\hat{X}_{\mathrm{in}}(\Omega)-\sqrt{2}S_{-}(\Omega)\hat{\hat{X}}_2^{(0)}(\Omega),$$

$$\hat{P}_{\mathrm{tel}}(\Omega)=\hat{P}_{\mathrm{in}}(\Omega)+\sqrt{2}S_{-}(\Omega)\hat{\hat{P}}_1^{(0)}(\Omega). \qquad (269)$$

Obviously, for unit-gain teleportation at all relevant frequencies, it turns out that the variance of each teleported quadrature is given by the variance of the input quadrature plus twice the squeezing spectrum of the quiet quadrature of a decoupled mode in a broadband squeezed state, as in Eq. (257). Thus the excess noise in each teleported quadrature due the teleportation process is, relative to the vacuum noise, twice the squeezing spectrum $|S_{-}(\Omega)|^2$ of Eq. (256).

In the teleportation experiment of Furusawa *et al.* (1998), the teleported states described fields at a modulation frequency $\Omega/2\pi=2.9$ MHz within a bandwidth $\pm\Delta\Omega/2\pi=30$ kHz. Due to technical noise at low modulation frequencies, the resulting nonclassical fidelity, $F=0.58\pm0.02$ (exceeding the limit of $1/2$ for classical teleportation of coherent states), was achieved at these higher frequencies Ω. The amount of squeezing was about 3 dB, where the broadband EPR source as described by Eq. (258) was generated via interference of two independent optical parametric oscillators. In a second coherent-state teleportation experiment in Pasadena (Zhang *et al.*, 2003), a fidelity of $F=0.61\pm0.02$ was achieved, which is a slight improvement over the first experiment. Finally, in the most recent continuous-variable quantum teleportation in Canberra (Bowen, Treps, *et al.*, 2003), the best fidelity observed was $F=0.64\pm0.02$.

E. Experimental dense coding

As described in Sec. IV.B, rather than the reliable transfer of quantum information through a classical channel via quantum teleportation, dense coding aims at transmitting classical information more efficiently using a quantum channel. Thus the roles of the classical channel and the quantum channel are interchanged. However, like quantum teleportation, dense coding also relies upon preshared entanglement. In a dense coding scheme, the amount of classical information transmitted from Alice to Bob is increased when Alice sends her half of a preshared entangled state through a quantum channel to Bob. In order to accomplish this, the local operations performed by Alice and Bob are interchanged compared to those in quantum teleportation: Alice encodes the classical information by unitarily transforming her half of the entangled state; Bob eventually retrieves this information through a Bell measurement on his part of the entangled state and the other part obtained from Alice. In a discrete-variable qubit-based implementation, two bits of classical information can be conveyed by sending just one qubit. As discussed in Sec. IV.B, comparing a continuous-variable implementation based on squeezed-state entanglement against heterodyne-detection-based single-mode coherent-state communication, the channel capacity of the latter, given by Eq. (188), is always (for any nonzero squeezing of the entangled state) beaten by the optimal dense-coding scheme described by Eq. (198). In order to double the capacity of single-mode coherent-state communication, the dense coding requires infinite squeezing. This is similar to the ideal continuous-variable quantum teleportation in which the fidelity limit of classical coherent-state teleportation is exceeded for any nonzero squeezing of the entanglement resource, and unit fidelity is achieved in the limit of infinite squeezing.

In the dense-coding experiment of Li, Pan, *et al.* (2002), bright EPR beams were employed, similar to the entanglement created by Silberhorn *et al.* (2001). However, as mentioned in Sec. VII.A.2, the squeezed states in the experiment of Silberhorn *et al.* were produced via the Kerr $\chi^{(3)}$ nonlinearity. The bright squeezed beams were then combined at a beam splitter to build entanglement. By contrast, the bright EPR entanglement in the dense-coding experiment of Li *et al.* was directly generated from a nondegenerate parametric amplifier (based on a $\chi^{(2)}$ interaction; see Sec. VII.A.1). In order to accomplish the dense-coding protocol on Bob's side, the usual continuous-variable Bell measurement as described in Sec. IV.B (using a 50:50 beam splitter and two homodyne detectors with strong local oscillator fields) must be replaced by a direct Bell measurement (Zhang and Peng, 2000) as a result of the nonzero intensity of the entangled beams. This direct Bell measurement corresponds to the direct detection of the two bright outputs from a 50:50 beam splitter. Eventually, the sum and the difference photocurrents yield

$$\hat{i}_+(\Omega) \propto \hat{X}_1'(\Omega) - \hat{X}_2'(\Omega) + X_s(\Omega),$$

$$\hat{i}_-(\Omega) \propto \hat{P}_1'(\Omega) + \hat{P}_2'(\Omega) + P_s(\Omega), \tag{270}$$

where, using the same notation as in Secs. VII.A.1 and VII.D, $X_s(\Omega)$ and $P_s(\Omega)$ are the quadratures corresponding to Alice's classical signal modulations, and $\hat{X}_j'(\Omega)$ and $\hat{P}_j'(\Omega)$ are those belonging to the entangled nondegenerate optical parametric amplifier beams. As described by Eq. (259), due to the EPR-type correlations at those frequencies where squeezing occurs, Bob can simultaneously retrieve Alice's classical modulations $X_s(\Omega)$ and $P_s(\Omega)$ with a better accuracy than that given by the vacuum noise limit of two uncorrelated beams. In the dense-coding experiment of Li, Pan, *et al.*, the nondegenerate optical parametric amplifier position quadratures $\hat{X}_j'(\Omega)$ and momentum quadratures $\hat{P}_j'(\Omega)$ were actually anticorrelated and correlated, respectively, corresponding to interchanged signs in the expressions of Eq. (270), i.e., $\hat{X}_1'(\Omega)+\hat{X}_2'(\Omega)$ and $\hat{P}_1'(\Omega)-\hat{P}_2'(\Omega)$. The measured variances were up to 4 dB below the vacuum noise limit.

On the other hand, the individual nondegenerate optical parametric amplifier beams are very noisy. The noise background in the signal channel, measured by Li, Pan, *et al.*, without exploiting the correlations with the other EPR beam, was about 4.4 dB above the corresponding vacuum limit. As a result, the signal is to some extent protected against eavesdropping; only the authorized receiver who holds the other half of the EPR beam can retrieve the transmitted signal. This potential application of continuous-variable dense coding to the secure transmission of classical information was first realized by Pereira *et al.* (2000). Other quantum cryptography protocols utilizing EPR-type continuous-variable entanglement were discussed in Sec. IV.D. In the next section, we shall turn to a non-entanglement-based continuous-variable quantum key distribution protocol, experimentally demonstrated by the Grangier group (Grosshans *et al.*, 2003).

As a final remark of the current section on continuous-variable dense coding, let us mention that the experiment of Li, Pan, *et al.* demonstrates the potential of such dense coding for unconditional signal transmission with high efficiency only when the distribution of the preshared entanglement is not counted as part of the communication (see Sec. IV.B). In other words, the entanglement distribution must be accomplished off-peak. Otherwise, no advantage can be gained via the dense-coding protocol, in agreement with Holevo's bound in Eq. (158). On the other hand, non-entanglement-based "true" quantum coding schemes (Schumacher, 1995) can be considered as well. These schemes may indeed outperform their classical counterparts, but would require a quantum computational step for the information decoding on Bob's side. An optical proof-of-principle experiment of this type has been performed in the single-photon-based discrete-variable regime, demonstrating a superadditive capacity unattainable without quantum coding (Fujiwara *et al.*, 2003). The conditional quantum gate required for the decoding was achieved in this experiment by encoding quantum information into the spatial and polarization modes of a single photon. To date, no quantum coding experiment of this type has been performed in the continuous-variable domain using the more practical continuous-variable signals. The main difficulty of such an experiment would be the continuous-variable quantum gate in Bob's decoding procedure. It would require a non-Gaussian operation based on nonlinearities beyond those described by a quadratic interaction Hamiltonian and the linear unitary Bogoliubov transformation in Eq. (51) (see Sec. VI).

F. Experimental quantum key distribution

In Sec. IV.D, we gave an overview of the various proposals for continuous-variable quantum key distribution. Some of these proposals are based on the use of entanglement and others are "prepare and measure" schemes that do not directly utilize entangled states.

As for experimental progress, a BB84-like (entanglement-free) quantum cryptography scheme was implemented by Hirano *et al.* (2003) at telecommunication wavelengths using four nonorthogonal coherent states. A somewhat more genuine continuous-variable protocol, also based on coherent states, was recently implemented by Grosshans *et al.* (2003). This scheme, proposed by Grosshans and Grangier (2002), relies upon the distribution of a Gaussian key (Cerf *et al.*, 2001). Alice continuously modulates the phase and amplitude of coherent light pulses and Bob eventually measures these pulses via homodyne detection. The continuous data obtained must then be converted into a binary key using a particular reconciliation algorithm (Cerf *et al.*, 2002). Complete secret key extraction can be achieved, for instance, via a reverse reconciliation technique (followed by privacy amplification; Grosshans *et al.*, 2003). This method, experimentally implemented by Grosshans *et al.* (2003), provides security against arbitrarily high losses, even beyond the 3-dB loss limit of direct reconciliation protocols, as discussed briefly in Sec. IV.D.

In the experiment of Grosshans *et al.* (2003), the mutual information between all participants, Alice, Bob, and Eve, was experimentally determined for different values of the line transmission, in particular, including losses of 3.1 dB. The measured values confirmed the potential security of the scheme according to the information-theoretic condition in Eq. (203), which is sufficient for secure key extraction using privacy amplification and error-correction techniques. Eventually, net key transmission rates of about 1.7 megabits per second for a loss-free line and 75 kilobits per second for losses of 3.1 dB were obtained. The signal pulses in the experiment of Grosshans *et al.* (2003) contained up to 250 photons and were emitted at a wavelength of 780 nm. The limitations of this experiment were considered to be essentially technical, allowing for further improvement on the present scheme. Implementing this or related schemes at telecommunication wavelengths could therefore lead to efficient, high-bit-rate quantum key distribution over long distances.

G. Demonstration of a quantum memory effect

The creation of long-lived atomic entanglement, as described in Sec. VII.B, is a first step towards storing optical quantum information in atomic states for extended periods and hence implementing light-atom quantum interfaces. Using a similar approach, a proof-of-principle demonstration of such a quantum memory effect was achieved in an experiment by the Polzik group (Schori *et al.*, 2002). In this experiment, the quantum properties of a light beam were (partially) recorded in a long-lived atomic spin state; thus this experiment goes beyond a previous one in which only a short-lived squeezed spin state of an atomic ensemble was generated via complete absorption of nonclassical light (Hald *et al.*, 1999).

Similarly to the experiment for the creation of atomic entanglement (Julsgaard *et al.*, 2001), the experiment of Schori *et al.* (2002) relies upon polarization and spin representation for continuous-variable quantum information, as discussed in Sec. II.F. Thus the light and atoms are described via Stokes operators and operators for the collective spin, respectively. The atom-light interaction employed in the experiment is again based on coupling of the quantum nondemolition type between the atomic spin and the polarization state of light, as described in Sec. IV.F.

For describing the experiment by Schori *et al.* (2002), we again consider an atomic sample classically spin polarized along the x axis, $\hat{F}_x \simeq \langle \hat{F}_x \rangle \equiv F$, and similarly for the light, $\hat{S}_x \simeq \langle \hat{S}_x \rangle \equiv S$. Hence again the only quantum variables involved in the protocol are the atomic operators $\hat{F}_y$ and $\hat{F}_z$ and the light operators $\hat{S}_y$ and $\hat{S}_z$, i.e., the y and z components of spin and polarization are effective phase-space variables. The quantum properties of light to be transferred to the atoms are those of a vacuum or a squeezed optical field, i.e., those of a (pure) Gaussian state of light. An off-resonant light pulse prepared in such a state propagates through the atomic sample along the z axis and leaves its trace on the sample. As for the relevant input-output relations of this interaction, we may now only write [see Eq. (205)]

$$\hat{F}_y^{(\mathrm{out})} = \hat{F}_y^{(\mathrm{in})} + aF\hat{S}_z^{(\mathrm{in})}, \tag{271}$$

$$\hat{S}_y^{(\mathrm{out})} = \hat{S}_y^{(\mathrm{in})} + aS\hat{F}_z^{(\mathrm{in})}. \tag{272}$$

In the experiment of Schori *et al.* (2002), the optical input state was squeezed in the Stokes operator $\hat{S}_y$ and correspondingly antisqueezed in $\hat{S}_z$. This antisqueezing was mapped onto the atomic state and eventually read out through a detection of the outgoing light. The protocol consists of the following steps: first, $\hat{S}_z$ is mapped onto the atomic variable $\hat{F}_y$, as can be seen in Eq. (271). However, as in the experiment for creating atomic entanglement, the protocol is slightly modified by applying a constant magnetic field oriented along the x axis. This gives rise to Larmor precession in which the value of the Larmor frequency determines the frequency component of light to be stored in the atomic sample. Including the magnetic field, the actual evolution of the atomic spin is more complicated than that described by Eq. (271). However, the coupling term responsible for the back action of light onto atoms per time interval dt is still given by $aF\hat{S}_z(t)dt$, leading to the corresponding change $d\hat{F}_y(t)$ depending on the value of $\hat{S}_z(t)$. Moreover, due to the external magnetic field, $\hat{F}_y(t)$ and $\hat{F}_z(t)$ get linked with each other such that $\hat{F}_z$ and hence $\hat{F}_y$ can be read out via $\hat{S}_y$ according to Eq. (272). For this last step, one can exploit the fact that $\hat{S}_y^{(\mathrm{out})}$ in Eq. (272) is more sensitive to $\hat{F}_z^{(\mathrm{in})}$ due to the squeezing of $\hat{S}_y^{(\mathrm{in})}$.

In the experiment of Schori *et al.* (2002), the power spectrum of $\hat{S}_y^{(\mathrm{out})}$ was measured, yielding clear evidence that the antisqueezed variable $\hat{S}_z^{(\mathrm{in})}$ was stored in the atomic sample. Hence it was shown that partial information about an optical Gaussian quantum state, i.e., the value of one quadrature variable could be recorded in an atomic sample. This storage of quantum information was achieved over a duration of approximately 2 ms. However, Schori *et al.* (2002) did not demonstrate full quantum memory of an optical Gaussian state. In order to accomplish this, two conjugate variables must be recorded and, for verification, the fidelity between the input and the reproduced output state has to be determined. For Gaussian signal states, this corresponds to reproducing values of the output variances sufficiently close to those of the input variances, similar to the verification of high-fidelity quantum teleportation. The experiment by Schori *et al.* (2002), however, represented a significant step towards full quantum memory, because it was shown that long-lived atomic spin ensembles may serve as storage for optical quantum information sensitive enough to store fields containing just a few photons. In fact, very recently, in another experiment by Polzik and colleagues, a complete high-fidelity demonstration of quantum memory for light based on atomic ensembles was given (Julsgaard *et al.*, 2004).

VIII. CONCLUDING REMARKS

The field of quantum information has typically concerned itself with the manipulation of discrete systems such as quantum bits, or qubits. However, many quantum variables, such as position, momentum, or the quadrature amplitudes of electromagnetic fields, are continuous, leading to the concept of continuous quantum information.

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

In some ways continuous-variable computation may not be so different from qubit-based computation. In particular, limitations due to finite precision make quantum floating-point operations, like their classical counterparts, effectively discrete. Thus we might expect a continuous-variable quantum computer to perform no better than a discrete quantum computer. However, for some tasks continuous-variable quantum computers are nonetheless more efficient. Indeed, in many protocols, especially those relating to communication, they require only linear operations together with classical feedforward and detection. This together with the large bandwidths naturally available to continuous (optical) variables appears to give them the potential for a significant advantage.

Notwithstanding these successes, the very practical optical continuous-variable approach, when based solely upon Gaussian transformations such as beam-splitter and squeezing transformations, feedforward, and homodyne detections, is not sufficient for implementing more advanced or "genuine" quantum information protocols. Any more sophisticated quantum protocol that is truly superior to its classical counterpart requires a non-Gaussian element. This may be included on the level of the measurements, for example, via state preparation conditioned upon the number of photons detected in a subset of the Gaussian modes. Alternatively, one may directly apply a non-Gaussian operation which involves a highly nonlinear optical interaction described by a Hamiltonian at least cubic in the mode operators.

Though a significant first step, communication protocols in which this non-Gaussian element is missing cannot fully exploit the advantages offered by quantum mechanics. For example, the goals in the Gaussian protocols of continuous-variable quantum teleportation and dense coding are reliable transfer of quantum information and increase of classical capacity, respectively. However, in both cases, preshared entanglement is required. Using this resource, via teleportation, fragile quantum information can be conveyed through a classical communication channel without being subject to decoherence in a noisy quantum channel. In entanglement-based dense coding, using an ideal quantum channel, more classical information can be transmitted than directly through a classical channel. For transferring quantum information over long distances, however, entanglement must be distributed through increasingly noisy quantum channels. Hence entanglement distillation is needed, and for this, Gaussian resources and Gaussian operations alone do not suffice. Similarly, true quantum coding would require a non-Gaussian decoding step at the receiving end. In general, any continuous-variable quantum computation that is genuinely quantum and hence not efficiently simulatible by a classical computer must contain a non-Gaussian element. Among the communication protocols, continuous-variable quantum key distribution appears in some sense exceptional, because even in a purely Gaussian implementation it may well enhance security compared to classical key distribution schemes.

The experiments accomplished so far in continuous-variable quantum information reflect the observations of the preceding paragraphs. Gaussian state preparation, including (multiparty) entangled states, and Gaussian state manipulation are techniques well understood and implemented in many laboratories around the globe. However, in order to come closer to real applications, both for long-distance quantum communication and for quantum computation, a new generation of experiments is needed, crossing the border between the Gaussian and non-Gaussian worlds. Beyond this border, techniques from the more traditional single-photon-based discrete-variable domain will have to be incorporated into the continuous-variable approaches. In fact, a real-world application of optical quantum communication and computation, possibly including atom-light quantum interfaces and atomic quantum memories, will most likely combine the assets of both approaches, the continuous-variable one and that based on discrete variables.

ACKNOWLEDGMENTS

S.L.B. currently holds a Wolfson-Royal Society Research Merit Award. This work was funded in part under Project No. QUICOV as part of the IST-FET-QJPC program. P.v.L. is grateful to M. Curty, J. Eisert, J. Fiurášek, A. Furusawa, G. Giedke, N. Lütkenhaus, and T. C. Ralph for very useful discussions. He acknowledges the financial support of the DFG under the Emmy-Noether program.

REFERENCES

Adesso, G., and F. Illuminati, 2004, quant-ph/0410050.

Adesso, G., A. Serafini, and F. Illuminati, 2004, Phys. Rev. Lett. **93**, 220504.

Agarwal, G. S., 1971, Phys. Rev. A **3**, 828.

Agrawal, G. P., 1995, *Nonlinear Fiber Optics* (Academic, New York).

Alber, G., A. Delgado, N. Gisin, and I. Jex, 2000, quant-ph/0008022.

Aoki, T., N. Takei, H. Yonezawa, K. Wakui, T. Hiraoka, A. Furusawa, and P. van Loock, 2003, Phys. Rev. Lett. **91**, 080404.

Arthurs, E., and J. L. Kelly, 1965, Bell Syst. Tech. J. **44**, 725.

Aspect, A., J. Dalibard, and G. Roger, 1982, Phys. Rev. Lett. **49**, 1804.

Ban, M., 1999, J. Opt. B: Quantum Semiclassical Opt. **1**, L9.

Banaszek, K., 1999, Phys. Lett. A **253**, 12.

Banaszek, K., A. Dragan, K. Wódkiewicz, and C. Radzewicz, 2002, Phys. Rev. A **66**, 043803.

Banaszek, K., and K. Wódkiewicz, 1998, Phys. Rev. A **58**, 4345.

Barnum, H., 1998, Ph.D. thesis (University of New Mexico, Albuquerque).

Bartlett, S. D., and B. C. Sanders, 2002, Phys. Rev. A **65**, 042310.

Bell, J. S., 1964, Physics (Long Island City, N.Y.) **1**, 195.

Bell, J. S., 1987, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, UK).

Bennett, C. H., 1992, Phys. Rev. Lett. **68**, 3121.

Bennett, C. H., H. J. Bernstein, S. Popescu, and B. Schumacher, 1996, Phys. Rev. A **53**, 2046.

Bennett, C. H., and G. Brassard, 1984, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Los Alamitos, CA), p. 175.

Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, 1993, Phys. Rev. Lett. **70**, 1895.

Bennett, C. H., G. Brassard, C. Crépeau, and U. M. Maurer, 1995, IEEE Trans. Inf. Theory **41**, 1915.

Bennett, C. H., G. Brassard, and N. D. Mermin, 1992, Phys. Rev. Lett. **68**, 557.

Bennett, C. H., G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, 1996, Phys. Rev. Lett. **76**, 722.

Bennett, C. H., D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, 1996, Phys. Rev. A **54**, 3824.

Bennett, C. H., and S. J. Wiesner, 1997, Phys. Rev. Lett. **69**, 2881.

Bernstein, H. J., 1974, J. Math. Phys. **15**, 1677.

Bogoliubov, N. N., 1947, J. Phys. (Moscow) **11**, 23.

Bohm, D., 1951, *Quantum Theory* (Prentice-Hall, Englewood Cliffs, NJ).

Boschi, D., S. Branca, F. D. Martini, L. Hardy, and S. Popescu, 1998, Phys. Rev. Lett. **80**, 1121.

Bose, S., V. Vedral, and P. L. Knight, 1998, Phys. Rev. A **57**, 822.

Bose, S., V. Vedral, and P. L. Knight, 1999, Phys. Rev. A **60**, 194.

Botero, A., and B. Reznik, 2003, Phys. Rev. A **67**, 052311.

Bouwmeester, D., J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, 1999, Phys. Rev. Lett. **82**, 1345.

Bouwmeester, D., J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, 1997, Nature (London) **390**, 575.

Bowen, W. P., P. K. Lam, and T. C. Ralph, 2003, J. Mod. Opt. **50**, 801.

Bowen, W. P., N. Treps, B. C. Buchler, R. Schnabel, T. C. Ralph, H.-A. Bachor, T. Symul, and P. K. Lam, 2003, Phys. Rev. A **67**, 032302.

Bowen, W. P., N. Treps, R. Schnabel, and P. K. Lam, 2002, Phys. Rev. Lett. **89**, 253601.

Brassard, G., and L. Salvail, 1994, in *Lecture Notes in Computer Science 765*, edited by Tor Helleseth (Springer, New York), p. 410.

Braunstein, S. L., 1998a, Phys. Rev. Lett. **80**, 4084.

Braunstein, S. L., 1998b, Nature (London) **394**, 47.

Braunstein, S. L., V. Bužek, and M. Hillery, 2001, Phys. Rev. A **63**, 052313.

Braunstein, S. L., N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, 2001, Phys. Rev. Lett. **86**, 4938.

Braunstein, S. L., and D. D. Crouch, 1991, Phys. Rev. A **43**, 330.

Braunstein, S. L., G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi, 2000, Phys. Rev. Lett. **84**, 3486.

Braunstein, S. L., C. A. Fuchs, and H. J. Kimble, 2000, J. Mod. Opt. **47**, 267.

Braunstein, S. L., C. A. Fuchs, H. J. Kimble, and P. van Loock, 2001, Phys. Rev. A **64**, 022321.

Braunstein, S. L., and H. J. Kimble, 1998a, Phys. Rev. Lett. **80**, 869.

Braunstein, S. L., and H. J. Kimble, 1998b, Nature (London) **394**, 840.

Braunstein, S. L., and H. J. Kimble, 2000, Phys. Rev. A **61**, 042302.

Braunstein, S. L., H. J. Kimble, J. Sørensen, A. Furusawa, and N. P. Georgiades, 1998, *Technical Digest Series (Optical Society of America)*, Vol. 7 (Optical Society of America, Washington, D.C.), p. 133.

Briegel, H.-J., W. Dür, J. I. Cirac, and P. Zoller, 1998, Phys. Rev. Lett. **81**, 5932.

Browne, D. E., J. Eisert, S. Scheel, and M. B. Plenio, 2003, Phys. Rev. A **67**, 062320.

Brune, M., S. Haroche, L. Davidovich, and N. Zagury, 1992, Phys. Rev. A **45**, 5193.

Bruß, D., D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, 1998, Phys. Rev. A **57**, 2368.

Bruß, D., A. Ekert, and C. Macchiavello, 1998, Phys. Rev. Lett. **81**, 2598.

Bužek, V., S. L. Braunstein, M. Hillery, and D. Bruß, 1997, Phys. Rev. A **56**, 3446.

Bužek, V., and M. Hillery, 1996, Phys. Rev. A **54**, 1844.

Bužek, V., C. H. Keitel, and P. L. Knight, 1995, Phys. Rev. A **51**, 2575.

Bužek, V., A. D. Wilson-Gordon, P. L. Knight, and W. K. Lai, 1992, Phys. Rev. A **45**, 8079.

Calderbank, A. R., E. M. Rains, P. W. Shor, and N. J. A. Sloane, 1997, Phys. Rev. Lett. **78**, 405.

Carter, S. J., P. D. Drummond, M. D. Reid, and R. M. Shelby, 1987, Phys. Rev. Lett. **58**, 1841.

Caves, C. M., 1982, Phys. Rev. D **26**, 1817.

Caves, C. M., and P. D. Drummond, 1994, Rev. Mod. Phys. **66**, 481.

Caves, C. M., and B. L. Schumaker, 1985, Phys. Rev. A **31**, 3068.

Caves, C. M., K. S. Thorne, R. W. P. Drever, V. D. Sandberg, and M. Zimmermann, 1980, Rev. Mod. Phys. **52**, 341.

Cerf, N. J., 2003, conference talk at the CVQIP workshop, Aix-en-Provence, unpublished.

Cerf, N. J., and S. Iblisdir, 2000a, Phys. Rev. A **62**, 040301(R).

Cerf, N. J., and S. Iblisdir, 2000b, in *Proceedings of the 5th International Conference on Quantum Communication, Measurement and Computing*, edited by P. Tombesi and O. Hirota (Kluwer Academic, Dordrecht).

Cerf, N. J., S. Iblisdir, and G. van Assche, 2002, Eur. Phys. J. D **18**, 211.

Cerf, N. J., A. Ipe, and X. Rottenberg, 2000, Phys. Rev. Lett. **85**, 1754.

Cerf, N. J., M. Lévy, and G. Van Assche, 2001, Phys. Rev. A **63**, 052311.

Chen, Z.-B., J.-W. Pan, G. Hou, and Y.-D. Zhang, 2002, Phys. Rev. Lett. **88**, 040406.

Chen, Z.-B., and Y.-D. Zhang, 2002, Phys. Rev. A **65**, 044102.

Cirel'son, B. S., 1980, Lett. Math. Phys. **4**, 93.

Clausen, J., T. Opatrný, and D.-G. Welsch, 2000, Phys. Rev. A **62**, 042308.

Clauser, J. F., M. A. Horne, A. Shimony, and R. A. Holt, 1969, Phys. Rev. Lett. **23**, 880.

Cochrane, P. T., G. J. Milburn, and W. J. Munro, 2000, Phys. Rev. A **62**, 062307.

Cochrane, P. T., T. C. Ralph, and G. J. Milburn, 2002, Phys. Rev. A **65**, 062306.

Cohen, O., 1997, Helv. Phys. Acta **70**, 710.

Collett, M. J., 1988, Phys. Rev. A **38**, 2233.

Curty, M., M. Lewenstein, and N. Lütkenhaus, 2004, Phys. Rev. Lett. **92**, 217903.

Danakas, S., and P. K. Aravind, 1992, Phys. Rev. A **45**, 1973.

Demkowicz-Dobrzański, R., M. Kuś, and K. Wódkiewicz, 2004, Phys. Rev. A **69**, 012301.

Deutsch, D., 1989, Proc. R. Soc. London, Ser. A **425**, 73.

Deutsch, D., A. Barenco, and A. Ekert, 1995, Proc. R. Soc. London, Ser. A **449**, 669.

Dieks, D., 1982, Phys. Lett. **92A**, 271.

DiVincenzo, D., 1995, Science **270**, 255.

DiVincenzo, D., P. Shor, J. Smolin, B. Terhal, and A. Thapliyal, 2000, Phys. Rev. A **61**, 062312.

Drummond, P. D., R. M. Shelby, S. R. Friberg, and Y. Yamamoto, 1993, Nature (London) **365**, 307.

Duan, L.-M., J. I. Cirac, P. Zoller, and E. S. Polzik, 2000, Phys. Rev. Lett. **85**, 5643.

Duan, L.-M., G. Giedke, J. I. Cirac, and P. Zoller, 2000a, Phys. Rev. Lett. **84**, 2722.

Duan, L.-M., G. Giedke, J. I. Cirac, and P. Zoller, 2000b, Phys. Rev. Lett. **84**, 4002.

Duan, L.-M., G. Giedke, J. I. Cirac, and P. Zoller, 2000c, Phys. Rev. A **62**, 032304.

Dür, W., H.-J. Briegel, J. I. Cirac, and P. Zoller, 1999, Phys. Rev. A **59**, 169.

Dür, W., and J. I. Cirac, 2000, J. Mod. Opt. **47**, 247.

Dür, W., J. I. Cirac, M. Lewenstein, and D. Bruß, 2000, Phys. Rev. A **61**, 062313.

Dür, W., J. I. Cirac, and R. Tarrach, 1999, Phys. Rev. Lett. **83**, 3562.

Dür, W., G. Vidal, and J. I. Cirac, 2000, Phys. Rev. A **62**, 062314.

Dušek, M., 2001, Opt. Commun. **199**, 161.

Einstein, A., B. Podolsky, and N. Rosen, 1935, Phys. Rev. **47**, 777.

Eisert, J., D. E. Browne, S. Scheel, and M. B. Plenio, 2004, Ann. Phys. (N.Y.) **311**, 431.

Eisert, J., S. Scheel, and M. B. Plenio, 2002, Phys. Rev. Lett. **89**, 137903.

Ekert, A. K., 1991, Phys. Rev. Lett. **67**, 661.

Filip, R., and L. Mišta, 2002, quant-ph/0201114.

Fiurášek, J., 2001, Phys. Rev. Lett. **86**, 4942.

Fiurášek, J., 2002, Phys. Rev. Lett. **89**, 137904.

Fiurášek, J., L. Mišta, and R. Filip, 2003, Phys. Rev. A **67**, 022304.

Fujiwara, M., M. Takeoka, J. Mizuno, and M. Sasaki, 2003, Phys. Rev. Lett. **90**, 167906.

Furusawa, A., and H. J. Kimble, 2003, in *Quantum Information with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati (Kluwer Academic, Dordrecht), p. 77.

Furusawa, A., J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, 1998, Science **282**, 706.

Gea-Banacloche, J., 1990, in *New Frontiers in Quantum Electrodynamics and Quantum Optics*, edited by A. O. Barut (Plenum, New York).

Giedke, G., and J. I. Cirac, 2002, Phys. Rev. A **66**, 032316.

Giedke, G., L.-M. Duan, J. I. Cirac, and P. Zoller, 2001, Quantum Inf. Comput. **1**, 79.

Giedke, G., J. Eisert, J. I. Cirac, and M. B. Plenio, 2003, Quantum Inf. Comput. **3**, 211.

Giedke, G., B. Kraus, L.-M. Duan, P. Zoller, J. I. Cirac, and M. Lewenstein, 2001a, Fortschr. Phys. **49**, 973.

Giedke, G., B. Kraus, M. Lewenstein, and J. I. Cirac, 2001b, Phys. Rev. Lett. **87**, 167904.

Giedke, G., B. Kraus, M. Lewenstein, and J. I. Cirac, 2001c, Phys. Rev. A **64**, 052303.

Giedke, G., M. M. Wolf, O. Krüger, R. F. Werner, and J. I. Cirac, 2003, Phys. Rev. Lett. **91**, 107901.

Giovannetti, V., S. Mancini, D. Vitali, and P. Tombesi, 2003, Phys. Rev. A **67**, 022320.

Gisin, N., and H. Bechmann-Pasquinucci, 1998, Phys. Lett. A **246**, 1.

Gisin, N., and S. Massar, 1997, Phys. Rev. Lett. **79**, 2153.

Gordon, J. P., 1962, Proc. IRE **50**, 1898.

Gottesman, D., 1999, in *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International, Cambridge, MA), p. 32.

Gottesman, D., A. Kitaev, and J. Preskill, 2001, Phys. Rev. A **64**, 012310.

Gottesman, D., and J. Preskill, 2001, Phys. Rev. A **63**, 022309.

Grangier, P., M. J. Potasek, and B. Yurke, 1988, Phys. Rev. A **38**, 3132.

Greenberger, D. M., M. A. Horne, A. Shimony, and A. Zeilinger, 1990, Am. J. Phys. **58**, 1131.

Grosshans, F., G. V. Assche, R. M. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, 2003, Nature (London) **421**, 238.

Grosshans, F., and N. J. Cerf, 2004, Phys. Rev. Lett. **92**, 047904.

Grosshans, F., and P. Grangier, 2001, Phys. Rev. A **64**, 010301(R).

Grosshans, F., and P. Grangier, 2002, Phys. Rev. Lett. **88**, 057902.

Hald, J., J. L. Sørensen, C. Schori, and E. S. Polzik, 1999, Phys. Rev. Lett. **83**, 1319.

Halvorson, H., 2000, Lett. Math. Phys. **53**, 321.

Hammerer, K., M. M. Wolf, E. S. Polzik, and J. I. Cirac, 2004, Phys. Rev. Lett. **94**, 150503.

Happer, W., and B. S. Mathur, 1967, Phys. Rev. Lett. **18**, 577.

Hardy, L., 1992, Phys. Rev. Lett. **68**, 2981.

Hillery, M., 2000, Phys. Rev. A **61**, 022309.

Hillery, M., V. Bužek, and A. Berthiaume, 1999, Phys. Rev. A **59**, 1829.

Hirano, T., H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, 2003, Phys. Rev. A **68**, 042331.

Hofmann, H. F., T. Ide, and T. Kobayashi, 2000, Phys. Rev. A **62**, 062304.

Holevo, A. S., 1982, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam).

Holevo, A. S., 1998, IEEE Trans. Inf. Theory **44**, 269.

Holland, M. J., M. J. Collett, D. F. Walls, and M. D. Levenson, 1990, Phys. Rev. A **42**, 2995.

Horodecki, M., and P. Horodecki, 1999, Phys. Rev. A **59**, 4206.

Horodecki, M., P. Horodecki, and R. Horodecki, 1996a, Phys.

Lett. A **223**, 1.

Horodecki, M., P. Horodecki, and R. Horodecki, 1998, Phys. Rev. Lett. **80**, 5239.

Horodecki, P., J. I. Cirac, and M. Lewenstein, 2001, quant-ph/0103076.

Horodecki, P., and M. Lewenstein, 2000, Phys. Rev. Lett. **85**, 2657.

Horodecki, R., P. Horodecki, and M. Horodecki, 1996b, Phys. Lett. A **210**, 377.

Huang, Y.-F., W.-L. Li, C.-F. Li, Y.-S. Zhang, Y.-K. Jiang, and G.-C. Guo, 2001, Phys. Rev. A **64**, 012315.

Huttner, B., N. Imoto, N. Gisin, and T. Mor, 1995, Phys. Rev. A **51**, 1863.

Ide, T., H. F. Hofmann, T. Kobayashi, and A. Furusawa, 2001, Phys. Rev. A **65**, 012313.

Jeong, H., J. Lee, and M. S. Kim, 2000, Phys. Rev. A **61**, 052101.

Jeong, H., W. Son, M. S. Kim, D. Ahn, and Č. Brukner, 2003, Phys. Rev. A **67**, 012106.

Julsgaard, B., A. Kozhekin, and E. S. Polzik, 2001, Nature (London) **413**, 400.

Julsgaard, B., J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, 2004, quant-ph/0410072.

Kärtner, F. X., and L. Boivin, 1996, Phys. Rev. A **53**, 454.

Kaye, P., and M. Mosca, 2001, J. Phys. A **34**, 6939.

Kim, M. S., J. Lee, and W. J. Munro, 2002, Phys. Rev. A **66**, 030301.

Kitagawa, M., and Y. Yamamoto, 1986, Phys. Rev. A **34**, 3974.

Klyshko, D. N., 1993, Phys. Lett. A **172**, 399.

Knill, E., and R. Laflamme, 1997, Phys. Rev. A **55**, 900.

Knill, E., R. Laflamme, and G. J. Milburn, 2001, Nature (London) **409**, 46.

Kok, P., and S. L. Braunstein, 2000, Phys. Rev. A **61**, 042304.

Korolkova, N., G. Leuchs, R. Loudon, T. C. Ralph, and C. Silberhorn, 2002, Phys. Rev. A **65**, 052306.

Korolkova, N., and R. Loudon, 2005 **71**, 032343.

Kraus, B., K. Hammerer, G. Giedke, and J. I. Cirac, 2003, Phys. Rev. A **67**, 042314.

Kraus, K., 1983, *Effects and Operations* (Springer-Verlag, Berlin).

Krüger, O., R. F. Werner, and M. M. Wolf, 2004, quant-ph/0410058.

Kuzmich, A., and E. S. Polzik, 2000, Phys. Rev. Lett. **85**, 5639.

Kuzmich, A., and E. S. Polzik, 2003, in *Quantum Information with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati (Kluwer Academic, Dordrecht), p. 231.

Kuzmich, A., I. A. Walmsley, and L. Mandel, 2000, Phys. Rev. Lett. **85**, 1349.

Kuzmich, A., I. A. Walmsley, and L. Mandel, 2001, Phys. Rev. A **64**, 063804.

Lance, A. M., T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, 2004, Phys. Rev. Lett. **92**, 177903.

Lee, J., M. S. Kim, and H. Jeong, 2000, Phys. Rev. A **62**, 032305.

Leonhardt, U., 1997, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, UK).

Levenson, M. D., R. M. Shelby, and A. Aspect, 1985, Phys. Rev. A **32**, 1550.

Li, F.-L., H.-R. Li, J.-X. Zhang, and S.-Y. Zhu, 2002, Phys. Rev. A **66**, 024302.

Li, X., Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng, 2002, Phys. Rev. Lett. **88**, 047904.

Lloyd, S., 1995a, Sci. Am. (Int. Ed.) **273**, 140.

Lloyd, S., 1995b, Phys. Rev. Lett. **75**, 346.

Lloyd, S., 1996, Science **273**, 1073.

Lloyd, S., and S. L. Braunstein, 1999, Phys. Rev. Lett. **82**, 1784.

Lloyd, S., and J.-J. E. Slotine, 1998, Phys. Rev. Lett. **80**, 4088.

Lütkenhaus, N., 2002, private communication.

Lütkenhaus, N., J. Calsamiglia, and K.-A. Suominen, 1999, Phys. Rev. A **59**, 3295.

Martini, F. D., and V. Mussi, 2000, Fortschr. Phys. **48**, 413.

Massar, S., and S. Pironio, 2001, Phys. Rev. A **64**, 062108.

Massar, S., and S. Popescu, 1995, Phys. Rev. Lett. **74**, 1259.

Mattle, K., H. Weinfurter, P. G. Kwiat, and A. Zeilinger, 1996, Phys. Rev. Lett. **76**, 4656.

Mermin, N. D., 1990, Phys. Rev. Lett. **65**, 1838.

Milburn, G. J., and S. L. Braunstein, 1999, Phys. Rev. A **60**, 937.

Mølmer, K., 1997, Phys. Rev. A **55**, 3195.

Mu, Y., J. Seberry, and Y. Zheng, 1996, Opt. Commun. **123**, 344.

Murao, M., D. Jonathan, M. B. Plenio, and V. Vedral, 1999, Phys. Rev. A **59**, 156.

Murao, M., M. B. Plenio, and V. Vedral, 2000, Phys. Rev. A **61**, 032311.

Namiki, R., and T. Hirano, 2004, Phys. Rev. Lett. **92**, 117901.

Nemoto, K., and S. L. Braunstein, 2003, quant-ph/0312108.

Nielsen, M. A., 1999, Phys. Rev. Lett. **83**, 436.

Nielsen, M. A., and I. L. Chuang, 2000, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK).

Nielsen, M. A., and J. Kempe, 2001, Phys. Rev. Lett. **86**, 5184.

Opatrný, T., V. Buzek, J. Bajer, and G. Drobný, 1995, Phys. Rev. A **52**, 2419.

Opatrný, T., G. Kurizki, and D.-G. Welsch, 2000, Phys. Rev. A **61**, 032302.

Ou, Z. Y., and L. Mandel, 1988, Phys. Rev. Lett. **61**, 50.

Ou, Z. Y., S. F. Pereira, and H. J. Kimble, 1992a, Appl. Phys. B: Photophys. Laser Chem. **55**, 265.

Ou, Z. Y., S. F. Pereira, H. J. Kimble, and K. C. Peng, 1992b, Phys. Rev. Lett. **68**, 3663.

Pan, J.-W., D. Bouwmeester, H. Weinfurter, and A. Zeilinger, 1998, Phys. Rev. Lett. **80**, 3891.

Parker, S., S. Bose, and M. B. Plenio, 2000, Phys. Rev. A **61**, 032305.

Parkins, A. S., and H. J. Kimble, 1999, J. Opt. B: Quantum Semiclassical Opt. **1**, 496.

Paul, H., 1995, *Photonen: Eine Einführung in die Quantenoptik* (Teubner, Leipzig).

Pereira, S. F., Z. Y. Ou, and H. J. Kimble, 2000, Phys. Rev. A **62**, 042311.

Peres, A., 1996, Phys. Rev. Lett. **77**, 1413.

Polkinghorne, R. E. S., and T. C. Ralph, 1999, Phys. Rev. Lett. **83**, 2095.

Preskill, J., 1998, *Physics 229: Advanced Mathematical Methods of Physics: Quantum Computation and Information* (California Institute of Technology), www.theory.caltech.edu/people/preskill/ph229

Ralph, T. C., 2000a, Phys. Rev. A **61**, 010303(R).

Ralph, T. C., 2000b, Phys. Rev. A **62**, 062306.

Ralph, T. C., 2000c, private communication.

Ralph, T. C., and P. K. Lam, 1998, Phys. Rev. Lett. **81**, 5668.

Ralph, T. C., W. J. Munro, and R. E. S. Polkinghorne, 2000, Phys. Rev. Lett. **85**, 2035.

Ramakrishna, V., M. V. Salapaka, M. Dahleh, H. Rabitz, and A. Peirce, 1995, Phys. Rev. A **51**, 960.

Reck, M., A. Zeilinger, H. J. Bernstein, and P. Bertani, 1994, Phys. Rev. Lett. **73**, 58.

Reid, M. D., 1989, Phys. Rev. A **40**, 913.

Reid, M. D., 2000, Phys. Rev. A **62**, 062308.

Reid, M. D., 2001, quant-ph/0103142.

Rosenbluh, M., and R. M. Shelby, 1991, Phys. Rev. Lett. **66**, 153.

Royer, A., 1977, Phys. Rev. A **15**, 449.

Rudolph, T., and B. C. Sanders, 2001, Phys. Rev. Lett. **87**, 077903.

Schmidt, E., 1906, Math. Ann. **63**, 433.

Schori, C., B. Julsgaard, J. L. Sørensen, and E. S. Polzik, 2002, Phys. Rev. Lett. **89**, 057903.

Schrödinger, E., 1935, Naturwiss. **23**, 807.

Schumacher, B., 1995, Phys. Rev. A **51**, 2738.

Scully, M. O., and M. S. Zubairy, 1997, *Quantum Optics* (Cambridge University Press, Cambridge, UK).

Seevinck, M., and J. Uffink, 2001, Phys. Rev. A **65**, 012107.

Shannon, C. E., 1948, Bell Syst. Tech. J. **27**, 379.

She, C. Y., 1968, IEEE Trans. Inf. Theory **IT-14**, 32.

Shelby, R. M., M. D. Levenson, S. H. Perlmutter, R. G. DeVoe, and D. F. Walls, 1986, Phys. Rev. Lett. **57**, 691.

Shor, P. W., 1995, Phys. Rev. A **52**, R2493.

Shor, P. W., J. Smolin, and B. Terhal, 2001, Phys. Rev. Lett. **86**, 2681.

Shor, P. W., and J. Preskill, 2000, Phys. Rev. Lett. **85**, 441.

Silberhorn, C., N. Korolkova, and G. Leuchs, 2002, Phys. Rev. Lett. **88**, 167902.

Silberhorn, C., P. K. Lam, O. Weiß, F. König, N. Korolkova, and G. Leuchs, 2001, Phys. Rev. Lett. **86**, 4267.

Silberhorn, C., T. C. Ralph, N. Lütkenhaus, and G. Leuchs, 2002, Phys. Rev. Lett. **89**, 167901.

Simon, C., G. Weihs, and A. Zeilinger, 2000, J. Mod. Opt. **47**, 233.

Simon, R., 2000, Phys. Rev. Lett. **84**, 2726.

Slusher, R. E., L. W. Hollberg, B. Yurke, J. C. Mertz, and J. F. Valley, 1985, Phys. Rev. Lett. **55**, 2409.

Takeoka, M., M. Ban, and M. Sasaki, 2002, J. Opt. B: Quantum Semiclassical Opt. **4**, 114.

Tan, S. M., 1999, Phys. Rev. A **60**, 2752.

Turchette, Q. A., C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, 1995, Phys. Rev. Lett. **75**, 4710.

Tyc, T., and B. C. Sanders, 2002, Phys. Rev. A **65**, 042310.

Vaidman, L., 1994, Phys. Rev. A **49**, 1473.

Vaidman, L., and N. Yoran, 1999, Phys. Rev. A **59**, 116.

van Enk, S. J., 1999, Phys. Rev. A **60**, 5095.

van Enk, S. J., and C. A. Fuchs, 2002, Quantum Inf. Comput. **2**, 151.

van Loock, P., 2002, Fortschr. Phys. **50**, 1177.

van Loock, P., and S. L. Braunstein, 2000a, Phys. Rev. Lett. **84**, 3482.

van Loock, P., and S. L. Braunstein, 2000b, Phys. Rev. A **61**, 010302(R).

van Loock, P., and S. L. Braunstein, 2001a, Phys. Rev. A **63**, 022106.

van Loock, P., and S. L. Braunstein, 2001b, Phys. Rev. Lett. **87**, 247901.

van Loock, P., and S. L. Braunstein, 2003, in *Quantum Information with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati (Kluwer Academic, Dordrecht), p. 111.

van Loock, P., S. L. Braunstein, and H. J. Kimble, 2000, Phys. Rev. A **62**, 022309.

van Loock, P., and A. Furusawa, 2003, Phys. Rev. A **67**, 052315.

van Loock, P., and N. Lütkenhaus, 2004, Phys. Rev. A **69**, 012302.

Vidal, G., and R. F. Werner, 2002, Phys. Rev. A **65**, 032314.

Vukics, A., J. Janszky, and T. Kobayashi, 2002, Phys. Rev. A **66**, 023809.

Walls, D. F., and G. J. Milburn, 1994, *Quantum Optics* (Springer-Verlag, Berlin).

Weinfurter, H., 1998, private communication.

Wenger, J., M. Hafezi, and F. Grosshans, 2003, Phys. Rev. A **67**, 012105.

Werner, R. F., 1989, Phys. Rev. A **40**, 4277.

Werner, R. F., 1998, Phys. Rev. A **58**, 1827.

Werner, R. F., and M. M. Wolf, 2001, Phys. Rev. Lett. **86**, 3658.

Weyl, H., 1950, *The Theory of Groups and Quantum Mechanics* (Dover, New York).

Wigner, E. P., 1932, Phys. Rev. **40**, 749.

Wilson, D., H. Jeong, and M. S. Kim, 2002, J. Mod. Opt. **49**, 851.

Wiseman, H. M., and J. A. Vaccaro, 2001, Phys. Rev. Lett. **87**, 240402.

Wolf, M. M., J. Eisert, and M. B. Plenio, 2003, Phys. Rev. Lett. **90**, 047904.

Wolf, M. M., G. Giedke, O. Krüger, R. F. Werner, and J. I. Cirac, 2004, Phys. Rev. A **69**, 052320.

Wootters, W. K., 1998, Phys. Rev. Lett. **80**, 2245.

Wootters, W. K., and W. H. Zurek, 1982, Nature (London) **299**, 802.

Wu, L.-A., H. J. Kimble, J. L. Hall, and H. Wu, 1986, Phys. Rev. Lett. **57**, 2520.

Yamamoto, Y., and H. A. Haus, 1986, Rev. Mod. Phys. **58**, 1001.

Yao, A. C.-C., 1995, in *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA), p. 352.

Yonezawa, H., T. Aoki, and A. Furusawa, 2004, Nature (London) **431**, 430.

Yuen, H. P., and M. Ozawa, 1993, Phys. Rev. Lett. **70**, 363.

Yuen, H. P., and J. H. Shapiro, 1980, IEEE Trans. Inf. Theory **26**, 78.

Yurke, B., M. Hillery, and D. Stoler, 1999, Phys. Rev. A **60**, 3444.

Zhang, J., and K. Peng, 2000, Phys. Rev. A **62**, 064302.

Zhang, T. C., K. W. Goh, C. W. Chou, P. Lodahl, and H. J. Kimble, 2003, Phys. Rev. A **67**, 033802.

Zukowski, M., A. Zeilinger, M. A. Horne, and A. K. Ekert, 1993, Phys. Rev. Lett. **71**, 4287.